Internet of Things xxx (xxxx) xxx

Contents lists available at ScienceDirect

Internet of Things

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

Review article

Blockchain for the IoT and industrial IoT: A review

Qin Wang[a,b,c,*], Xinqi Zhu[c,d], Yiyang Ni[e], Li Gu[c,d], Hongbo Zhu[a,b]

[a] Jiangsu Key Laboratory of Wireless Communications, Nanjing University of Posts and Telecommunications, Nanjing, China
[b] Engineering Research Center of Health Service System Based on Ubiquitous Wireless Networks, Nanjing University of Posts and Telecommunications, Ministry of Education, China
[c] College of Engineering and Computing Sciences, New York Institute of Technology - Nanjing Site, Nanjing, China
[d] College of Overseas Education, Nanjing University of Posts and Telecommunications, Nanjing, China
[e] School of mathematics and information technology, Jiangsu Second Normal University, Nanjing, China

ARTICLE INFO

Article history:
Received 1 March 2019
Revised 29 June 2019
Accepted 29 June 2019
Available online xxx

Keywords:
Blockchain
IoT
Industrial IoT
Decentralization
Security

ABSTRACT

The Internet of Things (IoT), especially the industrial IoT (IIoT), has rapidly developed and is receiving a lot of attention in academic areas and industry, but IoT privacy risks and security vulnerabilities are emerging from lack of fundamental security technology. The blockchain technique, due to its decentralization and information disclosure, was proposed as a decentralized and distributed approach to guarantee security requirements and motivate the development of the IoT and IIoT. In this paper, we first introduce the basic structure and main features of blockchain and summarize the security requirements to develop IoT and Industry 4.0. Then, we explore how blockchain can be applied to the IoT for Industry 4.0 using its security tools and technology. We describe the most relevant blockchain-based IoT applications to promote the functions and advantages of the blockchain technique on IoT and IIoT platforms. Finally, some recommendations are proposed to guide future blockchain researchers and developers.

1. Introduction

The advent of the Internet of Things (IoT) enhances traditional thinking of the past and allows connection of many, if not all, objects in the environment to the network. It can connect vehicles, household appliances, and other electronic devices together on the network, which, in turn, brings humans a more intelligent life. The system realizes real-time identification, location, tracking, and monitoring, and it triggers corresponding events automatically. Furthermore, IoT is the crucial part in the Industrial IoT (IIoT) that aims to produce intelligent manufacturing goods and establish smart factories with tight connections between customers and business partners.

The IoT is experiencing exponential growth and receiving a lot of attention in academic areas and industry, but the privacy risks and security vulnerabilities are emerging from the lack of fundamental security technology. Current security and privacy methods are inapplicable for IoT due to its decentralized topology and the resource constraints of mobile devices [1].

To guarantee the security of the IoT and IIoT, blockchain is proposed as a decentralized and distributed approach. It is a distributed ledger as all the blocks are chained together. It is able to track and coordinate transactions and save information

* Corresponding author at: Jiangsu Key Laboratory of Wireless Communications, Nanjing University of Posts and Telecommunications, address: No. 66 Xin Mofan Road, Nanjing 210003, China.
E-mail addresses: wangqin@njupt.edu.cn (Q. Wang), xzhu22@nyit.edu (X. Zhu), niyy@njupt.edu.cn (Y. Ni), lgu04@nyit.edu (L. Gu), zhb@njupt.edu.cn (H. Zhu).

https://doi.org/10.1016/j.iot.2019.100081
2542-6605/

for the billions of devices in the IoT [2]. The most important advantage of blockchain technology is decentralization, which realizes peer-to-peer transactions based on decentralized credits in distributed systems. It uses motion time stamping, distributed consensus, data encryption, and economic incentives. It reduces cost, increases efficiency, and provides solutions to the problem of insecure data storage in centralized organizations.

We are going to analyse the basics of blockchain and IoT, by conducting archival research. To study this problem, we explore the main features of blockchain, such as decentralization, smart contrasts, asymmetric encryption, access management [3] and others that can be taken on the IoT platform to promote its functions. And we conclude that blockchain would be an ideal and suitable concept for developing the IoT and IIoT. However, there are still some problems to be solved.

This paper is structured as follows. In Section 2, we focus on what a blockchain is and different attitudes from countries and companies towards blockchain technology. In Section 3, we introduce the IoT and IIoT and analyse their development disciplines and present issues. Then, we explore several blockchain based IoT and IIoT applications in Section 4. Also, the problems and limitations of blockchain are proposed in Section 5. We draw conclusions and propose future work in Section 6.

2. What is blockchain?

We cannot discuss the blockchain without mentioning Bitcoin first. Blockchain technology made its public debut in 2008 when Satoshi Nakamoto released the whitepaper Bitcoin. Even today, many people still regard Bitcoin and blockchain as the same thing. At its core, blockchain is a decentralized ledger that records transactions between two nodes in a permanent way without authentication from a third-party. This creates an extremely efficient process and reduces the cost of transactions below 1%. But Bitcoin is only one kind originating from the blockchain virtual currency. With blockchain development, it could be used for more than cryptocurrency. People started to invest in and explore how blockchain could alter different kinds of applications or operations. One of the most popular applications is to combine blockchain with the IoT.

