BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research
https://ojs.bilpublishing.com/index.php/jcsr

ARTICLE

Voting System Based on Blockchain

Zihan Guo Xiang He[*] Peiyan Zou

North China University of Science and Technology, Tangshan, China

ARTICLE INFO

Article history
Received: 13 January 2021
Accepted: 1 February 2021
Published Online: 18 April 2021

Keywords:
Blockchain
Voting system
Decentralization
Data cannot be tampered with

ABSTRACT

Online ballot box system has the advantages of high efficiency and environmental protection, but the existing network voting technology still has a lot of matter. Almost all electronic voting system could be proved to be intrusion. The administrator of the system could tamper with the data for benefit, and the system may be attacked by hackers. The safety and fairness of the existing network voting system depend entirely on the safety and credibility of the website itself, but these cannot guarantee the fairness of voting. Make full use of blockchain technology, so that voting, even if there are malicious participants, but also to ensure the correctness and safety of the vote. The introduction of block chain technology, block chain has decentralized, data tampering and other characteristics. P2P network is applied in the block chain layer to construct a distributed database, digital signature algorithm and encryption technology are used to ensure that the data cannot be tampered with, consensus network algorithm is used to ensure the consistency of the data in the network, and timestamp technology is applied to save the data blocks in a chain structure connected end to end. It paper focuses on the implementation of P2P network networking mode, node block synchronization, data and block verification mechanism and consensus mechanism to ensure data consistency in the network layer of block chain layer. Using time stamp, Merkle tree, asymmetric encryption and other technologies to design data blocks and use chain structure to store data blocks. Combined with the characteristics of blockchain, a fair and transparent voting system is constructed. Model aims to apply the block chain technology to the voting scenario and design a secure block chain voting architecture. It system is designed and developed based on the block chain system. It makes full use of its decentralization, removes the dependence of electronic voting on trusted third parties, and protects the privacy of voters and candidates. Data cannot be tampered with. Once the data are stored in the block chain, it cannot be tampered with. It provides a real and credible database.

1. Introduction

In order to indicate the origin of voting with blockchain matter, the following background is worth mentioning.

1.1 Discussion of Voting Issues

On the surface a lot of people might think voting is an easy thing to do, just cast your vote, count up the results and publish it. But it is not as simple as you think. Voters

**Corresponding Author:*
Xiang He,
Electronic information engineering, North China University of Science and Technology, Tangshan, China;
Email: 2216839099@qq.com

DOI: https://doi.org/10.30564/jcsr.v3i2.2797

must cast only one vote. We must prevent people from voting twice. With the rapid development of network technology, the traditional questionnaire survey method has fallen behind. It has a complicated voting procedure and takes a long time to complete the user's vote. The task of counting votes is very heavy, and it is easy to make statistical mistakes and is easy to be manipulated. Modern society is the network information age, and the use of network technology could improve people's work efficiency, save the cost of human and material resources, promote the development of society [5].

1.2 The Dilemma of Voting in the United States

With a crucial election looming in the United States, little progress has been made in ensuring the integrity of the voting system. Existing voting systems leave plenty of room for doubt: it is possible to mimic voters in the first place (though surveys have found this to be a negligible proportion in the us);Postal ballots could be changed or stolen; Election officials may miscount; And almost all electronic voting machines have proven to be breakable.

1.3 Blockchain Technology Solve the Matter

However, the booming blockchain technology in recent years may well resist the corruption of the authorities and hackers [1]. Blockchain is a new distributed infrastructure and computing paradigm, which USES ordered chain data structure to store data, USES consensus algorithm to update data, and USES cryptography technology to guarantee data safety [11,12,13,14]. Came up with the block chain to provide the basis for the emergence of a new electronic voting system, voting system based on block chain could be ruled out the possibility of manipulation, the decentralized, distributed network structure is suitable for the voting system, voting centers do not need special maintenance and management of sorting system and network, to ensure the transparency of the network, also to prevent the malicious vote or tamper with the vote fraud, cheat cheating, its anonymity, some voters' personal information could be hidden, protect personal privacy [3]. Voters could also verify and track their votes.

