Journal of Industrial Information Integration 15 (2019) 80–90

Contents lists available at ScienceDirect

Journal of Industrial Information Integration

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

The blockchain: State-of-the-art and research challenges

Lu Yang[a,b,c,*]

[a] University of Kentucky, Lexington, KY 40506, USA
[b] University of Manchester, Manchester M13 9PL, UK
[c] College of Charleston, Charleston, SC 29401, USA

ARTICLE INFO

Keywords:
Blockchain
Decentralization
Smart contract
Security
Privacy

ABSTRACT

The blockchain revolutionizes the creation of both scalable information technology systems and diversified applications by integrating the increasingly popular artificial intelligence, cloud computing, and big data. Various industries have recently begun to implement the exploration of blockchain. It will not take long for the blockchain to spread all over the world. In order to identify and further the development of the blockchain technology, this paper reviews the extant studies on the blockchain and its key components, blockchain-based IoT, blockchain-based security, blockchain-based data management, and the main applications based on the blockchain, and it delineates potential trends and challenges. This study provides a comprehensive overview of state-of-the-art blockchain and describes a forward-looking direction.

1. Introduction

At present, the blockchain has won numerous research recognition and public attention in the global innovation field. “The Economist” compares the blockchain with the “trust machine” and predicts that “the blockchain will redefine the world”. Similar to the next-generation information technologies, such as IoT [1], cloud computing [2], and big data [3], blockchain is a novel application model that combines the uniqueness and innovation of computing technologies, such as distributed data storage, decentralized and independent peer-to-peer transactions, automatic and intelligent consensus mechanisms, a programmable smart contract, and dynamic encryption algorithms [4–6]. According to the Gartner Report, from 2016 to 2017, the blockchain was rated as one of the highest “inflated expectations” among emerging technologies. The blockchain implements multi-party bilateral transactions in a distributed and decentralized environment, and explores the characteristics of full network record, information provenance, and tamper resistance [7,8].

In a narrow sense, a blockchain is a chained data structure that combines blocks of data and information in a chronological order and records the blocks in encrypted form as a distributed ledger that cannot be tampered with or forged. Broadly speaking, blockchain technology uses block-type data structures to validate and store data, uses distributed node consensus algorithms to generate and update data, and uses encryption to ensure data transmission and to access security. The script code contains smart contracts for programming and manipulating data in new distributed infrastructures and computing models [9–12].

The blockchain is still in the early stages of its development (Fig. 1). The first phase is the embryo phase, Blockchain 1.0 [13,14]. Cryptocurrencies are representative of this stage, and Bitcoin [15] is the most outstanding one.

In the second phase of Blockchain 2.0, the blockchain supports the creation of advanced smart contracts for achievable programs and commands [11,16], which gradually expands its application area and its scope. This phase should extend the blockchain application to different industries and should enable them to collaborate with each other. The adoption of blockchain technology not only solves the problem of trust, but it also enables more and more automated resource allocation on a global scale. Different from Blockchain 1.0, smart contract has been employed and embedded in the blockchain system to deal with the issues of mutual trust and identity among participants [17]. In particular, the Hyperledger Project is one of popular blockchain infrastructures associated with smart contract and permissioned authority.

The next generation of blockchain will be the era of programmable society with blockchain of things. The blockchain-related aspects will affect both human ideology and social form [6]. The distributed applications of artificial intelligence systems, such as Decentralized Application (Dapp), Decentralized Autonomous Organization (DAO), Decentralized Autonomous Corporation (DAC), are beginning to be seen [12,18,19] in the real world. Automation and intelligence are particularly prominent in the industry. Contemporary industry has entered a new era of Industry 4.0 [20,21]. In the near future, blockchain

* Corresponding author at: University of Kentucky, Lexington, KY 40506, USA.
E-mail address: luj@cofc.edu.

https://doi.org/10.1016/j.jii.2019.04.002
Received 1 January 2019; Received in revised form 6 April 2019; Accepted 9 April 2019
Available online 10 April 2019
2452-414X/

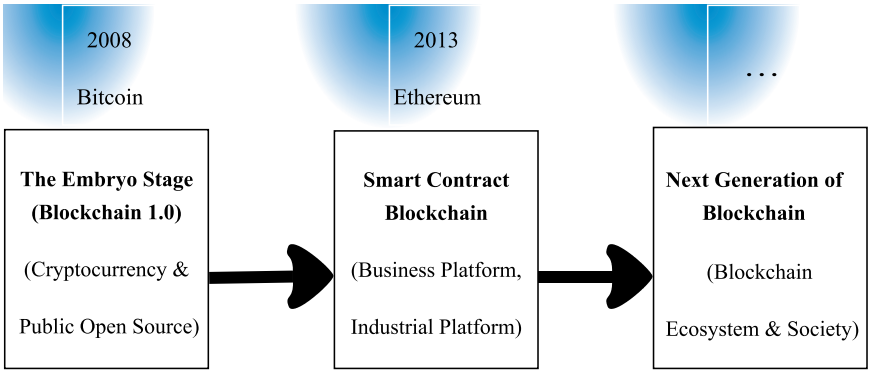

Fig. 1. The developing stages of blockchain.

technology will become a powerful tool for Industry 4.0 to use as it integrates and interoperates architectures, technologies, devices, and other related things to provide high quality products and services for society [22,23].

The blockchain has ushered in a new area of competition among different countries. The rapid development of blockchain technology has attracted widespread attention from governments, organizations, companies, and research institutions. The Canadian government has implemented a permissioned blockchain-based framework to address marijuana surveillance. The system tracks the producing process on-time, cuts regulatory costs, undermines illegal markets, and reduces crime [24]. In South Africa, the blockchain has begun to develop. Based on the comparison between Ethereum and other cryptocurrency, people are still trying to establish better modern monetary mechanisms to strengthen business and industry [25]. The global Blockchain Alliance Committee was established in Dubai,[1] and the International Organization for Standardization (ISO) constructed a dedicated Technical Committee and Standards for blockchains ISO/TC 307.[2] As the largest financial blockchain alliance organization, R3 CEV launched its first distributed general ledger application (Corda) specifically for banking and financial institutions. Big internet companies, like IBM, Microsoft, and Google, are trying to find proper blockchain-based mechanisms that will benefit business and improve infrastructure. Moreover, Stanford University (USA) launched the Center for Blockchain Research to seek fundamental changes in the way in which people and companies behave under the blockchain environment. Beijing University of Aeronautics and Astronautics (China) has established a blockchain laboratory that focuses on the development and applications of blockchains.

The paper is outlined as follows (Fig. 2). Section 1 is the introduction. Section 2 depicts an in-depth review of the foundations of the blockchain and illustrates the significance of smart contracts. The topics of blockchain-related IoT, security, and data management are described and explained in Sections 3–5, respectively. The major blockchain-based applications are discussed in Section 6. Section 7 addresses research challenges and future trends. The conclusion is in Section 8.

2. Background and current research of blockchain

In this section, we will introduce and explain the basic aspects in the blockchain such as blockchain architecture, blockchain classification, blockchain characteristics, and smart contracts in blockchain. In addition, two popular open source projects will be briefly introduced: Ethereum and Hyperledger.

2.1. Basic structure of blockchain

There is no centralized or hierarchical structure in the blockchain network. A blockchain is a decentralized system that consists of six layers: data, network, consensus, contract, service, and application. Data collection, validation, and manipulation are mainly processed within data and network layers [26–30]. Consensus and contract layers include smart contracts, consensus protocols, and incentive mechanisms [31]. Service and application layers implement blockchain-based activities into practice [10]. In Table 1, we briefly list the components or technologies associated with the six layers, respectively. As a promotion protocol, an incentive mechanism could be constructed as a separate layer [15]. The incentive layer is mainly used for various cryptocurrencies; it aims to promote resource sharing, to stimulate group intelligence, and to promote collaborative communication. In industrial practice, consortium and private blockchain platforms are set to a specific group, rather than to everyone. Thus, incentive mechanisms or mining activities are not mandatory. This change is more conducive to communications and transactions between participants in the broader blockchain systems [32]. According to the architecture, the blockchain includes three core elements: a timestamp-based chain block structure, a distributed storage mechanism based on a P2P network, and a consensus mechanism based on decentralized nodes [12].

We virtualize a scenario (a blockchain-based cloud service auction) to explain the activities of different layers in the blockchain system. In this case, the end-users are the potential buyers (bidders), and the companies or related agents are the potential sellers. Hence, the consortium blockchain architecture is an appropriate mechanism associated with the Hyperledger platform (service layer), e.g., the blockchain auction design (BA). Traditionally, an auctioneer, as an intermediary, is responsible for the auction. In the BA, there is no interruption or intervention in the transaction between the two participants. Authorized buyers and sellers submit bids and present information about cloud requirements. The data is verified and recorded in the public ledger, through which all transactions, claims, and payments are coordinated and executed (data layers). Participants are networked in a peer-to-peer mode without any third-party control (network layer). Based on a specific consensus algorithm in the BA, participants process the auctioning and contribute to the BA by sharing information and by conducting transactions (consensus layers). Appropriate algorithms and smart contracts are constructed and integrated into the BA for auction decisions (contract layer). As a regular blockchain framework, the BA can be used for other similar product or service auctions (application layers), as well [33].

