Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Blockchain for Internet of things applications: A review and open issues

Fei Chen [a,b], Zhe Xiao [a,b], Laizhong Cui [a,b,*], Qiuzhen Lin [a,b], Jianqiang Li [a,b], Shui Yu [c]

[a] *College of Computer Science and Engineering, Shenzhen University, China*

[b] *National Engineering Laboratory for Big Data System Computing Technology, Shenzhen University and Guangdong Laboratory of Artificial Intelligence and Digital Economy (SZ), China*

[c] *School of Computer Science, University of Technology Sydney, Australia*

ARTICLE INFO

Keywords:
Blockchain
IoT
Access control
Data security
Trusted third party
Automatic payment
Usage paradigm

ABSTRACT

Blockchain and the Internet of things (IoT) systems are attracting more and more research efforts from both academia and industry. Blockchain is rapidly evolving to be a new infrastructure for building robust distributed applications. Similarly, Internet of things is getting increasing deployment in the context of smart city, smart home, smart healthcare, etc. On the intersection of the two emerging areas, researchers are proposing to use blockchain to build more dependable IoT systems. This paper reviews the most recent research advances in this direction during the past four years. Specifically, we review, summarize, and categorize existing research works. We divide the research works into four groups according to the roles that the blockchain plays in IoT systems, i.e., access control platform, data security platform, trusted third party, and automatic payment platform. For each group, we also discuss future research challenges. From the review, we further summarize the usage paradigms and open issues on using blockchain to build dependable IoT systems. We hope this work serves as a reference of existing models for both researchers and engineers that are interested to leverage blockchain to build future IoT systems.

1. Introduction

Blockchain has attracted considerable research attention in recent years (Underwood, 2016; Swan, 2015; Cuomo, 2016; McWaters et al., 2016). It is a kind of decentralized distributed database, which originated from Bitcoin (Nakamoto et al., 2008). It features a combinative yet creative use of existing computer science techniques such as distributed data storage, point-to-point networking, consensus mechanism, and encryption algorithm. The blockchain relies on a consensus mechanism to enable everyone to agree on newly generated data block and work together to maintain all the blocks as a unique database. The blockchain has the characteristics of equal peers, open and transparent database, difficult to tamper with, secure communication, and multiparty consensus (Drescher, 2017; Cachin and Vukolić, 2017; Beck, 2018).

For blockchain applications, most of these existing landing applications still surround the topic of virtual currency (Nakamoto, 2009; Monero Core Team, 2014; Buterin, 2015; Wilcox, 2016; Peters et al., 2015) and games (Curran, 2019; Jordan, 2019). Researchers have proposed applications in the area of Internet of Things (IoT), medical care, agriculture, logistics, etc. However, these researches are still in an early stage.

To promote a better understanding of future potential blockchain applications, this paper presents a review of existing blockchain applications *in the IoT area*. Both the IoT and the blockchain are distributed networks of P2P; they are naturally compatible. The blockchain is considered to have great application potential in IoT application scenarios, such as supply chain, smart wearable devices, smart cities, smart homes, and automatic payment, as surveyed later in this paper.

1.1. Related work

Several surveys exist for blockchain, IoT, and the application of blockchain in IoT. We briefly discuss these survey work in three categories and summarize the limitation of the state-of-the-art surveys. First, several works reviewed technical details and general applications of blockchain. Zheng et al. (2018) reviewed the technologies and applications of the blockchain, including a taxonomy of blockchain, the consensus algorithms, and general applications of blockchain. Li et al. (2020) reviewed the security attacks and security vulnerabilities of blockchain systems. Casino et al. (2019) reviewed blockchain applications in various domains, including business, education, IoT, finance, privacy, etc. Feng et al. (2019) reviewed privacy protection techniques

[*] Correspondence to: Room 622, College of Computer Science and Engineering, Shenzhen University, China.
E-mail addresses: fchen@szu.edu.cn (F. Chen), 1810272052@email.szu.edu.cn (Z. Xiao), cuilz@szu.edu.cn (L. Cui), qiuzhlin@szu.edu.cn (Q. Lin), lijq@szu.edu.cn (J. Li), shui.yu@uts.edu.au (S. Yu).

https://doi.org/10.1016/j.jnca.2020.102839
Received 28 March 2020; Received in revised form 18 August 2020; Accepted 12 September 2020
Available online 17 September 2020

1084-8045/© 2020 Elsevier Ltd. All rights reserved.

for blockchain. Wu et al. (2019) reviewed blockchain theory and also its application in IoT.

Similarly, a few works reviewed the architecture, applications, and security of IoT. Atzori et al. (2010) reviewed the vision, enabling techniques in different disciplines, and potential applications of IoT. Alfuqaha et al. (2015) presented a more technological review of IoT on its underlying communication and application protocols, and its relationships with other areas such as big data, cloud computing and fog computing. Xu et al. (2014) reviewed the specific application of IoT in industrial environments.

Different from the above review works with a focus either on blockchain or IoT, some researchers also reviewed the application of blockchain for building better IoT systems. Fernandezcarames and Fragalamas (2018) reviewed optimized blockchain for IoT in the architecture, cryptographic algorithms, message time stamping mechanisms, and consensus algorithms. Khan and Salah (2018) reviewed the security issues of IoT and discussed how blockchain can be applied to solve these security issues. Lo et al. (2019) reviewed blockchain-enabled IoT applications from two perspectives, i.e., data management and thing management. Researchers also (Ferrag et al., 2018; Makhdoom et al., 2019) reviewed recent advances in blockchain technology and its impact on IoT applications with regard to security and performance. Ali et al. (2019b) and Dai et al. (2019) reviewed approaches integrating blockchain and IoT. Yang et al. (2019) summarized the integration of blockchain and edge computing. Viriyasitavat et al. (2019) also reviewed the application of blockchain for IoT in the system design perspective. Moreover, Sengupta et al. (2020) reviewed security issues in using blockchain for IoT applications.

Limitation with the state-of-the-art review. For the first two categories, their focus is on either blockchain or IoT, individually. For the third category, the reviews are on the interaction of blockchain and IoT. However, they are either on limited applications or detailed optimized blockchain technologies. Compared with these existing surveys, we review blockchain for IoT using a novel perspective: we focus on the distinguished functionality of a blockchain that can enhance existing IoT applications. Table 1 also lists a comparison with recent, state-of-the-art reviews of using blockchain for IoT system. Moreover, we summarize the general ideas on how to employ a blockchain to build dependable IoT applications after the review; for details, please refer to Section 7. We hope these general ideas could be useful for researchers and developers that will leverage blockchain in their IoT applications.

1.2. Our contribution

We survey the most recent research efforts on building IoT systems using blockchain in recent years, analyze the current research status, and discuss the research difficulties and challenges, hoping to provide a summarization of current state-of-the-art knowledge and some guidance for future research endeavors. We investigate the IoT applications based on blockchain from four perspectives, with an aim to understand how IoT benefits from the blockchain technology. The perspectives include access control, data security, trusted third parties, and automatic payment in the IoT.

Specifically, the access control perspective focuses on the management framework of the IoT and analyzes the role of the blockchain correspondingly. The data security perspective is to analyze how the blockchain protects data provenance and data integrity of data flows in the IoT. The trusted-third-party perspective uses the intrinsic value of blockchain (i.e., decentralized trust) to build different IoT applications. The automatic payment perspective employs the most direct application of blockchain and smart contracts; this is based on the consideration that the IoT economy also has different kinds of payment requirements. Besides, for each perspective, we categorize the surveyed work into groups. We also discuss the limitations of existing researches and potential future researches.

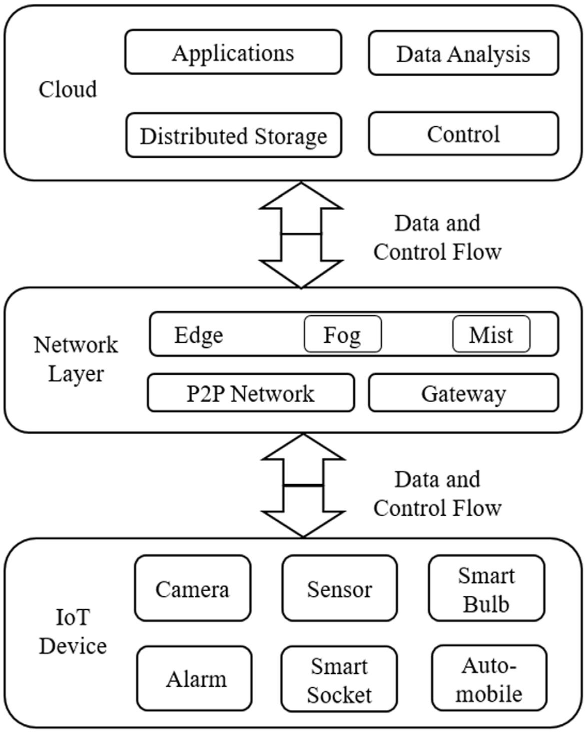


Fig. 1. Typical IoT system architecture.

The remainder of this paper is structured as follows: Section 2 overviews the basics of an IoT system and blockchain. This section also presents an explicit discussion on current challenges and difficulties in IoT, which could be solved using characteristics of the blockchain. Section 3 reviews the application of blockchain in access control for IoT systems. Section 4 reviews how blockchain could help protect IoT data provenance and integrity. Section 5 reviews how the blockchain works as a trusted third party for IoT systems. Section 6 reviews automatic payment enabled by blockchain for the IoT. Section 7 summarizes the usage paradigms of blockchain in IoT applications that we have learned in the review. Finally, Section 8 concludes the paper.

2. Background

In this section, we introduce the basics of IoT which includes the evolvement and the challenges of IoT systems. To make the paper self-contained, we also briefly present the basics of blockchain.

2.1. Overview of IoT

IoT systems establish mapping relations from the real world to the digital world using front-end computing devices and back-end services. The front-end device could be embedded computer systems equipped with sensors, such as temperature sensors, RFID tags/readers, wearable devices, flame detectors, cameras, mobile phones, etc. These front-end devices may be located in open environments, which are out of the system administrator's control. The back-end system is a software system; it integrates, processes, and analyzes the sensed information returned by the front-end devices; it may also output analyzed results to users.

Fig. 1 shows a typical three-layer IoT system (Amazon, 2019; Alibaba, 2019). The first layer is composed of IoT devices. The second layer is the communication network, where a gateway manages IoT devices in a local area and connects IoT devices to the Internet. The third layer is the service back-end, which provides storage and upper layer application services, including data processing and analysis.

Table 1
Comparison with recent reviews of using blockchain for IoT.

Year	Paper	Survey topics	Related sections in our paper	Differences/enhancements in our paper
2018	Fernandezcarames and Fragalamas (2018)	Blockchain design tailored for IoT	Section 2	Providing more detailed application oriented reviews
2018	Khan and Salah (2018)	IoT network level security using blockchain	Sections 3 & 4	Focusing more on application level usage scenarios
2018	Ferrag et al. (2018)	Blockchain threats and general IoT applications	Sections 3 & 5	Providing specific, in-depth case reviews
2019	Lo et al. (2019)	Data management and thing management using blockchain	Sections 3 & 4	Providing different review perspectives and more case reviews
2019	Makhdoom et al. (2019)	Blockchain evolvements, IoT threats, adoption challenges, coarse-grained application trends	Sections 3, 4 & 5	Providing a different perspective and a more elaborated fine-grained application reviews
2019	Ali et al. (2019b)	Blockchain basics, consensus mechanisms, typical applications in IoT systems	Sections 3, 4 & 5	Providing more specific, elaborated application reviews and comparisons
2019	Dai et al. (2019)	Approaches integrating blockchain and IoT and 5G networks	Sections 4 & 5	Providing different review perspectives and more case reviews
2019	Yang et al. (2019)	Integrated blockchain and edge computing	Section 4	Providing different review perspectives
2019	Viriyasitavat et al. (2019)	Discussing blockchain application for IoT from a system design perspective	Sections 3 & 4	Providing different review perspective and more specific, elaborated application reviews and comparisons
2020	Sengupta et al. (2020)	IoT security attacks and blockchain solutions	Sections 3 & 4	Providing more detailed application oriented reviews

Nowadays, the IoT application is gradually evolving from single applications to large-scale deployments, involving multi-organization and multi-agent collaboration. During this trend, there are also many obstacles in the development of IoT systems. We summarize the obstacles to be solved as follows:

- *Device security*. When IoT devices are in open environments, access control is a challenging issue, which aims to prevent unauthorized access.
- *Data privacy*. In the current, centralized IoT service model, the service provider cannot self-certify innocence, which may break user privacy. Also, the centralized single point of failure is likely to cause privacy leaks.
- *Architecture scalability*. The current IoT architecture is mainly based on centralized management. In the foreseeable future, the number of IoT devices will grow at a geometric level. How to handle a huge amount of IoT devices is challenging.
- *Vendor compatibility*. Currently, a unified IoT management platform and a unified language are still lacking. The communication between IoT devices provided by different manufacturers is to be resolved.
- *Multi-agent collaboration*. In its current form, an IoT system is mainly initiated and operated by a single entity. When peer collaboration is required, which relates to multiple entities (e.g., service providers and enterprises), establishing mutual trust is costly.

