ISSN: 2472-3703 DOI: 10.6911/WSRJ.201910_5(10).0013

Application Status of Blockchain in Internet of Things

Zhiring Tang[1, a]

[1]College of Nuclear Technology and Automation Engineering, Chengdu University of Technology, China

[a]zhirong_tang_1993@126.com

Abstract

In 2008, the concept of blockchain was first proposed by Nakamoto Satoshi, and in the following years, it became a core component of electronic currency bitcoin. With the development of social economy, the Internet of Things model stands out. However, more and more networked devices make the traditional business model insufficient to support its operation. In order to solve this problem, people have turned their attention to the blockchain. However, the blockchain technology is still not mature enough, and it is in the bottleneck of development. This paper briefly summarizes the current status of the blockchain application in the Internet of Things. The future of the Internet of Things will be one of the most closely related areas of cooperation with the blockchain.

Keywords

Blockchain; P2P; Internet of Things; imperfection.

1. INTRODUCTION

With the rapid development of the social economy, the whole world is becoming more and more digital and enters the sea of data through the Internet [1-3]. This also provides opportunities to create wealth while making our lives more convenient. However, what followed was the security of the data. In order to solve this problem, the blockchain was mentioned. The blockchain is essentially a decentralized database, which is an important concept of Bitcoin. The fire currency is combined with the Internet Finance Lab of Wudaokou Finance College of Tsinghua University and the “2014-2016 Global Bitcoin Development Research Report” issued by Sina Technology. The blockchain is the underlying technology and infrastructure of Bitcoin.

Blockchain is a distributed timestamp server technology used to implement bitcoin in P2P (peer-to-peer) digital cash systems, and cryptographically guaranteed non-tamperable and unforgeable distributed ledgers [4]. Use blockchain data structures to validate and store data, use distributed node consensus algorithms to generate and update data, use cryptography to secure data transfers and access, and use smart contracts composed of automated script code to program and operate A new distributed infrastructure and computing paradigm for data [5-8].

Since 2009, various kinds of bitcoin-like digital currencies have emerged, such as bitcoin, litecoin, dogecoin, OKcoinetc. In addition to the application of currency, there are also various derivative applications, such as Ethereum, Asch and other underlying application development platforms, as well as NXT, SIA, bit shares, MaidSafe, Ripple and other industry applications. Based on the public block chain. Public block chain means that any individual or group in the world can send a transaction, and the transaction can be effectively confirmed by the block chain, and anyone can participate in its consensus process. Public block chains are the earliest and most widely used block chains. The virtual digital currencies of bitcoins series are all based on public block chains. There is only one block chain corresponding to this kind of currency in the world [9-10].

Although Bitcoin is a controversial form of digital currency facing suspicion and distrust, its legal, social and economic impact has not been fully studied, so embedded technology has advantages in recording transactions. Block chains are based on currencies such as Bitcoin, but they can also be used in many other financial and commercial applications, such as agricultural and sideline industries, art industries, legal industries, insurance industries and so on. Among them, the application of block chains in the Internet of Things has great potential. In the future, the Internet of Things will be the most sparking area with block chains [11-13].

This article gives an overview of blockchain technology in Section 2. In Section 3, the application of block technology in the Internet of Things, in Section 4, the immature and measures of block-joining techniques are proposed, which are summarized in Section 5.

2. INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

Since blockchain technology is a P2P transaction and there is no supervision by a third-party central organization, a series of effective measures are proposed for the security and trust of blockchain transactions.

2.1. Distributed Ledger

The distributed ledger stores all past transactions. Consensus between blockchains means providing a protocol that can provide a unique status of the ledger verified by the system participants. Any node with an Internet connection can add blocks to the blockchain network and must have a protocol to provide a consistent view of the records to avoid confusion. In the blockade jargon, the "miner" is a blockchain network node that has the effect of verifying new transactions. When the miner validates the transaction, it places it in a new block that will be broadcast to other nodes in the network. Transaction accounting is done by multiple nodes distributed in different places, and each node records the complete account, so they can participate in supervising the legality of the transaction, and can also testify for it. Unlike traditional centralized accounting schemes, no single node can record accounts separately, thus avoiding the possibility of a single biller being controlled or being bribed to account for false accounts. On the other hand, since there are enough billing nodes, in theory, unless all the nodes are destroyed, the accounts will not be lost, thus ensuring the security of the account data.

