# Embedding Blockchain Technology Into IoT for Security: A Survey

Li Da Xu, *Fellow, IEEE*, Yang Lu, *Member, IEEE*, and Ling Li

***Abstract*—In recent years, the Internet of Things (IoT) has made great progress. The interconnection between IoT and the Internet enables real-time information processing and transaction implementation through heterogeneous intelligent devices. But the security, the privacy, and the reliability of IoT are key challenges that limit its development. The features of the blockchain, such as decentralization, consensus mechanism, data encryption, and smart contracts, are suitable for building distributed IoT systems to prevent potential attacks and to reduce transaction costs. As a decentralized and transparent database platform, blockchain has the potential to raise the performance of IoT security to a higher level. This article systematically analyzes state of the art of IoT security based on the blockchain, paying special attention to the security features, issues, technologies, approaches, and related scenarios in blockchain-embedded IoT. The integration and interoperation of blockchain and IoT is an important and foreseeable development in the computational communication system.**

***Index Terms*—Blockchain, decentralization, information communication technology (ICT), Internet of Things (IoT), security, smart contract.**

## I. Introduction

At PRESENT, the Internet of Things (IoT) is an enormous ecosystem. Its timeliness, convenience, inclusiveness, scalability, integration, and interoperability make IoT an unparalleled prospect for further development. Its applications extend to a wide range of fields, such as agriculture and food traceability, remote medicare and hospitality, location and navigation, logistics and operations, manufacturing and automation, smart city and home use, etc. At the same time, more and more security vulnerabilities have arisen—urgent issues that need to be solved. During the first half of 2017, the number of attacks on IoT devices increased by 280%. By 2021, corporate spending on information security related to IoT is projected to increase from the current \$83.5 billion to \$119.9 billion. Based on the architecture of IoT itself, many effective paradigms and protocols have been used to prevent or to eliminate potential security risks. But these have not been enough. IoT requires the assistance of appropriate technology and mechanisms to improve its overall security level. With the rapid development of the blockchain, its security functions have been revealed, and they have become potential approaches for IoT security, with a special focus on its decentralized and transparent system, as well as on its consensus mechanisms and privacy protocols, encrypted data and management, and smart contract agreement [1]–[4].

The IoT refers to a real-time information-sharing system for objects based, on Internet technology, using radio-frequency identification (RFID) and product electronic coding. IoT has gradually developed into an information industry chain, integrating the Internet as well as information and communication technologies, such as sensors and cloud computing. At this point in time, IoT has penetrated into many aspects of human life, such as Industry 4.0, the smart society, artificial intelligence (AI), and 6G. IoT is a network that connects as many things as possible, such as RFID, infrared sensors, global positioning systems, laser scanners, etc. The system connects all possible devices to the Internet for information exchange and communication, in order to intelligently identify, locate, track, monitor, and manage the entire network [5]–[8].

Blockchain is a peer-to-peer (P2P) distributed ledger technology based on encryption algorithms and a shared database technology on the Internet. Blockchain technically solves trust-relevant issues. The secure transmission of the hash chain-based encryption algorithm and the time stamp mechanism of the certificate value ensure data traceability and irreversible modification. Consistency algorithms are used to ensure the relationship between the node and the block data. Programmable smart contracts are guaranteed, based on the consistency of the automated script code and the Turing virtual machine. The blockchain is a powerful security system based on cryptography, communication technology, and the consensus mechanism. Blockchain is revolutionizing the IoT system, in a variety of aspects. The unique features of blockchain—its P2P decentralized network, its open and transparent multiparty consensus, and its untampered data—give IoT the ability to achieve higher security standards [9]–[11].

Blockchain technology can be applied to various systems, such as identity management, supply chain management, and the IoT. Using a P2P network of computers will run the protocols and will hold an encrypted and immutable copy of transactions on every node on the network. Blockchain and the related technologies have the potential to resolve several of the key security issues of IoT.

1) Blockchain ensures security of IoT through consensus mechanisms. The reason for the security issues is the lack of trust mechanisms between devices within the IoT

Manuscript received September 14, 2020; revised November 15, 2020; accepted February 8, 2021. Date of publication February 19, 2021; date of current version June 23, 2021. *(Corresponding author: Yang Lu.)*

Li Da Xu is with the IT&DS, Old Dominion University, Norfolk, VA 23529 USA.

Yang Lu is with the Department of Information Systems and Operations Management, University of Central Oklahoma, Edmond, OK 73034 USA (e-mail: ziiyuu@gmail.com).

Ling Li is with the Department of Information Technology & Decision Sciences, Old Dominion University, Norfolk, VA 23529 USA.

Digital Object Identifier 10.1109/JIOT.2021.3060508

TABLE I
COMPARISON BETWEEN CENTRALIZED AND DECENTRALIZED SYSTEM

| Citation (Google) | IoT Security | Blockchain-based Features | Blockchain-based IoT Attacks | Blockchain-based IoT Measures | Blockchain-based IoT Scenarios | Technical Challenges | Future Prospective | Comparison of Extant Papers | Article |
|---|---|---|---|---|---|---|---|---|---|
| **Survey Papers about IoT Security** | | | | | | | | | |
| 3282 | ✓ | | | | | ✓ | ✓ | ✓ | [1] |
| 1358 | ✓ | | | | | ✓ | | ✓ | [19] |
| 463 | ✓ | | | | | ✓ | ✓ | ✓ | [20] |
| 443 | ✓ | | | | | | ✓ | ✓ | [21] |
| 346 | ✓ | | | | | ✓ | | ✓ | [22] |
| 129 | ✓ | | | | | ✓ | ✓ | ✓ | [23] |
| 95 | ✓ | | | | | ✓ | ✓ | ✓ | [4] |
| **Survey Papers about Blockchain-based IoT Security** | | | | | | | | | |
| 2117 | ✓ | ✓ | | ✓ | | ✓ | | ✓ | [24] |
| 740 | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | [25] |
| 481 | | ✓ | | ✓ | | ✓ | ✓ | ✓ | [26] |
| 390 | | ✓ | ✓ | ✓ | | | ✓ | ✓ | [27] |
| 392 | | ✓ | | | ✓ | | ✓ | ✓ | [28] |
| 338 | | | | | ✓ | ✓ | ✓ | ✓ | [29] |
| 109 | | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | [30] |
| 96 | ✓ | ✓ | | ✓ | | | ✓ | ✓ | [31] |
| | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | This Paper |

system. Blockchain provides a mechanism that does not require trust between nodes.

2) Blockchain solves the reliability of IoT. The distributed network structure of blockchain guarantees that, even if one or more nodes are attacked, the data of the entire network system is still reliable and safe. When the system needs to prohibit a participant who behaves inappropriately, the consensus mechanism can be used to identify the participant through the 51% nodes agreement without affecting the overall performance.
3) Blockchain can significantly reduce equipment costs and increase the effectiveness of the entire IoT system. Blockchain makes full use of P2P computing to process hundreds of billions of transactions that occur in IoT. Blockchain can reduce costs incurred during the establishment and the maintenance of a centralized database. Meanwhile, the blockchain can make full use of the computing, storage capacity, and broadband of idle devices distributed in IoT, reducing calculation and storage costs.
4) Blockchain can extend the life cycle of products or services. IoT, under the blockchain model, transfers the responsibility of maintaining equipment to a self-maintaining community. This fact renders IoT not obsolete, regardless whether it is in a product life cycle or beyond a life cycle, but this will save infrastructure costs [12]–[18].

IoT and blockchain are emerging technologies that are attracting a lot of attention but, most importantly, security is a critical factor that affects the smooth and successful integration of blockchain into IoT, in order to improve the performance of IoT security. This article compares the extant survey (review) papers about IoT security. It is better to divide the selected papers into two categories: 1) survey papers about IoT security and 2) papers about blockchain-based IoT security. The selected papers were culled from popular academic databases, such as IEEE Xplore, Web of Science (WoS), and Scopus. Based upon the recent five-year citation (Google Scholar), 15 papers were selected (Table I). Seven papers are about IoT security and eight papers are about blockchain-based IoT security. Specifically, the papers about IoT security focus on IoT security and the related challenges and future directions. Most of the papers about blockchain-based IoT security discuss the way in which blockchain can be integrated into the IoT system for security and the relevant anti-measures against potential attacks to IoT. However, only a few of the

| | |
|---|---|
| Introduction | The Current Status/Brief Interpretation to IoT<br>Potential Integration of IoT and Blockhcain<br>A Summary and Comparison of Survey Papers about Blockchain-based IoT Security |
| Major Security Risks in IoT | Data Gathering/Data Transmission/Tag Embedded/Data Storing/Consensus Algorithm and Trust/Authentication and Access Control/Infrastructure |
| Characteristics of Blockchain-embedded IoT | Difference between Centralized and Decentralized Platform/Decentralization/Consensus Algorithm and Trust/Chronological and Distributed Data/Data Encryption/Smart Contract |
| Classification of Blockchain-based IoT Security | Taxonomy of Blockchain-based IoT Security<br>Structural Security (Sensor Layer, Network Layer, Application Layer)<br>Functional Security (Device Safety and Privacy Protection, Access Control, Identity Authentication, Data Assurance, Anti-DDoS Attack, IoT Self-Regulation) |
| Blockchain-based IoT Attacks | Abandon/DoS/DDoS/Equipment Injection/Falsifying/Link/Modifying/Public Block Modifying/Time Interval Destruction |
| Information Sharing Security | Three Categories of Blockchain (Public, Private, and Consortium)<br>Infrastructure of Blockchain-based Information Sharing |
| IoT Security Scenarios under Blockchain | Framework of Blockchain-based IoT Security/Decentralized and disintermediated IoT Platform/Data Processing and Provenance System/<br>Public Service (The Healthcare Industry, The Traffic Management, Smart City) |
| Challenges and Trends | Technical Challenges (Performance of IoT Data Processing, Consensus Mechanism, Network Bandwidth, Unreliable Data Communication, Inconsistency of Block Recording)<br>Research Trends (New Blockchain-based Business Mode, Integration of Blockchain and Edge Computing, Double-chained IoT Security Scheme, Interoperability of IoT, Blockchain, and 6G) |

Fig. 1. Roadmap of this article.

selected papers illustrate scenarios of attacks to IoT security under blockchain. Based upon the foundation of these papers, this article not only systematically illustrates the security related issues in IoT, but it also highlights the way in which blockchain-based mechanisms handle security in the entire IoT system, including features, functions, categories, measures, scenarios, challenges, future directions, etc.

Our article is a relatively comprehensive survey of blockchain-based IoT security. It aims to recognize and clarify IoT security issues under blockchain, from different perspectives. The goal of this article is to provide an in-depth survey of the use of blockchain technology to provide and improve the performance of IoT security and privacy. A detailed roadmap (Fig. 1) is offered, to provide readers with a clear view of the construct.

In Section I, readers are offered a general idea about the status of IoT development, a brief interpretation to IoT, the potential integration of IoT and blockchain, and a summary and comparison of survey papers about blockchain-based IoT security.

In Section II, readers become familiar with the IoT risks in data gathering, data transmission, embedded tags, data storing, authentication and access control, and infrastructure.

In Section III, readers get information about the differences between the centralized and decentralized platforms, decentralization, consensus algorithm and trust, chronological and distributed data, data encryption, and smart contracts.

In Section IV, readers learn about the taxonomy of blockchain-based IoT security; structural security, such as sensor layers, network layers, and application layers; and functional security, such as device safety upgrades, access control, identity authentication, data assurance, anti-Distributed Denial-of-Service (DDoS) attack, and IoT network self-regulation.

In Section V, readers become familiar with different types of attacks of abandon: Denial of Service (DoS), DDoS, equipment injection, falsifying, link, modifying, public block modifying, and time interval destruction.

In Section VI, readers recognize the three categories of blockchain: 1) public; 2) private; and 3) consortium and learn about the infrastructure of blockchain-based information sharing.

In Section VII, readers are exposed to the thinking about the framework of blockchain-based IoT security; the decentralized and disintermediated IoT platform; data processing and the provenance system; and public service, such as the healthcare industry, the traffic management, and the smart city.

In Section VIII, readers are exposed to two parts: 1) the technical challenges, such as the performance of IoT data processing, the consensus mechanism, network bandwidth, unreliable data communication and 2) the inconsistency of block recording; and research trends, such as a new blockchain-based business mode, the integration of the blockchain and edge computing for IoT security, a double-chained IoT security scheme, the interoperability of IoT, blockchain, and 6G.

This article is outlined as follows: Section II addresses the major security risks in IoT. Section III depicts blockchain-embedded IoT characteristics. Section IV discusses different categories of security issues in IoT. Section V briefly introduces blockchain-based IoT attacks. Section VI delineates blockchain-based information sharing security mechanisms. Section VII illustrates the IoT security framework and applications. Section VIII discusses technical challenges and research trends. The conclusion is found in Section IX.

## II. Major Security Risks in IoT

The IoT technology connects various appliances, equipment, and tools implemented with sensors, truly realizing real-time monitoring and intelligent management and operations. With the vigorous development of IoT, its security issues have gradually become prominent. Due to the structural deficits of IoT, the current level of security technologies and measures do not adapt well to the IoT ecosystem. In detail, the security issues in IoT are the risks of data gathering, data transmission, tags being embedded, data storing, authentication and access control, and IoT infrastructure [32]–[34].

