Survey on Blockchain for Internet of Things

Hongwen Hui, Xingshuo An, Haoyu Wang, Weijia Ju, Huixuan Yang, Hongjie Gao, and Fuhong Lin*
Department of Computer and Communication Engineering
University of Science and Technology Beijing

Abstract

The Internet of Things (IoT) refers to a network concept that extends its clients to any item for information exchange and communication. Blockchain is a new application paradigm of distributed data storage, point-to-point transmission, consensus mechanism, asymmetric encryption, intelligent contract and other computer technologies. Blockchain technology for IoT has been a hot topic in academia and industry. This paper mainly summarizes the main existing research results of the challenges faced by IoT, the technical characteristics of blockchain, the advantages of applying blockchain technology in IoT, security challenges (key management, intrusion detection, access control, privacy protection) and the technology to deal with them. Finally, the prospect of this industry would be summarized and discussed. On the basis of this study, we hope to put forward suggestions and provide references for future research orientation.

Keywords: Internet of Things (IoT); blockchain; intrusion detection; access control

1 Introduction

The IoT realizes the digitization of the real world. And it has a wide range of applications, mainly including the following fields: transportation and logistics, industrial manufacturing, health and healthcare, intelligent environment (home, office and factory), personal and social fields, etc. IoT, with a very broad market and application prospect, also has attracted a lot of attention from the academic circle [24,33,77]. In particular, the rapid development of the IoT will promote the progress of smart cities [95]. Blockchain is the underlying technology behind the cryptocurrency such as bitcoin, since the advent of blockchain technology [71] has attracted worldwide academic attention and research due to its unique technical characteristics. However, to this day, blockchain technology is primarily used for the transaction of the bitcoin in the world, and there are few other application fields except for that [1]. Most scholars only focus on theoretical research of blockchain technology. In the development plan of our country, we also attach great importance to the research on blockchain technology. In particular, the famous "Beihang chain", established by the team led by professor Cai from Beihang University, is the world leading-edge research in relevant fields.

However, the accumulation of data from IoT devices poses significant challenges for abundant data storage [61], network latency [99], user query, the finding of appropriate services [63], etc. Blockchain technology, with its functions of authentication, auditability and accountability, is a very promising network integration technology. Blockchain technology has the key characteristics of decentralization, traceability, anonymity and auditability [119]. One of the technological advantages of blockchain is that it can work in a distributed environment, which is attributable to the combination of three theories (Byzantine fault tolerance, free money theory, and information asymmetry theory) and five technologies (P2P network technology, timestamp, asymmetric encryption, intelligent contracts, and database technology). Many scholars began to study the advantages of blockchain technology to solve the challenges

Journal of Internet Services and Information Security (JISIS), volume: 9, number: 2 (May 2019), pp. 1-30

*Corresponding author: Department of Computer and Communication Engineering, University of Science and Technology Beijing, 30 Xueyuan Street, Haidian District, Beijing 100083, P. R. China, Email: FHLin@ustb.edu.cn

in IoT, and have made many achievements. For example, the researchers proposed a variety of new IoT architectures combined with the technical characteristics of the blockchain [23,56,62,81,82], mainly including the application of the intelligent contract [81], distributed technology [82] and the data integrity of blockchain [62]. This paper [28] holds the view that blockchain is a kind of state that can establish mutual trust without third-party supervision. As the basis of the second-generation Internet "value Internet" protocol, its status is comparable to that of the present the HTTP protocol. In the era of the IoT, we firmly believe that blockchain technology will also play a more important role in our daily life.

The advantages of blockchain are consolidating the IoT. However, there are many security problems in IoT that need to be solved urgently [57, 59, 91]. Firstly, authentication is a very important part of the IoT. For example, authentication becomes a necessary factor when applications can control building access and environmental control, or provide access to audio and video devices that may monitor users. But in some cases, even the most basic authentication was also omitted. Authentication key management in IoT is a key link in the encryption process. The introduction of blockchain technology provides a new idea for key management in IoT. Secondly, because of the massive heterogeneous devices in IoT, there are many weak nodes in the network. Intruders can easily invade these weak nodes to achieve illegal purposes. Blockchain-based intrusion detection technology can effectively identify intrusions in IoT, which is an important security measure in IoT. Thirdly, the number of users in IoT is large, especially when combined with edge computing, the network level is relatively complex, and the management of access rights to the system is a problem to be solved in IoT. Traditional access control has the characteristics of poor real-time dynamic and vulnerable to damage. The combination of blockchain and access control enhances the anonymity and operability of access control in IoT, which is an important research direction in IoT [29]. Finally, privacy disclosure has always been an important security risk in IoT. Whether in the perception layer, transmission layer and processing layer of the IoT, users' privacy leakage exists. The combination of blockchains and privacy protection provides a more anonymous and real-time security service for the privacy protection of the IoT.

The structure of this paper is as follows, shown in Fig. 1 and Table 1. In the next section, we introduce the basic characteristics and core technologies of blockchain, including the cryptographic technology and consensus mechanism used in the existing blockchain platform. The application of blockchain technology in IoT will addressing related problems in IoT. In Section 3, the research results in this aspect are summarized. In Section 4, we mainly review the security threats faced by blockchain for IoT and the existing research result at present. Brief summary and prospect of the future research direction are reported in Section 5.

2 Blockchain technology

In 2008, Nakamoto [71] offered the conception of Bitcoin. After the official release of the Bitcoin in 2009, blockchain technology, as its underlying technology with digital cryptocurrency, has step into peoples life. At present, there is no exact definition about the blockchain. The blockchain is built on the Internet. Based on the blockchain technology, a distributed peer-to-peer decentralized shared ledger is formed, and the formation of a data structure is connected in chronological order with a series of data blocks. It guarantees the intruder cant distort the transaction data protected by cryptography.

According to participants, the blockchain is partitioned into three types: public blockchains, private blockchains and consortium blockchains. The public chain was also called the permissionless blockchain, and it runs decentralized and distributed completely on the Internet. Peters et al. [75] pointed that the public chain is for publication, and any user node has access to the network at will without any authorization, and the node can send transactions or even participate in a consensus process for account-

Table 1: Summary advantages and security challenges of Blockchain in IoT

Content	References	Characteristic description
Blockchain technology	[6, 12, 14, 46, 50, 51, 69, 71, 73, 75, 80, 102]	[71] put forward the concept of bitcoin and made the blockchain step into peoples horizons; [75] introduced the workflow of blockchain; [73, 102] introduced the characteristics of decentralization and tamper resistance of blockchain
Blockchain-based new architecture	[13, 15, 22, 25, 36, 44, 55, 78, 96, 109, 110]	[78] presented three possible architectures of blockchain applications for the IoT front-end; [110] proposed a blockchain-based framework for updating IoT firmware devices; [36] proposed a traceability system architecture
Blockchain-based resource management	[4, 17, 21, 38, 43, 64, 86, 88, 93, 104, 108]	[108] convenient, [86,93] the limited resource and lower computation of mobile devices, [104] profit maximize
Blockchain-based data management	[37, 42, 45, 74]	[37, 74] Using the decentralization of blockchain technology to solve the problem of data sharing in IoT; [42, 45] the data in the blockchain technology cannot be easily tampered with, and the data Time-sensitive features enable traceability and auditability of data.
Blockchain-based key management	[7, 18, 32, 34, 54, 65, 94, 111, 116, 117, 120]	[34, 54, 111, 120] proposed a blockchain-based key management scheme in ITS, IoT device, healthcare and NDN; [18] proposed a blockchain-based key management system using anti-quantum cryptosystem
Blockchain-based intrusion detection	[2, 5, 9–11, 20, 35, 67, 68, 79, 97, 103]	[68] elaborated the possibility of combing blockchain technology and IDS; [79] and [11] focused on the trust computing and vulnerability scanning of blockchain-based IDS, respectively
Blockchain-based access control	[16, 19, 25, 40, 70, 72, 85, 92, 98, 101, 114, 122, 123]	[19, 25, 70, 72, 85, 92, 122, 123] use blockchain technology to construct a new access control model or system; [16, 40, 98, 101, 114] use blockchain technology combined with existing access control models to form blocks with IoT access control model featuring chain technology.
Blockchain-based Privacy-Preserving	[3, 26, 27, 30, 31, 41, 47–49, 52, 60, 83, 89, 90, 100, 105–107, 112, 113, 118, 121]	[100] information safety; [90] user's sensitive information; [31] data maintenance; [105] remote attestation security; [83] personal monitoring

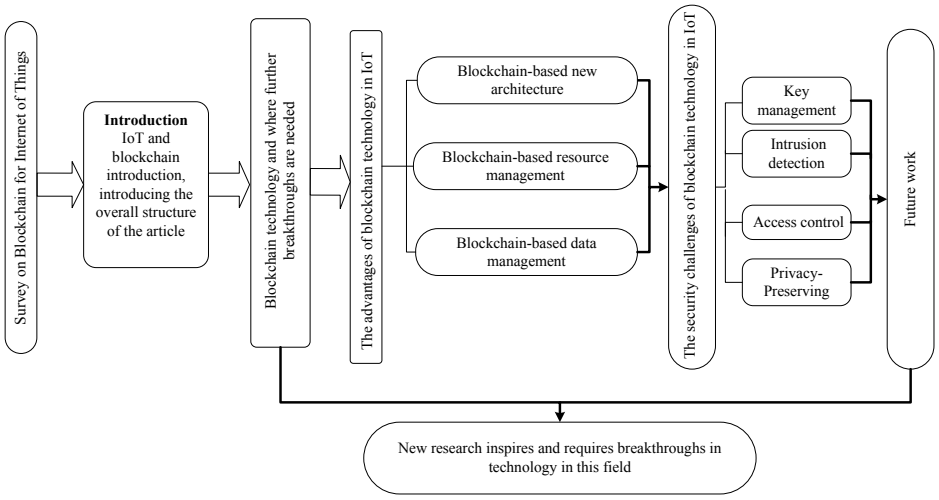


Fig. 1: Schematic map of the paper

ing. The mutual trust between two nodes is not required, because the network verifies the information through the principle of cryptography and the incentive mechanism of economics to ensure that the information cannot be tamper and reach a consensus at last. At present, the most representative of the public blockchain is Bitcoin and Ethereum. The consortium chain is also called the permission blockchain, which is a public ledger system initiated by multiple related organizations. Compared with the public blockchain, it has a clear access mechanism. Users need to register and be authorized when they enter into the network, and the reading and writing permissions of the data on the chain need to be carried out in accordance with the rules established by the alliance. The private chain is only used within the organization. It is the privatization of the public blockchain. The reading and writing of the data on the chain and the permission of charging to an account need to be carried out according to the rules of the organization.

Wang et al. [102] suggested that each new transaction is broadcasted to the entire network. The node that wants to participate in the accounting will verify the transaction information according to the signature attached to the transaction, and then package the data according to certain encryption rules. In the block, a node will obtain the permission of charging to an account by solving the consensus problem, and new block will be broadcasted in the network and added to the main chain. In the following the features of the blockchain and key technologies will be further explained.

2.1 Characteristics of blockchain

- **Decentralization**: Panarello et al. [73] believed that in the blockchain, the generation, verification, storage and transmission of data do not depend on any centralized organization, and each node has the same rights and obligations in the whole network and has the same status. Decentralization can also be understood, on the other hand, multi-centered. In the distributed system of blockchain, each node is highly autonomous, and each node can be regarded as a small center. Its outstanding advantage is when some nodes break down or even become infected and worsen, the blockchain can still keep working. This feature makes the blockchain extremely suitable for the distribution of IoT, because the number of connected devices in IoT keeps growing in recent years, which means that the amount of data processed at the same time can be significant. And Wang et al. [102] indicated that decentralized processing is very important and can reduce the risk of a single point

of failure.