2.2. Consensus Mechanism

The consensus mechanism is an algorithm for reaching a distributed consensus on blockchain transactions. It is a means of determining the validity of a record between all accounting nodes, which is both a means of identification and a means of preventing tampering. The blockchain proposes four different consensus mechanisms, which are applicable to different application scenarios, and strike a balance between efficiency and security. They are: workload proof, equity certificate, share authorization certificate mechanism, and small ant consensus algorithm. In the case of Bitcoin, the proof of the workload is used. In short, many nodes independently pass the ledger and they compete to first find a specific keyword, an identifier that can quickly verify it. Proof is a probabilistic iterative process, thus reducing the chance of generating blocks at the same time. Only when the accounting node of the whole network exceeds 51% is controlled, it is possible to forge a record that does not exist. This is basically impossible when there are enough nodes to join the blockchain, thus eliminating the possibility of fraud.

2.3. Smart Contract

Smart contracts are often considered an automated guarantee account and web server that can automate the execution of pre-defined rules and terms based on these trusted, non-tamperable data. In the case of insurance, if everyone's information (including medical information and risk-generating information) is authentic, it is easy to automate claims in some standardized insurance products.

2.4. Asymmetric Encryption and Authorization Technology

The transaction information stored on the blockchain is public, but the account identity information is highly encrypted and can only be accessed if authorized by the data owner, thereby ensuring data security and personal privacy.

3. PROBLEMS SOLVED BY BLOCKCHAIN IN THE INTERNET OF THINGS

3.1. Introduction to the Internet of Things

The Internet of Things is an interconnected object and a human world network that can interact with each other through unique addressing schemes and work with neighbors to achieve common goals. The main purpose of the Internet of Things is to share information about objects and provide a network of many physical objects connected to the Internet. These devices obtain information about the surrounding environment and communicate with the software system via the Internet. As a result of this rich interaction, they also generate a lot of data, which in turn can be used to enable dependent services.

With the continuous advancement of technology, the development and application of Internet of Things technology has achieved remarkable results in recent years. Currently, billions of sensors and intelligent controllers have been put into use worldwide, and this number is expected in the next few years. It will also grow exponentially. However, IoT technology also faces many problems and challenges, which may become a huge obstacle to the future development and application of the Internet of Things, and blockchain technology provides the possibility to solve these problems.

At present, there are many mature technology companies and startups that have been exploring these applications. They invest and do a lot of research on various solutions that might take advantage of the technology, the most famous of which is IBM. IBM was one of the first companies to announce their plans for the blockchain development. It has established several partnerships at several different levels and demonstrated their love for blockchain technology. It has published a report that points out that blockchain can be the best solution for the Internet of Things. In January 2015, IBM announced a project, the ADEPT project, a research project using P2P blockchain technology. IBM also established a proof-of-concept system with Samsung for the next generation of IoT systems based on IBM's ADEPT (autonomous decentralized peer-to-peer telemetry), which consists of three elements: Ethereum, Telehash and BitTorrent. Using the platform, both companies want to bring a device that automatically detects problems, updates automatically, and does not require any human intervention. These devices will also be able to communicate with other nearby devices to power the battery and save energy.

3.2. Reduce the Operating Costs of the Internet of Things

With the further application of IoT technology, the management and maintenance of hundreds of billions of IoT devices will bring huge cost pressures to manufacturers, operators and end users. The current IoT applications are basically based on a centralized architecture, that is, all data streams are aggregated into a single central control system. Although with the popularity and utilization of cloud computing technologies, IoT operators can now pass the cloud. The server cluster provides storage and exchange services for data generated by IoT smart devices. However, as the number of connected devices grows geometrically, the computational, storage, and bandwidth costs of centralized services will increase to an unaffordable level.

By using blockchain technology, IoT devices of different owners can transmit data directly through an encryption protocol, and can perform billing and settlement of data transmissions according to transactions. This requires designing an encrypted digital currency as the basic unit of transaction settlement in the IoT blockchain. All IoT device providers can add the blockchain support to the device before leaving the factory. Direct currency settlement between different operators.

