Literature Review on Block Chain: Technology, Principle and Development

WANG He[1], HU Zheng[2]

[1]Hankou University, Wuhan, HuBei, 430200, China

[2]Hankou University, Wuhan, HuBei, 430200, China

[1]1900091@student.uwtsd.ac.uk

[2]huzhengxueshu@163.com

Abstract. The block chain technology enjoys a promising development prospect. As one of the most popular technologies, block chain has been heatedly studied and researched by people from all walks of life. Based on an introduction to the technical background and basic concepts of block chain, by analyzing the technical architecture and working principle of block chain, this paper systematically explains the key technologies of block chain, namely decentralization, proof of work (POW), smart contract and Ethereum, and further discusses the development of the block chain technology, 5G, the Internet of Things and the future wireless network.

1. Introduction

The block chain technology is a distributed shared digital ledger supported by cryptography and stored in chronological order. Providing a secure, stable, transparent, auditable and efficient decentralized framework for transaction data recording and information exchange, the block chain technology will be a revolutionary technology to solve the trust crisis in the future society.

2. Technical Background of Block Chain

The block chain technology may lead to the second revolution of the Internet by transforming the "information Internet" into "value Internet". If the Internet, which is known as the "information superhighway", processes "information", then the block chain processes "value".

In the real world, one person transfers money to another via a center with sufficient credibility such as a bank, a payment institution or a witness. Likewise, there must be intermediaries involved when one transfers money to another in the digital world. For instance, the process of transferring money via Alipay is as follows: Alipay subtracts a certain amount of money from one person's account and then adds the same amount of money to another person's account. However, we need to pay for the credit cost for credit intermediaries such as banks and Alipay and other, which makes the financial industry the most profitable industry.

How to create decentralized digital cash or a kind of digital cash without credit intermediary has always been a difficult problem. Digital records can be copied, and the copies are exactly the same as the original records. Without a centralized database to record the data, how can we prevent the same sum of money from being spent twice? This is the so-called double payment or double spending. Before the advent of bitcoins, the major electronic cash systems, e.g. Alipay and PayPal, relied on centralized databases to avoid double spending, and such trusted third-party intermediaries were indispensable.

In the real world, behind cash transaction, there is a financial system related to currency: the central bank, commercial banks and third-party online payment institutions. In the digital world, to create a kind of disintermediated and decentralized electronic cash, a complete system should be well designed as well. This system is supposed to solve the following problems:

How can electronic cash be issued impartially and fairly without being controlled by any centralized organization or individual?

How to transfer cash directly to another person without the help of any intermediary?

How can counterfeit electronic cash be prevented?

In the digital world, this can be translated into the following question: how to prevent the electronic cash from being spent twice?

In 2008, Satoshi Nakamoto published a paper entitled *Bitcoin: A Peer-to-Peer Electronic Cash System*, where he improved previous centralized and decentralized electronic cash with his innovative ideas based on former research results, and created bitcoins, a peer-to-peer electronic cash system, thereby preventing double spending without the participation of any intermediary in transaction [1].

3. Basic Concepts of Block Chain

Block chain can be defined differently from different perspectives. From the perspective of bookkeeping, block chain is a distributed ledger technology that originates from bitcoins, and each data block that contains the information about a network transaction is used to verify the validity of information and generate the next block. From a technical point of view, block chain refers to a series of time-stamped data blocks generated using relevant cryptographic methods, and the node with the accounting right must be time-stamped in the head of the current data block to indicate the writing time of the data, thereby guaranteeing that each block is generated chronologically after the previous block is generated and each block contains the hash value of the previous block, so as to form a chain. From an economic perspective, block chain is a value Internet to improve cooperation efficiency, and a technology for "value representation" and "value transfer" in the digital world. The coin of the block chain is an encrypted digital currency that represents value on one side, and has the distributed ledger and decentralized network for value transfer on the other side.

