Journal of Hardware and Systems Security (2019) 3:338–364
https://doi.org/10.1007/s41635-019-00079-5

Blockchain in IoT: Current Trends, Challenges, and Future Roadmap

Pinchen Cui[1] · **Ujjwal Guin**[2] · **Anthony Skjellum**[3] · **David Umphress**[1]

Received: 1 May 2019 / Accepted: 24 September 2019 / Published online: 4 November 2019

Abstract

The Internet of Things (IoT) is one of the most promising technologies in the era of information technology. IoT enables ubiquitous data collections and network communications to bring significant and indispensable convenience and intelligence both to daily life and industrial operations. However, IoT is still confronting a number of challenges and manifesting a series of issues that need to be addressed urgently. Counterfeit hardware, software faults, security issues during communication, system management difficulties, and data privacy issues are significant issues for current IoT infrastructure. Meanwhile, blockchain, as an emerging information technology, has attracted huge public interest and has shown significant promise because of its decentralization, transparency, and security. The features of blockchain seem to be an ideal match for IoT, and by applying blockchain to an IoT environment, some of the aforementioned weaknesses can be addressed. This paper's purpose is to introduce the use of blockchain in IoT applications. We present various challenges facing an IoT system and summarize the benefits of adopting blockchain into IoT infrastructure. We primarily focus on illustrating the blockchain applications in IoT with refined capabilities and enhanced security. To shed light on blockchain in IoT research, we also discuss limitations and future directions.

Keywords Internet of Things · Blockchain · BIoT · Blockchain applications · Security

1 Introduction

Because of the rapid development of the Internet of Things (IoT), the number of devices connected to the Internet has grown at an unprecedented rate. The concept of IoT is to allow various types of devices to collect and exchange data through the network, which includes not only computers and smart phones but also cars, dishwashers, televisions, and other common household appliances connected to the Internet. A recent report from Gartner indicates that 8.4 billion connected things were in use in 2017, and that the number will reach 20.4 billion by 2020 [81]. Besides the massive number of devices that can be deployed, IoT also stands to open huge business prospects for various organizations, where over 800 billion dollars revenue would be generated by 2020 [18]. However, the large scale and heterogeneity of IoT are increasing the difficulties in design and management [211].

To address the challenges and limitations of implementing IoT infrastructure, an holistic technical evolution and innovation is necessary. Even though new standards, lightweight protocols, and novel frameworks have been proposed, some of the challenges of IoT remain unsolved. Service providers, device manufactures, customers, and researchers are seeking solutions to emerging problems in IoT, particularly those associated with addressing security at acceptable performance. Since the emergence of blockchain technology, certain classes of problems associated with IoT may be settled through the use of a reliable, distributed ledger technology. In the past 3 years, blockchain has attracted explosive public interest because of its distributed, decentralized, and transparent nature. We assert here that blockchain can be used to help IoT solve and bypass many of its perceived and identified limitations.

In this paper, we present an overview of IoT challenges in system design, data management, device management,

✉ Pinchen Cui
Pinchen@auburn.edu

✉ Ujjwal Guin
ujjwal.guin@auburn.edu

[1] Department of Computer Science and Software Engineering (CSSE), Auburn University, Auburn, AL, USA

[2] Department of Electrical and Computer Engineering (ECE), Auburn University, Auburn, AL, USA

[3] SimCenter, and the Department of Computer Science and Engineering, The University of Tennessee at Chattanooga, Chattanooga, TN, USA

service management, and security. Then, we demonstrate how blockchain can potentially help to address these limitations. To give an overview of the background, we perform a comprehensive review of blockchain technology. In addition, we illustrate blockchain usage in IoT within agriculture, energy, healthcare, industrial, smart city, smart home, and transportation domains. Since blockchain appears to be suitable to improve aspects of security for IoT, we analyze and discuss the use of blockchain for IoT access control, data assurance, counter tampering, key management, and trust. This paper also describes and summarizes the challenges and limitations of using blockchain in IoT. We discuss the form, fit, and function of blockchain for IoT, such as practical implementation cost, throughput and latency problems, on-chain security concerns, and maintenance and regulation issues. Furthermore, we investigate research trends and future roadmaps with regard to blockchain optimization for IoT applications.

1.1 IoT Challenges and Limitations

Although IoT architecture, protocols, and middleware enable different types of devices to connect and communicate, its heterogeneity and scalability cause certain issues. For instance, some resource-constrained devices cannot afford the overhead of typical registration, communication, and authentication protocols. To interoperate with these devices, resource-rich devices need to downgrade their protocols to a lightweight version so that all the devices can communicate and operate in a new, uniform manner. However, the security of such lightweight communication protocols and schemes face challenges [19, 210]. Therefore, when a large number of devices carry and transmit personal and sensitive data with weak security guarantees, counterfeit hardware, software malfunction, communication privacy, system management, and data storage create a new series of challenges for an IoT system.

As shown in Fig. 1, the challenges to implement IoT infrastructure can broadly be classified into five categories: system design, data management, device management, service management, and security [19, 21, 31, 52, 88, 210].

1. *System design:* From a single device perspective, the underlying embedded system needs to support efficient, reliable, and robust data collection and data transmission. Particularly for resource-constrained devices, a streamlined operating system (OS) and customized firmware are almost always needed to ensure these tiny devices can operate properly [33, 69, 122]. For the overall IoT system, the device needs to satisfy the requirements of availability, scalability, flexibility and cost efficiency. In addition, for various application domains, multiple factors need to be considered, including quality of service, latency, redundancy, mobility, and security. Generally, most IoT systems are designed on centralized architectures such that no matter how the underlying Machine to Machine (M2M) communications [198] and middleware communications (Gateway to Gateway) are handled, the system is connected to and managed by central (cloud) servers. Though the current paradigm works properly, the foreseeable growth of big data and IoT triggers the need for decentralized solutions.
2. *Data management:* Whether text, audio, video, discrete, and/or stream, IoT data is generated by a variety of devices and is likely to have inconsistent formats and semantics. Managing the large volume of heterogeneous data introduces a series of technical challenges. Data generated by digital sensors, automobiles, and electrical meters require processing (pruning, compression, labeling) before it can be used and stored, which is a non-trivial cost of processing power. After the data is collected and processed, another hard requirement is to provide data storage for the massive amount of data.

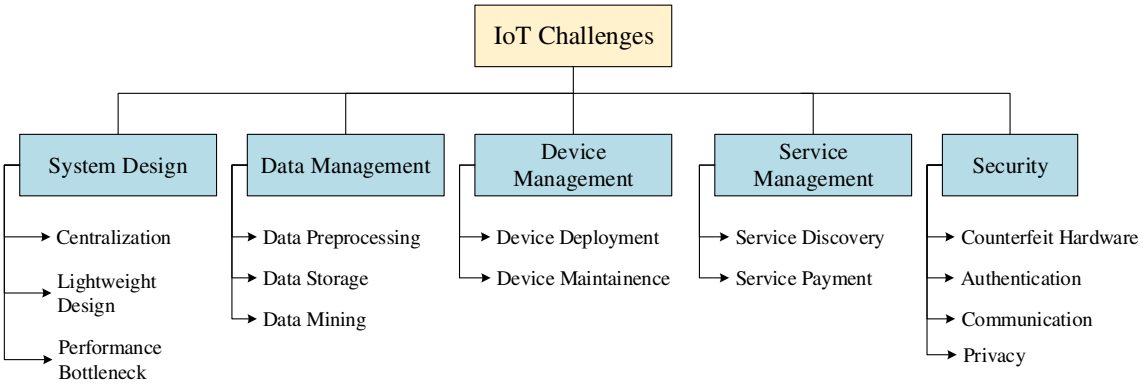

Fig. 1 Taxonomy of IoT Challenges [19, 21, 31, 52, 88, 210]

Actually, few organizations and enterprises are able to house all the IoT data collected from their networks [118]. Centralized data storage requires and relies on bandwidth and availability; migrating to distributed and decentralized storage may be a better option. To extract valuable information from stored data, appropriate data mining tools that are able to couple with big data are needed; however, data mining techniques against image and video data are another problem [118].

3. *Device management:* Managing a massive number of devices presents a further challenge. Besides the person power needed for the devices' deployment, the naming and addressing scheme of devices is also a concern. Millions of devices consume a large address space in the IPv4 context, and additional hardware/software support may be needed to enable IPv6 (e.g., ipv6EtherShield for Arduino platform "https://forum.arduino.cc/index.php?topic=106909.0"). Alternatively, some devices are only networked with local-area, low-power networks such as Zigbee and Bluetooth [25, 43]; still others may use even lower power, lower security networking protocols. Once device deployment is finished, another issue arises: how to keep the security credentials, firmware, and software on the devices up to date. Generally, a traceable, auditable, manageable, and reliable maintenance mechanism is critical for the infrastructure's operations; however, traditional methods cannot fulfill the requirements. Although some over-the-air (OTA) maintenance approaches are available [50, 112], their reliability and efficiency are still arguably low [36].
4. *Service management:* An IoT service provider may require careful consideration and strict configurations before granting customers direct access to such resources. This concern is based on infrastructure security. On the contrary, if all the available services are fully abstracted, exposed, and managed by the service provider, then customers need to query the service provider for any services of interest and are not able to discover the detail of the data source. The usage of services is based on the trust between the infrastructure's owner and customers. Therefore, a method to provide transparent and reliable service discovery and usage is required. Beyond that, the purchase of services also needs to be resolved. Instead of manually buying certain amounts of data or resources, a thing-to-thing data purchase would be more economical and efficient and automatically enable the devices to compensate and/or reimburse each other for services without any human interaction. Traditional payment methods are insufficient to handle these massive numbers of micro-transactions because of the limited capacity and high transaction costs [135]

.

5. *Security:* Security is always a major concern of modern network systems, especially for an IoT system, because of the manifold security issues observed on both the hardware and software levels. As mentioned above, tiny and inexpensive resource-constrained devices occupy a large portion of the IoT network. Unfortunately, the characteristics of low-power, small-memory, limited processing capability, and low-cost devices also imply the strong potential for vulnerabilities.

   For instance, power constraints also limit encryption functionality, which leads to poorly encrypted communication or no encryption at all [191]. (Furthermore, encryption replaces the problem of data privacy with the complexity of key management for net added security.) The hardware deficits not only confine device capabilities but also incur potential risks:

   – *Counterfeit hardware:* The risk of infiltrating counterfeit devices in IoT infrastructure has been observed in recent years. A report from Borderhawk mentioned that a steady stream unusual network traffic originated from a counterfeit IoT remote power manager [192]. It was estimated that the counterfeit devices have been installed by thousands of energy companies. In addition, the recent hardware hack reported by Bloomberg shows how the counterfeit hardware can create a stealth doorway into the network and compromise the security of an information system [160]. As most IoT devices are small, simple, and expensive to manufacture, it can be easy for an adversary to counterfeit a popular piece of hardware. Since most of the devices are manufactured in limited trust environments without sufficient regulations (and then are distributed through supply chains without reliable supervising), counterfeit hardware is on the rise. Though some cloud manufacturing approaches have been proposed to provide on-demand, manageability, traceability support [183, 184, 200], the manufacturing process still needs the participation of a centralized platform. The reliability of supervision can provide the trustworthiness of devices, and the blockchain can be the perfect candidate for providing that support.
   – *Device authentication:* Limited processing capability and insufficient memory space also cause problems in device authentication. Since encryption and digital signature are expensive for resource-constrained devices, lightweight yet reliable authentication solutions are needed. Recently, much work related to radio frequency identification (RFID) [76] and physically unclonable functions

(PUF) [93, 178] indicate the feasibility of energy-efficient, low-cost, and secure authentication for an IoT scheme. However, the deployment and management of such IDs face challenges as well [110]. Generally, it is inconvenient for both customers and manufacturers to track or maintain the IDs of devices. During system deployment, an administrator needs to solve the issue of how to store and protect the identities. Centralized identity management may confront the single point failure, which would cause the failed authentication or identity leak.

- *Device communication:* To achieve the best-quality transmission, such as Transmission Control Protocol (TCP) [106], it is necessary to provide high device resources. Handshakes and re-transmissions impose heavy loads for devices with limited processing resources and cause bandwidth congestion. In the past few years, several new protocols and standards that aim to offer lightweight, efficient, and secure communication for IoT have been proposed [21]. For example, CoAP is already widely used and tested by industry and academic researchers. However, the security of such protocols is still not guaranteed [158].
- *Data privacy:* Data privacy and user preference need immediate attention, as personal and sensitive data spread in the IoT networks [19, 210]. First, data access needs a reliable and flexible control that ensures no one can touch or leak others' personal data. Second, user preferences, such as device ownerships, device configurations, and specific policies need to be managed in a secure manner. The customer should be able to easily and smoothly obtain the data, change the preferences, or stop the services on his/her demand, all in such a way that no one could eavesdrop on, delay, or interrupt this procedure.

Despite the fact that IoT possesses a variety of attractive capabilities and has bright prospects, its limitations and challenges cannot be ignored. The aforementioned context only presents the issues briefly, and there are many solutions and methods proposed elsewhere to deal with these problems without using blockchain. However, the detailed descriptions of these solutions are out of the scope of this paper. This paper focuses on how to use blockchain technology to address some of the limitations of IoT. Note that even if the blockchain is integrated with IoT as discussed here, there is no perfect solution at this stage and not all the aforementioned issues in IoT can be solved using blockchain.

1.2 Blockchain Technology

The concept of blockchain originated from the cryptocurrency system Bitcoin, which was introduced by Satoshi Nakamoto in 2008 [146]. The fundamental features include hash-based block structure, a consensus algorithm (e.g., Proof-of-Work (PoW), Proof-of-Stake (PoS) [145]), and decentralized architecture. Advanced functionality such as the smart contract is supported by certain blockchains [28, 196]. Recently, blockchain as a distributed ledger system that can provide global data integrity and transparency is gaining increasing attention since data is the key factor of all modern systems. Both industrial and academic researchers are working toward the appropriate use of blockchain technology. Generally, blockchain can be used to enhance service transparency and availability. For instance, applications of blockchain-based identity providers, voting systems, financial services, and supply chain management have already emerged [150].

Blockchain applied IoT infrastructure (BIoT) is one of the other feasible uses of blockchain, which also has tremendous potential. Some companies and organizations have already started to investigate BIoT. For instance, IBM has integrated the Watson IoT Platform with blockchain, which ensures the transparency of provenance, operational, and maintenance records [105]. Airbnb has also heavily invested in blockchain research for addressing different IoT implementations, (e.g., the door to a rented home would be locked/unlocked when a user completed the payment to the owner over a blockchain [138]). The reason to consider adopting blockchain into IoT is that blockchain provides effective ways to address the constraints of IoT. A discussion of how blockchain can help IoT is depicted in the Table 1. Generally, blockchain offers reliability, scalability, and transparency for IoT and enhances the performance and security of the system. Investigating the fusion of blockchain and IoT can lead to a more effective and secure IoT scheme, which matches the expectations of most users and researchers.

1.3 Motivation and Contribution

There is an urgent need to point out all different challenges and provide guidance for future research on the seamless integration of IoT and blockchain. This paper aims to demonstrate the feasibility and current status of BIoT by reviewing related research off the past few years.