3.3. Solving the Privacy Protection Problem of the Internet of Things

With the continuous development of the Internet of Things industry, the issue of data security and privacy protection has received increasing attention. After the Snowden incident, the privacy of web services controlled by governments and large corporations was widely questioned. Especially in the field of Internet of Things, the current centralized service architecture stores and forwards all monitoring data and control signals from a central server. While IoT operators have consistently claimed that they can effectively protect users' data security and privacy, a series of security breaches and privacy breaches have made it impossible for users to truly trust operating service providers to fulfill their promises. Directly affect the daily life of users.

Blockchain technology provides the possibility of decentralization for the Internet of Things. As long as the data is not controlled by a single cloud service provider, and all transmitted data is strictly encrypted, the user's data and privacy will be even more Safety. Today, when big data analytics technology is widely used, users can use the value of the data themselves instead of being hijacked and outsourced by the operator.

3.4. Building A New Business Model Using Blockchain

In 2009, Osterwalder and Pigneur proposed a framework called “Business Model Canvas” in [13], and then Bucherer and Uckelmann combined the characteristics of the Internet of Things based on the framework. They then innovatively analyze business model canvases by integrating physical entities, IoT devices, and big data into four large blocks—infrastructure, value proposition, customers, and finance. In addition, they provide solutions for each block that corresponds to the Internet of Things. But there is no new model designed specifically for IoT conditions, and the potential of the block on the Internet of Things cannot be fully achieved. So our work is worth exploring.

The current collaboration and transaction of IoT devices can only be carried out under the same trust domain. In the future, the Internet of Things will not only connect devices together to complete data collection, but also collaborate independently under the given rule logic to complete various businesses. The application of value. The equipment connected to the Internet of Things can be intelligent.

3.5. Firmware Upgrade

According to Gartner's report, the Internet of Things era will transform our lives through network-connected IoT devices. By 2020, the number of IoT devices is expected to reach 25 billion, and the number will continue to increase. In [10], the authors mentioned that due to the increasing number of devices connected to the Internet of Things, the resources and capabilities of embedded devices are limited, and embedded devices have not yet applied strong security features. Many vulnerabilities in embedded devices are reported every day, and a new intrusion method has emerged on the Internet to invade embedded devices by using embedded devices.

In [10], a new firmware update scheme using blockchain technology is proposed. In the proposed solution, the embedded device requests its firmware update to block the chain nodes on the peer-to-peer distributed network. It then receives the response from the blockchain node to determine if its firmware is up to date. When the firmware is not up to date, the embedded device requests the metadata file to download the latest firmware from the peer firmware sharing network consisting of blockchain nodes. Even if the firmware version is up to date, the firmware integrity is checked through the blockchain node. Therefore, the proposed solution guarantees the correctness and up-to-dateness of the embedded device firmware in the Internet of Things era.

4. IMPERFECT BLOCK TECHNOLOGY

4.1. Blockchain Suitable for the Internet of Things

In Chapter 1, the consensus mechanism of the blockchain was introduced, and it was only possible to forge a non-existent record if it controlled more than 51% of the accounting nodes in the whole network. If the new blockchain of the Internet of Things is re-established, since the block generation time is relatively long, the stability of the blockchain and the security are weak and vulnerable to attack. Therefore, our proposal is not to design a new blockchain from scratch, but to develop distributed applications for the Internet of Things on a secure and stable blockchain. This can be done by leveraging a layered architecture. Among them is the proof of work and a large number of honest miners to ensure integrity and to avoid misbehaving miners gain most of their computing power.

So is the bitcoin block suitable? In [8], the author believes that the deployment and implementation of Bitcoin blockchain technology requires the participation of multiple nodes. Under the conditions of the Internet of Things, the computing power of each smart device is very limited, and the traditional blockchain is digging. Compared to mine nodes, its Hash computing power is even less than one-thousandth of that of GPU systems. In addition, the power consumption of IoT devices is also a problem that is strictly concerned in practical applications. Therefore, it is impossible to directly apply the existing blockchain technology to the application of the Internet of Things.

4.2. Key Security

A major feature of blockchain technology is that it is irreversible and cannot be forged, but only if the private key is safe. The private key is generated by each user and is responsible for the custody. In theory, there is no third party's participation, so once the private key is lost, it cannot do anything with the assets of the account. And in order to ensure the security of the blockchain, with the current computing power and technology, it is absolutely impossible to reverse the private key from the address. If feasible, all addresses on the entire blockchain lose security, and the assets on the blockchain lose their meaning.