2.2. Categories of blockchain

According to different applications and thresholds, blockchains are divided into three categories, public (permissionedless) chain, private (permissioned) chain, and consortium (hybrid) chain [32,34].

[1] https://www.gbbcouncil.org/. Accessed date: 08/25/2018.
[2] https://www.iso.org/committee/6266604.html. Accessed date: 08/20/2018.

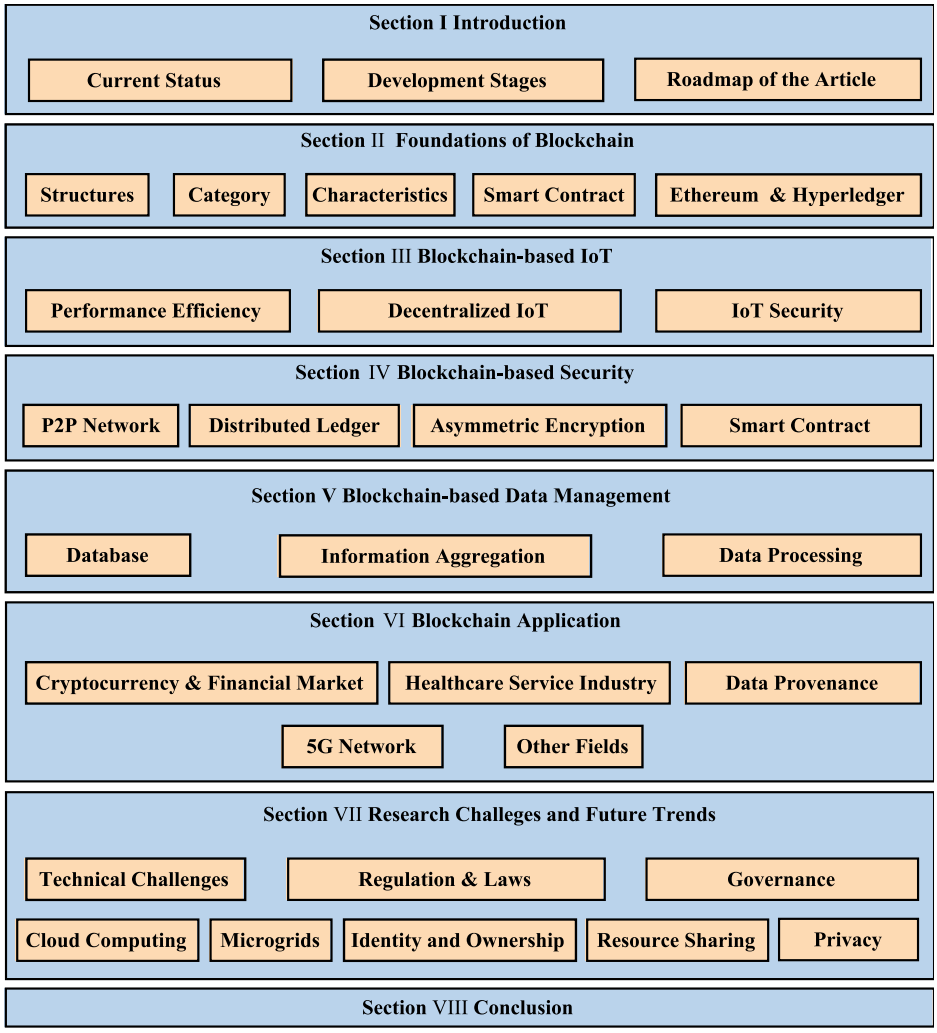

Fig. 2. Roadmap of the study.

Table 1
Introduction of six layers of blockchain.

Layers	Major technologies or components
Data layer	Data Block, chain structure, timestamp, Merkle tree, cryptography
Network layer	P2P network, verification mechanism, broadcast protocol
Consensus layer	PoW, PoS, DPoS, PBFT, …
Contract layer	Smart contract, script coding, incentive mechanism
Service layer	Ethereum, hyperledger, IBM Azure BaaS, …
Application layer	Cryptocurrency, healthcare, cloud service, …

The public (permissionedless) chain is a fully decentralized blockchain. Any node of the distributed system can participate in the reading, writing, verification, and consensus processes of the data on the chain, and can obtain corresponding economic incentives, according to the contribution. Public chains were the first to appear and are spread to many disciplines. Bitcoin is a typical public chain [35,36].

The private (permissioned) chain is a centralized blockchain. The access permission of the data on the chain is controlled by the central authority, and the read permission can be selectively opened to the public, mainly for internal data management or for the auditing of specific organizations. The private chain is not much different from other distributed storage mechanisms. The private chain is limited to specific organizations or small businesses, for a small group of entities [32,34].

The consortium (hybrid) chain is a partially distributed (multi-center) blockchain. The generation of each block is jointly determined by pre-selected nodes. Other nodes can only access the blockchain to be responsible for transactions, but do not participate in the consensus process. Through consensus agreement, multiple organizations can join together to build a consortium system for common purposes. The Hyperledger Project is a hybrid blockchain targeting business solutions [37,38].

2.3. Characteristics of blockchain

2.3.1. Decentralization

The blockchain consists of peer-to-peer blocks, each of which has the ability to record and store all transactions. Technically speaking, information is automatically shared and distributed between nodes without any third-party intervention. In this decentralized system, all participants and nodes are active to join the activities and transactions. Unlike the centralized authority of conventional mechanisms, decentralization is a distinct feature of the blockchain and attracts more attention [4,9,39].

2.3.2. Detrusting

Since blockchain technology is implemented in a decentralized system, data transfer between nodes in the network does not require mutual trust between participants. The blockchain is based on the principles of peer-to-peer network protocols and purely mathematical

methods, using decentralized structures or a partial-center structure which forms a trust relationship between network nodes and distributed system structures. The blockchain stores all of the transaction data in each block, causing the transaction to be detrusting. Trust is an important factor that plagues participants in trading. The blockchain employs a hash function and a consensus protocol to solve this problem. Participants don't need to take care of mutual trust relationships in the blockchain system. This mechanism will attract more participants to conduct more transactions [7,8].

2.3.3. Transparency

Through the blockchain, all participants share records and query data in nodes in a decentralized structure. The blockchain technology ensures that systems record and transfer data and information. Each participant can query the records in the blockchain to make the information in the distributed system transparent and consistent. Each transaction data of a distributed system is open and reliable. Each node of the same platform has the same permissions and obligations to access authorized information and allows other nodes on the same network to access this information [34,40].

2.3.4. Traceable and unforgeable

The blockchain uses timestamps to identify and to record each transaction, thereby enhancing the time dimension of the data. This allows the node to keep the order of transactions and to make the data traceable. The timestamp not only guarantees the originality of the data, but it also reduces the cost of transaction traceability. At the same time, it reinforces irreversible modifications to data or information. Once a transaction is validated and is added to the block, it will not be tampered with. Transactions need to be reviewed by most of the nodes of the system before they can be recorded. Even if an attacker has powerful computing capability, it is difficult for that attacker to evade the system and to modify the record. This can only occur when the attacker controls 51% or more of all nodes. This feature ensures that the blockchain system is stable and reliable, and solves “double spending” problems [41,39].

2.3.5. Anonymity

The blockchain encrypts data using asymmetric encryption techniques. This asymmetric encryption has two uses in blockchains: data encryption and digital signatures. Data encryption in the blockchain ensures the security of transaction data and reduces the risk of losing or falsifying transaction data. Transaction data is transmitted over the network and is digitally signed to indicate the identity of the signatory and whether the transaction has been identified. In the blockchain system, it is unnecessary to disclose the true identity of the node associated with the participant. This feature is controversial because it indirectly assists some illegal activities, such as money laundering, but at least it protects the privacy and security of the participants [42,7,16].

2.3.6. Credibility

The data exchange of the blockchain is completely dependent on self-control. It relies on each node to form a powerful calculation to defend against external attacks without human intervention. Participants can complete the transaction in a detrusting environment under conditions of complete anonymity. It protects the privacy of all of the involved parties and increases the security and credibility of the transaction. In addition, each node on the blockchain stores the complete data. As long as no more than 51% of all of the nodes in the network are occupied by hackers, the system is still secure and reliable [41,6].

Based upon the features addressed above, blockchain technology is clearly an integrated intelligent mechanism in which every single technology or protocol collaborates and interoperates with each other to form a decentralized and scalable ecosystem.

2.4. Smart contract in blockchain

A smart contract is programming language that is implemented through information technology. Smart contract appeared much earlier than blockchain technology. The concept of the smart contract is proposed by Nick Szabo.[3] A smart contract is a series of commitments defined in digital form. Smart contracts contain execution conditions and execution logic. Execution logic is automatically executed when the condition is met. From the user's point of view, a smart contract is an automatic guarantee plan. Smart contracts release or transmit the appropriate data only when certain conditions are met [16]. From a technical perspective, a smart contract is a web server. This server is not built on the Internet but is built on blockchains. Thus, specific contract programs can run on these servers [43].