Table 1 How blockchain can address IoT challenges

IoT challenges	How can blockchain help
System design: hierarchy-centralized IoT architecture has scalability, throughput, and security limitations	Blockchain can help to build up a decentralized IoT system that can overcome some of the constraints. The P2P communication scheme of blockchain is an ideal match for IoT. Efficient, reliable, robust, and scalable IoT system can be operated over the blockchain.
Data management: need distributed and reliable data storage	A blockchain system can be used to provide auditable data storage for an IoT environment and also can be used as an additional layer of cloud storage to provide data integrity guarantees.
Device management: difficulty of large-scale deployment and maintenance	Blockchain can help to maintain the security credentials, firmware, and applications on the devices in a reliable and efficient manner.
Service management: inefficient service discovery, indirect device usage, lack of flexibility in payment methods	Blockchain enables decentralized and automatic service discovery, allowing the reliable direct access to the IoT resources where the security and efficiency can be balanced. Blockchain also supports microtransactions among IoT devices.
Security: counterfeit problem, lack of communication security, data privacy concerns.	A blockchain system can provide reliable provenance tracking for IoT devices to solve the counterfeit problem. Refined access management, data assurance, and data privacy are also introduced by blockchain-based IoT solutions.

There already exists a few work that surveys blockchain into IoT [53, 55, 75, 77, 103, 111, 115]. The main contribution of our work is to provide a comprehensive analysis of blockchain in IoT, which covers not only the concepts but also all different applications and their security concerns. Compared with the previous works, our contributions are summarized as follows:

- We present a detailed taxonomy of different types of blockchains in this paper. A clear and straight forward overview of blockchain applications in different domains are also described in detail.
- We analyze and introduce up-to-date blockchain-based IoT applications and implementations. We explain and illustrate how blockchain could enhance different IoT applications.
- We systematically discuss the use of blockchain to enhance IoT security. Methods of using blockchain to enhance security (both hardware and software) in IoT scenarios are presented as well.
- The challenges and limitations of using blockchain in IoT applications are analyzed. The potential solutions and related works that were proposed to overcome the limitations are summarized as well.
- The blockchain in IoT research trend is analyzed in detail and the future roadmap is also presented.

The remainder of this paper is organized as follows. We present a systematic overview of blockchain in Section 2. We investigate the blockchain applications in IoT in Section 3. We introduce the use of blockchain for IoT security in Section 4. We discuss challenges and limitations in Section 5. We also summarize and elicit the research roadmap of blockchain for IoT in Section 6. Finally, we conclude the paper in Section 7.

2 Blockchain

Blockchain is a distributed ledger system running over a peer-to-peer (P2P) network [165]. It aims to provide reliable and traceable data, as well as value exchange among untrusted entities without involving a centralized third party The concept of blockchain was first introduced by Satoshi Nakamoto in the groundbreaking Bitcoin paper, which was originally proposed to solve the double-spending problem in digital currency systems ("https://en.bitcoin.it/wiki/Double-spending"). The success of Bitcoin triggered rapid development and public interest in blockchain technology. Particularly in the past 2years, the explosive appreciation of cryptocurrency has made blockchain a new technical "hot topic." Note that the cryptocurrency system is not fully equivalent to blockchain, as a cryptocurrency system always consists of blockchain, protocol, and currency [180]. Blockchain is actually a tool to build up the cryptocurrency system. Although blockchain is designed for cryptocurrency systems and transaction recording, blockchain now can be applied into various fields as it evolves. To introduce the functionality of blockchain and how to apply blockchain into IoT, the following subsections describe its fundamental characteristics.

2.1 Basic Concepts

The basic idea of blockchain is to collaborate on recording information, in such a way that the participants in the

network do not trust each other [146]. A public, auditable ledger helps provide verification and accountability for data [148]. Whenever an entity initiates a transaction, a group of "volunteer recorders" start to write down this new transaction in their own local ledger. And after a period of time, a selected ledger from these recorders, which contains a set of transactions, will be verified and attached to the public ledger [214]. The recorders are known as miners in the blockchain systems. The local ledgers owned by the recorders are known as data blocks. The algorithm used to select a block to attach to the main public ledger is called a consensus algorithm, and the public ledger formed by these selected data blocks is called the blockchain [214].

This whole procedure is protected by digital signatures; that is, each transaction is digitally signed using the private key of the sender [146]. As a result, the validity and integrity of a single transaction are guaranteed. The integrity of the entire blockchain is ensured with hash computations. To encourage miners, coins are assigned to them as a reward once they successfully append a block to the ledger [72].

2.2 Blockchain Transaction

The transaction is the minimum, fundamental data unit in the blockchain, which represents the action triggered by a participant [214]. To initiate a transaction, the participant needs to associate the transaction with the cryptography credentials. Each participant in the blockchain network holds a pair of public and private keys. By applying a series of hashing and encoding functions on the public key, a short and unique address is generated as the public address of the participant (as depicted in Fig. 2). Normally, the transaction contains the address of the sender and receiver, and it is signed by the sender's private key. Once a participant initiates a transaction, it needs to broadcast the transaction to its connected peers, and the peers that receive this transaction will continuously relay the transaction to subsequent peers (more details of the block/transaction propagation can be found in [124]. Each transaction and the block that contains all transactions are verified by the miners, and a valid transaction is not approved and

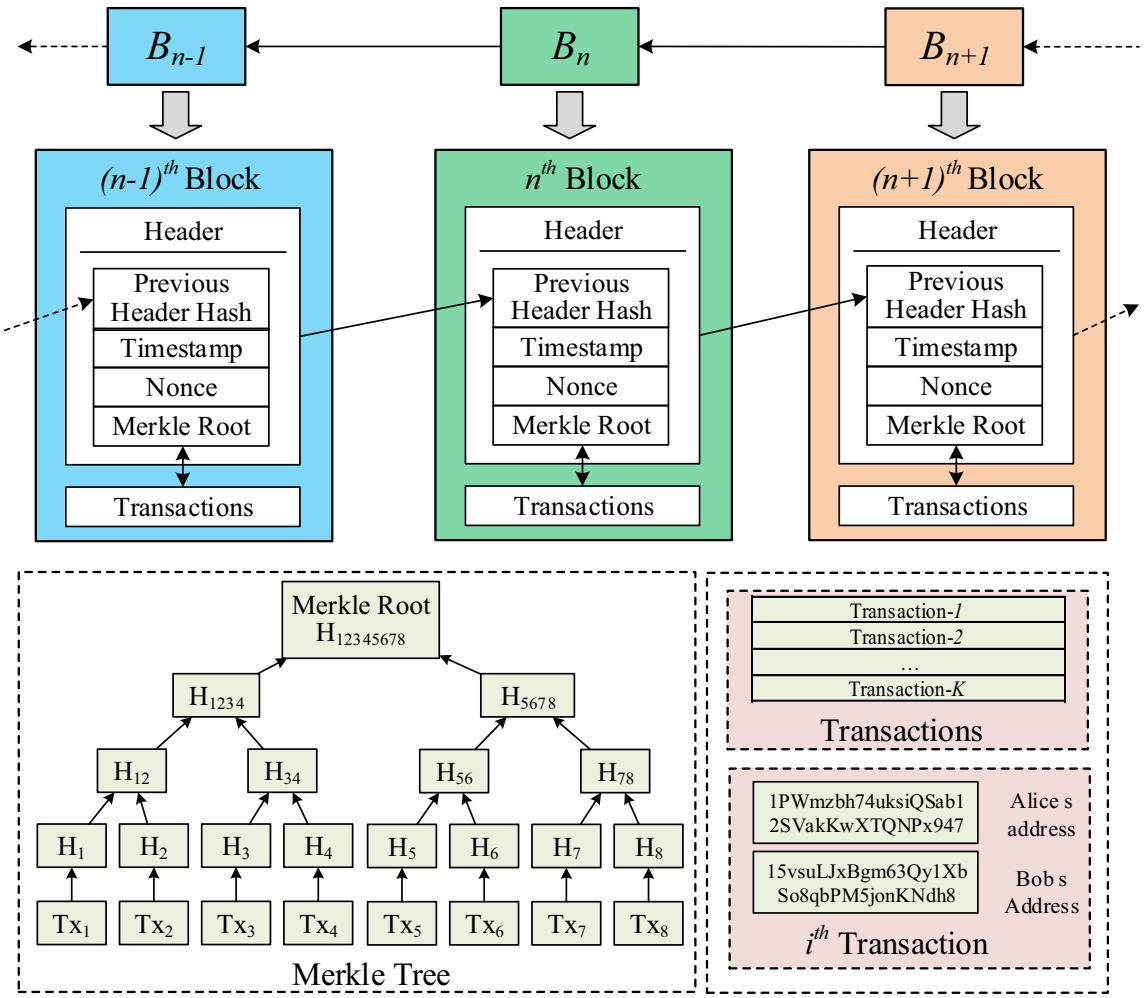

Fig. 2 Blockchain architecture (based on Bitcoin)

executed until specific requirements are satisfied (such as a certain amount of proof of work in Bitcoin, the transaction is approved until 6 blocks are appended which is a countermeasure to the double spending) [41].

2.3 Blockchain Structure

In a typical blockchain system such as Bitcoin or Ethereum, miners add valid transactions to a block, and a Merkle Root [139] is created for all these transactions as a digest or fingerprint [146]. As shown in the Fig. 2, a block header contains the hash of the previous block header, timestamp, a nonce, and the Merkle root of the transactions in the current block. All the blocks are connected in the form of a linked list, which is a type of data structure in which each data element contains a link to its successor or predecessor. As the whole network works on the same single chain, for a certain period of time, only a limited number of transactions can be validated by the newly generated block [72]. Thus, the block generation interval and the block size determine the transaction verification speed. For example, Bitcoin can append a new block with block size 1 MB every 10 min, which yields 3–7 transactions verified per second [72, 193].

Instead of packing a group of transactions into a block and forming a chain in a linked list, another blockchain structure has been proposed that is based on the concept of directed acylic graph (DAG). In the model of DAG blockchain, there is no need to encapsulate transactions into a block, and each transaction may represent a data point in the DAG. A notable DAG-based blockchain structure is Tangle, which was designed by IOTA [1]. In Tangle, one needs to verify two previous transactions and link the new transaction with the previous two to append a new transaction. An example of two types of blockchain structure is shown in Fig. 3. In the linked list blockchain, a certain number of transactions can be appended to the blockchain in a time interval. However, in a high transaction rate scenario, not all the transactions can be added, as with the transactions with red Tx tags in Fig. 3a. On the other hand, transactions and blocks can be appended to the blockchain in a flexible and efficient manner by using a DAGbased structure. As shown in Fig. 3b, the transactions with red Tx tags can also be added to the chain.

2.4 Consensus Algorithm

Regardless of what structure is used in the blockchain, a consensus algorithm is always needed to ensure fairness and security. The consensus algorithm is a required verification step for adding transaction records to the public ledger. As mentioned above, a new generated block is actually a selected ledger from all the miners; thus, a mechanism is needed to make all the miners reach the consensus about the selection. Note that this selection must not be biased in any sense. In an ideal model, every miner's ledger (in the processing block) should have the same chance to be selected. However, one could run multiple nodes to increase the possibility to be picked in the case of random selection. An attacker that controls a large number of nodes can practically manipulate the selection procedure. To prevent this, several algorithms emerged:

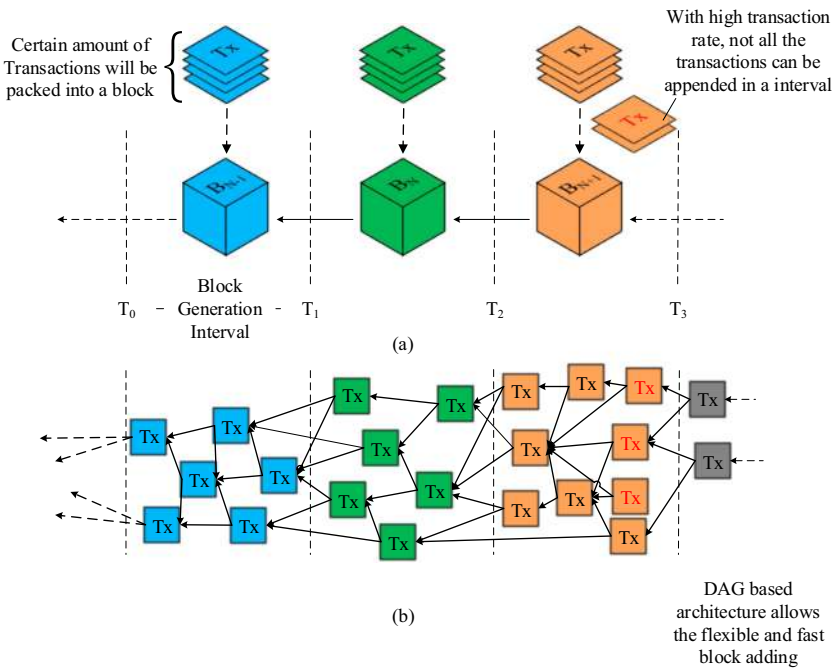

Fig. 3 Blockchain structures: **a** linked list–based blockchain [28, 146] **b** DAG-based blockchain [1, 39, 177]

- *Proof of Work* (PoW): In the PoW system, all miners compete to finish a computational resource–intensive task, and the first one that solves the task can append the current block to the public ledger. For example, the PoW in the Bitcoin system requires finding a nonce such that the hash of the current block header (including the nonce) is less than a specific value. This method improves security since the consumption of computational power increases the cost of selection participation, and once the computational puzzle is solved, all the other nodes can verify the answer easily. However, the drawback is the waste of resources: except for the winner of the mining, all the work of other nodes is simply wasted [203]. Note that all nodes in the blockchain system cannot participate in the mining due to excessive computational overhead.
- *Proof of Stake* (PoS): The PoS is an alternative consensus algorithm that requires less computational power than the PoW does. Instead of proving a certain amount of work has been done, miners must prove ownership of a certain amount of stake in the blockchain system. Ownership of the stake creates an implementation challenge, if a node does not own a certain amount of stake thus it can never be involved in the miner selection process. As a result, the wealthiest nodes can always control the blockchain. To address this issue, several variants of PoS have been proposed. For instance, in the Delegated Proof of Stake (DPoS) [42], stakeholders do not verify and append blocks by themselves but select a group of delegates to perform the block validating. Coin age, which was introduced by Peercoin ("https://peercoin.net/"), includes stake holding time as an additional measurement. Although PoS is more efficient compared with PoW, it is still not widely deployed: it occupies less than 2% of the market capitalization of existing digital currencies [123].
- *Byzantine Fault Tolerance* (BFT): The Byzantine Generals Problem [116] describes a conceptual situation that needs to reach a consensus among several generals. Blockchain can be considered a solution to this problem since it provides a consensus among remote and untrusted peers. However, solutions already existed before the blockchain was introduced. In addition, these solutions can be used as the consensus algorithm in blockchain, i.e., in the Practical Byzantine Fault Tolerance (PBFT) [48]. Each new block is selected when it is supported by more than 2/3 of nodes. Note that the reliable consensus can always be reached unless more than 1/3 of the network is compromised by the adversary.

Note that various consensus algorithms exist today, including Tendermint [109], XRP Ledger Consensus used by Ripple [61], SCP used by Stellar [137], Ouroboros from Cardan [60], Algorand proposed by Yossi et al. [83], and so on. In this article, we mention the details only for the mainstream algorithms. Interested readers can get detailed information from the aforementioned references.