### A. Risks of Data Gathering

The original data of IoT come from a terminal device and are collected by sensors and other devices. Due to the large number of sensing devices in the entire IoT system, the entire sensing control system presents multisource heterogeneity. Generally, sensors are relatively simple and cannot be monitored effectively for a long time. This brings greater security risks. In addition, terminal devices rarely take protective measures; attackers can easily obtain key node passwords and other identity information and can use the information to publish and convey incorrect information. A DoS attack is one common security attack that could affect the normal operation of the system [35], [36].

### B. Risks of Data Transmission

Since the total amount of data collected by sensors and other devices is not large, the complicated protection measures are usually not taken during information transmission. This gives attackers the opportunity to invade during data transmission. Once this happens, it will affect the IoT system, thereby damaging user rights and causing the system to fail to perform certain functions [23]–[25].

### C. Risks of Tag Being Embedded

After data collection, IoT usually transmits information directly to the control center, in a wireless format. However, this procedure is directly exposed, without good protection. Thus, if some tags are embedded in other substances, the terminal device will always be monitored. This will lead to the monitoring of a large amount of basic information and the leakage of personal and private information. It even raises social and public safety issues [22], [22].

### D. Risks of Data Storing

The IoT collects a lot of data and will also retain many users' personal and private information, such as their passwords, personal preferences, etc. Regarding the stored data, ways to prevent theft and destruction of data and ways to prepare, in time, if the above situation occurs, all countermeasures should be considered. In addition, when stored data are maliciously mixed with "dirty" data, the IoT system will appear to misfunction. Therefore, it is also necessary to consider how to deal with data pollution and other incidents [24], [27].

### E. Risks of Authentication and Access Control

Network authentication is usually divided into identity authentication and message authentication. Identity authentication requires a key to ensure reliability. However, in communication, if one of the secret keys is stolen, the data in the entire communication process can be stolen, causing losses to the system. Message identification and authentication, one of commonly used authentication methods in IoT, is a protection method to ensure the integrity and security of information when exchanging information. However, in the message authentication process, the message authentication code is usually static. The intruder can obtain the correct message authentication code through exhaustive or surveillance methods, and then pretend to be the receiver and interact with the involved parties. This phenomenon can lead to the leakage of a large amount of data, in the IoT system [28], [29].

### F. Risks of IoT Infrastructure

The current system architecture of IoT is a centralized and supervised architecture. In this architecture, the establishment of a system trust mechanism is very simple and a reliable third party is required to uniformly manage all device information in the system. With the continuous development of IoT technology, the number of IoT terminal devices will reach tens of billions. Such a huge quantity and data source will bring tremendous pressure to the third parties. Hence, IoT needs a more advanced architecture to reduce its reliance on third parties and to establish a new trust mechanism in order to improve the overall performance of the system [30]–[32].

## III. Characteristics of Blockchain-Embedded IoT

The terms "IoT" and "blockchain" both have the meaning of "connection," i.e., "net" and "chain." IoT is a technology that connects people, devices, and platforms through various sensing terminals to achieve information transmission and service. Blockchain is a technology that integrates cryptography, consensus protocols, a P2P network, and smart contracts for data exchange, processing, and storage. It can be seen that IoT and blockchain are two different dimensions of the information processing system: 1) IoT includes all of the entities with physical space and 2) aims to break through the information flow according to the communication protocol; blockchain focuses on safely managing the flow of information in a timely manner. Therefore, the link between IoT and

TABLE II
COMPARISON BETWEEN CENTRALIZED AND DECENTRALIZED SYSTEMS

| **Features** | **Centralized** | **Decentralized** |
|---|---|---|
| Transaction Mode | Centralization | Decentralization |
| Resource Consuming | High | Low |
| Transaction Costs | High | Low |
| Data Storage | Centralized Database | Decentralized Ledger |
| Data Security | Low | High |
| Data Privacy | Low | High |
| Information Transparency | Low | High |
| Flexibility | Supervised | Freedom |

blockchain lies in information storage, encryption security, and value transfer [37], [38].

IoT connects hundreds of millions of devices. Ensuring the privacy and the security of each device and interconnection between different devices is not easy to achieve. The P2P propagation has high network latency in the system. When the number of nodes is too large, the order of transactions observed by each node over a period of time may not be identical. Hence, IoT needs a mechanism to allow it to reach an agreement on the sequence of the transactions that occur within similar time periods. The consensus mechanism improves the privacy and the security of data transmitted between IoT devices. Blockchain is a powerful tool that can be used to construct a more secure IoT network by employing blockchain's major features: decentralization, consensus algorithm and trust, chronological and distributed data, data encryption, and smart contracts [39], [40].

Traditionally, all data, such as user account information and transaction history, are stored and regulated in the centralized database. Security and privacy are poor; once the database is attacked, the damaged data are difficult to recover. Users have only their own records and cannot know the transaction records of other users; thus, the establishment of the mutual trust network is affected. In a blockchain system, each node becomes an independent provider and receiver, and each entity is evenly dispersed. The form of the direct P2P platform has the potential to reduce unnecessary costs, such as power loss and transaction costs. It is also possible to conduct an information exchange between nodes in different regions and to allocate transactions across regions. All information and nodes can be anonymous, in order to ensure the security of the users. The decentralized system eliminates the need for a central supervision, improves data sharing and security, optimizes revenues and efficiency, and increases mutual trust between entities. The following table (Table II) briefly addresses the differences between the centralized and the decentralized platforms [12]–[16].

### *A. Decentralization*

The main feature of blockchain is decentralization. Unlike the traditional network system, in the blockchain network, the processes of data interaction, downloading, and verification do not have a supervised central node but, rather, a decentralized structure composed of multiple nodes within the system. Also, unlike the traditional structure, each node in the network does not rely on unified management, and the nodes' functions and roles are identical. When data are transmitted between different nodes, the receiving node will perform identity verification on the sending node. After the verification is executed, the received data record will be broadcast on the entire network. Blockchain, using mathematical algorithms to implement a trust mechanism, can effectively prevent the centralized structure of the IoT system from paralyzing the entire network due to malicious security attacks [14]–[16], [40]–[43].

This decentralization means that the flow of data between nodes is not limited to a central point and is not dependent on third parties. The blockchain-distributed nodes form a P2P network, which consists of verification, propagation, and consensus mechanisms. Under the premise of security between nodes, the collection, verification, storage, and dissemination of data can effectively avoid high-cost, high-risk, and inefficient problems in the centralized system. In a blockchain system, there is no centralized node and no managerial structure. Rather, many nodes constitute a distributed network. The various methods of security maintenance in the network depend on all the nodes that have authorities and capabilities within the network. Each node is equal, and there is no hierarchical mechanism among the nodes [14]–[16], [40]–[43].

Each node has a complete data record. When a node receives data from another node, the node verifies the identity and data of the other node. If the verification passes, the data received by the node will be propagated to other nodes and to the entire network. The verification, storage, maintenance, and transmission of data in a blockchain network are based on a distributed structure. The algorithm and protocol of the trust consensus mechanism replace the mutual trust construct between the centralized authorities. Hence, the blockchain optimizes the centralized structure of IoT and reduces the dependence of IoT on the centralized model. Blockchain has changed the way in which the IoT processes data, preventing damage to the entire system caused by a centralized IoT structure [14]–[16], [40]–[43].

### *B. Consensus Algorithm and Trust*

The consensus mechanism solves the problem of how blockchain can achieve consistency in distributed scenarios. It is one of the key factors of the blockchain system. The consensus mechanism ensures the fairness of each node in the P2P network. It is a part of the entire system and a unified agreement that all nodes need to follow. The consensus mechanism is a mechanism that motivates the system's ability to screen honest nodes and merge them to form an unchanging record. It depends on the distributed maintenance of each node to a common ledger database with unified content and it is difficult to tamper with, in the blockchain system. The maintenance process is not only a process in which each node in the blockchain competes to accept new transaction record, but it is also a process in which each node verifies the validity of the information recorded in the blockchain system. The blockchain consensus mechanisms include the Proof of Work (PoW), Proof of Share (PoS), Delegated Proof of Sake (DPoS), and practical Byzantine fault tolerance (PBFT) [24]–[27].

In the blockchain system, the address associated with the public key in the asymmetric encryption algorithm is used to redistribute user identities, so the traditional PKI-based certificate authority is no longer needed, thus avoiding the problem of certificate authority. The blockchain uses a consensus algorithm to decompose and establish a trust mechanism in the entire network. In this mechanism, there is no need to share identity information, just to replace the address to interact; nodes can also change their addresses. The consensus mechanism can resolve security issues in the information transmission of IoT and can protect the privacy of specific devices or users [13]–[17].

Due to the decentralization of blockchain, data transmission between nodes is secure, open, and transparent. The mechanisms of the blockchain technically avoid the crucial issue of trust between mutual parties; they implement algorithms to autonomously identify and verify the authentic entities and transactions. Blockchain retains all the transaction data in each block. Blockchain users can get all the data in blockchain without additional centralized processing. The feature of blockchain trust can be applied to the trust mechanism of IoT so that transactions between users can be implemented autonomously, without a trusting mechanism. Additionally, the data recorded in the ledger of the block are more transparent and reliable [12], [14]–[16], [41].

### *C. Chronological and Distributed Data*

Blockchain uses timestamps to identify and to record each transaction. A time dimension is added to the data, and the data have a time order. Sequential confirmation makes the data traceable. The timestamp method not only guarantees the originality of the data but it also reduces the traceability cost of the transaction. Time order data enhance the irreversible modification of information. The data of the common ledger are open and they are transparent to the involved parties. The timestamp, as an important parameter of the Proof of Existence (PoE), can confirm that some data must exist at a certain point. This ensures that the blockchain database is not tampered with. Time order is used to ensure the security of IoT data, preventing attackers from injecting a large amount of irrelevant data into the data platform, in order to prevent data services from being blocked [14]–[16], [44]–[47].

In the blockchain system, the function of a block is like a ledger. It can record all information exchanges on the entire blockchain, and the information records can be checked by other nodes at any time. Unlike the general recording method, the information records of a blockchain are scattered on all nodes without a center, forming a typical distributed database system. When some nodes are attacked or when data are damaged, other nodes still have complete information, so this will not affect the system. This feature will significantly improve the data and information storage security of IoT [45], [46].

### *D. Data Encryption*

In the blockchain system, when transmitting information, an asymmetric encryption algorithm is used to ensure data security. The principle of the asymmetric encryption algorithm is that both sending and receiving nodes need to generate a pair of public and private keys in advance for encryption and decryption. Before the sending nodes transmit to the receiving nodes, both nodes will share a public key with each other, then the sender uses the receiver's public key to encrypt the information, and the encrypted information can only be decrypted with the private key. Only the receiving node knows the private key, thus ensuring the reliability and security of the transmitted information [14]–[16].

Blockchain uses asymmetric encryption, including data encryption and digital signatures, to encrypt data. Data encryption in a blockchain ensures the security of data and reduces the risk of lost or corrupted data. In transaction processing, the blockchain uses a timestamp mechanism to generate an ID for each transaction. The user can query the relevant transaction data according to the ID. When the new block is verified, the current block is added to the main block. Each block uses a hash of an algorithm to identify its uniqueness. If an attacker intends to tamper with the data, more than half of the nodes must confirm. For the system and the structure of blockchain, this possibility is very small. Transaction data are transmitted over the network and is digitally signed, aiming to indicate the identity and approval of the data content. The digital signature algorithm commonly used is the elliptic-curve digital signature algorithm (ECDSA) [14]–[16], [48]–[50].

