ISSN 2616-7433 Vol. 2, Issue 3: 13-17, DOI: 10.25236/FSST.2020.020304

The Overview of Blockchain Technology Foundation and Application Research

Liu Chunhua

Yunnan Open University, Kunming Yunnan, 650223, China

ABSTRACT. *The technology of block connection has been paid more and more attention by the theorists, and many scholars have studied the foundation and application of blockchain technology from different angles, which has further promoted the technology. This paper summarizes and analyzes the foundation and application of blockchain technology, hoping to provide reference for the better development of blockchain technology.*

KEYWORDS: *Blockchain technology; Conceptual analysis; Transaction flow; Underlying framework*

1. Introduction

In bitcoin, the blockchain belongs to the underlying process technology category. The concept of blockchain is first proposed in Nakamoto's book, which is <Bitcoin: A peer-to-peer electronic cash system>. Later, on the basis of different academic background or perspective, different scholars have carried out related activities for the concept of blockchain. However, there is no uniform, generally accepted definition of blockchain for the multiple interpretations of blockchain in the current essay. The definition of a block chain is reflected in the following perspectives:

Firstly, from the perspective of data, some scholars think that blockchain belongs to the category of data structure. For example, in the view of Zou Jun and others, blockchain is a chain formed by blocks. Blocks belong to the content of structural data units. According to the relevant time sequence, data blocks are connected to form a linked data structure. Some scholars think that blockchain belongs to the category of database. For example, in Melanie Swan's <blockchain: a blueprint and guide for a new economy>, he proposed that blockchain technology belongs to the category of decentralized, open and transparent database. According to Mei Haitao and other scholars in China, blockchain is essentially a distributed database, eliminating deletion and update operations. Dong Hui and others think that blockchain is a database, which has the characteristics of decentralization, credibility and security, and uses the distributed form to record various transaction information. In Qin Yi's view, blockchain is an open general ledger database based on computer programs. According to Sun Guomao, blockchain technology belongs to the category of distributed reliable database. In the research review of Lin Xiaochi and others, it is systematically pointed out that through the form of chain, the data structure of block combination is blockchain, which contains many features, such as: recording data in time sequence, programmable, safe and reliable, collective maintenance, decentralization, etc. At the same time, it is also proposed that blockchain belongs to distributed database or distributed shared general ledger, which cannot be changed basically. Therefore, from the point of view of data, blockchain not only belongs to the category of data structure or distributed database, but also belongs to the category of data technology.

Secondly, the blockchain belongs to the category of distributed accounting technology or accounting system. For example, in Zhang Rui's view, the blockchain essentially belongs to the category of distributed accounting technology. In other words, the blockchain is the book, each page of the book is the block, and the bookkeeper is the node on the block. In He Pu et al.'s view, the block chain is better than each non-modifiable block. Each block is responsible for recording all transaction data generated during the corresponding period. In Yin Guanqiao's view, in essence, the block chain belongs to the category of distributed book technology, which is based on asymmetric encryption algorithm. Zhang Jian thinks that the essence of the blockchain is a decentralized accounting system consisting mainly of credit records and the clearing of credit records.

Thirdly, from a protocol perspective, the blockchain is essentially an Internet protocol similar to the HTTP protocol. In <The promise of the blockchain: The trust machine>, which is published in the prestigious US journal, it is argued that in the absence of third-party oversight, using the blockchain technique to build mutual trust can be identified as a blockchain for the underlying protocol on the “value internet” of the second-generation Internet. However, in the view of the domestic scholar Lin Xiaochi and others, in essence, the

ISSN 2616-7433 Vol. 2, Issue 3: 13-17, DOI: 10.25236/FSST.2020.020304

blockchain belongs to the category of Internet Protocol. There are many similarities between blockchain technology and Internet application protocol.

Fourth, from the perspective of economics, the blockchain belongs to the category of value Internet, which can meet the needs of shared economy. In Yu Bo's view, the blockchain technology is in the continuous maturity and development. It can drive the Internet from the information Internet to the value Internet, in the sharing economy, based on the new economic model of value. In the view of Shao Qifeng et al., in the absence of understanding between the two parties to the transaction, the blockchain can ensure the reliability of trust, and use decentralization to ensure the completion of the work of trusted value transmission, so the block chain can also be called the value Internet.