Smart contracts are the core technology of Blockchain 2.0 shared ledgers. Smart contracts also have the capability of processing data, operating asset transactions, and managing smart assets [11]. Smart contracts extend the blockchain's ability to manipulate data, but, at the same time they place higher demands on the security of its users and systems [44]. Hawk is a private (permissioned) blockchain architecture that implements smart contract and compiler techniques to secure transactions in a limited group of participants who are capable of being selected and verified [45]. A smart contract-embedded protocol was proposed to validate trust in a PKI (public key infrastructure) ecosystem which will be transparent and automatic [46]. In addition, some research depicts the ability to evaluate the effectiveness, scalability, and feasibility of smart contracts. Specifically, BDD (behavior-driven development) and TDD (test-driven development) are two useful alternatives to verify and estimate the accuracy of smart contracts [47,48].

2.5. Blockchain-based open source projects

2.5.1. Ethereum platform

In December 2013, Buterin proposed the Ethereum[4] blockchain platform and a complete programming language for writing smart contracts based on built-in Ethernet digital currency transactions. Ethereum has the potential to create a decentralized world-wide computer that never stops, and that is uncensored and automatically maintained. Ethereum is an open-source blockchain platform that uses smart contracts to offer services or applications. Ethereum is designed to employ EVM language (Ethereum Virtual Machine code) to run the program, and Solidity[5] is the most widely used compiler program [49,50].

2.5.2. Hyperledger platform

Unlike Bitcoin and Ethereum, Hyperledger is an enterprise-based, distributed ledger based on blockchain technology that employs a smart contract to enforce trust between participants. Hyperledger is designed for enterprise-level blockchain applications and introduces member management services [51]. In December 2015, the Linux Foundation launched the Hyperledger Project to develop a cross-industry business blockchain platform.[6] Hyperledger is a blockchain, but it is not a cryptocurrency. In the Hyperledger system, it is unnecessary to embed cryptocurrency or mining activity. The benefit of this change in Hyperledger is the throughput of the entire system. In general, Hyperledger does not enforce specific hardware, additional software, network infrastructure, or security modules. The Hyperledger platform is a relatively suitable system that can meet the various requirements of business activities [52]. Hyperledger offers multiple blockchain

[3] Szabo, N. (1997). The idea of smart contracts. Nick Szabo's Papers and Concise Tutorials, 6.

[4] https://www.ethereum.org/. Accessed date: 08/27/2018.

[5] https://solidity.readthedocs.io/en/v0.4.25/. Accessed date: 08/25/2018.

[6] https://www.hyperledger.org/. Accessed data: 09/01/2018.

projects, such as Sawtooth, Iroha, Fabric, Burrow, Indy, Caliper, Cello, Composer, Explorer, Quilt, and the most notable project among them is Hyperledger Fabric.

3. Blockchain-based IoT

The future world will have all things connected [1,53]. Sweden Ericsson's latest research report[7] shows that in 2018, the number of sensors, devices, and machines connected to IoT will exceed the number of mobile phones, making it the largest connected device category. By 2022, nearly 18 billion of the world's 29 billion connected devices will become IoT devices. However, two challenges have hampered the development of IoT: low security and high operational and maintenance costs. The blockchain is able to communicate with diverse IoT-related devices and to motivate the intelligent architecture to perform more efficiently and safely [54,5].

3.1. Performance efficiency

IoT is a network system that connects things based on the internet, and establishes information sharing and exchange. The destination of IoT is to achieve convenience, efficiency, and intelligence. The establishment of IoT is based on infrastructure and high-end technology [55]. The security model based on closed source code can no longer adapt to the development of technology, and open source technology (as a new mode) can promote the development of IoT [28]. The open source system is not vulnerable to government intervention or other targeted attacks. Thus, open source systems offer benefits in the IoT of home automation, as well as for automotive and other devices. When the profits of IoT cannot meet market expectations, the cost of IoT will seem too high. Existing IoT solutions are not working very efficiently, and the maintenance costs of the central cloud and of large servers are also very expensive. Blockchain technology can reduce these high costs through its advantages and technical features [30].

The existing centralized management architecture of IoT has security risks [56]. By using blockchain and smart contracts, IoT will provide a safer, more dynamic solution [1]. Specifically, P2P data transactions between millions of IoT-related devices will be more secure and private [57]. As pointed out by [5], blockchain technology enhanced data dispersion, encryption, and punctuality.

When blockchain technology is applied to IoT, all of the involved nodes need to participate. Although there are many IoT terminals, the number of IoT devices with computing power is very limited. The consensus mechanism is a mechanism by which blockchain nodes reach consensus on the entire network. It ensures that the most recent block is accurately added to the blockchain, keeping the blockchain information stored consistently by the node. The consensus mechanism solves the problem of blockchain consistency and efficiency in distributed scenarios. There are more than ten types of consensus mechanisms that are employed on blockchain platforms, and PoW is an outstanding mechanism for blockchain platforms [35,58,59,60].

In addition, IoT-related devices can be protected because consensus protocols and smart contracts can build permission and communication prototypes. The blockchain-based platform, the BaaS (blockchain as a service) management system, provides us with on-demand cloud infrastructure manufacturing, intelligent diagnostics and machine maintenance, traceability, product certification, customer-to-machine and machine-to-machine transactions, and asset registration. Meanwhile, BaaS saves energy and costs and prevents denial of service (DoS) attacks [57,61].

[7] https://www.ericsson.com/en/mobility-report/internet-of-things-forecast. Accessed date: 07/23/2018.

3.2. Blockchain-based IoT security

Due to the topology and resource constraints of IoT, traditional security technologies and methods are not fully applicable to IoT architecture [62,63]. The decentralization and data encryption of blockchain technology are particularly well-suited for building distributed security systems. Blockchain improves the security of IoT. The decentralization of the blockchain provides a secure environment for IoT and forms a truly distributed system. Trust and smart contracts enhance trust mechanisms in IoT and reduce potential costs. Time series data and data encryption ensure data security in IoT [64].

In the future, the blockchain will increasingly be combined with big data, cloud computing, IoT, mobile Internet and other technologies. Blockchain-based systems also face many other security challenges in their operations and maintenance processes, and need to adopt other related technologies to deal with them [65], for example: key management technology, ciphertext access control technology, anti-DDoS attack technology, etc. [63].

4. Blockchain-based security

Assuming that an attacker in the network intends to plunder a cryptocurrency or double spend a crypto graphical coin, the block that the attacker generates must be written in the long-term blockchain ledger. However, other verified nodes in the network will not accept blocks created by the attacker. If the attacker cannot generate or mine blocks faster than other verified nodes, the attacker's block will be abandoned. When an attacker has more than 50% of the overall computing power, the attacker can easily merge the created blocks into a long-term blockchain and threaten the blockchain system. However, it is very difficult for an attacker to obtain more than 50% computing power from technical perspective [66].

Blockchain technology is generally considered to integrate the following key technologies: P2P network, distributed ledger, asymmetric encryption, and smart contract. These technologies make blockchain technology a new generation of information processing technology that is secure, reliable, open, fair, efficient, and intelligent. Specifically, safety is the top priority. Without a guaranteed secure platform, the blockchain cannot be popularized.

4.1. P2P network

Compared with the traditional client/server mode information system, the blockchain adopts a P2P network structure with decentralized, fault-tolerant, privacy protection, and load balancing. According to the design and network architecture, P2P networks are divided into three types: hybrid P2P, unstructured P2P, and structured P2P [4]. Studies have shown that real networks have the characteristics of a small-world model: the average length of the feature path is small, and the aggregation coefficient is large [67]. The blockchain network can be designed and operated according to a small-world model. The nodes are categorized into a series of non-recording nodes and a series of candidate recording nodes according to whether a node is selected for recording. The small-world model can dynamically ensure the stability of the entire network under the condition of node changes (adding, exiting, or changing), as well as the robustness of the blockchain network and the integrity and consistency of the transaction data [68,69].

4.2. Distributed ledger

Traditional databases provide basic operations for adding, deleting, changing, and querying data. However, in the blockchain, there are only two operations: adding and querying. Traditional databases are divided into centralized databases and distributed databases. A distributed database distributes the data in the original centralized

database to multiple data storage nodes connected through the network for greater storage capacity and higher concurrent access. The blockchain is a distributed ledger technology with different storage methods and data structures from the traditional distributed technology. In this way, blockchain technology realizes the data provenance, thus ensuring the authenticity and security of the data [70,7].