### *E. Smart Contract*

The IoT responds and executes the actions needed to meet the established conditions and rules, and the process should be performed step by step. Some operations rely on the status parameter to determine whether to perform the next step, making the operation complex and time consuming. Hence, multiple operations cannot be efficiently performed automatically and continuously. A smart contract is a set

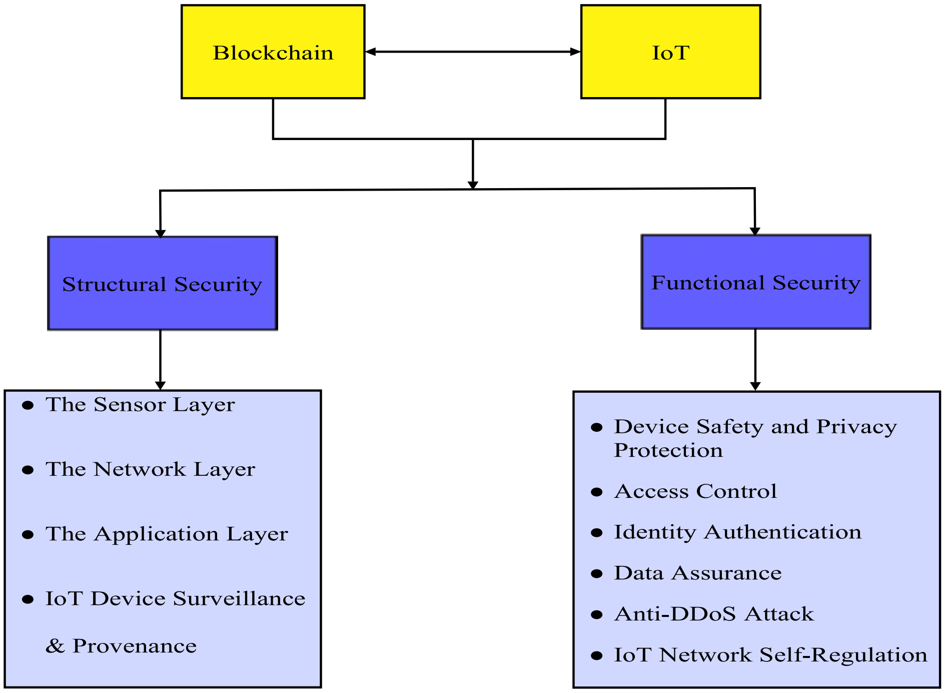

Fig. 2. Taxonomy of blockchain-based IoT security.

of commitments defined in a digital form. From the user's point of view, a smart contract is an automatic guarantee program. When certain conditions are met, the smart contract automatically releases and transmits the corresponding information. From a technical perspective, a smart contract is a Web server. This server is not built on the Internet, but runs specific contract programs on the blockchain. Smart contracts are programmable contracts. They convert transactions between users into a code that is stored in a blockchain and is tagged with a unique blockchain address. The blockchain platform enables smart contracts to self-manage and even to have legal force. Smart contracts strengthen the mutual trust mechanism between Internet users and achieve mutual trust [14]–[16], [48]–[50].

As long as the contract conditions are met, the chain code of the smart contract can automatically perform multiple operations in succession. Smart contracts automate the business logic, as well as legal rights and obligations, provide the foundation for security and privacy protection, and increase the efficiency of IoT. According to each user's requirement, smart contracts can automatically employ different protection mechanisms, according to their different levels of privacy information [51]–[54].

## IV. Classification of Security in IoT

### A. Taxonomy of Blockchain-Based IoT Security

Blockchain relies on the powerful computing power generated by consensus algorithms, such as PoW for distributed systems, to prevent external attacks and to ensure data security. It solves the general problem of the Byzantine mechanisms and it establishes a decentralized and trustworthy system. It completes the value transfer in the process of information sharing and exchange, fulfilling the requirements of information availability and reliability [55]–[57].

IoT is a comprehensive system that, possibly, consists of everything. As an emerging technology, blockchain is capable of changing the transaction process of IoT and can improve security performance throughout the whole system. As indicated in Fig. 2, our review will illustrate IoT security issues from both the structural and the functional perspectives. Specifically, the structural security focuses on three IoT layers: 1) the sensor layer; 2) the network layer; and 3) the application layer, as well as on IoT device surveillance; the functional security includes device safety upgrade, privacy protection, access control, identity authentication, data assurance, anti-DDoS mechanism, and IoT network self-regulation.

### B. Structural Security

IoT applications have grown in various fields but, due to the multiple-source heterogeneity, openness, and universality, the IoT and related objects still need to resolve security issues. One critical challenge for IoT security comes from the underlying architecture of the IoT ecosystem; it is based on a centralized infrastructure interconnected with a server and a device. All devices are identified, authenticated, and connected by a centralized server that supports huge processing and storage capacity.

According to their differing perspectives, scholars express various views on the IoT structure. Our study focuses on the security issues that mainly involve three layers: 1) the sensor layer; 2) the network layer; and 3) the application layer [1], [2], [58]. The layers of IoT security are improved by the blockchain. Different types of attacks to these layers

TABLE III
SECURITY ISSUES OF THE THREE IoT LAYERS

| **Layers** | **Security Issues** | **Technical Requirements** | **Blockchain Security Effects** |
|---|---|---|---|
| The Sensor Layer | Signal leakage and interference, forgery or spoofing, label embedding threat, illegal access, DDoS, … | Intrusion detection technology, identity authentication, device management, secure storage, anti-DDoS attacks, … | Decentralization<br>Transparency<br>Openness<br>Fairness<br>Encryption<br>Privacy<br>Time Order |
| The Network Layer | Data transmission, cross-network authentication between heterogeneous networks, network eavesdropping and interruption, DDoS, … | Transmission encryption, access authentication, integrity protection, … | |
| The Application Layers | Information openness and privacy, verification and access control, physical security, data security, DDoS | Physical protection, identity authentication, access control, data encryption storage, firmware upgrade | |

are addressed in Table III. Associated with the three layers of IoT, a blockchain can participate in the success of its security by implementing diversified mechanisms and protocols.

*1) Security Issues in the Sensor Layer:* The sensor layer is the basis for the development and the application of IoT. Its main function is to collect, identify, and control information. The sensing layer consists of malicious devices and gateways. The sensing nodes have multisource heterogeneity, but the function is simple and lacks effective monitoring. Terminal nodes are more vulnerable to attacks [4].

The attacker intercepts, forges, falsifies, and replays the data or the command transmitted in the sensor network in order to obtain individual bits of sensitive information or to cause information transmission errors. The attacker takes advantage of the vulnerability of the IoT terminal to acquire the identity and password. The attacker performs illegal or malicious attacks through the pseudo-identity, which communicates with other nodes, issuing false information, replacing devices, and initiating a DDoS attack. The data collected through the sensor layer are transmitted wirelessly. The data, or even the user, are under monitoring, which directly leads to the disclosure or the destruction of information [3], [59].

As the weakest link in IoT security, IoT terminals can improve security performance by integrating a security chip into IoT devices to provide a reliable security hardware execution environment. To strengthen IoT terminal devices, the devices can directly participate in the blockchain transaction as a blockchain node. For the weak terminal of IoT, the terminal uses the integrated blockchain software development kit (SDK) as the client and connects the IoT gateway in the blockchain. When the terminal node participates in blockchain transactions, the device's unique identifier and private key information must be stored securely. The security chip provides a chip-level trusted identifier, sensitive information secure storage, and an encrypted secure computing environment for the terminal node. Blockchain generates the security and the reliability of transaction information [60], [61].

*2) Security Issues in the Network Layer:* The network layer mainly accesses the information of the sensing layer through the network (such as the wireless communication network, Internet, and satellite network) and transmits data to the IoT platform. It is completed in this manner since the collected information needs to be transmitted in real time through various networks.

Since the amount of data transmitted by devices in IoT is small, there is no encryption algorithm to protect the data. Data may be stolen, tampered with, attacked, and/or destroyed during transmission. The IoT is an open network in which multiple networks overlay. With the development of network convergence and the increasing complexity of network architectures, more and more communication protocols appear. When data are transferred from one network to another, a variety of issues, such as authentication, key negotiation, data confidentiality, and integrity protection, is involved [15], [62], [63].

*3) Security Issues in the Application Layer:* The application layer is the bridge between the IoT system and the user. It provides customized services, authentication, privacy protection, and user action instructions to the processing layer. At the same time, the application layer also has information processing and resource management functions. The application layer is directly related to the external entities and holds a large amount of private information [64]–[66].

The application layer stores large amounts of user data and involves several questions: how to store data efficiently to avoid data loss or corruption? how to isolate data for multitenant applications? how to prevent data services from being blocked? and how to quickly recover data errors? Each of these questions is related to IoT security. In addition, an attacker could inject a large amount of irrelevant data into the original data, causing system misjudgment and data contamination. The authentication approach of the application layer is the message verification between the sender and the receiver code. However, during the communication process, the authentication code is static and is easily used by others, resulting in incorrect authentication and security issues [3], [16].

*4) IoT-Embedded Device Surveillance and Synchronization:* IoT devices operate in centralized systems in which the trust mechanism is relatively easy to set up but requires a trusted third party to monitor all devices. However, the trusted third party cannot handle the increasing large number of devices infinitely [18]. Decentralized operation systems reduce the operational processes of the physical network. Meanwhile, it becomes necessary to establish a new mutual trust mechanism in order to maintain the consensus between devices and to ensure the performance of the system [39]. Different devices are connected by layers within the infrastructure. A security layer, the security abstraction layer, is capable of detecting and separating malicious devices [63]. Although the extra layer makes the entire structure more complicated, the present technology and protocol can fulfill the configuration of finding abnormal working devices and keeping system consistency. Another effective method integrates the blockchain network with a software paradigm, aiming at limiting possible attacks such as software-defined networking (SDN) [67], [68].

The integration of IoT and blockchain is at the early stage. With further development, the deficiency of the integration, such as insufficient computational and storage capacity and limited communication resources, will become clear. Blockchain synchronization is an effective way to balance the traffic between the blockchain system and the IoT-related devices. In other words, certain blockchain mechanisms can help each IoT device stay synchronized toward the protocol of smart contracts, thus guaranteeing the security of the IoT network [40], [69].

### *C. Functional Security*

The accessing of large-scale IoT terminal devices establishes a crucial challenge to network capacity expansion and to centralized platform performance. As a heterogeneous converged network, IoT not only has the same security issues as sensor networks, mobile communication networks, and the Internet but also has its particularities, such as a device safety upgrade and privacy protection, access control, identity authentication, data assurance, anti-DDoS mechanism, and IoT network self-regulation.

*1) Device Safety Upgrade and Privacy Protection:* In the network, remotely updating the firmware of embedded devices is one of the important means of protecting IoT. Through the blockchain network, the firmware vendor publishes the latest version of the firmware information to the distributed ledger of each verification node. The device node initiates a verification request to the verification node or to another neighboring device node associated with the smart contract, consensus mechanisms, and other methods, in order to confirm the latest firmware and the firmware integrity of the device. An on-time upgrade ensures firmware upgrade security through encryption and signatures and helps minimize the impact of attacks against firmware vulnerabilities [2], [3], [7].

One of the most well-known studies in the IoT communities is privately and securely executing queries over sensed and prepared data on IoT devices, due to the devices' limited and inefficient query processing abilities. A well-designed and privacy-preserving blockchain-based scheme can protect the privacy of IoT devices and can improve the overall communication efficiency within the network. Popular query service companies, such as Google, Facebook, Amazon, are eagerly seeking practical and effective anti-attack queries to protect security and privacy throughout IoT [70], [71]. Meanwhile, research is paying much attention to technical issues and to the feasibility of the queries. Blockchain has the potential to be implemented to solve these challenges. For example, Ethereum has been proposed for auditing and privacy preserving in database, cloud, and fog computing, and across the entire IoT. Associated with blockchain and with the relevant technologies, a reliable auditing system could be designed by the extant queries, such as SQL, MapReduce, etc., [72], [73].

*2) Access Control:* The data generated in IoT include a large amount of personal information that is private. If this privacy information is disclosed, it will bring huge losses to users. As one of the basic technologies of data protection, access control ensures that data can only be accessed by a user with permission. Access control is based on an authorization policy that controls access to certain resources in order to reduce illegitimate intrusions and to ensure authorized access to resources. The access control mechanism of the system mainly consists of authentication, authority, and auditing [74], [75]. The blockchain-based IoT platform can separate data and data access authority, and it can implement a decentralized personal data management system. An application needs the authority of the owner to access the data. The system checks the signature and all of the records to verify that the application has access to the appropriate data. Blockchain fully records the activities of the application, and users in the system can change the access rights of the data at any time [76]. Since resource constraints exist in practice, access control balances the device implementation and the consumption of resources to secure the devices and the IoT network [77]. In addition, access control can be programmed to update for IoT devices; this will help them to become available, accountable, agile, and adoptable among different nodes within the network [78], [79].

When the blockchain is combined with IoT, access control is one of the key technologies for IoT data protection. The combination has two main types. One type is the integration of the blockchain and the existing access control model. Blockchain is the trusted entity of the existing access control model; blockchain is combined with the role-based access control (RBAC) model, with the attributes-based access control (ABAC) model, and with capability-based access control (CapBAC) model. The other type is based on the different modes of blockchain. Blockchain is not only used as a trusted entity, based upon the characteristics of blockchain, but it even includes a transaction or smart contract that is constructed for access control, such as the Bitcoin-based access model and the Ethereum-based smart contract access control [28], [80], [81]. The detailed features of each model are listed in Table IV.

TABLE IV
BLOCKCHAIN RELATED ACCESS CONTROL MODEL

| Types | Features |
|---|---|
| RBAC<br>(Roled-based Access Control) | Implementing cross-organizational authentication using blockchain to resolve cross-organizational access control issues in RBAC. |
| ABAC<br>(Attributes-based Access Control) | Ensuring that malicious users cannot modify user identity attributes and access control policies. The strategy and authority of blockchain are open to prevent one party from fraudulently refusing to enforce activity. |
| CapBAC<br>(Capability-based Access Control) | Being used as a trusted database to store IoT data. Using blockchain to record authority, usage, transaction, etc.. |
| Blockchain-based | Using blockchain for storage access and authority. Storing access control policies on blockchain and managing access authority through blockchain transactions. |
| Ethereum-based & Smart Contract | The main function of access control is achieved through smart contracts. Blockchain is used for data source management, and all information about data changes is recorded through smart contracts. |

Since blockchain has the ability to enforce the integrity of all of its participants at the technical level, blockchain can play the role of a third party that provides a reliable environment for access control in IoT. As a trusted platform in IoT access control, blockchain provides computing and storage capabilities for IoT. Computing and storage are used as the major approaches. Some are focusing on the storage capacity of blockchain, some are focusing on the computational power of blockchain, and more are focusing on both computing and storage [82], [83].