2.1. Blockchain development

The blockchain technique is not a new concept, but it is recently developed with its specific advantages in guaranteeing transaction security. In November 2008, a paper written by Satoshi Nakamoto was published online, titled “Bitcoin: A Peer-to-Peer Electronic Cash System”. It described one electronic trading system that did not depend on any third party and was quite different from the present ones. Then, in January 2009, bitcoin was created by Satoshi Nakamoto, with the first block (Genesis block) that can be mined.

Because of the rise of Bitcoin, more and more different cryptocurrencies have been introduced. This has led to monetary system chaos and the emergence of many opportunistic people making money through it. So cryptocurrency suffered a blow, but most countries and companies attach more importance to blockchain technology. Some countries even refer to blockchain technology at the national strategic level [4–11]. Many countries and companies have high expectations for blockchain technology. Well-known companies, such as Alibaba, and Google, have also introduced related projects to study blockchain, so in the future, the blockchain will be a very objective technology [12].

We term from 2009–2013 blockchain 1.0, where bitcoin is a representative and people used blockchain in digital currency applications. In the following two years, it was developed to blockchain 2.0, where smart contracts are combined with digital currency to optimize a wider range of scenarios in financial areas. There were two typical applications during this period: one is the bitcoin-based trading market, and the other is currency exchanges. The investments by venture capitalists in blockchain start-ups rose from $93 million to $550 million in three years from 2013, according to [13]. It is forecast to grow to $2.3 billion by 2021. Now, the blockchain has developed to the era of programmable blockchains aiming to provide decentralized and distributed solutions for a variety of IoT and IIoT applications [14].

2.2. Concept and structure of blockchain

Overall, blockchain is composed of three core parts: block, chain, and network:

1. Block: this can be thought of as a list of bills that cannot be modified. Once you record something into blocks, every node can inquire everything in this block. The size, period and triggering events for blocks depend on the type of blockchain.
2. Chain: this has the function of linking a list of blocks. Blockchain is founded on linking all the blocks.
3. Network: this is a set of nodes. In a traditional network, routes are thought of as nodes, whereas in a blockchain network, the blocks are the nodes.

In detail, the structure of a blockchain can be seen in Fig. 1. It shows the components of a block, the algorithms it uses, and the relationship between blocks. One block can be divided into two parts including the header and body [15]. The block header involves pre-block hash, a timestamp (indicating the writing time of the block data), Nonce (whose value is adjusted by miners so that the hash of the block is larger than the hash of the next block), and the Merkle root (quickly summarizing and verifying the existence and integrity of block data). The block body records the transaction information details and the number of transactions.

Please cite this article as: Q. Wang, X. Zhu and Y. Ni et al., Blockchain for the IoT and industrial IoT: A review, Internet of Things, https://doi.org/10.1016/j.iot.2019.100081

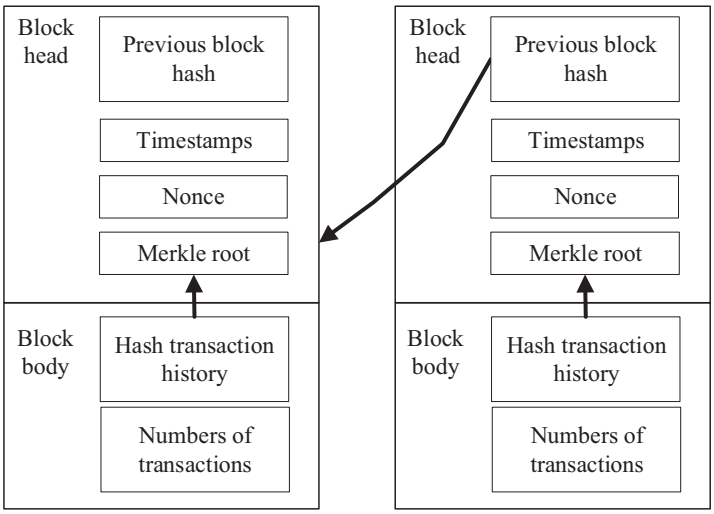

Fig. 1. Structure of a blockchain.

Through the difficulty value of the Proof of Work (PoW) consensus process, the correct Nonce is found first, and the miners who have been verified by all miners will receive the current block accounting rights. These records are generated by the hash process of the Merkle root to count in the block header. When a new transaction happens, the information is broadcast to the all network participants. All miners who have received the transaction will verify it by validating the transaction signature. The miners order and pack the transactions into timestamp blocks. Then, they broadcast the blocks back to the network. The network nodes verify that the blocks contain valid transactions and refer to the previous block of the chain by deploying a kind of hash algorithm. The blocks that are not verified by nodes will be discarded. Therefore, a blockchain provides a trusting strategy for information exchange or resource trading scenarios.