4.3. Asymmetric encryption

Asymmetric encryption is the basic technology used to ensure the security of blockchain. Asymmetric encryption consists of two keys: a public key and a private key [46]. Asymmetric encryption has two uses in blockchains: data encryption and digital signatures [39]. Through the in-depth study of blockchain technology and the need for blockchain applications, asymmetric cryptography is not only used for transaction signature and verification, but also for encrypting data recorded in blockchains. Multi-signature technology is a useful tool [71]. An important mechanism of the blockchain is that the data recorded in the block needs to be verified by other nodes. But, since some information should not be disclosed, we can use blind signature technology to fulfill this requirement and can achieve the privacy and security goals.

4.4. Smart contract

From a security perspective, the characteristics of smart contracts are the same as those of blockchain data: distributed, authenticated, consistent, and non-tampered. And, smart contracts are also used as a guarantee for security as technical means [45]. In the smart contract, the rights and obligations of the participants, the trigger conditions for the execution of the contract, and the corresponding results are specified. Once a smart contract is added to the blockchain, it can be executed objectively and accurately, without any impact. After providing a secure blockchain environment, the security of smart contracts is highly dependent on the contract code. If there is a problem with the implementation logic in the contract code, it will seriously affect the security of the blockchain. A more effective solution is to provide a smart contract template. Smart contract templates have been professionally reviewed and tested for verification. Users only need to fill in the relevant input data when using the smart contract template [72].

5. Blockchain-based data management

From the data management perspective, the blockchain is a database system built on a peer-to-peer network that provides trusted data management capabilities. The trusted database management system ensures the credibility of the system at three levels, the reliability of the storage, the credibility of the processing, and the credibility of the external access [36,3].

The premise of sharing information and resources is the accumulation of information, that is, the storage and organization of information through some methods and technologies [73]. In the decentralized environment, all information and resources are allocated to each node and are not accumulated to form an information resource center. The blockchain implements the ledger and chain structure in linking data. Hence, the key to realizing information aggregation is to solve the problem of information storage.

Depending on whether or not the information resources are stored directly in the block, the information aggregation is categorized into two ways: (1) The information resource chain mode. Information is stored directly in the block, and information and resource are collected in the blockchain. (2) The information resource index chain mode. Only the information index is stored in the block, and the information and resources are stored in the local server, such as cloud. Information and resource are collected outside the blockchain [16,74].

The blockchain on the peer-to-peer network realizes the accumulation of information through the linked blocks, and constructs the sharing of information and resources through the copy of the blockchain. The blockchain itself has the dual functions of information accumulation and sharing. Therefore, the information and resources sharing on the blockchain is consistent with the blockchain network construction and scale expansion. Expansion of the blockchain network can be used to achieve a wider sharing of information and resources. More devices and individuals can join the blockchain network and can share more information and resources [4].

The purpose of data management is to keep data as confidential, integrity-driven, and available as possible, whether the data is from an IoT system, a cloud framework, or another channel [36]. The tradeoff between preserving privacy and enhancing transparency is something that we need to consider. For instance, in a blockchain-based data sharing framework, the owner has full control of the data. How to release the authority to other users and still secure the information is the alternative that the decentralized cloud storage system seeks to fulfill by smart contract and cryptographical keys [75]. In an IoT network, data is malicious and dynamic. The blockchain technology is an effective tool to enhance data integrity and identity verification, and it provides users with more reliable and consistent data in the cloud environment [76]. A medical data sharing system, MeDShare, monitors custodians and authenticates owners to access and manage data from cloud providers [77]. The blockchain improves the performance of MeDShare regarding security and permission without trust or intervention. Moreover, the blockchain is also a powerful instrument that improves the performance of government information resource sharing. The P2P decentralized data sharing system promotes sharing efficiency and reduces potential data-related costs [78].

Additionally, the blockchain network collects a huge amount of data. The blockchain can harness appropriate mechanisms protecting data to a higher-level security [74]. A data management system, proposed by [79], seeks to secure personal data. The blockchain and protocol from an automatic access-control manager to supervise anonymous transacting peers.

6. Major blockchain-based applications

The efficiency performance and the cost reduction brought by the blockchain provide new ideas for economic prosperity and social development. Individual users can trade electronically, share resources fairly, and create value intelligently. Using blockchain technology, users can record data and information on a decentralized platform using unforgeable ledgers. A digital encryption can ensure data security and individual privacy. Its industry application advantages are to optimize business processes, to reduce operating costs, and to increase synergies. These advantages are reflected in the fields of cryptocurrency and finance markets, the healthcare industry, data provenance, 5G, and other fields.

6.1. Using blockchain in cryptocurrency and financial markets

Cryptocurrencies, such as Bitcoin, are the most popular application scenarios for the blockchain technology. As of now, the market value of the global digital cryptocurrency market exceeds 200 billion US dollars, and Bitcoin is called “digital gold” [27]. One Bitcoin current price reaches more than 6300 US dollars and takes up more than half of the total market value of cryptocurrencies.[8] Meanwhile, as a basic technology, the blockchain provides anonymity and privacy as a customer or market's request, while guaranteeing security. The gradual increase of cross-border capital flow is bothering the financial regulation of the central bank and is impacting the traditional banking system [7]. The booming of Bitcoin has quickly attracted public attention, since the

[8] https://coinmarketcap.com/. Accessed date: 09/19/2018.

blockchain technology has potential to improve integrity, security, and authenticity through appropriate frameworks that are widely used in practice, such as charity and fundraising, taxi service, insurance, pet care, diamond manufacturing, etc. [27,80]. Cryptocurrency is different from conventional currency. Its value is related to the market and it is not controlled by the monetary authorities. In the financial market, as a new financial tool and investment method, blockchain-based cryptocurrency has attracted the attention of many speculators [81,82].

Blockchain is an effective tool for solving the issues of the financial industry. For example: (1) The reconciliation and settlement costs between financial institutions are very high and there exist many complex processes. (2) In the securities market, the transaction process takes a long time with high costs. (3) Assets Management is primarily managed by intermediaries, which increases transaction costs and the risk of counterfeiting. (4) User identification. User data between different financial institutions is difficult to interact effectively. (5) In the case of cross-border transactions, both parties often have insufficient trust and need for intermediary guarantees. The blockchain is able to establish the precise, timely and multifaceted supervision. For instance, point-to-point value transfer, distributed technologies and digital assets, establishing mechanisms through smart contracts to ensure compliance with contracts, digital identity recognition [27,80].

6.2. Using blockchain in the healthcare service industry

The application of blockchain technology in the medical field has been developed to some extent. For instance, it is used in a personal health database and information sharing center, in a smart medical assistance platform, and in a deep analysis of the challenges faced by blockchain technology in the medical field [83,84]. The electronic health record (EHR) is a digital record of patients, and includes basic information, medical history records, test results, treatment records, drug descriptions, and diagnostic effects [85]. The blockchain allows medical institutions, patients, and other related parties to access electronic health data across different platforms [86,87]: HDG [88], MedRec [89], PSN [90], and BBDS [91]. The decentralized structure of the blockchain securely collects the stored data and enables medical data to be updated in real time on each network node. Persistent storage on cloud servers reduces the risk of loss of medical data and/or sensitive information, and increases the security and the reliability of medical information. For individuals, health data and medical records are used to check an individual's health status, and the system automatically assesses their health status based on their medical data and rates a personal health condition [92]. For doctors, they can use a health database allows for faster understanding of patient contraindications and instrument diagnostics. For hospitals and medical research institutions, the medical database is for big data analysis and mining, and reasonable monitoring of medical orders, drugs, and so on. The embedded smart contracts in the blockchain can form medical contracts and vouchers to build an intelligent medical management system [93].

6.3. Using blockchain in data provenance

Similar to database logging, the blockchain maintains a collection of all operations and processes on the ledgers. However, the data query and analysis processing functions provided by the blockchain are relatively simple. As a trusted data management system, data provenance on blockchains is an important issue. Data provenance refers to the management of data processing and addresses the status and the source of the data [70]. Data provenance is conducted in the context of scientific data management, data warehousing, and data asset management [74]. Smart contract and blockchain technology, applied to digital assets, can implement data provenance and can verify the authenticity and ownership of the asset. Product traceability is one type of data provenance [94,95]. Traditional methods primarily use unique identifiers (RFID or QR codes) to correlate product-related information for product traceability and authenticity queries. Blockchain technology can be constructed to form a multi-participating traceability chain. Participants are production companies, logistics, distributors, retailers, and quality supervisors. Just like the blockchain, the tracing system is open, transparent, and unforged. By integrating online and offline synchronization, information is written to the blockchain. Based on data collected in real time, participants can keep abreast of the production, transportation and sales of the products in order to take countermeasures and strengthen multi-party cooperation [73].

6.4. Using blockchain in 5G network

The next generation mobile communication network, 5G, will coordinate heterogeneous devices and applications to improve energy efficiency, network capacity, and resource accessibility [96]. How to allocate slices dynamically between participants, such as mobile virtual network operators, over-the-top providers, and industry vertical market players, regarding their different needs, is not an easy task to deal with [96]. The blockchain and smart contracts construct a business model to collaborate industrial automation processes and the related manufacturing equipment to achieve efficient operations. A network slice broker is a potential resource allocation facility in the 5G manufacturing environment. The blockchain-based cloud radio over optical fiber network (C-RoFN) is a good attempt to adopt an anonymous access identification mechanism to cut the network operating and connecting costs and to make common agreements among the parties mentioned above [97].