2.5 Smart Contract

A smart contract is an automated agreement enforced by tamper-proof execution of computer code [54]. In the context of blockchain, smart contracts are scripts stored on the blockchain system that enable users to have general-purpose computations occur on the chain [53]. These scripts can be triggered and executed autonomously when certain conditions are satisfied. For example, a contract can be used to provide automatic currency exchange service that transfers a certain number of coins to some units of specific tokens. Smart contracts can be applied to various fields, including B2B international transfers, central clearing, mortgages, and crowd funding [181]. Note that few blockchains (e.g., Ethereum [28] and HyperLedger [26]) support smart contracts.

2.6 Network Type

Based on how the data is managed and accessed in the blockchain system, we can classify the blockchain into two types: permissionless and permissioned blockchain. In a permissionless blockchain, a participant can join the network without any approval or registration, and all the nodes can initiate or verify transactions. On the other hand, access to the network is permissioned, and the operations needed to perform or verify transactions be also under administrator control in a permissioned blockchain. Examples of both permissionless and permissioned blockchains are depicted in Fig. 4.

2.7 Security

A blockchain system is vulnerable to an adversary if he or she controls 51% of the computational resources. This attack is known as a 51% attack, especially applicable to the PoW blockchain. If an adversary possesses more than 51% of the computational power of a blockchain system, he or she can control the blockchain and generate valid blocks faster than the rest of the network. Although it seems impossible to perform the 51% attack on a widely used blockchain like Bitcoin and Ethereum, the attacks have been successfully executed on some other blockchains. Recently, the cryptocurrency Verge ("https://vergecurrency.com/") suffered several rounds of 51% attacks that caused over $1.7 million dollars to be stolen [17]. At least $18 million has been falsified from Bitcoin Gold in another 51% attack [10]. Those lesser-known blockchains do not have

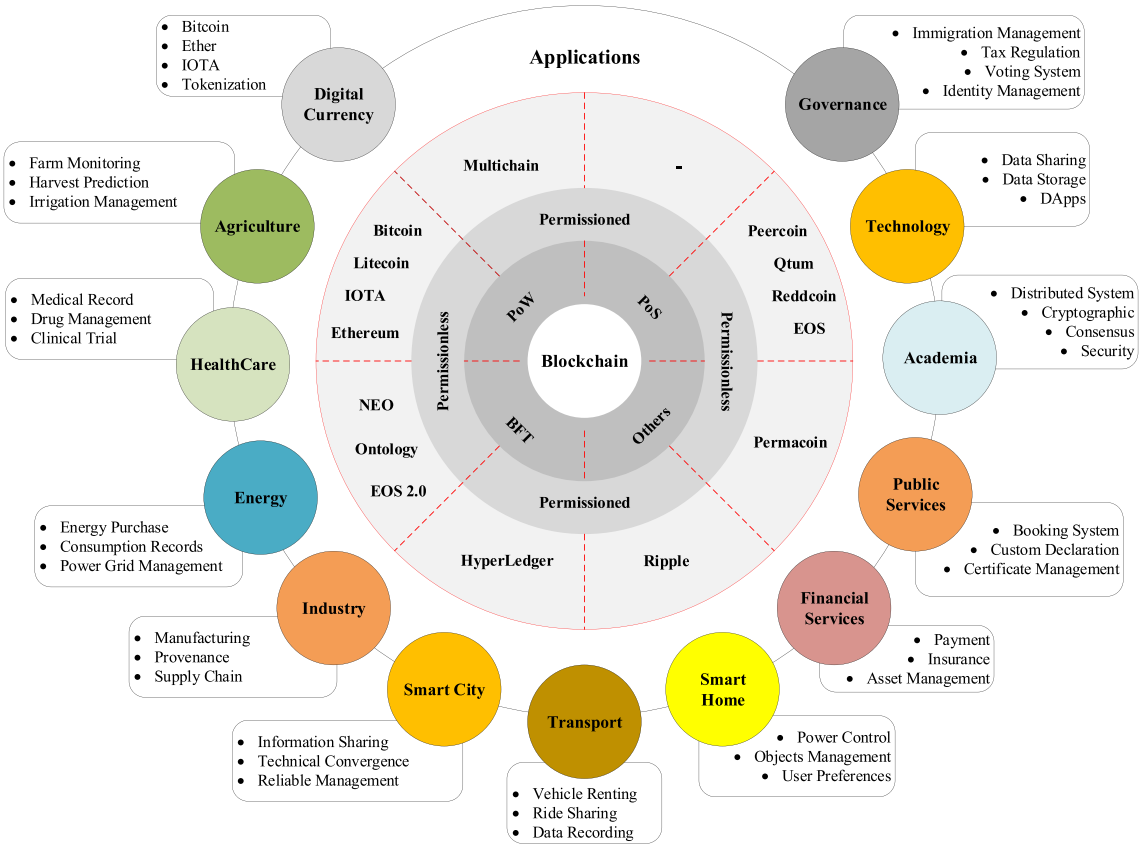

Fig. 4 Blockchain taxonomy and blockchain applications

sufficient overall computational power; thus the attacker could easily rent computational resources from the market [14] to launch the 51% attack.

PoS-based blockchain systems seem to perform better against 51% attacks because they rely on the idea that the higher stake holders have less interest and motivation to attack the chain, since the attack could risk the value of their stake. However, PoS systems confront the problem of *Nothing at Stake* (NaS): to maximize profit, a stakeholder can mine and verify multiple conflicting blocks without risking their stake [123].

3 Blockchain Applications in IoT

To overview the blockchain and blockchain applications, we need to create a taxonomy and a summary. Although various metrics can be used for a taxonomy of blockchains, such as the amount and existence of transaction fee, what state channel is used, and whether a native currency system is enabled, blockchain systems are typically categorized based on either consensus algorithms or network access types [180, 185, 201, 213] because these two attributes determine the network access and underlying mechanism of the blockchain. Here, as illustrated in Fig. 4, we perform a comprehensive and visualized taxonomy of blockchain systems based on these two factors in the inner circular area with a red boundary. We also describe blockchain applications in various fields in the peripheral blocks.

The consensus algorithms can be broadly classified into four types—PoW, PoS, BFT, and others (described in Section 2.4). All these four types are shown in the 2nd ring of Fig. 4. The 3rd ring describes the network type of blockchain systems, it could be either persimmisoned or permissonless. Note that, blockchain systems with all these four types of consensus algorithms could be either permissioned or permissionless. For example, multichain is a PoW-based permissioned blockchain, shown in the 4th ring. On the other hand, Bitcoin is a PoW-based permissioned blockchain. HyperLedger is a BFT-based permissionless blockchain. The last (e.g., 5th) ring consists of application and implementation examples of blockchain in various domains. For example, blockchain can be used to provide farm monitoring in agriculture, drug management in healthcare, asset management in financial services, etc.

From a IoT perspective, blockchain is a promising technology that can offer multidimensional reinforcements for the IoT infrastructure. As mentioned in Section 1.3, blockchain can contribute to the following aspects:

- *Service management*: As we know, the native and fundamental component of blockchain is the transaction, and the transaction-based blockchain architecture can help with the IoT service payment, which also enables IoT objects to perform real-time, automatic, and micro-transactions in a M2M manner. The concept and a case study of the blockchain-based IoT trading and business model are illustrated in [135, 208]. Using blockchain not only eliminates the need for human interaction but also decreases the cost of developing a payment model for specific services. Meanwhile, blockchain architecture can help to provide service and name discovery in the IoT system [62]. The proposed blockchains can be abstracted into multiple layers: the service regulators layer (government, organizations), the service providers layer, and the users layer. The regulator layer defines services and, for each service, corresponding service providers act as blockchain peers inside this layer. Similarly, all the devices used for a particular service are registered as blockchain peers in the service provider layer. At the user layer, one could discover, locate, pay for, and access a service without knowing IP or MAC addresses of the related devices. In short, blockchain enables the reliable regulating, payment, and logging for the IoT services.
- *Device management*: As the system owner needs to deploy and maintain a large number of objects with appropriate network and software configurations, the management of all these devices in the IoT system is challenging. Samaniego [162] and Sharma et al. [172] introduced the design of combining blockchain and software-defined networking (SDN) to address the networking management for all the devices. SDN is considered to be an appropriate technique that effectively improves the efficiency of the networking configurations. However, in a large-scale SDN-enabled system, a notable problem is the asynchronous status of the flow rule table [172]. By adding a blockchain layer over the SDN, the problem can be solved. As the result, the integrated system can perform direct deployment, configuration, and management of IoT components. It not only simplifies the device management but also enables fog computing and edge computing to provide additional usable resources for constraint devices. Moreover, new blockchain-based architecture improves the IoT system's performance and capacity, as it is more efficient, secure, and robust [168, 172]. Managing and maintaining the software and firmware for a huge number of devices are also daunting tasks. The problem becomes especially harder when some of the devices are not secured by design. It is essential to fix and patch the vulnerabilities of the firmware and software before adversaries get advantages from these flaws. Boudguiga et al. [44] use blockchain to provide better availability and accountability for IoT software maintenance. As manufacturers have the responsibility to notify of vulnerabilities and provide updates for the flaws, the blockchain can be used as a platform for manufacturers to update the devices reliably. Lim et al. [130] utilized blockchain to provide data integrity during firmware verification of the IoT devices.
- *Data management*: To refine the data management of IoT, Shafagh et al. [167] and Liu et al. [134] introduced auditable IoT data storage and sharing systems based on blockchain. In their design, the blockchain works as the middleware between the data storage services and the IoT devices. Blockchain does not directly store the original data but maintain the references and access control to the IoT data. Blockchain controls, verifies, records, and protects the storage and usage of the IoT data. The inherent reliability and robustness of blockchain ensures the trust and data security for both users and service providers.

Overall, blockchain is the enabler technique of building a smart management mechanism in IoT systems. Blockchain can enable smart manufacturing, remote maintenance, reliable supply chain management, auditable service, and additional security in IoT infrastructure. In the past few years, many blockchain-based IoT applications emerged in many areas, such as agriculture [46, 121, 131, 132, 189, 190], energy [78–80, 87, 117, 125, 127], healthcare [27, 70, 71, 85, 95, 129, 154, 161, 205], industry [35, 102, 143, 144, 176, 188, 202], smart cities [40, 104, 157, 159, 169–171, 174, 179], smart homes [20, 65, 74, 98, 173], and transportation [11, 51, 120, 204].

The following sections briefly introduces the blockchain applications in IoT.

3.1 Agriculture

Recently, IoT has become a vital component of the modern agricultural system. The power of IoT enables smart sensing of a farm's cultivated area [119, 212]. Real-time monitoring of temperature, humidity, disease, and insect damage make a significant contribution to crop growth and harvest prediction. Additionally, a prototype of a blockchain-based agriculture system is proposed in [132], where both the individual farms and the government can get benefits by using the shared information and knowledge. An example is to help the construction and maintenance planning of irrigation canals [132].

The use of blockchain in IoT agriculture applications also helps to provide transparency and traceability for crop and food supply chain [46, 121, 131, 132, 189, 190]. Leng et al. [121] proposed to use a blockchain-integrated system

to provide transparent and secure transaction recording for agriculture supply chain. Moreover, the rent-seeking and matching of resources can be self-adaptively completed. In addition, since food safety is always a public issue, blockchain- and IoT-based agriculture systems can enable reliable food safety by gathering and exposing information about food production, processing, warehousing, and selling. Tian [189] introduced a method of using RFID and blockchain to enhance food safety. Caro et al. [46] implemented a blockchain-based smart agriculture system, which enables the traceability of agriculture products in the supply chain.

3.2 Energy

Smart grid is a revolutionary technique in the electricity power system [94] that enables efficient and automated management via network connections. IoT is the core component and enabler technology of smart grid. By extracting energy data from smart sensors and meters, efficient energy measurement and management can be performed [175]. However, the smart grid has some limitations in complexity and reliability. As power system complexity increases, managing the system becomes challenging. In addition, the utility companies may face problems with convincing customers of the reliability of meter readings.

Blockchain can be an appropriate tool to solve some of the problems that exist in the smart grid. Researchers have proposed different blockchain-based solutions to address these issues. Laszka et al. [117] propose to make the system more manageable by replacing the original local grid with transactive microgrids. Their proposed framework introduces the design of blockchain-based energy transactions, in which grid nodes can use to perform privacy-preserving energy trading. Gao et al. [79] introduced a smart contract–based smart grid system, which ensures the transparency and provenance of energy consumption. Similar ideas have been proposed in [80, 87], which use blockchain to securely monitor and record the use of energy. A consortium blockchain applied energy trading framework is elicited in [125] to secure energy trading and achieve an optimal pricing strategy. Moreover, a blockchain-based data protection framework is demonstrated in [127], which provides the robust and reliable protection against cyber attacks. Blockchain is also used to provide secure, reliable, and auditable neighboring energy trading in smart grid [78].

3.3 Healthcare

Blockchain is also considered a revolutionary technique for healthcare systems [140]. Blockchain-based healthcare implementations fulfill the urgent demands of availability, security, and transparency or privacy, which already play an important role in clinical trials, healthcare data sharing, electrical patient records (EPRs) management, drug tracking, and healthcare device tracking [126]. Meanwhile, smart healthcare, as the most successful and significant application of IoT, would be more preferable and reliable if it could combine with and get benefits from blockchain technology [161].

Data sharing among healthcare organizations can contribute to treatment and medical research; however, the privacy of patient needs to be guaranteed. Esposito et al. [71] demonstrated the need for blockchain in healthcare data sharing and described the design of blockchain-based architecture to ensure privacy and efficiency. Yue et al. [205] illustrated a blockchain scheme that enables the patient to own and control his or her medical data. A prototype is implemented in a smartphone, in which the user can view, determine, and limit the sharing of data. In addition, an elaborate discussion and analysis of blockchain-based healthcare data sharing system is performed in [95]. It is also worth mentioning that Liang et al. [129] introduced an integrated blockchain system that connects IoT wearable devices, patients, healthcare providers, and health insurance providers all together to provide reliable data sharing and collaboration. The same concept has been applied in [85, 154], and a blockchain-enabled IoT system is created to monitor the patient health condition and to record the information into blockchain. Another work from Angeletti et al. [27] aims to offer information privacy in clinical trials. Using blockchain and IoT, individuals can keep their data private until an agreement is reached, and the clinical research institute can ensure that it is acquiring appropriate, useful, and authentic data from individuals.

3.4 Industry

With the emergence of Industry 4.0 [84, 166], IoT has become the backbone technology of cyber-physical systems (CPS), which enable smart sensing and supermatic operations. In addition, smart manufacturing provides remote machine diagnostics and supply chain management provided by the industrial IoT, which can further be enhanced by blockchain.