3. IoT and Industrial IoT

3.1. Introduction of the IoT and Industrial IoT

3.1.1. IoT

At the conceptual level, IoT refers to the interconnection and interoperability among our everyday devices (computers, laptops, phones, watches, and other handheld embedded devices), as well as the device autonomy, perception, and situational awareness. A connected device equipped with sensors or actuators senses its surrounding environment, understands what is happening and decides intelligently and independently or communicates with the other nodes or users to make the best decisions. In short, IoT aims to add computer-based logic to plenty of things (objects), which can then be monitored or controlled by analytics or engines [16].

The development of the IoT is increasingly suited to the needs of humanity. It combines vehicles, healthcare, wearables, retail, logistics, manufacturing, agriculture, utilities, appliances, etc. [2]. According to the 2020 conceptual framework, the IoT is expressed as a simple formula [17].

$$\text{IoT} = \text{Services} + \text{Data} + \text{Networks} + \text{Sensors}$$

Thus, IoT is a combination of data from sensors and networks that provide different intelligent services.

3.1.2. Industrial IoT

IIoT refers to the trend or concept of using process automation and data exchange in the current manufacturing industry. It brings together applications of the IoT, network augmentation system and cloud computing [18]. The IIoT is used together with Cyber-Physical Systems (CPS) for Industry 4.0 to digitize and understand the supply market, manufacturing, and sales, and it finally achieves convenient, effective, and personalized products [19,20]. CPS are mechanisms monitored or controlled by computer-based algorithms that are tightly integrated with users and the network, such as autonomous automobile systems, smart homes, medical monitoring, and robotics systems.

IIoT is a fusion of many new technologies, such as autonomous machines, advanced robotics, big data, cloud/edge computing, digital ubiquity, smart factories, machine learning, AI, and cyber physical on the basis of IoT [21].

IIoT mainly applies instrumentation, connected sensors, and other devices to machinery, vehicles in the transport, and the energy and industrial sectors. Traditional IoT applications such as Internet-connected refrigerators are a subset of IIoT [22]. It has four design principles [18]:

Please cite this article as: Q. Wang, X. Zhu and Y. Ni et al., Blockchain for the IoT and industrial IoT: A review, Internet of Things, https://doi.org/10.1016/j.iot.2019.100081

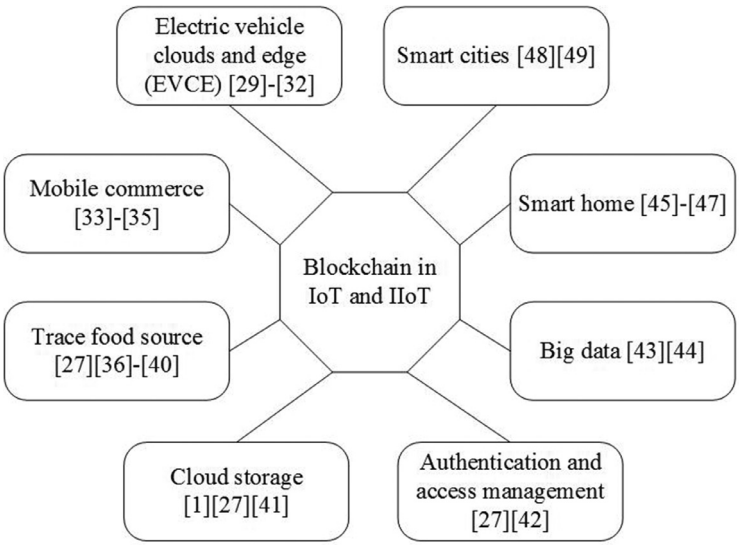

Fig. 2. Blockchain applications in the IoT and IIoT.

1. Interoperability: the possibility that machines and related components connect and communicate with people.
2. Information transparency: the necessity of creating virtual copies of the physical world.
3. Technical assistance: essential comprehensive aggregation and information visualization to support human capabilities.
4. Decentralization of decisions: the ability of a network-enabled system to independently make decisions and perform its own specialized functions.

The IIoT based on the IoT provides a seamless way for data transmission across different workplaces. Real-time monitoring systems and data transfer have the ability to optimize and increase productivity, get better quality products, and help businesses become more intelligent and efficient [20,23].

3.2. Issues that need to be resolved

However, for the IoT and IIoT to be developed rapidly, there are still some technical issues to solve, such as interoperability difficulty, security vulnerability, lack of data analysis and transmission and absence of IT and OT convergence. One of the biggest problems to be solved is security vulnerability.

As manufacturing processes become more intelligent, most connected computing devices in the information network share information directly with the cloud and are therefore subject to security threats and attacks easily. This threat can take many forms, as IoT devices have proven to be more likely to contain easily exploitable vulnerabilities, such as the growing number of cybercriminal targets to expand their botnets. IoT-based Distributed Denial of Service (DDoS) attacks have shown their power to undermine business [24].