Since the block chain technology adopts the one-way hash algorithm, each newly generated block is advanced strictly according to the linear order of time. Due to the irreversibility and irrevocability of time, any attempt to invade and tamper with the data information in the block chain can be easily traced, and the counterfeiting is extremely costly, which restrains relevant illegal acts [2].

4. Technical Architecture of Block Chain

Table 1. Hierarchical structure of blockchain.

Application layer	Programmable currency, programmable finance and programmable society
Contract layer	Code, algorithm and smart contract
Actuator layer	Issuance mechanism and distribution mechanism
Consensus layer	Proof of work (POW)
Network layer	P2P network and broadcasting mechanism
Data layer	Data block, hash function, chain structure, asymmetric encryption and timestamp

Where,

- Data layer. The block chain system packages a batch of transactions into blocks and organizes transaction data in blocks. The words "block" and "chain" describe the characteristics of the structure of data used in the block chain technology. A "block" is a data unit that records the transaction information of bitcoins. The "chain" of the blocks is accomplished by the hash value of data in the block head, and this hash value serves as the unique identification of all blocks. The only block linked can be found in the block chain based on the harsh value of the parent block recorded in the block head. In this way, a chain tracing from the latest block to the first block is established according to a sequence of

hash values that link each block to its respective parent block, thereby forming a chained data structure for all blocks 3.

- Network layer. Since block chain is a distributed network, the decentralized and dynamically changing P2P network is applied. The nodes in the network are geographically dispersed but equal servers, and there is no central node. Any node can freely join or exit the network 4.
- Consensus layer. The consensus mechanism is the core engine of the block chain system. In a distributed system without mutual trust, it is difficult for the nodes to reach an agreement, also known as network-wide consensus, within a very short period of time. Block chain is exactly such a distributed network where the nodes reach a consensus via the consensus mechanism, which directly achieves point-to-point transactions without the participation of any intermediate institutions.
- Actuator layer. To encourage more users to participate in the consensus mechanism and improve the security of the system, an incentive mechanism is set up to reward users who participate in the consensus mechanism. For instance, in the case of bitcoins, the nodes involved in bookkeeping are referred to as the miners, and the nodes that successfully gain the bookkeeping right will receive bitcoins as a reward.
- Contract layer. As the “virtual machines” at the bottom of the block chain, the data layer, the network layer and the consensus layer are responsible for data representation, data dissemination and data verification respectively, while the contract layer is a programming algorithm established based on these virtual machines. Taking bitcoins as an example, the contract layer executes a simple scripting language to control the transaction of bitcoins in the Internet trading market. Such scripting language is the embryonic form of smart contract, which brings about the first programmable global currency in human history. Smart contract can be simply understood as a computer program that executes automatically under certain conditions.
- Application layer. The application layer provides programs and interfaces for a variety of application scenarios, and users interact through various applications deployed in the application layer, without having to consider technical details of the underlying block chain. The block chain technology is currently applied in the following six typical scenarios, namely digital currency, data storage, data authentication, financial transactions, asset management and election voting. Digital currency is the earliest application of the block chain technology, and the most typical case must be bitcoins. The digital currency can be used to buy goods or services in the digital currency system.

5. Working Principle of Block Chain

As a pioneering work about the application of the block chain technology, bitcoin is essentially a digital currency generated by the distributed network, and its issuance process does not rely on the central authority. With the transaction of bitcoins as the case, the working principle of block chain is illustrated as follows:

- Broadcast each transaction to every node of the network to make it valid.
- Upon receiving the transaction information, the miner node records this transaction on the ledger. Once recorded, the transaction information is irrevocable and cannot be deleted randomly.
- The miner node confirms the transaction through the bitcoin software running on the personal computer.
- To stimulate the enthusiasm of miners, the system rewards the miners with 25 bitcoins for the transactions they’ve recorded and confirmed (As set by the system, the number of bitcoins as a reward will be halved every 4 years).
- There is only one reward which will be given to the first miner who solves the problem. The system will provide a problem which is supposed to be worked out within ten minutes. The one who can solve this problem using hash algorithm within the shortest time will be given the bookkeeping right and win the corresponding reward.
- The miner winning the bookkeeping right will broadcast the transaction to the whole network, the ledger will be made public, and the other miners will check and confirm these accounts. If the transaction has been confirmed by more than 6 miners, it will be successfully recorded.