- **Tamper-proof**: After data block formed, the node will broadcast it to the whole network system. All other nodes will verify, if the results of verification are right, the contents of the ledger would get updated correspondingly, so that the local ledger is consistent with the consensus version on the network. Any change of data in block within a certain rule and period is not achievable. A large number of terminal devices are deployed in IoT, and Alsaadi et al. [6] pointed that an intruder can acquire data within a node through a physical capture and further uses the information to masquerade as a legitimate node to modify the transmitted data content or to attack other nodes. The tamper-proof feature of the blockchain can overcome this shortcoming of IoT and reinforce the protection for data.

- **Self-trust**: Each node of the blockchain can exchange information without mutual trust. Because each node has a same content of ledger which is open and transparent in the blockchain network, this decentralized deployment is complemented by cryptography and an open consensus mechanism to ensure the data on blockchain has a strong credibility, and any behavior of the node is expected.

- **Anonymity**:In the blockchain, transaction information is on-limits and diaphanous, the identity messages of users are anonymous. Each user has a couple of keys (public key and private key). The user applies the private key to sign the message, other users verify the information by sender's public key, and no one can infer the private key via public key, which guarantees the safety of the data and the privacy of the user and is extremely attractive for applications and service in IoT that require assure the confidentiality and privacy.

2.2 Key technology

The integrity, tamper resistance and traceability of data in the blockchain are realized by cryptography technology. The confidence between different nodes and the consistency of the ledger content of each node are achieved by the consensus mechanism.

2.2.1 Cryptography technology

There are three common techniques in cryptography are mainly used in the blockchain: asymmetric encryption, hash algorithms, and Merkle tree.

- **Asymmetric encryption**: The general encryption algorithm has two types: symmetric encryption and asymmetric encryption. The main application in the blockchain is the asymmetric encryption algorithm, which usually refers to that when the information is encrypted and decoded, users make use of two asymmetric ciphers, owner can publish the public key, and the other is kept out of the secret. While sending a message, you can apply one key to encrypt the messages. To unlock it, users must use the other one. The encryption technology in the blockchain is mainly used for the following aspect, such as information encryption, login authentication, and digital signature and so on. In information encryption, when the sender (A) sends the information to the accepter (B), it applies B's public key to encrypt the information; when B receives the information, it decrypts the data with its own private key. Apply own private key to encrypt the message for sender, and use senders public key to decrypt the information to confirm that the message was indeed sent by the sender for receiver in digital signature.

- **Hash algorithms**: The hash algorithm converts an arbitrary length binary numeral into a binary digit of a fixed length which is referred to hash number. It represents a significant change in the hash number when there is a slight difference in the input, and it is almost impossible to find a different input for the same hash value.

  In the blockchain, the block includes block header and block body. The previous blocks hash number and a hash number obtained by the Merkle tree of all transaction data of the current block are covered in the block header, so that after the block is connected by chronological order, each block is associated with the two blocks, before and after. If the intruder wants to tamper with a transaction, it will cause the hash value of this block to change. In order to admit that the tampering transaction is valid by other nodes, it needs to calculate all the block from the tampering block to current block and acknowledged by other nodes, which is almost impossible to achieve.

- **Merkle tree**: Merkle [69] proposed that the Merkle tree is a data structure with tree-shaped, and its nodes are usually called Merkle Hash Tree because they are all composed of hash values. Each transaction in the blockchain is converted to a hash value, and these hash values are hashed from the bottom to the top according to a binary tree or a multi-fork tree, resulting in a unique Merkle root value.

Wang et al. [102] proposed that IoT can communicate with Ad Hoc protocol, and the message will be transmitted to the destination hop by hop which gives the intruder opportunity to tamper with the data. IoT could use blockchain technology to solve some problems. The data about blockchain validates it according to the previous blocks and through these cryptographic techniques, and the blockchain can ensure that the data is irreversible and tamper-resistant in IoT without a central server.

2.2.2 Consensus mechanism

A core notion of the blockchain mentioned above is decentralization, the nodes are equal to each other, which requires a mechanism to ensure that all nodes can cooperate effectively. Such a mechanism in the blockchain is called a consensus mechanism whose essence is an algorithm for establishing trust between each nodes. The consensus mechanism first appeared in distributed systems which exists before the emergence of blockchain technology. At present, the common consensus mechanism in blockchain covers PoW (Proof of work) [71], PoS (proof of stake) [46], Casper [12] DPoS (Delegated proof of stake) [51] and PBFT (Practical Byzantine Fault Tolerance) [14].

The main feature of the PoW is that the node completes a certain difficult work to get a result, and the verifier can easily check the result to verify if the node has completed the corresponding work, because monitoring the overall process of the work is far less directly than verifying the result which is more efficient. PoS is mainly about that the difficulty of generating a block that is related to the size of the shares the nodes own in the whole network; DPoS is an effective supplement to the PoS, and the node can become a shareholder with a certain amount of money in this algorithm. The amount of money also determines the owners influence. Each shareholder can give his voting rights to a representative. Rifi et al. [80] presented that the result will be irreversible if votes are more than 51

2.2.3 The technological challenges of blockchain

Based on the existing research conclusions, there are two technical bottlenecks in the current blockchain technology, which seriously limit its wide application. One is the regulatory security problem. In spite of the decentralization of the blockchain that makes it possible to avoid many problems in the traditional centralized system structure, it also causes trouble about the lack of effective management and monitoring of the blockchain network. This is also the main reason why government departments and

Table 2: Performance comparison of blockchain consensus mechanism

Property / Mechanism	P1	P2	P3	P4	P5	P6
PoW	$\surd(\frac{1}{2})$	Lowest	All nodes	Highest	Highest	slow(minutes)
PoS	$\surd(\frac{1}{3})$	Low	All nodes	High	Low	slow(minutes)
Casper	$\surd(\frac{1}{3})$	High	Partical nodes	High	Low	fast(second)
DPoS	$\surd$	High	Partical nodes	Low	Low	fast (second)
PBFT	$\surd(\frac{1}{3})$	High	Partical nodes	Low	Low	fast(second)

Remark: where P1, P2, P3, P4 and P5 represent fault tolerance, consensus efficiency, which node can participate in the consensus, degree of decentralization, energy dissipation and time to generate a block, respectively.

some enterprises hold a negative attitude towards blockchain technology. The other one is the transaction with time delay. The block chain packages transaction data into the block and obtains Merkle tree through multi-level hash operation to ensure data integrity and non-tampering characteristics. It leads to extremely decrease the transactions velocity. For example, it takes 10 minutes to initially complete a transaction in PoW mechanism, about an hour for six blocks to be generated and confirmed [109].

In addition, because blockchain has realized the distributed storage, which has great advantages when encounters an application scenario with massive data, such as IoT. In order to enable blockchain technology to play an important role in IoT, we must solve regulatory security problem and transaction time delay problem of blockchain at first. This is the focus of our further research. Any technology will go through many twists and turns from being proposed to being widely used. In conclusion, we are optimistic about the improvement of blockchain technology and its prospects for widespread use in IoT.

3 The advantages of blockchain technology in IoT

Many scholars have applied the technical characteristics of blockchain to solve the corresponding problems in IoT, and made many significant achievements. In this section, we mainly present the latest research results in three aspects: new architecture, data management and resource management in IoT based on blockchain technology.

3.1 Blockchain-based new architecture

In recent years, the IoT has drawn wide attention from the industry and scholars, and has developed rapidly due to the proliferation of smart devices. At present, IoT devices have been widely used in smart home, automobile, aerospace and other fields [44]. The IoT is the bridge that integrates the real world with the Internet, thus facilitating data sharing among smart devices [25]. At the same time, in the practical application scenarios of the IoT, there are many challenges in hardware devices, data storage, network monitoring and other aspects. For example, IoT networks generate large amounts of data, as a result, the monitoring of networks and the transmission of data packets from the IoT user end to the server face great challenges [13]. Li et al. [55] emphasized that the existing identity authentication of IoT devices mainly relies on the CA server as an intermediary, which is prone to machine failure and service failure.

Blockchain as a decentralized way of trading, which has aroused the intense interest and the widespread attention of the scholars. Blockchain has the core attributes of anonymity, security, data integrity and

distributed storage [109]. Therefore, many scholars have proposed that these advantages of blockchain technology will be used to solve the existing problems in IoT. In the next section, we mainly reviews the latest research results by using blockchain to propose a new architecture to solve the problem of IoT.

Pustišek et al. [78] presented three possible architectures of blockchain applications for the IoT front-end and proprietary communication architecture between IoT devices and remote blockchain clients. The aim is further reduce network traffic, and also hoped that blockchain can improve the development of mobile technologies with low-power, low-bitrate. At present, this assumption is only limited to experimental simulation and has not been realized in the industrial IoT. Özyılma et al. [22] established a universal IoT gateway based on blockchain technology for better management of a large number of IoT devices. Taking full advantage of the technological advantages of blockchain, the blockchain-based a new IoT back end platform-has built that is resistant to distributed denial of service (DDOS) that attacks a distributed storage data. Yohan et al. [110] proposed a blockchain-based framework for updating IoT firmware devices. This framework not only provides security verification for firmware issued by device manufacturers, but also maintains the integrity of distributed firmware to terminal devices.

The combination of the IoT and the blockchain technology will generate huge application prospects and provide solutions to many existing challenges in IoT. Teslya et al. [96] developed a new architecture that combines Smart-M3 information sharing platform and blockchain platform. The main advantage of this architecture is to use the smart contract of blockchain to complete the information exchange among smart space components. Profit is the driving force of economic prosperity and incentive mechanism is the core of blockchain technology. Cebe et al. [15] builted a new internet-oriented incentive platform to motivate and attract detectors to participate in backtracking intrusion detection and contributed their detection results by using the incentive mechanism of blockchain technology. Consumers on the platform are able to proactively maintain the normal operation of the platform, because the mechanism can give them benefits, similar to mining in Bitcoin. Using blockchain technology for traceability, Hong et al. [36] proposed a traceable system architecture to solve the quality problems of agricultural products on the market, which can trace a series of information such as the origin and distributor of a certain commodity in real time.

3.2 Blockchain-based resource management

With the progress of science and the development of society, in many scenarios (such as Smart City, Smart Factory, Smart Manufacturing, Smart Retail, and so on), edge computing is mainly used in IoT, which is used to provides the computing power, which is near the data source [88]. Therefore, the solutions of resource management in edge computing can also solve the problem of resource management in IoT to some extent.

Due to the limited resource and lower computation of the mobile devices which is used to store resource [86], in order to achieve the resource management in the mining process by blockchain, Xiong et al. [104] proposed one way that offloads some of the mining process to a third party, which is known as edge computing service provider. As for this, through a two-stage Stackelberg game it maximizes the profit between the edge computing service provider and the individual utilities of the miners. Luong et al. [17], after deep learning, developed an optimal auction for the edge resource management. Furthermore, it constructed a multi-layer neural network architecture, which is based on an analytical solution of the optimal auction.