Blockchain is an ideal solution for IIoT security. The work in [25,26] proposed a blockchain platform for IIoT. This platform, with smart contracts deployed, enables development of different distributed applications for manufacturing using a decentralized, trustless, peer-to-peer network for IIoT applications.

4. Future human industrial development direction: blockchain-based IoT and IIoT

The blockchain is a real-time ledger of records that are stored in a distributed, point-to-point manner and are independent of any central authority. Each record is encrypted and time stamped, and users can only have the rights to access and edit the blocks for which they have the private key. Each block is linked to the previous and the next block, and the entire chain is updated each time a change is made [27,28]. It is extremely difficult or impossible to edit or delete data blocks when the blocks are recorded on the blockchain ledger. Thus, it protects communication and transaction security.

Since blockchain has so many innovative features, it has been and will be widely used to develop IoT and IIoT. Some representative blockchain applications are summarized in Fig. 2 and introduced in the following subsections.

4.1. Electric vehicle clouds and edge (EVCE)

EVCE is an attractive network paradigm to aggregate the destroyed idle resource of vehicles to a common pool. The coexistence of hybrid cloud and edge computing is centreless in which information exchange is done without pre-assigned

Please cite this article as: Q. Wang, X. Zhu and Y. Ni et al., Blockchain for the IoT and industrial IoT: A review, Internet of Things, https://doi.org/10.1016/j.iot.2019.100081

trust relationships. To address security issues, the blockchain technique is proposed as a potential solution with features of decentralization, anonymity, trust, and co-participation [29,30].

In an EVCE computing network, both energy resources and information are exchanged, collaborated, and reallocated among vehicles. The vehicles can be spontaneous network operators, mobile data calculators, or virtual power plants in different cases as needed. In [29], a security scheme was built by blockchain to establish distributed consensus via data coins and energy coins based on timestamps and hash tree algorithms such as PoW and proof of stake (PoS). The information and energy trading records among vehicles were encrypted and structured into blockchains in a linear chronological order so that the transaction information could not be tampered with easily.

To satisfy the ever-increasing energy resource demands of IIoT applications with growing numbers of devices, a localized blockchain-enabled secure energy trading system among vehicles was built in [31] and [32]. The authors proposed a consortium blockchain to perform consensus processes among vehicles. It enables distributed charging and discharging transaction security and privacy without a trusted third party.

4.2. Mobile commerce

Due to the boom of mobile commerce (m-commerce), data security problems are becoming more and more important and need to be addressed. Blockchain as a distributed database was proposed to secure transactions at mobile nodes to support direct device-to-device m-commerce data exchange and sharing. An Android system-based implementation process was introduced in [33]. Blockchain makes sure that the data exchange between devices does not need the involvement of any third party. The work in [34] introduced how smart contracts radically and transparently redefine the interactions between interacting parties on a distributed network. A smart contract is first built between the seller and buyer containing the exact transaction information [35]. Both participants confirm this contract and publish it in the blockchain system. As a result, both get what they want securely with the help of the blockchain.

4.3. Trace food source

Trace food source is the biggest application for blockchain to help improve the IoT. The traditional food chain starts from manufacturers, through suppliers, to vendors, and this makes food information very confusing and increases the difficulty of tracing food sources.

Blockchain makes sure that each transaction is time-stamped and digitally signed and can be traced back to a specific time period, and the corresponding party is found on the blockchain by the public address. This is because of the non-repudiation of the blockchain: ensuring that someone cannot verify the authenticity of his or her signature on the file, or that the author's identity is the transaction they initiated, making the system more reliable. The conversion of ledger global status and the blockchain auditing function provide a company with security and transparency for each iteration [36,37].

Blockchain ensures the security of the supply chain and can be convenient for handling crisis situations, for example, product recalls because of security breaches. The public availability of blockchains means that each product can be traced to the source of raw materials, and the transactions can be linked in a chain to users identifying vulnerable IoT devices [27].

Now, IBM and Walmart work together to make the food chain transparent. They signed an agreement with Tsinghua University to generate transparency and efficiency in supply chain record-keeping. Tsinghua University is also working with Yonghui Superstores to record the fish supply chain in the store. Instead of traditional paper tracking and manual inspection systems, blockchain provides a different transaction system. Retailers can know who the suppliers trade with. Since transactions are not stored in any single node, it is almost impossible to modify information easily. At the same time, it is easy for consumers to access relevant information about goods such as factory and processing data, production and expiration time by scanning the QR code using a smartphone, and they can get service in the event of product failure. The government can check the blockchains regulating relevant food departments [38].

Without blockchain, it usually took 6 days, 18 h and 26 min for Walmart to trace mangoes back to the original farm. Now, with the help of blockchain, consumers need just 2.2 s to get all the detailed information about goods [39].

In addition, Alibaba released Green Hand to generate e-passports for physical goods. Consumers can scan the QR code to know the detailed information about their goods, which ensures the authenticity of the items [40].

4.4. Cloud storage

Cloud storage plays a vital role in IoT development. As we all know, cloud storage is also a vulnerable link in IIoT development.

