Technical Characteristics and Model of Blockchain

Yang Xinyi
College of big data and software
University Of Chongqing
Chongqing, China
e-mail: y17783490121@163.com

Zhang Yi
College of big data and software
University Of Chongqing
Chongqing, China
e-mail: cquzhangyi@cqu.edu.cn

Yulin He
Chongqing Aerospace college of Vocational Technology
Chongqing University
Chongqing, China
e-mail: 1040944072@qq.com

***Abstract*—Blockchain technology is the underlying infrastructure and support technology to build trust of Bitcoin. It is not only an emerging technology that relies on pure mathematical method to create trust relationship in a distributed environment but also an innovative combination of hash algorithm, asymmetric cryptography, time stamp, consensus mechanism and many other technologies, with characteristics of decentralization, trustlessness, collective maintenance, reliable database, openness, security and untamperability, anonymity, verifiability and traceability, programmable and so on. This paper mainly introduces the technical characteristics and models of block chain, summarizes the development status and branch classification of Blockchain, and outlines the future application of Blockchain technology.**

Keywords-Blockchain; Bitcoin; distributed; decentralization; trustlessness; technical model

I. INTRODUCTION

The concept of Blockchain is derived from the article "Bitcoin: A Peer-to-Peer Electronic Cash System (bit currency: a peer-to-peer electronic cash system) [1] published by a scholar named Satoshi Nakamoto after the outbreak of the global financial crisis in 2008.

In the article, it is believed that: first, when dealing with peer-to-peer electronic payment information, there are inherent shortcomings of lack of trust. Though a financial institution is depended on as a reliable third party, there still exist problems such as unavoidable frauds and personal information disclosures. Second, the existence of financial intermediaries will increase the costs and limit the actual minimum size of transaction. Third, digital signature can solve the problem of electronic currency identity itself. If a third party is still needed to support preventing from double consumption, the system will lose value.

Based on the above three existing problems, Satoshi Nakamoto proposed a digital credit system for peer-to-peer value transmission, that is, Bitcoin. The basic design framework of the Bitcoin uses cryptographic methods to solve problems of trust between users, allowing them to directly achieve online payment and fully get rid of third party intermediary financial institutions when reaching an agreement. Its innovation lies in changing the traditional central payment mode and creating a brand new electronic money system which is decentralized and trustless. Bitcoin is the first application of Blockchain technology in the field of financial payment.

Then, Bitcoin was officially born in January 3, 2009 and rapidly hot, causing great attention all over the world. Blockchain technology, as the underlying protocol of Bitcoin [2], was gradually discovered by researchers. On October 31, 2015, a cover article of "The Economist" named "The promise of the Blockchain: the trust machine" [3] believed that Blockchain technology had the great potential to transform the mode of economic operation and cooperation between people. It is the technology of "creating trust". Blockchain technology lets people who have no particular confidence in each other collaborate withought having to go through a neutral central authority. Simply put, it is a machine for creating trust. The publication of this article has attracted extensive attention in the area of Blockchain technology.

II. DEVELOPMENT STATUS

A. Development and Applications

In recent years, Blockchain technology has become a revolution of Internet financial technology and a great innovation of basic information technology in the future. But it is not a new technology itself. Blockchain technology involves basic techniques accumulated over the past few decades in many fields, such as mathematics, cryptography, computer science, which is a new application mode combined with distributed data storage, peer-to-peer transmission, consensus mechanism, and encryption algorithm.

Blockchain technology can effectively solve the problems of high cost, low efficiency and unsafe data storage in the traditional central financial system, reduce the risk of

978-1-5386-7223-5/18/$31.00 ©2018 IEEE

trust, optimize the business process of financial institutions, and drive the birth of a new business model which is widely concerned by the government and the financial domain. In the " Distributed ledger technology: beyond Blockchain" [4], the British government has proposed that the Blockchain technology is still in the early stage of development. To live up to the full potential of the Blockchain and related technology, it is necessary to deal with other problems of privacy protection, security, performance and extensibility.