2.2. Blockchain basics

Blockchain structure. A blockchain is a linked list constructed by hash pointers. Each block has both data and a hash pointer directing to the previous block; it also contains a digest of the block data, which prevents any modification of the block. We use Bitcoin as an example to illustrate the basic structure.

Fig. 2 shows the block structure (Narayanan et al., 2016; Drescher, 2017). Each block consists of two parts, i.e., a block header and a block body. The block header contains the following elements: (1) `block version` which specifies the block validation rule set; (2) `nonce` which is a random number used for achieving consensus through proof of work; (3) `nBits` which is a target threshold of effective block hash used in mining a new block through proof of work; (4) `timestamp` which denotes the time; (5) `Merkle root` which is the hash digest of all the transactions contained in a block; (6) `current block hash` which is the hash value of the current block data; and (7) `previous block hash` which is the hash value of the previous block.

The transaction data in the block body is organized by a classical data structure in cryptography called *Merkle tree* (or Hash tree) (Merkle, 1987). The Merkle tree is computed as in Fig. 3. Specifically, group every two blocks and create a data structure with two hash pointers for each group. Each hash pointer corresponds to one data block. These new data structures compose the next level of the tree. Next, these data structures are again grouped in pairs and follow the same procedure as before to create another level of the tree. Finally, a binary tree is formed. The root of the tree is called *Merkle root*. The Merkle tree is able to prevent malicious modification of all the transaction data in the bottom level of the tree. Suppose one attacker wants to modify some transaction data. To avoid detection, the attacker needs to find some data to replace the data in the leaf level of the tree, with a constraint that the root value of the Merkle tree remains the same. However, this is hard because this implies a hash collision for the cryptographic hash function employed to construct the Merkle tree.

Blockchain working mechanism. Blockchain is a distributed public ledger; all nodes in the network maintain the same ledger. This requires all nodes to reach a consensus on a new block. The blockchain consensus is generally achieved by electing a miner who has the billing rights for the new block; the miner packs transactions into a new block and broadcasts the new block to the entire network. The process of miners competing for billing rights is called mining and the mechanism that enables the mining is called the consensus algorithm (Narayanan et al., 2016; Drescher, 2017). There are four main consensus algorithms: Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT).

The two most successful blockchains, i.e., Bitcoin and Ethereum, are using the PoW consensus algorithm. Ethereum is now gradually moving to PoS. We use Bitcoin's PoW as an example to show how miners get billing rights through mining. The miner first needs to listen to the transaction broadcasts on the network and verify that the signature of the transaction is valid. Miners also need to maintain a blockchain network and listen to new blocks to ensure the ledger is synchronized with the entire network and mining on the longest chain. Then the transaction data is composed into a candidate block; the miner needs to find a random number, i.e., the *nonce* in the blockhead, which is

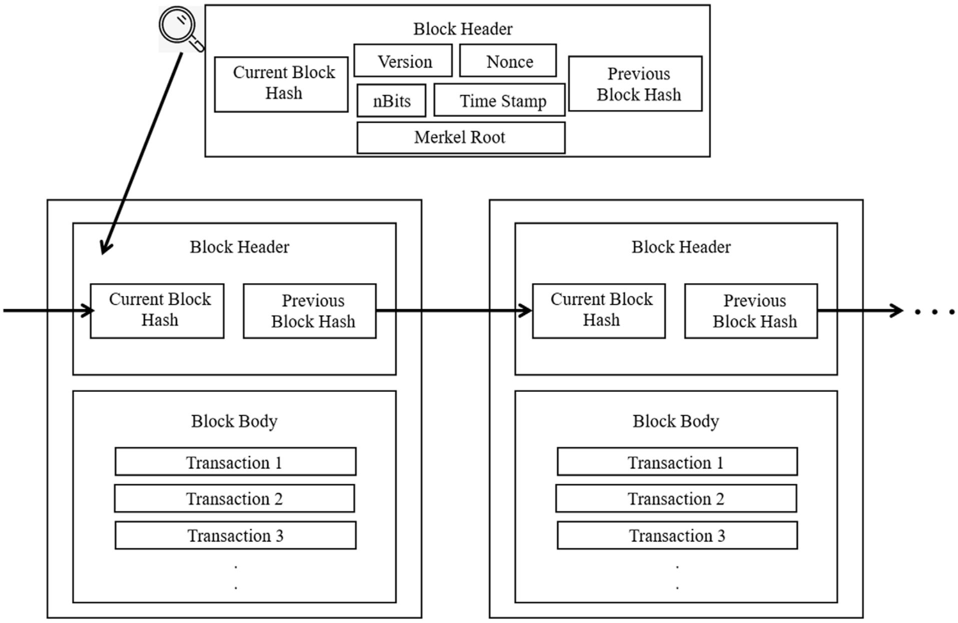


Fig. 2. Blochchain structure.

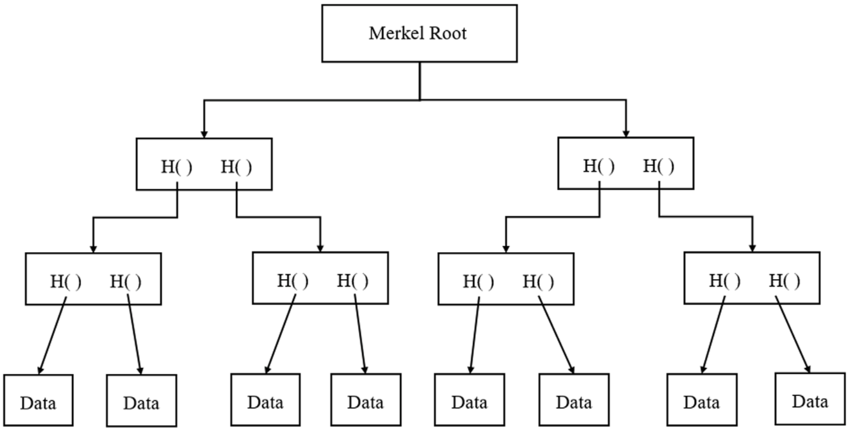


Fig. 3. Merkle tree.

the most important part of the miners' workload. When the miner finds a random number *nonce* that makes the hash of the entire block within the threshold *nBits*, the miner broadcasts the block to the entire network. Once other miners verify the block and accept the block, the block becomes the newest block of the chain. Mining then continues for the next block.

Smart contract. The concept of smart contract was first proposed several decades ago by a cross-disciplinary legal scholar, which defined a smart contract as "a set of commitments defined in digital form, including agreements on which contract participants can enforce these commitments" (Szabo, 1996). Before the blockchain appeared, smart contracts had not been widely used because of the unsolved trust problem. Although the computer system can automate the contract, the company providing the service is still able to manipulate the contract. The emergence of blockchain provides an excellent environment for smart contracts (Buterin, 2014; Kosba et al., 2016; Savelyev, 2017). The decentralization and modification-proof nature of the blockchain allow smart contracts to be trusted.

Smart contracts are not only used as commercial and legal contracts, but also are often used as an automated information exchange platform. Smart contracts can be used for access control management of IoT devices, detecting fraudulent use of valuables, handling auto insurance claims, protecting patient privacy in clinical trials, and more. Many blockchain communities have gradually provided the programming interface for smart contracts, which is promoting smart contract applications. One prominent example is the increasing usage of smart contracts of Ethereum.

2.3. Review organization

Fig. 4 briefly shows our review organization. We divide the review on blockchain for IoT applications into four areas according to the roles blockchain plays, i.e., access control platform, data security platform, trusted third party, and automatic payment platform. This categorization is upper-layer application scenario oriented; we believe this is an intuitive approach. For each area, we also categorize the review into two subgroups.

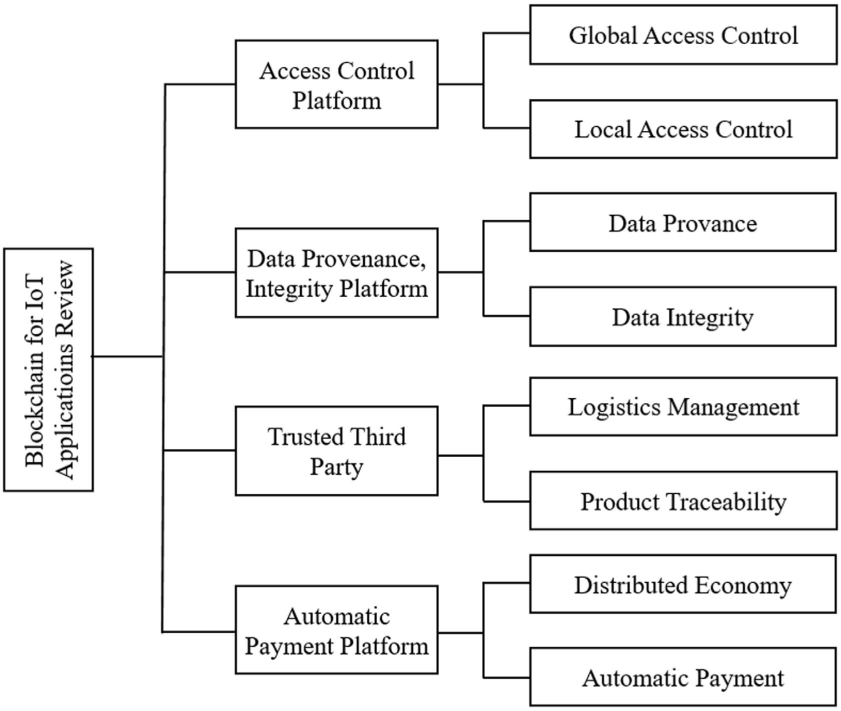


Fig. 4. Review organization.

3. Blockchain for IoT: Access control

This section reviews existing researches on applying blockchain to IoT access control. First, we introduce what access control is, explain the importance of access control to the IoT, and summarize the new requirements of IoT systems in the aspect of access control. Then in Sections 3.1 and 3.2, we review the detailed application of blockchain for IoT access control. We categorize the review into two groups. In the first group, the blockchain not only acts as a distributed ledger, but also utilizes smart contracts to provide *global* functions such as authentication, authorization, and key management according to the access control policy. We refer to the first group as global access control. In the second group, the blockchain is only used as a distributed ledger, which stores access and verification rules and separates authentication and authorization from storage in a local manner. We refer to the second group as local access control. Finally, we discuss future research challenges for blockchain based access control.

Access control is a set of methods that can tag, organize, and manage data and devices in a system (Sandhu and Samarati, 1994). Theoretically, each device can only operate on its data. However, with the development of IoT technology, IoT devices are required to be more intelligent, which demands multiple IoT devices collaborating to read and write data. But in this situation, how to ensure that data operations between devices do not cross the border? This involves access control strategies between different devices and different service providers. Access control is the first element that a device encounters when it accesses the network.

Blockchain serves as a potential solution to enable access control in IoT systems based on its ability to establish an unique trust, as reviewed in later subsections. Using blockchains to manage message flows and command flows provides transparency and reliability. However, the IoT environment puts some new challenges on access control:

- **Flexible and fine-grained control**. Access control in the IoT should not be limited to a fixed policy. Instead, according to the needs and characteristics of different subjects and objects, implementing a “customized” access control policy is needed.
- **Distributed architecture**. Nodes in the network share data with other nodes. This kind of sharing should not require the intervention of third-party entities. In this way, the management of IoT systems could be eased.
- **Lightweight implementation**. Many devices in the IoT have low memory, low power, and low computing capability. The overhead (including storage, computing, and communication) of the underlying access control mechanism should be small.
- **Scalability and Heterogeneity**. Because of the growing number of IoT devices, combined with multiple technologies and different collaborative environments, access control mechanisms should be scalable and suitable for multiple environments.

3.1. Global access control

This section reviews researches that use blockchain to implement global access control for IoT systems using smart contracts. For each reviewed work, we introduce the application scenarios and design goals of the access control scheme, outline the methods used in the proposed scheme, discuss the specific technical details, and finally summarize the advantages and disadvantages of the proposed scheme.

