Proceedings of the 3rd International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/4/20230470

Analysis on issues and challenges of IoT and the solution based on blockchain technology

Sicong Lyu

Jinling Institute of Technology, Nanjing, Jiangsu, China

lsc17851188212@gmail.com

Abstract. With the development of science and technology, the Internet of Things (IoT) has become an area of great influence and potential. However, the deficient data security and privacy problems of the current IoT systems seriously limit its application. This is due to the fact that the information exchange and data authentication in IoT must be done through the central server. In order to solve the fraud possibility of device, false authentication, unreliable data sharing, eliminating the concept of a central server, the block chain (BC) technology was adopted as part of the Internet of things used to improve the above problems. This paper elaborates the component interaction in the Internet of things which bring security and privacy problems, and introduces the existing block chain technology, the application of Internet of things. Various challenges of IoT and IoT with BC as well as future research directions are summarized.

Keywords: Internet of Things, Data Security, Blockchain, Central Server, Record of Data.

1. Introduction

The Internet of things (IoT) is actually on the basis of the Internet, the use of radio frequency identification technology, wireless data communication technology, sensor technology and other technologies to make the original independent existence of equipment connected to each other, and finally realize the intelligent identification, positioning, tracking, monitoring, control and management functions of a network. The Internet of things cannot only realize the information exchange between things, but also realize the information exchange between things and people.

IoT is a innovative application of numerous technologies that would achieve intelligent collaboration, including information processing technologies, wireless communication technologies, electronic actuator and sensor technology, as well as the trending progress in big data analytics and machine learning. The integration of all these technologies can complicate and make it difficult to work with a wider range of larger applications. Due to the complexity of IoT device integration and the distributed nature of network interconnection and its components, everything in IoT relies on a central server for data sharing and authentication. This makes interconnection between devices unreliable and allows attackers to share user data through authentication using false identities.

In the current situation, most of the devices that constitute the Internet of Things are lightweight and low energy consumption, which leads to the implementation of core programs and main functions of these devices will occupy most of the available computing power and energy, so it is difficult to maintain a secure state and protect user privacy under limited conditions. At present, some advanced security

DOI: 10.54254/2755-2721/4/20230470

frameworks are highly centralized, which causes that these security frameworks are often not suitable for the Internet of Things due to its distributed nature, complex scale and many-to-one nature of traffic. Therefore, security and privacy protection applicable to the Internet of Things should be lightweight, scalable and distributed. Blockchain (BC) technology has the potential to solve these difficulties due to its distributed, secure and private characteristics. Therefore, this paper expounds the security and privacy issues in the Internet of Things through qualitative analysis. And look forward to the future development direction through the application of blockchain technology and the Internet of Things.

2. The issues and challenges of IoT

2.1. Security issues and challenges

With the increasing number of devices connected to the Internet, the potential for security vulnerabilities to be exploited is increasing. A network attack enters an IoT device with a security vulnerability and either reprograms the device or invalidates the device[1]. A compromised device cannot provide adequate protection for the data stream, which can result in the theft of user data. In addition, when equipment failure or failure will also lead to the emergence of security vulnerabilities. In order to prevent these dangerous behaviors, appropriate measures must be taken to ensure the safety of equipment.

Maintaining competitive costs and overcoming technical barriers is a big challenge for IoT manufacturers who need to design more comprehensive security features. With the emergence of potential security design flaws, simply increasing the number and attributes of IoT devices may increase the attack probability. In addition, IoT devices are highly interconnected, and every device with poor network-connected security has an impact on the security and resilience of the global Internet, not just the local Internet. Take the United States, for example, an unprotected refrigerator or TV infected with malware may be able to send thousands of harmful emails to recipients around the world via its owner's home's Wi-Fi Internet connection.

To make matters worse, in a hyper-connected world, people may be less able to carry out their daily activities without using Internet services or IoT devices. Lawbreakers are taking advantage of the growing demand for IoT devices and Internet services to gain more access to devices and users' privacy. Once a person is hurt by a cyber attack, he may unplug the TV connected to the Internet, but once he falls victim to a malicious act, he cannot easily turn off the traffic control systems, smart electricity meter or implanted artificial pacemaker.