6.5. Using blockchain in other fields

For a specific electric vehicle, a blockchain-based billing system tracks the charging records accurately and instantly and prevents individual's modification on the records [98]. A blockchain-based lottery framework maintains transparency and fairness among participants [99]. As a database, the blockchain securely records the watermark data and authenticates the multiple copyrights chronologically by timestamp. Also, the blockchain technology is suitable for the insurance industry, in that it supports various processes among peers for time-saving and information security [100]. To address security and identity issues, maritime management uses blockchains to collaborate with traditional systems and methods [101]. In addition, since the blockchain is a decentralized, secure, transparent and scalable platform, it will furnish the development of the future energy internet [102].

7. Research challenges and future trends

The blockchain has been developing for only about ten years, since the initiation of Bitcoin. There are still many technical difficulties, such as consensus mechanisms, storage and data management, and chain structures, as well as research challenges such as regulation and governance. In this section, we will focus on blockchain-related challenges and potential directions.

7.1. Technical challenges

The blockchain is not a simple combination of one or more technologies, but the integration of multiple technologies. These techniques are constructed in new structures to create new ways to record, to store, and to express data. The following three aspects have potential to improve the blockchain system from a technical perspective.

7.1.1. Consensus mechanism

In the practical transaction, the blockchain consensus protocol consumes a large amount of computing resources and power, leading to low-system throughput and long-system latency [35]. However, the blockchain requires higher operational and more compatible

capabilities for the existing platforms. Designing an interaction mechanism to aggregate and to utilize the group intelligence of distributed consensus nodes is an important issue that the blockchain needs to deal with. Although the foundation of blockchain technology is relatively mature, there are still many problems to be solved in protocol improvements. The target is how to construct the consensus mechanisms to improve system throughput. For example, the consensus algorithm of main nodes selection from a few trusted nodes, the asynchronous consensus algorithm of increasing the probability of high correctness, the consensus algorithm of reduction of network broadcasts based on specific security premise, the consensus algorithm based on trusted hardware, and the consensus algorithm combining the advantages of PoW and PBFT [58–60]. Until now, we have a number of protocols specific to the standards and features of different blockchain platforms. The research on consensus mechanisms has been compared and analyzed from different angles. The common goal is to seek better protocols that can achieve higher levels of energy and cost saving, tolerated power of adversary, identity and execution, scalability, security and privacy, etc. [32].

7.1.2. Scalability and capacity

The blockchain requires each node in the system to maintain a backup of the data, which is unrealistic for the growing mass data storage [32]. Although lightweight verification nodes can solve the problem to some extent, there is still a need to research and to design more effective industrial solutions. In a blockchain system, each network node stores all of the historical transaction data. While this guarantees data openness, transparency, and high availability, it also brings data privacy and performance issues. A single node cannot store data indefinitely. The rapid growth of transaction volume and data volume bring the potential to solve the issue of scalability through two ways: by expanding the blockchain storage or by restructuring the blockchain [103].

7.1.3. Chain structures

The single-chain design of the blockchain platform limits the overall processing power of the system to a single compute node. Other potential chain structures are multi-chain, side-chain, and cross-chain. The multi-chain design scheme realizes segmentation storage and the concurrent execution of unrelated transactions [104,105]. This case not only improves the scalability of the system, but it also enhances the entire network not to be limited to a single node. Also, the inter-chain isolation ensures the privacy of the transaction data. Sidechain is a blockchain technology that enables digital asset transactions by anchoring bitcoin. It primarily addresses the single application and limited performance of the Bitcoin platform. The side chain is an independent blockchain, with its own ledgers, consensus mechanisms, transaction types, and smart contracts [10]. By creating a separate sidechain for each application that is anchored to the main chain, the blockchain can be extended to support multiple applications. Multi-chain and side-chain can solve the problems and deficiencies of existing blockchains. In addition, in the face of many different types of blockchain platforms, cross-chain technology can achieve interoperability and can lead mutual trust to higher levels [106].

7.2. Regulation and laws

Although the blockchain has changed society in many aspects, it has also challenged legal and law systems. Especially in its early stage of development, due to the uniqueness of the blockchain technology and the lag of legal supervision, it triggered a series of legal issues [18]. A comprehensive understanding of the characteristics of the blockchain helps to establish and to improve laws and regulations related to the blockchain activities. Many countries are actively deploying blockchain technology and are improving regulatory measures, e.g., decentralization and legal application and jurisdiction issues, anonymization and internet real name issues, reliability and deletion rights issues, as well as transparency and personal data privacy issues. Moreover, in the field of national governance and social governance, technology and law are mutual substitutes [107]. If the cost of a technology solution is lower than the legal solution in a social scenario, then the technical tool can replace the legal form as the primary means of order generation. Distributed verifiable databases and smart contracts facilitated by blockchain technology have the potential to change technical and legal boundaries and to form new governance models. But technology solutions can also raise the level of the efficiency and the certainty of the law, such as equality and justice [108]. How to absorb the institutional innovation brought on by technology, while avoiding the social physics position that technology determines everything and protecting the legal value will become an important factor determining the virtuous circle of blockchain technology [108,109].

7.3. Governance

On the one hand, the blockchain has broad application prospects in governance and services, and it can be seen in the transformation of government roles and functions, the flattening of government organizational structures, the transparency of governance and service processes, the performance of government innovation, the security of government data, and the establishment of smart and trustworthy governments [110,111]. On the other hand, blockchain technology poses many challenges to the government's conventional functions, management mechanisms, laws, and regulations [110,111]. Once again, the blockchain is a decentralized system with no third-party intervention. The government is a centralized authority with management and control. How to stimulate the greater role of the blockchain under the overall management of the government is a sensitive issue that needs urgent resolution. Meantime, for the government itself, the blockchain also provides a broader space for its development [112].

7.4. Research trends

7.4.1. Cloud computing

Similar to blockchain technology, cloud computing is essentially a service and a product of integrating computer technology and network technology, such as distributed computing, parallel computing, network storage, virtualization, and load balancing [2]. The interoperation of the blockchain and cloud computing provides infrastructure support for the application of blockchain technology and reduces the time and labor costs of platform deployment. Blockchain as a service is the platform that adopts cloud computing to implement blockchain-based applications to different industries and services [113,114].

7.4.2. Microgrids

Electricity trading includes energy trading, transmission rights trading, and ancillary services trading. Microgrid as an effective means of accessing distributed power sources in smart grids; the microgrid can effectively integrate various distributed energy sources, increase the penetration rate of renewable energy, and make up for the defects of power grid concentration [115]. The blockchain provides new ideas and methods for the development of microgrids. The blockchain is used as the underlying architecture to construct the power trading system and distribution system as well as the microgrid database that participants can used to share the information [116]. In addition, various smart contracts have been established for the microgrid, such as power purchase contracts, transmission contracts, and payment settlement contracts [117,118].

7.4.3. Identity and ownership management

Identity management is a potential market. Identity management has a high industry threshold due to the privacy and sensitivity of the data. From the perspective of identity information, there are still many

problems in obtaining information: (1) insufficient data, (2) poor data correlation, and (3) out-of-date or faked data. Ownership management is mainly used for the management and traceability of property rights and copyrights, including cars, houses, art, digital publications, etc. Ownership management has several major problems: (1) product verification and management ownership, (2) transaction security and reliability, and (3) privacy protection. Using blockchain technology, ownership can be written on the blockchain and no one can modify it. Once the contract is made, the blockchain will ensure accurate contract execution and track asset ownership. The blockchain confirms the ownership through timestamps and hashing algorithms, and proves the existence, authenticity and uniqueness of valuations such as text, video, and audio, and provides digital proofs that cannot be tampered with. Once ownership is verified, the records are stored in the common ledger to protect the uniqueness of ownership [119–122].

7.4.4. Resource sharing

The main challenges of resource sharing include: (1) high costs, (2) user identity ratings, and (3) shared service management. Blockchain-based platform makes it easy to implement a low-cost, reliable trading system. For data sharing, the questions are how to assess the value of the data, how to trade and exchange the data, and how to prevent the data. The common ledger formed by the blockchain tracks and manages the data flow between multiple parties in real time, and effectively reduces the management cost of the data sharing process by controlling access rights. It is possible to construct a consolidated energy sharing system. Blockchain can be applied to the energy associated network. Its advantages include: (1) no central organization for scheduling control, (2) universal cross-energy system for energy system information, (3) data confidentiality and reliability, 4) a decentralized energy trading system associated with multi-signature and anonymous encrypted information enables peers to anonymously negotiate energy prices and ensure transaction security, and 5) Solving accurate measurement problems, interaction problems, Self-discipline control, and optimization decisions [123–125].

