Review on the principle, Progress and Application of Block chain Technology

Yipeng Xu¹, Kexin Guan², Lei Lei³

¹School of Mathematics and Science, TianGong University, Tianjin, China
²College of Information Engineering, Sichuan Agricultural University, Ya'an, Sichuan, China
³School of Computer Science, Wuhan University, Wuhan, Hubei, China

Abstract-In recent years, electronic currencies such as bitcoin have been favored by people. As the core technology of Bitcoin, blockchain has attracted the attention of more and more experts and scholars at home and abroad. The changes of its classification mode, service mode and application requirements lead to the diversified development of core technology forms. Blockchain is a distributed ledger technology, which evolves into a complete storage system based on logic control functions such as intelligent contracts. Block chain technology is based on decentralized point-to-point transmission network, using cryptography principles and consensus mechanism to ensure the coherence of each node participating in the distributed system, and to ensure the accuracy, consistency, non-tampering or deletion of the recorded information. All these ensure the establishment of a sharing system with high privacy, high security and high efficiency. In this paper, the basic principles and characteristics of blockchain technology are analyzed, and the research status and application of this technology in the financial system are summarized in detail.

1. Introduction
In 2008, Satoshi Nakamoto put forward the concept of "blockchain" in the Bitcoin White Paper, and established the Bitcoin network in 2009, developing the first block-the "founding block". It uses encryption technology to achieve decentralized effective data currency and online payment system, and the blockchain technology that serves it is equivalent to a public ledger recording bitcoin transactions that have taken place throughout the network.[1] From the beginning of blockchain 1. 0-digital currency (currency transfer, exchange and payment systems), blockchain 2. 0-contracts (smart assets and contracts), to the current blockchain 3. 0-digital society (beyond monetary, financial, and market applications), this new technology is rapidly gaining recognition around the world. By the end of 2016, there were nearly 500 blockchain startups around the world, attracting a total investment of US $1.8 billion. Goldman Sachs partnered with other investment firms to inject $50 million into Circle bitcoin to carry out blockchain technology reserves and exploration research. In December 2015, the Nasdaq Stock Exchange, one of the world's leading financial institutions, launched Linq, a securities trading platform based on blockchain technology, and completed its first secure transaction on December 30, a milestone in the decentralization of global financial markets. In April 2016, Microsoft announced that it would work with the R3 Alliance to study and develop a global framework based on blockchain technology, and launch Blockchain asa Service services on Microsoft's cloud service platform Azure. In June 2017, in the 13th five-year Development Plan of Information Technology in China's Financial Industry, issued by the people's Bank of China,
Blockchain technology, artificial intelligence and big data cognitive analysis were also listed as "major tasks and key projects" during the 13th five-year Plan period[2].

Blockchain technology has not only become the focus of global attention, but also developed into a frontier field of academic research. This paper makes a systematic literature review on the research situation of this technology at home and abroad. Through screening, 58 closely related literatures are found, which can be roughly divided into three categories according to related fields-financial infrastructure change, Internet of things and smart city, which will be classified and summarized in the following sections.

2. The principle and characteristics of blockchain

Blockchain is a new application technology which uses distributed data storage, point-to-point direct transmission, uses consensus mechanism to connect nodes in the network, and uses encryption algorithm to ensure accuracy. This technology solves the problems of "trust" and data storage. In a narrow sense, it is a kind of chained data structure which combines the data blocks in a sequential way according to the time order, and ensures that it can not be tampered with and can not be forged in the way of cryptography. In a broad sense, it is the use of block chain data structure to verify and store data, the use of distributed node consensus algorithm to generate and update data, the use of cryptography to ensure the security of data transmission and access, and the use of automated script code, a new distributed infrastructure and computing paradigm for programming and manipulating data.