Applying blockchain to IoT access control also requires solving a series of problems caused by the terminal nodes. There are a large number of terminal nodes in the network. How to effectively manage the nodes is a challenging task. Second, it is necessary to consider that there is the storage pressure brought by the large number of nodes to blockchain. The third need to consider is the impact of the vast nodes on the access control and the related transactions. Since the popular blockchains, Bitcoin and Ethereum take a long time for transactions, they are difficult to use directly for IoT access control [76], [81].

Blockchain can solve the dynamic problem of nodes in IoT. Since the identity of the user in blockchain is proven by its key, the node can be connected anytime, anywhere. The blockchain network can operate as long as the node's signature is correct. On the other hand, blockchain uses a P2P network architecture. When a user node needs to access the network, it only needs to connect to other blockchain nodes in the network. It is not based on the geographic location between nodes; the node only needs to select and connect to the blockchain nodes that exist in the network. Hence, for the dynamics of the node movement, frequent access, or exit, blockchain is able to deal with various access controls [75]–[79].

*3) Identity Authentication:* In the IoT, identity authentication technology is used to prevent illegal or unauthorized terminal devices from connecting to the IoT network or from launching malicious attacks, and to ensure the security of the IoT. The authentication credentials are registered to blockchain, and the device access rights can be set through the smart contract. When an IoT device requires access or authentication to the IoT platform, the blockchain system authenticates and manages the identity of the access device, based on the node consensus mechanism, to ensure that the device safely accesses IoT. Blockchain-based IoT device authentication can avoid the single point of failure risk of the centralized authentication technology and, thus, can ensure the integrity and reliability of the IoT device's identity [1], [2], [14].

*4) Data Assurance:* Traditional database systems manage discrete data, while IoT platforms handle streaming data. Streaming data are real-time and continuous, and, therefore, have the potential to be attacked or tampered with. Under the era of big data, the storage and the processing of massive amounts of data in IoT are vulnerable to attacks. IoT uses sensors to capture and store data through a centralized database. Other unstructured data are stored in the cloud. However, data need to be transmitted repeatedly during use, causing the central server to become overloaded, and jeopardizing data security. IoT applications need to cooperate with the security and the confidentiality of the data. Especially in the wireless transmission of IoT, it is necessary to prevent data leakage and illegal use. In an IoT system, data are stored and managed by a central entity. Misconduct of data management or failure of accurate processing can result in a data loss or a leak. Blockchain-based data operation systems adopt a decentralized architecture that eliminates the security risks of centralization [84], [85].

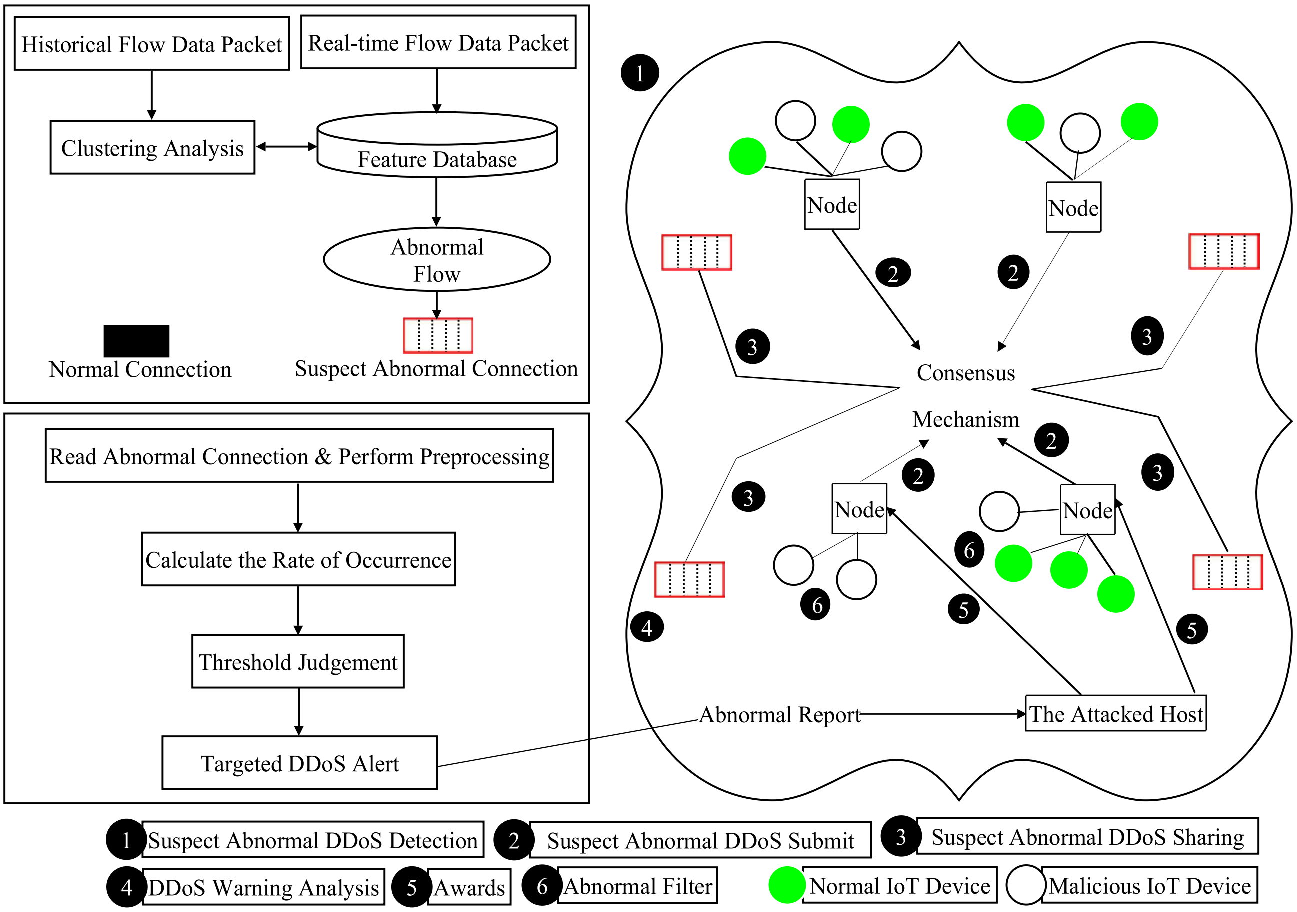

Fig. 3. Architecture of the anti-DDoS scheme.

The traceability of blockchain can also be applied to manipulate private data, in order to ensure data authenticity. The data manipulation process is transparent, and data are auditable to the user. Blockchain converts the complete information into different blocks. Each block contains only a small portion of the complete information and is asymmetrically encrypted using a hash function, with a chain structure of the Byzantine, Merkle Tree, and timestamp, in order to ensure data integrity and consistency. Since it is difficult to attack even one block of information, the complete information within the system is considerably less likely to be attacked [86], [87].

*5) Anti-DDoS Attack:* In December 2016, the Mirai virus ravaged the United States. The virus formed a botnet by infecting IoT devices and launched a DDoS attack on the domain name resolution server, causing more than half of the U.S. network to crash. The main reason for the success of the IoT botnet attack is that the traditional network security model is flawed. Due to the lack of reliable authentication and consensus mechanisms, a single point of nontrust may spread to multiple nontrust points, infecting to the entire IoT system [88], [89].

The distributed structure of blockchain is used to combat DDoS attacks and to increase system throughput. The DDoS attack sends a large number of requests to the central node of the target system, consuming the computing resources or the network resources of the central node and causing the target system to crash [90]. The blockchain system can provide a distributed noncentralized structure. Each node of blockchain has a complete record that can verify the data of other nodes. Hence, blockchain can be applied to build database systems, as well as to the domain name system (DNS), to eliminate single-point failure, to effectively defend against DDoS attacks, and to ensure the security of the system [91].

Some IoT devices are infected by malware viruses, forming a large-scale IoT botnet and posing a huge threat to IoT services. In the system, most devices connect to the network through an IoT gateway. If the device that initiated the DDoS attack can be disconnected from the IoT gateway, the risk of the IoT service being attacked can be reduced. A blockchain network can be established between the IoT gateways and the deployed smart contracts to verify, log in to, and disconnect DDoS attacks. For example, if the home smart device is controlled and performs a DDoS attack on an IoT service, when the IoT service verifies the DDoS attack, it will notify the IoT gateway. The IoT gateway will broadcast that it has been controlled and it will initiate a DDoS attack. If the attack is verified, the attack information can be written to the blockchain ledger. Then, all of the IoT gateways will disconnect all of the controlled smart parties to defend against the same DDoS attacks throughout the entire network [3], [92]. We constructed the architecture for an anti-DDoS scheme, which is described in Fig. 3. A plurality of nodes forms a blockchain network that processes a detection abnormal activity on the IoT devices that are targeted

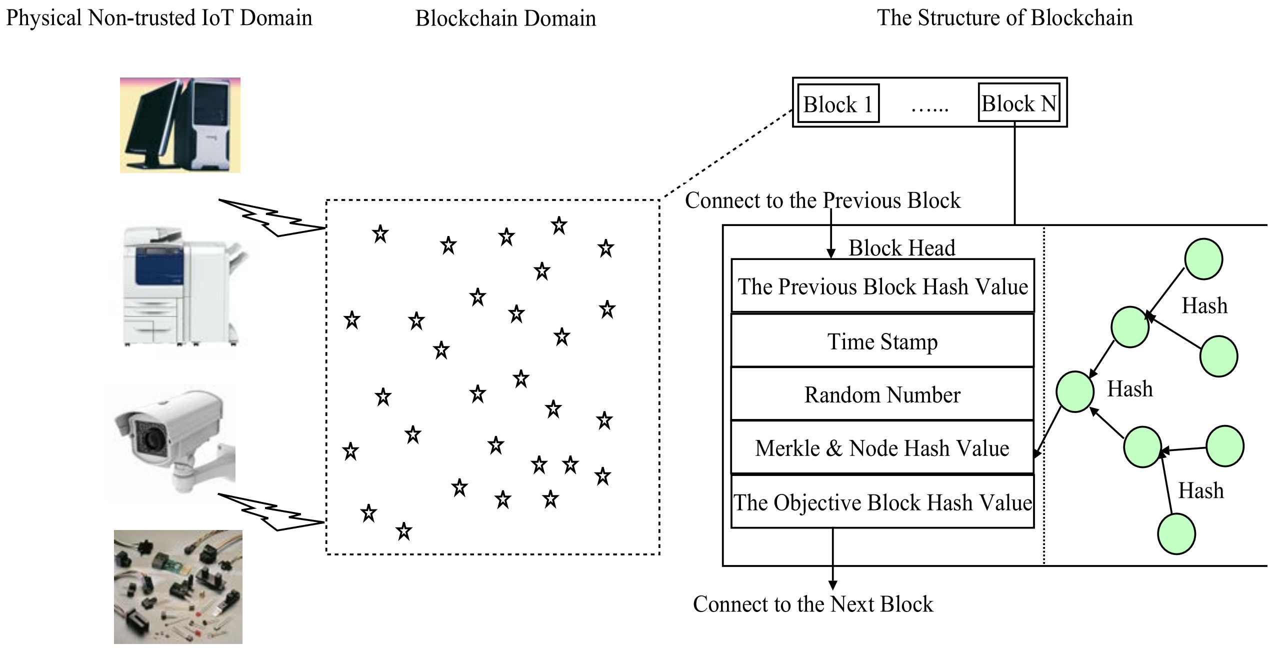
Physical Non-trusted IoT Domain
Blockchain Domain
The Structure of Blockchain
Block 1
……
Block N
Connect to the Previous Block
Block Head
The Previous Block Hash Value
Time Stamp
Random Number
Merkle & Node Hash Value
The Objective Block Hash Value
Hash
Hash
Hash
Connect to the Next Block

Fig. 4. One example of applying the blockchain in IoT.

by suspicious DDoS abnormal connections initiated by the IoT device. Then, the node submits the preliminary detection result to blockchain to share information of suspected DDoS abnormal connection. Based on the database's sharing suspected DDoS abnormal connections, a smart contract is executed to analyze some targeted IP associated with DDoS alert. The targeted IP acknowledges the alert and sends the reward to the corresponding node. After receiving the reward, the node filters the DDoS connection by the IoT device, based on the newly added DDoS alert.