In-depth surveys of blockchain in the industrial IoT are performed in [143, 188]. Bahga et al. [35] pointed out that blockchain-based industrial IoT can be applied to on-demand manufacturing, smart diagnostics, supply chain management, product certification, and machine to machine (M2M) transactions. They demonstrated a blockchain-based architecture that enables the efficient and secure decentralized IoT service, which allows a user to provision and transact with the machines directly. Moreover, a smart

contract–based maintenance and diagnostics prototype is implemented in their work, which can sense the condition of the system and automatically sends notification to a user when a part replacement is needed. Sikorski et al. [176] illustrated a blockchain-applied M2M electricity market scheme for the chemical industry. They also implemented a proof-of-concept system that allows the energy consumer to buy electricity from an energy provider via smart contracts. In addition, a use of blockchain in material industry supply chain management is demonstrated in [144], where blockchain provides tamper-proof manufacturing, provenance, and distribution for composite materials. Nevertheless, credit-based trust system can be implemented with blockchain in industrial IoT scenarios [102, 202]. Blockchain could record and manage trust score of the network, while the service publishing and event logging are taken into account as well.

3.5 Smart City

A smart city is an automatic and holistic management and convergence of technology, institutions, and human factors [147]. In the technology vision, IoT is the fundamental and crucial component of the urban-scale information communication technology (ICT) platform [206]. As the blockchain can provide benefits to the IoT infrastructure in many aspects, it is reasonable and necessary to investigate the usage of blockchain for smart city applications.

Sun et al. and Rivera et al. provided a detailed survey of how blockchain can enhance smart cities in both economy and technical perspectives [159, 179]. Ibba et al. [104] proposed and demonstrated design of a blockchain-based smart city system to sense and manage data in an effective and secure manner. Biswas et al. [40] briefly illustrated the approach of using blockchain to secure smart city applications. Sharma et al. [169–171] demonstrated the design of efficient, sustainable, reliable blockchain-based network architecture for smart cities. An information-sharing blockchain over a vehicular network is described in [169], and scalable Li-Fi communication applied network architecture is introduced in [171]. Sharma et al. demonstrated the use of blockchain-based architecture to enable the integration of smart home, smart industry, smart healthcare, smart building, and smart transportation technologies for the smart city scheme in [170]. A similar integration and share of economy information via blockchain is also demonstrated in [157]. Moreover, Shen et al. [174] propose to combine machine learning technique with blockchain to provide privacy-preserving data processing in smart city applications.

3.6 Smart Home

IoT applications are beginning to direct modern life toward the fusion of convenience and intelligence, as smart wearables and network-enabled home appliances raise the quality of our daily life to a new level. As in the smart city sector, smart home applications can benefit by leveraging the features of blockchain.

Fernández et al. [74] proposed a design of a ZigBee-based smart power outlet system for smart homes. Applying blockchain to this system allows remote control and automatic monitoring of power use. Aggarwal et al. [20] introduced the use of blockchain to provide and manage energy trading between smart grid and smart home systems. Another interesting application of using blockchain to build up a smart door lock system is demonstrated in [98], where the blockchain is used for authentication, recording, and payment. Dorri et al. [65] presented a case study of an optimized blockchain system to ensure the security and privacy of smart home applications. A consortium blockchain-based system is implemented to ensure the data privacy of smart home [173], where an additive homomorphic encryption is applied to encrypt the IoT data.

3.7 Transportation

The concepts and examples of using blockchain to strengthen the vehicular network are briefly mentioned in the Section 3.5. There is no doubt that blockchain can be applied to build or reinforce an intelligent transportation system (ITS). Several solutions and designs have emerged recently in this domain. For instance, IBM introduced a blockchain-based freight transportation solution, which can reduce or eliminate fraud or errors and also improve efficiency and security [11]. Instead of focusing on the supply chain or logistics, some researchers aim to utilize blockchain in smart traveling [51, 204]. A blockchain-involved transportation system allows the user to securely and efficiently rent or share a vehicle. In addition, payment to the services and the reputation management of the services can be achieved with smart contracts.

Lei et al. [120] proposed a method of using blockchain to provide key management to secure the ITS. In a traditional design of ITS, vehicles periodically transmit safety messages during the travel, and the system collects data via infrastructures built along the roads at specific intervals. For a particular region, the credentials of the vehicle and infrastructures are managed by a central authority. However, whenever the vehicle travels into a new region, the system needs to perform re-keying and

re-establishment procedures. In their proposed blockchain-applied architecture, the key transfer time can be shortened and the security of the procedure can be guaranteed.

4 Blockchain for IoT Security

Blockchain is an ideal option to provide decentralized security. The characteristics of high availability, tamper resistance, and transparency can fulfill the security requirements for IoT infrastructure. In this section, we present the use of blockchain for IoT security. In Fig. 5, we briefly describe the following measures for addressing security concerns: access control, data assurance, hardware counterfeit and tampering, key management, and trust.

4.1 Access Control

Access management in an IoT system is a challenging problem. How the device and data are being accessed directly determine the security of the system; however, the traditional centralized access control systems cannot fulfill the all the requirements for an IoT system. Some of the weaknesses of the centralized access control systems are summarized in [152] as follows:

1. It is hard to achieve end-to-end security.
2. Centralization creates a single point of failure on whose availability and reliability the security of the entire system relies.
3. As the access control is managed by a remote/local central entity, the user cannot be involved in the control of his or her own data.
4. Centralized service providers can make illegitimate use of data (e.g., Prism Program [15]).
5. Running a centralized access control system for a large number of devices is expensive.
6. For some IoT scenarios that require device mobility or collaborative management, a centralized access control system is not well fitted.

These limitations lead to the proposal of using blockchain to provide an available and reliable access control mechanism.

A blockchain-based access control system has better support of mobility, accessibility, scalability, and transparency. Ouaddah et al. [151] briefly demonstrate an access control framework named FairAccess, in which the blockchain is used to store, manage, and enforce the access policies. A simple case study is implemented on the Raspberry Pi, and the framework is able to securely manage the access of a camera. However, the limitation of FairAccess is that it requires the tokens as the cost and fee for creating and verifying the policies. A similar framework was introduced in [68], where a framework with no tokens and fewer transactions are involved. Ding et al. [63] propose to use blockchain as an attribute authority and key generation center for IoT infrastructure. The proposed access control management framework is decentralized and scalable, and further increases system robustness.

Novo [149] implements a prototype system based on CoAP to provide large-scale access management in the IoT system. The proposed framework consists of three parts: IoT network, management hub, and blockchain network. All data access inside the IoT network is recorded, verified, and managed by the blockchain. Since the edge devices or sensors may not afford the overhead of blockchain operations, the management hub works as the agent (miner) of the blockchain network. In addition, a design and evaluation of a blockchain-based access control system for IoT is illustrated in [199]. It shows that the system performs with acceptable processing delay and latency.

Preserving privacy for the IoT system is another focus of access control. Ensuring availability and transparency of data access is important, but it is more important to prevent

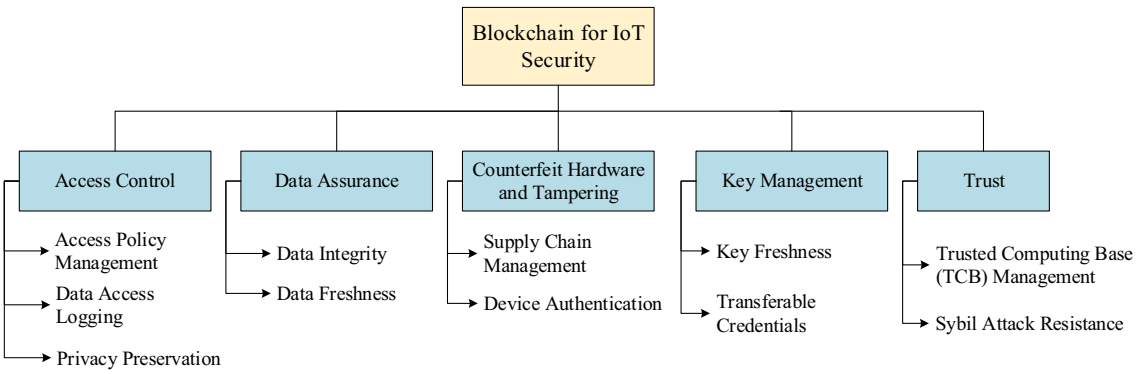

Fig. 5 Blockchain for IoT security

the reading or leaking of others' data and configurations. A general platform based on blockchain, IPFS [24], is designed to provide privacy for IoT data. By utilizing a private sidechain, all the data operations are logged and validated. In the work of Cha et al. [49], IoT service providers can obtain user consent on privacy policies without modifying legacy IoT devices by using blockchain and smart contracts. The user can query the Blockchain Connected Gateway to check the device information or access the data provided by the device without connecting to the device directly.

4.2 Data Assurance

In addition to data privacy and access, data integrity, and reliability also require our attention. An IoT system keeps sensing and generating large volumes of data. Since most of the data is transmitted via untrusted channels, there are potential risks of data tampering and data loss during the transmission. From the storage perspective, when the data is accumulated in the central database, it is a critical and severe problem to ensure the integrity and freshness of the data. We believe that blockchain is an appropriate technique to address the data provenance and data integrity problems. The hash function–based blockchain systems inherently address data integrity. They also provide the timestamp as a useful freshness reference.

Different researchers are already working on addressing data security issues using blockchain. Liang et al. [128] introduced a blockchain-based data assurance system for drones. The system consists of four components: drone, control system, blockchain network, and cloud server. The drone collects image or video data and receives commands from the control system. The cloud server logs the command records sent by the control system and stores the raw data in a database. The blockchain stores the hashed data records to provide data integrity and generates receipts for data validations. The implementation of a blockchain network in the proposed system is based on Tierion and Chainpoint [8]. As briefly mentioned in Section 3, blockchain-based IoT data storage systems can always provide additional and reliable data protection. Another similar example is [133], which also used blockchain to perform data verification and assure data integrity. They used blockchain to store the hashes of uploaded data and established and evaluated a proof-of-concept system based on Ethereum and *InterPlanetary File System* (IPFS) protocol [38]. To ensure the time synchronization of IoT services and guarantee the freshness and reliability of data, a blockchain-based time synchronization method is proposed in [73], where an IoT node could verify and synchronize the time by reading the time consensus result in the blockchain.

4.3 Counterfeit Hardware

The continuous growth of counterfeit electronics devices poses a serious threat to critical IoT infrastructures due to their inferior quality and has become one of the major concerns of the government and industry [23, 91, 92, 155, 187, 207]. Most low-cost edge devices are manufactured in limited-trust environments lacking relevant government regulations (e.g., to curtail counterfeiting and infiltration of threats at manufacture), move through supply chains without strong controls, and then are deployed in critical infrastructures worldwide. Attacks on the IoT system can originate from untrusted hardware by exploiting existing communication protocols and network traffic. Hardware attacks against a system can occur with physical tampering of a device and/or by the introduction of a counterfeit device [22, 56, 57, 186, 187] into the system.

The detailed descriptions for counterfeit ICs can be found in [89, 91, 92, 187]. However, we consider devices rather than ICs for IoT perspective. Counterfeit devices can be described as non-authentic devices. These fake devices can be manufactured with inferior quality parts, those can be reclaimed from discarded electronics. In addition, an adversary can produce devices with the bill-of-materials similar to the authentic ones. An adversary can also tamper the device to create a backdoor, which can be used for malicious purposes. Counterfeit IoT devices could be potentially installed with a malware, or even controlled by adversary as a bot. According to Nokia Threat Intelligence Report, 78% of malware activities in 2018 are driven by IoT botnets [6]. The first Mirai malware–based IoT botnet DDoS attack took down hundreds of web services for hours (including Github, Twitter, and Netflix). These attacks not only damaged the targeted services but also affected the IoT devices owners—the attack on Krebs cost the devices' owners approximately $320,000 on excess power and bandwidth consumption [16].

The detection of counterfeit electronics in the IoT infrastructure manifests a variety of challenges. It is difficult to detect whether devices or appliances have been tampered with. It is also hard to imagine how the user can know and detect an eavesdropping microphone embedded in a smart bulb or smart television. For an IoT infrastructure, an untrusted employee may also try to tamper with some devices for his or her own benefit. Moreover, for IoT devices that have high mobility like drones, if the protection cannot fully cover all regions of travel, then the devices would have higher potential risk of being tampered with. Even a verification mechanism is provided, it is hard to keep verifying a large amount of devices in a regular interval.

To solve the mentioned challenges, Guin et al. [90] introduces a blockchain-based framework to prevent and

detect hardware counterfeit and tampering. The proposed framework has four main components: physically unclonable functions (PUF) [82, 86, 178], global blockchain, local blockchain, and a secure communication protocol [93]. An SRAM PUF [86, 195] is used as the device identity generator that can generate unique strings for each device. A global identity blockchain is used for manufacturers of edge devices to register their devices. Once a device is registered, anyone can globally access its identity. Blockchain eliminates the need of central or local database for storing device IDs, which helps to solve the single point of failure problem. The inherent immutability feature of blockchain ensures the data integrity and also prevents the adversaries from tampering the data records. However, if a system is built upon traditional centralized database, all the data records could be altered and affected once the database is compromised. In addition, the distributors and customers can directly verify the device using the blockchain without querying the specific manufacturer's database.

The system proposed in [90] needs manufacturers to upload a cryptographic hash of the ID from PUF into the global blockchain such that an entity in the supply chain can verify the true identity of a device. However, it is required to authenticate every device in a regular interval when an IoT device (edge nodes) is deployed in the field. This prevents an adversary (e.g., a rogue or a compromised employee) put a counterfeit device into the IoT infrastructure. The communication between the gateway and edge node has to be very low cost. To provide that support a low-cost communication protocol [93] is used, which uses a secret key for transferring the PUF response to the gateway to verify the identity of the edge node in the field. Note that this secret key can also be generated from the PUF. A local blockchain contains the hash of device ID for identity verification.

Authenticity is not the only benefit of using blockchain, Islam et al. proposed a method that uses PUF and blockchain to enhance authenticity and traceability in the supply chain [108]. All the electronic parts or IoT devices can be registered, managed, and protected by a blockchain. Origin manufacturer, current and previous owners, and all the traces in supply chain can be recorded in the blockchain. This detailed information helps the customer to make their inference on the authenticity and reliability of IoT devices.

4.4 Key Management

With the expanding scale of IoT systems, key management becomes extremely challenging and requires immediate solution. For some applications, it may not be feasible to upgrade an IoT device to enhance security once it has been deployed. The key used for encryption, if present, needs to be refreshed securely to address long-term security. Blockchain can be used to address key management issues that the current IoT systems are suffering.

We have already mentioned in Section 3.7 that a key management framework for vehicular network using blockchain is proposed in [120]. In addition, multiple blockchains are used in [156] to provide a decentralized access control system for IoT networks. These blockchains are separately used to store public credentials, network contextual information, events logs, and access rules. The particular blockchain responsible for key management is the relationship blockchain, which maintains the credentials like keys and IDs, and also records the relationships among entities in the system. An authorized internal member could be registered on the chain only by storing a simple identity into the blockchain. However, an external member would need to upload the public key for that purpose. Another work from Kravitzet al. [114] proposed permissioned blockchain to provide rotatable and transferable key management for IoT system. A user could use, update, and manage the keys in one or a group of devices.

4.5 Trust

An adversary can easily disrupt the trust in the IoT system by spoofing or forging identities. For instance, the Sybil Attack [67] is based on interference with system reputation: one could register a large number of nodes to affect the consensus or the reputation of the entire system. Blockchain is a suitable solution for the trust management, as already proven by the PoW mechanism in Bitcoin; by increasing the cost of participation, trust is achievable. However, trust of nodes or peers is not the only concerning factor. Even when all devices are benign and trusted, the user still needs to determine whether data from the authenticated devices is always trustworthy.