First, the IoT network of centralized cloud models has a high-cost problem. IoT devices are connected, identified, and authenticated by a cloud server, where storage and processing are typically performed. Even if the devices are a few feet apart, their connection is certainly through the Internet. With blockchain technology, decentralization can be achieved without centralizing entities. Devices communicate directly and exchange distributed data with each other, automatically performing operations through smart contracts.

Second, any block of the IoT architecture can become a point of failure or a bottleneck that could damage the entire network. For example, IoT nodes are vulnerable to DDoS attacks, data theft, etc. Criminals can also damage systems and

Please cite this article as: Q. Wang, X. Zhu and Y. Ni et al., Blockchain for the IoT and industrial IoT: A review, Internet of Things, https://doi.org/10.1016/j.iot.2019.100081

abuse data. If the IoT device connected to a server is corrupted, every node connected to that server may be affected. The blockchain verifies the validity of the device identity and encrypts and verifies the transaction to ensure that only the message originator can send it, along with the timeline in the chain, which helps users know the details of the device or data chain clearly. Because the records are shared, a single point of failure record does not occur [1,41].

Third, centralized cloud models are easily manipulated. One cannot ensure that the information is used properly by collecting real-time data. The blockchain technology immutability and decentralized access detects and blocks malicious operations. If a blockchain update for a device is corrupted, the system rejects it [27].

4.5. Authentication and access management

Traditional systems use a centralized architecture and simple login, which is still dangerous for employees and customers who are vulnerable to stealing or cracking passwords. Blockchain technology provides strong authentication and addresses single-point attacks, validating devices and users under a distributed public key infrastructure, and replacing traditional passwords with specific Security Socket Layer (SSL) certificates. And the management of certificate data is done on the blockchain, which makes it almost impossible for an attacker to use a fake certificate [42].

Blockchain identity authentication and access management techniques can be used to enhance IoT security. For example, with this technology, information about proof of goods, identity, credentials and digital rights can be stored securely. On the condition that the entered original information is accurate, the blockchain will be unchanged. For physical assets in IoT devices, individuals can individually store cryptographic hashes of the device firmware in a private blockchain. This kind of system using a blockchain creates a permanent record of device status and configuration [27].

4.6. Big data

In the IIoT, human genetic data is more important than ever before due to intelligent production. The business needs of blockchain financial services are strong, bringing big data and related analysis tools to the ledger provided by the complete blockchain. Recently, a consortium of more than forty Japanese banks signed a contract with a blockchain technology called Ripple to use the blockchain to facilitate the transfer of funds between bank accounts and perform real-time transfers at very low cost. Traditional real-time transfers are expensive, and one of the important reasons is the potential risk factor. Double spending, where the same security token is used twice, is the exact problem of real-time transfer. The use of blockchains can largely avoid this risk. Big data analytics speed up the procedure to identify consumer spending patterns and risky transactions faster than it currently is. This reduces the resource or economic cost of real-time transactions [43].

In IoT industries other than the economic industry, the main driver of blockchain technology is data security. In the smart health, retail, and administration sectors, businesses have begun experimenting with blockchains to process data to prevent hacking or data breaches. In Industry 4.0, human genetic data is more important than ever before due to intelligent production. In India, the government has established a gene database system based on block links for 50 million people [44].

4.7. Smart home

The smart home is described as a crucial application of ubiquitous computing that incorporates intelligence into dwellings management and operation [45]. By using blockchains, each device within the home can request data from the other internal devices to provide certain services. For example, when someone enters the home, the motion sensor sends the data to the light bulb so that the light can be turned on automatically, and the miner assigns the shared key to each other direct communication device. Once the key is received and is verified as valid, the device will directly communicate. The benefits of this approach are twofold. The first is that the miners and owners have a list of devices that share data. The second is that the communication between device nodes is protected with a shared key [46].

Without cloud storage, data can be stored locally and authenticated by using a shared key. To grant a key, the device needs to send a request to the miner, and if it has storage rights, the miner generates a shared key and sends the device and the stored key. By receiving the key, the local storage generates a starting point containing the shared key. With a shared secret, devices can store data directly in local storage.

By receiving the monitor transaction, the miner sends the current data of the requested device to the requester. If the requester is allowed to receive data for a period of time, the miner periodically sends the data until the requester sends a close request to the miner and revokes the transaction. Monitor transactions enable homeowners to watch cameras or other devices that send periodic data [47].

4.8. Smart cities

One of the important goals in the IIoT is to build a smart environment, including providing autonomous machines, which is known as smart cities. Smart Cities are aimed to combine technology, government and society together to enable the following representative characteristics: smart economy, smart mobility, smart environment, smart people, smart living, and smart governance [48].

Please cite this article as: Q. Wang, X. Zhu and Y. Ni et al., Blockchain for the IoT and industrial IoT: A review, Internet of Things, https://doi.org/10.1016/j.iot.2019.100081

It is obvious that blockchain provides a decentralization platform for building smart cities [49]. For example, the real-time status of on-street parking can be understood through blockchain technology, which not only reduces the trouble of parking for the owners but also relieves traffic pressure.

