International Journal of New Developments in Engineering and Society
ISSN 2522-3488 Vol. 3, Issue 1: 01-07, DOI: 10.25236/IJNDES.19101

Research on Development Method of Application System based on Blockchain

Rong Wang

School of Network Security and Informatization, Weinan Normal University, Weinan, China,

ABSTRACT. *The blockchain was first used as the underlying "book" recording technology for bitcoin, which originated in 2009. After several years of development and improvement, it has gradually become a new type of distributed, decentralized, and trusted technology solution. Especially in the past two years, the blockchain has gradually separated from Bitcoin, and has become a hot spot for technological innovation. It has created a new data distributed storage technology, which has guided changes in system and programming concepts and may subvert the present. The organizational model of the business community. The characteristics of the blockchain are analyzed from the technical and application levels, and the classification of the blockchain is given. The design requirements of the blockchain are mined, and the application requirements of the blockchain consistency and scalability are analyzed in depth. The application system development method of blockchain and blockchain modeling are studied. The double-chain design model of account blockchain (abbreviated as ABC) and trading blockchain (TBC) is proposed. The contract is deeply analyzed, and the application principle of parallel execution model of chain code is put forward. Finally, the application technology of blockchain is summarized and forecasted.*

Keywords*: Blockchain, Application System, Develop Method*

1. INTRODUCTION

Bitcoin can be understood as a brand new digital currency in a narrow sense, and in a broad sense is considered a decentralized digital currency payment system. "Zhongben Cong" invented and adopted a technical solution called blockchain to record and maintain the transaction book of Bitcoin. There is no central server in the blockchain technology solution, and each computing device running the blockchain software is a peer node in the blockchain network, and no trust relationship needs to be established between the nodes, and any multiple nodes in the system The data of all information exchanged in the system for a period of time is calculated and recorded into a data block (block) by a cryptographic algorithm, and the fingerprint (hash) of the data block is generated for linking the next data block and verifying, through the collective Verify and maintain the way to build a reliable database. Bitcoin's blockchain technology revolutionized the "Byzantine general problem" with unchangeable, unforgeable and fully traceable security features, enabling a trustless consensus network system. This kind of consensus network system, which does not need to trust a central node, is fundamentally different from the organizational structure of today's human society and the Internet system, and is an organizational structure closer to nature and humanity. More and more technology giants, research institutions and technology groups have recognized the disruptive nature of blockchain technology and are involved in the study of blockchain.

2. BLOCKCHAIN APPLICATION SYSTEM REQUIREMENTS AND ARCHITECTURE DESIGN

In a distributed environment, data needs to use a coherence protocol to ensure consistency. The public chain mainly uses the proof of work (PoW) and the proof of stake mechanism; PBFT and CBFT are mainly used. In general, the higher the blockchain system, the better, but the consensus is expensive. Many computing power and node communication are spent on the consensus mechanism. For example, PBFT requires 3 rounds of voting, each round is adopted. Broadcast communication method. Each communication needs to be signed and unsigned, plus each transaction must be signed and unsigned. Therefore, 80% of the computing power is spent on consensus processing. Using different consensus algorithms will produce completely different The blockchain architecture and processes face different research issues. The problem facing PoW (public chain) is speed and scalability. The problem facing PBFT (license chain) is concurrency. PoW relies on the computing power of nodes to complete consensus. PBFT does not need it.

Blockchain is different from traditional databases. There are many differences between using blockchain development application systems and traditional systems. For example, using blockchain technology to develop a banking system can save many intermediate links, simplify processes, and save costs. Traditional The software architecture will also change. For example, IBM changed the traditional MVC (model, view, control) design pattern to MVBC (model, view, blockchain, control). Design blockchain application system also There is a new problem, that is, you can put functions on the application system, or put them on the blockchain and execute them with chain code. Many people praise the code on the chain, but the code execution on the chain consumes a lot of computing power. The code on the chain needs to build blocks, and building blocks is an expensive operational process that requires a consensus protocol. It is recommended that most of the functionality should be in the application system, with only a few features in the chain code.

Scalability has always been a challenge for blockchain systems, ranging from the first generation of bitcoin blockchains to the second generation of Ethereum blockchains. Despite the wide variety of solutions, each The solution has its flaws. For example, Ethereum proposes an infinite expansion of the solution mentioned in the white paper, which still cannot be achieved after two years. Some solutions abandon the definition of blockchain to solve scalability requirements, such as BigchainDB, RSCoin. They abandon the need for multiple copies of the blockchain to increase the speed of the transaction. It is yet to be observed whether these systems deviate from the traditional blockchain definition. In general, such systems are abandoned. The need for multiple copies, so it needs to be complemented in other aspects to increase security. The scalability of the Beihang chain is divided into 3 steps: (1) Using the CBFT parallel algorithm to do Byzantine General Vote to improve the speed of building blocks; (2) propose ABC, TBC dual-chain architecture, protect privacy, parallel computing, save computing power, simplify application architecture; (3) use ABC, TBC double-chain features, make a Chain can be split into two at runtime Chain, there are two different sets of hardware to execute the two chains separately to improve the speed. There are three mechanisms, which can use the original defined blockchain, high speed and scalability.

