Research on the Application of Cryptography on the Blockchain

Research on the Application of Cryptography on the Blockchain

Sheping Zhai[1,2], Yuanyuan Yang[1*], Jing Li[1], Cheng Qiu[1] and Jiangming Zhao[1]

[1] School of Computer Science & Technology, Xi'an University of Posts & Telecommunications, Xi'an, Shaanxi, 710121, China

[2] Shaanxi Key Laboratory of Network Data Analysis and Intelligent Processing, Xi'an,Shaanxi, 710121, China

[*]Corresponding author's e-mail: yangyy0614@163.com

Abstract. Blockchain is an innovative application model that integrates distributed data storage, peer-to-peer transmission, consensus mechanisms, digital encryption technology and other computer technologies. It is decentralized, secure, and Information disclosure. In the blockchain, digital encryption technology has a core position. The security of user information and transaction data is a necessary condition for the promotion of blockchain. The development of cryptography technology promotes and restricts the further development of blockchain. This paper outlines the infrastructure of blockchain, including the data layer, network layer, consensus layer, contract layer and application layer. The principles of encryption technology is introduced briefly, such as hash function, asymmetric cryptosystem, digital signature. The application of cryptography in all levels of blockchain is analyzed, including data layer, network layer, consensus layer, etc. It shows that cryptography runs through the whole blockchain system. The existing security problems of blockchain is analyzed, and the future research direction is expected.

1. Introduction

Blockchain is a distributed database with features of decentralized, traceable, non-tamperable, secure and reliable features. It integrates P2P (Peer-to-Peer) protocol, digital encryption technology, consensus mechanism, smart contract and other technologies together. Abandoning the maintenance mode of the traditional central node and adopting the method of mutual maintenance by multiple users to realize the information supervision among multiple parties, thereby ensuring the credibility and integrity of the data. The blockchain platform can be divided into public chain, private chain and alliance chain. All nodes in the public chain can join or withdraw freely; the private chain strictly limits the qualification of participating nodes; the alliance chain is jointly managed by several participating institutions. Bitcoin was proposed by Nakamoto in 2008[1], which is the most successful case of digital currency, and is also the most typical application of blockchain. In addition, the blockchain has expanded its unique application value in many aspects and has shown its potential to reshape society.

As a representative of distributed database, blockchain stores all user transaction information on the blockchain, which has high requirements for the security performance of blockchain. Blockchain is a decentralized peer-to-peer network. Nodes do not need to trust each other and there is no central node. Therefore, transactions on the blockchain also need to ensure the security of transaction information on unsecured channels and to maintain the integrity of transactions. It can be seen that cryptography

technology occupies the most central position in the blockchain. In blockchain, cryptography technology is mainly used to protect user privacy and transaction information, and ensure data consistency, etc.[2] This paper briefly introduces the cryptographic techniques such as hash algorithm, asymmetric encryption algorithm and digital signature, also elaborates the blockchain infrastructure, the blockchain structure, bitcoin address, digital currency trading and other technologies of blockchain, and also explains how cryptography technology protects privacy and transaction maintenance in the blockchain in detail.

2. Blockchain infrastructurs

According to Melanie Swan, founder of the Blockchain Science Institute, blockchain technology has experienced two phase, the first one is the blockchain 1.0 phase of multi-technology portfolio innovation represented by Bitcoin, the second one is the blockchain 2.0 phase represented by Ethereum, which is transferred by digital assets. Typical applications of blockchain technology mainly include Bitcoin, Ethereum, Hyperledgers, etc. Although the implementations are different, there are many commonalities in the overall architecture. As shown in Table 1, the blockchain platform can be divided into five levels: network layer, consensus layer, data layer, contract layer and application layer.

Table 1. Blockchain architecture.

	Bitcoin	Ethereum	Hyperledger
Application layer	Bitcoin trading	Ethereum trading	Enterprise blockchain
Network layer	TCP-based P2P	TCP-based P2P	HTTP/2-based P2P
Contract layer	Script	Solidity/Script EVM	Go/Java Docker
Consensus layer	PoW	PoW/PoS	PBFT/SBFT
Data layer	Merkle tree	Merkle patricia tree	Merkle Bocket tree

The data layer mainly uses the block data structure to ensure the integrity of data storage. Each node in the network encapsulates the data transactions received over a period of time into a time-stamped data block and links the block to the current longest main blockchain for storage. This layer involves the main techniques of block storage, chain structure, hash algorithm, Merkle tree, time stamp and so on.