To achieve the above proposal, there are three key issues that need to be addressed. Problem 1 is the DDoS anomaly detection. One method of detecting a DDoS is to analyze the data flow: it can directly determine the characteristics of the protocol (such as SYN FLOOD), and it can detect whether the IoT device has completed the TCP connection initialization with a three-time connection. If it has not completed the connection by the third time, it is likely to be DDoS abnormal attack. The other kind of attack does not have obvious protocol differences (such as UDP FLOOD). Thus, it is more difficult to detect this type of DDoS attack. There is no difference between the UDP communication of the controlled IoT device and that of a normal IoT device. In general, IoT device activity functions are stable and fixed, and the data packet content is regular, as well. By clustering the contents of historical UDP data packets to characterize several types of groups, real-time detection on a UDP connection to determine anomalies shows strong potential [88], [91]. Problem 2 is how to comprehensively analyze the suspicious DDoS abnormal connections. In a traditional solution, data integration analysis still uses the cloud. The cloud serves as a summary of all the information. In the analysis center, if a downtime occurs, the entire solution will fail. Under the existing centralized architecture, the single-point attack problem cannot be solved. It is considered that blockchain implements distributed ledger technology and the sharing of the analysis of preliminary detection results without using the cloud. There is the possibility of mutual trust, as well as the existence of malicious nodes. In order to achieve a secure and reliable sharing analysis between nodes, the blockchain can guarantee the following points.

1) *Consistency:* When there are malicious nodes, each node can still record other nodes correctly. The submitted data are consistent with the data stored in each node.
2) *Cannot Be Modified:* The records approved by each node cannot easily be tampered with.
3) *Anonymous:* The attacker cannot speculate the behavior of the node based on the submitted information [89], [90].

Problem 3 is how to ensure compliance with source-side deployment detection and prevention. Two methods are the establishment of incentives to attract users to accept safety measures for their IoT devices and the establishment of a reward mechanism from the DDoS attack victim to the abnormal result submitter. DDoS attack victims receive a DDoS alert to avoid losses, so they offer rewards. The submitter will receive a reward for the anomalous result that corresponds to this alert. The reward process is open, transparent, and verifiable. Blockchain writes reward rules into the smart contract, makes the whole process transparent to all the nodes, and verifies the reward distribution process [90]–[92].

*6) IoT Network Self-Regulation:* In an untrusted Internet environment, how to build trust between IoT devices is a challenge. Typically, a third party is required as an intermediary between devices. Through the blockchain, an IoT device trust relationship can be established without a third-party intervention, and interaction between devices can be performed directly. Blockchain creates an open and transparent rule through the algorithm and redefines how to generate credits to create a mutual-trust network. In this system, all of the rules are prerepresented in the form of an algorithm. Service participants do not need to know the relevant information of the other nodes, but mutual trust and transaction security are guaranteed without centralized third-party intervention. Organizational trust can be identified, and only trust algorithms can be used to establish mutual trust and to eliminate unified account updates and verification processes. Activities can be recorded, transferred, and stored for service transactions, as well [2], [4], [10].

## V. Blockchain-Based IoT Attacks

Just as the traditional IoT system has many drawbacks that attacks can take advantage of, the blockchain-based IoT security system does, as well. Based on the features of blockchain, attackers change their strategies and construct new attacks on the blockchain-based IoT system. In this section, we list popular blockchain-based IoT security attacks (Table V), such as abandon, DoS, DDoS, equipment injection, falsifying, link, modifying, public block modifying, and time interval destruction, among others. Blockchain-based IoT attack is a hot topic in the disciplines of both IoT and blockchain. In this article, popular attacks of interpretation and potential anti-measures are briefly addressed and discussed.

### *A. Abandon Attack*

Abandon refers to a node that holds auditing rights, discards its members' transactions, and isolates the members in the blockchain system. When a node finds that its transaction has not been processed, it can change its associated blockchain and initiate a request to the neighboring blockchain. In the IoT network, terminal devices or nodes are vulnerable to the attack of abandon. A distributed block or node has the ability to deal with abandon because of the features of decentralization and independent of the blockchain [23]–[25], [93]–[95].

### *B. Denial-of-Service Attack*

In a DoS attack, the attacker sends so many transactions to the target node that it exceeds its processing capability, leaving it with no resources to handle the transactions from other nodes. A DoS attack is one of the popular attacks in the blockchain and in IoT. We can construct effective logical algorithms to prevent IoT from the DoS attack. The anti-DoS measures are: 1) the IoT node does not send transactions to other nodes unless it matches the entities in its key list and 2) the overlapping nodes between each private blockchain have a threshold of the maximum transaction rate. If the threshold is exceeded, the key list is updated to prevent the node from continuously sending transactions to the target node. In practice, the algorithms and mechanisms still need improvement to more effectively defend against the DoS attack [22], [23], [93]–[95].

### *C. Distributed Denial of Service Attack*

In a DDoS attack, the attacker uses multiple nodes. The anti-measures are: 1) infecting device nodes is very difficult due to the use of asymmetric encryption key management mechanism; 2) in private blockchain, node devices can only communicate with other devices by establishing a shared key between nodes; 3) the authorization is required before information exchange between different private blockchain nodes; 4) using a double-chained structure, the information transaction in the data block chain is invalid, and *vice versa*; and 5) the method of preventing DoS attacks is also useful for preventing DDoS. There are different measures to take against DDoS, for different purposes and principles; an appropriate approach should be adopted [21]–[24], [93]–[95].

### *D. Equipment Injection Attack*

Equipment injection is defined as when the attacker injects fake nodes into the network to gain access to private information. The encryption keys are suitable to resolve this attack in the IoT network. The injected device will be isolated, because local communication requires a shared key between the private blockchain nodes.

### *E. Falsify Attack*

A falsify attack occurs when the attacker generates a block by forging a transaction and creating a falsified consensus. The IoT node can detect the falsified block in the verification process by verifying the output and the owner of the ledger. In order to achieve this goal, different consensus mechanisms are the key [26], [93]–[95].

### *F. Link Attack*

Link attack occurs when the attacker uses the same ID to link transactions in multiple transactions or blockchains in the system to find real-world identifiers corresponding to anonymous nodes. A well-designed defending mechanism occurs when the node uses a unique private key in the transaction and uses a partial blind signature algorithm and a one-time public-key address [27], [93]–[95].

### *G. Modify Attack*

A modify attack occurs when stored data are modified or deleted in the system. The stored transaction includes a hash of the stored data, used as evidence to store the data, or last modified to ascertain whether the data were modified or deleted. It will not be recovered once it has been modified. A modification of the mechanism can prevent data from being modified or deleted [28], [29], [93]–[95].

### *H. Public Block Modify Attack*

A public block modify attack occurs when the attacker broadcasts a fake ledger and uses it as the longest ledger, causing other nodes to use the attacker's ledger as a real ledger in the system. The consistency algorithm used limits the number of blocks that can be generated in a time interval, which limits the number of malicious blocks that can be added, preventing an attacker from generating the longest ledger or from using it as an actual ledger [30], [31], [93]–[95].

TABLE V
BLOCKCHAIN-BASED SECURITY ATTACKS IN IoT

| Attacks | Attacking Mode | Defending Mechanism |
|---|---|---|
| **Abandon** | A node that holds auditing rights discards its members' transactions and isolates the members. | When a node finds that its transaction has not been processed, it can change its associated private blockchain and initiate a request to the neighboring private blockchain. |
| **Denial of Service (DoS)** | The attacker sends so many transactions to the target node that exceed its processing capability, leaving it with no resources to handle the transactions from other nodes. | 1) The IoT node does not send transactions to other nodes unless it matches the entities in its key list; 2) the overlapping nodes between each private blockchain have a threshold of the maximum transaction rate. If the threshold is exceeded, the key list is updated to prevent the node from continuously sending transactions to the target node. |
| **Distributed Denial of Service (DDoS)** | The attacker uses multiple nodes for a denial of service attack. | 1) Infecting device nodes is very difficult due to the use of asymmetric encryption key management mechanism; 2) in private blockchain, node devices can only communicate with other devices by establishing a shared key between nodes; 3) authorization is required before information exchange between different private blockchain nodes; 4) using a double-chained structure, the information transaction in the data block chain is invalid, and vice versa; 5) the method of preventing DoS attacks is also useful for preventing DDoS. |
| **Equipment Injection** | The attacker injects fake nodes into the network to gain access to private information. | The injected device will be isolated because local communication requires a shared key between the private blockchain nodes. |
| **Falsify** | An attacker generates a block by forging a transaction and creating a falsified consensus. | The IoT node can detect the falsified block in the verification process by verifying the output and owner of the ledger. |
| **Link** | The attacker uses the same ID to link transactions in multiple transactions or blockchains to find real-world identifiers corresponding to anonymous nodes. | The node uses a unique private key in the transaction and uses a partial blind signature algorithm and a one-time public key address. |
| **Modify** | Malicious cloud storage modifies or deletes stored data. | The stored transaction includes a hash of the stored data, used as evidence to store the data or last modified to ascertain whether the data was modified or deleted. It will not be recovered once it has been modified. |
| **Public Block Modify** | The attacker broadcasts a fake ledger and uses it as the longest ledger, causing other nodes to use the attacker's ledger as a real ledger. | The consistency algorithm used limits the number of blocks that can be generated in a time interval, which limits the number of malicious blocks that can be added, preventing an attacker from generating the longest ledger or using it as an actual ledger. |
| **Time Interval Destruction** | A malicious ledger generates multiple blocks in a consensus cycle. | Nodes can detect that the number of blocks they receive during the consensus period exceeds the number of allowed blocks, thereby reducing the trust rate of the malicious node before it is isolated. |

### *I. Time Interval Destruction Attack*

A time interval destruction attack occurs when a malicious ledger generates multiple blocks in a consensus cycle in the system. Nodes can detect that the number of blocks they receive during the consensus period exceed the number of allowed blocks, thereby reducing

TABLE VI
THREE CATEGORIZATIONS OF BLOCKCHAIN

| Category | Example | Consensus | Advantage | Disadvantage |
|---|---|---|---|---|
| Public Blockchain | Bitcoin | PoW | Decentralized, dynamic, scalable, supports a consensus of over 100,000 nodes | Consumes a lot of electricity and computing, low throughput, high latency, 51% of attacks |
| | Ethereum | PoW/PoS, Ethash, Casper | Solve the issue of PoW calculation concentration, reach a second-level consensus | Transitioning from PoW to PoS, consume more computing and electricity |
| Consortium Blockchain | Hyperledger | PBFT | Solve Byzantine failure problems, pluggable consensus mode, multiple consistency algorithms | Scenarios with fewer than 20 nodes, the algorithm complexity is high |
| | quorum | Raft/BFT | Reach a second-level consensus, the consensus result is consistent and correct | The algorithm is high complexity, a neutralization mechanism. |
| Private Blockchain | | PBFT | Able to resolve Byzantine failures and quickly reach consensus | Applicable to scenarios with less than 20 nodes, high algorithm complexity |

the trust rate of the malicious node before it is isolated [89]–[91].

## VI. Blockchain-Based Information Sharing Security Mechanism for IoT

### A. Potential Integration of Blockchain for IoT Security

The purpose of IoT information sharing security is to share information while ensuring information security. Information security includes confidentiality, integrity, availability, authenticity, traceability, and reliability.

For the requirements of security, ownership, and confidentiality, algorithms, such as the Rivest–Shamir–Adleman (RSA), Elgamal, Rabin, Diffie–Hellman (DH), and elliptic-curve cryptography (ECC) are integrated into blockchain to create mechanisms for asymmetry encryption and multisignature. The Merkle tree and its variants used in the blockchain system support simplified payment verification (SPV), which verifies transactions without needing a complete blockchain to meet integrity requirements. In addition, the Merkle tree improves the efficiency of blockchain operations by storing partial data. This is the potential that blockchain can be applied to IoT devices and systems [96]–[100].

Blockchain systems use encryption to protect data. All of the nodes need to verify the data before writing it to the block. Once it is written, users can publicly query the nodes in the blockchain network, which helps to eliminate information gains and to reduce trust costs. The node that has the authority, in blockchain needs, to mark the timestamp in the current block header as the recorder of the data. Thus, the blocks on the main chain are arranged in chronological order. As a PoE, the timestamp adds a time dimension to the data and is highly verifiable [101]. Combined with the chain structure of the blockchain, it meets the requirements of traceability. The newly generated data in the blockchain need to be verified by all or most of the nodes to be written to the shared ledger, and the ledger, then, is maintained by all blockchain nodes. Hence, it is difficult to tamper with or to have forgery committed against it.

### B. Infrastructure of Blockchain-Based Information Sharing in IoT

Blockchain is categorized into three classes (Table VI): 1) the public blockchain; 2) the consortium blockchain; and 3) the private blockchain. There are no centralized official organizations or regulatory agencies in the public chain. Participating nodes are free to enter and to leave the network. The right to read and write data is not limited by the system. The number of participating nodes in the public chain is large, and the trust degree of the nodes is the lowest among the three categories of blockchain. The consortium blockchain comprises institutions and other agencies. It applies only to members. The permissions of participation, read, and write are based on specific rules. Compared with the public chain, the consortium chain has fewer nodes, with a certain degree of trust among the nodes. Typical consensus algorithms are the Byzantine fault tolerance (BFT) and PBFT. The private chain is established by the private organization itself, and different nodes have different permissions. The private chain assumes that the participating nodes do not attack and further relax the assumption of the consensus mechanism. Typical consensus mechanisms are Paxos and Raft; these do not consider Byzantine failures [102], [103].