Tapas et al. (2018) proposed implementing access control strategies on the blockchain for the smart city application. This work aimed to reduce the trust demand for the third parties. They proposed a *Stack4Thing* framework based on the OpenStack platform. The authors' previous work implemented a role-based access control policy using the keystone subsystem in OpenStack (Longo et al., 2017). However, it faces the problem of the trusted third-party. Thus, they proposed to use smart contract instead of keystone for authentication and delegation. It uses two smart contracts to complete role-based access control. The Role.sol contract defines roles, where each role has different permissions and physical resources. The Delegation.sol contract defines the relationship between users and roles and physical resources. When a user accesses a resource, the access is redirected to Delegation.sol contract which further queries the contract Role.sol; after validation, the Delegation.sol contract returns the authorization result.

Combined together, the two contracts achieve the access control goal on chain. Compared with traditional access control, this mechanism is an enhancement of traditional methods by replacing the traditional centralized authorizer with the distributed blockchain. Using blockchain as the distributed, trusted, highly available middleware reduces the trust requirement and improves the auditability.

Zhang et al. (2018) proposed an access control mechanism for general IoT applications, which can flexibly define access control policies based on smart contracts. The proposed scheme uses three smart contracts, including the Access Control Contract (ACC), the Judge contract (JC), and the Register contract (RC). The ACC contract defines an access control policy for the objects. ACC contains the resources of the objects, the operations allowed for each resource, and the permissions of each resource to the subject. JC is used to record bad behaviors of the subject and to punish bad behaviors. RC is used to maintain and manage all subject-to-object access control mapping, which manages all operations on the ACC. To access a resource of an object, one subject queries the RC to get the address on the corresponding ACC; the subject later contacts the ACC to request the access; the ACC may also call the JC to record a malicious access request. The proposed scheme is also a kind of enhancement of traditional access control schemes. Because the storage on the Ethereum is expensive, one limitation of the scheme is that it has considerable storage and computing overhead.

Pouraghily et al. (2018) proposed an interesting blockchain based IoT access control application. They envisaged a scenario in which the camera control in a rented house should be directed to the tenant by the household. It is very convenient to use a smart contract to manage the camera's permissions. As long as the house rent contract is initiated when the lease contract is signed, the video stream information will be encrypted by the tenant's public key to ensure that the tenant's privacy is not leaked. The blockchain serves as an automatic platform that performs access control operations to protect the tenant's privacy.

Huh et al. (2017) proposed a remote IoT device management system that involves access control. They defined two smart contracts to monitor and manage the electrical devices in the home. Users can send messages through the mobile phone to control the IoT devices in the home. The blockchain mainly solves the problem of access control using a smart contract. In the contract, when the electricity consumption achieves a threshold, the contract automatically controls the air conditioner to run in energy-saving mode. In this application, blockchain also serves as an automatic access control platform. The solution has limitation in scalability. When the roles and objects in the family are larger, it is cumbersome to initialize the device information and access control information on the smart contract.

There are also many IoT application scenarios where a clear role definition is not always available. In this respect, Di Pietro et al. (2018) proposed a reputation-based IoT trust system. They used smart contract to store and implement access control policies. The system records the user's reputation and grants rights or penalizes unlawful users based on reputation. The system achieves access control in a way similar to traditional centralized authorization system; the difference now is that the centralized authorization system is replaced with a smart contract. Because assessing a user's reputation requires accessing the user's historical behavior data, one risk is that the user's privacy may be breached in the proposed scheme.

Ouaddah et al. (2016) proposed a more general framework for access control of IoT applications, which considers the new requirements of emerging IoT applications. The proposed access control framework is divided into two layers. Each organization in the first layer adopts a distributed peer-to-peer management scheme. Each organization defines and implements its own authorization policy. The second layer, due to limited device resources in the IoT environment, each organization is managed internally by an authorized management node set, which approves and manages the authentication and authorization data for the resources. Access control permissions are defined by a token similar to Bitcoin, which reduces communication costs, simplifies verification complexity, and achieves more flexibility. Although this scheme is complicated, the idea of implementing access control is still using smart contract to implement existing access control mechanisms.

Outchakoucht et al. also proposed an access control framework for the Internet of Things (Outchakoucht et al., 2017). The access control strategy is defined on the blockchain smart contracts. By introducing reinforcement learning algorithms, they dynamically adjusted the access control policies in the smart contracts. The authorization result of each access request is fed back to a third-party agent as an environment variable; the agent then returns the execution result to the contract after training. Environmental variables include factors such as trust, integrity, credit rating, and so on. The introduction of reinforcement learning can help optimize access control policies. At the same time, the introduction of the third-party agent may increase potential security risks.

Novo proposed a new IoT management architecture for role and permission arbitration (Novo, 2018). In this work, blockchain smart contracts serve as the central management entity and define access control policies on the contracts. Similarly, other researchers proposed blockchain-based IoT access control delegation framework (Ali et al., 2019a; Pal et al., 2019; Xu et al., 2018; Alphand et al., 2018). The new novelty is that these works can achieve fine-grained access to secure resources by defining a set of operations for a single resource. The blockchain is used to ensure the security, trustworthiness, verifiability, and decentralization of the delegation service. The access control strategy is also implemented using blockchain smart contracts.

3.2. Local access control

Global access control relies on smart contracts to achieve authentication and authorization services. A few disadvantages exist. The use of blockchain in the IoT is greatly limited due to high latency and low throughput. Besides, the proof of work blockchain requires large computational overhead and transaction costs. If all the large amounts of data generated by IoT devices are linked through blockchain transactions, the costs are huge, which may be unbearable. Some time-sensitive devices are also plagued by blockchain transaction delays. Therefore, researchers also proposed local access control mechanisms that move the computation to a local node while storing the detailed access control rules on the blockchain.

Barger et al. (2018) proposed to use the Hyperledger Fabric to manage the IoT access control plane. They leverage the cloud object store to store the objects off-chain, which decouples the data plane and control plane. They proposed to enable access control using smart contracts on the blockchain.

Andersen et al. (2017) proposed an access control architecture WAVE for smart city applications. The proposed scheme solves the problem of heterogeneity and cross-trust domain interaction, as well as out-of-order-delegations. The blockchain only stores access control rules, which are expressed using a data structure called trust proxy graphs (DoTs). Verifying permission only requires constructing a valid path from the visitor to the device on the DoTs, which greatly reduces the overhead of storing and managing access rights. The proposed system WAVE has been deployed more than 500 days on hundreds of devices and thousands of resources.

Shafagh et al. (2017) proposed a blockchain based distributed access control layer for sharing IoT data. The scheme also employs the method of separating the data plane from the control plane. The proposed scheme uses blockchain to store access control rules. Each data stream is defined with an access right and the data owner can cancel the sharing of data. When a data item is requested, the storage nodes in the system checks whether the access is allowed using the access rules in the blockchain. At the control plane, the proposed scheme supports low-cost data sharing with frequent update keys by introducing key regression and re-encryption-based techniques. In the data plane, using the temporal correlation of IoT data, blocks are compressed before encryption, which reduces bandwidth and storage overhead. In addition, distributed storage is advocated in the proposed scheme.

Dorri et al. (2017, 2016) proposed a blockchain based smart home application, which supports access control. The proposed scheme integrates a blockchain miner with the gateway. The gateway is responsible for authentication, authorization, auditing, and key management using traditional centralized access control methods; the blockchain is only responsible for storing access control policies and permissions. It also eliminates the need for PoW consensus, reducing latency and saving computing power. Their solution is divided into three layers, i.e., smart home layer, cloud storage layer, and overlay layer. The work (Dorri et al., 2017) discussed the design of the smart home layer in detail, while cloud storage and overlays are discussed in detail in Dorri et al. (2016). The smart home layer includes smart devices, local storage, and local blockchain. The local blockchain is a secure private chain with one or more local devices as miners. Each block in the blockchain has a policy header that holds the access control list. The overlay consists of miner nodes, which are grouped into clusters; one node is selected as the Cluster Head (CH). The CH is responsible for maintaining the blockchain of the overlay layer. Each CH maintains three tables, i.e., the list that is allowed to access the collection of resources within the cluster, the smart home list that is connected to the cluster, and the transaction list that is forwarded by other CH in the network. Cloud storage is responsible for storing data for smart devices and can create ledgers for each user and device. This is a hybrid (centralized and distributed) two-tier blockchain architecture that eliminates POW and is more lightweight.

Singh et al. also proposed a smart home access control architecture (Singh et al., 2019), which employs cloud computing to provide secure management services for smart home networks. To ensure the security of the smart home network, they proposed a security analysis method, which analyzes and identifies the correlation between the characteristics of the traffic to resist DDOS/DOS attacks. The role of the blockchain is to serve as an infrastructure layer for the IoT devices. Specifically, the blockchain is used to authenticate the devices, store data for the devices, authorize access for the devices, etc.

Wan et al. used the Bitcoin structure to design an access control architecture for the smart factory application (Wan et al., 2019). The proposed architecture has five layers: the sensing layer, the management hub layer, the storage layer, the firmware layer, and the application layer. The sensor layer is used for data collection. The management hub layer is a consensus node network that is different from the blockchain transaction nodes which are responsible for submitting transactions. It is responsible for data upload, encryption, and packaging to generate blocks. At the same time, the management hub is responsible for access control policies of the device resources. It also flexibly defines access control policies according to the needs of different requirements. The storage layer is the blockchain. The architecture uses a private chain. Multiple management hubs form a network of leading nodes. They also proposed a new algorithm that uses pre-set feature values to select the leader nodes in turn. The firmware layer involves the underlying implementation techniques to connect each layer. The proposed architecture can enhance security requirements while having better flexibility and scalability. As a management structure of a single organization, compared with the traditional centralized method, the private chain may bring a relatively large communication overhead.

Short summary. Table 2 summarizes the reviewed work on IoT access control using blockchain. The 'Policy' column indicates whether the access policy is implemented globally or locally. The 'Scenes' column means the application scenario of the work. The 'Objectives' is design goal of the access control scheme; 'D' denotes 'Distributed'; 'F' denotes 'Flexible and Fine-grained'; 'L' denotes 'Lightweight'; 'S' denotes 'Scalable'. The 'Position' column is a description of which layer of the IoT architecture in Fig. 1 is implemented in each work. The 'Role' column indicates the role of the blockchain. The 'Disadvantage' column lists the shortcomings of those works. As is shown in Table 2, most of the works have only solved two challenging issues. Because in different scenarios, the requirements for access control, security, privacy, time sensitivity, and memory sensitivity vary a lot. Correspondingly, the demand for blockchain performance is different. When the blockchain is used as a tamper-proof database, it only needs to provide strong integrity protection and auditability. When blockchain smart contract is used to implement the access control policy, it requires multiple interactions and high throughput. The advantage of the first approach is the ability to automate access control validation, while the second approach reduces the throughput burden of the blockchain. Regarding the pros and cons of the two approaches, it depends on the detailed application scenario. Indeed, the access control in the reviewed works comes in different forms, e.g., centralized and distributed.

3.3. *Future research challenges*

Current IoT systems are rapidly evolving in its scale and architecture. The IoT devices are growing; new techniques, such as cloud computing, fog computing, etc, are employed in IoT systems. Many challenges need to be solved to design blockchain-based access control schemes for IoT. One challenge is on performance. The scale of the IoT is growing sharply and managing IoT devices that grow exponentially is a great challenge to the performance of blockchain. The throughput and latency issues of the blockchain may affect the efficiency of IoT management. In particular, the blockchain based on the PoW consensus not only has the problem of throughput and delay, but also consumes a lot of computing resources.

Another challenging issue is on user privacy protection. Blockchain uses consensus to maintain a ledger. All the nodes are able to see the transactions. Enforcing access control on the chain may leak user's privacy because whether subjects are able to access an object is recorded on the chain. In order to prevent such leakage, techniques such as zero-knowledge proof could be used for privacy protection. However, it may incur more complexity and inefficiency. The design also depends on the detailed application.

Security of the smart contract that enforces access control is also an issue. There are also many security issues about the blockchain itself. Although the blockchain is considered to contribute to the security protection of the IoT, the combination of the two technologies however is still difficult to guarantee the overall security of the IoT system. Smart contracts may be implemented with flaws. For example, Ethereum was found to have transaction order dependencies, time stamp dependencies, re-entrant attacks, contract calls vulnerabilities, etc., which could be exploited by hackers. This may lead to system anomalies, unauthorized access, privacy issues, etc., which is thus also a major threat to the IoT system security.

4. Blockchain for IoT: Data provenance and integrity

In this section, we review recent research works using blockchain to protect the provenance and integrity of IoT data. We first briefly introduce what data provenance and data integrity mean for IoT and then review detailed research works. Correspondingly, we categorize existing researches into two groups: one is to ensure data provenance; another is to protect data integrity.