Additionally, for the time being, there are already many cases in different industries combining blockchain and IoT applications. In the entertainment industry, B2EExpand is the first gaming company on the Steam to create cross-game video games on the basis of an Ethereum blockchain. Guts uses blockchain technology to create a ticketing ecosystem to eliminate ticket fraud and the secondary ticket market. In the retail industry, Warranteer makes it easier for users to access product information and support. In the financial area, Ripple is supposed to be a global payment solution provider by connecting payment providers, banks, companies and digital asset exchanges for global, on-demand billing. In the area of healthcare, the MedRec Company uses blockchain to record transaction information for patients, facilities, and medicine providers. It saves time, money and repeatability between facilities and providers, enabling any health care provider to securely access patient records. At the same time, they can access their anonymous medical records in large quantities for research.

Blockchain has been applied to almost all aspects of people's production and life. The technology is mature in some areas, such as the mobile economy and tracing food source. However, most applications in areas such as smart city and smart home still stay in the experimental stage. The reduction of the production cost and computational complexity is the premise of the quantitative production of blockchain. In addition there is a lack of responsive international standards.

5. Limitations and recommendations of blockchain-based systems

The blockchain has been widely researched by academic peers due to its decentralized feature for IoT applications. Whereas the state-of-the-art methods still have some limitations, by conquering these challenges, the capabilities and effectiveness of blockchain technology can be improved and should be further investigated in the near future [47].

5.1. Relatively poor performances

Compared to traditional centralized databases, blockchain solutions often perform poorly, mainly because of the scalability aspects of their consensus mechanisms and performance issues. It often results in lower transaction throughput and higher latency. But the IoT and IIoT have exponential growth of data transmission. Ethereum may modify and improve this limitation [35,50].

5.2. Complicated privacy issues

Each participating device in the blockchain is identified by its public key. All transaction information is public. By analysing the data, interested parties can identify patterns and establish connections between addresses and ultimately make informed inferences about the actual identity behind them [51–54]. But, you can make the pattern recognition difficult by having the device use a new key for each transaction [55].

5.3. Increasing complexity

The complexity of the mining algorithm grows as the number of transactions increases. When the mobile or IoT devices are low-battery with power constrained, they are not always capable of completing the substantial computing and data exchange required by blockchains. Therefore, the design of energy-efficient blockchain protocols and algorithms is one of the significant challenges in the near future.

5.4. Standardized test platform

In the near future, if users or developers want to apply blockchains to the IoT and IIoT, one of the biggest things is how to test the stability, performance, and security of the application. Thus, it is necessary to build a standardized test platform and have all people agree with the criteria. In this way, verification is valid and users have the motivation to use blockchain-based products.

6. Conclusion and future work

In this paper, we aim at providing a comprehensive review about blockchain for the IoT and Industrial IoT, which have attracted the wide interest. With the combination of blockchain, IoT and IIoT will be the huge technological leaps that bring significant improvements to various aspects of human life, such as Electric vehicle clouds and edge (EVCE), mobile commerce, food source trace and so forth, all of which are going to make our society smarter.

The discovery suggests that blockchain is an ideal and suitable concept for developing the IoT and IIoT that creates transparent, supervisable, safe and convenient IoT and industry chains. The blockchain and IoT combination paves the way for new and novel business models and distributed IoT applications. There have been many solutions for the IoT and IIoT platforms to promote their functions, such as food logistics management. However, there are still some limitations that need to be solved in the future.

Please cite this article as: Q. Wang, X. Zhu and Y. Ni et al., Blockchain for the IoT and industrial IoT: A review, Internet of Things, https://doi.org/10.1016/j.iot.2019.100081

Declaration of interests

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

Acknowledgments

This research was supported in part by the National Natural Science Foundation of China (61801238, 61701201, and 61871446), the Natural Science Foundation of Jiangsu Province (No. BK20170758), the Natural Science Foundation for colleges and universities of Jiangsu Province (No. 17KJB510011), and New York Institute of Technology 2018 Global Faculty Research and Creativity Grants.