Fifthly, the blockchain is a technical solution or a new technology integrated by a variety of technologies. For example, in Mu Qiguo's view, the blockchain is a technical solution to jointly maintain a reliable database using a decentralized and de-trusted approach. In Chen Linyan's view, the blockchain will not rely on third parties. For network data, it can use its own distributed nodes to carry out storage, verification, transmission and communication technology solutions. In the view of Dong Hui et al, block chain is a new technology that combines the knowledge of many subjects, including mathematics, cryptography, computer science and so on. Yan Yong thinks that the so-called blockchain is to use a series of technologies to flexibly cooperate with the resulting set of technologies, including cryptographic principles, security hash algorithms, consensus mechanisms, and so on.

2. The Research on Blockchain Trading Process

As for the main transaction process of blockchain, it mainly includes: creating new transactions, using P2P, carrying out network communication activities, verifying transactions, using P2P network communication to verify the results, and recording transactions in the account book. In other words, from generation to propagation in the network, to utilization of workload, demonstration activities, verification of the whole network node, and finally recording in the blockchain. As for the specific transaction process, the first is the generation of the transaction. For the previous transaction and the next owner, the current owner will sign a digital signature through the private key, and attach the signature at the end of this currency, so that the transaction order will be completed. For the transaction list, the current owner will carry out the whole network broadcast activity. For the received transactions, all nodes will be included in a block. Using the workload proving mechanism equivalent to solving a mathematical problem, each node will obtain the right to create a new block and try its best to get the reward of digital currency. Then, when each node finds a solution, within the scope of the whole network, it will broadcast all time stamped transactions recorded in the block. Other nodes in the whole network are responsible for carrying out relevant checks and checking the correctness of the block's accounting. In the absence of any errors, it will carry out the next block's competitive activities, such a legal accounting is generated from this.

The transaction process of blockchain mainly includes the following points:

First, create and build a new transaction. Then make a transaction list;

Second, transport the relevant nodes, and carry out the whole network broadcasting activities for the new data recording information;

Third, the receiving node is responsible for carrying out relevant records and inspection activities for the received data and information content;

Fourthly, for the block, each receiving node of the whole network implements the consensus algorithm;

Fifth, after the block completes the consensus algorithm process, it will formally carry out storage activities in the blockchain.

For example, the transaction process of blockchain mainly includes the following steps for the bitcoin:

In the first step, for the previous transaction and the next owner B, owner A can sign the digital signature through its private key, attaching the signature at the end of the coin, and making the transaction order. In this case, owner B can set the receiver address as the public key;

In the second step, for the transaction list, private A broadcasts on the whole network, so that bitcoin will be sent to owner B. All nodes will be summarized into one block for the accepted transaction information content;

In the third step, by solving a mathematical problem, each node will have certain rights, so that it can create a new block and fight for the reward of acquiring bitcoin. In this process, new bitcoin will be produced;

ISSN 2616-7433 Vol. 2, Issue 3: 13-17, DOI: 10.25236/FSST.2020.020304

In the fourth step, when a node finds a solution, it will carry out the whole network broadcast and check with other nodes of the whole network for all time stamped transactions recorded in the block;

In the fifth step, as for the correctness of the block accounting, other nodes of the whole network are responsible for checking. After confirming that there is no error, they will compete for the next block, forming a legal accounting blockchain.

3. The Research on the Blockchain Infrastructure

Generally speaking, the infrastructure aspect of blockchain is mainly composed of six levels: data layer, network layer, consensus layer, incentive layer, contract layer and application layer. The details are as follows:

3.1 Data Layer

On the technical aspects of the data layer, it mainly refers to the data block, asymmetric encryption, timestamp, etc., which is mainly to ensure the data decentralized distributed storage, the existence of the check block data and the realization of the complete goal, so as to ensure the traceability and non-tampering of the data.

3.2 Network Layer

On the composition of network layer, distributed networking mechanism, data dissemination mechanism and data verification mechanism are the main contents. Using the network layer, the construction of network environment and transaction channel is realized, and the rules of node reward are defined.

3.3 Consensus Level

In the consensus layer, all kinds of consensus algorithms of network nodes are included, the workload proof mechanism, the authorization stock proof mechanism, the rights and interests proof mechanism and so on belong to its main content. In the decentralization system, the decision-making power is relatively high, through the consensus layer, it can ensure the high consensus on the validity of the block data. In the blockchain, the consensus layer belongs to one of the core technologies.

3.4 Incentive Level

Through the incentive layer, the economic factors can be concentrated in the blockchain technology system. The distribution mechanism of economic incentive belongs to the main content of incentive layer. In the bitcoin blockchain, through the “mining” mechanism, it can encourage the majority of participants to continue to provide computational power, and then obtain corresponding incentives;

3.5 Contract Layer

In the contract layer, all kinds of scripts, algorithms and intelligent contracts belong to its main content. The contract layer belongs to the category of business logic and algorithm, which is based on the blockchain virtual machine.