7.4.5. Privacy protection

With the rapid development of ICT, privacy issues have received increasing attention, such as medical data and financial data. Issues involving important personal privacy need to be protected from major losses. Blockchain security and trust mechanisms make blockchain and privacy protection a good combination, enabling to effectively manage data transparency and access rights. Cryptocurrency is treated as an incentive to increase anonymity in a secure and fair transaction process and to protect against attacks, such as anti-DoS and Sybil attacks. The distributed hashing algorithms are employed to encrypt data and ensure availability and scalability through a smart contract. The blockchain solves the problem of controlling personal and sensitive data without third-party intervention and calculation and analysis based on the original data but without disclosing it [8,126,127].

8. Conclusion

The blockchain embeds many computing skills and algorithms, such as consensus protocols, distributed ledgers, timestamps, the Merkle Tree, and digital cryptographical keys. As a decentralized architecture, the blockchain integrates many advanced technologies, such as, IoT, cloud computing, and data mining. The blockchain technology provides us with a decentralized system without third-party intervention. The application of the blockchain expands from Bitcoin to other disciplines. It is potential that the world will become a more blockchain-based ecosystem.

The blockchain is featured as distributed storage, time series data, data untampered, decentralization, smart contracts, high security and trust. The emergence of the blockchain is a phenomenon of information and knowledge. Blockchain research is the process of informationization and standardization. In this paper, we have reviewed the blockchain and the related important aspects, especially the state-of-the-art of the blockchain, three important blockchain-based issues (IoT, security, and data), and blockchain applications in the industry, as well as its potential challenges and future directions.

Declaration of interest

None.

References

[1] L. Xu, W. He, S. Li, Internet of Things in industries: a survey, IEEE Trans. Ind. Inf. 10 (4) (2014) 2233–2243.
[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, A view of cloud computing, Commun. ACM 53 (4) (2010) 50–58.
[3] L. Xu, L. Duan, Big data for cyber physical systems in Industry 4.0: a survey, Enterp. Inf. Syst. 13 (2) (2019) 148–169.
[4] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman, Blockchain technology: beyond bitcoin, Appl. Innov. 2 (2016) 6–10.
[5] M. Conoscenti, A. Vetrò, J.C. De Martin, Blockchain for the Internet of Things: a systematic literature review, Proceedings of the IEEE/ACS International Conference of Computer Systems and Applications (AICCSA), 2017, pp. 1–6 [Online]. Available: http://ieeexplore.ieee.org/document/7945805/.
[6] Y. Lu, Blockchain and the related issues: a review of current research topics, J. Manag. Anal. 5 (4) (2018) 231–255.
[7] A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, Princeton, NJ, USA, 2016.
[8] Y. Lu, Blockchain: a survey on functions, applications and open issues, J. Ind. Integr. Manag. 3 (4) (2018) 1850015published online.
[9] K. Croman, et al., On scaling decentralized blockchains, Proceedings of the 3rd Workshop Bitcoin Blockchain Research, 2016, pp. 106–125.
[10] M. Pilkington, Blockchain technology: principles and applications, Handbook of Research on Digital Transformations, Edward Elgar Publishing, Cheltenham, UK, Northampton, MA, USA, 2016, pp. 225–265 Chapter 11.
[11] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, Proceedings of the 23rd ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 254–269.
[12] Y. Yuan, F.Y. Wang, Blockchain and cryptocurrencies: model, techniques, and applications, IEEE Trans. Syst. Man Cybern. Syst. 48 (9) (2018) 1421–1428.
[13] M. Swan, Blockchain: Blueprint for A New Economy, O'Reilly Media, Inc., Sebastopol, CA, USA, 2015 Beijing, Cambridge, Tokyo.
[14] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, V. Santamaría, To blockchain or not to blockchain: that is the question, IT Prof. 20 (2) (2018) 62–74.
[15] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.
[16] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the Internet of Things, IEEE Access 4 (2016) 2292–2303.
[17] H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, J. Xing, Hyperconnected network: a decentralized trusted computing and networking paradigm, IEEE Netw. 32 (1) (2018) 112–117.
[18] Y. Lu, Artificial intelligence: a survey on evolution, models, applications and future trends, J. Manag. Anal. 6 (1) (2019) 1–29.
[19] F. Wessling, C. Ehmke, M. Hesenius, V. Gruhn, How much blockchain do you need? Towards a concept for building hybrid DApp architectures, Proceedings of the 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), IEEE, 2018, pp. 44–47.
[20] L. Xu, E. Xu, L. Li, Industry 4, state of the art and future trends, Int. J. Prod. Res. 56 (8) (2018) 2941–2962.
[21] Y. Lu, Industry 4.0: a survey on technologies, applications and open research issues, J. Ind. Inform. Integr. 6 (2017) 1–10.
[22] W. He, L. Xu, Integration of distributed enterprise applications: a survey, IEEE Trans. Ind. Inform. 10 (1) (2014) 35–42.
[23] L. Li, China's manufacturing locus in 2025: with a comparison of "Made-in-China 2025" and "Industry 4.0", Technol. Forecast. Soc. Change 135 (2018) 66–74.
[24] B. Abelseth, Blockchain tracking and cannabis regulation: developing a permissioned blockchain network to track Canada's cannabis supply chain, Dalhous. J. Interdiscip. Manag. 14 (2018) Available: https://ojs.library.dal.ca/djim/article/view/7869.
[25] L. Butgereit, C. Martinus, A comparison of two blockchain architectures for inspiring corporate excellence in South Africa, Proceedings of the Conference on Information Communication Technology and Society (ICTAS), IEEE, Mar. 2017, pp. 1–6.
[26] R.C. Merkle, Protocols for public key cryptosystems, Proceedings of the Security and Privacy, IEEE, 1980122-122.
[27] F. Tschorsch, B. Scheuermann, Bitcoin and beyond: a technical survey on decentralized digital currencies, IEEE Commun. Surv. Tutor. 18 (3) (2016) 2084–2123.
[28] O. Alphand, et al., IoT Chain: a blockchain security architecture for the Internet of Things, Proceedings of the Wireless Communications and Networking Conference (WCNC), IEEE, 2018, pp. 1–6.