2.2. Privacy issues and challenges

IoT generally refers to a large-scaled network formed by a number of devices possessing sensors and collecting data from the surrounding environment. The data collected by such networks often contains human information. Compared to data collectors, device users are more concerned about how data is collected and used in the Internet of Things, although these users have different tolerance for the privacy issues that may be caused by the data. Some seemingly secure IoT data streams can also harm users' privacy. By merging or linking individual streams of data together, it is often possible to create a digital portrait of an individual that is more intrusive and accurate than a single IoT stream. For example, when a user's toothbrush is connected to the Internet, it is possible for the toothbrush to capture and send full information about a person's brushing habits and dental health, while at the same time, this user's health-monitoring software or device can submit his exercise data, and the smart fridge at his home can capture his weekly food list and analyze his dietary preferences, a very personal physical health report is presented.

In some cases, users may not even be aware that an IoT device has collected their personal information and transmitted this private information to a third party. A common phenomenon: smart TVS, Internet-connected game consoles, and other home video and video devices are constantly monitoring the sounds and images in the user's room with their own voice recognition and recording capabilities. These devices can upload the data to a cloud server for use by individuals or organizations,

DOI: 10.54254/2755-2721/4/20230470

which may explain why some online shopping platforms are always quick to show what people just said they wanted.

Whatever people's attitudes toward the collection and analysis of their private data, this highlights the value of these streams of private information to businesses and organizations that pursue the collection and use of personal information. The problem of information leakage in the Internet of things poses a challenge to legal and regulatory authorities. Since these privacy issues concern people's fundamental rights and the credibility of the Internet, they must be properly addressed.

2.3. Legal, regulatory, rights issues and challenges

The development of Internet of things devices is changing people's understanding of social lifestyle, which has led to a lot of IoT-related legal and regulatory issues, these issues are very wide-ranging. Creating new laws and policies to address and ameliorate the negative impacts of the Internet of Things is a big challenge, which magnifies many existing problems. For example, for the accessibility of IoT devices for people with disabilities, how the new IoT devices compatible with the original accessibility standards and legal provisions. In addition, with the development of wireless IoT devices, the enormous scale of the devices and the radio frequency (RF) noise and interference caused by them make it more difficult to use the available RF spectrum reasonably. The IoT equipment brings about intellectual property issues, equipment legal ownership issues, and how to protect the environment under the premise of disposal of waste equipment, and so on, are emerging challenges.

2.4. Emerging economy and development issues and challenges

Although the Internet and communications infrastructure has greatly increased in popularity in many developing countries, in some areas there is a significant gap with developed countries in terms of ensuring reliable, high-speed and secure access. The IoT is likely to put pressure on Internet and telecommunications infrastructure and resources to some extent, and current challenges may inhibit opportunities for IoT in emerging regions. In addition, given that wireless technologies underpin many IoT implementations, the need to pay special attention to spectrum management is also a challenge. While cloud services and big data analytics are enabling many IoT services and facilities to take advantage, some emerging economies need to overcome inadequate data center infrastructure to build advanced IoT systems.

3. Blockchain technology and its merits

3.1. The concepts of blockchain technology

Blockchain is a tamper-proof technology based on the ledger, as shown in Figure 1, it is not a newly invented technology, but a latest application style of distributed data storage, point-to-point transmission, the consensus mechanism, the encryption algorithm and other computer technologies[2]. Block-chain is an crucial notion of Bitcoin. It is fundamentally a decentralized database, which has the characteristics of decentralization, tamper-proof, whole-process trace, traceable, collective maintenance, openness and transparency.

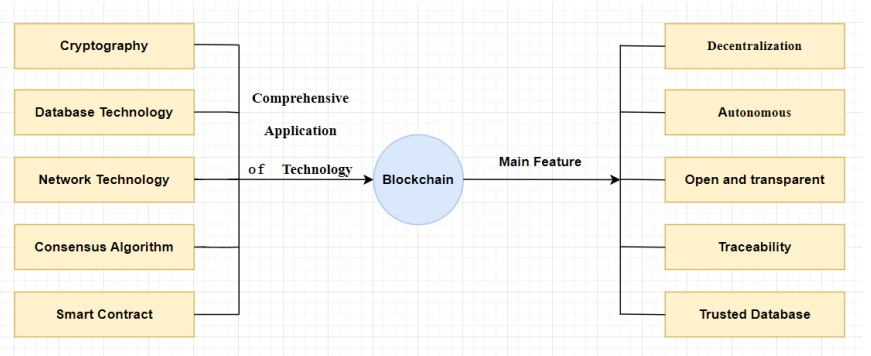

Figure. 1 Main features of blockchain[2].