Each record made by the miner forms a block, this transaction will be time-stamped, and each newly formed block will be pushed forward in strict accordance with the timeline, thereby forming a complete time chain. Besides, each block contains the hash value of the previous block, which ensures that the blocks are connected in chronological order without being tampered with, forming an irreversible chain called block chain.

Once confirmed as correct by other miners, these records will be determined to be legal, and the miners will enter the next round of competition for the bookkeeping right [5].

6. Key Technologies of Block Chain

6.1. Decentralization

With banks as the credit intermediaries, users have to pay the credit cost. How can we operate without the credit endorsement of central institutions such as banks? Block chain, which is designed to solve problems concerning trust and reduce the cost of trust, aims to realize decentralization and live without credit intermediaries.

Decentralization is a subversive feature of the block chain. Without central institutions or central servers, all transactions take place in the applications installed on individuals' computers or mobile phones. The verification, accounting, storage, maintenance and transmission of block chain data are all based on a distributed system, which not only saves resources and simplifies transactions, but also avoids the risk of being controlled by centralized agents. The block chain technology stores data on a time-stamped block chain structure, adding a time dimension to the data, which is strongly verifiable and traceable [6].

6.2. POW

When designing the bitcoin system, Satoshi Nakamoto creatively combined the competition of computing power with economic incentives, and all nodes participate in a consensus process known as POW to verify and record transactions in the bitcoin network. The POW consensus process is commonly known as "mining", and the nodes involved in mining are referred to as miners. In other words, the miners compete for the right of recording payments into a public ledger. Usually, users contribute their computing resources to compete to solve a mathematical problem. The first miner who successfully solves the mathematical problem will gain the bookkeeping right of the block and be rewarded with certain bitcoins allocated by the Bitcoin system. It is the responsibility of the rewarded miners to package all bitcoin transactions in the current period into a new block and link them to the main chain of bitcoins in chronological order [7].

6.3. Smart Contract

Smart contracts refer to "a piece of code written to implement predetermined rules", and the code is used to control the transfer of digital assets on the block chain. External applications execute all kinds of transactions by calling smart contracts. When there is an asset transaction between two parties involved in a smart contract on the block chain, a piece of code will be automatically triggered to automatically complete the specific transaction. Such code is the smart contract.

6.4. Ethereum

A "Turing-complete" programming language is required to realize the smart contract. To put it simply, a "Turing-complete" programming language is able to work out all the problems in the world that can be calculated. Ethereum, as a Turing-complete scripting language that can implement all calculations on the block chain, can be used to create "smart contracts" and control the state transition of the block chain, that is, the transfer of digital assets on the block chain.

With Ethereum as the platform, developers can create their own block chain applications. There are three types of applications on Ethereum: (1) Financial applications. Such applications include electronic currency, financial derivatives, hedging contracts, storage wallets, wills and even some final

employment contracts. For example, the smart contract can record all information about the ownership of securities, so the smart contract is applicable to the registration and clearing of securities. (2) Semi-financial applications. A typical example of such application is self-implementation incentives to solve computing problems. (3) Non-financial applications. Online voting and decentralized management are commonly seen non-financial applications. Online voting can be written into smart contracts that can be directly triggered according to the voting results [8].

7. Development Prospect of Block chain

7.1. 5G and Block chain

5G refers to the 5th generation wireless communication network technology with high data transmission rate, low transmission delay, wide network coverage and massive equipment access. Its core purpose is to realize a social and economic system with the Internet of everything, and to build an intelligent digital society. Although 5G breaks the bottleneck of 4G, it still faces problems in security and privacy, e.g. disclosure of data information. By combining block chain with 5G, the shortcomings of block chain such as transmission delay and poor scalability can be solved by the 5G technology, and the challenges faced by the 5G technology can be overcome by the strengths of the block chain technology such as information protection, tampering prevention and traceability.