In the article named "BLUEPRINT FOR A NEW ECONOMY" [5], the application of Blockchain is divided into three stages in accordance with application scopes and development stages by Melanie Swan as following: Programmable currency, Programmable finance, and Programmable society (from Blockchain 1.0 to 3.0).

At the beginning of 2009, Blockchain technology came into being as a underlying technique supporting for digital currency application to carry out payment, circulation and other monetary function of decentralization. ensuring people make direct transactions of virtual currencies like Bitcoin, Litecoin, etc. without third party intermediaries to establish a basis for trust.

Around 2014, the significant value of the Blockchain technology which began to be realized by the researchers was not only limited to support for functions of digital currency, but also to have more optimization and application in the whole financial field, such as to register, confirm or transfer various types of assets and contracts based on the distributed ledger function of Blockchain technology. All financial transactions can be transformed into Blockchains, including stocks, private equity, public financing tools, bonds, mortgages, property rights, hedge funds, annuity, pension and all types of financial derivatives, such as futures, options, default swaps, and so on.

Combined with intelligent contracts, the Blockchain, which had the characteristics of decentralization, transparency and untamperability, shortening payment cycles, reducing costs of payment, increasing transparency of the transaction, was able to be applied in the field of cross-border payments, digital bills, bank credit, asset securitization, supply chain finance, and insurance industry without any intervention by the third party agencies. Ethereum and hyperledger, which are the most representative applications of Blockchain, release the two important development trends of Blockchain technology in the future: the public chain which is applied to the public and the alliance chain which is applied to the enterprises.

With the rise of Blockchain technology applied in the financial field, its technical advantages had gradually been shown in other industries and fields such as government, medical, scientific, educational, cultural and artistic fields that even covered almost all aspects of human social life. This technology provided a decentralization and low-cost trust mechanism for the information self-proof and sharing , realized the verification and transfer of virtual property, and no longer relied on any third-party trust certification authority The block chain has built a centralization and low cost trust mechanism, which not only promotes the innovation of productivity, but also promotes the transformation of production relations, and reconstructs the logic of social and economic operation.

Programmable currency is the value exchange basis of programmable finance as well as programmable finance is the development kernel of programmable society. Up to now, programmable currency is still the most extensive and popular application of Blockchain technology.

B. The Classification of Blockchain:

According to the access right which decided whether it was necessary to obtain permissions of chain nodes for accessing Blockchain, Blockchain was divided into three categories: public Blockchains, consortium Blockchains and private Blockchains. Public Blockchains stressed the importance of anonymity and decentralization, while consortium Blockchains and private Blockchains which focused more on efficiency became centralization to some extent.

1) Public Blockchains:

A public Blockchains is a kind of Blockchain that anyone in the world can access, read, or send a transaction which can be effectively confirmed, participate in the consensus process. It is a completely decentralization, distributed and public digital ledger that is under no control of any individual or organization. This ledger is open and transparent. Inside data security is guaranteed by encryption technology. However, there are inadequacies that costs of operation and maintenance of public Blockchains is high, and speed of transaction is slow. Public Blockchains are the most widely used Blockchains at present represented by Bitcoin, Ethereum, Bitshares, Ripple, and Hyperledger.

2) Consortium Blockchains:

Consortium Blockchains can be seen as "partial decentralization Blockchains" which are open to a group of organizations particularly. Its consensus process is controlled by a series of nodes which are pre-selected internally as the bookkeepers who determine the generation of each block. As for other nodes, authorization is required for entry and exit Blockchains. They can participate in the transaction, but have no right to account. There are usually good network connections between bookkeepers. So this block chain can use consensus algorithms with non-workload-proof. It provides higher transaction processing speed, lower transaction and maintaince costs, and better data security than public Blockchains. Fabric is the representative of consortium Blockchains.

3) Private Blockchains:

A private Blockchains is completely open to a single individual or ganization. In general, writing and reading authority management is required strictly for data access and usage which make a certain centralization control. Private Blockchains are applied in some scenarios including database management, internal audit inside an enterprise or even government's budget, implementation, or industry statistics. The representative of the private Blockchains is: R3 Corda.