DOI: 10.54254/2755-2721/4/20230470

*3.1.1. Decentralization.*Blockchain networks do not rely on additional centralized hardware or management agencies, but are maintained by all participants together. Through distributed storage and point-to-point transmission network, the communication between nodes does not need to go through the central node, and each node realizes self-verification, transmission and management of information. So the operation of the network is not affected by any node.

3.1.2. Open and transparent. The so-called openness means that the block-chain is without charge for everyone who wants to join it and acquire the total data. The entire network is extremely transparent, and only the solitary information of each section is proceed. The data account of block-chain and execution rules can be reviewed and trailed by the complete network nodes, with high pellucidity, which is more open than the traditional centralized mode that keeps data in its own database and never makes it public.

3.1.3. Autonomous. The autonomy of blockchain is due to the fact that it is based on norms and protocols. The construction of blockchain system relies on machine trust, which needs to be written into specific mathematical algorithms to establish rules for the system, and each node must abide by this rule and cannot be broken. The rules and protocols adopted in the blockchain are agreed upon, and the data verification and exchange conducted by all nodes will not be affected by human intervention, so every transaction on the blockchain is accurate and true.

3.1.4. Traceability. Data is permanently stored and chronologically generated in the form of electronic records called blocks. A blockchain is blocks put together in a chain fashion, which is why blockchain is traceable.

3.1.5. Information cannot be altered. Information is immutable, which means it's stored permanently on the blockchain once it's verified. Once the transaction information is linked, changes to the database by a single node are ineffective and almost impossible to implement unless everyone agrees or controls more than 51% of the nodes in the system simultaneously. So the information in the blockchain is very secure and can be protected from artificial data changes. Blockchain technology can be used to create credit at a very low cost, which has many advantages through mathematical principles rather than traditional credit institutions. For example, real estate certificates, marriage certificates, degree certificates and other documents notarized on the blockchain are very reliable, not just in a certain region but all over the world.

3.2. Blockchain technology as solution for IoT

Using blockchain technology would be an effective measure to the security and privacy problems of the IoT [2]. Traditional secure computing protocols are very complicated and cannot perform well in large-scale environments due to the complexity of communication and computation, while blockchain has a trusted database, the data account of each node is independent, so the data of the blockchain network will not be affected by any node's data change[2]. The blockchain does not permit any kind of tampering with the available data, but the chain approach can effectively maintain the data recorded in the blockchain in order. This maintained transaction is shared with the network of participating nodes. By using cryptography to identify each node participating in the transaction sharing process, the concept of a central server is eliminated and data is allowed to flow through a blockchain distributed ledger for secure authentication.

4. Blockchain for IoT

4.1. The blockchain approach for IoT

The three main components of IoT are Networked Sensors and Actuators (TNSA), Raw Information and Processed Data Storage (R-IP-DS), and Analytics and Computing Engine (ACE). Many data