Data provenance is a kind of data security mechanism that describes the origin of the data, the owner of the data, and the transformations on the data (Buneman et al., 2001). Data integrity denotes that the data is not tampered with; thus, the data could be trusted (Denning and Denning, 1979).

With the advent of the era of big data, data is more valuable than ever. The demand for data continues to grow, and at the same time, the requirements for data security continue to increase. IoT systems generate massive amounts of data; for example, many smart devices and sensors are collecting data. Therefore, IoT systems urgently need

Table 2
Blockchain for IoT: Access control platform.

Work	Policy	Scenes	Objectives	Position	Role	Disadvantages
Tapas et al. (2018)	Global	Smart city	D	Layer 3	TPA	Not flexible
Zhang et al. (2018)	Global	Normal	D,F	Layer 2	TPA	Heavy weight
Pouraghily et al. (2018)	Global	Hardware sharing	D	Layer 2	TPA	Low scalability
Huh et al. (2017)	Global	Smart home	D	Layer 2	TPA	Low scalability
Di Pietro et al. (2018)	Global	Normal	D,S	Layer 2	TPA	Data security
Ouaddah et al. (2016)	Global	Normal	D,F,S	Layer 2	TPA	Computing limit
Outchakoucht et al. (2017)	Global	Normal	D,F,S	Layer 2	TPA	Security problem
Novo (2018)	Global	Normal	D,F	Layer 2	TPA	Low scalability
Barger et al. (2018)	Local	Normal	D,L	Layer 2	DB	Incomplete
Andersen et al. (2017)	Local	Smart city	D,L,S	Layer 2	DB	Not flexible
Shafagh et al. (2017)	Local	Normal	D,F	Layer 2	DB	Extra storage overhead
Dorri et al. (2017, 2016)	Local	Smart home	D,L	Layer 2	DB	Extra time overhead
Singh et al. (2019)	Local	Smart home	D,F,S	Layer 2	DB	Computing burden
Wan et al. (2019)	Local	Smart factory	D,F,S	Layer 2	DB	Communication overhead

data security solutions. Due to the distributed nature of the IoT, centralized solutions such as traditional data protection schemes, firewalls, log audits, etc. may not be applicable. In contrast, blockchain is distributed, difficult to tamper, which is thus considered to be suitable for protecting IoT data security. We now review existing recent research works in this direction with a focus on data provenance and integrity.

4.1. Data provenance

Ramachandran and Kantarcioglu (2018) proposed a system called *SmartProvenance* to protect data provenance. In the proposed scheme, the blockchain records the data provenance path. The data source is agreed through a voting smart contract. They also used a tracking smart contract to record data dynamic paths. For new data modification, the operation is first verified by participants in the blockchain, and is then voted to get approval through a random threshold voting contract on the chain. The proposal strengthens the supervision and management of data provenance and improves auditability.

Liang et al. (2017) proposed a data provenance scheme in cloud environments, where data is generated by cloud users. They proposed a *ProveChain* architecture in which the blockchain is used as a distributed security database and as a distributed trust center to protect user privacy. In the ProveChain solution, the first is to use a "hook" technique to monitor, collect user operations, and collect provenance data. This is different from monitoring with a contract in Ramachandran and Kantarcioglu (2018). The data is then hashed into a Merkle tree which is anchored into the blockchain. When the provenance data is stored in the blockchain, the user ID is hashed and cannot be associated with the real identity, which protects user privacy. Finally, the auditor retrieves the transaction from the blockchain to verify the data provenance. It is worth noting that ProveChain is also a centralized architecture; in this application, the blockchain serves as a platform for building trust of the provenance data.

The above two solutions for securing data sources mainly record the data source path, improve auditability, and rely on third parties to audit and verify the data. In contrast, Casado-Vara et al. (2018) proposed a different method to improve data quality and false data detection. By introducing a cooperative algorithm based on game theory, the algorithm runs in the edge computing layer of IoT systems, reducing the error caused by the IoT sensor. The blockchain is used for ensuring the data origin by storing the sensed data into the sidechain controlled by the IoT gateway. Later, the sidechain data is packed and inserted into the outside blockchain. This reduces the interaction of the device with the blockchain and increases throughput.

In the medical field, the reliability of data provenance is highly valued; there are also more stringent requirements on the authenticity and quality of the provenance data. Clinical trials recruit volunteers and collect medical data from volunteers, for which ensuring data quality and protecting volunteer privacy are extremely important. Angeletti et al. (2017) proposed the use of blockchain to protect the provenance of medical data and volunteer privacy. The collected data is first hashed by the IoT gateway; later, the hash is recorded in the blockchain. The IoT data still remains in the volunteers' IoT device side. Only after the volunteers joining in the final clinical trial, the data is transmitted to the clinical research institute. To protect the reliability of data provenance, the institute validates the data using the hash that has been previously recorded in the blockchain. Griggs et al. (2018) proposed the use of blockchain to protect the data security of remote patient monitoring systems. The medical data collected by the sensors is uploaded directly to the smart contract through the blockchain nodes. By analyzing and processing medical data, the contract automatically informs patients and medical staff, thereby achieving real-time patient monitoring and medical intervention. Blockchain nodes are deployed at the data collection layer to protect the privacy and security of the source data.

4.2. Data integrity

Krishnan et al. (2018) proposed an architecture, which is similar to the typical IoT-cloud architecture shown in Fig. 1, for data security protection of IoT applications, e.g., a smart city application. It proposed to use middleware as a common interface between IoT devices and the cloud applications. Middleware is responsible for subsystem data routing, terminal device registration and management, and sensor data storage. The access control policy is implemented between the second layer and the third layer. The innovation lies in the use of blockchain for data integrity protection between sensors and gateways. The sensed data is hashed into linked blocks. It also adds an RSSI parameter related to signal strength to protect the unforgeability of communication data. This work is a direct application of the blockchain technique.

Song et al. (2018) proposed using Hyperledger Fabric to protect data integrity and availability in the IoT-cloud architecture. With Fabric's containerization, the network operates as a separate private system between the edge and the cloud. Each edge node runs a Hyperledger Fabric node; all sensor data are packed into blocks and recorded in the blockchain. The proposed scheme relies on the tamper-proof and decentralized property of the blockchain to protect IoT data integrity and availability.

Liu et al. (2017) also proposed to introduce blockchain in the IoT cloud framework. The difference is to use Ethereum to store cloud data hashes. They defined four smart contracts that express the agreement between users and cloud service providers to verify data integrity. The integrity and availability protecting idea is similar to Song et al. (2018). One limitation of the prosed scheme is the high expense that is needed to run the smart contracts.

The blockchain is also employed to protect the integrity of car mileage data and prevent odometer fraud (Chanson et al., 2017). Existing solutions to solve odometer fraud has serious privacy issues because data is published to public databases. To mitigate the privacy leakage, Chanson et al. used blockchain to record car mileage data and protected user privacy through encryption using the user's private key. The hash of the encrypted data is stored in a public blockchain, e.g. Ethereum. The decentralized nature of the blockchain ensures that no third party can manipulate the data.

Data in the medical field is very sensitive. Researchers also attempted to use blockchain to secure electronic medical records (EMR). Azaria et al. (2016) proposed a distributed record management system *MedRec* which uses blockchain technology to manage EMR. The solution addresses issues including data ownership, data privacy, and data integrity for different patients and different hospitals. Data ownership is achieved using patient authorization. Data privacy is obtained by encryption using the patient's key. Data integrity is guaranteed by hashing patients' encrypted data and sending the hash to the tamper-proof blockchain. The proposed scheme used three smart contracts: the first is the Registration Contract (RC), which manages the identity of the entity; the second is the Patient–Provider Relationship Contract (PPR), which records the patient's relationship with the medical institution and access rights; the third is the Summary Contract (SC) which is responsible for managing and locating PPR. The three smart contracts combined together protect data security. The main role of the blockchain is still to serve as a decentralized, immutable database.

To improve data protection and blockchain performance, Gaetani et al. (2017) proposed a two-layer blockchain architecture. The first layer is a private chain; it uses a lightweight consensus protocol to improve throughput and quickly reach a consensus. The second layer uses a public chain based on the POW consensus to periodically embed the hash value of the data from the first layer chain into the second layer POW blockchain. It achieves data integrity protection in the public PoW blockchain level; it also reduces resource consumption and improves throughput.

In the power generation area, Gai et al. (2019) proposed using blockchain to protect user data privacy in power transactions in neighboring areas. In order to prevent link attacks from data mining algorithms, they used blockchain smart contracts to implement power transactions and proposed an account protection mechanism to hide user account information. Liang et al. (2019) proposed to use blockchain to protect data transmission security in the power grid. Dabbaghjamanesh et al. proposed an optimization algorithm to solve the problem of power allocation planning while using blockchain to protect the data security and privacy of its process. Similarly, researchers also proposed to use blockchain to protect communication key distribution using blockchain in the edge computing scenario of smart grids (Wang et al., 2019), and to protect privacy for IoT devices (Cha et al., 2018; Yu et al., 2018; Puthal et al., 2018).

Short summary. Table 3 lists a summary of reviewed works on blockchain based IoT data security. The 'Scenes' column means the application scenario of the work. The 'platform' column is the public blockchain platform that was used. The 'Contract' column indicates whether the work used smart contracts. The 'Data' means what kind of data is stored in blockchain. The 'Advantage' column lists the strengths of those works. As is shown in Table 3, most of the works used Ethereum to protect data security. Only a few works choose to use smart contracts.

4.3. Future research challenges

Currently, blockchain serves as a preliminary solution to data security of IoT data as reviewed above. To make these solutions practical, a couple of research challenges need to be solved in future. The first is on new approaches to increase performance. In current blockchain systems, performance is often an issue, especially for the public chain. Compared with the public blockchain, the consortium blockchain has higher throughput and stronger control ability; however, it requires higher trust requirements than the public blockchain. Therefore, combining the consortium blockchain and the public blockchain is a potential solution. Other solutions are also possible, which remain to be studied.

Another research challenge is to improve data provenance reliability. In existing researches, blockchain is used to protect the provenance data; but in fact, the blockchain cannot really guarantee the reliability of the data source which is input by real world entities. Similarly, the blockchain can build trust in different trust domains, but it only guarantees that the data exchange and storage is not tampered with and leaked. Indeed, the blockchain is hard to recognize the validity of the input data. Therefore, it is often necessary to seek a way to prove that the input data is correct, which is difficult and application dependent. Cryptographic mechanisms such as authentication and digital signature could be used to establish such a reliability. This approach may add costs for the blockchain and smart contracts. Other approaches remain to be studied.

Ensuring the security of smart contracts is also challenging. A smart contract is a piece of code that can be executed automatically. However, code could also be vulnerable and be attacked. Indeed, real world contracts have been attacked (Dice2Win Team, 2019). When employing smart contracts to protect IoT data security, approaches to ensure the contract code and logic security worth studying.

5. Blockchain for IoT: Trusted third party

In this section, we review how blockchain works as a role of the trusted third party. We first present the importance of a trusted third party for online services. Then we review the trusted third party application of blockchain in the IoT area of supply chain management (SCM). At the end, we also discuss future research challenges faced in this area.

Trust is the core of online transactions that spread among different, remote parties. Traditionally, people use the endorsement of an authority to establish a bridge of trust between buyers and merchants. However, the cost of such mechanism maintaining a trusted third party is enormous. This is because trusted third parties need to establish a set of public databases and provide a range of functions, such as customer service, transaction management, processing claims, and fund settlement. This means that trusted third parties must be "honest" and "responsible". Further, trusted third parties face significant risks. Because trusted third parties manage all transaction data and provide services to customers and merchants, many external and internal attacks exist. Once a trusted third party server is down, all connected services are interrupted.

Blockchain, with its specificity of distributed trust, has become a solution for replacing traditional third parties. Through decentralization, distributed storage, and other mechanisms, blockchain ensures that all nodes in the system can automatically and securely exchange data in a lack of trust. Replacing or reducing the original trusted third party with blockchain automates the management processes, reduces costs, and increases overall efficiency. Moreover, the blockchain cannot be modified, which ensures the consistency and integrity of the data. Thus, blockchain can exert its potential in many areas by establishing a global trust.

We divide the reviewed IoT based supply chain solutions using blockchain as a trusted third party into two categories. The first is logistics management; the second is product traceability. In logistics management, the blockchain is mainly used to integrate the core data of each part of the supply chain, which helps to analyze the performance of supply chain management. Later, smart contract is used to realize the automation of the transaction processes of involving parties. In product

Table 3
Blockchain for IoT: Data provenance and integrity platform.