Some trust management schemes rely on the concept of the trusted computing base (TCB) [101], which is widely used as a baseline to ensure an environment and all data from that environment are trustworthy. In [153], the reliability of the sensed data from IoT devices is addressed by combining the ARM TrustZone [7] with blockchain. Running the blockchain node inside the trust zone of a chip can achieve remote attestation and management of TCB. Asiri et al. [29] introduced a Sybil attack–resistant IoT trust model that uses blockchain. In this model, the trust problem of the local system can be addressed by using the Chaincode and endorsement policy of HyperLedger Fabric. The underlying concept is simple: some of nodes in the blockchain network work as the blockchain CA to validate and evaluate the trust of the system instead of involving a third party CA. Hammi et al. [97] proposed to create bubbles (groups) in IoT infrastructure and register all the bubbles and bubble members in blockchain. Therefore, all

the communication and data in the bubbles are protected and trusted, and all the communication attempts from outside the bubble are blocked.

As most of the IoT infrastructures rely on a central management system, which is generally maintained by third parties, the trust of services provided by them always remains one's concern. A decentralized blockchain-based framework is proposed to replace the third party data management authority in IoT infrastructures [32]. With the help of blockchain and Intel SGX hardware, a local trusted execution environment can be established, which could further replace and outperform a third-party data processing service [32]. Similarly, a blockchain-based nonreputation service scheme for IoT is described in [202], where the blockchain works as a service publisher and event recorder. In addition, Ma et al. introduced a blockchain-based key management system for IoT infrastructure, where the central key generation center can be eliminated and the trust can be preserved [136].

On the other hand, the trust of all the participants along with the third-party service providers in the IoT infrastructures can be managed by blockchain as well. Zhang et al. proposed a blockchain-based smart manufacturing system, which aims to reduce the "trust tax" paid by the participants [209]. Blockchain enables the transparent data management in the manufacturing and distribution procedure, the manufacturer, distributor, customer, stakeholder, and government could all get benefits. A similar idea of ensuring trust among IoT participants via blockchain is demonstrated in [182].

As long as a IoT service is publicly accessible and centrally managed, trust will always remain an inevitable issue. The operations and behaviors of infrastructure owners, data producers, and data buyers need to be regulated in a reliable and traceable manner. The access to data, use of devices, and payments to services need to be secure and auditable. It has been proved that blockchain could be an ideal option to provide secure trust management in IoT infrastructures. Further development and investigation of blockchain in IoT applications have far prospect.

5 Challenges and Limitations

As a result of the rise of cryptocurrency, investigation into uses of blockchain beyond cryptocurrency has become an attractive focus for both industry and academia. A number of blockchain applications in IoT have also been implemented and discussed in both academia and industry, and some of the examples are already introduced in Section 3. Though the blockchain could enhance and refine various aspects of IoT, the design and implementation of blockchain is in the nascent phase. Besides the benefits that IoT could gain from blockchain, it is very relevant to address a series of underlying challenges and limitations. In this section, we focus on discussing the challenges of using blockchain in the IoT perspective. We present a discussion on the applicability and necessity of using blockchain in IoT scenario, followed by the analysis of the cost of implementing blockchain in IoT. Then, we discuss the throughput and latency limitations of the blockchain as well as the on-chain privacy and security problems. In addition, we discuss the maintenance and regulation of blockchain-based services.

5.1 Applicability and Necessity

For some application domains, blockchain is an ingenious and practical complement for both data management and security. But not all the services and scenarios require the adoption of blockchain, and it is inadvisable and unnecessary to insist on using blockchain. To determine whether an application must involve blockchain, the following should be considered:

- *Trust among entities:* If all participants of the IoT network trust each other or the IoT service is acceptable for a trusted central authority, then the need for blockchain is dramatically decreased.
- *Need for data sharing:* Besides the trust of the system, if the data itself does not have to be shared among the entities, e.g., the data is private, even the hash of the data or the number of data entries is not allowed to be shared. Then, the introduction of blockchain in IoT is not significant. In addition, blockchain is suitable and useful in data sharing when the data owners need a common platform for such a purpose, meanwhile the data itself and the data sharing procedure cannot be controlled by one or a group of entities. For example, one needs to share the data with other nodes in the network but each time only wants to share it with only one receiver where it is not allowed to expose the data to any third party.
- *Implementation cost:* A limitation of using blockchain as a data platform for IoT is the cost of data storage in the chain. IoT generates huge amount of data, so one should primarily consider two cost factors: (i) *Data storage cost:* If the data needs to be uploaded and shared through a public chain, it is necessary to consider cost per data byte and whether it is worth storing a large volume of data in the blockchain. However, if the blockchain is only used for storing the policies and identities, the cost should be affordable. (ii) *Data protection cost:* Transparency is a main advantage of blockchain; however, when it turns to data storage, transparency could be a drawback. If the aim is to provide privacy in a transparent chain, the data stored

in the chain may need to be hashed or encrypted. As a consequence, the size of the stored data could increase, especially for the sensor data. For instance, a temperature sensor generates raw data points a few bytes in length (e.g., 25 °C). However, after the SHA-3-256 hashing, the data becomes 32 bytes long. The additional storage cost can be neglected when the frequency of data upload is low or the overall data amount is limited.

5.2 Implementation Cost

Generally, blockchain is not a lightweight solution. The PoW mining procedure is especially resource intensive, since it requires miners to continuously perform hashing to add a block in the chain. Even for a resource-sufficient device like a desktop computer, efficient mining requires certain hardware resources. Thus, it is not yet practical to involve mining into resource-constrained devices in an IoT system. For the PoW-based blockchain applications in the IoT, the edge device at most can work as the simple blockchain node, which can only receive data blocks and initiate new transactions. One needs to use separate resource-sufficient devices to mine for the blockchain network. Another situation is more severe: the IoT device cannot even afford the overhead of running as a simple node because the processor power or the memory size limits the constraint device to run a blockchain client and join the blockchain network. In this case, an agent or gateway device is required to receive, relay, and upload the data. An example of the scenario is described in [149]. The resource limitation actually decouples the blockchain layer with the IoT layer and makes those miners in the blockchain become the local central authorities. This decoupling is clearly a violation of the original intention for using blockchain.

5.3 Throughput and Latency

The block generation and transaction processing speed of the blockchain increase the latency and impede the throughput of a system that uses blockchain. This problem becomes more severe for the IoT scheme, since the blockchain system takes time to achieve a consensus, even for a small IoT infrastructure with a limited transaction rate. The system needs a certain amount of time to append the new data into the blockchain, and this minimum latency cannot be eliminated. The default block generation time of Bitcoin is around 10 min, and Ethereum's is around 17 s. For some other services, this latency is intolerable and it is necessary to find a way to further reduce the block generation interval [72]. A scaled IoT system requires a platform that can handle thousands of transactions every second. However, the traditional design of a blockchain system, such as Bitcoin, can only support 3–7 transactions per second. With some modification and optimization of the original design, Ethereum can still only process 20 transactions per second. The throughput of such blockchain design cannot fulfill IoT requirements.

5.4 On-Chain Privacy and Security

As stated previously, when we enjoy the benefits provided by blockchain, a reliable method to preserve privacy is needed as well. Note that blockchain is suitable for providing privacy and security for IoT applications, but it does not mean the blockchain itself does not face any privacy and security challenges. On-chain privacy is still an ongoing research problem. One of the most notable methods is the zero-knowledge proofs (ZKP), which allows peers to authenticate one other or verify a statement without revealing the identity [37]. ZeroCash is a cryptocurrency built upon the ZKP [164], and Hawk [113] is a ZKP-based framework that provides privacy-preserved smart contracts. These two implementations also demonstrate the feasibility of using ZKP to achieve privacy in blockchain systems.

When it comes to blockchain applications in IoT, security issues are a different story. First, the practical ZKP scheme divides into two types: either it requires multiple interactions between two peers or it relies on a trusted setup of common reference strings (CRS) on both peers. Using an interactive model requires multiple times of communications for proving and verifying, which also provide additional and unaffordable traffic overhead for constrained devices. There is also an issue with the difficulty of securely pre-deploying the CRS in thousands of different types of IoT devices. Second, the proving and verifying procedure of ZKP are resource intensive and time consuming [113]. The detailed overhead of enabling ZKP in blockchain is yet to be evaluated.

It is promising to incorporate zero-knowledge proof (ZKP) to improve the privacy of blockchain instances. However, the integration of ZKP-based blockchain in IoT still remains challenging and is in its infancy. Hardjono et al. introduces a conceptual ZKP-based blockchain system to securely and anonymously commission IoT devices into cloud [100], but the real implementation of ZKP-based blockchain in IoT is estimated to complete. Another ZKP-based blockchain system is described in [87], which aims to ensure the reliable energy consumption records in smart grid. However, the ZKP used in this system is more like a ring signature, and it requires a user to register multiple pseudonyms (keys) to hide their real identities. Each authentication procedure needs to be associated with a pseudonym (key).

Homomorphic computation could be another potential choice to further solve the on-chain data privacy problem.

An example is described in [215] as Beekeeper system. In the proposed Beekeeper, the encrypted data sent by IoT devices can be processed by other members of the blockchain (servers) without decrypting the data. However, the processing and operation on the data are still limited to simple addition and multiplication. A similar experimental use of additive homomorphic encryption (only supports addition) is shown in [173]. Note that, ZKP mainly provides privacy of user credentials and identities, while homomorphic computation in Beekeeper focuses on data privacy. Hashing and encryption of data provide a baseline data privacy in blockchain, but ensuring privacy during data processing needs further investigation.

Smart contract security is another major concern of blockchain applications. Most of the novel capabilities provided by blockchain applications need the support of smart contracts, and the security of smart contract has its own challenges. Ethereum, as one of the most popular smart contract platform, has smart contract issues such as vulnerability of smart contract coding, like the example in DAO [9], which utilizes the unchecked fallback functions. Another type of vulnerability is to play with the gas mechanism (transaction fee) in Ethereum. For instance, an issue has been found in King of the Ether Throne [13]: by only including a small amount of gas in a refund transaction, the transaction could be intentionally failed. In addition, keep storing data in an array in the smart contract may continuously increase the gas cost of the contract operations related to this array. At a certain point, because of the huge gas cost, the array cannot be altered anymore. Some other details and examples of the vulnerabilities are demonstrated in [30].

5.5 Maintenance and Regulation

The blockchain application owner needs to consider the drawbacks of anonymity. If the service is not running on the permissioned scheme and the user has the access to the blockchain, it may lead to some potential risks. Since a user maintains a secret identity in the blockchain, interacting with unknown peers faces legal obligations and reputation risks.

Immutability is also a double-edged sword of blockchain. As the blockchain is a tamper-resistant system such that each block appended into the chain is immutable, one could not modify, replace, or discard an appended block on the chain. However, it is needed to correct mistakes and exceptions inside a system. A block may contain an appropriate transaction with a huge amount of money sent to a wrong receiver, a smart contract with flaws can be published, and incorrect data entries may be uploaded into the contract. For a traditional system that uses databases, these problems can be fixed easily. But reversing the data stored in the blockchain may require careful consideration, supervising, and a certain amount of payment (hard fork a blockchain to reverse mistakes [142]). Although Ethereum allows republishing of a smart contract or removing some contents stored in the contract, it also introduces some further concerns, e.g., the security of the system relies on the reliability of the contract owner.

Another issue that has been less frequently discussed is the termination of blockchain services. Unlike a traditional service, the service vanishes after shutting down the server and removing the database. A blockchain is a collaborative recording system that starts within a same genesis block. Even if the service provider decides to stop the operations, one could still continuously work on this chain for one's own purpose. One could fake the original service or run it for some illegitimate uses.

For the IoT perspective, maintenance of blockchain services encounters additional security challenges. Since most of IoT devices are resource-constraint, most of them cannot work as a full blockchain node. Namely, the computational mining power is usually separately configured or even outsourced. The outsourced mining pool manager for a large-scale blockchain-based IoT service could decide to hop to other mining tasks for more mining rewards, this situation is described as "coin hopping attack" [216]. When such attack occurs, the victim service would be halted due to lack of mining power, and those smart devices typically lack the ability to sense a pool manager's behavior due to the limitation of computational power [216].

6 BIoT Research Roadmap

Hundreds of blockchain-related papers have been published in conference proceedings, journals, or magazines in the last decade, and the rate and number of publications maintains a rapid growth due to the promising future of blockchain. Blockchain in IoT is a subsection of the blockchain research domains that also get extensive attention in the research community. In this section, we present and analyze the overall status of blockchain usage in IoT.

A variety of researches and applications prove the feasibility and practicability of using blockchain in IoT. However, as described in Section 5, there are still several challenges that need to be addressed, some problems require solutions, and some implementations and designs of the application can further be refined. Currently, we are just at the beginning of a long journey of blockchain in IoT research. Although the prospect is bright, the future directions need to be discussed and analyzed. Further optimization and adoption of blockchain is urgently needed to make the blockchain more suitable and available for IoT systems. In addition, a detailed and comprehensive

measurement of the application in a practical and scaled system has never been performed even though some of the concepts and prototypes of blockchain applications in IoT are proposed, introduced, and implemented. Moving forward one more step, the potential of joint points in other scenarios also need to be analyzed despite blockchain already being applied in a few IoT application domains. In this section, we also briefly introduce the roadmap of blockchain in IoT research with regard to all the aspects mentioned above.

6.1 Research Trend

To present an overview of the blockchain and blockchain in IoT research, we show a timeline in Fig. 6. In 2015, 7 years after Satoshi Nakamoto introduced blockchain, favor toward and investigation of using blockchain in IoT increased. Although there were a few works that mention

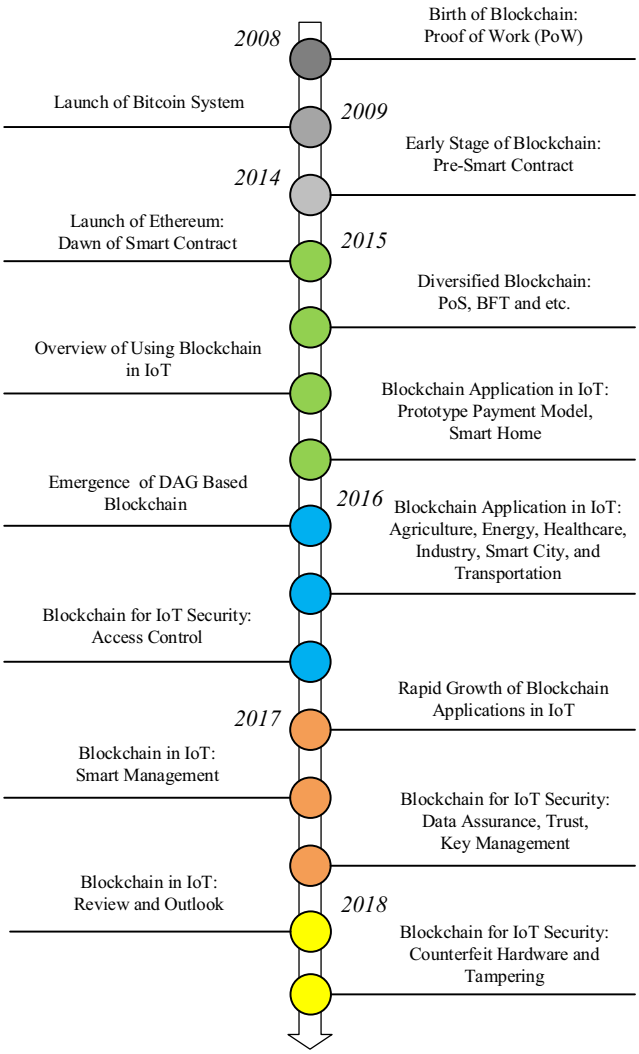

Fig. 6 Timeline of Blockchain and Blockchain in IoT

the convergence of blockchain and IoT between 2008 and 2015, the fusion was just demonstrated in a general view without specific and practical implementation. The real revolutionary technique that triggered the development of blockchain applications in IoT was the smart contract, and the practical smart contract platform was launched by Ethereum in 2015. After several initial attempts to use blockchain in IoT in 2015, there is an increasing research trend. In this paper, we surveyed 97 blockchain in IoT papers since 2015, and the publication trend is described in Fig. 7. It is shown the publication number is expected to keep rising in coming years.