TABLE VII
SCENARIOS OF BLOCKCHAIN-BASED IoT SECURITY

| Scenarios | | Security Issues | Effects of Blockchain |
|---|---|---|---|
| Decentralized and Disintermediated Platform | | Information leakage, forgery or spoofing | Decentralization<br>Transparency |
| Data Processing & Provenance | | Data transmission, cross-network authentication | Openness<br>Fairness |
| Public Services | The Healthcare Industry | EMR, information sharing, smart wearables | Encryption<br>Privacy |
| | Traffic Management | Information delivery, verification and access control | Time Order |
| | Smart City & Home | Individual privacy, network security | |

Blockchain applications are primarily based on the public chain. Any node can freely join the blockchain network and can maintain ledger data. This makes the public chain more credible, but identification and data privacy can lack safety. First, the public network is used for different scenarios of IoT, such as smart traffic, smart healthcare, smart agriculture, etc. Second, the consortium chain is used for different areas of the scenario. Consortia are formed in different authorities of the same industry. Only a member of the alliance can maintain the blockchain data, while other nonauthorized nodes cannot. Finally, the private chain is used between the nodes in the area. Only these nodes can maintain the data. This fundamentally eliminates the possibility of unauthorized nodes accessing the data. Since the data block chain is mainly used for source data collection, the requirements of timeliness and security are higher than that of the transaction block chain. The private chain is more appropriate and secure; the transaction blockchain can adopt the consortium or the public chain, according to the specific application scenario [11]–[15].

## VII. IoT Security Scenarios Under Blockchain

The challenge for IoT security is the existing ecosystem of IoT servers and user terminals. Device connectivity and information processing on the central server cannot accommodate the rapidly evolving transactions. The adoption of blockchain can improve the IoT system and can raise the security level of the entire platform [28]. This section highlights major applications of the blockchain-based IoT security (Table VII), such as a decentralized platform, data processing and provenance, public services, the healthcare industry, traffic management, data provenance, and smart city and home use.

### *A. Framework of Blockchain-Based IoT Security Application*

Both blockchain and IoT are characterized by decentralization and distribution. Security features, such as authentication and data security storage, have the potential to address security issues. Blockchain is used to enhance the security of IoT and is classified into the physical untrusted domain and the blockchain domain (Fig. 4). The physical untrusted domain contains different types of IoT terminal devices. The device sends information possessed (e.g., device identity information, location information, transaction information, etc.) to the network in the blockchain domain and in the blockchain system. The node completes the encrypted recording and the storage of information to ensure the authenticity and integrity of the device domain information in IoT.

### *B. Decentralized and Disintermediated IoT Platform*

The integration of the blockchain and IoT will change the original relationship between the involved entities. IoT has the potential to connect all the things, and blockchain can achieve value transfer and benefit sharing. On the basis of the interconnections of people, things, and platform, the blockchain establishes nodes, in a production relationship, that automatically form a connection based on the programs and protocols. This is a revolutionary change to the business model based on a centralized platform. Although IoT implements the decentralized communication of peer nodes, the relationship between nodes still depends on centralized third-party intervention. Hence, the future business model may build a weak centralized or decentralized paradigm. The impact of a third party on the entire platform ecosystem will be reduced [26].

With the development of wireless communication technologies, more and more IoT application scenarios have been achieved. The intervention of a third party not only increases costs but it also reduces efficiency. User information may also be compromised. Blockchain enables P2P payments without third-party intervention. As a complementation, decentralization and centralization will be complemented into a more powerful and secure IoT system. Vehicle of Things is one of the rapidly developing fields [104].

### *C. Data Processing & Provenance System*

Blockchain can be used to process private data, effectively preventing data loss and damage caused by malicious attacks. Blockchain protects information by data encryption. The output hash is encrypted using the private key. For verification, the receiver decrypts the hash string using the public key, and then recalculates the hash to validate integrity. Once the data are stored in blockchain, users can access the data and can manage their private information without having to access the original data. Users can also use blockchains to protect the copyright and ownership of their property, such as patents, videos, music, etc. [90]–[92], [105].

Blockchain records data in blocks associated with secure protocols, thereby improving the security of the entire blockchain network. Blockchain can monitor and manage malicious IoT-related devices. Once the data or the device appears to be abnormal, the corresponding protection program will be immediately executed, in order to ensure the security and reliability of the system. For example, the integration of food safety and IoT enables complete monitoring of the food production and transportation chains. Blockchain guarantees the authenticity and integrity of a variety of food manufacturing processes [106]–[108].

### D. Public Services

The public services of IoT have been extended to all aspects of people's lives, such as the healthcare industry, traffic management, and smart cities. However, there are still many security problems when using IoT in public services. The blockchain technology can provide protection to prevent privacy leakage and the security of service data transmission in public services.

*1) Healthcare Industry:* A blockchain-based IoT healthcare system enables the processing of smart contract information among different parties, such as the patient, doctor, insurance company, and pharmaceutical supplier, in a safe, transparent, scalable environment. The medical data are stored in a common ledger and are processed smoothly. Specifically, electronic medical records (EMRs) will be more convenient and more scalable to adopt through the use of the decentralized blockchain platform [109]–[113]. Moreover, smart wearable devices are increasingly being applied in the medical industry [114], [115]. For example, a smart bracelet can detect an individual's heart rate and can record the user's movements and sleep conditions. This information can be recorded and transmitted to the terminal nodes connected to IoT. Blockchain encrypts personal information to ensure the integrity and the security of the information.

*2) Traffic Management:* The inclusion of IoT has greatly improved the performance of transportation, but there are still great security risks. For instance, information obtained through electronic sensors needs to be shared with users through a traffic command center. There may be a delay in the information distribution process; users may not get information on time. If the database is attacked, the entire transportation system will be stagnant. IoT traffic effectively uses sensors, communication technologies, and AI and combines with blockchain to build an open distributed network. Each user can receive traffic information directly and can share current traffic status. In the near future, driverless automatic driving can be achieved with the use of the blockchain-based IoT platform [116]–[118].

*3) Smart City:* The IoT is a powerful system that provides residents with sufficient resources and convenient services in a smart city system, which consists of smart home, smart health, smart energy, smart traffic, smart parking, and smart cleaning. A smart city system is a comprehensive ecosystem in which individual information is stored and the related requested transactions occur. The answers to questions regarding how to keep personal information private and secure, how to ensure the safe and effective use of available resources, and how to improve the smooth operation of the entire system are related to the common development of people and society. Blockchain is becoming more and more popular in practice, adopting encryption protocols and consensus mechanisms to prevent any compromise to personal information, as well as adopting a decentralized algorithm and a smart contract paradigm to construct a safe network and to guarantee a higher performance smart city system. A blockchain embedded IoT platform will not only protect individual privacy and safety for a smart city system, but it will change the original operation process from centralization to at least partial decentralization [119]–[121].

## VIII. Research Challenges and Future Trends

By adopting blockchain and related technologies, the IoT network can effectively solve data management, trust, security, and privacy issues. IoT can use the security mechanism of blockchain to establish a trusted encryption system and to improve network security performance. However, unlike general blockchain techniques that are typically applied to a distributed system, the communication of IoT devices is highly dependent on the underlying physical characteristics (e.g., the bandwidth and performance of communication). When the communication quality is poor, the communication between the nodes will be unequal. This will cause problems, such as the inability to verify the block and waste computing resources, and it will destroy the consistency of the blockchain system. On the other hand, due to the large number of IoT devices and data, the generation rate of blockchains and the capacity of blocks are very high. Blockchain can enhance the security of IoT, but the application of blockchain in IoT runs contrary to the low block capacity of blockchain and the channel propagation. Therefore, the application of blockchain enhances the security of IoT. However, there are still some technical issues in practice, including the performance of IoT data processing, consensus mechanisms, network bandwidth and capacity limitations, unreliable data communication, and the inconsistency of block recording.

### A. Technical Challenges

*1) Performance of IoT Data Processing:* The computing power and the storage capacity of IoT devices are, generally, weak. This restricts the application of blockchain in IoT security. Cryptography is the basis for ensuring the security and the reliability of blockchains. Especially, in the consortium chain, it is necessary to use data signature technology for transaction identification and identity authentication and to protect privacy through data encryption technology. For some IoT devices, it is impossible to perform signature or encryption because of their poor computing performance. Currently, hardware encryption engines, such as integrated security chips, can provide signature/encryption computing capabilities and can improve device encryption computing power. In addition, the account data of the blockchain node needs to consume a large amount of storage space and, usually, IoT devices cannot meet the storage requirements. Not all information is necessary to be recorded in the distributed ledger. It is better to distinguish which type of data needs to be recorded and which type of data can be recorded by other methods [38]–[40], [78].

*2) Consensus Mechanisms:* In the public chain, the PoW algorithm is used to implement the consensus mechanism. Although the PoW mining algorithm solves the transaction consistency problem, it causes a lot of wasted resources. In addition, mining incentives can lead to highly concentrated mining pools. The decentralized design has a long-term consensus period, with only seven transactions per second. In the consortium chain, the BFT algorithm is used to implement the consensus mechanism, which solves the problem of low efficiency and high resource consumption of the PoW algorithm. The BFT algorithm provides a large number of signature verifications for comprehensive P2P communication monitoring anomalous behavior. But the communication complexity is high, which brings heavy system overhead and reduces the consensus efficiency and the node scalability. This is far from meeting the blockchain requirements for IoT security expectation. Hence, consensus algorithms need to be modified and improved in order to meet the development of IoT security [11], [15], [101].

*3) Network Bandwidth:* The application of the blockchain has spread, and the number of nodes in the distributed ledger system has also increased. In the P2P architecture network, only a small number of nodes are interconnected, and the current network can fulfill its bandwidth requirements. In future IoT applications, the number of nodes in blockchain will be increasing sharply. The large number of interconnections and broadcasts between nodes can easily cause broadcast storms and can consume too much network bandwidth. As a result, the performance of the IoT network could be degraded or even paralyzed. As one type of cloud computing, edge computing has the potential to deal with distributed nodes communication. It is likely that the problem of network bandwidth requirements for large-scale deployment blockchains can be solved in IoT [4], [7], [43].

*4) Unreliable Data Communication:* Unlike computer nodes in the Internet, IoT devices are affected by the transmission of physical underlying information. IoT devices can communicate via wireless access, such as by distributed drones and automotive network communications. If the quality of the wireless link is poor, the information transmission of the node will be unreliable, resulting in a change in the topology of the blockchain network. The verification node would not be able to receive the information of some devices normally, resulting in an incomplete data process in the blockchain system. Since the blocks are stored in a chronological order, node communication is unreliable, and lost data cannot be recovered [44]–[47], [84].

*5) Inconsistency of Block Recording:* In the IoT, the amount of data generated varies by location and device due to computer, communication capabilities, and services. This causes the node to synchronize the IoT data record and the block sequence, resulting in a network node. Incomplete or inconsistent records can result in inconsistent (forked) blockchains. The hierarchical blockchain architecture is one of the ways to solve the inconsistency problem. The upper main blockchain verifies and stores the entire network data by deploying nodes with large computing power and capacity. The lower sub-blockchain manages data for some physical areas or device components and blocks blockchain data for different layers to perform block management. Record rates can vary, reducing the pressure to maintain consistency across large network sizes [93], [107], [116].

### *B. Research Trends*

*1) New Blockchain-Based Business Mode:* In the future, IoT will connect devices together to process data transactions. It is also desirable that devices connected to IoT will have intelligent various applications and will work independently, under given rule logic, to achieve commercial value. It is necessary to reliably record the transaction requests sent by smart devices, in order to ensure the validity of transactions. For the IoT, under the current centralized architecture, it may be difficult to accomplish the above-mentioned autonomous collaboration and effective transactions because the parties involved in such collaboration and transactions often belong to different stakeholders and have difficulty determining trust relationships. Thus, the cooperation and the transactions of IoT devices can only be performed under the same trust domain. This greatly reduces the actual commercial value of IoT applications.

Blockchain can provide direct transactions for trusted intermediaries. Autonomous distributed P2P telemetry (ADEPT) is a joint authentication system developed by IBM and Samsung, using blockchain. This technology builds a distributed network of smart devices and verifies the feasibility of a decentralized IoT architecture. ADEPT enables the devices connected to it to communicate securely and efficiently and to implement complex business logic. For example, when its level of washing powder is insufficient, the smart contract control of the washing machine in a home can directly purchase the powder from the supplier, and blockchain will directly confirm the order and complete the payment operation between the smart devices connected to the ADEPT. The blockchain of things has the potential to develop the smart of things [1]–[4], [122].

*2) Integration of Blockchain and Edge Computing for IoT Security:* Edge computing is an open platform that integrates network, computing, storage, and application core functions on the side close to the source, in order to provide near-end services. Its applications are launched at the edge, accelerating the responsiveness of Web services and meeting the industry's basic needs for real-time business, application intelligence, and security and privacy protection [123].