1.4 The Matter Requirements

1) How to use block chain technology to construct an underlying design or a set of algorithms to solve the matter of online voting?

2) Evaluate the possible matter of blockchain technology in solving voting matter and try to improve.

3) Cybersafe and voting experts agree that blockchain is unnecessarily complex and no more secure than other network voting. Can blockchain technologies be combined with other technologies to reduce complexity and improve safety?

2. The Description of the Matter

2.1 For the Use of Blockchain Technology to Construct an Underlying Design or a set of Algorithms to Solve the Matter of Online Voting

To meet the requirements of individuals, enterprises, institutions and governments, design a fair, fair and transparent voting system. The voting system has the following three sub-indicators:

1)Ensure that voting data cannot be usurped;

2) The voting data could be traced and verified;

3)Vote anonymously to ensure the privacy of voters;

Blockchain is decentralized. Data cannot be tampered with, and it is safe and reliable. Once the data is stored in the blockchain, it cannot be tampered with. Blockchain is a real and reliable database that cannot be tampered with. Therefore, blockchain technology is the best solution to guarantee the fairness and safety of the voting system.

2.2 Analysis of Blockchain Technology in Solving Voting Matter

Blockchain technology is communal in many fields because it is distributed and untamable. Despite the advantages of the technical principle, it still requirements to be developed by human beings. Since it is a human software product, it is inevitable that there will be safety holes, which may ultimately make products using blockchain technology vulnerable. From a legal perspective, identification verification is difficult, time-consuming and often inaccurate, voters are sometimes wrongly singled out as ineligible to vote, and unqualified people are sometimes allowed to vote and repeat votes occur. Recounts (and recount requests) are common because ballots are counted inefficiently and conflicting agreements make auditing slow and difficult. Lawsuits proliferate when candidates seek an advantage. Whenever this happens, public confidence in the electoral system and results will lead over time to a lack of confidence in elected officials and governments, which may lead to lower voter turnout in the future. Voters' feelings, prejudices, confusion, misunderstandings and fears about the new voting technology are likely to be inflamed and used for political gain. It will create more confusion and mistrust, slowing the procedure needed to construct the necessary legal support around the newer voting forms. It runs counter to the direction we need to move towards a safe and more accurate electoral system.

In addition, other challenges, such as the current block-

DOI: https://doi.org/10.30564/jcsr.v3i2.2797

chain technology does not well support the required speed and breadth, are also a question of whether a national blockchain election could be held. Also, blockchain is only as good or bad as its ecosystem, inputting wrong information and blockchain will do a great job storing it! While blockchains are immutable, the voting tools voters might use may not be. Voting from smartphones sounds great, but smartphones are one of the least secure electronic devices on the market. Someone could change your vote before the phone is sent to the blockchain. Therefore, there are still many matters and drawbacks in applying blockchain technology to solve the voting matter, and we could only construct the model under some ideal conditions [6].

2.3 How to Reduce the Complexity of Blockchain Technology and Improve the Safety through the Combination of Other Technologies

The electronic voting procedure includes: the voting initiator initiates the voting, the voting certification registration center completes the distribution and screening of the votes, the voters who are distributed the votes conduct the voting, after the voting is completed, the counting center completes the counting of the votes and the publication of the results. As voting results often affect personal interests, participants in online electronic voting may become dishonest due to the matter of being falsely recognized, coerce, bribe-taking, and existence of internal ghosts, etc. These dishonest participants may tamper, falsify, replay and deny voting data, thus affecting the correctness of voting results. In particular, the third party may have a ghost, so that its credibility is difficult to be guaranteed. In the whole voting system, only the voting initiator is credible and honest when he/she initiates the voting. However, through the introduction of blockchain technology, the decentralized registration and certification center is realized, the dependence of electronic voting on trusted third parties is removed, and the privacy of voters and candidates is protected. At the same time, the project provides an electronic voting system scheme based on verifiable secret sharing and other technologies, which could effectively guarantee the safety of electronic voting. Blockchain technology is one of the research hotspots in the field of network safety and fintech. It is a kind of point-to-point decentralized data sharing technology, and the data stored in it do not need to rely on a trusted third party. In other words, the data stored in it cannot be tampered with, forged, refuted, impersonated, and reproduced, so as to effectively guarantee the data safety and automatically form a credit relationship between nodes [2]. Up to now, blockchain technology has successfully protected the safety of more than $100 billion of digital assets such as bitcoin, and its safety has been fully verified [10]. If the blockchain technology could be effectively utilized, it may not need to rely on trusted third parties to complete safety authentication [4]. Based on the advantages of blockchain technology, if blockchain technology could be combined with artificial intelligence, big data and other technologies, the complexity of blockchain technology could be greatly reduced.