DOI: 10.54254/2755-2721/4/20230470

security and privacy issues may arise from the interaction between these three IoT components. When the flow of data from the data acquisition unit (usually something with a network of sensors and actuators), to the information processing and storage unit (usually the original information processing and report status in the form of data storage), the flow of the data on the Internet must be through some agreements, which makes the external impact likely to mislead or distort agreement, Hackers, for example, can control how data is processed. In the interaction between R-IP-DS and ACE, there is a risk that the computing engine could be hacked or controlled by an external user, resulting in an analysis interruption. During the interaction between ACE and TNSA, according to the feedback of the computational algorithm to be sent, the corresponding thing should be acted upon, in this case, hacking and negative control of the feedback loop may arise. In addition, in each individual component, the wrong protocol can cause the data loss. As a result, these serious data security and privacy issues will hamper the development of IoT, and blockchain technology has the ability to solve the problems faced by IoT systems. As shown in Figure 2, in an IoT system, almost all of the collected data is maintained in a central server. If devices want to access data that they must interact with using a centralized network, the data flow occurs through a central server. While most current IoT systems rely on the concept of centralized servers, there is a growing demand for IoT and its applications. In the future, centralized servers will not be an effective approach for large-scale IoT systems. In addition, the sensor devices of IoT systems collect information from centralized objects and transmit the data to a central server via wired or wireless networks, which then performs analysis about user requirements. In order to handle the massive amount of data processed in large-scale IoT systems, it is necessary to increase the amount of Internet infrastructure. The best way to solve these problems is to build a distributed network. Blockchain enables IoT systems to track a large number of connected and networked devices, coordinate transactions between devices, and improve the privacy and reliability of IoT systems due to its support for "peer-to-peer networking (PPN), distributed file sharing (DFS), and autonomous device coordination (ADC)" capabilities. Based on the distributed ledger shown in Figure 2, message passing from point to point becomes faster. In large-scale IoT systems based on blockchain technology, data streams will become more secure. Such systems can record historical operations, old transactions from smart devices, and more personal data. In addition, it has the ability to allow self-direction, distributed file sharing, eliminating single control permissions, and so on. Large-scale IoT systems based on blockchain technology also have economic advantages, reducing the cost of developing large-scale Internet infrastructure.

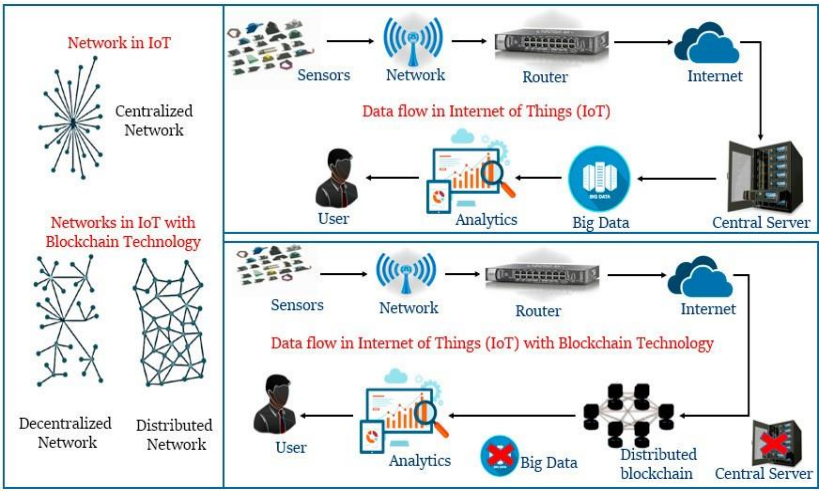

Figure. 2. Data flow in two IoT network types[3].

4.2. Some applications

4.2.1. IOTA. IOTA is an open source decentralized ledger that provides secure communications and payments between machines on the Internet of Things. This platform can use fewer resources to achieve

DOI: 10.54254/2755-2721/4/20230470

high transaction performance, high block validity, and high data integrity[4]. In this way, the problem of the limitation of block chain is solved effectively. The IOTA features tamper-proof data, sense of micro-transactions, and low resource requirements, making it ideal for IoT. IOTA uses a Tangle mechanism. Because of this mechanism, IOTA does not need all nodes to confirm every transaction, but only some nodes can do it, which makes IOTA free of handling fee and extremely fast transfer speed. So for these computing power is not strong, and the number of IoT devices, the payment can be completed quickly. In 2018, the European Commission approved IOTA and the European Smart Cities Alliance to work together to create smart positive energy cities[5]. In addition, IOTA and Volkswagen demonstrated a proof of concept for an autonomous vehicle and announced a partnership with the International Transportation Innovation Center (ITIC) to jointly develop an autonomous vehicle testbed.

4.2.2. IoTeX. IoTeX is an automatically scalable and privacy-centric blockchain infrastructure project. To build a blockchain platform supporting IoT applications with lightweight, private and easily extensible blockchain underlying technology. Founded in 2017 as a Silicon Valley open source project, IoTeX is committed to building the world's leading privacy-centric high-performance blockchain platform[6]. The team consists of PHDS, senior engineers, and experienced ecosystem developers in areas such as cryptography, distributed systems, and machine learning. IoTeX aims to become a trusted computing and application platform for intelligent everything, collaboration and value exchange between developers and people. IoTeX is committed to combining blockchain, trusted hardware and edge computing to achieve trusted interconnection of everything and link the world with blocks.