2.1. The principle of blockchain

In 1982, Leslie Lambert and others raised the question of Byzantine generals-how to ensure the correctness and consistency of the transmission of information content in distributed systems, and how to accurately identify the participants of malicious sabotage? this is the basic problem in peer-to-peer information communication. The emergence of blockchain technology solves these problems. Any node in the network can participate in the mining of new blocks. Hashing and Merkle tree value algorithms are used to simplify and sort out the unrecorded transaction data in the system broadcast. Through the workload, it is proved that the consensus mechanism of (POW) gets "bookkeeping rights", so that the new blocks are successfully connected to the main chain, and the results are published throughout the network. In turn, Bitcoin was awarded as a reward for the success of this verification. Blockchain technology makes use of the consensus mechanism of workload proof in the distributed system where the decision-making and inspection rights are highly dispersed, so that any node in the network has the right to participate in mining, which ensures fairness and fairness; and because each node is independent of each other, if a node is attacked or maliciously destroyed, it will not affect the whole system.

2.2. Features of blockchain

First, decentralization is the most basic feature of blockchain technology, which no longer relies on the central processing center to build the trust relationship between nodes, and at the same time breaks...
away from the intervention of third-party institutions, and uses distributed storage to delegate rights and obligations to each participating node, and the damage or loss of any node will not affect the operation of the whole network. Second, de-trust and transparency are also important features of this technology. The whole network uses distributed accounting, operating rules and information data are open to the whole network and maintained by all nodes, and its system uses open source programs to allow participating nodes to edit and adjust, so the nodes in the network can trade safely without knowing each other. Third, anonymity, there is no need for trust between nodes, so there will be no need to disclose the relevant information of each node. And for the transmission of private information or data, an asymmetric encryption algorithm is used to protect its security, and only a pair of matching public keys and private keys can unlock the encrypted content. Finally, this feature cannot be tampered with or deleted. Once the transaction information is verified and added to the main chain, it will be permanently saved and cannot be modified, maliciously tampered with or deleted. It is precisely because blockchain technology has so many characteristics and advantages that it has been widely used in different fields, such as finance, medicine, public security management, traffic governance, food safety and so on.

3. Application of blockchain technology

3.1. Financial infrastructure changes

Financial infrastructure refers to the hardware facilities and institutional arrangements in financial application, including payment and clearing system, corporate governance, accounting standards, reputation system and financial supervision. The development of financial infrastructure can promote larger and more efficient accumulation of industrial capital, thereby enhancing the ability to withstand external shocks[3].

In terms of payment and settlement systems, with the development of Internet, Internet of things, cloud computing and blockchain technologies, payment methods around the world are also undergoing great changes. Friedrich (2017) and others proposed that blockchain technology affects the financial structure of the payment industry and makes the traditional business model begin to reform. By using blockchain technology, peer-to-peer transactions can be carried out directly without a third party as a "trust agent", which improves the payment methods of P2P transactions, cross-border transactions and cross-currency transactions. Nguyen (2016) et al. analyzed the use of the characteristics of blockchain to reduce payment costs, make the transaction payment process completely transparent, and improve the execution speed and efficiency of transaction payment. Automatic recording and monitoring of information in the process of transaction payment makes the purpose and destination of remittance or payment clearer and helps to combat financial crimes such as money laundering. Chen Qiyan (2016) proposed that blockchain technology can improve the automatic accountability of the system and effectively reduce the trust risk of the payment system, which is of great significance to optimize the business processes of financial institutions and improve their competitiveness.

In the aspect of financial transactions, blockchain spontaneously produces credit value in the decentralized system, which enables the financial market to establish a management mechanism of non-central endorsement institutions, so as to achieve "financial disintermediation". This has a subversive impact on the existing business models such as third-party payment and fund trusteeship. In the Internet, blockchain technology is widely used in the business model of financial transactions, such as equity crowdfunding, network lending, Internet insurance, securities or banking business. Zhu (2016) and others studied the existing defects and problems in China's traditional crowdfunding market, and proposed to use blockchain technology to establish an equity crowdfunding platform to simplify the trading and transfer procedures of crowdfunding stocks; so that investors and entrepreneurs can conduct peer transactions to solve the problems of compliance and fund management security. Yermack (2015) pointed out that blockchain technology provides a new way to trade and track the ownership of financial assets, using this technology for stock listing, trading and
voting and other activities, shareholders can benefit from lower transaction costs, faster trading speed, more accurate records and higher transparency.[4]