The management of resources has relatively high requirements for equipment carrying resources. For this reason, it is convenient to manage resources, and many lectures are devoted to study the equipment on the basis of that characteristic, in which the scholars improved resource management by solving equipment problems. With an amount of data produced exponentially by the IoT devices due to the growth of the technologies, it needs a security infrastructure to store and process data. But the limited

resource of the low-power [108] IoT devices cant bear them. To solve the forementioned problem, Özyılma et al. [22], using the decentralized and trustless architecture properties of blockchain, proposed an IoT gateway which can be seen as a blockchain node and an event-based messaging mechanism to the end-to-end IoT devices. Moreover, when the extensive devices were connected together, it may results the limitation for current model of server. Based on this, Hun et al. [38] built an IoT system using blockchain, by which the server-client [21] can control and configure IoT devices.

In addition, to defend against the hackers intrusion through the leakage of the IoT devices, the software and hardware located on the equipment should be updated for a temporary period. To achieve an benefitting effects, Yohan et al. [110] proposed a firmware update framework in the light of blockchain technology for IoT devices [93]. The firmware produced by the manufacturer will have a secure verification through the framework. Alblooshi et al. [4] offered a trusted ownership management for medical IoT (MIoT) devices on the basis of Ethereum blockchain.

For some specific application domains, smart grid [43] for instance, Lombardi et al. [64], in order to resolve the phenomenon that security threads may occur by introducing transactive energy into the smart grid, introduced an infrastructure that based on blockchain and smart contracts to support reliable and cost-effective transactive energy.

3.3 Blockchain-based data management

With the continuous development of the IoT technology, more and more IoT terminal devices with different shapes and functions are connected to the IoT network, and these devices also keep collecting data all the time, thus generating Massive Data. The phenomenon shows that the supervision of the entire IoT state and the transmission of IoT terminal data to the server center will greatly increase the communication overhead; at the same time, the massive data will bring some economic benefits for people, and it is dedicated to connecting various distributed. The IoT data sharing on exchange platform emerged as the times require, which puts higher requirements on IoT data exchange - decentralized interaction and fidelity of data sources. The emergence of blockchain technology has made it possible to solve the above problems. For the consensus mechanism in the blockchain, the data can not be tampered, and the timing features effectively solve the problems of data sharing in IoT [37, 74] and data traceability [36, 42].

However, due to the excessive amount of data stored in IoT network database, if you want to obtain high-efficiency IoT status monitoring performance, you are required to possess a powerful server, which undoubtedly increases the cost of network service providers. Casado-Vara et al. [13] proposed a novel closed-loop control system with adaptive and accelerated search model to promote the monitoring performance of the IoT, especially the IoT network based on blockchain. The nonlinear control model proposed by them adopts the idea of queuing theory and forms a new method for calculating the optimum value of blocks in the mining sequence. At the same time, they designed an accelerated search system that uses hash-maps to make the regulatory process more faster, more adaptable and more robust.

In order to deal with the problem of excessive concentration of data on the IoT, blockchain is gradually used as a decentralized storage solution. However, due to the low storage capacity of IoT devices, traditional lightweight IoT devices cannot store all blockchains. To this end, Kim et al. [45] proposed the Storage Compression Consistency (SCC) algorithm. The core idea of the algorithm is to compress a blockchain in every device to ensure storage capacity. When the IoT device does not have enough storage space, it is convenient to use the SCC algorithm to compress the blockchain, which reduces the storage space by 63% compared with the existing solution.

In addressing IoT data sharing, Papadodimas et al. [74] proposed a distributed data application(Dapp) which shares date by using blockchain characteristics and exchanges date with IoT sensors. The applications they proposed combine the characteristics of blockchain and the IoT environment. The above applications interoperate through the smart contract on Ethereum, a platform for sharing (purchasing and

peddling) IoT air sensor quality measurement and control. Huang et al. [37] proposed a distributed solution by using blockchain for trusted exchange of IoT data. The program was designed and implemented on the basis of Ethereum and smart contract prototype system by analyzing the three main demand indicators in IoT data exchange.

In terms of IoT data traceability, Lin et al. [42] proposed a credible, self-organizing and open eco-food traceability system based on blockchain and IoT technologies. The system can involve all parties involved in an intelligent agro-ecosystem, even if there is no trust relationship among them. At the same time, they use smart contract technology to help law enforcement find problems and handle them in a timely manner. Hong et al. [36] proposed a traceability system for agricultural products proposed, which utilizes batch technology and blockchain characteristics. The system is reliable, credible and scalable by using the consortium blockchain as the underlying network and the IoT terminal as the recorder.

Many research results show that the blockchain technology will have a huge application market. In particular, the blockchain technology combined with the IoT has brought new impetus to the development of the IoT and will bring about great social and industrial changes. Meanwhile, blockchain oriented to the IoT will also face some new technical challenges, especially security issues. In the next section, we will review the latest research achievements of scholars related to safety issues.

4 The security challenges of blockchain technology in IoT

The development of technology has led to the emergence of many security issues in IoT, such as key management, intrusion detection, access control, and privacy protection. The blockchain is considered to be the possible method for solving the above security problems because of its anonymization, distribution, and other characteristics. The current research of these security problems are summarized in this section as follows.

4.1 Blockchain-based key management

The rapid development of IoT and the valuable data generated by IoT devices lead to a higher demand for data security especially for the key management. However, the current key management strategies cannot be applied to the IoT devices with limited resource. Therefore, it is essential to study key management with respect to security problems in IoT to ensure the safety of users' data.

4.1.1 Blockchain-based key management case

With the rapid development of mobile technology, the number of IoT devices has proliferated. The distributed network adopted by IoT devices has the characteristics of topological dynamics, centerless distribution, and high dynamics of node membership status, which makes the key management more complicated. Key management mainly provides services such as key generation, key distribution and key update for all legal members of the group. Currently, sub-key management mainly provides services for all legal members of the group, the main process architecture as shown in Fig. 2. In addition, there are two complementary classes of key management schemes in distributed networks: centralized key management technology and distributed key management technology. The centralized key management scheme, highly dependent on the key management center, is subject to significantly delay in cross-domain key transmission and single point of failure. Hence, the key management is difficult to adapt to the highly dynamic distributed network environment [32]. As for distributed key management protocols, many related researches in recent years. Among them, common distributed key agreement protocols include

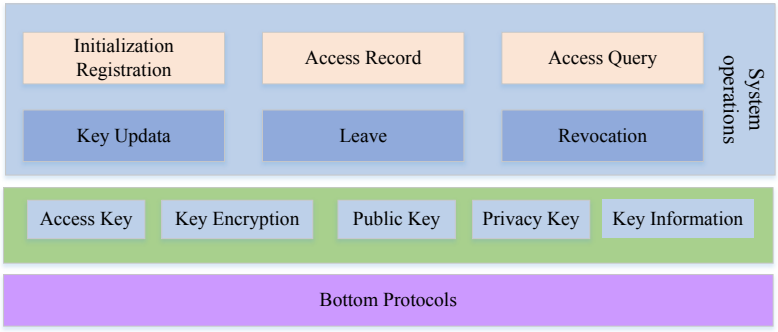


Fig. 2: Blockchain-based key management framework

BD (burmester-desmedt) protocol [120], STR protocol, TGDH (Tree-based group diffie-Hellman) protocol [116] and so on. The BD protocol communication is large while the computational is small. The calculation of the extended and the traffic of the TGDH protocol is relatively small, and the key storage is large.

Yu et al. [111] proposed a wireless network multicast establishment protocol with anonymous members, in which the key transmission is constructed without leakage the information of the receiver. However, this protocol scheme lacks the authentication and key confirmation mechanism and cannot provide a forward direction. He et al. [34] designed an efficient key exchange handshake protocol in the mobile environment, in which the management mechanism is complex and not suitable for dynamic group networks. The application of the above protocol scheme in dynamic group communication with dynamic changes of group members is not effective. Therefore, it is necessary to design a centerless key management scheme in a dynamic distributed network environment.

In recent years, blockchain has been gradually applied to IoT to protect users' data. Lei et al. [54] presented a key management framework in heterogeneous networks. Intelligent Transportation Systems (ITS) is composed of two parts. The first part is a new network topology based on a decentralized blockchain structure; the second part aims to reduce the key transmission time during the handover of the vehicle based on a dynamic transaction collection period. Since bitcoin is an open source payment system, there are several key management techniques, such as stealth address technology proposed to enhance bitcoin in these years. The major trend in blockchain systems is the use of stealth address technology to make different payments for the same payee. The common feature of the techniques is that it allows the public key to be derived independently of the private key. Courtois et al. [18] summarized the specification of these technologies and compared all the major variants used in the actual systems. These techniques can be designed based on two different ECC arithmetic attributes and the way they are combined. Then, they proposed a new stealth address method to improve the robustness for different attacks. In IoT environment, it is preferable that the cryptographic material has good freshness. However, an efficient scheme using a "short" public key is not yet available. Tedeschi et al. [94] solves this problem by considering a new key-negotiation method integrating with the Blockchain technology.

Besides, healthcare is another important application of blockchains. Since the healthcare system involves a large amount of private information, certain security scheme must be established to protect the private data in the healthcare blockchain. It is well known that the core of the security mechanism is key management scheme. Hence, the appropriate key management scheme must be designed. Zhao et al. [117] designed a lightweight backup and recovery scheme by using the body sensor networks for key management of the healthy blockchains. The analysis shows that the proposed scheme has higher

security and performance. Lou et al. [65] proposed a blockchain-based key management method in Named Data Networking (NDN) to solve the problem of the lack of the mutual trust among different sites. In this research, all site nodes form a chain of licensed blocks for storing the public key hashes to guarantee the authenticity. Meanwhile, the aims of the proxy gateway in authentication is to reduce the frequent communication between routers and blockchains. The results show that the proposed scheme can support fewer verification numbers and higher verification efficiency.

Classic digital signature algorithm has been applied to the cryptocurrency, such as Bitcoin and Ethereum. An et al. [7] proposed a blockchain-based key management scheme using anti-quantum cryptosystem, which can resist the attacks of quantum adversaries and ensure long-term security.

Ma et al. [66] presented a blockchain-based distributed key management architecture, which not only complicated computing functions but also reduced the latency and multi-blockchains running in the cloud. The proposed architecture uses the blockchain technology to protect the decentralized, fine-grained auditability, high scalability, scalability requirements and the privacy protection principles for the hierarchical access control in IoT. The results reveals that the multi-block chain structure improves the system performance. As the size of the network increases, the scalability also improved correspondingly.

4.1.2 Future work

The blockchain was first proposed as a basic supporting technology of Bitcoin, which built the block-chained data structures and realized data sharing, auditing, management, and collective maintenance for all members in the distributed network. The data to be transmitted is encapsulated into a block and is broadcasted to the network for the collective mining process of all members to realize the synchronization of the block data throughout the network. If the message is authenticated, the new block is appended to the local ledger. The data to be delivered can be directly sent to the destination member instead of passing the data through the central manager to maintain the block data backup, which can facilitate the spread of cross-domain information and ensure the integrity and the reliability of the transmitted data. The distributed structure based on blockchain network has better robustness in dealing with the single point of failure. Therefore, the blockchain can be considered as a solution to key management problems. At present, the research of blockchain-based key management in IoT is still in its infancy. In the future, we will design or consider the efficient hash function to promote the persistence of the blockchain-based key management in IoT. Besides, to overcome the difficulty of implementing key management and excessive communication overhead while keeping the same level of anonymity for the IoT devices with limited computation resource, we will design a new blockchain-based key management and the transmission process. Furthermore, since the current research achieves the balance among the energy consumption, bandwidth usage and communication latency, future research in this area aims to study the security analysis of the current works and design an evaluating system to analysis the performances of bandwidth, energy and latency requirements. Meanwhile, we will consider the efficient storage of key data schemes and retrieval of blockchain.