III. CONCEPTS AND CHARACTERISTICS

In structure, the Blockchain is an irreversible data structure formed by a series of data blocks connected linearly in time order. The information stored in each block is encryptd with asymmetric cryptographic algorithms to ensure the security of its data access and transmission. In the system, each data block records and updates node data and transaction information according to the specified consensus algorithm of distributed node. The validity of the data can be verified by hash algorithm for any block.

On the definition, Richard Brown, the chief scientific officer of the distributed ledger organization, proposed that the Blockchain is a decentralized shared ledger, which is a technical solution to collectively maintain a reliable database through methods of decentralization [6]. This database technical scheme includes SHA (secure hash algorithm), asymmetric cryptographic cryptography, time stamp, consensus mechanism and other technologies with characteristics of decentralization, trustlessness, collective maintenance, reliable database, openness, security and untamperability, anonymity, verifiability and traceability, programmable and so on.

- Decentralization: decentralization is the most essential and prominent feature of the Blockchain. in the Blockchain system, record, storage, transmission, verification, maintenance and many other processes are based on the distributed system structure. Trust relations between chain nodes are established using a pure mathematical method (asymmetric cryptography) under no mandatory control of any central authority or regulatory agency which can manipulate the data unilaterally. So the Blockchain system can save a lot of intermediary costs without additional third party management institutions. In this distributed peer-to-peer network, each distributed node in the network is relatively independent. They share data and has equal rights and obligations.data corruptiona or exception of any node will not affect the operation of the whole data system, guaranteeing better reliability and robustness of Blockchain system.

- Trustlessness: based on the principle of cryptography, the Blockchain system protects message contents and confirms the identity of sender through the privacy and unforgability of asymmetric cryptography, ensuring that the recording, transferring and storing processes of value exchange activities is reliable in Blockchain system. It also solve the problem of ownership confirmation in transaction process of distributed system through distributed consensus algorithm, guaranteeing the consistency of the data record and storage. This achieves that chain nodes participating in the whole system only need to follow a fixed algorithm to automatically reach a consensus and trust on transactions without establishing mutual trust before when exchanging data.

- Collective maintenance: a Blockchain system uses a consensus algorithm to select specific nodes for adding new blocks to a existing Blockchain and a economic incentive mechanism to encourage more chain nodes to participate in the validation process of data blocks. All nodes in the distributed system are relatively independent. They share data, possess equal rights and obligations, and co-maintain data information in the Blockchain, leading to the lowe.

- Reliable database: Data information will be permanently preserved in the block chain system, and kept as the same complete copy of the database stored in each node. The reliability and integrity of data information is guaranteed by the fully redundant and multi-replica database, which effectively solved the "Byzantine fault tolerance" problem.

- Openness: The technical foundation of Blockchain is open source. In addition to the private information of transaction parties which is encrypted, data information of the Blockchain is open to all. Any node in the network can query the data of Blockchain and develop related applications through an open interface. Therefore, data content and operating rules of the whole system is highly public and transparent. There exists no deception between nodes.

- Security and untamperability: Blockchain system uses a chain structure formed by data blocks with time stamp which are closely connected in time order to store data information. Each block is encrypted with hash algorithm and permanently recorded once generated. And it can not be tampered and deleted by less than 51% nodes of the whole system. Moreover, In the aspect of authority management, the access authority management is controlled by multiple private key rules.

- Verifiability and traceability: Blockchain system uses time stamp technology to add the time dimension for data block. Each data block stores the hash values which uniquely identify of the current block and parent block.

- Anonymity [7]: the data exchange between nodes follows a fixed algorithm without mutual trust, so the identity information of the nodes in the system does not need to be open or verified. So the information transfer can be carried out anonymously.

- Programmability: Blockchain technology can provide a flexible script code system to support users to create advanced smart contracts, currency or other decentralization applications. This can optimize the form of transaction, and improve the economic efficiency of our society.