References

[1] A. Dorri, S.S. Kanhere, R. Jurdak, Blockchain in internet of things: challenges and solutions, 2016, arXiv preprint arXiv:1608.05187.
[2] T.M. Fernández-Caramés, P. Fraga-Lamas, A review on the use of blockchain for the internet of things, IEEE Access 6 (2018) 32979–33001.
[3] O. Novo, Blockchain meets IoT: an architecture for scalable access management in IoT, IEEE Internet of Things J. 5 (2) (2018) 1184–1195.
[4] L. Mearian. Ethereum explores a fix for blockchain's performance problem. https://www.computerworld.com/article/3245928/emerging-technology/ethereum-explores-a-fix-for-Blockchains-performance-problem.html. January 5, 2018.
[5] Z. Chen. How should we regulate blockchain? It depends on which country you ask. http://fortune.com/2018/06/25/Blockchain-cryptocurrency-technology-regulation-bitcoin-ethereum/. June 25, 2018.
[6] M. Cabrera. Cryptocurrency and blockchain investor gives suggestions to global governments regulating new technologies. https://www.cio.com/article/3263324/Blockchain/cryptocurrency-and-Blockchain-investor-gives-suggestions-to-global-governments-regulating-new-techn.html. March 27, 2018.
[7] A. Kaplan. How alibaba is championing the application of blockchain technology in china and beyond – Tue Jul 10. https://smartereum.com/7630/how-alibaba-is-championing-the-application-of-Blockchain-technology-in-China-and-beyond-tue-jul-10/ July 11, 2018.
[8] Z. Huang. China's crackdown on crypto hasn't stopped its tech giants from flirting with blockchain. https://qz.com/1256536/baidu-tencent-alibaba-bat-are-flirting-with-Blockchain-despite-chinas-ban-on-cryptocurrency/ April 19, 2018.
[9] W. Suberg. Internet giant baidu unveils energy-efficient 'Super Chain' Blockchain Protocol. https://cointelegraph.com/news/internet-giant-baidu-unveils-energy-efficient-super-chain-Blockchain-protocol. Jun 3, 2018.
[10] A. Levy. Why mark zuckerberg just put some of his best execs on blockchain. https://www.cnbc.com/2018/05/09/zuckerberg-invests-in-Blockchain-to-keep-facebook-relevant.html. March 22, 2018.
[11] O. Kharif; M. Bergen. Google is working on its own blockchain-related technology. https://www.bloomberg.com/news/articles/2018-03-21/google-is-said-to-work-on-its-own-Blockchain-related-technology. May 9, 2018.
[12] Q. Chen. In the world of cryptocurrency buzz, blockchain is the real winner. https://www.cnbc.com/2018/01/10/in-the-world-of-cryptocurrency-buzz-Blockchain-is-the-real-winner.html. January 12, 2018.
[13] Markets and Markets, Statista estimates, Market for Blockchain Technology Worldwide (2018). Accessed: Apr. 10https://www.statista.com/statistics/647231/worldwide-blockchaintechnology-market-size.
[14] J. Hu. What are the timetables for the blockchain national standards? http://baijiahao.baidu.com/s?id=1600160721567265567&wfr=spider&for=pc. May 11, 2018.
[15] Y. Yuan, F.-Y. Wang, Blockchain: the state of the art and future trends, Acta Automatica Sinica 42 (4) (2016) 481494.
[16] Daniel Minoli, Benedict Occhiogrosso, Blockchain mechanisms for IoT security, Internet of Things 1 (2018) 1–13.
[17] L. Atzori, A. Iera, G. Morabito, Understanding the internet of Things: definition, potentials, and societal role of a fast evolving paradigm, Ad Hoc Netw 56 (2017) 122–140.
[18] D. Underwood, Industry 4.0, key design principles (April 24, 2017). https://kingstar.com/industry-4-0-key-design-principles/.
[19] A. Rojko, Industry 4.0 concept: background and overview, Int. J. Interact. Mobile Technol. 11 (5) (2017) 77.
[20] M. Zaouini. Nine challenges of industry 4.0. http://iiot-world.com/connected-industry/nine-challenges-of-industry-4-0/.
[21] Unknown. Industry 4.0: the fourth industrial revolution – guide to industrie 4.0. https://www.i-scoop.eu/industry-4-0/.
[22] J. Gold. What is the industrial IoT? [And why the stakes are so high]. https://www.networkworld.com/article/3243928/internet-of-things/what-is-the-industrial-iot-and-why-the-stakes-are-so-high.html. February 2, 2018.
[23] N. Joshi. Blockchain meets industry 4.0 - what happened next? https://www.allerin.com/blog/5659-2. September 5, 2017.
[24] M. Patel. How to solve common challenges of industrial ioT. https://www.einfochips.com/blog/how-to-solve-common-challenges-of-industrial-iot/. November 23, 2017.
[25] N. Teslya, I. Ryabchikov, Blockchain-based platform architecture for industrial ioT, in: Proceedings of the 2017 21st Conference of Open Innovations Association (FRUCT), 2017, pp. 321–329.
[26] A. Bahga, V.K. Madisetti, Blockchain platform for industrial internet of things, J. Softw. Eng. Appl. 9 (2016) 533–546.
[27] N. Kshetri, Can blockchain strengthen the internet of things?, It Professional 19.4(2017):68–72.
[28] H. Watanabe, Can blockchain protect Internet-of-Things? 2018, https://arxiv.org/ftp/arxiv/papers/1807/1807.06357.pdf.
[29] S.K. Datta, et al., Vehicles connected resources: opportunities and challenges for the future, IEEE Vehic. Tech. Mag. 12 (2) (2017) 26–35.
[30] L. Hong, Z. Yan, Y. Tao, Blockchain-Enabled security in electric vehicles cloud and edge computing, IEEE Netw. 32 (3) (2018) 78–83.
[31] M. Conoscenti, A. Vetrò, J.C. De Martin, Blockchain for the internet of Things: a systematic literature review, in: Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016, pp. 1–6.
[32] J. Kang, R. Yu, X. Huang, S. Maharjan, et al., Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains, IEEE Trans. Ind. Inf. 13 (6) (2017) 3154–3164.
[33] Z. Li, J. Kang, R. Yu, et al., Consortium blockchain for secure energy trading in industrial internet of things, IEEE Trans. Ind. Inf. 14 (8) (2018) 3690–3700.
[34] K. Suankaewmanee, D.T. Hoang, D. Niyato, et al., Performance analysis and application of mobile blockchain, in: Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC), 2018, pp. 642–646.
[35] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303.
[36] Zhang Y., J. Wen, The IoT electric business model: using blockchain technology for the internet of things, Peer-to-Peer Netw. Appl. 10 (4) (2017) 983–994.
[37] S. Ravindra. The role of blockchain in cybersecurity. https://www.infosecurity-magazine.com/next-gen-infosec/Blockchain-cybersecurity/ January 8, 2018.
[38] S. Ramamurthy. Leveraging blockchain to improve food supply chain traceability. https://www.ibm.com/blogs/Blockchain/2016/11/leveraging-Blockchain-improve-food-supply-chain-traceability/ November 16, 2016.
[39] S. Charlebois. How blockchain technology could transform the food industry. https://theconversation.com/how-Blockchain-technology-could-transform-the-food-industry-89348. December 19, 2017.