3.2. Internet of Things
The Internet of things is an innovation based on the Internet. The information contained in the Internet of things can make us have a better understanding of the surrounding environment. However, the old business model has been difficult to meet the requirements of the current e-commerce model. The current Internet of things system usually takes the cloud as the center, which will not only have the impact of network delay, but also have the side effect of mutual constraints between sensors and actuators. Samaniego (2017) and others evaluated the effective means of using blockchain technology to permanently store data and related code, which can better store data in Internet of things devices more effectively and securely.

In the decentralized Internet of things system, blockchain technology establishes an infrastructure to promote the cooperation between transaction processing and interactive devices, and realizes the operation flow between machines. It solves the security problems in the traditional business model of the Internet of things, such as high cost, lack of trust, information leakage and so on. Let each block play its role, so that the scale of the Internet of things continues to expand, while ensuring privacy, security, efficiency and untrusted transactions in the network, so as to form an intelligent, decentralized autonomous Internet of things network, really let the Internet of things link everything.

3.3. Smart city
Smart city is an integrated system. It is not only a network city, but also a digital city and an information city. Smart cities are the combination of the Internet of Things and the Internet, through the rapid calculation, analysis and processing of data, so as to perform real-time on the participants, equipment and infrastructure in the network, especially the public industries such as transportation, energy, commerce, security or medical Monitoring and management.

Health care data is the basis of health care intelligence, and data sharing is an important link to make the medical and health system more intelligent and the quality of health care service higher. Xiao Yue (2016) and others believe that using APP-HDG healthcare database based on blockchain technology to store and record patient-related data does not rely on the intervention of a third party, so as to reduce the risk of disclosure of patients' private information and enable patients to easily and safely own, control and share their own data. Having massive and complete medical care, big data will speed up the progress of research and development, quickly understand the models and trends of controlling public health and diseases, and provide help for overcoming more incurable diseases.

Intelligent Transportation system ((Intelligent Transportation Systems,ITS) is a comprehensive application of advanced science and technology to transportation, service management and vehicle manufacturing to strengthen the relationship among vehicles, roads and participants, so as to form a safe, efficient, environmentally friendly and energy-saving comprehensive transportation system. Yony Yuan (2016) designed a seven-layer conceptual model for intelligent transportation system, proposed a research framework of intelligent transportation system based on block chain, and mainly studied the relationship between B2ITS (block-chain-base intelligent transportation systems) and PTMS (parallel transportation management system).

In the new energy-saving society, consumers should be turned to producers. Green (2017) and others introduced that micro-power companies use block chain technology to buy the remaining electricity to the users who need it, so as to save the cost of power generation. At present, some power companies support and are using blockchain technology to trade electricity and manage payment systems. The use of blockchain technology will change the way electricity is produced, consumed and traded, and promoting this transformation can bring significant economic advantages to cities. Janusz (2017) and others believe that blockchain technology can change the engineering industry by promoting the transformation and operation of industry 4.0, and propose that the use of blockchain can promote M2M (machine-to-machine) interaction and establish M2M power market under the
background of chemical industry and Internet of things. Power producers (surplus) and power consumers trade independently in the network, so as to improve the full use of electric energy and save resources.

4. Existing problems and hidden dangers of blockchain technology

With the rapid development and popularization of Bitcoin in recent years, the research and application of blockchain technology in various fields has also shown an explosive growth trend, especially in the financial field is a brand-new reform. such as monetary or financial asset settlement, payment systems, intelligent contracts and risk management in the financial market and so on. However, there are still some limitations and problems to be solved in blockchain technology.