Although edge computing reduces the security of IoT, the coverage of edge computing is severely limited by the large number of terminal devices in IoT. Security issues continue to be exposed, leading to unresolved security issues in IoT and to many new security issues in edge computing. These can result in no security measures for data in edge computing devices, data leakage, data tampering, data corruption, and a lack of privacy. From the perspective of edge computing, its security systems fall into four categories: 1) data security; 2) identity authentication; 3) privacy protection; and 4) access control. Blockchain can deal with trust issues, data security issues, identity permission issues, and privacy protection issues in nonsecure environments, as well as other issues [56], [124].

*3) Double-Chained IoT Security Scheme:* In view of the lack of credit guarantee mechanisms and the information safety problems in IoT, information sharing, data tampering, and decentralization research have been carried out. Moreover, a lightweight information sharing security mechanism of IoT is another direction for growth. Based on the blockchain, the data blockchain and the transaction blockchain can be combined into a double-chain mode to protect data collection and information transactions. Specifically, the data blockchain uses the consensus mechanism to form a data ledger to prevent tampering or destruction of the stored data; meanwhile, the transaction blockchain provides decentralized, tamper-proof, traceable, and efficient ledger to support payment activities and behavioral records between the different nodes of IoT [1], [125].

*4) Interoperability of IoT, Blockchain, and 6G:* Integrating blockchain into IoT will enhance the effectiveness and improve the overall performance of the entire IoT system. Both IoT and blockchain have the potential to be employed for the development of the next generation of mobile communication 6G. 6G will be a more distributed network that will achieve seamless connection throughout space, sea, sky, and land. As a comprehensive network, IoT will assist to accomplish all potential connections of 6G; as a distributed platform, blockchain will be used for each single terminal to guarantee the security and performance of 6G. How to adjust the infrastructures of IoT and the transaction procedure of the blockchain will be an interesting question [1], [4], [8], [10].

## IX. Conclusion

The IoT will be increasingly combined with technologies, such as AI, big data, cloud computing, and deep learning. Security issues and the corresponding technologies will become more and more abundant and advanced. In addition to traditional security methods, the security of IoT will be integrated with the blockchain to make information and systems more reliable and more stable.

Both blockchain and IoT have the feature of decentralization, which makes integration more likely. Blockchain offers reliable information interaction, complete data storage, trusted node authentication, and other security functions. In IoT, the blockchain can provide access authentication, data protection, and anti-DDoS attacks on a large number of devices, effectively providing privacy and anonymity protection for IoT devices, and reducing single points through flexible data interaction and node consensus. The risk of failure may be exacerbated by malicious attacks, such as botnets. However, while on the one hand, block generation inconsistency will occur due to the huge difference in the computing and communication capabilities of IoT devices, on the other hand, accessing large devices will result in a huge increase of data in the blockchain. This adds to the challenges for the data processing and storage capabilities of the blockchain system. In future applications, blockchain systems need to be further improved to support IoT security more effectively.

Developing a security infrastructure for the IoT requires collaboration, coordination, and integration for each IoT-related entity. Blockchain has the capability of stimulating seamless communication and the interaction of related devices within the IoT ecosystem. Based on the blockchain, the data in IoT can be converted into blocks with a decentralized structure and can be constructed into a mutual trust mechanism by smart contracts and by other blockchain-based protocols. The blockchain consensus mechanism and decentralized platform provide a secure and scalable environment for IoT to achieve a truly distributed database and a consistent architecture. Blockchain has the potential to implement advanced performance paradigms for IoT, in order to prevent security attacks and privacy breaches.

## References

[1] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[2] L. D. Xu and W. Viriyasitavat, "Application of blockchain in collaborative Internet-of-Things services," *IEEE Trans. Comput. Soc. Syst.*, vol. 6, no. 6, pp. 1295–1305, Dec. 2019, doi: 10.1109/TCSS.2019.2913165.

[3] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Kona, HI, USA, 2017, pp. 618–623.

[4] Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019.

[5] S. Li and L. Xu, *Securing the Internet of Things*. Cambridge, MA, USA: Syngress Publ., 2017.

[6] S. Li, L. Xu, and S. Zhao, "The Internet of Things: A survey," *Informat. Syst. Front.*, vol. 17, no. 2, pp. 243–259, 2015.

[7] A. Whitmore, A. Agarwal, and L. D. Xu, "The Internet of Things—A survey of topics and trends," *Informat. Syst. Front.*, vol. 17, no. 2, pp. 261–274, 2015.

[8] Y. Lu, "Industry 4.0: A survey on technologies, applications and open research issues," *J. Ind. Inf. Integr.*, vol. 6, pp. 1–10, Jun. 2017.

[9] Y. Lu, "Artificial intelligence: A survey on evolution, models, applications and future trends," *J. Manag. Anal.*, vol. 6, no. 1, pp. 1–29, 2019.

[10] Y. Lu and X. Zheng, "6G: A survey on technologies, scenarios, challenges, and the related issues," *J. Ind. Inf. Integr.*, vol. 19, Sep. 2020, Art. no. 100158.

[11] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, *Blockchain Technology: Beyond Bitcoin*, vol. 2, Appl. Innovat. Inst., San Francisco, CA, USA, 2016, pp. 6–10.

[12] M. Pilkington, "Blockchain technology: Principles and applications," in *Handbook of Research on Digital Transformations*. Cheltenham, U.K.: Edward Elgar Publ., 2016, ch. 11.

[13] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Honolulu, HI, USA, Jun. 2017, pp. 557–564. [Online]. Available: http://ieeexplore.ieee.org/document/8029379/

[14] Y. Yuan and F.-Y. Wang, "Blockchain and cryptocurrencies: Model, techniques, and applications," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 9, pp. 1421–1428, Sep. 2018.

[15] F. R. Yu, J. Liu, Y. He, P. Si, and Y. Zhang, "Virtualization for distributed ledger technology (vDLT)," *IEEE Access*, vol. 6, pp. 25019–25028, 2018.

[16] Y. Lu, "The blockchain: State-of-the-art and research challenges," *J. Ind. Inf. Integr.*, vol. 15, pp. 80–90, Sep. 2019. [Online]. Available: https://doi.org/10.1016/j.jii.2019.04.002

[17] Y. Lu, "Blockchain and the related issues: A review of current research topics," *J. Manag. Anal.*, vol. 5, no. 4, pp. 231–255, 2018. [Online]. Available: https://doi.org/10.1080/23270012.2018.1516523

[18] Y. Lu, "Blockchain: A survey on functions, applications and open issues," *J. Ind. Integr. Manag.*, vol. 3, no. 4, 2018, Art. no. 1850015. [Online]. Available: https://doi.org/10.1142/ S242486221850015X

[19] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.

[20] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[21] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017.

[22] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Security Appl.*, vol. 38, pp. 8–27, Feb. 2018.

[23] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[24] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[25] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[26] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[27] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for Internet of Things security: A position paper," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 149–160, 2018.

[28] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. (AICCSA)*, Agadir, Morocco, Nov. 2017, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/7945805/

[29] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[30] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[31] X. Wang *et al.*, "Survey on blockchain for Internet of Things," *Comput. Commun.*, vol. 136, pp. 10–29, Feb. 2019.

[32] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Addressing security and privacy issues of IoT using blockchain technology," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 881–888, Jan. 2021.

[33] B. K. Mohanta, A. Sahoo, S. Patel, S. S. Panda, D. Jena, and D. Gountia, "DecAuth: Decentralized authentication scheme for IoT device using ethereum blockchain," in *Proc. IEEE Region 10 Conf. (TENCON)*, Kochi, India, 2019, pp. 558–563.

[34] S. S. Panda, B. K. Mohanta, U. Satapathy, D. Jena, D. Gountia, and T. K. Patra, "Study of blockchain based decentralized consensus algorithms," in *Proc. IEEE Region 10 Conf. (TENCON)*, Kochi, India, 2019, pp. 908–913.

[35] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100227.

[36] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial Internet of Things," *J. Comput. Sci. Commun.*, vol. 9, pp. 533–546, Oct. 2016.

[37] O. Alphand *et al.*, "IoTChain: A blockchain security architecture for the Internet of Things," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Barcelona, Spain, 2018, pp. 1–6.

[38] P. Danzi, A. E. Kalor, C. Stefanovic, and P. Popovski, "Analysis of the communication traffic for blockchain synchronization of IoT devices," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kansas City, MO, USA, May 2018, pp. 1–7.

[39] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. IEEE 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, PyeongChang, South Korea, 2017, pp. 464–467.

[40] K. R. Özyılmaz and A. Yurdakul, "Work-in-progress: Integrating low-power IoT devices to a blockchain-based infrastructure," in *Proc. IEEE Int. Conf. Embedded Softw. (EMSOFT)*, Seoul, South Korea, Oct. 2017, pp. 1–2.

[41] H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing, "Hyperconnected network: A decentralized trusted computing and networking paradigm," *IEEE Netw.*, vol. 32, no. 1, pp. 112–117, Jan./Feb. 2018.

[42] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *IJ Netw. Security*, vol. 19, no. 5, pp. 653–659, 2017.

[43] J. C. Song, M. A. Demir, J. J. Prevost, and P. Rad, "Blockchain design for trusted decentralized IoT networks," in *Proc. IEEE 13th Annu. Conf. Syst. Syst. Eng. (SoSE)*, Paris, France, Jun. 2018, pp. 169–174.

[44] 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. IEEE 3rd Int. Conf. Comput. Commun. (ICCC)*, Chengdu, China, Dec. 2017, pp. 1180–1184.

[45] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018.

[46] N. Rifi, E. Rachkidi, N. Agoulmine, and N. C. Taher, "Towards using blockchain technology for IoT data access protection," in *Proc. IEEE 17th Int. Conf. Ubiquitous Wireless Broadband (ICUWB)*, Salamanca, Spain, Sep. 2017, pp. 1–5.

[47] G. Ayoade, V. Karande, L. Khan, and K. Hamlen, "Decentralized IoT data management using blockchain and trusted execution environment," in *Proc. IEEE Int. Conf. Inf. Reuse Integr. (IRI)*, Salt Lake City, UT, USA, Jul. 2018, pp. 15–22.

[48] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, 2018.

[49] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst.*, Bhubaneswar, India, Dec. 2017, pp. 1–6.

[50] R. Agrawal *et al.*, "Continuous security in IoT using blockchain," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Calgary, AB, Canada, Apr. 2018, pp. 6423–6427.

[51] N. Szabo, *The Idea of Smart Contracts*, Nick Szabo's Papers Concise Tuts., Washington, DC, USA, Jun. 1997. [Online]. Available: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html

[52] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proc. 23rd ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 254–269.

[53] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," IACR Cryptol. ePrint Archive, Lyon, France, Rep. 2015/675, 2015. [Online]. Available: http://eprint.iacr.org/2015/675.pdf

[54] C. S. Kouzinopoulos *et al.*, "Implementing a forms of consent smart contract on an IoT-based blockchain to promote user trust," in *Proc. IEEE Innovat. Intell. Syst. Appl. (INISTA)*, Thessaloniki, Greece, Jul. 2018, pp. 1–6.

[55] W. Viriyasitavat, T. Anuphaptrirong, and D. Hoonsopon, "When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities," *J. Ind. Inf. Integr.*, vol. 15, pp. 21–28, Sep. 2019. [Online]. Available: https://doi.org/10.1016/j.jii.2019.05.002

[56] D. Xu, L. Xiao, L. Sun, and M. Lei, "Game theoretic study on blockchain based secure edge networks," in *Proc. IEEE Int. Conf. Commun. China (ICCC)*, Oct. 2017, pp. 1–5, doi: 10.1109/ICCChina.2017.8330529.

[57] S. Biswas, K. Shaif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework for secure transactions in IoT," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4650–4659, Jun. 2019, doi: 10.1109/JIOT.2018.2874095.

[58] C. Li and L.-J. Zhang, "A blockchain based new secure multi-layer network model for Internet of Things," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, Honolulu, HI, USA, Jun. 2017, pp. 33–41.

[59] U. Banerjee, C. Juvekar, A. W. Arvind, and A. P. Chandrakasan, "An energy-efficient reconfigurable DTLS cryptographic engine for end-to-end security in IoT applications," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, San Francisco, CA, USA, 2018, pp. 42–44.

[60] T. Faisal, N. Courtois, and A. Serguieva, "The evolution of embedding metadata in blockchain transactions," in *Proc. IEEE Int. Joint Conf. Neural Netw. (IJCNN)*, Rio de Janeiro, Brazil, 2018, pp. 1–9.

[61] M. Banerjee, J. Lee, Q. Chen, and K.-K. R. Choo, "Blockchain-based security layer for identification and isolation of malicious things in IoT: A conceptual design," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Hangzhou, China, Jul. 2018, pp. 1–6.

[62] A. Freier, P. Karlton, and P. Kocher, "The secure sockets layer (SSL) protocol version 3.0," IETF, RFC 6101, 2011.

[63] T. Dierks and E. Rescorla, "The transport layer security (TLS) protocol version 1.2," IETF, RFC 5246, 2008.

[64] M. Korczyński and A. Duda, “Markov chain fingerprinting to classify encrypted traffic,” in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, Toronto, ON, Canada, 2014, pp. 781–789.

[65] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, “DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks,” *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sep. 2017.