Please cite this article as: Q. Wang, X. Zhu and Y. Ni et al., Blockchain for the IoT and industrial IoT: A review, Internet of Things, https://doi.org/10.1016/j.iot.2019.100081

[40] L. Dong. What's the future of blockchain in China? https://www.weforum.org/agenda/2018/01/what-s-the-future-of-Blockchain-in-china/?from=timeline. January 11, 2018.
[41] N. Joshi. Distributed cloud storage with blockchain technology. https://www.allerin.com/blog/distributed-cloud-storage-with-Blockchain-technology. June 23, 2017.
[42] S. Ravindra. The role of blockchain in cybersecurity. https://www.infosecurity-magazine.com/next-gen-infosec/Blockchain-cybersecurity/ January 8, 2018.
[43] A. Venkat. Introduction to blockchains & what it means to big data. https://www.kdnuggets.com/2017/09/introduction-blockchain-big-data.html.
[44] T Ahram, A Sargolzaei, S Sargolzaei, et al., Blockchain technology innovations, in: Proceedings of the Technology & Engineering Management Conference, IEEE, 2017, pp. 137–141.
[45] Dragos Mocrii, Yuxiang Chen, Petr Musilek, IoT-based smart homes: a review of system architecture, software, communications, privacy and security, Internet of Things 1 (2018) 81–98.
[46] A. Dorri, S.S. Kanhere, R. Jurdak, et al., Blockchain for IoT security and Privacy: the case study of a smart home, in: Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops, 2017.
[47] M.A. Ferrag, M. Derdour, M. Mukherjee, Blockchain technologies for the internet of things: research issues and challenges, IEEE Internet of Things J. (2018), doi:10.1109/JIOT.2018.2882794.
[48] Dario Bruneo, et al., An iot service ecosystem for smart cities: the# smartme project, Internet of Things 5 (2019) 12–33.
[49] S.N. O.Scekic, S. Dustdar, Blockchain-supported smart city platform for social value co-creation and exchange, IEEE Internet Comput 23 (1) (2019) 19–28.
[50] B. Marr. 30+ Real examples of blockchain technology in practice. https://www-forbescom.cdn.ampproject.org/c/s/www.forbes.com/sites/bernardmarr/2018/05/14/30-real-examples-of-Blockchain-technology-in-practice/amp/. May 14, 2018.
[51] E. Frontier. https://www.ethereum.org/ Mar. 15, 2016.
[52] S. Meiklejohn et al., A fistful of bitcoins: characterizing pay- ments among men with no names, in Proceedings of the Conference Internet Measurement Conference, Oct. 2013, pp. 127–140. http://dl.acm.org/ citation.cfm?doid=2504730.2504747.
[53] D. Ronand, A. Shamir, Quantitative Analysis of the Full Bitcoin Transaction Graph, Springer Financial Cryptography and Data Security, 2013, pp. 6–24 http://link.springer.com/chapter/10.1007/978-3-642-39884-1_2.
[54] T. Robinson. Bitcoin is not anonymous. http://www.respublica.org.uk/disraeli-room-post/2015/03/24/bitcoin-is- not-anonymous/.
[55] Coinalytics—Blockchain Intelligence. http://coinalytics.co/ accessed on Mar. 15, 2018.

Please cite this article as: Q. Wang, X. Zhu and Y. Ni et al., Blockchain for the IoT and industrial IoT: A review, Internet of Things, https://doi.org/10.1016/j.iot.2019.100081