4.2 Blockchain-based intrusion detection

In 1980, Anderson [9] proposed the concept of intrusion detection for the first time. In 1990, Heberlein et al. [35] introduced it into the network system. Intrusion detection system (IDS) is a kind of security mechanism for dynamic monitoring and prevention of system intrusion [8, 58]. It mainly detects the present intrusion of system users and attempts of intruders outside the system to make use of the system's security defects to invade the system by monitoring the network, system state, behavior and system usage.

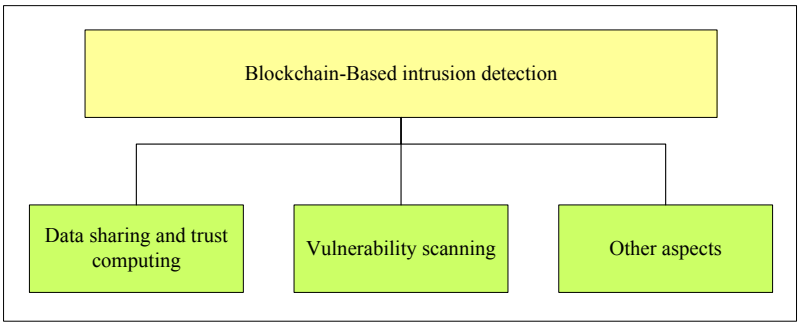


Fig. 3: Application of blockchain-based intrusion detection in IoT

4.2.1 Research status of blockchain-based IDS

Blockchain technology has a positive impact on handling privacy issues caused by data exchange and inhibiting internal intrusion. With blockchain technology, the use of trusted third party can be avoided. The use of trusted third party is inevitable in traditional collaborative IDS. The distributed nature of blockchain allows the system to be immune to single point of failure. Many blockchain-based intrusion detection techniques have been proposed for many aspects of the IoT, as shown in Fig. 3.

Modern IDS must be based on the collaborative communication among distributed IDS, requiring extensive data sharing and trust computing among entities [20]. Meng et al. [68] elaborated the possibility of combining blockchain and IDS, and discussed the applicability of blockchain technology in solving data sharing and trust computing problems in the collaborative detection, and pointed out the direction of future work. Papadodimas et al. [74] proposed a distributed application based on blockchain. It combines blockchain with the IoT to share IoT sensor data. This application operated by smart contracts was used on Ethereum. Qu et al. [79] focused on the credibility verification method. In order to establish the relationship between the IoT and the blockchain with respect to device credibility verification, a framework with layers, intersect and self-organization blockchain structure was proposed. Agrawal et al. [2] studied the single point of failure in intrusion detection system and proposed a blockchain-based IoT security solution. This solution builds trust by using the immutability and decentralization of the blockchain. The authors also proposed a mechanism for establishing a system of continuous security without users intervention by continuously evaluating the legal existence of users in valid IoT-Zone.

The construction of the IoT requires the deployment of a large number of network connection objects. Although anti-virus software can be used to identify security problems before the installation of IoT devices, unidentified vulnerabilities and emerging vulnerabilities will still be exploited to launch malicious attacks. Blockchain technology provides an idea for solving these problems. Boudguiga et al. [11] studied the possibility of using blockchain to update software, patch vulnerabilities and prevent malicious attacks for IoT objects. They proposed a peer-to-peer mechanism that use blockchain infrastructure to facilitate updates between objects with limited access in IoT. Wu et al. [103] proposed SmartRetro, a blockchain-based incentive platform, to address the issue of exploiting new vulnerabilities in IoT systems to launch malicious attacks. It can motivate and attract more distributed detectors to participate in tracing back vulnerability detection and provide feedback. Through smart contract, consumers in the platform can obtain automatic security feedback of their IoT system. Kim et al. [44] studied the hacker risk of IoT devices and proposed a model to solve the security vulnerability of sensor multi-platform by using blockchain technology. This model is based on the blockchain core algorithm and uses blockchain technology to overcome the weaknesses of sensor devices such as automobiles, airplanes and closed-

circuit television.

There is still a lot of work to do to study the application of blockchain-based intrusion detection in other aspects. Tselios et al. [97] studied the elevated vulnerability of software-defined networks to specify the type of attacks, when it is used to support IoT-related networking elements, described the design principles of introducing blockchain paradigms, and proposed the reason for taking blockchain as an important security factor for solutions involving SDN and IoT. Alexopoulos et al. [5] studied the use of blockchain technology as a mechanism to improve collaborative intrusion detection system. It is believed that some characteristics of blockchain have a positive effect on the trust calculation of intrusion detection system. They introduced the way to use blockchain technology to protect the alarms generated by each node while ensuring that only trusted alarms are exchanged between the collaboration nodes, with the goal of improving the collaborative IDS. Banerjee et al. [10] proposed a security abstraction layer for IoT systems based on blockchain. This security layer can provide us with a logical view of the system containing trusted devices. The purpose of this security layer is to detect untrusted devices and isolate them, and to provide authorization, authentication and auditing services by blockchain and smart contract. Mendez et al. [67] introduced the application of blockchain in protecting the home edge network, and proposed the idea of using blockchain technology power by Ethereum to protect consumerhome-based IoT devices and their surrounding networks.

4.2.2 Challenge and future research

Research work on blockchain-based intrusion detection is limited. There are still many problems unsolved with intrusion detection, such as massive false alerts and overhead package with limited handling [68]. In an intrusion detection system, it is important to generate accurate alerts to inform administrators of anomalies in the network. How to ensure the exchange of trusted alarms between nodes is an important challenge. False alarms can reduce the detection performance and increase the burden of IDS. Overhead package will greatly reduce the detection performance of IDS. Overhead package that exceeds the IDS processing power can only be discarded. There are also some problems in the blockchain such as energy and cost, latency and complexity. These problems are hinderance to the development of blockchain-based intrusion detection technology, but they also provide the direction for future research.

The focus of future research efforts is to combine the advantages of blockchain and intrusion detection to solve the above problems and achieve a better performance and balance benefits and costs. The main applications of blockchain-based intrusion detection in the future will be in data sharing, trust computing, and alert exchange.

4.3 Blockchain-based access control

The IoT will generate a huge amount of data, which has a large amount of personal privacy. Once this private information is leaked, it will bring huge losses to users. As one of the cornerstone technologies of data protection, access control can ensure that data can only be accessed with the users permission. Therefore, research on the access control mechanism under the IoT has become one of the important part of the IoT security and privacy protection.

4.3.1 Access control architecture

When combining blockchain technology with the IoT, access control, as one of the key technologies for IoT data protection, has become a major combination. This section describes a new research method in the current research, namely, a novel distributed access control model architecture utilizing the characteristics of blockchain technology. By taking advantage of the features of blockchain, an access control

method based on transaction or smart contract is designed. The current related work is mainly stated as follows. Ma et al. [66] proposed a novel distributed key management architecture (BDKMA) based on blockchain which can solve the problem that centralized cloud center is not suitable for user privacy. Their scheme utilizes blockchain technology to meet the requirements of high audit accuracy and high applicability due to the wide distribution of devices in IoT, meanwhile ensure the privacy protection principle of layered access control. The author also designs the system operation method, and introduces different authorization allocation patterns and group access patterns to enhance the scalability. Le et al. [53] proposed CapChain a blockchain-based access control framework. The proposed architecture allows users to easily share and authorize their access rights meanwhile maintain maximum privacy in public places. In order to protect users' personal privacy information, they use the anonymous feature of blockchain technology to reduce the sensitivity of sensitive information, including user identity and related information. They also built a test platform as a proof of concept.

IoT devices are spread across all aspects of our daily lives, and the level of data privacy security of IoT devices determines whether they are widely used or not. Base on this, Pinno et al. [76] proposed a blockchain-based IoT access authorization architecture. Following the trend of the IoT, the architecture proposed by them is transparent to users, easy to operate and has very high scalability and fault tolerance. At the same time, due to the distributed characteristics, the model architecture also has high compatibility. Finally, they designed a way to establish security relationships among users, the devices, and the two, assigning attributes to those security relationships and authorizing them in access control. Z Zhang et al. [115] proposed a contract-based intelligent framework, which includes multiple access control contracts (ACCs), a judge contract (JC) and a registration contract (RC), thus enabling decentralized secure access control of IoT systems. ACC provides access control methods to achieve static and dynamic access verification based on preset policy methods by detecting the behavior of things. ACC, JC and RC implement access control based on Ethereum smart contract blockchain platform. By putting forward the dynamic access control scheme, Hwang et al. [39] solved the problem of the existing direct data communication access control method among devices, and solveed the dynamic environment problem of the IoT. They are trying to use blockchain to change the over-centralized access control method of the Internet of things into a semi-centralized or even decentralized method.

Through the research and analysis of the above documents, the framework idea formed by extracting the commonalities in their articles is the decentralized blockchain access control framework. The main idea of the design is that the resource owner first publishes the resource access control strategy. In the blockchain, when the resource requester wants to access the resource, the access control policy of the blockchain is directly directed, and the access control policy running in the blockchain determines whether to grant access. We have adjusted the process summarized in references [87] as shown in Fig. 4. The advantage is that it takes full advantage of the blockchain's computing and storage capabilities, and the control strategy is chained up to curb the ultra-authority behavior for auditing, but the shortcomings are also obvious. It is easy to record the policy and authority grants on the nodes of the blockchain. Attacker attack.

4.3.2 Access control system and model

Another major combination is to combine the current access control models such as RBAC, ABAC, etc. with blockchain technology, to make the blockchain a trusted entity of the access control model, and to design access control by using the characteristics of the blockchain. System or model would be presented in this section. The relevant work of the current research is stated as follows. Zyskind et al. [124] addressed the privacy concerns of using third-party application services and proposed a decentralized personal data management system making users effectively control and manage their personal information. Sedgewick et al. [85] demonstrated the way decentralized control mode of adaptive systems integrating

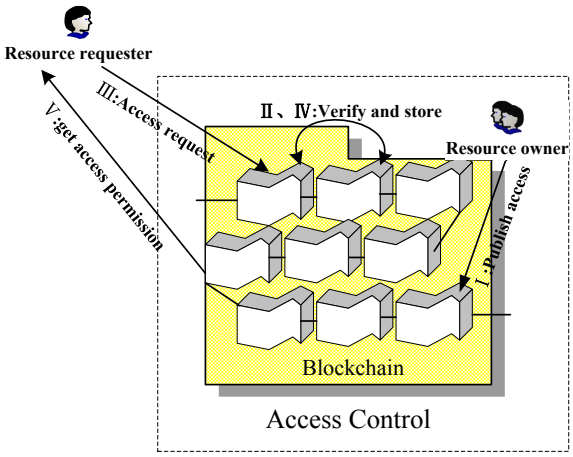


Fig. 4: Decentralized blockchain access control model

with adaptive systems can protect network nodes from attacks by constantly changing user permissions in access control policies. They also showed that licensed blockchains are better at keeping networks of IoT devices consistent even in the presence of malicious nodes. Sukhodolskiy et al. [92] provided the distributed ledger, on the basis of the blockchain, for storage in the cloud environment of untrusted data sets of the multi-user system prototype of access control. The system provides all meaningful security immutable log of events, such as key generation, access strategy allocation, change or cancel, access request. The author proposes a set of encryption protocols to ensure the privacy of encryption operations, which require a key or private key, and only the ciphertexts of hash codes can be transmitted through the blockchain ledger.