4.1. Safety problem

(1) 51% attack problem. Decentralization is the main feature of the distributed ledger system, so all kinds of malicious attacks pose a threat to the security of the blockchain. Among them, the 51% attack problem based on POW consensus algorithm is the most important. When the malicious attack nodes of the whole network hold 51% of the total computing power, they can launch attacks on the whole network and maliciously tamper with or delete the total ledger. Alireza (2015) et al believe that although the block chain is designed as a completely decentralized network, the distribution of market mining rights centers by several large mining areas increases the risk of attack by 51%. Eyal et al. (2014) introduced a selfish attack in a mining area in which miners involved in mining will receive more than their fair share of income, so they will attract a large number of miners to join and privatize the new blocks they have discovered, thus increasing the total power of calculation and generating 51 per cent risk of attack.

(2) the problem of anonymity. For the security and privacy of the information recorded in the protected block chain, the designer uses cryptography to encrypt the content of the transmitted information, and only the parties with a complete set of public and private keys can unlock the encrypted content. Crosby et al. (2016) explained that although the cryptographic principles used in the current blockchain seem indestructible, there is no third party to help retrieve the key if the key is acquired or stolen. And with the advent of quantum computing, encryption keys may be quickly cracked, thus destroying the foundation of the block chain. Chen (2017) et al proposed to anonymize the transaction system by using information that is not directly related to the system, such as the number of identity transactions and the timestamps sent and received.

4.2. Disadvantages of the consensus mechanism

The commonly used POW consensus algorithm mechanism in blockchain technology highly depends on the computing power contributed by participating nodes in the network to solve the SHA256 mathematical problem. Since only a valid new block can be generated among many competing nodes, other resources consumed by the participating nodes are "wasted", and a lot of power resources are also wasted.

King (2012) proposed a new work proof mechanism-ownership proof mechanism (proof of stake, POS), which can effectively improve the shortcomings of POW consensus algorithm. The holder of Bitcoin consumes the age of the currency he owns to gain the right to generate new blocks. The more money is consumed, the more likely it is to obtain bookkeeping rights. Compared with POW, POS mechanism does not need to consume a lot of resources and energy, and can better save the cost of mining.

4.3. Efficiency problem

Efficiency is also one of the urgent problems to be solved in blockchain technology. In the blockchain network, only one transaction can be processed per second, and the theoretical maximum can only handle 7 transactions per second, while the VISA credit card network can handle up to 10,000 transactions per second, and Twitter can process 15,000 transactions per second. The second is the
confirmation time of new transactions, the generation time of a new block is 10 minutes, so the confirmation waiting time of transactions is about 10 minutes, which limits the application of blockchain technology in small transactions and short-term transactions to a great extent.

4.4. Regulatory policy
At present, there is not a complete standardized rule or policy at home and abroad to manage and supervise the use of blockchain technology. In order to promote the orderly and long-term development of the application of blockchain, the use standard of blockchain should be issued as soon as possible. Relevant organizations and legislatures should understand and investigate the operating mechanism of blockchain technology and its impact, and more pertinently formulate relevant regulatory policies and regulations to manage the use of new technologies, so as to improve the security and reliability of emerging technologies, so as to better serve the public and create new business models and applications.

5. Future development direction and suggestions of blockchain technology
(1) Industry interconnection and data sharing-new P2P online loan model
With the rapid improvement of computer processing power, the Internet has generated massive amounts of user network behavior data in daily operations. These data are huge in scale and various in variety, but there is huge value hidden in them waiting to be mined. Online lending, also known as P2P online lending, a typical model is to provide a service platform for online credit companies, where both borrowers and borrowers bid freely and finally reach a deal. The application of blockchain technology will change the traditional operation mode of the online loan industry and replace the role of an intermediary online loan platform, so that the borrower and lender can directly conduct transactions, thereby improving transaction efficiency and information transparency, and reducing costs and fraud risks.