[66] C. Tselios, I. Politis, and S. Kotsopoulos, “Enhancing SDN security for IoT-related deployments through blockchain,” in *Proc. Conf. Netw. Funct. Virtualization Softw. Defined Netw. (NFV-SDN)*, Berlin, Germany, Nov. 2017, pp. 303–308.

[67] K. Fan *et al.*, “Blockchain-based secure time protection scheme in IoT,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4671–4679, Jun. 2019, doi: 10.1109/JIOT.2018.2874222.

[68] G. Zyskind, O. Nathan, and A. S. Pentland, “Decentralizing privacy: Using blockchain to protect personal data,” in *Proc. Security Privacy Workshops (SPW)*, San Jose, CA, USA, 2015, pp. 180–184.

[69] L. Wu, X. Du, W. Wang, and B. Lin, “An out-of-band authentication scheme for Internet of Things using blockchain technology,” in *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, Maui, HI, USA, Mar. 2018, pp. 769–773.

[70] R. Lu, “A new communication-efficient privacy-preserving range query scheme in fog-enhanced IoT,” *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2497–2505, Apr. 2019.

[71] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, “Querying in Internet of Things with privacy preserving: Challenges, solutions and opportunities,” *IEEE Netw.*, vol. 32, no. 6, pp. 144–151, Nov./Dec. 2018.

[72] S. Linoy, H. Mahdikhani, S. Ray, R. Lu, N. Stakhanova, and A. Ghorbani, “Scalable privacy-preserving query processing over ethereum blockchain,” in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Atlanta, GA, USA, Jul. 2019, pp. 398–404.

[73] H. Mahdikhani, R. Lu, Y. Zheng, J. Shao, and A. A. Ghorbani, “Achieving $O(\log^3 n)$ communication-efficient privacy-preserving range query in fog-based IoT,” *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5220–5232, Jun. 2020.

[74] D. Li, W. Peng, W. Deng, and F. Gai, “A blockchain-based authentication and security mechanism for IoT,” in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Hangzhou, China, Jul. 2018, pp. 1–6.

[75] S.-C. Cha and K.-H. Yeh, “An ISO/IEC 15408-2 compliant security auditing system with blockchain technology,” in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Beijing, China, May 2018, pp. 1–2.

[76] W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, “An anti-quantum transaction authentication approach in blockchain,” *IEEE Access*, vol. 6, pp. 5393–5401, 2018.

[77] O. J. A. Pinno, A. R. A. Gregio, and L. C. E. De Bona, “ControlChain: Blockchain as a central enabler for access control authorizations in the IoT,” in *Proc. IEEE Global Commun. Conf.*, Singapore, Dec. 2017, pp. 1–6.

[78] A. Boudguiga *et al.*, “Towards better availability and accountability for IoT updates by means of a blockchain,” in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, Paris, France, Apr. 2017, pp. 50–58.

[79] D. W. Kravitz and J. Cooper, “Securing user identity and transactions symbiotically: IoT meets blockchain,” in *Proc. Global Internet Things Summit (GIoTS)*, Geneva, Switzerland, Jun. 2017, pp. 1–6.

[80] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, “Smart Contract-Based Access Control for the Internet of Things,” *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1594–1605, Apr. 2019.

[81] D. Hussein, E. Bertin, and V. Frey, “A community-driven access control approach in distributed IoT environments,” *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 146–153, Mar. 2017.

[82] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, “Network-level security and privacy control for smart-home IoT devices,” in *Proc. IEEE 11th Int. Conf. Wireless Mobile Comput. Netw. Commun. (WiMob)*, Abu Dhabi, UAE, 2015, pp. 163–167.

[83] M. Chiang and T. Zhang, “Fog and IoT: An overview of research opportunities,” *IEEE Internet Things J.*, vol. 3, no. 6, pp. 854–864, Dec. 2016.

[84] X. Liang, J. Zhao, S. Shetty, and D. Li, “Towards data assurance and resilience in IoT using blockchain,” in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Baltimore, MD, USA, Oct. 2017, pp. 261–266.

[85] M. Singh, A. Singh, and S. Kim, “Blockchain: A game changer for securing IoT data,” in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Singapore, Feb. 2018, pp. 51–55.

[86] E. Karafiloski and A. Mishev, “Blockchain solutions for big data challenges: A literature review,” in *Proc. IEEE 17th Int. Conf. Smart Technol.*, Ohrid, Macedonia, Jul. 2017, pp. 763–768.

[87] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, “Blockchain based data integrity service framework for IoT data,” in *Proc. IEEE Int. Conf. Web Serv.*, Honolulu, HI, USA, Jun. 2017, pp. 468–475.

[88] S. T. Zargar, J. Joshi, and D. Tipper, “A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks,” *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2046–2069, 4th Quart., 2013.

[89] A. Sahi, D. Lai, Y. Li, and M. Diykh, “An efficient DDoS TCP flood attack detection and prevention system in a cloud environment,” *IEEE Access*, vol. 5, pp. 6036–6048, 2017.

[90] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, “A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers,” *J. Supercomput.*, vol. 74, pp. 6428–6453, Apr. 2017.

[91] A. Dorri, S. S. Kanhere, and R. Jurdak, “Towards an optimized blockchain for IoT,” in *Proc. ACM 2nd Int. Conf. Internet Things Design Implement.*, Pittsburgh, PA, USA, 2017, pp. 173–178.

[92] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the IoT: Mirai and other botnets,” *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[93] R. H. Weber, “Internet of Things—New security and privacy challenges,” *Comput. Law Security Rev.*, vol. 26, no. 1, pp. 23–30, 2010.

[94] B. Lee and J.-H. Lee, “Blockchain-based secure firmware update for embedded devices in an Internet of Things environment,” *J. Supercomput.*, vol. 73, no. 3, pp. 1152–1167, 2017.

[95] A. Banafa, *IoT and Blockchain Convergence: Benefits and Challenges*, IEEE Internet Things, Piscataway, NJ, USA, 2017. [Online]. Available: https://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html

[96] A. Al Hasib and A. A. M. M. Haque, “A comparative study of the performance and security issues of AES and RSA cryptography,” in *Proc. 3rd Int. Conf. Converg. Hybrid Inf. Technol.*, vol. 2. Busan, South Korea, 2008, pp. 505–510.

[97] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, Jul. 1985.

[98] M. Bellare and P. Rogaway, “The exact security of digital signatures-how to sign with RSA and Rabin,” in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, 1996, pp. 399–416.

[99] L. Harn, M. Mehta, and W.-J. Hsin, “Integrating Diffie-Hellman key exchange into the digital signature algorithm (DSA),” *IEEE Commun. Lett.*, vol. 8, no. 3, pp. 198–200, Mar. 2004.

[100] X. Du, M. Guizani, Y. Xiao, and H.-H. Chen, “Transactions papers a routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks,” *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1223–1229, Mar. 2009.

[101] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, “Survey of consensus protocols on blockchain applications,” in *Proc. IEEE 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Coimbatore, India, 2017, pp. 1–5.

[102] M. Vukolić, “The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication,” in *Proc. Int. Workshop Open Problems Netw. Security*, 2015, pp. 112–125.

[103] G. Liang, B. Sommer, and N. Vaidya, “Experimental performance comparison of Byzantine fault-tolerant protocols for data centers,” in *Proc. IEEE INFOCOM*, Orlando, FL, USA, 2012, pp. 1422–1430.

[104] W. He, G. Yan, and L. D. Xu, “Developing vehicular data cloud services in the IoT environment,” *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1587–1595, May 2014.

[105] L. Zhou, L. Wang, Y. Sun, and P. Lv, “BeeKeeper: A blockchain-based IoT system with secure storage and homomorphic computation,” *IEEE Access*, vol. 6, pp. 43472–43488, 2018.

[106] T. Dey, S. Jaiswal, S. Sunderkrishnan, and N. Katre, “HealthSense: A medical use case of Internet of Things and blockchain,” in *Proc. IEEE Int. Conf. Intell. Sustain. Syst. (ICISS)*, Palladam, India, Dec. 2017, pp. 486–491.

[107] J. Cheney, L. Chiticariu, and W.-C. Tan, “Provenance in databases: Why, how, and where,” *Found. Trends Databases*, vol. 1, no. 4, pp. 379–474, 2009.

[108] F. Tian, “An agri-food supply chain traceability system for China based on RFID & blockchain technology,” in *Proc. IEEE Int. Conf. Serv. Syst. Serv. Manag.*, Kunming, China, Jun. 2016, pp. 1–6.

[109] F. Tian, “A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things,” in *Proc. Int. Conf. Serv. Syst. Serv. Manag. (ICSSSM)*, 2017, pp. 1–6.

[110] R. Guo, H. Shi, Q. Zhao, and D. Zheng, “Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems,” *IEEE Access*, vol. 6, pp. 11676–11686, 2018.

[111] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[112] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE 18th Int. Conf. e-Health Netw. Appl. Serv. (Healthcom)*, Munich, Germany, Sep. 2016, pp. 1–3, doi: 10.1109/HealthCom.2016.7749510.

[113] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare: 'MedRec' prototype for electronic health records and medical research data," in *Proc. IEEE Open Big Data Conf.*, vol. 13, 2016, p. 13. [Online]. Available: https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a∼10e7346780f4ab0a.pdf

[114] L. Catarinucci *et al.*, "An IoT-aware architecture for smart healthcare systems," *IEEE Internet Things J.*, vol. 2, no. 6, pp. 515–526, Dec. 2015.

[115] J. Wei, "How wearables intersect with the cloud and the Internet of Things: Considerations for the developers of wearables," *IEEE Consum. Electron. Mag.*, vol. 3, no. 3, pp. 53–56, Jul. 2014.

[116] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC)*, Rio de Janeiro, Brazil, Nov. 2016, pp. 2663–2668.

[117] 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 Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.

[118] Y. Gupta, R. Shorey, D. Kulkarni, and J. Tew, "The applicability of blockchain in the Internet of Things," in *Proc. 10th Int. Conf. Commun. Syst. Netw.*, Bengaluru, India, Jan. 2018, pp. 561–564.

[119] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *Proc. IEEE 18th Int. Conf. High Perform. Comput. Commun. IEEE 14th Int. Conf. Smart City IEEE 2nd Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Sydney, NSW, Australia, Dec. 2016, pp. 1392–1393.

[120] R. Rivera, J. G. Robledo, V. M. Larios, and J. M. Avalos, "How digital identity on blockchain can contribute in a smart city environment," in *Proc. IEEE Int. Smart Cities Conf. (ISC2)*, Sep. 2017, pp. 1–4.

[121] J. Branger and Z. Pang, "From automated home to sustainable, healthy and manufacturing home: A new story enabled by the Internet-of-Things and industry 4.0," *J. Manag. Anal.*, vol. 2, no. 4, pp. 314–332, 2015.

[122] M. Samaniego and R. Deters, "Internet of Smart Things—IoST: Using blockchain and clips to make things autonomous," in *Proc. IEEE Int. Conf. Cogn. Comput. (ICCC)*, Honolulu, HI, USA, 2017, pp. 9–16.

[123] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2017.

[124] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Netw.*, vol. 32, no. 3, pp. 78–83, May/Jun. 2018.

[125] Y. Qian *et al.*, "Towards decentralized IoT security enhancement: A blockchain approach," *Comput. Elect. Eng.*, vol. 72, pp. 266–273, Nov. 2018.

**Li Da Xu** (Fellow, IEEE) received the B.S. and M.S. degrees in information science and engineering from the University of Science and Technology of China, Hefei, China, in 1978 and 1981, respectively, and the Ph.D. degree in systems science and engineering from Portland State University, Portland, OR, USA, in 1986.

He is an Academician of the European Academy of Sciences, the Russian Academy of Engineering (formerly, USSR Academy of Engineering), and the Armenian Academy of Engineering. He is a 2016–2020 Highly Cited Researcher in the field of engineering named by Clarivate Analytics (formerly, Thomson Reuters Intellectual Property & Science).

**Yang Lu** (Member, IEEE) received the B.S. degree from Jilin University, Changchun, China, in 2004, and the M.S. degree from the University of Manchester, Manchester, U.K., in 2006, and the Ph.D. degree in information and communication technology from Old Dominion University, Norfolk, VA, USA, 2020.

He has published research papers in refereed journals published by major publishers, such as Elsevier, IEEE, Taylor & Francis, and World Scientific.

**Ling Li** received the M.A. and Ph.D. degrees from the Ohio State University, Columbus, OH, USA, in 1994 and 1996, respectively.

She is an Eminent Scholar and a University Professor with Old Dominion University, Norfolk, VA, USA, where she is the Chair of the Department of Information Technology and Decision Sciences. She has published in IEEE Transactions on Industrial Informatics, IEEE Transactions on Systems, Man, and Cybernetics: Systems, IEEE Transactions on Cybernetics, IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews, IEEE Transactions of Information Technology in Biomedicine, IEEE Internet of Things Journal, IEEE Systems Journal, and other journals.

Dr. Li served as an Associate Editor of IEEE Transactions on Industrial Informatics. She is a Certified Fellow of Association for Supply Chain Management.