6.2 Optimization and Adoption of Blockchain

Before blockchain can be adopted into IoT and before an IoT-oriented blockchain application can be implemented, the blockchain has to overcome the limitations of resource intensity and throughput bottleneck. Resource and energy intensity are mainly incurred by the difficulty of reaching consensus. Most of the current blockchain applications in IoT use PoW consensus mechanism; as the original and representative consensus algorithm, PoW is supported by a variety of blockchain systems. It is also reasonable to select PoW as the first option to implement a blockchain application in IoT. However, prevalence and popularity do not indicate that an option can be suitable. A few other consensus algorithms like PoS and BFT are also competitive, but they are less investigated in IoT applications.

PoS- and BFT-based blockchains have better scalability and efficiency compared with the traditional PoW-based blockchain instances [26, 137, 193]. The overall system throughput and latency are proved to be significantly improved as well. In addition, PoS and BFT require less computational resources as there is no need for hash computations as a part of Proof of Work. The overall energy consumption per transaction in Bitcoin system is around 620 KWh (power consumed by all the active nodes; the average reachable nodes in Bitcoin network is around 10,000 nodes [2], and note that part of them are involved in a particular transaction relay and mining.), whereas Ethereum uses around 27 KWh [3, 4]. Even for the most resource intensive consensus algorithms, the power consumption could be optimized and deducted. While running blockchain clients with same test benchmark on Raspberry Pi, the power consumption per client of Hyperledger is only half of Ethererum client [163]. It is reasonable and promising to adopt lightweight consensus algorithm in IoT scenarios. Currently, research is ongoing to develop lightweight consensus algorithms.

Instead of using the current algorithms, developing a new and appropriate algorithm could be more suitable for a

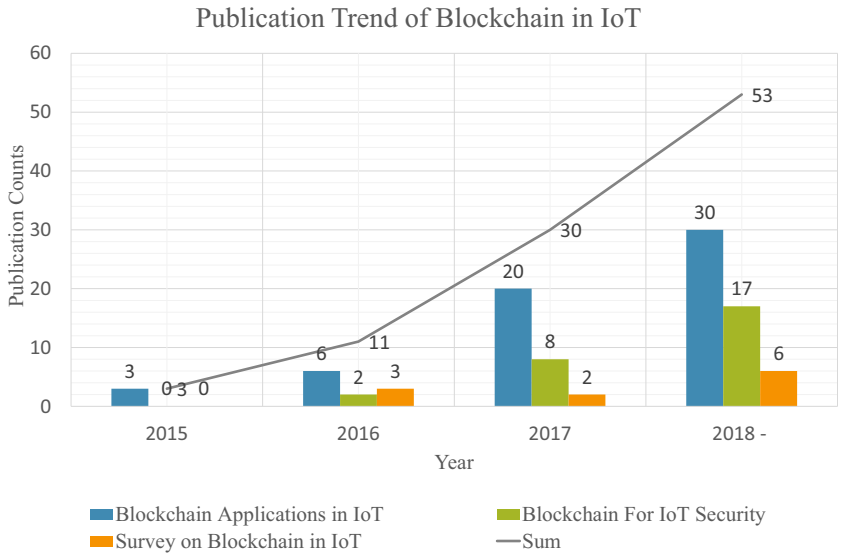

Fig. 7 Trend of blockchain research in IoT

specific IoT application. Some of the researchers mentioned or performed the design of lightweight algorithms for IoT scenarios [66, 90]; however, the implementation and analysis of such algorithms are yet to be performed. It is worth mentioning that the essential goal of the consensus algorithm in blockchain is to provide a secure and random selection mechanism, which also ensures the selected participant can be verified and accepted by the whole network. Some of the researchers mentioned that the verifiable random function (VRF) [141] is an ideal match for the blockchain consensus problem, and several VRF-based blockchain architectures also emerged [60, 83]. Basically, VRF is a pseudo-random function that can be used in the blockchain to randomly select users in a private and non-interactive way [64, 83]. VRF-based blockchain attracts incredible public interest, which is also a proof of its potential. A notable example is the Cardano, which launched in October 2017 but has already climbed into the top 10 cryptocurrency list [5]. Elaborate introduction and description of VRF are out of the scope of this paper, but using VRF-based blockchain in IoT is an undiscovered and interesting path.

On the other hand, the blockchain structure itself suffers from the overall system performance. The traditional linked list–based structure is restricted by the block size and block generation interval problems, and it is worth investigating the use of a different blockchain structure. As introduced in Section 2, IOTA uses a DAG-based architecture, and some other DAG-based blockchains are described in Meshcash [39] and SPECTRE [177]. A DAG-based blockchain allows parallel and concurrent block appending, which significantly enhance the throughput and latency of the system [39, 83, 177]. If a DAG-based blockchain architecture can be adopted into IoT, the overall performance and scalability can be improved. Thus, developing and adopting the DAG-based blockchain (or blockchain with other structures) within an IoT scheme could be a noteworthy future direction. An experimental DAG-based blockchain for industrial IoT is implemented in [102]. The main purpose is to create a credit (reputation) system for IoT devices over blockchain. In addition, sidechain [34] is another solution of improving the efficiency of blockchain systems. Vara et al. [47] utilize the feature of sidechain to achieve an improved efficiency in IoT-blockchain management, where sidechains are created along with the main blockchain to store IoT data. All the sidechain data are appended into the main chain via a blockchain queuing system.

In addition, some of the other characteristics of blockchain can be further refined for the IoT scenario. The CAP theorem states that a distributed system cannot achieve consistency, availability, and partition tolerance at the same time [45]. Generally, blockchain gives up short-term consistency to achieve global availability and partition tolerance. Although the whole network will finally see the same public ledger, each node may have a different view of the public ledger at a particular time. This problem may be enlarged in the IoT scheme since IoT devices may not be active and online all the time due to the energy saving or limited channel access. When IoT devices participate in a blockchain network, the sleep period may cause an inconsistency between the device local blockchain and the global blockchain. It would be an interesting topic to accelerate the procedure of updating the local blockchain to a global one. Especially for the IoT applications, this procedure cannot be resource intensive or involve heavy communications. A trial example related to this topic is performed in [58]. In addition, lightweight

synchronization protocol and lightweight blockchain client for IoT are implemented in [59]. In the proposed approach, an aggregation scheme is defined to reduce the duty cycle of device, and the overall communication cost is reduced as well.

6.3 Blockchain-Oriented System

The integration of blockchain and IoT is still facing challenges due to the fact that running blockchain is power and resource intensive, whereas IoT devices are normally resource constraint. The optimization of blockchain in IoT is not only limited to the protocol establishment and software implementation but also refers to an all-sided hardware and system support. The design of blockchain-oriented hardware, the implementation of blockchain-oriented operating system and platform also need to be taken into account. Blockchain-oriented hardware that focuses on blockchain operations could further promote seamless integration of blockchain and IoT. This is promising and practical. IBM recently introduced a CPU capable of running blockchain operations, which is smaller than a grain of salt and costs only 10 cents [12]. This tiny computer can monitor, analyze, communicate, and act on data. It could be embedded and integrated into IoT hardware to provide additional, efficient, and reliable support for blockchain operations.

Running blockchain on IoT device is confronted with some other limitations. Since the hardware architecture of IoT devices are different with normal computers and servers. Not all the up-to-date blockchain implementations can be directly deployed on IoT devices. For example, maintaining and developing blockchain for an ARM-based hardware system is still insufficient. In addition, implementation of blockchain-oriented firmware or operating system for IoT devices is also necessary. The simplification and conduction of redundant functionality and the optimization and customization of system design could potentially help the integration of blockchain and IoT. Some pioneers have already started the investigation of blockchain-oriented IoT operating system [197].

6.4 Measurement and Practical Proofs

In the early stages of technology development, the technology always lacks measurement and proofs. For the blockchain applications proposed in the IoT paradigm, it is difficult to tell the amount of overhead from the introduced solution. The memory usage, CPU utilization, and energy consumption of the blockchain architecture remain uncertain. Even when a prototype system is built up, the baseline of hardware and resource requirements are always unclear. Meanwhile, though some of the works analyze the throughput and latency of using blockchain in IoT [96, 99, 194], the measurement of performance ceilings and comparisons with other methods are still open. Furthermore, the measurement and proof of the availability, consistency, scalability, stability, and security within a long-term living practical system also require our attention. Further investigation of detailed measurements and proofs may give other researchers a better overview and guidelines.

6.5 Potential Application Domains

The current research on using blockchain in IoT already covers the majority of the application domains, and here we briefly introduce a few other potential application domains that may be of interest:

- *Smart retail*: IoT can contribute to smart inventory management with refined accuracy and improved efficiency [107]. IoT solutions not only provide data collection and data connection between the point of sale (PoS) system and the inventory system but also allow the customer to use their mobile devices to check and locate the inventory. In addition, introducing blockchain into the retail scheme may create another revolution. Besides the logistic and supply chain management benefits it provides, blockchain can enable direct selling as well. Since the provenance, manufacturing, distribution, and sale are all recorded by the blockchain, it is possible for the producer and customer of a product to establish a precise and private retail channel.
- *Smart education*: Along with the development of IoT, education is also evolving at a very accelerated rate. By using smartphones, tablets, and computers, course schedules, homework assignments, and examination grading are moving in an efficient and paperless direction. Furthermore, students' behavior, learning habits, and knowledge mastery can be further collected, tracked, and analyzed by using IoT smart terminal devices, which enable custom and elaborate smart education. Adding blockchain into the smart education scenario is also reasonable, as blockchain can introduce additional transparency and fairness in education resource sharing, assignment grading, and course evaluation. Especially, blockchain can also contribute to certificate management in the education system.
- *Environment monitoring and disaster prevention*: There are several difficulties and drawbacks to deploying manpower for environment monitoring. First, it is difficult and expensive to cover a large area. Monitoring a entire piece of forest with only a few individuals is not practical and efficient. Second, it is hard for the individuals to consistently monitor the environment all

year long. Third, the monitoring of dangerous or tough environment zones like snowy mountains, volcanoes, and deserts causes challenges. Thus, it is reasonable to use IoT to achieve available and consistent monitoring in such environments. On the other hand, information integration, analysis of information correlation, and collection of individual reports are needed in a disaster prevention paradigm. Blockchain may help in long-term environmental data management and sharing.

7 Conclusion

The Internet of Things (IoT) and blockchain are two of the most promising technologies in this decade. The convergence of these two technologies is absolutely necessary and requires our attention and investigation. In this paper, we illustrated the decentralized, transparent, and tamper-resistant features of blockchain, which can enhance data management, service management, device management, and security of IoT. We summarized the blockchain applications used to refine IoT system performance and security within the agriculture, energy, healthcare, industry, smart city, smart home, and transportation domains. We then briefly analyzed and discussed the limitations of using blockchain in an IoT environment. We also presented the current research trends of and a future roadmap for blockchain in the IoT applications to provide a baseline guideline for adoption.

Acknowledgments This material is based upon work supported by the National Science Foundation under Grants Nos. 1755733 and 1663616.

Compliance with Ethical Standards

Disclaimer Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

References

1. The Tangle, http://iotatoken.com/IOTA_Whitepaper.pdf
2. Bitnodes, https://bitnodes.earn.com/dashboard/?days=90, Accessed September 2019
3. Bitcoin Energy Consumption Index, https://digiconomist.net/bitcoin-energy-consumption, Accessed July 2019
4. Ethereum Energy Consumption Index, https://digiconomist.net/ethereum-energy-consumption, Accessed July 2019
5. Top 100 Cryptocurrencies By Market Capitalization, https://coinmarketcap.com/currencies/cardano/historical-data/?start=20170826&end=20180826
6. 78% of malware activity in 2018 driven by iot botnets, nokia
7. Arm trustzone. https://www.arm.com/products/silicon-ip-security
8. Chainpoint. https://tierion.com/chainpoint/
9. The dao attacked: code issue leads to $60 million ether theft. https://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-thef t/
10. Hackers compromised the cryptocurrency bitcoin gold. http://fortune.com/2018/05/29/bitcoin-gold-hack/
11. Ibm and maersk form global joint venture applying blockchain to shipping logistics. https://www.ibm.com/industries/travel-transportation/freight-logistics
12. Ibm's blockchain-ready cpu is smaller than a grain of salt, costs just 10 cents. https://www.research.ibm.com/5-in-5/crypto-anchors-and-blockchain/
13. King of the ether throne refund issue. http://www.kingoftheether.com/postmortem.html
14. Nicehash: Largest crypto-mining marketplace. https://www.nicehash.com/?lang=en
15. Nsa prism program taps in to user data of apple, google and others. https://goo.gl/2RCCQB
16. Study: attack on krebsonsecurity cost IoT device owners $323k. https://krebsonsecurity.com/2018/05/study-attack-on-krebsonsecurity-cost-iot -device-owners-323k/
17. Verge suffers 51% attack yet again. https://blockexplorer.com/news/third-times-a-charm-verge-suffers-51-attack-yet-again/
18. Abomhara M, Køien GM (2014) Security and privacy in the internet of things: current status and open issues. In: 2014 International conference on privacy and security in mobile systems (PRISMS), pp 1–8
19. Abomhara M, Køien GM (2014) Security and privacy in the internet of things: current status and open issues. In: 2014 International conference on privacy and security in mobile systems (PRISMS)
20. Aggarwal S, Chaudhary R, Aujla GS, Jindal A, Dua A, Kumar N (2018) Energychain: enabling energy trading for smart homes using blockchains in smart grid ecosystem. In: Proceedings of the 1st ACM MobiHoc Workshop on Networking and Cybersecurity for Smart Cities, SmartCitiesSecurity'18, pp 1:1–1:6
21. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M (2015) Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Communications Surveys Tutorials
22. Alam M, Chowdhury S, Tehranipoor M, Guin U (2018) Robust, low-cost, and accurate detection of recycled ics using digital signatures. In: IEEE International symposium on hardware oriented security and trust (HOST)
23. Alam M, Tehranipoor M, Guin U (2017) Tsensors vision, infrastructure and security challenges in trillion sensor era. J Hardw Syst Secur 1(4):311–327
24. Ali MS, Dolui K, Antonelli F (2017) Iot data privacy via blockchains and ipfs. In: Proceedings of the Seventh International Conference on the Internet of Things, IoT '17, pp 14:1–14:7
25. Alliance Z (2009) Ieee 802.15. 4 zigbee standard
26. Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, Caro AD, Enyeart D, Ferris C, Laventman G, Manevich Y, Muralidharan S, Murthy C, Nguyen B, Sethi M, Singh G, Smith K, Sorniotti A, Stathakopoulou C, Vukolic M, Cocco SW, Yellick J (2018) Hyperledger fabric: a distributed operating system for permissioned blockchains
27. Angeletti F, Chatzigiannakis I, Vitaletti A (2017) The role of blockchain and iot in recruiting participants for digital clinical trials
28. Anonymous: White paper: next-generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/White-Paper