[29] H. Orman, Blockchain: the emperors new PKI? IEEE Int. Comput. 22 (2) (2018) 23–28.
[30] A.M. Saghiri, et al., A Framework for cognitive internet of things based on blockchain, Proceedings of the 4th International Conference on Web Research (ICWR), IEEE, 2018, pp. 138–143.
[31] I. Eyal, E.G. Sirer, Majority is not enough: Bitcoin mining is vulnerable, Commun. ACM 61 (7) (2018) 95–102.
[32] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: architecture, consensus, and future trends, Proceedings of the IEEE International Congress on Big Data (BigData Congr.), 2017, pp. 557–564 [Online]. Available: http://ieeexplore.ieee.org/document/8029379/.
[33] Y. Lu, X. Zheng, Block chain based double auction design, Proceedings of the American Conference of Information Systems (AMCIS), SCUIT, 2018 [Online]. Available: https://aisel.aisnet.org/amcis2018/StrategicIT/Presentations/10/.
[34] I.C. Lin, T.C. Liao, A survey of blockchain security issues and challenges, Int. J. Netw. Secur. 19 (5) (2017) 653–659.
[35] L.S. Sankar, M. Sindhu, M. Sethumadhavan, Survey of consensus protocols on blockchain applications, Proceedings of the 4th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, 2017, pp. 1–5.
[36] T.T.A. Dinh, R. Liu, M. Zhang, G. Chen, B.C. Ooi, J. Wang, Untangling blockchain: a data processing view of blockchain systems, IEEE Trans. Knowl. Data Eng. 30 (7) (2018) 1366–1385.
[37] K.L. Brousmiche, T. Heno, C. Poulain, A. Dalmieres, E.B. Hamida, Digitizing, securing and sharing vehicles life-cycle over a consortium blockchain: lessons learned, Proceedings of the 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE, 2018, pp. 1–5.
[38] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, Z Wang, Consortium blockchain-based malware detection in mobile devices, IEEE Access 6 (2018) 12118–12128.
[39] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where is current research on blockchain technology?—a systematic review, PLoS One 11 (10) (2016) e0163477[Online]. Available: https://J.s.plos.org/plosone/article?id=10.1371/J..pone.0163477.
[40] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J.A. Kroll, E.W. Felten, Sok: research perspectives and challenges for bitcoin and cryptocurrencies, Proceedings of the IEEE Symposium on Security and Privacy (SP), IEEE, 2015, pp. 104–121.
[41] G.O. Karame, E. Androulaki, S. Capkun, Double-spending fast payments in bitcoin, Proceedings of the 2012 ACM Conference on Computer and Communications Security ACM, 2012, pp. 906–917.
[42] F. Reid, M. Harrigan, An analysis of anonymity in the bitcoin system, Security and Privacy in Social Networks, Springer, New York, 2013, pp. 197–223.
[43] L. Yu, W.T. Tsai, G. Li, Y. Yao, C. Hu, E. Deng, Smart-contract execution with concurrent block building, Proceedings of the 11th IEEE Symposium on Service-Oriented System Engineering (SOSE), IEEE, 2017, pp. 160–167.
[44] K. Delmolino, M. Arnett, A. Kosba, A. Miller, E. Shi, Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab, Proceedings of the International Conference on Financial Cryptography and Data Security, Springer, Berlin, Heidelberg, 2016, pp. 79–94.
[45] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: the blockchain model of cryptography and privacy-preserving smart contracts, (2015) Cryptology ePrint Archive, Tech. Rep.[Online]. Available: http://eprint.iacr.org/2015/675.pdf.
[46] A. Buldas, R. Laanoja, A. Truu, Keyless signature infrastructure and PKI: hash-tree signatures in pre-and post-quantum world, Int. J. Serv. Technol. Manag. 23 (1-2) (2017) 117–130.
[47] Z. Gao, L. Xu, L. Chen, N. Shah, Y. Lu, W. Shi, Scalable blockchain based smart contract execution, Proceedings of the 23rd International Conference on Parallel and Distributed Systems (ICPADS), IEEE, 2017, pp. 352–359.
[48] C.F. Liao, C.J. Cheng, K. Chen, C.H. Lai, T. Chiu, C. Wu-Lee, Toward a service platform for developing smart contracts on blockchain in BDD and TDD styles, Proceedings of the 10th International Conference on Service-Oriented Computing and Applications (SOCA), IEEE, 2017, pp. 133–140.
[49] G. Wood, Ethereum: a secure decentralised generalised transaction ledger, Ethereum Project Yellow Paper. (2014) [Online]. Available: https://pdfs.semanticscholar.org/ac15/ea808ef3b17ad754f91d3a00fedc8f96b929.pdf.
[50] C. Chen, J. Wang, F. Qiu, D. Zhao, 'Resilient distribution system by microgrids formation after natural disasters, IEEE Trans. Smart Grid 7 (2) (2016) 958–966.
[51] C. Cachin, Architecture of the hyperledger blockchain fabric, (2016) [Online]. Available: https://www.zurich.ibm.com/dccl/papers/cachindccl.pdf.
[52] C. Saraf, S. Sabadra, Blockchain platforms: a compendium, Proceedings of the International Conference on Innovative Research and Development (ICIRD), IEEE, 2018, pp. 1–6.
[53] S. Li, L. Xu, S. Zhao, The internet of things: a survey, Inf. Syst. Front. 17 (2) (2015) 243–259.
[54] M. Samaniego, R. Deters, Blockchain as a service for IoT, Proceedings of the IEEE International Conference on Internet of Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData), IEEE, Chengdu, China, 2016, pp. 433–436.
[55] A. Whitmore, A. Agarwal, L.D. Xu, The internet of things-a survey of topics and trends, Inf. Syst. Front. 17 (2) (2015) 261–274.
[56] S. Li, L. Xu, Securing the Internet of Things, Syngress Publishing, Cambridge, MA, 2017.
[57] A. Bahga, V.K. Madisetti, Blockchain platform for industrial Internet of Things, J. Comput. Sci. Commun. 9 (10) (2016) 533–546.
[58] J. Garay, A. Kiayias, N. Leonardos, The Bitcoin backbone protocol: analysis and applications, Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, Berlin, Heidelberg, 2015, pp. 281–310.
[59] M. Vukolić, The quest for scalable blockchain fabric: proof-of-work vs. BFT replication, Proceedings of the IFIP WG 11.4 Workshop Open Res. Problems Netw. Secur. (iNetSec), Springer, Cham, 2015, pp. 112–125 [Online]. Available: http://www.vukolic.com/iNetSec_2015.pdf.
[60] A. Gervais, G.O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, S. Čapkun, On the security and performance of proof of work blockchains, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 2016.
[61] S. Huh, S. Cho, S. Kim, Managing IoT devices using blockchain platform, Proceedings of the 19th International Conference on Advanced Communication Technology (ICACT), IEEE, 2017, pp. 464–467.
[62] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: the case study of a smart home, Proceedings of the International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), IEEE, 2017, pp. 618–623.
[63] Y. Lu, L.D. Xu, Internet of Things (IoT) cybersecurity research: a review of current research topics, IEEE Int. Things J. Early Access (2018) 1–1, doi:10.1109/JIOT.2018.2869847.
[64] C. Li, L.J. Zhang, A blockchain based new secure multi-layer network model for Internet of Things, Proceedings of the IEEE International Congress on Internet of Things (ICIOT), IEEE, 2017, pp. 33–41.
[65] N. Rifi, E. Rachkidi, N. Agoulmine, N.C. Taher, Towards using blockchain technology for IoT data access protection, Proceedings of the 17th International Conference on Ubiquitous Wireless Broadband (ICUWB), IEEE, 2017, pp. 1–5.
[66] D. Puthal, N. Malik, S.P. Mohanty, E. Kougianos, C. Yang, The blockchain as a decentralized security framework, IEEE Consum. Electron. Mag. 7 (2) (2018) 18–21.
[67] K.Y. Hui, J.C. Lui, D.K. Yau, Small-world overlay P2P networks: construction, management and handling of dynamic flash crowds, Comput. Netw. 50 (15) (2006) 2727–2746.
[68] D.J. Watts, S.H. Strogatz, Collective dynamics of 'small-world' networks, Nature 393 (1998) 440–442.
[69] M.E.J. Newman, Scientific collaboration networks. I. Network construction and fundamental results, Phys. Rev. E. 62 (1) (2001) 016131.
[70] J. Cheney, L. Chiticariu, W.C. Tan, Provenance in databases: why, how, and where, Found. Trends Databases 1 (4) (2009) 379–474.
[71] N.Z. Aitzhan, D. Svetinovic, Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams, IEEE Trans. Depend. Secur. 15 (5) (2018) 840–852.
[72] P. Dai, N. Mahi, J. Earls, A. Norta, Smart-contract value-transfer protocols on a distributed mobile application platform, (2017) [Online]. Available: https://qtum.org/uploads/files/cf6d69348ca50dd985b60425ccf282f3.pdf.
[73] Y. Chen, et al., Big data analytics and big data science: a survey, J. Manag. Anal. 3 (1) (2016) 1–42.
[74] E. Karafiloski, A. Mishev, Blockchain solutions for big data challenges: a literature review, Proceedings of the IEEE Int. Conf. Smart Technol. Ohrid, Macedonia, 2017, pp. 763–768.
[75] S. Wang, Y. Zhang, Y. Zhang, A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems, IEEE Access 6 (2018) 38437–38450, https://doi.org/10.1109/ACCESS.2018.2851611 Early Access. doi:.
[76] B. Liu, X.L. Yu, S. Chen, X. Xu, L. Zhu, Blockchain based data integrity service framework for IoT data, Proceedings of the IEEE Int. Conf. Web Services, Honolulu, HI, USA, 2017, pp. 468–475.
[77] Q. Xia, E.B. Sifah, K.O. Asamoah, J. Gao, X. Du, M. Guizani, MeDShare: trust-less medical data sharing among cloud service providers via blockchain, IEEE Access 5 (2017) 14757–14767 [Online]. Available: http://ieeexplore.ieee.org/document/7990130/.
[78] L. Wang, W. Liu, X. Han, Blockchain-based government information resource sharing, Proceedings of the 23rd International Conference on Parallel and Distributed Systems (ICPADS), IEEE, 2017, pp. 804–809.
[79] G. Zyskind, O. Nathan, A. Pentland, Decentralizing privacy: using blockchain to protect personal data, Proceedings of the IEEE Symposium on Security and Privacy Workshops, IEEE Computer Society, 2015, pp. 180–184, , https://doi.org/10.1109/SPW.2015.27.
[80] M. Apostolaki, A. Zohar, L. Vanbever, Hijacking Bitcoin: routing attacks on cryptocurrencies, Proceedings of the Security and Privacy (SP), IEEE, 2017, pp. 375–392, , https://doi.org/10.1109/SP.2017.29.
[81] W. Mougayar, The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, John Wiley & Sons, Hoboken, New Jersey, USA, 2016.
[82] M. Iansiti, K.R. Lakhani, The truth about blockchain, Harv. Bus. Rev. (2017) 118–127.
[83] M. Mettler, Blockchain technology in healthcare: the revolution starts here, Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 2016, pp. 1–3, , https://doi.org/10.1109/HealthCom.2016.7749510.
[84] A. Ekblaw, A. Azaria, J.D. Halamka, A. Lippman, A case study for blockchain in healthcare: MedRes prototype for electronic health records and medical research data, Proceedings of the IEEE Open & Big Data Conference, 2016, p. 13. Available: https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf.
[85] X. Zhang, S. Poslad, Blockchain support for flexible queries with granular access control to electronic medical records (EMR), Proceedings of the 2018 IEEE International Conference on Communications (ICC), IEEE, 2018, pp. 1–6.
[86] T.T. Kuo, H.E. Kim, L Ohno-Machado, Blockchain distributed ledger technologies for biomedical and health care applications, J. Am. Med. Inform. Assoc. 24 (6)