7.2. Block chain and the Internet of Things

The Internet of Things, as a distributed node network embedded with sensors, electronic software, small computing memory, actuators and communication devices, can be seen everywhere in people's daily life. Facing numerous devices in the Internet of Things, the centralized server framework with high transmission delay and untimely updated equipment information seems to be incompatible with present needs. The hazards caused by the centralized framework have appeared frequently. For instance, in the Internet of Vehicles, traffic accidents caused by transmission and processing delay in self-driving technology occur frequently. Therefore, by building a distributed framework of the Internet of Things in the wireless environment using the block chain technology, direct communication can be achieved between devices and the time of uploading data to cloud servers can be reduced, which ultimately improves the processing efficiency of devices in the Internet of Things. Moreover, the 5G technology with wide coverage can increase the network capacity of the Internet of Things, thereby enhancing the decentralization of the block chain. In addition, the block chain technology is used to isolate block data and establish a decentralized distributed ledger to track, execute and store large amounts of data information. Block chain is applicable to various fields of the Internet of Things. Especially since the rise of smart contracts, a great number of studies have been carried out on the application of the block chain technology in fields such as the Internet of Vehicles, smart city, smart grid, smart home, wearable devices, supply chain management and agriculture based on the Internet of Things.

7.3. Wireless Network and Block chain in the Future

The idea of 6G is to realize the integration of space, heaven and earth. As a new generation of high-speed Internet of Things, the 6G technology is able to transmit the massive data accumulated on the block chain in just a few seconds. Currently, the research on the block chain technology applied in the 6G wireless network has not yet started. With the proposal of the key technology of 6G, more attention has been paid to the integrating point between block chain and 6G technologies. It goes without saying that the block chain will become an indispensable part in the information technology revolution in the future network era [9].

8. Conclusion

With the rapid development and popularization of bitcoins, an explosive growth trend has also been found in the research and application of block chain technology. The block chain technology is considered to be the 5th innovation of computing paradigm after mainframe, personal computer, Internet

and mobile/social network. It is the 4th milestone in the evolutionary history of credit after consanguineous credit, precious metal credit and central bank paper currency credit [10]. Block chain is essentially a technical solution to solve the problem of trust and reduce the cost of trust, the purpose of which is to decentralize and eliminate credit intermediaries. By means of data encryption, timestamp, distributed consensus and economic incentive, the block chain technology achieves point-to-point transaction, coordination and cooperation based on decentralized credit in a distributed system where nodes do not need to trust each other, thereby providing solutions to common problems such as high cost, low efficiency and insecure data storage in centralized institutions.

References

[1] Fang Jun. Introduction to Block chain[M]. China Machine Press, 2019.1
[2] Zhang Liang, Liu Baixiang. Overview of Block chain Technology[J]. Computer Engineering. 2019, (5)
[3] Xie Hui, Wang Jian. Study on Block Chain Technology and Its Applications[J]. Netinfo Security, 2016, (9)
[4] Zhu Liehuang, Gao Feng et al. Survey on Privacy Preserving Techniques for Block chain Technology[J]. Journal of Computer Research and Development. 2017, 54 (10)
[5] Ku Yezi. Dear Customer, the Block chain You Purchased Has Arrived! 2016.9
[6] http://www.mobiletrain.org.Working Principle of Block chain Technology. www.sohu.com/a/275522080_100111840, 2018.11.15
[7] He Pu, Yu Ge. Survey on Block chain Technology and Its Application Prospect[J]. Computer Science. Apr.2017
[8] Cui Han. Definition and Application of Smart Contract. www.elecfans.com/block chain/1090017.html, 2019.8.24
[9] Cao Bin, Lin Liang et al. Review of Block chain Research[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition). Feb. 2020
[10] Yuan Yong, Wang Feiyue. Block chain: The State of the Art and Future Trends[J]. Acta Automatica Sinica, 2016, 42(4)