Work	Scenes	Platform	Contract	Data	Advantages
Ramachandran and Kantarcioglu (2018)	Data platform	Ethereum	Yes	Data path	Supervision and auditability
Liang et al. (2017)	Cloud computing	Prove chain	No	User operations	Data reliability
Casado-Vara et al. (2018)	Smart home	Ethereum	No	Sensor data	Data accuracy
Angeletti et al. (2017)	Medical	Ethereum	No	Dash(medical data)	Data quality and user privacy
Griggs et al. (2018)	Medical	Ethereum	Yes	Sensor data	Real-time
Krishnan et al. (2018)	Smart city	Uncertain	No	Hash(sensor data)	Collected data integrity
Song et al. (2018)	Cloud computing	Hyperledger	No	Sensor data	High throughput
Liu et al. (2017)	IoT-Cloud	Ethereum	Yes	Hash(cloud storage)	Low storage overhead
Chanson et al. (2017)	Odometer fraud	Ethereum	No	Hash(mileage data)	Blockchain potential application
Azaria et al. (2016)	Medical	Ethereum	Yes	Electronic medical records	Secure and flexible
Gaetani et al. (2017)	IoT-Cloud	Uncertain	No	Hash(cloud storage)	Balanced blockchain performance

traceability, the role of the blockchain is mainly to provide a database that cannot be tampered with to prevent fraud. It is worth noting that product traceability is broader in scope than data provenance that we have discussed in Section 4.1. Data provenance focuses on the origin of an entity; in contrast, product traceability focuses on all states of many related entities during their life cycles. Data sources, destinations, and intermediate processes in product traceability are more diverse than data provenance.

5.1. Logistics management

The purpose of supply chain management is to optimize supply chain operations at minimal cost. The method is to coordinate all the resources in each enterprise and role involved in the supply chain from the beginning of the purchase order to the final customer confirmation. The blockchain improves the reliability of the supply chain by increasing the constraints on the various steps and roles, i.e., improving the exchange of information. Blockchain can therefore rely on its information integration capabilities to securely collect data for assessing the performance of supply chain management without the participation of a third party.

Hackius and Petersen (2017) surveyed a number of relevant practitioners to understand their views on blockchain technology and supply chain management. The final conclusion is that practitioners generally believe that supply chain management will benefit from blockchain technology and that blockchain technology is likely to be applied in supply chain management. Tijan et al. (2019) also investigated many cases and studied the possibility and challenges of blockchain technology in supply chain management.

Kuhi et al. (2018) studied the performance evaluation model of supply chain management and compared the benefits of different blockchain technologies as a solution. The work was based on early cross-industry performance assessment coordination, which divided the performance indicators of supply chain management into three layers. The first layer is the performance index (PI) calculated according to the measurement technical parameters (TP) of the resources involved; the second layer is the key performance indicator (KPI) generated by different PIs; the third layer is the overall performance index calculated by the KPI. They then evaluated the technical characteristics and advantages of several blockchain techniques for this problem. Specifically, the Ethereum smart contract is powerful, but has the expense of privacy and performance issues; Hyperledger addresses privacy and performance scaling issues through PBFT and fine-grained access control, but requires more trust. In this work, the blockchain is thus used to validate and verify the supply chain data, which further ensures the accuracy of these indicators. Similarly, Fu and Zhu (2019), proposed a blockchain-based supply chain risk assessment model

Arumugam et al. (2018) proposed an intelligent logistics solution consisting of three components, Smart Contracts System (SCS), Logistics Planner (LP), and Condition Monitoring (CM). The SCS is used to establish consumer and supplier terms, including time, price, responsibility and accountability, etc. The SCS also accepts updates from the planner and the status monitoring module to determine whether the performer is performing according to the terms and conditions based on the updated message. If there is a violation of the rules, it may fine or cancel the order. The LP is responsible for designing and implementing the optimal transportation solution. The CM is used to deploy intelligent hardware to collect and process data at multiple levels and locations. This work realizes the upper-level planning in the logistics industry and divides the whole into three modules. Smart contracts implement responsibility division and accountability mechanisms. Combined with IoT smart devices and artificial intelligence, planning, monitoring and tracing products are made possible. Blockchain and smart contracts replace the role of trusted third parties, which has the advantage of simplifying logistics management processes, reducing management costs, and improving the quality of service for users.

Li et al. (2018) used blockchain as a logistics management solution for charitable donations. The biggest challenge in philanthropy is that it is difficult to establish trust between fund raisers, recipients, and non-profit organizations. The charity logistics management platform proposed in this work provides a platform for information sharing among donors, charities, government supervision departments, and recipients. At each important point, the government oversight department acts as a responsible party to supervise the data. It uses smart contracts to complete complaints and penalty functions. They simulated the social welfare generated by social welfare activities based on the classic maximum flow algorithm and proved that the blockchain platform can increase the trust of charity projects. In this scenario, the government's oversight function is difficult to replace, but the need for third-party data management is eliminated. The blockchain provides a platform for public information sharing, which is also a form of trusted third party.

Because most researches on blockchain in logistics applications are mainly focused on the technical part and business process modeling, there is no unified standard for validating the overall solution and strategy. To solve this issue, Perboli et al. (2018) designed a standard method for designing blockchain technology use cases for logistics applications. They defined roles, functions, relationships, and key elements in logistics. They also validated their approach in a food use case.

5.2. Product traceability

Blockchain is also used to trace the supply chain and identify authenticity. The function of the blockchain in supply chain management is mainly to provide distributed ledgers, collect and manage information, and improve the transparency of information. Many companies have begun a pilot to use blockchain technology for tracing products. The academic community is also actively discussing the feasibility of the traceability using blockchain. Korpela et al. (2017) discussed the state and development trends of blockchain-based digital supply chains at the time in 2017.

The purpose of product traceability is to protect product quality. Zhang et al. believed that blockchain plays an important role in the quality control of supply chain management (Zhang et al., 2019). In a milk production use case, they discussed a method for blockchain to manage supply chain data and control the quality of milk production. There are 6 major processes in milk production , including harvesting, transportation, storage, testing, processing, and packaging. Storing the provenance information of raw materials on the blockchain can enable manufacturers to track the source, time, production, transportation and distribution of raw materials throughout the production life cycle. The data stored on the blockchain requires the approval of multiple stakeholders, which increases data responsibility and transparency. At the same time, blockchain can also simplify device management, including verification and authorization.

RFID technology is the key technology in the field of traceability to connect real-world items to the digital world. But the current research on RFID technology relies on the traditional centralized database. In order to better apply the blockchain in the field of traceability, Sidorov et al. (2019) proposed a robust ultra-lightweight two-way authentication RFID protocol. The blockchain is used to assist the authentication of RFID tags and store the tracing data from the tags securely on the chain. They performed a detailed security analysis and the protocol was secure in terms of key disclosure, replay, man-in-the-middle, desynchronization, and tracking attacks. The protocol can help build a lightweight and secure blockchain-based supply chain management system.

Li and Wang (2018) proposed a blockchain traceability framework to achieve traceability of agricultural products and ensure the authenticity of the agricultural products. First, physical sensors are installed in the farm to collect information about fertilization, watering, pests, etc. The sensed data are automatically input into the tracing system. This work uses Oracle's blockchain cloud service *BCS* and its front-end open source framework to build a blockchain-based traceability solution. The blockchain serves as a platform to store the sensed data.

Christidis and Devetsikiotis (2016) also discussed the application of blockchain for supply chain management. For the roles of manufacturer, dealer, and the consumer, a blockchain maintains a public database in which the data updates are encrypted and verified. Each role that maintains this public database together verifies data updates. The blockchain also serves as a trusted platform to store the supply chain data.

Abeyratne and Monfared (2016) proposed a conceptual model of supply chain management based on blockchain for cardboard box manufacturing. In the process of making cardboard boxes, RFID tag is used as input to the system. When the wood enters the supply chain, it is tagged; later, each hand-over step can scan the tag to read the data and write new data. The rights management is done by smart contract. In this way, every step in the supply chain can be traced back. Similar to previous works, the traceability relies on the dependability of the data, which is assured by the blockchain.

Cao et al. proposed a steel supply chain traceability system (Cao et al., 2019). They combine blockchain, sensors, RFID and GPS technologies to manage and trace the production, distribution, consumption and supervision of steel. Each product has an RFID tag, which is the virtual identity of the product in the system. The product traceability system can track product information through the electronic product code system and product RFID tags at the distribution nodes. The system can trace the source of the product from bottom to top. The data is transparent to the consumer and the consumer can confirm the product quality. At the same time, products can be tracked from top to bottom. Once problems are found, they can be located and dealt with in time. They implemented and validated the system on the Hyperledger platform.

Westerkamp et al. (2018) proposed a distributed supply chain management system based on blockchain smart contracts. In their proposed system, goods are represented by tokens. Tokens can be transferred, split, combined and authenticated. Token represents the circulation of goods in various roles in the network, just like the way products are circulated in reality. They implemented the system in Ethereum and evaluated the system. The system has strong scalability and flexibility. The transaction records of tokens are stored on the blockchain, which is difficult to tamper with and facilitates the traceability of commodities. However, the reliability of the mapping relationship between tokens and commodities is a potential problem; that is, how to determine the accuracy of the input data is a potential concern.

Short summary. Table 4 summarizes the reviewed work on supply chain management using blockchain. The 'Scenes' column means the application scenario of the work. And the "Challenges" indicates the challenges that the work needs to face. As is shown in Table 4, most of those works use Ethereum and *Smart Contract*, because the supply chain management Because supply chain management requires automated services provided by *Smart Contract*. Meanwhile, the three challenges we discussed are the common challenges of most blockchain-based supply chain management solutions.

5.3. Future research challenges

Saberi et al. (2019) systematically analyzed the obstacles of blockchain based supply chain management, which includes four aspects: obstacles from within the supply chain organization, barriers to supply chain partnerships, system-related barriers to implementing blockchain in the supply chain, and challenges from external stakeholders.

We discuss three further research challenges. The first research issue is on improving throughput. Low throughput is the bottleneck of blockchain technology, which limits the application of blockchain. For supply chain management, the volume of data that are managed could be very large. This requires a large throughput of the blockchain. Potential solutions could use ledger sharding, private chain, different consensus protocols, and off-chain techniques.

The second is asset digitization. The problem of asset digitization is the issue of associating physical things with digital ledgers. The blockchain can only guarantee the trust inside the system. For external data, the blockchain cannot verify it. In order to realize the value of the blockchain, asset needs to be digitized. Potential solutions could be divided into two categories. One is the introduction of a third party that can prove the reliability of the input data. But this may sacrifice part of the decentralization property. Another is to solve the digitization problems of assets using novel techniques. This may require the development of IoT devices which can enable unique identification in the real world.

The third issue is error tolerance. The blockchain is a tamper-proof ledger; however, in the event of an error, the loss may be irreparable. This is different from a centralized solution where a centralized solution can roll back the database after an error. At present, this problem seems to be difficult to solve; it relies on increasing the degree of centralization. However, this also depends on the underlying application scenario. The requirements in many scenarios should not be completely decentralized due to requirements for supervision.

6. Blockchain for IoT: Automatic payment platform

This section reviews economics and payments in IoT systems based on blockchain. For modern IoT systems, payment is a natural requirement. This is because human life is becoming more and more digitalized; for example, smart meters which are typical IoT devices are used to charge electricity and water usage. Then the corresponding

Table 4
Blockchain for IoT: Trusted third party.

Work	Scenes	Blockchain platform	Smart contract	Challenges
Hackius and Petersen (2017)	Logistics and supply chain	/	/	Regulatory uncertainty, benefit quantization.
Kuhi et al. (2018)	Performance measurement in logistics	Ethereum	Yes	Throughput, error tolerance.
Arumugam et al. (2018)	Smart logistics	Ethereum	Yes	Throughput, asset digitization, error tolerance.
Li et al. (2018)	Public philanthropy logistics	Ethereum	Yes	Throughput, asset digitization, error tolerance.
Perboli et al. (2018)	Food logistics management	Ethereum	Yes	Throughput, asset digitization.
Zhang et al. (2019)	Smart manufacturing	Ethereum	Yes	Throughput, asset digitization.
Sidorov et al. (2019)	Product traceability	/	/	Throughput, error tolerance.
Li and Wang (2018)	Agricultural product tracking	BCS (Oracle's blockchain cloud service)	Yes	Throughput, asset digitization, error tolerance.
Christidis and Devetsikiotis (2016)	Container tracking	Uncertain	Yes	Throughput, asset digitization, error tolerance.
Abeyratne and Monfared (2016)	Cardboard supply chain tracking	Ethereum	Yes	Throughput, asset digitization, error tolerance.
Cao et al. (2019)	Steel supply chain tracking	Hyperledger	Yes	Asset digitization, error tolerance.
Westerkamp et al. (2018)	Supply chain tracking	Ethereum	Yes	Throughput, asset digitization, error tolerance.

payment is also digitalized using credit cards or mobile payments for these IoT devices. For blockchain, payment is inherently supported. Thus, it is pretty natural to integrate IoT payments and blockchain into a whole system.