The consensus layer mainly includes a consensus mechanism, which enables each node to reach a consensus on the validity of block data in the decentralized system[2]. The consensus mechanism mainly has PoW, PoS, PBFT and SBFT. The smart contract that is mainly included in the contract layer is the basis of the blockchain programmable feature. The computerized program that can automatically execute the contract terms is stored in the blockchain in the form of code and data sets. Smart contracts, driven by time or events, are executed by blockchain nodes in a distributed manner. All relevant terms are coded, automatically settled, and triggered by signatures or other external data messages. The network layer includes various data transmission protocols and verification mechanisms. The blockchain is a typical P2P network. All nodes are connected through a planar topology and have no central nodes. Any two nodes can be freely traded, and any node can join or leave the network at any time. The P2P protocol in the blockchain is mainly used for information transmission between nodes. The application layer mainly includes Bitcoin, Ethereum and Hyperledger and so on. Bitcoin is mainly for digital currency transactions. Ethereum adds

decentralized applications based on digital currency. Hyperledger do not support digital currency transactions, mainly are enterprise-level blockchain applications.

3. Hash and block structure

The hash algorithm is a function that maps a sequence of messages of any length to a shorter fixed-length value, and is characterized by susceptibility, unidirectionality, collision resistance, and high sensitivity[3]. Hash usually used to ensure data integrity, that is, to verify the data has been illegally tampered with. When the data tested changes, its hash value also changes correspondingly. Therefore, even if the data is in an unsafe environment, the integrity of the data can be detected based on the hash value of the data.

SHA is a type of cryptographic hash function issued by the National Institute of Standards and Technology (NIST) with the general characteristics of a cryptographic hash function. The SHA256 algorithm is a class of the SHA-2 algorithm cluster, which generates a 256-bit message digest. The algorithm's calculation process includes two stages: message preprocessing and main loop. In the message preprocessing stage, binary bit filling and message length filling are performed on the information of any length, and the filled message is divided into several 512-bit message blocks. In the main loop phase, each message block is processed by a compression function. The input of the current compression function is the output of the previous compression function, and the output of the last compression function is the hash value of the original message.

RIEPEMD, a summary of the RACE original integrity check message, is a hash function algorithm developed by the COSI research team of the University in Leuven, Belgium. RIPEMD-160 is the most common version of RIPEMD[5]. As the SHA series functions, the first step of the algorithm is message complement, and the complement method is identical to the SHA series algorithm. The core of the processing algorithm is the compression function, which is a loop, where each loop consists of 16 step functions. Using different original logic functions in each loop, the processing of the algorithm is divided into two different cases, with five of the two original logic functions running in reverse order. After all 512-bit packet processing is completed, the resulting of 160-bit output is the hash value of the original message.

For blockchain, hash functions can be used to perform block and transaction integrity verification. In the blockchain, the hash value of the information of the previous block is stored in the header of each block, and any user can compare the calculated hash value with the stored hash value. In turn, the integrity of the information of the previous block is detected. Similarly, the hash function can be used to generate public-private key pairs.

The hash pointer is a data structure that contains, in addition to the usual pointers, some data information and password hashes associated with the information. A normal pointer is used to retrieve information, and a hash pointer is used to verify that the information has been tampered[6]. As shown in Figure 1, the blockchain is a list of hash pointers, each of which is connected by using a hash value. It is verified according to the hash value whether the data contained in the block is changed, thereby ensuring the integrity of the block information.

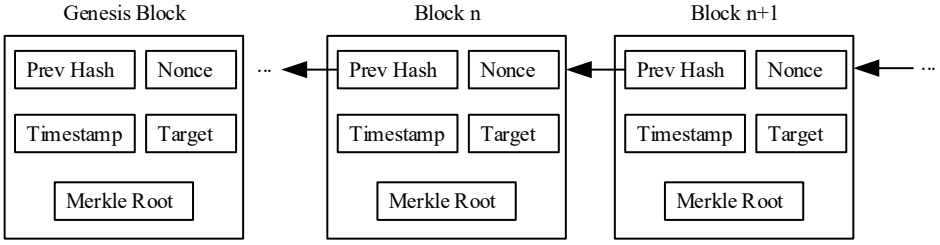

Figure 1. Blockchain structure.