Due to the complexity and heterogeneity of the current IoT structure, it brings new security risks and challenges to its own system. Traditional access control technologies are no longer able to meet these emerging new risks and challenges, and are too central to be reliable. Therefore, the new access control model based on blockchain technology in the Internet of Things environment emerges at the historic moment. Ding et al. [25] proposed a new attribute-based IoT system access control scheme, which records the distribution of attributes to avoid single point of failure and data tampering by using blockchain technology. Mora et al. [70] proposed a case in which Blockchain promises to mediate security and privacy to overcome failures and Cyberinfrastructure hacking. They discussed how to start implementing an integrated blockchain control access system. Cruz et al. [19] proposed an RBAC by using smart contract (RBAC-SC), which uses Ethereum's intelligent contract technology to implement role-based access control across domains. RBAC-SC uses smart contracts and blockchain technology as a multifunctional infrastructure to build the trust and approval relationships that are essential in the RBAC model, to implement authentication protocols and to verify users' access to roles. Zhu et al. [123] proposed a novel transaction-based access control (TBAC) platform, which integrates the existing standard attribute based on access control (ABAC) model with the block chain technology, and constructs a standard attribute access control model based on the block chain technology. The proposed platform has four types of transactions and describes the TBAC access control process of subject registration, object hosting and publishing, access request and authorization with cryptocurrency cryptoscripts. Zhu et al. [122] presented a new digital asset management platform named dam-chain. The platform integrates the ABAC model and blockchain technology, emerging alongside transaction-based access control (TBAC). In the proposed platform, ABAC could provide an authorization mechanism that meets a variety of

requirements and could host digital assets into the blockchain, where transactions act as verifiable and traceable intermediaries for access requesters. The authors also proposed four types of transactions to describe TBAC access control procedures. Novo [72] proposed a new architecture for coordinating and balancing roles and permissions in IoT. The new architecture takes advantage of the distributed nature of blockchain technology to build a decentralized IoT access control system and evaluate it in real IoT cases.

In the field of intelligent medical care of the IoT, Zhang et al. [114] proposed an access control solution proposal for sharing electronic medical records (EMR) based on blockchain, which is called BBACS (block-based access control scheme). Unlike existing blockchain-oriented EMR access schemes, their access control models can cross the proxy layer (gateway) in order to quickly grant access and control rights to users, meanwhile maintain consistency with the underlying blockchain data structure.

By studying the data storage and sharing scheme of distributed storage system, Wang et al. [101] proposed a scheme that combines the interplanetary file system of distributed storage system, Ethereum blockchain and attribute-based encryption (ABE) technology. The proposed scheme enables data owners to distribute secret keys and encrypt shared data for data users by specifying access policies, and it implements fine-grained access control over data. Jemel et al. [40] proposed a new access control model called Timely CP-ABE. The model has two main features. First, the author introduces a blockchain distributed access control mechanism based on user legality verification. Second, as the name implies, they add a time dimension for CP-ABE-based file security sharing. Ulybyshev et al. [98] gave a blockchain-based solution that relies on role-based(RBAC) and attributor-based access control ABAC and prevents unauthorized data access, ensuring the integrity of the software modules updated and original data. In addition, their solution detects data leaks by authorized blockchain network participants behind the scene in the face of unauthorized entities. Their methods are used for data forensics/origination when determining the identity of entities accessing/updating/transferring sensitive network data or sensitive software. In addition, Cha et al. [16] proposed the design of the blockchain access control gateway which dynamically maintains the personal privacy information of device users in the blockchain Internet of Things system. Because the gateway can filter or hide the sensitive information of user devices, and add permission control to access sensitive information. It can effectively prevent the disclosure of personal privacy information. To validate and securely manage privacy preferences, the authors proposed a robust digital signature mechanism. In addition, they used blockchain networks as the infrastructure for resolving disputes over privacy data processing and maintenance.

As mentioned above, the model formed by the common features of the above model is a semi-central blockchain access control model. The design idea is that there is still a centralized authorization server, and the resource requester first sends an access to the authorization server. The request, if the policy agrees, sends a transaction granting access rights to the blockchain, and the blockchain records the access right and notifies the resource requester, then the resource request to access the resource first needs to tell the blockchain to use the access right. The key point is to use the blockchain as a trusted storage platform in a non-trusted IoT environment, and we have adjusted the process summarized [87] as shown in Fig5. The advantage is that the granting and use of permissions are recorded on the chain, which cannot be forged and traced, and coud facilitate audition. However, the disadvantage is that it cannot be guaranteed. The third-party authorization server is fair and secure.

4.3.3 Future work

In summary, the emergence of blockchain technology provides new ideas and research directions for IoT access control solutions under high-speed development. From the above research, we can see that the combination of blockchain and IoT access control can effectively solve the problem of massive IoT data security and privacy issues, the reliability of access control over-centralization, and the dynamic

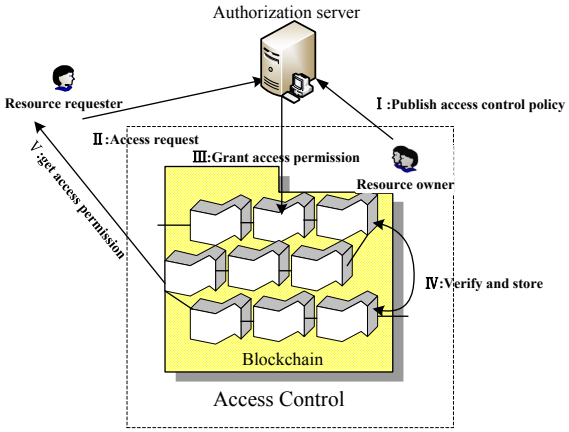


Fig. 5: Semi-central blockchain access control model

changes of access control strategies. However, the current research is still in the exploratory stage, and the application of technology is still not mature. In the future work, it is necessary to solve the following problems.

- Making plan and combination of new models

  From the current research, the combination of blockchain and traditional access control are nothing more than the above two ways. Although it can overcome, in a certain degree, the shortcomings of the traditional access control model in the Internet of Things environment. However, due to the distributed nature of the blockchain, important access control strategies are stored in the widely distributed lightweight IoT device block nodes. It is easy to cause block nodes to be attacked and infiltrated, which would cause the system failure. Therefore, how to design a new blockchain access control model and architecture and how to find a new combination of ideas, safe and reasonable distribution of IoT tasks and access control permissions are topics worth studying.

- Cross-domain access to the Internet of Everything

  Cross-domain access has always been a research hotspot in the field of access control. However, in today's IoT environment, IoT systems are often independent and single, such as smart transportation, smart medical care, smart security, etc. Due to the lack of mutual trust mechanism, it is difficult to reach a consensus, so cross-domain access cannot be achieved, which is obviously inconsistent with the ultimate goal of the Internet of things. Therefore, how to use the blockchain's trust mechanism that can reach consensus in a non-trusted environment to realize cross-domain access in IoT environment is a problem worth studying in the future.

- System performance optimization and throughput efficiency

  Since the blockchain technology is introduced in IoT access control, the shortcomings such as long transaction time, low system throughput and poor storage query performance caused by the consensus of the blockchain itself are inevitable. How to design a consensus mechanism in IoT environment and improve system throughput are topics worth studying in the future.

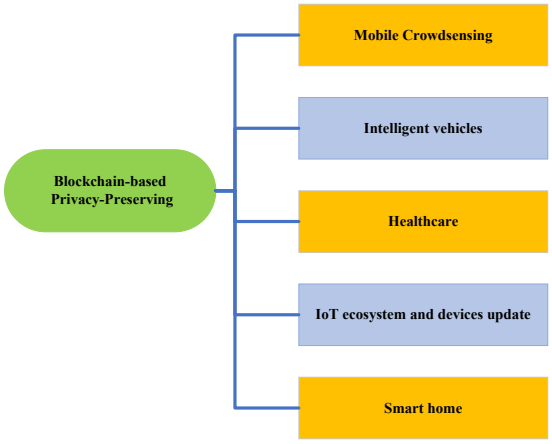


Fig. 6: Application of blockchain-based privacy-preserving in IoT

4.4 Blockchain-based Privacy-Preserving

Benefiting from the development of big data technology, communication technology and wireless sensing technology occurred and developed. In many fields, IoT has been achieved growth development such as Healthcare [113], Mobile Crowdsensing [41], Intelligent vehicles [89], Smart home [49], as shown in Fig 6. It is still plagued with privacy and security vulnerabilities [47]. The blockchain technology, underpinning Bitcoin, the first cyptocurrency system [71], has been thought as the potential tools to settle the privacy-preserving issues for its distributed, secure, and private characteristics [26]. Based on this, the rest of this subsection will have an overview of the privacy-preserving [112] issues existing in multiple domains under IoT, and the solutions by using the blockchain technologies.

4.4.1 Mobile Crowdsensing

The emerging mobile crowdsensing paradigm is a novel class of mobile IoT applications [30], which is a promising sensing paradigm that leverages the sensing capability of the pervasive mobile devices to perform various sensing tasks (i.e., healthcare, Traffic monitoring etc.) [106]. To motivate the skilled users to participate in finishing the sensing tasks, Wang et al. [100] proposed a privacy-perserving blockchain incentive mechanism in crowdsensing applications. As the transaction information may disclose user information, a k-anonymity privacy protection has been proposed by using a node cooperation verification approach. Furthermore, during the process, that is, transmitting messages to and from the platform, the workers location privacy [48] may get revealed. In order to solve this privacy problem, Yang. et al. [107] proposed a blockchain privacy-preservation crowdsensing system, which can protects the privacy of worker locations and increases the success rate of the assigned work.

4.4.2 Intelligent vehicles

As one of the key members of IoT—vehicular network [3], there also are some security issues in the vehicle-to-grid(V2G) networks. Since electric vehicles(EVs) received electricity from two parts that include both the grid and other EVs, the above pattern will generate an extensive payment records of electricity usage [90]. Gao et al. [31] designed a blockchain-based privacy preserving payment mechanism for V2G networks, because the mechanism that is based on a blockchain technique introduces a

registration and data maintenance process and enables data to be shared meanwhile secures user's sensitive attributes. Furthermore, some real-time and effective integration of all the involved messages (roads, vehicles, environments) should be treated more cautiously with the strong privacy protect requirement. And the privacy protection model shouldn't be focused only on the centralized network. To solve the above problem, Xu et al. [105] proposed a remote attestation security model dependent on a privacy-preserving blockchain, which divides the model into two parts. In the first step, a credible identity and integrity of the vehicle must be submitted to the network; in the second step, the vehicles in the network calculate the nodes and summarize the sub-conclusions, then write them into the blockchain blocks.

4.4.3 Healthcare

With the rapid growth of information technology, the quality, efficiency, and cost of healthcare have increased greatly. Some IoT-based wearable technology has been adopted to record the diagnosis and treatment process for patients outside of the conventional clinical environment. Despite these advantages, privacy is an essential trouble for any personal monitoring technology [83]. Dwivedi et al. [27] proposed that a blockchain could provide sucurity management and analysis of the big data about healthcare. Due to the leakages of the blockchain, a novel framework of modified blockchain models has been designed for IoT devices, which uses the distributed nature of the devices and other properties of the network.