IV. THE TECHNICAL MODEL

In general, the technical model of Blockchain consists of six parts. They are the data layer, the network layer, the

consensus layer, the incentive layer, the contract layer and the application layer from bottom to top [8]. Among them, the first three layers which undertake the functions of data representation, data propagation and data validation respectively are the essential elements of the Blockchain technology. If there is a lack of any one of the three, it can not be called the real Blockchain technology. While the incentive layer, contract layer and application layer are not the necessary elements for all Blockchain applications. Some Blockchain applications do not contain these three layers of structure.

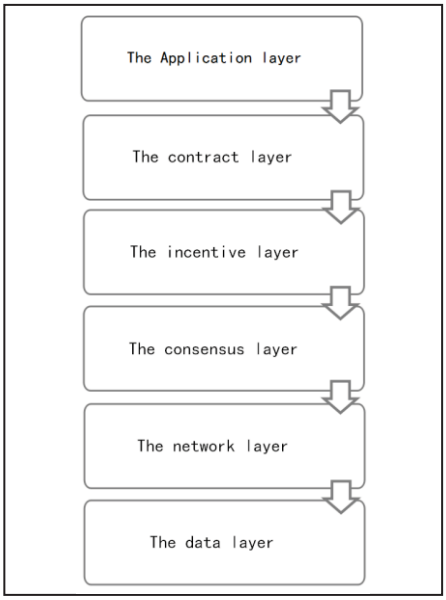

Figure 1. The structure of Blockchain technical model.

A. The Data Layer

The data layer of the Blockchain technical model mainly describes the physical form of the Blockchain. It encapsulates underlying technologies in the entire Blockchain, including data block and chain structure, hash function, Merkle tree, asymmetric public key data encryption and time stamp technology. In terms of data storage, block chain database is implemented by chain structure of data blocks. In the aspect of data security, the Blockchain system uses Merkle tree structure to record transaction information, and ensure that the transaction between nodes can be carried out safely in the case of decentralization through a variety of cryptographic algorithms and techniques, such as asymmetric encryption (RSA, ECC, etc.), digital signature, digital certificate, multi signature technology, etc.

B. The Network Layer

The Blockchain system is essentially a P2P network (also called point-to-point network or peer-to-peer network) with automatic networking mechanism. Nodes in the chain automatically constitutes an Internet system by exchanging, recording and updating data information. Unlike the centralized network with central servers, any one of the nodes in the P2P network is both a client and a server, leading to that resource sharing is no longer dependent on the central server. The network layer in the Blockchain system mainly implements the connection and communication of network nodes, including distributed P2P networking mechanism, data dissemination mechanism and data validation mechanism.

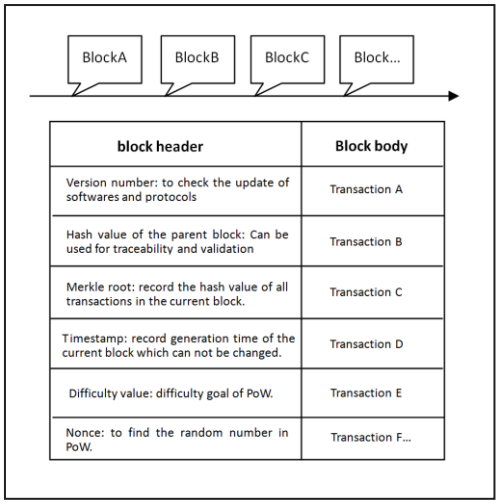

Figure 2. The structure of each block.

C. The Consensus Layer

The theoretical basis of this layer is Byzantine fault tolerance (BFT). To avoiding operational errors, network delays, system crashes, malicious attacks and other system errors (Byzantine errors) [9]. The consensus layer of Blockchain system aims at solving the problem of how to construct the block ,ensure the correctness and consistency of all nodes, and maintain the unity of the whole block chain in Blockchain, a decentralized, trustless and unsupervised distributed asynchronous system. And the core is the construction and validation of blocks.