In the followings, we begin with distributed economies in IoT systems, then proceed to automatic payments, and discuss future work in the end. For each reviewed paper, we first introduce application scenario, then describe the blockchain solution.

6.1. Distributed economy

Sun et al. (2016) discussed the relationship between smart cities and blockchains from the perspective of sharing economy. They first introduced the relationship between smart cities and the sharing economy: the core of smart cities are societal drivers, economic drivers, and technology enablers. The ultimate goal of a smart city is to achieve smart governance of life, people, the environment and the economy. The middle link is the optimal allocation of urban resources, including space, transportation, services, food, goods and money. Then they defined the framework of a smart city from the perspective of sharing economy, including human, technology, and organization. The blockchain provides the foundation for decentralized, automated, transparent, and privately sharing services.

Huckle et al. (2016) explored how to use the blockchain to create distributed sharing economic applications that enable the sharing economy using IoT and blockchain. They envisioned three scenarios, i.e., *autopay*, *foreign currency exchange*, and *digital rights management*. Autopay includes auto refueling, automatic parking payment, automatic retail and more. Automation of the blockchain can reduce costs and smart contracts can customize payment permissions for each member. Foreign currency exchange may use smart contract for exchange currency on mobile apps by reading the contract information through QR code, NFC, and other technologies. The decentralization of the blockchain ensures that money is safe and that transaction records retain forever. Digital copyright protection may use smart contracts to record authors' copyright and enable automatic rewards for authors.

Kaid and Eljazzar (2018) examined the impact of blockchain and enterprise resource planning (ERP) integration. The various departments in the supply chain organization may be independent of each other; information exchange and currency transactions often occur among them. ERP in the supply chain is very complicated because it requires collecting data from multiple independent departments, such as product information, logistics and transportation information, transaction accounts, and so on. Often due to distrust, the organization's information is opaque. Therefore, integrating the blockchain with the ERP can improve the transparency of the information; the data guaranteed by the blockchain cannot be tampered with. The use of smart contracts to achieve currency transactions within the organization provides decentralized trust.

Zhang and Wen (2017) discussed a new e-business model based on blockchain in the IoT platform. E-business in IoT emphasizes information exchange and currency transactions between physical entities. Among the models they defined, e-business goods mainly include two types, i.e., paid data and smart property. The paid data includes a series of data such as temperature and humidity collected by the sensor, as well as other data that can be used for trading. Smart property refers to property that can prove ownership on the blockchain, such as houses, parking spaces, cars, bets, and energy which can be controlled by digital devices, such as electricity, oil, and gas. The entities of the traditional e-business model include Customer, Company, and Government. The entities in their proposed model only include Customer and Distributed Autonomous Corporations (DAC). The difference is that the DAC is decentralized and the services provided are not attended by third parties. The blockchain enables automated management of IoT e-business. Hence, blockchain-based solutions are less expensive and more efficient than traditional solutions that require third-party participation. This application has great potential in the future smart city scenario.

Shahid et al. (2019) proposed a sharing economy leasing model. In this model, a concept of Sharing Economy-Trust Point (SE-TP) is proposed. SE-TP is an entity's leasing institution. It runs blockchain nodes to upload transaction data. In the blockchain network, all users have unique accounts; leased items have unique tags; users employ smart contracts for transactions. Blockchain reduces the cost of establishing trust between users by making information transparent.

Similarly, Rahman et al. (2019) proposed a smart city sharing economy service architecture combining edge computing, AI technology, and blockchain. Abdur Rahman et al. (2019) proposed a sharing economy framework based on the Internet of Things and blockchain. Li and Huang (2019) proposed a blockchain-based e-commerce workflow management framework. In addition, Wu et al. (2017b) focused on the blockchain-based sharing economy credit rating. Hin (2019) studied the challenges and future development trends of the blockchain economy.

6.2. Automatic payment

Strugar et al. (2018) proposed an IOTA (which is a blockchain platform (Popov, 2018)) based electric vehicle (EV) billing platform. The platform realizes machine-to-machine (M2M) unattended electric vehicle purchase transaction and features free transaction fee. The platform is divided into three layers, i.e., physical layer, network layer, and service layer. The physical layer includes smart meter, Main Controller (MC), and EVSE Controller (EVSEC). The smart meter is the main sensor of the billing platform; it is used to measure the amount of electricity consumed. The EVSE is the Electric Vehicle Supply Equipment. The MC transmits the data collected by the physical layer to a higher layer through the MQTT communication protocol. The network layer uses the IOTA as a distributed database for storing transaction data. It introduces a flash channel (FC) chain payment which is released to the IOTA after the transaction is completed in the FC. Through the IOTA, FC, and MQTT protocols, the network layer can quickly transfer sensor data to the application layer. The service layer provides services for consumers based on the physical and network layers, including EAV charging services and data mining. They envision embedding the application in the EV. The application uses GPS and AI to locate the appropriate charging post and initiates the charging process. After the charging is complete, the payment channel is closed and published to Tangle.

Wu et al. (2017a) proposed to use the blockchain to enable smart grid demand side management. They used blockchain to record power calculation models and pricing models; they also used smart contracts to store transaction data and automatically transfer assets. The framework consists of two main roles, i.e., Power Management Center (PMC) and Generator. PMC is responsible for power flow forecasting and power generation scheduling to protect the grid's load within a reasonable range. Generator is a distributed microgrid that is responsible for generating electricity. Scheduling a distributed microgrid requires collecting data and issuing adjustment announcements based on the power flow calculation model. Then compensate the generator price based on the pricing model. They used multi-chain to provide an open and transparent platform for storing calculations, pricing models, and transactional data to prevent fraud. Smart contracts are used to complete automatic asset transfers, which in general reduces the cost of communication and manual management. The system roughly works as follows. PMC releases the power generation adjustment protocol on the multi-chain and pre-stores the amount to compensate for the power adjustment of the Generator. The associated Generator reads the protocol and decides whether to accept the agreement. If the generator agrees, it adjusts the generator power to match the adjustment protocol. Then it posts the transaction information, including the adjustment details, to the multi-chain. After consensus, the transaction information is permanently recorded on the blockchain. The PMC verifies the details of the adjustment; if the agreement is met, it triggers the smart contract and sends the power adjustment compensation to the Generator.

Pouraghily and Wolf (2019) proposed a lightweight payment protocol for IoT systems based on blockchain. They used a ticket based verification protocol (TBVP) to accommodate transactions in low-power devices. They introduced two logically separate entities, Contract Manager (CM) and Transaction verifier (TV). CM is responsible for establishing smart contracts for joint accounts, depositing funds, preparing transactions, closing contracts, and requesting funds. The TV is responsible for accepting the message and verifying it. They separated the verification process from the function of the blockchain node. The IoT device only needs to perform some encryption, decryption, and verification processes, but not needing to interact with the blockchain. In this scheme, the CM is integrated with the IoT gateway. Each trust domain requires only one CM, i.e., one blockchain node.

Hou et al. (2019) proposed the use of blockchain to protect the privacy of private energy transactions in the energy area. They proposed a transaction model that uses blockchain smart contracts to act as a token bank. Buyers need to exchange tokens from the token bank to purchase energy. Because frequent transactions will cause too much data on the chain and power will be lost during transmission, the author also introduced an optimization algorithm to achieve a balance between data volume, transmission loss, and economic benefits.

Short summary. Table 5 listed the reviewed work on automatic payment platform usage of blockchain for IoT systems. The 'Scenes' column denotes the application scenario; the 'Contribution' column denotes the detailed contribution of the reviewed work.

6.3. Future research challenges

In future, blockchain based IoT payment solutions face three challenges. The first is to support low-power devices. In smart city shared economy scenarios, there is an important assumption that sensor data is shared and traded. In order to achieve cross-trust domain transactions of IoT data, as well as reducing costs, the blockchain nodes should be as close as possible to the data generator. However, many IoT components have limited computing and communication resources. It is challenging to support operations required as a blockchain node.

The second challenge is to reduce fees. For IoT applications, there are a lot of machine-to-machine small transactions. However, in the PoW-based blockchain, a fee is charged for each transaction as a bonus for miners. High fees for the IoT systems are burdensome. IOTA's Tangle framework (Popov, 2018) could partially solve this challenge.

The third challenge is to improve throughput. In order to pursue security and decentralization, blockchain inevitably leads to low throughput problems. For each change of the ledger, it is broadcast to the global blockchain network to achieve consensus, which lowers the throughput. It is very challenging to improve throughput. Using private chain may be a solution. More solutions need further deep research.

7. Lessons learned and open issues

In this section, we first summarize the general ideas for the above reviewed four categories. The general ideas could be used in future development of blockchain enabled IoT systems. Then we discuss open issues for building more dependable IoT systems using blockchain.

7.1. General ideas behind the four reviewed application scenarios

In this survey, we first reviewed the use of blockchain in enabling access control for IoT systems. *The surveyed works mainly modeled the blockchain as a robust global unique centralization medium*. All the access control functionality is supported automatically in this centralization medium. Centralization normally makes the design and development logic easy for practical applications. However, achieving a robust centralization is not easy for distributed systems. Specifically, due to reasons such as trust, network delay, and node entry as well as exist, building a centralization service for distributed systems is hard. In this respect, blockchain can be seen as a centralized computing machine. It achieves centralization through a consensus mechanism. Thus it provides a new way for distributed application development.

Second, we reviewed the use of blockchain in proving data provenance and protecting data integrity for IoT systems. *The reviewed works mainly used the blockchain as a trusted storage medium*. The trajectory and fingerprint of data are stored in this trusted storage. No adversary is able to modify the data maliciously because of the consensus mechanism required by the blockchain. Trust storage is a natural requirement for many security applications. It means that the life cycle of the data stored can be traced back faithfully. The blockchain achieves the trust properties through hash chain and consensus. That is, a malicious entity is not able to modify the blockchain data unless most of the blockchain nodes are compromised.

Third, we reviewed blockchain's use in the trusted third party scenario for IoT systems. *The reviewed works mainly modeled the blockchain as a trusted central computing machine*. This trusted central computing machine not only supports data storage but also computation on the stored data. Combined together, it supports various trustful distributed applications, e.g., logistic management and product tracing. Establishing a trusted central computing machine is not easy. Blockchain uses the consensus mechanism and the smart contract mechanism to accomplish this. Thus it also has some cost in computation delay and large storage requirement. Despite this cost, this trusted central computing machine has potentiality to automate workflow of and simplify the design of distributed applications.

Table 5
Blockchain for IoT: Automatic payment platform.

Work	Scenes	Contribution
Sun et al. (2016)	Smart city sharing economy	Defined a smart city and a shared economic framework from a conceptual perspective
Huckle et al. (2016)	Foreign currency exchange digital copyright	Provided more perspectives for blockchain and shared economy
Kaid and Eljazzar (2018)	Enterprise Resource Planning (ERP)	Used blockchain to solve the problem of payment and information management in enterprises
Zhang and Wen (2017)	E-Business	Proposed an e-commerce automation management scheme based on blockchain
Shahid et al. (2019)	Sharing economy	Proposed and implemented a blockchain-based shared economy leasing system
Rahman et al. (2019)	Smart city, Sharing economy	Proposed a blockchain infrastructure to support IoT-enabled sharing economy
Abdur Rahman et al. (2019)	Sharing economy	Proposed a blockchain based shared economic service framework
Li and Huang (2019)	E-Commerce logistics	Proposed a blockchain enabled work-flow management system
Wu et al. (2017b)	Circular economy	Used a blockchain to build a credit system for a circular economy
Hin (2019)	Circular economy	Discussed the research focus and challenges of blockchain and digital economy
Strugar et al. (2018)	Electric vehicle, Charging billing	Proposed an automatic management scheme for charging electric vehicles
Wu et al. (2017a)	Smart grid	Proposed an automatic charging management scheme for smart grid
Pouraghily and Wolf (2019)	IoT resource horizontal integration	Proposed a lightweight payment protocol for blockchain-based IoT system
Hou et al. (2019)	P2P Energy trading	Proposed to use virtual coin to buy energy efficiently

Fourth, we reviewed blockchain's use in the payment service for IoT systems. *The reviewed works mainly leveraged the blockchain to transfer digital money in order to obtain a service.* Blockchain payment is automatic by the use of smart contract. The smart contract writes the payment condition in the blockchain; once the condition is met, the payment is done automatically. However, the payment in practice is normally tedious and may sometimes require law suit engagements. Thus, automatic payment is a huge advantage of blockchain. The payment service also incentivizes many application developments and deployments.