The blocks in blockchain hold all the data information of the whole network, mainly composed of the block header containing metadata and the block body containing all transaction data[7]. The block header encapsulates the previous block hash, the current block's difficulty target, and the current block

solution random number, Merkle root, and timestamp. The block body contains a list of transactions for storing transaction information.

Prev Hash: The block hash is a key segment of the blockchain. This field is the hash value of the data information of the previous block, and all the blocks on the chain are sequentially connected.The resulting longest main chain from the creation of the block to the current block is finally formed. Each block not only has the location information of the previous block, but also can verify the integrity of the data contained in the block according to the previous block hash value.

Nonce: The header information of each data block contains a random number, and the initial value is 0. The node running the bitcoin mining machine continuously performs a SHA256 operation on the overall data of the block. When the SHA256 value calculated by the current random number does not meet the requirements, then the random number is increased by one unit, and the SHA256 operation is continued. Until the SHA256 value is less than the current data block SHA256 value, then a new data block is generated and the P2P network accepts the new data block. Therefore, the process of generating a new block is actually a process of calculating the SHA256 value and comparing it with the target value. This process of bitcoin data block generation is called Proof of Work.

Timestamp: The blockchain technique requires that the node must have a timestamp in the current data block header to indicate the write time of the block data. The blocks on the main chain are arranged in chronological order. The timestamp can be used as a proof of the existence of block data, helping to form a blockchain database that is not tamperable and unforgeable.

Target: The target is to make the computing power of the entire network approximately the difficulty level required to generate a block every 10 minutes. The target is automatically recalculated by the blockchain network based on the results of the past two weeks. The target is determined by the SHA256 value in the block. The SHA256 value in the control block header should fall within the controllable range target range to increase or decrease the target.

Merkle Root: The Merkle Tree is a hash binary tree originally proposed by the famous cryptographer Merkle to quickly verify the integrity of large-scale data. As shown in Figure 2, the Merkle tree typically contains the transaction database for the block, the root hash of the block header, and all branches along the underlying block data to the root hash. The Merkle tree operation usually groups the data of the block and inserts the generated new hash value into the Merkle tree. Until the last root hash is left and recorded as the Merkle root of the block header, it is finally constructed into a tree structure. Bitcoin uses a double SHA256 hash function, which is to pass two SHA256 hash operations on the original data of arbitrary length, and use 256-bit binary digits for unified storage and identification.

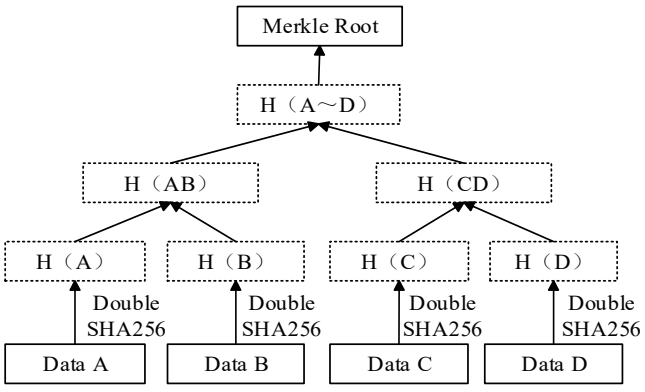

Figure 2. Merkle tree.

Transaction list: The transaction list contains a lot of details of the transaction record, including the time of each transaction, transaction number, bitcoin amount, payer and other information. In the data block, each bitcoin is written and received together, so each bitcoin can be traced back.

4. Public key system and Bitcoin

The core technologies of cryptography include symmetric encryption and asymmetric encryption. Asymmetric encryption, called public key encryption, can well solve the problem of early distribution of keys in symmetric encryption. In an asymmetric encryption algorithm, the encryption key and the decryption key are different, and are called a public key and a private key, respectively. The private key usually needs to be generated by a random number algorithm, and the public key is calculated by performing an irreversible algorithm. The asymmetric encryption algorithm has the advantages of separate public and private keys, which can be transmitted over unsecured channels. Similarly, it has the disadvantages of low processing speed and low encryption strength, and it is necessary to ensure the security of the asymmetric encryption algorithm based on mathematical problems.