(2) Reshape the operation mode of accounting, auditing and other industries
In the traditional accounting industry, there are some phenomena, such as accounting information distortion, subjective bias and even financial report fraud, while in the audit industry, there are a series of problems, such as complicated audit document processing, long time delay, lack of verification of the authenticity of the audit report, and so on. With the embedding of blockchain technology, companies no longer need to hire professionals to audit the books internally, and all transactions can be recorded in the blockchain. Whether accountants, auditors or regulators can manage and monitor the company's books in real time by tracking the progress of the blockchain. This not only reduces the audit dependence on auditors, but also improves the efficiency of business management. The new operation mode of accounting, auditing and other industries has changed the traditional mode of manual recording of paper-based account books, which not only provides a reliable guarantee for the transaction records of economic activities, but also reduces the investment of manpower and material resources. It saves time and cost, and reduces the probability of illegal events.

(3) Change data acquisition methods and promote academic research
For academic research, the acquisition of data is very important, not only requires the quantity of data but also to ensure its quality. The data recorded and stored by blockchain technology have a high degree of credibility and transparency, which ensures the authenticity of the data used in scientific research. With the in-depth application of this technology in the financial field, blockchain will become the preferred trading platform for consumers, and the recorded data will effectively and truly reflect the behavior orientation of investors, thus greatly promoting the related research of the financial industry.

(4) Implement and promote relevant management standards and policies
On August 1 this year, the National Committee of experts on Internet Financial Security Technology issued the guidelines for Compliance Blockchain in view of the current research and development of blockchain technology and the existing problems, which includes four parts: an overview of blockchain, the necessity of compliance blockchain, guidelines, summary and prospects
for compliance blockchain. The guidelines not only analyze the research progress of blockchain technology in detail, but also put forward methods and suggestions for its regulatory level. Moreover, more detailed regulatory policies can be formulated for different types of blockchain structures. For example, institutions using alliance chains can consult and coordinate with each other, improve or improve the management and supervision system according to the relevant information or characteristics of the participants in the alliance; when using private chains, you can set conditions for participation or exit restrictions, and adjust the corresponding management plan according to different circumstances.[5]

(5) Development of blockchain technology application-digital currency

Digital money does not rely on any physical objects, but through cryptographic technology and various algorithms to create, circulate and maintain a virtual currency, it can allow two independent individuals to initiate and complete transactions through the Internet. At present, there are nearly 700 digital currencies in the world, including Ethernet coin, Lettercoin, Ribo coin and so on. With the successful test of the digital bill trading platform based on blockchain technology promoted by the people's Bank of China in February 2017, the legal tender issued by the platform will also be put into trial operation. Although digital currency is developing rapidly in the world, there are many problems hidden in it. The use of digital currency is convenient for the people, but there are still many problems to be solved, and various countries are constantly trying to sum up experiences and lessons, so that digital currency can better contribute to financial development.

6. Conclusion

The impact of the popularity of blockchain technology on many industries is transformative. There will be some new roles to replace traditional roles, and it will also cause huge changes to the underlying foundation of some industries. Blockchain technology not only represents a new model for future information or data storage, but also an important development direction for interaction between people, industries, industries, and countries. It will subvert the financial industry, reshape the operation execution system, and promote the generation of new business models, reduce people's dependence on the traditional financial industry, and will integrate the "generation gap" between new finance and traditional finance.

References

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[EB / OL]. https://bitcoin.org/bitcoin.Pdf, November 1st2008.
[2] People's Bank of China. The 13th Five-Year Development Plan of Information Technology in China's Financial Industry [EB/OL]. http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3333848/index.html, June 27, 2017.
[3] Ouyang Lan. Thinking about the financial infrastructure of emerging market economies [J]. Journal of Jianghan University, 2005(1): 68-70
[4] Jin Hong. The application of blockchain technology in the banking industry [J]. The Banker, 2016(7): 17-19.
[5] Zhao Longmei. Research on P2P-based virtual electronic currency bitcoin lending model [D]. Hefei: School of Computer Science and Technology, Anhui University, 2015.