7.2. Open issues

In the review of the four categories, we have discussed *specific* future research challenges for each application scenario. Now we discuss open issues that are more fundamental. The first important open issue is on understanding blockchain performance. For IoT applications, both public chain and consortium chain are used. Generally, consortium chain is more efficient than public chain; however, it requires trust assumptions. How their performance change with the number of nodes, consensus protocols, network conditions etc. is still not well understood. After this understanding, finding methods to improve blockchain performance to match IoT applications is also open.

Another open issue is to understand the security of the blockchain platform itself. Blockchain is often used to enhance the security of IoT applications. However, as a kind of software, the blockchain itself has security issues. Indeed, researchers have already found vulnerabilities for smart contracts. This may cause serious consequences especially for payment applications as well as other applications. Understanding the security of the blockchain platform requires systematic research.

We also note that existing researches on using blockchain for the Internet of Things applications are in their early stages. The main of the works are proof-of-concept researches. It is interesting to build benchmarks for these applications and to have real, larger implementations. Benchmarks are helpful to build more efficient IoT applications using blockchain.

8. Conclusion

In this paper, we have reviewed the most recent research works that used blockchain to build dependable IoT systems. In the review, we categorized the application of blockchain's use in IoT systems into four application scenarios, i.e., access control, data provenance and integrity, trusted third party, and automatic payment platforms. For each IoT application scenario, we also discussed future challenging research directions. Finally, we summarized the general ideas on how to leverage the blockchain corresponding to the four application scenarios. We also discussed fundamental issues on enabling better blockchain assisted IoT systems. Among them, increasing blockchain performance to support large scale applications is the most common yet most important challenge. Besides, securing the blockchain infrastructure itself is also important to support upper layer dependable IoT applications.

Declaration of competing interest

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

Acknowledgments

This work was partially supported by National Natural Science Foundation of China under Grant No. (61872243, 61876110, 61772345, 61702342, U1713212), National Key R&D Program of China under Grant No. 2018YFB1800302, Guangdong Basic and Applied Basic Research Foundation (2020A151501489), the Pearl River Young Scholars Funding of Shenzhen University, and the Science and Technology Plan Projects of Shenzhen (JCYJ20180305124126741, JCYJ201908 08142207420, GJHZ20190822095416463, JCYJ20190808164211203).

References

Abdur Rahman, M., Loukas, G., Maruf Abdullah, S., Abdu, A., Sadiqur Rahman, S., Hassanain, E., Arafa, Y., 2019. Blockchain and IoT-based secure multimedia retrieval system for a massive crowd: Sharing economy perspective. In: Proceedings of the International Conference on Multimedia Retrieval. ACM, pp. 404–407.

Abeyratne, S.A., Monfared, R.P., 2016. Blockchain ready manufacturing supply chain using distributed ledger. Int. J. Res. Eng. Technol. 5 (9), 1–10.

Alfuqaha, A.I., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M., 2015. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutor. 17 (4), 2347–2376.

Ali, G., Ahmad, N., Cao, Y., Asif, M., Cruickshank, H., Ali, Q.E., 2019a. Blockchain based permission delegation and access control in internet of things (BACI). Comput. Secur. 86 (9), 318–334.

Ali, M.S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., Rehmani, M.H., 2019b. Applications of blockchains in the internet of things: A comprehensive survey. IEEE Commun. Surv. Tutor. 21 (2), 1676–1717.

Alibaba, 2019. Alibaba IoT solutions. https://www.alibabacloud.com/solutions/IoT.

Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G., Rousseau, F., Tourancheau, B., Veltri, L., Zanichelli, F., 2018. IoTChain: A blockchain security architecture for the internet of things. In: 2018 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, pp. 1–6.

Amazon, 2019. AWS IoT. https://aws.amazon.com/iot/.

Andersen, M.P., Kolb, J., Chen, K., Fierro, G., Culler, D.E., Popa, R.A., 2017. Wave: A Decentralized Authorization System for Iot via Blockchain Smart Contracts. Tech. Rep. UCB/EECS-2017-234, EECS Department, University of California, Berkeley.

Angeletti, F., Chatzigiannakis, I., Vitaletti, A., 2017. Privacy preserving data management in recruiting participants for digital clinical trials. In: Proceedings of the First International Workshop on Human-Centered Sensing, Networking, and Systems. ACM, pp. 7–12.

Arumugam, S.S., Umashankar, V., Narendra, N.C., Badrinath, R., Mujumdar, A.P., Holler, J., Hernandez, A., 2018. IoT enabled smart logistics using smart contracts. In: 8th International Conference on Logistics, Informatics and Service Sciences. IEEE, pp. 1–6.

Atzori, L., Iera, A., Morabito, G., 2010. The internet of things: A survey. Comput. Netw. 54 (15), 2787–2805.

Azaria, A., Ekblaw, A., Vieira, T., Lippman, A., 2016. Medrec: Using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD). IEEE, pp. 25–30.

Barger, A., Manevich, Y., Bortnikov, V., Tock, Y., Factor, M., Malka, M., 2018. Shared cloud object store, governed by permissioned blockchain. In: Proceedings of the 11th ACM International Systems and Storage Conference. ACM, p. 114.

Beck, R., 2018. Beyond bitcoin: The rise of blockchain world. Computer 51 (2), 54–58. http://dx.doi.org/10.1109/MC.2018.1451660.

Buneman, P., Khanna, S., Wang-Chiew, T., 2001. Why and where: A characterization of data provenance. In: International Conference on Database Theory. Springer, pp. 316–330.

Buterin, V., 2014. A next-generation smart contract and decentralized application platform. https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf.

Buterin, V., 2015. Ethereum. https://ethereum.org/.

Cachin, C., Vukolić, M., 2017. Blockchain consensus protocols in the wild. arXiv:1707.01873.

Cao, Y., Jia, F., Manogaran, G., 2019. Efficient traceability systems of steel products using blockchain-based industrial internet of things. IEEE Trans. Ind. Inform. http://dx.doi.org/10.1109/TII.2019.2942211, preprint.

Casado-Vara, R., de la Prieta, F., Prieto, J., Corchado, J.M., 2018. Blockchain framework for IoT data quality via edge computing. In: Proceedings of the 1st Workshop on Blockchain-Enabled Networked Sensor Systems. ACM, pp. 19–24.

Casino, F., Dasaklis, T.K., Patsakis, C., 2019. A systematic literature review of blockchain-based applications: current status, classification and open issues. Telemat. Inform. 36, 55–81.

Cha, S.-C., Chen, J.-F., Su, C., Yeh, K.-H., 2018. A blockchain connected gateway for BLE-based devices in the internet of things. IEEE Access 6, 24639–24649.

Chanson, M., Bogner, A., Wortmann, F., Fleisch, E., 2017. Blockchain as a privacy enabler: an odometer fraud prevention system. In: ACM International Joint Conference on Pervasive and Ubiquitous Computing. ACM, pp. 13–16.

Christidis, K., Devetsikiotis, M., 2016. Blockchains and smart contracts for the internet of things. IEEE Access 4, 2292–2303.

Cuomo, J., 2016. How businesses and governments can capitalize on blockchain. http://www.ibm.com/blogs/think/2016/03/16/how-businesses-and-governments-can-capitalize-on-blockchain/.

Curran, B., 2019. Blockchain games: The current state of blockchain gaming technology. https://blockonomi.com/blockchain-games/.

Dai, H.-N., Zheng, Z., Zhang, Y., 2019. Blockchain for internet of things: A survey. IEEE Internet Things J. 6 (5), 8076–8094.

Denning, D.E., Denning, P.J., 1979. Data security. ACM Comput. Surv. 11 (3), 227–249.

Di Pietro, R., Salleras, X., Signorini, M., Waisbard, E., 2018. A blockchain-based trust system for the internet of things. In: Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies. ACM, pp. 77–83.

Dice2Win Team, 2019. Fair games that pay ether. https://dice2.win/.

Dorri, A., Kanhere, S.S., Jurdak, R., 2016. Blockchain in internet of things: challenges and solutions. arXiv preprint arXiv:1608.05187.

Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P., 2017. Blockchain for IoT security and privacy: The case study of a smart home. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops. IEEE, pp. 618–623.

Drescher, D., 2017. Blockchain Basics. Apress, Berkeley, CA.

Feng, Q., He, D., Zeadally, S., Khan, M.K., Kumar, N., 2019. A survey on privacy protection in blockchain system. J. Netw. Comput. Appl. 126, 45–58.

Fernandezcarames, T.M., Fragalamas, P., 2018. A review on the use of blockchain for the internet of things. IEEE Access 6, 32979–33001.

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

Fu, Y., Zhu, J., 2019. Big production enterprise supply chain endogenous risk management based on blockchain. IEEE Access 7, 15310–15319.

Gaetani, E., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., Sassone, V., 2017. Blockchain-based database to ensure data integrity in cloud computing environments. In: The First Italian Conference on Cybersecurity (ITASEC17).

Gai, K., Wu, Y., Zhu, L., Qiu, M., Shen, M., 2019. Privacy-preserving energy trading using consortium blockchain in smart grid. IEEE Trans. Ind. Inf. 15 (6), 3548–3558.

Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T., 2018. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J. Med. Syst. 42 (7), 130.

Hackius, N., Petersen, M., 2017. Blockchain in logistics and supply chain: trick or treat? In: Proceedings of the Hamburg International Conference of Logistics. pp. 3–18.

Hin, L.H., 2019. Blockchain economy: The new era of digital economy. Int. J. Sci. Res. Sci. Technol. 6 (4), 351–358.

Hou, W., Guo, L., Ning, Z., 2019. Local electricity storage for blockchain-based energy trading in industrial internet of things. IEEE Trans. Ind. Inf. 15 (6), 3610–3619.

Huckle, S., Bhattacharya, R., White, M., Beloff, N., 2016. Internet of things, blockchain and shared economy applications. Procedia Comput. Sci. 98, 461–466.

Huh, S., Cho, S., Kim, S., 2017. Managing IoT devices using blockchain platform. In: 2017 19th International Conference on Advanced Communication Technology (ICACT). IEEE, pp. 464–467.

Jordan, J., 2019. Top 10 most anticipated blockchain games for 2019. https://www.blockchaingamer.biz/features/3283/most-anticipated-blockchain-games/.

Kaid, D., Eljazzar, M.M., 2018. Applying blockchain to automate installments payment between supply chain parties. In: 2018 14th International Computer Engineering Conference (ICENCO). IEEE, pp. 231–235.

Khan, M.A., Salah, K., 2018. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 82, 395–411.

Korpela, K., Hallikas, J., Dahlberg, T., 2017. Digital supply chain transformation toward blockchain integration. In: Proceedings of the 50th Hawaii International Conference on System Sciences.

Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C., 2016. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: 2016 IEEE Symposium on Security and Privacy (SP). pp. 839–858. http://dx.doi.org/10.1109/SP.2016.55.

Krishnan, K.N., Jenu, R., Joseph, T., Silpa, M., 2018. Blockchain based security framework for IoT implementations. In: 2018 International CET Conference on Control, Communication, and Computing. IEEE, pp. 425–429.

Kuhi, K., Kaare, K., Koppel, O., 2018. Ensuring performance measurement integrity in logistics using blockchain. In: 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI). IEEE, pp. 256–261.

Li, M., Huang, G., 2019. Blockchain-enabled workflow management system for fine-grained resource sharing in E-commerce logistics. In: 2019 IEEE 15th International Conference on Automation Science and Engineering (CASE). IEEE, pp. 751–755.

Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q., 2020. A survey on the security of blockchain systems. Future Gener. Comput. Syst. 107, 841–853.

Li, J., Qu, F., Tu, X., Fu, T., Guo, J., Zhu, J., 2018. Public philanthropy logistics platform based on blockchain technology for social welfare maximization. In: 2018 8th International Conference on Logistics, Informatics and Service Sciences (LISS). IEEE, pp. 1–9.

Li, J., Wang, X., 2018. Research on the application of blockchain in the traceability system of agricultural products. In: IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference. IEEE, pp. 2637–2640.

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., Njilla, L., 2017. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In: Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. IEEE Press, pp. 468–477.

Liang, W., Tang, M., Long, J., Peng, X., Xu, J., Li, K.-C., 2019. A secure fabric blockchain-based data transmission technique for industrial internet-of-things. IEEE Trans. Ind. Inf. 15 (6), 3582–3592.