Elliptic Curves Cryptography is a common public key encryption algorithm. The security depends on the difficulty of the elliptic curve discrete logarithm problem[8]. The public key encryption algorithm used in the blockchain is secp256k1 in the elliptic curve. secp256k1 is based on an elliptic curve over a finite field. Due to its special construction, its optimized implementation can achieve a 30 percent improvement over other curves. The constant of secp256k1 can effectively avoid the possibility of backdoors.

The key pair in the Bitcoin system consists of a private key and a unique public key derived from it. The key pair is generated by public key encryption. In the payment link of bitcoin transactions, the recipient's address is generated by a public key, called the bitcoin address, which is the payee[9]. As shown in Figure 3, the private key is a number, usually randomly selected, and the public key is generated by encrypting the private key by elliptic curve multiplication. And a single-entry encrypted hash function is used to generate the bitcoin address through the public key.

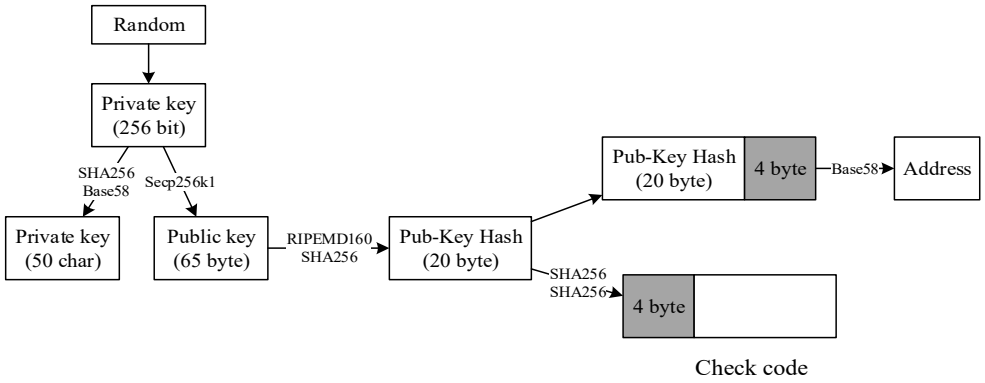

Figure 3. Bitcoin address generation process.

Generating a Bitcoin private key essentially selects a number between 1 and 2^{256}, and it is necessary to ensure that the result of the selection is unpredictable or non-repeatable. Bitcoin uses the random number generator of the operating system to generate a 256-bit random number as a private key, and multiplies the randomly generated private key k by the defined generation point G on the curve to obtain another point on the curve. That is, the corresponding public key K. The elliptic curve relies on the discrete logarithm problem. The relationship between k and K is fixed, but it can only be a single operation, that is, K is obtained from k, and k is difficult to obtain from K. The generation of currency addresses uses different algorithms on different platforms.

Bitcoin uses the SHA256 and RIPEMD160 double hashes to derive the bitcoin address; Ethereum uses the Keccak256 algorithm to generate the Ethereum address[10]. In Bitcoin, the public key K is used as input, and its SHA256 hash value is calculated. Recalculate the RIPEMD160 hash value to get a 160-bit number as the public key hash. Finally, the public key hash is Base58 encoded to form a bitcoin address. Base58 is a widely used encoding format, not only for Bitcoin, but also for other crypto currencies, which combines effective compression, easy reading, and error diagnosis. Bitcoin uses Base58Check in Base58 encoding. A 4-byte error check code is added to the encoded data to effectively check for errors in the transcription.

5. Digital signature and currency trading

The digital signature system usually consists of two parts: a signature algorithm and a verification algorithm. The signature algorithm is used to generate a digital signature on the message, the signature is usually controlled by the signature key, the signature algorithm or the signature key is kept secret, and is controlled by the signer. The verification algorithm is used to verify the digital signature of the message, and the message can be verified according to the signature effectively. The verification algorithm is usually controlled by the verification key, but the verification algorithm and the verification key are public, so the person who needs to verify the signature can easily verify it.

In a cryptocurrency system in which the blockchain is the underlying technology, the digital currency owner hashes the content of the previous transaction order of the digital currency and the address of the next owner. The data digitally signed with its own private key is appended to the end of the transaction list and sent to the recipient. The recipient needs to verify the received information to prove the information of the previous owner, and then verify the owner of the transaction. Each transaction in the blockchain records the current owner, previous owner, and next owner of the currency. Therefore, the whole process of money can be traced back, effectively avoiding double payment, false transactions and other issues[11].