(2017) 1211–1220.
[87] C. Esposito, A. De Santis, G. Tortora, H. Chang, K.K.R. Choo, Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. 5 (1) (2018) 31–37.
[88] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control, J. Med. syst. 40 (10) (2016) 218.
[89] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, MedRec: using blockchain for medical data access and permission management, Proc. International Conference on Open and Big Data (OBD), IEEE, 2016, pp. 25–30.
[90] J. Zhang, N. Xue, X. Huang, A secure system for pervasive social network-based healthcare, IEEE Access 4 (2016) 9239–9250, https://doi.org/10.1109/ACCESS.2016.2645904.
[91] Q. Xia, E.B. Sifah, A. Smahi, S. Amofa, X. Zhang, BBDS: blockchain-based data sharing for electronic medical records in cloud environments, Information 8 (2) (2017) 44 [Online]. Available: https://www.mdpi.com/2078-2489/8/2/44.
[92] G. Magyar, Blockchain: solving the privacy and research availability tradeoff for EHR data: a new disruptive technology in health data management, Proceedings of the 30th Neumann Colloquium (NC), IEEE, 2017, pp. 000135–000140.
[93] R. Guo, H. Shi, Q. Zhao, D. Zheng, Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems, IEEE Access 776 (99) (2018) 1–12.
[94] F. Tian, An agri-food supply chain traceability system for china based on RFID & blockchain technology, Proceedings of the International Conference on Service Systems and Service Management, IEEE, 2016, pp. 1–6.
[95] H.M. Kim, M. Laskowski, Towards an ontology-driven blockchain design for supply chain provenance, Proceedings of the 26th Workshop on Information Technologies and Systems, Dublin, Ireland, 2016 Available: https://doi.org/10.1002/isaf.1424.
[96] J. Backman, S. Yrjölä, K. Valtanen, O. Mämmelä, Blockchain network slice broker in 5G: slice leasing in factory of the future use case, Proceedings of the Internet of Things Business Models, Users, and Networks, IEEE, 2017, pp. 1–8.
[97] H. Yang, Y. Wu, J. Zhang, H. Zheng, Y. Ji, Y. Lee, BlockONet: blockchain-based trusted cloud radio over optical fiber network for 5G fronthaul, Proceedings of the Optical Fiber Communication Conference, Optical Society of America, 2018W2A-25.
[98] S. Jeong, N.N. Dao, Y. Lee, C. Lee, S. Cho, Blockchain based billing system for electric vehicle and charging station, Proceedings of the 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), IEEE, 2018, pp. 308–310.
[99] D.Y. Liao, X. Wang, Design of a blockchain-based lottery system for smart cities applications, Proceedings of the 3rd International Conference on Collaboration and Internet Computing (CIC), IEEE, 2017, pp. 275–282.
[100] M. Raikwar, et al., A Blockchain Framework for Insurance Processes, Proceedings of the 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE, 2018, pp. 1–4.
[101] D.G. Mamunts, et al., The use of authentication technology blockchain platform for the marine industry, Proceedings of the Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus, IEEE, 2018, pp. 69–72.
[102] T. Yang, et al., Applying blockchain technology to decentralized operation in future energy internet, Proceedings of the Conference on Energy Internet and Energy System Integration (EI2), IEEE, 2017, pp. 1–5.
[103] I. Eyal, A.E. Gencer, E.G. Sirer, R. van Renesse, Bitcoin-NG: a scalable blockchain protocol. (2015) [Online]. Available: http://arxiv.org/abs/1510.02037.
[104] L. Kan, Y. Wei, A.H. Muhammad, W. Siyuan, G. Linchao, H. Kai, A multiple blockchains architecture on inter-blockchain communication, Proceedings of the International Conference on Software Quality, Reliability and Security Companion (QRS-C), IEEE, 2018, pp. 139–145.
[105] H. Jin, X. Dai, J. Xiao, Towards a novel architecture for enabling interoperability amongst multiple blockchains, Proceedings of the 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2018, pp. 1203–1211.
[106] J. Singh, J.D. Michels, Blockchain as a service (BaaS): providers and trust, Proceedings of the 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE, 2018, pp. 67–74.
[107] R. La Porta, F. Lopez-de-Silanes, A. Shleifer, The economic consequences of legal origins, J. Econ. Lit. 46 (2) (2008) 285–332.
[108] J.C. Bertot, P.T. Jaeger, D. Hansen, The impact of polices on government social media usage: issues, challenges, and recommendations, Gov. Inform. Q. 29 (1) (2012) 30–40.
[109] D.S. Pradeepkumar, K. Singi, V. Kaulgud, S. Podder, Evaluating complexity and digitizability of regulations and contracts for a blockchain application design, Proceedings of the 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), IEEE, 2018, pp. 25–29.
[110] N. Diallo, et al., eGov-DAO: a better government using blockchain based decentralized autonomous organization, Proceedings of the International Conference on eDemocracy & eGovernment (ICEDEG), IEEE, 2018, pp. 166–171.
[111] F.S. Hardwick, R.N. Akram, K. Markantonakis, Fair and transparent blockchain based tendering framework-a step towards open governance, arXiv preprint arXiv:1805.05844, published online, 2018. Available: https://arxiv.org/abs/1805.05844.
[112] H. Hou, The application of blockchain technology in E-government in China, Proceedings of the 26th Int. Conf. Comput. Commun. Netw. (ICCCN), 2017, pp. 1–4 [Online]. Available: http://ieeexplore.ieee.org/document/8038519/.
[113] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, A. Akutsu, The blockchain-based digital content distribution system, Proceedings of the Fifth International Conference on Big Data and Cloud Computing (BDCloud), IEEE, 2015, pp. 187–190.
[114] C. Xu, K. Wang, P. Li, S. Guo, J. Luo, B. Ye, M Guo, Making big data open in edges: a resource-efficient blockchain-based approach, IEEE Trans. Parallel Distrib. Syst. 30 (4) (2019) 870–882.
[115] F. Imbault, M. Swiatek, R. de Beaufort, R. Plana, The green blockchain: managing decentralized energy production and consumption, Proceedings of the 17th IEEE Int. Conf. Environ. Elect. Eng., 1st IEEE Ind. Commercial Power Syst. Eur. (EEEIC/I CPS Eur.), 2017, pp. 1–5 [Online]. Available: http://ieeexplore.ieee.org/document/7977613/.
[116] K. Tanaka, K. Nagakubo, R. Abe, Blockchain-based electricity trading with digital grid router, Proceedings of the International Conference on Consumer Electronics-Taiwan (ICCE-TW), IEEE, 2017, pp. 201–202.
[117] G. Kim, J. Park, J. Ryou, A study on utilization of blockchain for electricity trading in microgrid, Proceedings of the International Conference on Big Data and Smart Computing (BigComp), IEEE, 2018, pp. 743–746.
[118] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, F.Y. Wang, Blockchain-enabled smart contracts: architecture, applications, and future trends, IEEE Trans. Syst. Man Cybern. Syst. (2019) 1–12, https://doi.org/10.1109/TSMC.2019.2895123 Early Access.
[119] P. Dunphy, F.A. Petitcolas, A first look at identity management schemes on the blockchain, IEEE Secur. Priv. 16 (4) (2018) 20–29.
[120] Z. Yang, K. Yang, L. Lei, K. Zheng, V.C. Leung, Blockchain-based decentralized trust management in vehicular networks, IEEE Int. Things J. (2018) Early Access, 1–1.
[121] C. Lin, D. He, X. Huang, M.K. Khan, K.K.R. Choo, A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems, IEEE Access 6 (2018) 28203–28212.
[122] W. Wang, D.T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, ..., D.I. Kim, A survey on consensus mechanisms and mining strategy management in blockchain networks, IEEE Access 7 (2019) 22328–22370.
[123] N.Z. Aitzhan, D. Svetinovic, Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams, IEEE Trans. Dependable Secure Comput. 15 (5) (2018) 840–852.
[124] J.J. Sikorski, J. Haughton, M. Kraft, Blockchain technology in the chemical industry: machine-to-machine electricity market, Appl. Energy 195 (2017) 234–246.
[125] J. Huang, L. Kong, G. Chen, M.Y. Wu, X. Liu, P. Zeng, Towards secure industrial IoT: blockchain system with credit-based consensus mechanism, IEEE Trans. Ind. Inform. (2019), https://doi.org/10.1109/TII.2019.2903342 Early Access..
[126] E. Heilman, F. Baldimtsi, S. Goldberg, Blindly signed contracts: anonymous on-blockchain and off-blockchain bitcoin transactions, International Conference on Financial Cryptography and Data Security, Springer, Berlin, Heidelberg, 2016, pp. 43–60.
[127] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, M.A. Imran, Blockchain-enabled wireless internet of things: performance analysis and optimal communication node deployment, IEEE Int. Things J. (2019) Early Access, 1–1, doi:10.1109/JIOT.2019.2905743.