4.4.4 IoT ecosystem and IoT devices update

In IoT environment, data needs to be collected and exchanged from many devices for different requirements, the process which can be described as publishing/subscribing models. The models should meet the basic needs of protecting the users sensitive information, but it may face the problem of single point failure, due to the existing IoT ecosystem mostly dependent on a centralized server [121]. To solve the problem, Lü et al. [52] proposed a privacy-preserving publishing/subscribing model by using blockchains, and used a public key encryption with equality test technologies to guarantee the identity authorization to protect the privacy-preserving data. Moreover, in the wake of burgeon in science and technology, it is essential to have the IoT devices upgraded to resist the different attacks at each levels [30]. Followed by the update of the IoT devices, users privacy may be revealed in a certain degree. Motivated by dealing with the leakage of sensitive information, Zhao et al. [118] proposed a novel privacy-preserving software updating protocol based on a blockchain. It requires the vendor delivers the updates, therefore, so as to provide financial incentive to the transmission nodes who deliver the updates to the IoT devices, it would make a commitment by using a smart contract.

4.4.5 Smart home

IoT is now considered as a promising technology for the consumer electronics market, and correspondingly, smart home [60] has been considered as one of the market segments with very high potential for IoT deployment, such as to enable home automation and energy management [84]. As smart home consists of amount of sensors devices that can generate, process, and exchange vast data that may contain sensitive information of users in the network, it may cause the privacy and security issues. Since the blockchain technologies are used to provide security safeguard in IoT, there may be lots of other new problems due to the high bandwidth and delays [47]. To solve the above mentioned problems, Dorri et al. [47] proposed a new secure, private, and lightweight method for IoT, which not only can eliminate the overhead delays etc., but also maintain its security and privacy. The author uses the method in smart home field by proposing an architecture which consists of three layers(smart homes, overlay and cloud storages). Furthermore, in the lecture [26], Ali Dorri made a deeper and detailed elaboration for various components and functions of the smart home framework.

4.4.6 Future work

As mentioned above, the current use of the characteristics of blockchain technology has become a good solution to the privacy protection in IoT. However, due to the characteristics of blockchain technology, privacy protection and controllable regulation are contradictory in the Internet of Things architecture that introduces blockchain technology. Therefore, future research work may focus on:

- encryption scheme with privacy protection

  Cryptography is called the art of solving coding problems, and the privacy protection of IoT, on account of blockchain, cannot be separated from the support of cryptography. Therefore, the design of encryption schemes with privacy protection and transaction concealment is an important issue worth studying in future privacy protection field of the IoT.

- Secure multi-party computing

  Secure multi-party computing is to settle the collaborative computing matter of protecting privacy for groups that lack of mutual trust, and at the same time not to disclose the input of each participant. Therefore, the multi-party computing technology for the privacy protection of user identity information is also a problem worth studying in the privacy protection field of the Internet of Things.

- Seek balance

  The transparency, traceability, auditability and other characteristics of the blockchain technology lead to the fact that in the blockchain system, controllable supervision and privacy protection become the opposite sides of each other. In the future research work, how to proportion privacy protection and controllable regulation is a crucial task. How to find a balance among preventing, detecting and tracing the illegal data and protecting users' privacy information is an important issue in future research.

5 Conclusion

The interconnection of all things is the trend of the future, and we are stepping into such an era of the IoT. The combination of block chains and the IoT has led to the further development of many new technologies. In the environment of the IoT, the number of heterogeneous terminal connections and the amount of data transmission are very large. The entry of blockchain can solve the existing problems of the IoT. The decentralized architecture of blockchain reduces the pressure of the old central computing of the IoT, and provides more possibilities for the innovation of the organizational structure of the IoT. However, the issue of privacy and security has always plagued the IoT. In the data transmission side or in the process of data transmission, there will be security risks. The accuracy and unauthorized modification of blockchain records make the data available. Data is no longer controlled solely by the center, and all transmitted data is strictly encrypted, so the user's data and privacy will be safer.

We mainly summarize the latest research results of applying blockchain in IoT, including the prominent advantages of blockchain technology in IoT and the security challenges. We introduce the characteristics and essential attributes of blockchain technology, and also point out the technical bottleneck faced by blockchain technology. This is the focus of future research work and the obstacles to be removed. Combined with the technological advantages of blockchain, there are many applications in IoT, especially in the security of the IoT. As blockchain technology itself needs to be researched and developed, blockchain technology for the IoT has many aspects that need to be made a further breakthrough

and improvement. The review of the current work on the existing technical challenges and research gaps is mentioned and the future research focuses are suggested.

References

[1] Coinmarketcap crypto-currency market capitalizations. `https://coinmarketcap.com` [Online; accessed on May 1, 2019].

[2] R. Agrawal, P. Verma, R. Sonanis, U. Goel, A. De, S. A. Kondaveeti, and S. Shekhar. Continuous security in iot using blockchain. In *Proc. of 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'18), Calgary, Alberta, Canada*, pages 6423–6427. IEEE, April 2018.

[3] K. Alam, M. Saini, and A. El-Saddik. Toward social internet of vehicles: Concept, architecture, and applications. *IEEE Access*, 3:343–357, March 2015.

[4] M. Alblooshi, K. Salah, and Y. Alhammadi. Blockchain-based ownership management for medical iot (miot) devices. In *Proc. of the 2018 13th International Conference on Innovations in Information Technology (IIT'13), Al Ain, United Arab Emirates*, pages 151–156. IEEE, November 2018.

[5] N. Alexopoulos, E. Vasilomanolakis, N. R. Ivánkó, and M. Mühlhäuser. Towards blockchain-based collaborative intrusion detection systems. In *Proc. of International Conference on Critical Information Infrastructures Security, Lucca, Italy*, pages 107–118. Springer International Publishing, October 2017.

[6] E. Alsaadi and A. Tubaishat. Internet of things: features, challenges, and vulnerabilities. *International Journal of Advanced Computer Science and Information Technology*, 4(1):1–13, 2015.

[7] H. An, R. Choi, and K. Kim. Blockchain-based decentralized key management system with quantum resistance. In *Proc. of the 19th World Conference on Information Security Applications (WISA'18). Jeju Island, Korea*, volume 11402 of *Lecture Notes in Computer Science*, pages 229–240. Springer, Cham, August 2018.

[8] X. An, X. Zhou, X. Lü, F. Lin, and L. Yang. Sample selected extreme learning machine based intrusion detection in fog computing and mec. *Wireless Communications and Mobile Computing*, 2018:1–10, January 2018.

[9] J. P. Anderson. Computer security threat monitoring and surveillance. Technical report, James P. Anderson Company, 1980.

[10] M. Banerjee, J. Lee, Q. Chen, and K. R. Choo. Blockchain-based security layer for identification and isolation of malicious things in iot: A conceptual design. In *Proc of the 27th International Conference on Computer Communication and Networks (ICCCN'27), Hangzhou, China*, pages 1–6. IEEE, August 2018.

[11] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, and R. Sirdey. Towards better availability and accountability for iot updates by means of a blockchain. In *Proc. of 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW'17), Paris, France*, pages 50–58. IEEE, April 2017.

[12] V. Buterin. Ethereum white paper: a next generation smart contract and decentralized application platform. `http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf` [Online; accessed on May 1, 2019], 2013.

[13] R. Casado-Vara, P. Chamoso, F. D. Prieta, J. Prieto, and J. M. Corchado. Non-linear adaptive closed-loop control system for improved efficiency in iot-blockchain management. *Information Fusion*, 49:227–239, September 2019.

[14] M. Castro and B. Liskov. Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems*, 20(4):398–461, November 2002.

[15] M. Cebe, B. Kaplan, and K. Akkaya. A network coding based information spreading approach for permissioned blockchain in iot settings. In *Proc. of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous'18), New York, New York, USA*, pages 470–475. ACM, November 2018.

[16] S. Cha, J. Chen, C. Su, and K. Yeh. A blockchain connected gateway for ble-based devices in the internet of things. *IEEE Access*, 6:24639–24649, January 2018.

[17] N. Cong-Luong, Z. Xiong, P. Wang, and D. Niyato. Optimal auction for edge computing resource management in mobile blockchain networks: A deep learning approach. In *Proc. of the 2018 IEEE International Conference on Communications (ICC'18), Kansas City, Missouri, USA*, pages 1–6. IEEE, May 2018.

[18] N. T. Courtois and R. Mercer. Stealth address and key management techniques in blockchain systems. In *Proc. of the 3rd International Conference on Information Systems Security and Privacy (ICISSP'17), Porto, Portugal*, pages 559–566. Scitepress, February 2017.

[19] J. Cruz, Y. Kaji, and N. Yanai. Rbac-sc: Role-based access control using smart contract. *IEEE Access*, 6:12240–12251, March 2018.

[20] T. Cruz, L. Rosa, J. Proenca, L. Maglaras, M. Aubigny, L. Lev, J. Jiang, and P. Simões. A cybersecurity detection framework for supervisory control and data acquisition systems. *IEEE Transactions on Industrial Informatics*, 12(6):2236–2246, December 2016.

[21] D. David, M. Rajappa, T. Karupuswamy, and S. Iyer. A dynamic-identity based multimedia server client authentication scheme for tele-care multimedia medical information system. *Wireless Personal Communications*, 85(1):241–261, November 2015.

[22] K. R. Özyılma and A. Yurdakul. Designing a blockchain-based iot with ethereum, swarm, and lora: the software solution to create high availability with minimal security risks. *IEEE Consumer Electronics Magazine*, 8(2):28–34, February 2019.

[23] K. R. Özyılmaz and A. Yurdakul. Integrating low-power iot devices to a blockchain-based infrastructure: work-in-progress. In *Proc. of the 13th ACM International Conference on Embedded Software (EMSOFT'17), Seoul, South Korea*. IEEE, October 2017.

[24] X. Deng, P. Jiang, X. Peng, and C. Mi. An intelligent outlier detection method with one class support tucker machine and genetic algorithm toward big sensor data in internet of things. *IEEE Transactions on Industrial Electronics*, 66(6):4672–4683, June 2019.

[25] S. Ding, J. Cao, C. Li, K. Fan, and H. Li. A novel attribute-based access control scheme using blockchain for iot. *IEEE Access*, 7:38431–38441, March 2019.

[26] A. Dorri, S. Kanhere, R. Jurdak, and P. Gauravaram. Blockchain for iot security and privacy: The case study of a smart home. In *Proc. of the 2017 IEEE international conference on pervasive computing and communications workshops (PerCom Workshops'17), Kona, Hawaii, USA*, pages 618–623. IEEE, March 2017.

[27] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh. A decentralized privacy-preserving healthcare blockchain for iot. *Sensors*, 19(2):1–17, January 2019.

[28] T. Economist. The promise of the blockchain: The trust machine. `https://www.economist.com/leaders/2015/10/31/the-trust-machine` [Online; accessed on May 1], October 2015.

[29] A. Fahad, I. Elgendi, S. Kumudu, S. Kumudu, D. Sharma, and A. Jamalipour. Blockchain in iot security: A survey. In *Proc. of the 2018 28th International Telecommunication Networks and Applications Conference (ITNAC'18), Sydney, New South Wales, Australia*, pages 296–299, May 2018.

[30] M. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal*, 6(2):2188–2204, November 2018.

[31] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren. A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. *IEEE Network*, 32(6):184–192, November 2018.

[32] M. Guo, H. Liaw, M. Chiu, and D. Deng. On decentralized group key management mechanism for vehicular ad hoc networks. *Security and Communication Networks*, 9(3):241–247, February 2019.