3. Models

In order to achieve the decentralization of the blockchain, the data cannot be tamper-proof, safety and credibility requirements, the blockchain layer will use the P2P network to construct a distributed database, using digital signature algorithms and encryption technology to ensure data non-tamperable, consensus algorithm to ensure the network The consistency of the data, and the use of timestamp technology to save the data block in a chain structure connected end to end As shown in Figure 1, the blockchain layer is divided into a network layer and a storage layer [11,12,13,14]. The network layer realizes the construction of the network, and the verification mechanism and the consensus mechanism ensure the safety and consistency of the data. The design focus is on constructing the P2P network, realizing the verification mechanism and the consensus mechanism. The storage layer encapsulates the data block, and the data block is stored in a chain of end to end. The design focus is to construct the data block structure and the chain of the block by using timestamp, hash function, Merkle tree, asymmetric encryption and other techniques to storage. The blockchain layer will be based on maven, with Java as the development language.

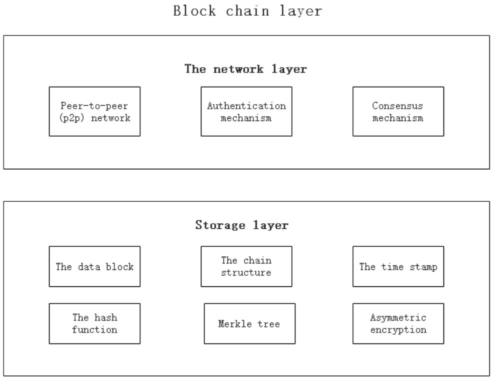

Figure 1. Block chain

3.1 Block Chain Layer Design

3.1.1 Node P2P Network Construction

The blockchain system is a distributed, decentralized system with nodes that are peer-to-peer, autonomous, and free to join. Therefore, this design uses a peer-to-peer network as the networking mode. P2P networks have the ad-

DOI: https://doi.org/10.30564/jcsr.v3i2.2797

vantages of decentralization, scalability, decentralization, and robustness. They could organize nodes participating in data check and accounting, so that the system could run stably under decentralization. There is no central node in the P2P network, and the nodes are interconnected through a flat topology. Each node has the same functionality and provides network services. Each node has the functions of discovering new nodes, synchronizing blocks, applying layer network routing, verifying block data, and propagating block data.

Constructing a P2P network is the initialization procedure of the blockchain layer. If a new node joins the P2P network for the first time, the IP addresses of other nodes in the network are required. DNS seed A DNS server that provides the IP address of a node on a P2P network to help discover nodes. Therefore, the DNS seed method is used to join the P2P network, and the TCP protocol is used, and the port 8333 is used. The joining procedure is as follows.

1）Connection seed node

2）Receive node IP address list

3）The nodes in the connection list

4）When one or more connections are established, the node sends its own IP address to its neighbors. Neighboring nodes will forward IP addresses, allowing more nodes to receive IP addresses, ensuring a more stable connection.

The specific flow chart of constructing a P2P network is as follows.

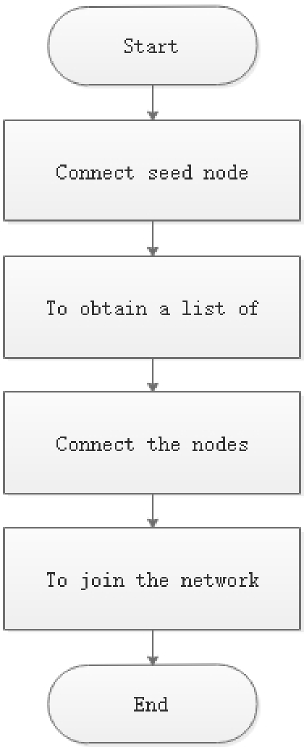

Figure 2. P2P Network flow chart

3.1.2 Block Synchronization

When a node joins a P2P network, there is no blockchain data or the data is incomplete. You need to request data blocks from other nodes. It procedure is called block synchronization and is the initialization procedure of the blockchain layer. The node will first load and verify the local data block first, which is divided into block verification and Block data verification. First verify whether the previous block is on the main chain, and after completing the block verification, perform block data verification. After verifying the local data block, the node performs block synchronization.