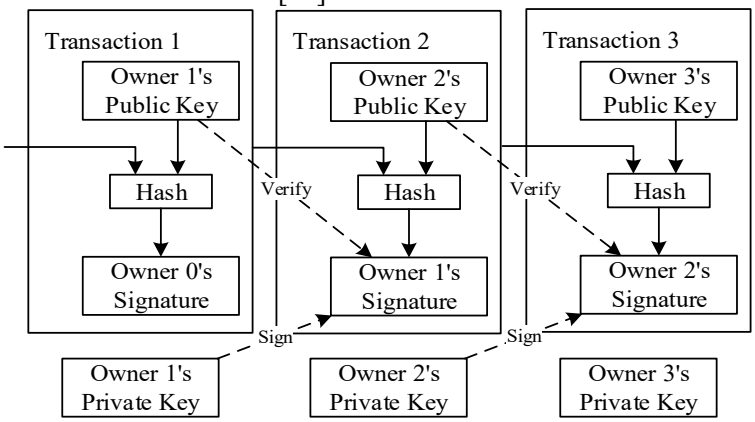

Figure 4. Signing and verification of the transaction.

As shown in Figure. 4, user 2 performs payment transactions with user 3. When User 2 needs to pay 10 Bitcoins to User 3, the amount and the source of the Bitcoin are first recorded on the transaction slip. The ten bitcoins of the user 2 are from the user 1, and therefore, to complete the payment transaction of the user 2 to the user 3, it is necessary to record the source of the bitcoin, the amount of the payment, and the digital signature of the user 2.

In the transaction authentication process, the signature is mainly completed by the payer. The payer of the transaction first hashes the transaction data information of the previous transaction to obtain its hash value. The payer encrypts the hash using its own private key. The encrypted data is sent to the recipient simultaneously as the digital signature of the previous transaction data message and the previous transaction data. After receiving the information, the receiver will verify the legality of the transaction and use the same hash function as the previous step to obtain a hash summary from the received transaction data information. Finally, the payer's public key is used to decrypt the additional digital signature of the previous step to obtain another hash digest.By comparing the two summaries, the validity of the order can be ensured. If the two contents are the same, the recipient can confirm the order is valid.

6. Blockchain consensus mechanism

The consensus mechanism is used to determine the accounting nodes in the blockchain network and is used to confirm the transaction information, thereby ensuring the consistency of the data of each block. The early Bitcoin blockchain used a Proof of Work mechanism. This mechanism relies heavily on node computing power to ensure consistent accounting for bitcoin network distributed accounting. The PoW mechanism relies on the computing power competition between distributed nodes to ensure the

consistency and security of the entire network blockchain data. Each node needs to rely on its own power to solve the SHA256 calculation problem, that is, to find a suitable random number Nonce, so that the SHA256 hash value of the block header original data is smaller than the setting value of the difficulty target in the block header: $H(n \| h) \leq t$.

H is the SHA256 hash function; *n* is the random number Nonce; *h* is the block header data, mainly including the previous block hash, Merkle root, etc.; *t* is the difficulty target, the smaller the t value, the harder the n value is found; The node that is first found can obtain the accounting rights of the new block. The consensus process of PoW in the blockchain network is as follows:

- Each new transaction is broadcast to all nodes in the blockchain network.
- In order to construct a new block, each node collects all transactions received since the previous block was generated, and calculates the Merkle root of the block header based on these transactions.Increase the Nonce of the block header from 0 to 1, until the twice SHA256 hashe value of the block header are less than or equal to the set value of the target.
- The whole network node participates in the calculation at the same time. If a node first finds the correct random number, the node will obtain the new block's billing rights and mining reward, and broadcast the block to the entire network.
- After receiving the new block, the other nodes verify the validity of the transaction and the random number Nonce in the block. If correct, the block is added to the local blockchain, and the next block is built based on the block. .

With the development of blockchain technology and the emergence of various competitive currencies, researchers have proposed various mechanisms that can be reached without relying on computing power. For example, PoS and DPoS, as well as some distributed consistency algorithms, such as PBFT, Raft, etc., these consensus mechanisms have their own advantages and disadvantages, and the application scenarios are also different.