Although the blockchain is called a distributed database, its operation is very different from that of a traditional database. It is not the same as a relational database, but also an object database, a NoSQL database, or a temporal database. The same. High-speed blockchains are very different from low-speed blockchains: in low-speed environments, transactions are handled in a serial manner, so the consistency of low-speed blockchains is not a problem; in high-speed environments, transactions and Building blocks are parallel, so consistency is a new problem. Because traditional databases are individual transactions, and blockchains are built to maintain consistency. Blockchain consistency issues are not the same as traditional database consistency issues. For example, in a blockchain, there can be tens of thousands of transactions per second, and multiple blocks can be created per second, so each block can have tens of thousands of transactions. In these transactions, there may be many transactions with the same data. There is a connection. For example, in the CCTV micro-movie project, there will be tens of thousands of people broadcasting the same video in a few seconds, so in one piece, there may be thousands of on-demand broadcasts of the same video. If using a traditional database, each Times Broadcasting is a write, and there can be no more than one write in the same transaction on the same data. However, on the CCTV micro-movie platform, it must be allowed to have thousands of writes in one block at the same time. On a data.

The code on the chain was originally called a smart contract, giving people the impression of a smart and legally protected contract. But in fact neither is. The traditional smart contract does not have a matching legal framework, not effective. The legal contract of the power. The participants of the smart contract also have no relevant legal provisions and framework to protect. If supported by the legal framework, the code on the chain can become a contract. The execution of the code on the chain is closely related to the construction, so its execution The model interacts with the building process, so that the code on the chain becomes a difficult problem in theory. The difficulty lies in: every time you build a block, you need to find the code on the chain that must be started, and the code on some chains. In the system, the code must be executed before building the block. If there is a lot of data involved, and the code on the chain is very complicated, this will cause the code on the chain to conflict with the building block. Although the code on the chain is theoretically a difficult problem, But it is still available in the actual system.

3. BLOCKCHAIN APPLICATION DEVELOPMENT METHOD

At present, there is usually only one blockchain in the blockchain application, and all the accounts, contracts, transactions, etc. are placed on this blockchain. For example, the POC made by the Bank of Japan and the model of the European Central Bank still use the old style. General ledger structure. In May 2015, the European Banking Association (EBA) proposed a general chain concept. All institutions that join must share their internal account information with other participating institutions (There is no privacy. All participating organizations participate in the voting as a node in the chain to maintain the consistency of the accounts. The design of this generic chain does not meet the actual financial needs, because there is no protection of privacy. This architecture causes a large number of systems. Different data also violates the principles of software engineering. This design has poor scalability and low throughput. With the increase of services and the increase of nodes, the traffic will be very large and the delay will be higher and higher, so the performance will be lower. A new architecture is that all participating organizations share metadata and protocols, but do not share data (data is an account). All participating organizations can Trading units each other, and ensure privacy. According to this concept, there are at least two types of the following block chain.

1) ABC account blockchain (account blockchain): ABC only stores account information and post-transaction information, but does not execute transactions;

2) TBC trading blockchain: The TBC only stores information useful for transactions and performs related transactions.

ABC is responsible for inquiring, saving accounts, building blocks. For example, ABC stores financial institutions or household account information, and an account information in a chain is shared, which makes account information difficult to tamper with. At the same time, ABC also provides scalability, namely: When the blockchain processing size exceeds the limit, it can be split into multiple sub-ABCs, which are managed by different machines to maintain a balanced workload. A blockchain (chain 1) (as shown in Figure 6, block 1, block 2 Block 3) can be divided into two blockchains, the first (chain 2) is block 1, block 2, block 3, block 4A, and the second (chain 3) is block 1, block 2, block 3, block 4B And the two blockchains are consistent with the definition of the blockchain.

1) Block sub-chains: Chains 2, Chains 3 are block sub-chains. Each block has a timestamp; both use the hash encryption information of the previous block, and each transaction is verified;

2) Multiple independent copies: each node of chain 2, chain 3 has the same information, and works independently, mutual suspicion, mutual supervision;

3) Byzantine General vote: Chain 2, Chain 3 Both use the Byzantine General question to vote, tolerate less than one-third of the nodes maliciously cheated or hacked.