3.6 Application Layer

In blockchain, all application scenarios and cases are the application layer, and programmable money, programmable finance and programmable society are the main contents of the application layer. In the architecture of the application layer, regarding the most typical innovation points, it not only includes the timestamp-based chain block structure, the consensus mechanism of distributed nodes and the economic incentive based on consensus computing force, but also includes the flexible and programmable intelligent contract blockchain technology.

ISSN 2616-7433 Vol. 2, Issue 3: 13-17, DOI: 10.25236/FSST.2020.020304

4. The Research on the Application of Blockchain Technology

4.1 The Link of the Blockchain

The blockchain is to connect the independent block together, and the chain situation is basically the same. In each block, it mainly includes two parts: block head and block body. In the block header, there are hash values with random numbers. In fact, the hash value of the previous block is the hash value of the previous block.

4.2 Consensus Mechanisms

Bitcoin promotes the generation of blockchain. At the same time, blockchain plays an important role in bitcoin's technical architecture. Generally, blockchain can be regarded as a decentralized accounting system in the Internet. In the decentralized node environment, blockchain needs to ensure the consistency of accounting data of all honest nodes. The use of blockchain can promote the transmission of trusted information on untrusted channels, value transfer issues, and be properly handled. However, through the consensus mechanism, even in the distributed scenario, it can also solve the problem of consistency of accounting data of blockchain nodes, which lays the foundation for the security performance of bitcoin system. At present, the consensus mechanism of blockchain mainly includes PoW,PoS,DPoSand distributed consistency algorithm.

4.3 Trading Rules

The basic module that constitutes a block is block chain transaction. Blockchain transactions are also responsible for recording the actual effective content of the blockchain. In other words, a transfer is a blockchain transaction. For a payment transfer transaction of bitcoin, the transaction rules mainly include: firstly, input and output activities should be carried out for the transaction, and the input and output content cannot be empty. Secondly, in the transaction pool, the UT XO search activity should be carried out for the input transaction content. If the search finds out the relevant content, the transaction activity should be rejected. Then, for each input aspect of the transaction, the corresponding output should be UT XO. Finally, the input unlocking script and the corresponding output locking script should be used to jointly verify whether the transaction conforms to the relevant provisions.

4.4 Merkle Tree

In blockchain technology, Merkle tree is an important data technology. Merkle tree belongs to the category of hash binary tree. Each node has at most two subtrees, and each node represents a structured data. Using Merkle tree, for the data information in the block, it can quickly carry out induction activities in a short time, and also can verify the authenticity and integrity of the data. In general, in the operation process, the data in the hash block can be grouped. In the Merkle tree, the new hash value formed is inserted. Using this recursive form, the last root hash value is recorded as the Merkle root of the block head. The binary tree used by bitcoin is a common Merkle tree. In each hash node of the binary tree, two adjacent data blocks or hash values are included.

4.5 Timestamps

In general, using timestamps, one can verify the existence of complete data in a given time. Through the blockchain database, the recorder in the whole network can carry out the bookkeeping activities according to each block, with the time seal on it, which can reflect the writing time of the data, and then guarantee the non-change and forgery of the database. In a blockchain, the first active or inventor only needs to be stamped with a timestamp to prove an activity or the original inventor after launching the release activity.

5. Conclusions

The research and application of blockchain in the industry is still in the period of theoretical discussion and practical imagination. It is difficult to effectively deal with the problems and limitations of blockchain, lacking specific application. For blockchain, although the academic community has carried out relevant discussion activities, the relevant literatures mainly focuses on some conceptual issues. Therefore, the research on blockchain will focus on the practical application of technology, laws and regulations and regulatory issues in the

ISSN 2616-7433 Vol. 2, Issue 3: 13-17, DOI: 10.25236/FSST.2020.020304

future. With the continuous development of blockchain technology and the in-depth development of people's understanding of blockchain, the era of “blockchain +” will be ushered in in the near future

References

[1] Zeng Shiqin, Huo Ru, Huang Tao, Liu Jiang (2019). Overview of blockchain technology research: principle, progress and application. Journal of communications, no.9, pp.1-18.
[2] Li Fengyang, Qin Xing (2018). Agricultural order platform based on blockchain. Jiangsu agricultural science, no.3, pp.1-6.
[3] Gong Yongli, Fang Zeming (2019). Research on the application prospect of “blockchain + tax” collection and management mode. Value engineering, no.36, pp.158-160.
[4] Luan Xin (2019). Actively promote the construction of smart contracts in blockchain. Learning times, pp.15-16.