4.3. Network Delay

In [11], the authors suggest that network out-of-synchronization is also one of the causes of block-connected anomalies. This dramatic anomaly caused by network delays can lead to repeated consumption attacks, that is, converting all coins into goods twice. More specifically, blockchain anomalies depend on the wrong commitment state of the blockchain. Once the status of the false promise is not submitted, there is no way to observe the problematic state a posteriori and there is no way to confirm the problem. The authors suggest that the prevention of anomalies depends entirely on the programming of smart contracts, and the irregularities that may arise when rearranging newly generated and reordered are written to the smart contract for exclusion.

4.4. Anonymous Fraud

The anonymity of the block system is like a double-edged sword, which brings convenience to some scams. Although blockchain technology can prevent fraud, it cannot detect fraud itself. Hackers may find unpredictable ways to steal money and swindle. In [], the authors propose techniques and methods that require innovation to detect attacks. Existing techniques using machine learning and data mining algorithms may find new applications in detecting fraud and intrusions based on blockchain transactions. By monitoring and detecting behavior patterns based on analysis of people's transaction history, and supervising machine learning methods such as deep learning neural networks, support vector machines and Bayesian belief networks can help detect abnormal behavior.

5. CONCLUSION

In this paper, block chain technology and its application in the Internet of Things are briefly introduced. Block chain can solve the operation cost, privacy protection and open a new business model for the Internet of Things. Some imperfections of block chains and bottlenecks in the development of block chains in the Internet of Things are also listed. In the future, our update speed will be greatly improved, which is reflected in some online games, such as warship world point-to-point update data. The development and application of Internet of Things technology has achieved remarkable results. Billions of sensors and intelligent controllers have been put into use worldwide by now. It is expected that this number will double in the next few years. The future of the Internet of Things must be promising. It will subvert the basic structure of the existing industry and allow hundreds of billions of devices in the world to collaborate automatically. The cooperation between block chains and the Internet of Things will solve the problems of the Internet of Things more fundamentally and bring more possibilities to the Internet of Things.

REFERENCES

[1] Mauro C, Kumar E S , Chhagan L , et al. A Survey on Security and Privacy Issues of Bitcoin [J]. IEEE Communications Surveys & Tutorials, 2018, Vol. 20 (4), 3416 - 3452.

[2] Wang H, Chen K , Xu D . A maturity model for blockchain adoption [J]. Financial Innovation, 2016, Vol. 2(1), p12.

[3] Mukhopadhyay U, Skjellum A , Hambolu O , et al. A brief survey of Cryptocurrency systems[C]// Privacy, Security & Trust. IEEE, 2017.

[4] Bozic N, Pujolle G , Secci S . A tutorial on blockchain and applications to secure network control-planes[C]// 2016 3rd Smart Cloud Networks & Systems (SCNS). IEEE, 2016.

[5] Tian F. An agri-food supply chain traceability system for China based on RFID & blockchain technology[C]// 2016 13th International Conference on Service Systems and Service Management (ICSSSM). IEEE, 2016:1-6.

[6] Zhu H, Zhou Z Z . Analysis and outlook of applications of blockchain technology to equity crowdfunding in China [J]. Financial Innovation, 2016, 2(1):29.

[7] Xu, Jennifer J. Are blockchains immune to all malicious attacks? [J]. Financial Innovation, 2016, 2(1):25.

[8] Aitzhan N Z, Svetinovic D. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams [J]. IEEE Transactions on Dependable & Secure Computing, 2016, Vol. 18(5), 840 - 852.

[9] Conoscenti M, Vetrò A, Martin J C D. Blockchain for the Internet of Things: A systematic literature review[C]// Computer Systems & Applications. 2017.

[10] Lee B, Lee J H . Blockchain-based secure firmware update for embedded devices in an Internet of Things environment [J]. The Journal of Supercomputing, 2016.

[11] Natoli C, Gramoli V. The Blockchain Anomaly [J]. 2016.

[12] Zhang Y, Wen J. The IoT electric business model: Using blockchain technology for the internet of things [J]. Peer-to-Peer Networking and Applications, 2017, Vol. 10(4), 983-994.

[13] Samaniego M, Deters R . Blockchain as a Service for IoT[C]// 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2017.