The consensus layer is one of the core technologies of the blockchain. It mainly encapsulates common understanding mechanisms and consensus algorithms, which can make all nodes in the blockchain system reach a consensus on the accounting right and validity of the next block efficiently in the decentralized system. This is not only a trust mechanism of the block chain system, but also an overseeing governance mechanism of the block chain community, having the effect on the security and reliability of the whole system. At present, there have been more than ten common consensus mechanisms, including the most well-known PoW (Proof of Work), PoS (Proof of Stake) [10], and DpoS (Delegated Proof of), etc.

D. The Incentive Layer

The incentive layer occurs mainly in public Blockchains. Integrating economic factors into the Blockchain technology system, it combines moderate economic incentive mechanisms with consensus processes to encourages more nodes to participate in verification and accounting processes of the Blockchain system and form a stable consensus on

the history of the Blockchain. Incentive mechanisms mainly include economic distribution mechanisms and distribution mechanisms that motivate nodes to observe the rules to participate in the accounting nodes, and punishes the nodes that do not comply with the rules.Thus it can converge massive nodes, promoting the whole Blockchain system to develop towards the direction of security and maximization of interests.

E. The Contract Layer

The contract layer is a business logic and algorithm built on the Blockchain system. It combines various scripts, algorithms (as functions) of the block chain system with the data (as states) of the system to realize custom smart contracts. Smart contracts clearly stipulate the rights and obligations of both parties in transactions. When it reaches the agreed execution conditions, smart contracts will be executed automatically without a third party. It is not only a computer protocol installed on the contract layer implementing the contract by means of informationization, but also a basis of realizing the trustlessness and programmability of Blockchain system.

Digital encrypted currencies, including Bitcoin, mostly uses simple non-Turing-complete script code to control transaction processes, which is an embryonic form of smart contracts. With the development of Blockchain technology, more complex and flexible Turing-complete scripting language for advanced smart contracts such as Ethereum have already appeared up till now in the world. That enables block chains to support many applications of macro finance and social systems.

F. The Application Layer

The application layer of the Blockchain technical model encapsulates various application scenarios and cases.It deploys the Blockchain technology to more applications in fields of digital currency, data storage, data authentication, financial transaction, asset management, election voting and so on. The programmable finance and society in the future will also be built on the application layer.

V. CONCLUSION

Blockchain technology, which is well-known as an underlying infrastructure and support technology to build trust of Bitcoin, has developed rapidly and received much attentions in recent years. On the basis of its development status and branch classification, our fruitful work has mainly presented a depth analysis for the technical characteristics and model of Blockchain technology. These findings has not only emphasized the significant research value of this technology but also suggested its promising applications in the future. And the future effort is required to better grasp and drive the development trend of Blockchain, which is remain to be explored.

ACKNOWLEDGMENT

This research was supported by Chongqing Science and Technology Commission Funded Research Project, fund number CSTC 2008AB3014.

REFERENCES

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[OL]. [2017-01-25]. Http://Bitcoin.org/Bitcoin.pdf

[2] Zou Jun. Blockchain technical guide. China Machine Press. Dec 2016.

[3] The promise of the blockchain: the trust machine. The Economist. Oct 2015.

[4] UK Government Office for Science. Distrubuted Ledger Technology : beyond Blockchain[R]. UK Government Chief Scientific Adviser, 2016. Https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

[5] Swan M. Blockchain: Blueprint for a New Economy[M]. Sebastopol, CA: O'Relly Media, Inc, 2015.

[6] Lin Xiaoxuan. Application of Blockchain technology in financial industry. China Finance, 2016, 8.

[7] Anonymous. New kid on the Blockchain. New Scientist, 2015, 225(3009): 7.

[8] Yuan Yong, Wang Feiyue. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4) : 481-494.

[9] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine Generals Problem[J]. Acm Transactions on Programming Languages & Systems, 2016, 4(3): 382-401.

[10] Larimer D. Transactions as proof-of-stake[OL]. [2017-07-05]. https://bravenewcoin.com/assets/Uploads/TransactionsAsProofOfStake10.pdf.