[33] S. Halder, A. Ghosal, and M. Conti. Dfficient physical intrusion detection in internet of things: a node deployment approach. *Computer Networks*, 154:28–46, May 2019.

[34] D. He, C. Chen, S. Chan, and J. Bu. Secure and efficient handover authentication based on bilinear pairing functions. *IEEE Transactions on Wireless Communications*, 11(1):48–53, January 2012.

[35] L. T. Heberlein, G. V. Dias, K. N. Levitt, B. Mukherjee, J. Wood, and D. Wolber. A network security monitor. In *Proc. of 1990 IEEE Computer Society Symposium on Research in Security and Privacy (RISP'90), Oakland, California, USA*, pages 296–304. IEEE, May 1990.

[36] W. Hong, Y. Cai, Z. Yu, and X. Yu. An agri-product traceability system based on iot and blockchain

technology. In *Proc. of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN'18), Shenzhen, China*, pages 254–255. IEEE, August 2018.

[37] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, and L. Xie. A decentralized solution for iot data trusted exchange based-on blockchain. In *Proc. of the 3rd IEEE International Conference on Computer and Communications (ICCC'17). Chengdu, China*, pages 1180–1184. IEEE, December 2017.

[38] S. Huh, S. Cho, and S. Kim. Managing iot devices using blockchain platform. In *Proc. of the 2017 19th international conference on advanced communication technology (ICACT'17), Pyeongchang, South Korea*, pages 464–467, February 2017.

[39] D. Hwang, J. Choi, and K. Kim. Dynamic access control scheme for iot devices using blockchain. In *Proc. of 2018 International Conference on Information and Communication Technology Convergence (ICTC'18). Jeju, South Korea*, pages 713–715. IEEE, October 2018.

[40] M. Jemel and A. Serhrouchni. Decentralized access control mechanism with temporal dimension based on blockchain. In *Proc. of 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE'17). Shanghai, China*, pages 177–182. IEEE, November 2017.

[41] H. Ji, L. Su, H. Xiao, and K. Nahrstedt. Inception: Incentivizing privacy-preserving data aggregation for mobile crowd sensing systems. In *Proc. of the 2016 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing (ISMAHNC'16), Paderborn, Germany*, pages 341–350. ACM, July 2016.

[42] L. Jun, Z. Shen, A. Zhang, and Y. Chai. Blockchain and iot based food traceability for smart agriculture. In *Proc. of the 3rd International Conference on Crowd Science and Engineering (ICCSE'18). Singapore, Singapore*, pages 1–6. ACM, March 2018.

[43] S. Karnouskos. Cyber-physical systems in the smartgrid. In *Proc. of the 2011 9th IEEE International Conference on Industrial Informatics (INDIN'11), Lisbon, Portugal*, pages 26–29. IEEE, July 2011.

[44] S. K. Kim, U. M. Kim, and J. H. Huh. A study on improvement of blockchain application to overcome vulnerability of iot multiplatform security. *Energies*, 12(3):402–415, January 2019.

[45] T. Kim, J. Noh, and S. Cho. Scc: storage compression consensus for blockchain in lightweight iot network. In *Proc. of the 2019 IEEE International Conference on Consumer Electronics (ICCE'19). Las Vegas, Nevada, USA*, pages 1–4. IEEE, January 2019.

[46] S. King and S. Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. `https://eprint.iacr.org/2018/248.pdf` [Online; accessed on May 1, 2019], 2018.

[47] P. Kotzanikolaou, S. Maniatis, E. Nikolouzou, and V. Stathopoulos. Evaluating common privacy vulnerabilities in internet service providers. In *Proc. of the 2009 3rd International ICST Conference on e-Democracy (IICD'09), Athens, Greece*, pages 161–170. IEEE, September 2009.

[48] J. Krumm. A survey of computational location privacy. *Personal and Ubiquitous Computing*, 13(6):391–399, August 2009.

[49] S. Kum, M. Kang, and J. Park. Iot delegate: smart home framework for heterogeneous iot service collaboration. *KSII Transactions on Internet and Information Systems*, 10(8):3958–3971, August 2016.

[50] L. Lamport, R. Shostak, and M. Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, July 1982.

[51] D. Larimer. Delegated proof-of-stake (DPOS). `https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper` [Online; accessed on May 1, 2019], April 2014.

[52] P. Lü, L. Wang, H. Zhu, W. Deng, and L. Gu. An iot-oriented privacy-preserving publish/subscribe model over blockchains. *IEEE Access*, 7:41309–41314, March 2019.

[53] T. Le and M. W. Mutka. Capchain: A privacy preserving access control framework based on blockchain for pervasive environments. In *Proc. of 2018 IEEE International Conference on Smart Computing (SMARTCOMP'18). Taormina, Italy*, pages 57–64. IEEE, June 2018.

[54] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet of Things Journal*, 4(6):1832–1843, December 2017.

[55] D. Li, W. Peng, W. Deng, and F. Gai. A blockchain-based authentication and security mechanism for iot. In *Proc. of the 2018 27th International Conference on Computer Communication and Networks (ICCCN'18),*

Hangzhou, China, pages 1–6. IEEE, October 2018.

[56] F. Liao, S. Bao, C. Cheng, and K. Chen. On design issues and architectural styles for blockchain-driven iot services. In *Proc. of the 2017 IEEE international conference on consumer electronics-Taiwan (ICCE-TW'17), Taipei, Taiwan*, pages 351–352. IEEE, June 2017.

[57] F. Lin, L. Qian, X. Zhou, Y. Chen, and D. Huang. Cooperative differential game for model energy-bandwidth efficiency tradeoff in the internet of things. *China Communications*, 11(1):92–102, May 2014.

[58] F. Lin, Y. Zhou, X. An, I. You, and K. R. Choo. Fair resource allocation in an intrusion-detection system for edge computing: Ensuring the security of internet of things devices. *IEEE Consumer Electronics Magazine*, 7(6):45–50, November 2018.

[59] F. Lin, Y. Zhou, I. You, J. Lin, X. An, and X. Lü. Content recommendation algorithm for intelligent navigator in fog computing based iot environment. *IEEE Access*, 7:53677–53686, April 2019.

[60] H. Lin and N. Bergmann. Iot privacy and security challenges for smart home environments. *Information*, 7(3):1–15, July 2016.

[61] J. Liono, P. P. Jayaraman, A. K. Qin, T. Nguyen, and S. F. D. Qdas: Quality driven data summarisation for effective storage management in internet of things. *Journal of Parallel and Distributed Computing*, 127:196–208, May 2019.

[62] B. Liu, X. Yu, S. Chen, X. Xu, and L. Zhu. Blockchain based data integrity service framework for iot data. In *Proc. of the 2017 IEEE International Conference on Web Services (ICWS'17), Honolulu, Hawaii, USA*, pages 468–475. IEEE, June 2017.

[63] Y. Liu, T. Zhu, Y. Jiang, and X. Liu. Service matchmaking for internet of things based on probabilistic topic model. *Future Generation Computer Systems*, 94:272–281, November 2018.

[64] F. Lombardi, L. Aniello, S. De-Angelis, A. Margheri, and V. Sassone. A blockchain-based infrastructure for reliable and cost-effective iot-aided smart grids. In *Proc. of the 2018 Living in the Internet of Things: Cybersecurity of the IoT-2018 (LITCI'18), London, UK*, pages 1–6. IEEE, March 2018.

[65] J. Lou, Q. Zhang, Z. Qi, and K. Lei. A blockchain-based key management scheme for named data networking. In *Proc. of 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN'18), Shenzhen, China*, pages 141–146, August 2018.

[66] M. Ma, G. Shi, and F. Li. Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the iot scenario. *IEEE Access*, 7:34045–34059, March 2019.

[67] D. Mendez and B. Yang. Blockchain-based whitelisting for consumer iot devices and home networks. In *Proc of the 19th Annual SIG Conference on Information Technology Education (SIGITE'18), Fort Lauderdale, Florida, USA*, pages 7–12. ACM, October 2018.

[68] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han. When intrusion detection meets blockchain technology: a review. *IEEE Access*, 6:10179–10188, January 2018.

[69] R. C. Merkle. Protocols for public key cryptosystems. In *Proc. of the 1980 IEEE Symposium on Security and Privacy (SP'80), Oakland, California, USA*, pages 122–122. IEEE, April 1980.

[70] O. B. Mora, R. Rivera, V. M. Larios, J. R. Beltrán-Ramírezet, R. Maciel, and A. Ochoa. A use case in cybersecurity based in blockchain to deal with the security and privacy of citizens and smart cities cyberinfrastructures. In *Proc. of 2018 IEEE International Smart Cities Conference (ISC2'18), Kansas City, Misouri, USA*, pages 1–4. IEEE, September 2018.

[71] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. `https://bitcoin.org/bitcoin.pdf` [Online; accessed on May 1, 2019].

[72] O. Novo. Blockchain meets iot: An architecture for scalable access management in iot. *IEEE Internet of Things Journal*, 5(2):1184–1195, April 2018.

[73] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito. Blockchain and iot integration: A systematic survey. *Sensors*, 18(8):1–37, August 2018.

[74] G. Papadodimas, G. Palaiokrasas, A. Litke, and T. Varvarigou. Implementation of smart contracts for blockchain based iot applications. In *Proc. of the 9th International Conference on the Network of the Future (NOF'18), Poznan, Poland*, pages 60–67. IEEE, November 2018.

[75] G. W. Peters and E. Panayi. Understanding modern banking ledgers through blockchain technologies:

Future of transaction processing and smart contracts on the internet of money. banking beyond banks and money. In *Banking Beyond Banks and Money*, pages 239–278. Springer, Cham, September 2016.

[76] O. J. A. Pinno, A. R. A. Grégio, and L. C. E. D. Bona. Controlchain: Blockchain as a central enabler for access control authorizations in the iot. In *Proc. of 2017 IEEE Global Communications Conference (GLOBECOM'17). Singapore, Singapore*, pages 1–6. IEEE, December 2017.

[77] J. Portilla, G. Mujica, J. S. Lee, and T. Riesgo. The extreme edge at the bottom of the internet of things: a review. *IEEE Sensors Journal*, 19(9):3179–3190, May 2019.

[78] M. Pustišek and K. Andrej. Approaches to front-end iot application development for the ethereum blockchain. *Procedia Computer Science*, 129:410–419, January 2018.

[79] C. Qu, M. Tao, J. Zhang, X. Hong, and R. Yuan. Blockchain based credibility verification method for iot entities. *Security and Communication Networks*, 2018:1–11, June 2018.

[80] N. Rifi, N. Agoulmine, N. C. Taher, and E. Rechkidi. Blockchain technology: Is it a good candidate for securing iot sensitive medical data? *Wireless Communications and Mobile Computing*, 2018:1–11, December 2018.

[81] N. Rifi, E. Rachkidi, E. Agoulmine, and C. Taher. Towards using blockchain technology for iot data access protection. In *Proc. of the IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB'17), Salamanca, Spain*, pages 1–5. IEEE, January 2017.

[82] V. Román and J. Ordieres-Meré. [wip] iot blockchain technologies for smart sensors based on raspberry pi. In *Proc. of the 11th IEEE Conference on Service-Oriented Computing and Applications (SOCA'18), Paris, France*, pages 216–220. IEEE, January 2019.

[83] A. B. S. Avancha and D. Kotz. Privacy in mobile technology for personal healthcare. *ACM Computing Surveys*, 45(1):1–56, November 2012.