7. Security issues in blockchain

The global ledger that stores transaction information in blockchain technology is public, and any node that joins the blockchain network can obtain a complete copy. By analyzing the transaction records in the global ledger, potential attackers may pose a threat to the user's transaction privacy and identity privacy. Trading privacy threats means that an attacker can obtain valuable information by analyzing transaction records. For example, the fund balance and transaction details of a specific account, the flow of specific funds, and so on. The identity privacy threat means that the attacker can obtain the identity information of the trader by combining some background knowledge based on analyzing the transaction data.

In order to counter this attack, we usually use coinjoin, ring signature, Zero-Knowledge Proof and so on. Dash uses a coin measure, Consolidating multiple transactions into a single transaction by a coin node, thereby hiding the relationship between the payment address and the payment address.However, the effect of the coin is too dependent on the number of users participating in the coin, and the large amount of transactions is easy to be cracked. The analyst can also analyze the user's private information by a certain method, and the mechanism of the coin is easy to crack and cannot achieve the desired effect. Therefore, it is necessary to add a cryptographic mechanism to ensure the security of the mixed currency. Menero uses a ring signature, which recognizes the verification signature, and does not know the identity of the signer, thereby hiding the identity information of the sender of the transaction. Zerocash uses zero-knowledge proof to prove the correctness of the transaction to the verifier without leaking the transaction information and additional information. However, the use of cryptography requires a lot of computing resources, and needs to modify the underlying protocol to reduce the efficiency of the blockchain.

Data security and privacy protection in the blockchain are severely challenged, and advanced cryptography techniques can effectively solve such problems, but there are still weak links. The private key is generated by the random number generator in the computer system, which is called pseudo-random, has certain regularity, and has the threat of being cracked. Although the SHA-2

algorithm does not have an effective method to crack this series of algorithms, once it is cracked, the privacy and security of all data in the blockchain will no longer exist.

In future research, it is necessary to develop a coin-rich mechanism under the protection of cryptography mechanisms, and to minimize the performance requirements.A more secure and reliable cryptographic encryption algorithm is needed to improve the security of the blockchain.

8. Conclusion

This study introduces the main applications of cryptography in the blockchain and analyzes existing problems. Firstly, starting from the blockchain infrastructure, the blockchain technology is simplified. Secondly, the cryptography technology is introduced to elaborate the blockchain. Finally, the existing security problems in the blockchain are analyzed. It shows that digital encryption technology runs through the blockchain system and is the core technology of the blockchain system. This paper emphasizes that the research of cryptography plays a decisive role in the development of blockchain, and prospects the future research direction of blockchain technology.

References

[1] Nakamoto, S. (2008) Bitcoin: A peer-to-peer electronic cash system. Consulted., 165: 55-61.
[2] Zhu, Y., Gan, G.H., Deng, D. (2016) Security Research in Key Technologies of Blockchain. Information Security Research., 12: 1090-1097.
[3] Liu, X.F. (2017) Research on blockchain performance improvement of Byzantine fault-tolerant consensus algorithm based on dynamic authorization. Zhejiang University.
[4] Wang, X., Lai, X., Feng, D. (2005) Cryptanalysis of the Hash Functions MD4 and RIPEMD. Advances in Eurocrypt., 3494: 1-18.
[5] Shen, Y., Wang, G. (2017) Improved preimage attacks on RIPEMD-160 and SHA-160. Ksii Transactions on Internet & Information Systems., 12: 727-746.
[6] Wang, H.Q., Wu, T. (2017) Cryptography in Blockchain. Journal of Nanjing University of Posts and Telecommunications., 37: 61-67.
[7] Yuan, Y., Wang, F. (2016) Current Status and Prospects of Blockchain Technology Development. Acta Automatica Sinica., 42: 481-494.
[8] Miyaji, A. (1994) Elliptic Curves Suitable for Cryptosystems. Ieice Transactions on Fundamentals of Electronics Communications & Computer Sciences., 77: 98-105.
[9] He, P., Yu, G., Zhang, Y.F. (2017) Prospective review of blockchain technology and application. Computer Science., 44: 1-7.
[10] Zhai, S.P., Li, Z.Z. (2018) The data block chain of the key technologies Consistency. Computer Technology and Development., 8: 1-6.
[11] An, Q.W. (2017) Research and application of key technologies for decentralized transactions based on blockchain. Donghua University.