4.2.3. WTC. On November 30, 2016, the 5th anniversary of the death of Charlie Walton, the inventor of RFID technology. In order to commemorate this great scientist, the project was founded on the same day and officially named Walton chain[7]. Walton chain is an underlying public chain of commercial ecology. As a leader in blockchain IoT, Walton Chain uniquely combines blockchain technology with RFID technology. On this chain, merchants can set up various sub-chain to meet their needs, and monitor the production of all goods, logistics, warehousing and retail process. As a typical business ecological chain, the main feature of Walton chain is to ensure various data (including commodity flow data, property ownership data, etc.) true and credible. Through the self-developed card reader chip and tag chip, all data of offline physical goods in the process of circulation can be automatically and quickly linked, avoiding human interference and minimizing the possibility of data tampering, so as to create a fair, transparent, traceable, real and credible new generation of business ecosystem.

4.3. C Challenges in Blockchain Technology Integrated IoT

Although blockchain technology can overcome the reliability and privacy issues of IoT when integrated with it, the application of blockchain technology to the Internet of Things will also face many challenges, such as the limitation with storage, technological development shortcomings, lack of experienced workforce, lack of appropriate laws, regulations and criteria, computing capabilities, excessive energy consumption and scalability issues. The following are the challenges of the IoT integrated blockchain method.

4.3.1. Scalability. The blockchain has possibility to suspend due to the huge load of the transaction. In 2019, Bitcoin storage capacity has exceeded 197 GB. If IoT is combined with blockchain, then the load issue will be even more serious.

Limitation with Storage: In IoT ecosystem, Sensors and actuators require much less storage capacity than ledger based blockchain technology. In a blockchain, since digital ledgers are stored on every IoT node, this will increase storage capacity significantly and also become a heavy burden on every connected device. This is a very challenging problem.

4.3.2. Lack of skills and skilled workforce. The BC belongs to the category of new technology. At present, few people have a full understanding of this technology. Therefore, when this technology is applied to

DOI: 10.54254/2755-2721/4/20230470

the field of the Internet of Things, a lot of training is needed to improve the cognitive and technical ability of employee.

4.3.3. Rules and regulation. The IoT-BC will work on a global scale, so implementing this approach on a global scale will require facing different regional laws and regulations. In addition, blockchain technology has not had any legal norms to follow until now, which is one of the most challenging issues to solve.

4.3.4. Computing capabilities. As the IoT system is characterized by diversity and connectivity through a large network, the situation will become more and more complex with the integration of blockchain technology. This is a challenge to the computational power of the algorithms when it comes to running the encryption of everything connected to blockchain-based IoT systems.

5. Conclusion

Disruptive technologies have always been hugely controversial. Although many people are skeptical about blockchain technology, there is no denying that it is a major technological revolution that can solve the existing problems of the Internet of Things. This paper analyzes the main problems and challenges that the Internet of Things must solve, and also introduces blockchain technology and its application in the Internet of Things. Blockchain is expected to radically improve data security and privacy issues in the Internet of Things, and the integration of these two technologies will greatly boost the development of blockchain and the Internet of Things. It concludes with an overview of possible future challenges, more research to be done. Future research should aim to determine which IoT applications are best suited for implementing blockchain-based security mechanisms at a practical level, and how to implement IoT-enabled distributed ledgers (databases) in the best way.

References

[1] Karen Rose, Scott Eldridge, Lyman Chapin (2015). The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World. The Internet Society (ISOC). 34-71.
[2] Liu, YiHe; Zhang, Shuang (2020). Information security and storage of Internet of Things based on block chains. Future Generation Computer Systems, 106, 296–303. 4-5.
[3] Kumar, Nallapaneni Manoj; Mallick, Pradeep Kumar (2018). Blockchain technology for security issues and challenges in IoT. Procedia Computer Science, 132, 1815–1823. 3-5
[4] Tanweer Alam. Blockchain and its Role in the Internet of Things (IoT). International Journal of Scientific Research in Computer Science, Engineering and Information Technology. Vol 5(1), 2019. 4-5.
[5] IoTa.org, https://www.IoTa.org/
[6] /IoTex.io, https://IoTex.io/
[7] WTC(waltonchain.org), https://www.waltonchain.org/#/