[84] F. Santoso and N. Vun. Securing iot for smart home system. In *Proc. of the 2015 IEEE International Symposium on Consumer Electronics (ISCE'15), Madrid, Spain*, pages 1–2. IEEE, June 2015.

[85] P. E. Sedgewick and R. D. Lemos. Self-adaptation made easy with blockchains. In *Proc. of the 13th International Conference on Software Engineering for Adaptive and Self-Managing Systems (ICSEASS'18). Gothenburg, Sweden*, pages 192–193. ACM, May 2018.

[86] M. Sharma, A. Gupta, and J. Singh. Blockchain-based resource discovery for the intercloud. In *Proc. of the 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS'17), Model Inst Engn and Technol, Jammu, India*, pages 92–97. IEEE, December 2017.

[87] J. Shi and R. Li. Survey of blockchain access control in the internet of things. *Journal of Software*, 30(6), 2019.

[88] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu. Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 3(5):637–646, October 2016.

[89] M. Singh and S. Kim. Introduce reward-based intelligent vehicles communication using blockchain. In *Proc. of the 2017 International SoC Design Conference (ISOCC'17), Seoul, South Korea*, pages 15–16. IEEE, November 2016.

[90] E. Sortomme and M. El-Sharkawi. Optimal scheduling of vehicle-to-grid energy and ancillary services. *IEEE Transactions on Smart Grid*, 3(1):351–359, March 2012.

[91] J. Su, F. Lin, X. Zhou, and X. Lü. Steiner tree based optimal resource caching scheme in fog computing. *China Communications*, 12(8):161–168, August 2015.

[92] I. Sukhodolskiy and S. Zapechnikov. A blockchain-based access control system for cloud storage. In *Proc. of 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus'18). Moscow, Russia*, pages 1575–1578. IEEE, January 2018.

[93] M. Taneja. A framework for power saving in iot networks. In *Proc. of the 2014 3rd International Conference on Advances in Computing, Communications and Informatics (ICACCI'14), New Delhi, India*, pages 369–375. IEEE, September 2014.

[94] P. Tedeschi, G. Piro, and G. Boggia. When blockchain makes ephemeral keys authentic: a novel key agreement mechanism in the iot world. In *Proc. of 2018 IEEE Globecom Workshops (GC Wkshps'18), Abu Dhabi, United Arab Emirates*, pages 1–6. IEEE, December 2018.

[95] H. Teng, Y. Liu, A. Liu, N. Xiong, Z. Cai, and T. Wang. A novel code data dissemination scheme for internet of things through mobile vehicle of smart cities. *Future Generation Computer Systems*, 94:351–367, May 2019.

[96] N. Teslya and I. Ryabchikov. Blockchain-based platform architecture for industrial iot. In *Proc. of the 2017 21st Conference of Open Innovations Association (FRUCT'17), Helsinki, Finland*, pages 321–329. IEEE, November 2017.

[97] C. Tselios, I. Politis, and S. Kotsopoulos. Enhancing sdn security for iot-related deployments through blockchain. In *Proc. of 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN'17), Berlin, Germany*, pages 303–308. IEEE, November 2017.

[98] D. Ulybyshev, M. Villarreal-Vasquez, B. Bhargava, G. Mani, S.Seaberg, P. Conoval, R. Pike, and K. J. ́blockhub:́ blockchain-based software development system for untrusted environments. In *Proc. of 2018 IEEE International Conference on Cloud Computing (CLOUD'18). San Francisco, California, USA*, pages 582–585. IEEE, July 2018.

[99] M. Veeramanikandan and S. Sankaranarayanan. Publish/subscribe based multi-tier edge computational model in internet of things for latency reduction. *Journal of Parallel and Distributed Computing*, 127:18–27, May 2019.

[100] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang. A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. *IEEE Access*, 6:17545–17556, March 2018.

[101] S. Wang, Y. Zhang, and Y. Zhang. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *IEEE Access*, 6:38437–38450, June 2018.

[102] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng. Survey on blockchain for internet of things. *Computer Communications*, 136:10–29, February 2019.

[103] B. Wu, Q. Li, K. Xu, R. Li, and Z. Liu. Smartretro: Blockchain-based incentives for distributed iot retrospective detection. In *Proc. of the 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS'15), Chengdu, China*, pages 308–316. IEEE, October 2018.

[104] Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han. Optimal pricing-based edge computing resource management in mobile blockchain. In *Proc. of the 2018 IEEE International Conference on Communications (ICC'18), Kansas City, Missouri, USA*, pages 1–6. IEEE, May 2018.

[105] C. Xu, H. Liu, P. Li, and P. Wang. A remote attestation security model based on privacy-preserving blockchain for v2x. *IEEE Access*, 6:67809–67818, November 2018.

[106] L. Yang, M. Zhang, S. He, M. Li, and J. Zhang. Crowd-empowered privacy-preserving data aggregation for mobile crowdsensing. In *Proc. of the 2018 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing (ISMAHNC'18), New York, New York, USA*, pages 151–160. ACM, June 2018.

[107] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. Deng. A blockchain-based location privacy-preserving crowdsensing system. *Future Generation Computer Systems-the international of escience*, 94:408–418, May 2019.

[108] Y. Yao, X. Cai, , and G. Giannakis. On energy efficiency and optimum resource allocation of relay transmissions in the low-power regime. *IEEE Transactions on Wireless Communications*, 6(4):2917–2927, December 2005.

[109] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander. Where is current research on blockchain technology?–a systematic review. *PloS one*, 11(10):1–27, October 2016.

[110] A. Yohan and N. W. Lo. An over-the-blockchain firmware update framework for iot devices. In *Proc. of the 2018 IEEE Conference on Dependable and Secure Computing (DSC'18), Kaohsiung, Taiwan*, pages 1–8. IEEE, December 2018.

[111] S. Yu, K. Ren, and W. Lou. Attribute-based on-demand multicast group setup with membership anonymity. *Computer Networks*, 54(3):377–386, February 2010.

[112] M. Zhang, J. Chen, L. Yang, and J. Zhang. Dynamic pricing for privacy-preserving mobile crowdsensing: A reinforcement learning approach. *IEEE Network*, 33(2):160–165, March 2017.

[113] P. Zhang, D. Schmidt, J. White, and G. Lenz. Blockchain technology use cases in healthcare. *Advances in Computers*, 111:1–41, March 2018.

[114] X. Zhang, S. Poslad, and Z. Ma. Block-based access control for blockchain-based electronic medical records

(emrs) query in ehealth. In *Proc. of 2018 IEEE Global Communications Conference (GLOBECOM'18). Abu Dhabi, United Arab Emirates*, pages 1–7. IEEE, December 2018.

[115] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan. Smart contract-based access control for the internet of things. *IEEE Internet of Things Journal*, 6(2):1594–1605, April 2019.

[116] Z. Zhang, Y. GUO, W. Liu, and J. Lv. Group key agreement protocol based on m-tree and dh protocol. *Computer Engineering*, 34(1):161–169, January 2010.

[117] H. Zhao, P. Bai, Y. Peng, and R. Xu. Efficient key management scheme for health blockchain. *CAAI Transactions on Intelligence Technology*, 3(2):114–118, June 2018.

[118] Y. Zhao, Y. Liu, Y. Yu, and Y. Li. Blockchain based privacy-preserving software updates with proof-of-delivery for internet of things, 2019.

[119] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4):372–375, October 2018.

[120] W. Zhou, Y. Xu, and G. Wang. Decentralized group key management for hierarchical access control using multilinear forms. *Concurrency & Computation Practice & Experience*, 28(3):631–645, March 2016.

[121] X. Zhou and S. Chen. Study on insulation detection method of electric vehicles based on single point of failure model. In *Proc. of the 2016 11th International Forum on Strategic Technology (IFOST'16), Novosibirsk, Russia*, pages 191–194. IEEE, June 2016.

[122] Y. Zhu, Y. Qin, G. Gan, Y. Shuai, and W. Chu. Digital asset management with distributed permission over blockchain and attribute-based access control. In *Proc. of 2018 IEEE International Conference on Services Computing (SCC'18). San Francisco, California, USA*, pages 193–200. IEEE, July 2018.

[123] Y. Zhu, Y. Qin, G. Gan, Y. Shuai, and W. Chu. Tbac: transaction-based access control on blockchain for resource sharing with cryptographically decentralized authorization. In *Proc. of 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC'18). Tokyo, Japan*, pages 535–544. IEEE, July 2018.

[124] G. Zyskind and O. Nathan. Decentralizing privacy: using blockchain to protect personal data. In *Proc. of 2015 IEEE Security and Privacy Workshops (SPW'15). San Jose, California, USA*, pages 180–184. IEEE, May 2015.

Author Biography

Hongwen Hui was born in Shanxi province, China in 1991. He received his Master degree from Xinjiang University, in 2018. He is currently a Ph. D student in School of Computer and Communication Engineering, University of Science and Technology Beijing, P. R. China. His main research interests are application of blockchain technology.

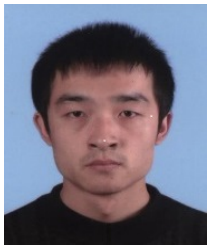
Xingshuo An was born in Shandong province, China in 1988. He received his Master degree from University of Science and Technology Beijing, in 2014. He is currently a Ph. D student in School of Computer and Communication Engineering, University of Science and Technology Beijing, P. R. China. His research direction is fog computing and network security.

Haoyu Wang was born in Jilin province ,China in 1989. He is currently a Ph.D student in school of Computer and Communication Engineering,University of Science and Technology Beijing, P.R.China. His research direction is edge computing and blockchain.

Weijia Ju received her undergraduate degree from Qingdao University of Science and Technology. Present she is a postgraduate in department of Computer and Communication Engineering, University of Science and Technology Beijing. Her main research direction is blockchain.

Huixuan Yang was born in Hebei province, China in 1997. She received her bachelor degree from University of Science and Technology Beijing, in 2018. She is currently a graduate student in School of Computer and Communication Engineering, University of Science and Technology Beijing, P. R. China. Her research direction is Blockchain and data mining.

Hongjie Gao received her M.S. degree from School of Mathematics and Physics, University of Science and Technology Beijing, China in 2017. At present, she is pursuing her Ph.D. degree in School of Computer and Communication Engineering, University of Science and Technology Beijing, China. Her research interests include game theory, data privacy and security in mobile crowdsensing.



Fuhong Lin received his M.S. degree and Ph.D. degree from Beijing Jiaotong University, Beijing, P. R. China, in 2006 and 2010, respectively, both in Electronics Engineering. Now he is an associate professor in department of Computer and Communication Engineering, University of Science and Technology Beijing, P. R. China. His research interests include Edge/Fog Computing, Network Security, and Big Data. He won "Provincial and Ministry Science and Technology Progress Award 2" in 2017. His two papers won "Top 100 most Cited Chinese Papers Published in International Journals" in 2015 and 2016. He served as co-chair of the first and third IET International Conference on Cyberspace Technology, and general chair of the second IET International Conference on Cyberspace Technology. He was the leading editor of the Special issue "Recent Advances in Cloud-Aware Mobile Fog Computing" for Wireless Communications and Mobile Computing. Currently, he also serves as a reviewer more than 10 international journals including IEEE Transactions on Industrial Informatics, IEEE Access, Information Sciences, IEEE IoT Journal, The Computer Journal and China Communications. He received the track Best Paper Award from IEEE/ACM ICCAD 2017.