29. Asiri S, Miri A (2018) A sybil resistant IoT trust model using blockchains. In: 2018 IEEE International conference on blockchain (blockchain-2018)
30. Atzei N, Bartoletti M, Cimoli T (2017) A survey of attacks on ethereum smart contracts (sok). In: International conference on principles of security and trust. Springer
31. Atzori L, Iera A, Morabito G (2010) The internet of things: a survey Computer networks
32. Ayoade G, Karande V, Khan L, Hamlen K (2018) Decentralized iot data management using blockchain and trusted execution environment. In: 2018 IEEE International conference on information reuse and integration (IRI). IEEE, pp 15–22
33. Baccelli E, Hahm O, Gunes M, Wahlisch M, Schmidt TC (2013) Riot os: towards an os for the internet of things. In: 2013 IEEE Conference on computer communications workshops (INFOCOM WKSHPS)
34. Back A, Corallo M, Dashjr L, Friedenbach M, Maxwell G, Miller A, Poelstra A, Timón J, Wuille P (2014) Enabling blockchain innovations with pegged sidechains. http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains, pp 72
35. Bahga A, Madisetti V (2016) Blockchain platform for industrial internet of things. J Softw Eng Appl 09:533–546
36. Barcena MB, Wueest C (2015) Symantic security response: insecurity in the internet of things
37. Ben-Sasson E, Chiesa A, Tromer E, Virza M (2014) Succinct non-interactive zero knowledge for a von neumann architecture. In: Proceedings of the 23rd USENIX Conference on Security Symposium, SEC'14
38. Benet J (2014) IPFS - content addressed, versioned P2P file system
39. Bentov I, Hubácek P, Moran T, Nadler A (2017) Tortoise and hares consensus: the meshcash framework for incentive-compatible, scalable cryptocurrencies. IACR Cryptology ePrint Archive
40. Biswas K, Muthukkumarasamy V (2016) Securing smart cities using blockchain technology. In: 2016 IEEE 18Th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/smartcity/DSS), pp 1392–1393
41. Bitcoin confirmation. https://en.bitcoin.it/wiki/Confirmation
42. Bitshares: Delegated proof of stake. https://bitshares.org/technology/delegated-proof-of-stake-consensus/
43. Bluetooth S (2003) Bluetooth specification
44. Boudguiga A, Bouzerna N, Granboulan L, Olivereau A, Quesnel F, Roger A, Sirdey R (2017) Towards better availability and accountability for iot updates by means of a blockchain. In: 2017 IEEE European symposium on security and privacy workshops (euros PW), pp 50–58
45. Brewer E (2012) Cap twelve years later: how the "rules" have changed. Computer 45(2):23–29
46. Caro MP, Ali MS, Vecchio M, Giaffreda R (2018) Blockchain-based traceability in agri-food supply chain management: a practical implementation. In: 2018 IoT vertical and topical summit on agriculture-tuscany (IOT tuscany). IEEE
47. Casado-Vara R, Chamoso P, De la Prieta F, Prieto J, Corchado JM (2019) Non-linear adaptive closed-loop control system for improved efficiency in IoT-blockchain management. Inf Fusion 49:227–239
48. Castro M, Liskov B et al (1999) Practical byzantine fault tolerance. In: OSDI, vol 99, pp 173–186
49. Cha SC, Chen JF, Su C, Yeh KH (2018) A blockchain connected gateway for BLE-based devices in the internet of things. IEEE Access
50. Chandra H, Anggadjaja E, Wijaya PS, Gunawan E (2016) Internet of things: over-the-air (ota) firmware update in lightweight mesh network protocol for smart urban development. 22nd Asia-Pacific Conference on Communications (APCC)
51. Chen W, Ma M, Ye Y, Zheng Z, Zhou Y (2018) IoT service based on jointcloud blockchain: the case study of smart traveling. In: 2018 IEEE Symposium on service-oriented system engineering (SOSE), pp 216–221
52. Chiang M, Zhang T (2016) Fog and Iot: an overview of research opportunities. IEEE Internet of Things Journal
53. Christidis K, Devetsikiotis M (2016) Blockchains and smart contracts for the internet of things. IEEE Access
54. Clack CD, Bakshi VA, Braine L (2016) Smart contract templates: foundations design landscape and research directions
55. Conoscenti M, Vetrò A, Martin JCD (2016) Blockchain for the internet of things: a systematic literature review. In: 2016 IEEE/ACS 13Th international conference of computer systems and applications (AICCSA), pp 1–6
56. Cui P, Guin U (2019) Countering botnet of things using blockchain-based authenticity framework. In: IEEE Computer society annual symposium on VLSI (ISVLSI)
57. Cyr B, Mahmod J, Guin U (2019) Low-cost and secure firmware obfuscation method for protecting electronic systems from cloning. IEEE Internet of Things Journal 6(2):3700–3711
58. Danzi P, Kalør AE, Stefanovic C, Popovski P (2017) Analysis of the communication traffic for blockchain synchronization of IoT devices. CoRR arXiv:1711.00540
59. Danzi P, Kalør AE, Stefanović Č, Popovski P (2019) Delay and communication tradeoffs for blockchain systems with lightweight iot clients. IEEE Internet J 6(2):2354–2365
60. David B, Gaži P, Kiayias A, Russell A (2018) Ouroboros praos: an adaptively-secure, semi-synchronous proof-of-stake blockchain. In: Advances in cryptology – EUROCRYPT
61. David DS (2014) The ripple protocol consensus algorithm
62. Daza V, Pietro RD, Klimek I, Signorini M (2017) Connect: contextual name discovery for blockchain-based services in the iot. In: 2017 IEEE International conference on communications (ICC), pp 1–6
63. Ding S, Cao J, Li C, Fan K, Li H (2019) A novel attribute-based access control scheme using blockchain for iot. IEEE Access 7:38,431–38,441
64. Dodis Y, Yampolskiy A (2005) A verifiable random function with short proofs and keys. In: Public key cryptography - PKC 2005
65. Dorri A, Kanhere SS, 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 (percom workshops), pp 618–623
66. Dorri A, Kanhere SS, Jurdak R, Gauravaram P (2017) LSB: a lightweight scalable blockchain for iot security and privacy. CoRR arXiv:1712.02969
67. Douceur JR (2002) The Sybil attack. In: Druschel P, Kaashoek F, Rowstron A (eds) Peer-to-Peer Systems
68. Dukkipati C, Zhang Y, Cheng LC (2018) Decentralized, blockchain based access control framework for the heterogeneous internet of things. In: Proceedings of the Third ACM Workshop on Attribute-Based Access Control
69. Dunkels A, Gronvall B, Voigt T (2004) Contiki - a lightweight and flexible operating system for tiny networked sensors. In: 29th annual IEEE international conference on local computer networks
70. Dwivedi AD, Srivastava G, Dhar S, Singh R (2019) A decentralized privacy-preserving healthcare blockchain for iot. Sensors

71. Esposito C, Santis AD, Tortora G, Chang H, Choo KR (2018) Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput 5(1):31–37
72. Eyal I, Gencer AE, Sirer EG, Van Renesse R (2016) Bitcoin-ng: a scalable blockchain protocol. In: Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation, NSDI'16
73. Fan K, Wang S, Ren Y, Yang K, Yan Z, Li H, Yang Y (2018) Blockchain-based secure time protection scheme in iot. IEEE Internet of Things Journal
74. Fernández-Caramés TM (2015) An intelligent power outlet system for the smart home of the internet of things. Int J Distrib Sensor Netw 11(11):214,805
75. Fernández-Caramés TM, Fraga-Lamas P (2018) A review on the use of blockchain for the internet of things. IEEE Access
76. Finkenzeller K (2003) RFID handbook: fundamentals and applications in contactless smart cards and identification, 2nd edn. Wiley Publishing
77. Fremantle P, Aziz B, Kirkham T (2017) Enhancing iot security and privacy with distributed ledgers - a position paper. In: Proceedings of the 2nd International Conference on the Internet of Things, Big Data and Security. SCITEPRESS – Science and Technology Publications
78. Gai K, Wu Y, Zhu L, Qiu M, Shen M (2019) Privacy-preserving energy trading using consortium blockchain in smart grid. IEEE Transactions on Industrial Informatics
79. Gao J, Asamoah KO, Sifah EB, Smahi A, Xia Q, Xia H, Zhang X, Dong G (2018) Gridmonitoring: secured sovereign blockchain based monitoring on smart grid. IEEE Access
80. Gao J, Asamoah KO, Sifah EB, Smahi A, Xia Q, Xia H, Zhang X, Dong G (2018) Gridmonitoring: secured sovereign blockchain based monitoring on smart grid. IEEE Access 6:9917–9925
81. Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016. https://www.gartner.com/newsroom/id/3598917 (2017)
82. Gassend B, Clarke D, Van Dijk M, Devadas S (2002) Silicon physical random functions. In: Proceedings of the ACM Conference on Computer and Communications Security (CCS). ACM
83. Gilad Y, Hemo R, Micali S, Vlachos G, Zeldovich N (2017) Algorand: Scaling byzantine agreements for cryptocurrencies. In: Proceedings of the 26th Symposium on Operating Systems Principles, SOSP '17
84. Gilchrist A (2016) Industry 4.0: the industrial internet of things, 1st edn. apress, Berkely
85. Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T (2018) Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J Med Syst 42(7):130
86. Guajardo J, Kumar SS, Schrijen GJ, Tuyls P (2007) Fpga intrinsic pufs and their use for ip protection. In: International workshop on cryptographic hardware and embedded systems. Springer
87. Guan Z, Si G, Zhang X, Wu L, Guizani N, Du X, Ma Y (2018) Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. IEEE Commun Mag 56(7):82–88
88. Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of things (Iot): a vision, architectural elements, and future directions Future generation computer systems
89. Guin U, Asadizanjani N, Tehranipoor M (2019) Standards for hardware security. GetMobile: Mob Comput Commun 23(1):5–9
90. Guin U, Cui P, Skjellum A (2018) Ensuring proof-of-authenticity of Iot edge devices using blockchain technology. In: IEEE International conference on blockchain
91. Guin U, DiMase D, Tehranipoor M (2014) Counterfeit integrated circuits: detection, avoidance, and the challenges ahead. Journal of Electronic Testing (1)
92. Guin U, Huang K, DiMase D, Carulli J, Tehranipoor M, Makris Y (2014) Counterfeit integrated circuits: a rising threat in the global semiconductor supply chain. Proceedings of the IEEE
93. Guin U, Singh A, Alam M, Canedo J, Skjellum A (2018) A secure low-cost edge device authentication scheme for the internet of things. In: International conference on VLSI design
94. Gungor VC, Sahin D, Kocak T, Ergut S, Buccella C, Cecati C, Hancke GP (2011) Smart grid technologies: communication technologies and standards. IEEE Transactions on Industrial Informatics, pp 7
95. Guo R, Shi H, Zhao Q, Zheng D (2018) Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access
96. Gupta Y, Shorey R, Kulkarni D, Tew J (2018) The applicability of blockchain in the internet of things. pp 561–564
97. Hammi MT, Hammi B, Bellot P, Serhrouchni A (2018) Bubbles of trust: a decentralized blockchain-based authentication system for iot. Comput Secur 78:126–142
98. Han D, Kim H, Jang J (2017) Blockchain based smart door lock system. In: 2017 International conference on information and communication technology convergence (ICTC)
99. Han R, Gramoli V, Xu X (2018) Evaluating blockchains for iot. In: 2018 9Th IFIP international conference on new technologies, mobility and security (NTMS)
100. Hardjono T, Smith N (2016) Cloud-based commissioning of constrained devices using permissioned blockchains. In: Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security, pp 29–36. ACM
101. Hendricks J, Van Doorn L (2004) Secure bootstrap is not enough: Shoring up the trusted computing base
102. Huang J, Kong L, Chen G, Wu MY, Liu X, Zeng P (2019) Towards secure industrial Iot: blockchain system with credit-based consensus mechanism. IEEE Transactions on Industrial Informatics
103. Huckle S, Bhattacharya R, White M, Beloff N (2016) Internet of things, blockchain and shared economy applications. Procedia Comput Sci 98:461–466
104. Ibba S, Pinna A, Seu M, Pani FE (2017) Citysense: blockchain-oriented smart cities. In: Proceedings of the XP2017 Scientific Workshops, XP'17
105. IBM: Integrate waston IoT with blockchain. https://www.ibm.com/internet-of-things/spotlight/blockchain
106. IETF: Transmission control protocol (1981) https://tools.ietf.org/html/rfc793
107. Intel: why IoT is a top priority for retail. https://www.intel.com/content/www/us/en/internet-of-things/solution-briefs/smart-retail-solutions-top-10.html
108. Islam MN, Kundu S (2019) Enabling ic traceability via blockchain pegged to embedded puf. ACM Trans Des Autom Electron Syst (TODAES) 24(3):36
109. Jae K Tendermint: consensus without mining
110. Jia X, Feng Q, Fan T, Lei Q (2012) Rfid technology and its applications in internet of things (IoT). In: 2012 2Nd international conference on consumer electronics, communications and networks (CECNet)
111. Khan MA, Salah K (2018) Iot security: review, blockchain solutions, and open challenges. Fut Gener Comput Syst 82:395–411
112. Kim JY, Hu W, Shafagh H, Jha S (2018) Seda: Secure over-the-air code dissemination protocol for the internet of things. IEEE Transactions on Dependable and Secure Computing