Liu, B., Yu, X.L., Chen, S., Xu, X., Zhu, L., 2017. Blockchain based data integrity service framework for IoT data. In: 2017 IEEE International Conference on Web Services (ICWS). IEEE, pp. 468–475.

Lo, S.K., Liu, Y., Chia, S.Y., Xu, X.S., Lu, Q., Zhu, L., Ning, H., 2019. Analysis of blockchain solutions for IoT: A systematic literature review. IEEE Access 7, 58822–58835.

Longo, F., Bruneo, D., Distefano, S., Merlino, G., Puliafito, A., 2017. Stack4Things: a sensing-and-actuation-as-a-service framework for IoT and cloud integration. Ann. Telecommun. 72 (1–2), 53–70.

Makhdoom, I., Abolhasan, M., Abbas, H., Ni, W., 2019. Blockchain's adoption in IoT: The challenges, and a way forward. J. Netw. Comput. Appl. 125, 251–279.

McWaters, R., Bruno, G., Galaski, R., Chaterjee, S., 2016. The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services. https://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services/, World Economic Forum.

Merkle, R.C., 1987. A digital signature based on a conventional encryption function. In: Proceedings of Crypto. pp. 369–378.

Monero Core Team, 2014. MONERO. https://web.getmonero.org/.

Nakamoto, S., 2009. Bitcoin. https://www.bitcoin.org/.

Nakamoto, S., et al., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Working Paper, https://bitcoin.org/bitcoin.pdf.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S., 2016. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.

Novo, O., 2018. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet Things J. 5 (2), 1184–1195.

Ouaddah, A., Abou Elkalam, A., Ait Ouahman, A., 2016. Fairaccess: a new blockchain-based access control framework for the internet of things. Secur. Commun. Netw. 9 (18), 5943–5964.

Outchakoucht, A., Hamza, E., Leroy, J.P., 2017. Dynamic access control policy based on blockchain and machine learning for the internet of things. Int. J. Adv. Comput. Sci. Appl. 8 (7), 417–424.

Pal, S., Rabehaja, T., Hitchens, M., Varadharajan, V., Hill, A., 2019. On the design of a flexible delegation model for the internet of things using blockchain. IEEE Trans. Ind. Inform. http://dx.doi.org/10.1109/TII.2019.2925898, preprint.

Perboli, G., Musso, S., Rosano, M., 2018. Blockchain in logistics and supply chain: A lean approach for designing real-world use cases. IEEE Access 6, 62018–62028.

Peters, G., Panayi, E., Chapelle, A., 2015. Trends in cryptocurrencies and blockchain technologies: A monetary theory and regulation perspective. J. Financ. Perspect. 3 (3).

Popov, S., 2018. The tangle. https://iota.org/IOTA_Whitepaper.pdf.

Pouraghily, A., Islam, M.N., Kundu, S., Wolf, T., 2018. Privacy in blockchain-enabled iot devices. In: 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI). IEEE, pp. 292–293.

Pouraghily, A., Wolf, T., 2019. A lightweight payment verification protocol for blockchain transactions on IoT devices. In: 2019 International Conference on Computing, Networking and Communications (ICNC). IEEE, pp. 617–623.

Puthal, D., Malik, N., Mohanty, S.P., Kougianos, E., Yang, C., 2018. The blockchain as a decentralized security framework future directions. IEEE Consum. Electron. Mag. 7 (2), 18–21.

Rahman, M.A., Rashid, M.M., Hossain, M.S., Hassanain, E., Alhamid, M.F., Guizani, M., 2019. Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city. IEEE Access 7, 18611–18621.

Ramachandran, A., Kantarcioglu, M., 2018. Smartprovenance: a distributed, blockchain based dataprovenance system. In: Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. ACM, pp. 35–42.

Saberi, S., Kouhizadeh, M., Sarkis, J., Shen, L., 2019. Blockchain technology and its relationships to sustainable supply chain management. Int. J. Prod. Res. 57 (7), 2117–2135.

Sandhu, R.S., Samarati, P., 1994. Access control: principle and practice. IEEE Commun. Mag. 32 (9), 40–48.

Savelyev, A., 2017. Contract law 2.0:'Smart'contracts as the beginning of the end of classic contract law. Inf. Commun. Technol. Law 26 (2), 116–134.

Sengupta, J., Ruj, S., Bit, S.D., 2020. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J. Netw. Comput. Appl. 149, 102481.

Shafagh, H., Burkhalter, L., Hithnawi, A., Duquennoy, S., 2017. Towards blockchain-based auditable storage and sharing of IoT data. In: Proceedings of the 2017 on Cloud Computing Security Workshop. ACM, pp. 45–50.

Shahid, M.R., Mahmood, S., Hafeez, S., Zahid, B., Jabbar, S., Ashraf, R., 2019. Blockchain based share economy trust point: Case study based validation. In: Proceedings of the 3rd International Conference on Future Networks and Distributed Systems. ACM, p. 41.

Sidorov, M., Ong, M.T., Sridharan, R.V., Nakamura, J., Ohmura, R., Khor, J.H., 2019. Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains. IEEE Access 7, 7273–7285.

Singh, S., Ra, I.-H., Meng, W., Kaur, M., Cho, G.H., 2019. SH-BlockCC: A secure and efficient internet of things smart home architecture based on cloud computing and blockchain technology. Int. J. Distrib. Sens. Netw. 15 (4).

Song, J.C., Demir, M.A., Prevost, J.J., Rad, P., 2018. Blockchain design for trusted decentralized iot networks. In: 2018 13th Annual Conference on System of Systems Engineering (SoSE). IEEE, pp. 169–174.

Strugar, D., Hussain, R., Mazzara, M., Rivera, V., 2018. M2M billing for electric autonomous vehicles. arXiv preprint arXiv:1804.00658.

Sun, J., Yan, J., Zhang, K.Z., 2016. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financ. Innov. 2 (1), 26.

Swan, M., 2015. Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc..

Szabo, N., 1996. Smart contracts: building blocks for digital markets. EXTROPY: J. Transhumanist Thought.

Tapas, N., Merlino, G., Longo, F., 2018. Blockchain-based IoT-cloud authorization and delegation. In: 2018 IEEE International Conference on Smart Computing (SMARTCOMP). IEEE, pp. 411–416.

Tijan, E., Aksentijević, S., Ivanić, K., Jardas, M., 2019. Blockchain technology implementation in logistics. Sustainability 11 (4), 1185.

Underwood, S., 2016. Blockchain beyond bitcoin. Commun. ACM 59 (11), 15–17.

Viriyasitavat, W., Da Xu, L., Bi, Z., Hoonsopon, D., 2019. Blockchain technology for applications in internet of things—Mapping from system design perspective. IEEE Internet Things J. 6 (5), 8155–8168.

Wan, J., Li, J., Imran, M., Li, D., et al., 2019. A blockchain-based solution for enhancing security and privacy in smart factory. IEEE Trans. Ind. Inf. 15 (6), 3652–3660.

Wang, J., Wu, L., Choo, K.-K.R., He, D., 2019. Blockchain based anonymous authentication with key management for smart grid edge computing infrastructure. IEEE Trans. Ind. Inform. http://dx.doi.org/10.1109/TII.2019.2936278, preprint.

Westerkamp, M., Victor, F., Küpper, A., 2018. Blockchain-based supply chain traceability: Token recipes model manufacturing processes. In: 2018 IEEE International Conference on Internet of Things (iThings). IEEE, pp. 1595–1602.

Wilcox, Z., 2016. Zcash. https://z.cash/.

Wu, X., Duan, B., Yan, Y., Zhong, Y., 2017a. M2M blockchain: The case of demand side management of smart grid. In: 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS). IEEE, pp. 810–813.

Wu, H.-T., Su, Y.-J., Hu, W.-C., 2017b. A study on blockchain-based circular economy credit rating system. In: International Conference on Security with Intelligent Computing and Big-Data Services. Springer, pp. 339–343.

Wu, M., Wang, K., Cai, X., Guo, S., Guo, M., Rong, C., 2019. A comprehensive survey of blockchain: From theory to IoT applications and beyond. IEEE Internet Things J. 6 (5), 8114–8154.

Xu, R., Chen, Y., Blasch, E., Chen, G., 2018. Blendcac: A blockchain-enabled decentralized capability-based access control for IoTs. In: 2018 IEEE International Conference on Internet of Things (iThings). IEEE, pp. 1027–1034.

Xu, L.D., He, W., Li, S., 2014. Internet of things in industries: A survey. IEEE Trans. Ind. Inf. 10 (4), 2233–2243.

Yang, R., Yu, F.R., Si, P., Yang, Z., Zhang, Y., 2019. Integrated blockchain and edge computing systems: A survey, some research issues and challenges. IEEE Commun. Surv. Tutor. 21 (2), 1508–1532.

Yu, Y., Li, Y., Tian, J., Liu, J., 2018. Blockchain-based solutions to security and privacy issues in the internet of things. IEEE Wirel. Commun. 25 (6), 12–18.

Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., Wan, J., 2018. Smart contract-based access control for the internet of things. IEEE Internet Things J. 6 (2), 1594–1605.

Zhang, Y., Wen, J., 2017. The IoT electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Netw. Appl. 10 (4), 983–994.

Zhang, Y., Xu, X., Liu, A., Lu, Q., Xu, L., Tao, F., 2019. Blockchain-based trust mechanism for iot-based smart manufacturing system. IEEE Trans. Comput. Soc. Syst. 6 (6), 1386–1394.

Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H., 2018. Blockchain challenges and opportunities: a survey. Int. J. Web Grid Serv. 14 (4), 352–375.

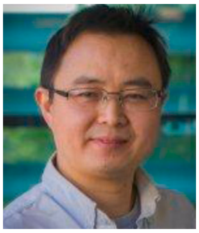
Fei Chen received the PhD degree in computer science and engineering from The Chinese University of Hong Kong in 2014. He is currently an Associate Professor with College of Computer Science and Software Engineering, Shenzhen University, China. His research interests include data protection and privacy, and distributed systems and applications.

Zhe Xiao is master student with College of Computer Science and Engineering, Shenzhen University, China. Email: 1810272052@email.szu.edu.cn. His research interests include data privacy and protection.

Laizhong Cui Laizhong Cui received the B.S. degree from Jilin University, Changchun, China, in 2007, and the Ph.D. degree in computer science and technology from Tsinghua University, Beijing, China, in 2012. He is currently an Associate Professor with the College of Computer Science and Software Engineering, Shenzhen University, China. He led a project of the National Natural Science Foundation, and several projects of Guangdong Province and Shenzhen City. His research interests include future Internet architecture, edge computing, IoT, computational intelligence, software-defined network, and machine learning.

Qiuzhen Lin received the B.S. degree from Zhaoqing University and the M.S. degree from Shenzhen University, China, in 2007 and 2010, respectively. He received the Ph.D. degree from Department of Electronic Engineering, City University of Hong Kong, Kowloon, Hong Kong, in 2014. He is currently an Associate Professor in College of Computer Science and Software Engineering, Shenzhen University. He has published over 30 research papers since 2008. His current research interests include artificial immune system, multi-objective optimization and dynamic system.

Jianqiang Li received the B.S. and Ph.D. degrees in automation from the South China University of Technology, Guangzhou, China, in 2003 and 2008, respectively. He is a Professor with the College of Computer and Software Engineering, Shenzhen University, Shenzhen, China. He led three projects of the National Natural Science Foundation and three projects of the Natural Science Foundation of Guangdong Province, China. His current research interests include data analysis, embedded systems, and the Internet of Things.



Shui Yu received his B. Eng (Electronic Engineering) and M. Eng (Computer Science) degree from University of Electronic Science and Technology of China, P. R. China in 1993 and 1999, respectively. He also obtained an Associate Degree in Mathematics from the same university in 1993. He received his PhD (Computer Science) from Deakin University in 2004. He is currently a Senior Lecturer of School of Information Technology, Deakin University, Melbourne, Australia. Before joining Deakin University, Dr Yu was a Lecturer of Computer College in University of Electronic Science and Technology of China. He has a good experience of industry, especially in network design and software development organization and implementation. His research interests include Big Data Theory and Application, Networking Theory and Application, and Mathematical Modeling. He dedicates himself in advance human understanding of networks and information, including their measurement, representation, analysis, and application. As a semi-mathematician, he targets on narrowing the gap between theory and application using mathematical tools. Dr Yu is a Guest Professor of South West University of China, an overseas expert of the national 111 project at Beijing Jiaotong University. Dr Yu is a Member of AAAS, ACM, and a Senior Member of IEEE.