The TBC is responsible for building blocks and executing transactions. The TBC is only used as a channel (or location) for transactions and settlements. It does not store account information between the two parties, and the data stored in the TBC is also encrypted so that only the participating organizations can see the data. With ABC and TBC dual-chain architecture, each organization can have its own account blockchain. Only when information needs to be traded must it be shared on the trading blockchain. This mechanism means that after the transaction, the bank Or the organization can give access to the blockchain authority, and the data of the underlying client can only be seen by the relevant banks and regulatory agencies. In the CCTV blockchain application system, the ABC and TBC concepts are heavily used, and in foreign countries, Financial institutions also use this architecture designed by the Northern Airlines chain. The following example analyzes the computing power requirements when using a single-chain architecture. The Shanghai Stock Exchange had 97,735,200 accounts in 2014, and in May 2016, the daily trading volume was 12.18 million, an average of 846 times. There are at least 110 brokers, 20 banks in China, and there are also CSRC and trading centers. At least 150 (n) computing nodes are required. ICBC has 465 million individual customers and 509. .20 banks and other corporate clients about at least three billion accounts.

Each node in the ABC chain processes 18 transactions per second. Therefore, each node needs to query 0.2 billion   18=3.6   108 transaction query calculations per second. Each ABC chain processes 3.6   109 times per second for all nodes. Transaction query calculation. The workload of all nodes in an ABC chain is far less than the workload of one node in a common chain. In general, no more than 10 organizations participate in each transaction, such as exchanges, banks, clearing houses, clearing houses, etc. According to the Panda model, each ABC chain can trade with multiple organizations, and irrelevant organizations do not need to participate in transactions. Therefore, each ABC chain participates in several TBC chains without participating in all TBC chains. Therefore, The number of TBCs and accounts can be changed. If there is a clearing house structure, about 10 TBC chains are enough (a clearing house can support many organizations), assuming a worst case requires 20 TBC chains, each TBC chain has 30 nodes. Participate in consensus calculations. Each node has 10,000 accounts at a time (the old account can remain in the TBC history, but cannot be traded), which means that there are 10,000 accounts on a single TBC. Easy, 20 TBC chains indicate that 200,000 accounts can be traded at that time. Each TBC chain requires 30   30   R=3600 building block exchange messages per second, plus 14 400 (3600   4) building blocks. Encryption calculation. This is far less than the workload of one node in a common chain. Each TBC chain (30 nodes) has to deal with 10.8 (3600   30) building blocks exchange messages per second, 43.2 (108,000   4 10,000 blocks of cryptographic calculations, so the workload of all nodes in each TBC chain is only slightly larger than the workload of one node in a common chain. 10 million transactions per day, and each TBC chain processes an average of 2 million per day (10 million 4/20) transaction message, averaging 139 (2 million/(60 60 T) transactions per node per second, processing 556 transaction encryption calculations per node per second. Less than one node per common chain Workload. There are only 10,000 accounts per TBC node, far less than the ABC chain (0.2 billion) and the general one chain (3 billion) accounts, so each TBC transaction query workload will be far less than the ABC chain and general A chain transaction query workload.

Currently, the smart contract used in the blockchain system is intended to create an upgraded version of the code contract that cannot be tampered with and manipulated, and claims to be used in finance, trade, internet of things, registration, etc. But The DAO event makes People see the non-intelligent, non-contractual nature of the "smart contract." Smart contracts are not the legally defined contracts. The "smart contract" assumption is that code execution on the blockchain becomes legal. Contract. Data is difficult to be tampered with on the blockchain. This is obviously an unsuccessful assumption. To be a contract requires multi-method verification. Only use data or databases that are difficult to tamper with, and the contract is legally different. Far away. In the traditional reliable database management system (DBMS), the transaction should have four characteristics ACID (ISO/IEC10026-1:1992): atomicity, consistency (Consistency, isolation, durability. CAP theory states that distributed computing systems cannot simultaneously ensure consistency, availability, and partition tolerance. In the blockchain database, the ACID principle is not followed. The blockchain uses distributed ledgers to ensure data consistency, and builds blocks to maintain consistency. Each block contains many transactions. Blockchain The transaction mode is different from the traditional database transaction.

4. CONCLUSION

This paper begins with the blockchain components and application characteristics, discusses the blockchain requirements, including consistency requirements, software design requirements, scalability requirements, database requirements and chain code requirements. On this basis, the design of the Beihang chain system is designed. Architecture. The open blockchain connector OBCC was first proposed and the Java version of the blockchain connector, JBCC, was implemented.

REFERENCES

[1] Qing Sihan(2015). Critical Infrastructure Security Protection. Information Network Security, No.2, PP. 1-6

[2] Wang Hongkai, Wang Zhiqiang, Gong Xiaogang(2014). Discussion on Mobile Internet Security Problems and Protective Measures. Information Network Security, No.9, PP. 207-210.

[3] Wang Xueqiang, Lei Lingguang, Wang Yuewu(2014). Research on Mobile Internet Security Threats. Information Network Security, No. 9, PP. 30-33.
[4] Yu Lian, Deng Enyan(2017). Blockchain Technology. Chinese Computer Society Newsletter, 2017,Vol. 13, No.5, PP. 10-15.
[5] Cai Weide, Zhao Wei, Zhang Chi, Yu Lian(2016). Discussion on the British Central Bank Digital Currency RSCoin. Electronic Finance, 2016, No.10, PP. 78-81.