113. 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)
114. Kravitz DW, Cooper J (2017) Securing user identity and transactions symbiotically: Iot meets blockchain, pp 1–6
115. Kshetri N (2017) Can blockchain strengthen the internet of things? IT Prof 19(4):68–72
116. Lamport L, Shostak RE, Pease MC (1982) The byzantine generals problem. ACM Trans. Program. Lang Syst
117. Laszka A, Dubey A, Walker M, Schmidt D (2017) Providing privacy, safety, and security in iot-based transactive energy systems using distributed ledgers. In: Proceedings of the Seventh International Conference on the Internet of Things, IoT'17
118. Lee I, Lee K (2015) The internet of things (iot): applications, investments and challenges for enterprises 58
119. Lee M, Hwang J, Yoe H (2013) Agricultural production system based on iot. In: 2013 IEEE 16Th international conference on computational science and engineering, pp 833–837
120. Lei A, Cruickshank H, Cao Y, Asuquo P, Ogah CPA, Sun Z (2017) Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal
121. Leng K, Bi Y, Jing L, Fu HC, Van Nieuwenhuyse I (2018) Research on agricultural supply chain system with double chain architecture based on blockchain technology. Futur Gener Comput Syst 86:641–649
122. Levis P, Madden S, Polastre J, Szewczyk R, Whitehouse K, Woo A, Gay D, Hill J, Welsh M, Brewer E, Culler D (2005) TinyOS: an operating system for sensor networks
123. Li W, Andreina S, Bohli JM, Karame G (2017) Securing proof-of-stake blockchain protocols. In: Garcia-Alfaro J, Navarro-arribas G, Hartenstein H, Herrera-Joancomartí J (eds) Data privacy management, cryptocurrencies and blockchain technology
124. Li X, Jiang P, Chen T, Luo X, Wen Q (2017) A survey on the security of blockchain systems. Future Generation Computer Systems
125. Li Z, Kang J, Yu R, Ye D, Deng Q, Zhang Y (2017) Consortium blockchain for secure energy trading in industrial internet of things. IEEE Transactions on Industrial Informatics
126. Liam B, William JB, Jonathan C, Owen L (2018) Applications of blockchain within healthcare. In: Blockchain in healthcare today, vol 1
127. Liang G, Weller SR, Luo F, Zhao J, Dong ZY (2018) Distributed blockchain-based data protection framework for modern power systems against cyber attacks. IEEE Transactions on Smart Grid
128. Liang X, Zhao J, Shetty S, Li D (2017) Towards data assurance and resilience in iot using blockchain. In: IEEE Military communications conference (MILCOM)
129. Liang X, Zhao J, Shetty S, Liu J, Li D (2017) Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), pp 1–5
130. Lim J, Kim Y, Yoo C (2019) Chainveri: Blockchain-based firmware verification system for iot environment. In: 2018 IEEE International conference on blockchain (blockchain-2018) (to appear in
131. Lin J, Shen Z, Zhang A, Chai Y (2018) Blockchain and iot based food traceability for smart agriculture. In: Proceedings of the 3rd International Conference on Crowd Science and Engineering. ACM, pp 3
132. Lin YP, Petway JR, Anthony J, Mukhtar H, Liao SW, Chou CF, Ho Y (2017) Blockchain: the evolutionary next step for ict e-agriculture
133. Liu B, Yu XL, Chen S, Xu X, Zhu L (2017) Blockchain based data integrity service framework for iot data. In: IEEE International conference on web services (ICWS)
134. Liu S, Wu J, Long C (2018) Iot meets blockchain: parallel distributed architecture for data storage and sharing. In: IEEE International conference on blockchain
135. Lundqvist T, de Blanche A, Andersson HRH (2017) Thing-to-thing electricity micro payments using blockchain technology. In: Global internet of things summit (GIoTS)
136. Ma M, Shi G, Li F (2019) Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the iot scenario. IEEE Access 7:34,045–34,059
137. Mazières D (2015) The stellar consensus protocol: a federated model for internet-level consensus
138. Media Q Airbnb just acquired a team of bitcoin and blockchain experts, https://qz.com/657246/airbnb-just-acquired-a-team-of-bitcoin-and-blockchain-experts/
139. Merkle RC (1988) A digital signature based on a conventional encryption function. In: A conference on the theory and applications of cryptographic techniques on advances in cryptology, CRYPTO '87
140. Mettler M (2016) Blockchain technology in healthcare: the revolution starts here. In: 2016 IEEE 18th international conference on e-health networking, applications and services (healthcom), pp 1–3
141. Micali S, Rabin M, Vadhan S (1999) Verifiable random functions. In: 40th annual symposium on foundations of computer science (cat. no.99CB37039)
142. Michael del C Ethereum executes blockchain hard fork to return dao funds. https://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-i nvestor-funds/
143. Miller D (2018) Blockchain and the internet of things in the industrial sector. IT Prof 20(3):15–18
144. Mondragon AEC, Mondragon CEC, Coronado ES (2018) Exploring the applicability of blockchain technology to enhance manufacturing supply chains in the composite materials industry. In: 2018 IEEE International conference on applied system invention (ICASI), pp 1300–1303
145. Mukhopadhyay U, Skjellum A, Hambolu O, Oakley J, Yu L, Brooks R (2016) A brief survey of cryptocurrency systems. In: 2016 14th annual conference on privacy, security and trust (PST), pp 745–752
146. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf
147. Nam T, Pardo TA (2011) Conceptualizing smart city with dimensions of technology, people, and institutions. In: Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times, dg.o '11, pp 282–291
148. Neisse R, Steri G, Nai-Fovino I (2017) A blockchain-based approach for data accountability and provenance tracking. In: Proceedings of the 12th International Conference on Availability, Reliability and Security. ACM, pp14
149. Novo O (2018) Blockchain meets iot: an architecture for scalable access management in iot. IEEE Internet J PP(99):1–1
150. Olleros FX, Zhegu M, Olleros FX, Zhegu M (2016) 11 blockchain technology: principles and applications. Edward Elgar Publishing, Incorporated
151. Ouaddah A, Kalam AAE, Ouahman AA (2016) Fairaccess: a new blockchain-based access control framework for the internet of things. Security and Communication Networks
152. Ouaddah A, Mousannif H, Elkalam AA, Ouahman AA (2017) Access control in the internet of things: big challenges and new opportunities. Computer Networks

153. Park J, Kim K (2017) Tm-coin: trustworthy management of tcb measurements in iot. pp 654–659
154. Pham HL, Tran TH, Nakashima Y (2018) A secure remote healthcare system for hospital using blockchain smart contract. In: IEEE Globecom workshops (GC wkshps). IEEE
155. Pinchen C, Ujjwal G Countering botnet of things using blockchain-based authenticity framework. To Appear
156. Pinno OJA, Gregio ARA, Bona LCED (2017) Controlchain: Blockchain as a central enabler for access control authorizations in the iot. In: GLOBECOM 2017 - 2017 IEEE Global communications conference, pp 1–6
157. Rahman MA, Rashid MM, Hossain MS, Hassanain E, Alhamid MF, Guizani M (2019) Blockchain and iot-based cognitive edge framework for sharing economy services in a smart city. IEEE Access 7:18,611–18,621
158. Rahman RA, Shah B (2016) Security analysis of iot protocols: a focus in coap. In: 2016 3Rd MEC international conference on big data and smart city (ICBDSC)
159. Rivera R, Robledo JG, Larios VM, Avalos JM (2017) How digital identity on blockchain can contribute in a smart city environment. In: 2017 International smart cities conference (ISC2), pp 1–4
160. Robertson J, Riley M (2018) The big hack: how China used a tiny chip to infiltrate u.s companies
161. Salahuddin MA, Al-Fuqaha A, Guizani M, Shuaib K, Sallabi F (2017) Softwarization of internet of things infrastructure for secure and smart healthcare. Computer 50(7):74–79
162. Samaniego M, Deters R (2017) Virtual resources & blockchain for configuration management in iot
163. Sanju S, Sankaran S, Achuthan K (2018) Energy comparison of blockchain platforms for internet of things. In: 2018 IEEE International symposium on smart electronic systems (iSES)(formerly inis). IEEE, pp 235–238
164. Sasson EB, Chiesa A, Garman C, Green M, Miers I, Tromer E, Virza M (2014) Zerocash: decentralized anonymous payments from bitcoin. In: 2014 IEEE Symposium on security and privacy (SP), vol. 00
165. Schollmeier R (2001) A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In: 2001. Proceedings. First international conference on Peer-to-peer computing. IEEE, pp 101–102
166. Schwab K (2016) The fourth industrial revolution
167. Shafagh H, Burkhalter L, Hithnawi A, Duquennoy S (2017) Towards blockchain-based auditable storage and sharing of iot data. Proceedings of the 2017 on Cloud Computing Security Workshop, pp 45–50
168. Sharma PK, Chen MY, Park JH (2018) A software defined fog node based distributed blockchain cloud architecture for iot. IEEE Access 6:115–124
169. Sharma PK, Moon SY, Park JH (2017) Block-vn: a distributed blockchain based vehicular network architecture in smart city. JIPS 13:184–195
170. Sharma PK, Park JH (2018) Blockchain based hybrid network architecture for the smart city. Fut Gener Comput Syst 86:650–655
171. Sharma PK, Rathore S, Park JH (2018) Distarch-scnet: blockchain-based distributed architecture with li-fi communication for a scalable smart city network. IEEE Consum Electron Mag 7(4):55–64
172. Sharma PK, Singh S, Jeong YS, Park JH (2017) Distblocknet: a distributed blockchains-based secure SDN architecture for iot networks. IEEE Communications Magazine
173. She W, Gu ZH, Lyu XK, Liu Q, Tian Z, Liu W (2019) Homomorphic consortium blockchain for smart home system sensitive data privacy preserving. IEEE Access
174. Shen M, Tang X, Zhu L, Du X, Guizani M (2019) Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart cities. IEEE Internet of Things Journal
175. Shrouf F, Ordieres J, Miragliotta G (2014) Smart factories in industry 4.0: a review of the concept and of energy management approached in production based on the internet of things paradigm. In: 2014 IEEE International conference on industrial engineering and engineering management
176. Sikorski JJ, Haughton J, Kraft M (2017) Blockchain technology in the chemical industry: machine-to-machine electricity market. Applied Energy
177. Sompolinsky Y, Lewenberg Y, Zohar A (2016) Spectre: A fast and scalable cryptocurrency protocol. IACR Cryptology ePrint Archive
178. Suh G, Devadas S (2007) Physical unclonable functions for device authentication and secret key generation. In: Proceedings of ACM/IEEE on design automation conference
179. Sun J, Yan J, Zhang KZK (2016) Blockchain-based sharing services: what blockchain technology can contribute to smart cities. Finan Innov 2(1):26
180. Swan M (2015) Blockchain: blueprint for a new economy, 1st edn. O'Reilly Media, Inc
181. Swanson T Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger system. http://www.ofnumbers.com/wpcontent/uploads/2015/04/Permissioned-distributed-ledgers.pdf
182. Tang B, Kang H, Fan J, Li Q, Sandhu R (2019) Iot passport: a blockchain-based trust framework for collaborative internet-of-things. In: Proceedings of the 24th ACM Symposium on Access Control Models and Technologies. ACM, pp 83–92
183. Tao F, Cheng Y, Xu L, Zhang L, Li BH (2014) Cciot-cmfg: cloud computing and internet of things-based cloud manufacturing service system. IEEE Trans Indust Inf 10(2):1435–1442
184. Tao F, Zhang L, Venkatesh VC, Luo Y, Cheng Y (2011) Cloud manufacturing: a computing and service-oriented manufacturing model. Proc Instit Mech Eng Part B: J Eng Manuf 225(10):1969–1976
185. Tasca P, Thanabalasingham T, Tessone CJ (2017) Ontology of blockchain technologies. principles of identification and classification. CoRR arXiv:1708.04872
186. Tehranipoor M, Guin U, Bhunia S (2017) Invasion of the hardware snatchers. IEEE Spectrum
187. Tehranipoor M, Guin U, Forte D (2015) Counterfeit integrated circuits: detection and avoidance. Springer, Berlin
188. Teslya N, Ryabchikov I (2017) Blockchain-based platform architecture for industrial iot, pp 321–329
189. Tian F (2016) An agri-food supply chain traceability system for China based on rfid and blockchain technology. In: 2016 13Th international conference on service systems and service management (ICSSSM)
190. Tian F (2017) A supply chain traceability system for food safety based on haccp, blockchain and internet of things. In: 2017 International conference on service systems and service management
191. Trappe W, Howard R, Moore RS (2015) Low-energy security: limits and opportunities in the internet of things. IEEE Security Privacy
192. Valerio P Borderhawk found counterfeit iot devices installed (2018). https://iot.eetimes.com/copycats-pose-a-serious-security-threat-to-the-iot/
193. Vukolić M (2015) The quest for scalable blockchain fabric: proof-of-work vs. bft replication. In: International workshop on open problems in network security. Springer, Berlin

194. Walker MA, Dubey A, Laszka A, Schmidt DC (2017) Platibart: a platform for transactive iot blockchain applications with repeatable testing. In: Proceedings of the 4th Workshop on Middleware and Applications for the Internet of Things, M4IoT '17, pp 17–22
195. Wang W, Singh A, Guin U, Chatterjee A (2018) Exploiting power supply ramp rate for calibrating cell strength in SRAM PUFs. In: IEEE Latin-american test symposium
196. Wood G Yellow paper: Ethereum: a secure decentralised generalised transaction ledger. https://github.com/ethereum/yellowpaper
197. Wright CS, Savanah S Operating system for blockchain iot devices (2019). US Patent App 16/097,497
198. Wu G, Talwar S, Johnsson K, Himayat N, Johnson KD (2011) M2m: from mobile to embedded internet. IEEE Communications Magazine 49(4):36–43
199. 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 blockchain (blockchain-2018)
200. Xu X (2012) From cloud computing to cloud manufacturing. robotics and Computer-Integrated Manufacturing
201. Xu X, Weber I, Staples M, Zhu L, Bosch J, Bass L, Pautasso C, Rimba P (2017) A taxonomy of blockchain-based systems for architecture design. In: 2017 IEEE International conference on software architecture (ICSA)
202. Xu Y, Ren J, Wang G, Zhang C, Yang J, Zhang Y (2019) A blockchain-based non-repudiation network computing service scheme for industrial iot. IEEE Transactions on Industrial Informatics
203. Yli-Huumo J, Ko D, Choi S, Park S, Smolander K (2016) Where is current research on blockchain technology?—a systematic review. PLOS ONE 11(10):1–27
204. Yuan Y, Wang FY (2016) Towards blockchain-based intelligent transportation systems. In: IEEE 19Th international conference on intelligent transportation systems (ITSC)
205. Yue X, Wang H, Jin D, Li M, Jiang W (2016) Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J Med Syst 40(10):218
206. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M (2014) Internet of things for smart cities. IEEE Internet J 1(1):22–32
207. Zhang Y, Guin U (2019) End-to-end traceability of ics in component supply chain for fighting against recycling. IEEE Transactions on Information Forensics and Security
208. 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
209. Zhang Y, Xu X, Liu A, Lu Q, Xu L, Tao F (2019) Blockchain-based trust mechanism for iot-based smart manufacturing system. IEEE Transactions on Computational Social Systems
210. Zhang Z, Cho MCY, Wang C, Hsu C, Chen C, Shieh S (2014) Iot security: ongoing challenges and research opportunities. In: 2014 IEEE 7Th international conference on service-oriented computing and applications
211. Zhang ZK, Cho MCY, Wang CW, Hsu CW, Chen CK, Shieh S (2014) Iot security: ongoing challenges and research opportunities. In: 2014 IEEE 7th international conference on service-oriented computing and applications
212. chun Zhao J, feng Zhang J, Feng Y, xin Guo J (2010) The study and application of the iot technology in agriculture. In: 2010 3Rd international conference on computer science and information technology
213. Zheng Z, Xie S, Dai H, Chen X, Wang H (2017) An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE International congress on big data (bigdata congress)
214. Zheng Z, Xie S, Dai HN, Wang H (2016) Blockchain challenges and opportunities: a survey Work Pap.–2016
215. Zhou L, Wang L, Sun Y, Lv P (2018) Beekeeper: a blockchain-based iot system with secure storage and homomorphic computation. IEEE Access 6:43,472–43,488
216. Zhu S, Li W, Li H, Tian L, Luo G, Cai Z (2018) Coin hopping attack in blockchain-based iot. IEEE Internet of Things Journal