The block synchronization procedure is as follows:

1) Request data block information from the node that has established the connection, determine whether the node times out when it is timed, and request other nodes if it times out;

2) The requested node will first send the block height, and the requesting node compares the received block height with the local block, such as the height of the block, and issues a request to acquire the data block;

3) Verify the validity of the data block;

4) Continue to send the synchronization request until the node with the highest block height is found, and the procedure of requesting the data block synchronization is as shown in the figure.

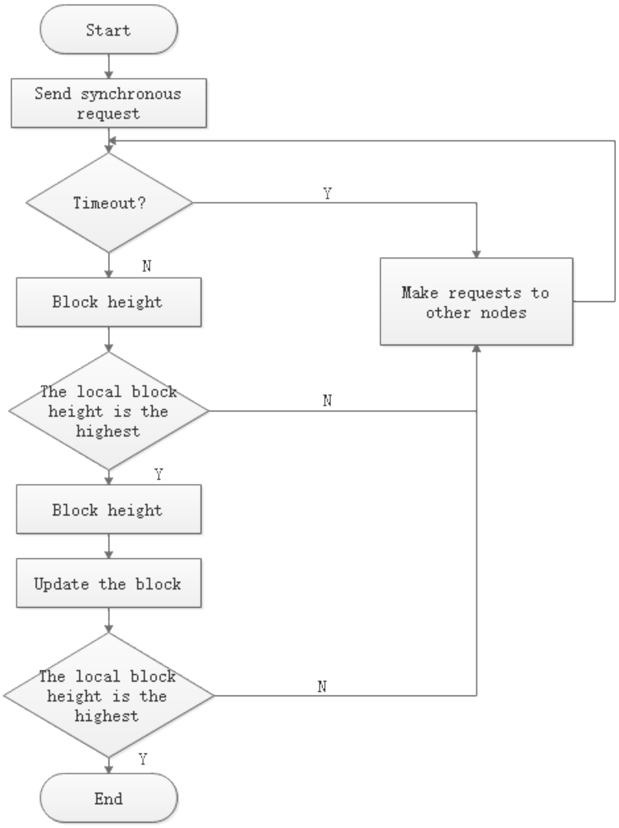
Start
Send synchronous request
Timeout?
Y
N
Make requests to other nodes
Block height
The local block height is the highest
N
Y
Block height
Update the block
The local block height is the highest
N
Y
End

Figure 3. Block synchronization flow chart

DOI: https://doi.org/10.30564/jcsr.v3i2.2797

3.1.3 Data Verification Mechanism

The verification mechanism guarantees that the data cannot be tampered with. Each node in the P2P network continuously receives data. After receiving the data, the node will verify the validity of the data at the first time. The node verifies the data structure and digital signature, and only the data that meets all the conditions is valid. If the data is invalid, it is discarded. If the data is valid, the valid data is stored in the data pool. The node that obtains the billing rights broadcasts the block to the entire network, and other nodes verify the validity of the block, including the random number in the block header, the timestamp, and the data in the block body. If the block is valid, it is stored in the blockchain. Otherwise, discard.

It design uses an elliptic curve digital signature algorithm (ECDSA) [14]. The private key is d and the public key is (E, P, n, Q).

1) Choose a random integer k, between [1, n-1]

2) Calculate kP = (x1, y1) and r = x1 mod n. If r = O, skip to step 1. Otherwise, continue to the next step.

3) Calculate s = k-1 {h(m) + dr} mod n (h is the hash algorithm). If s = O, skip to step l. Otherwise, continue to the next step.

4) Signature information m is Cr, s)

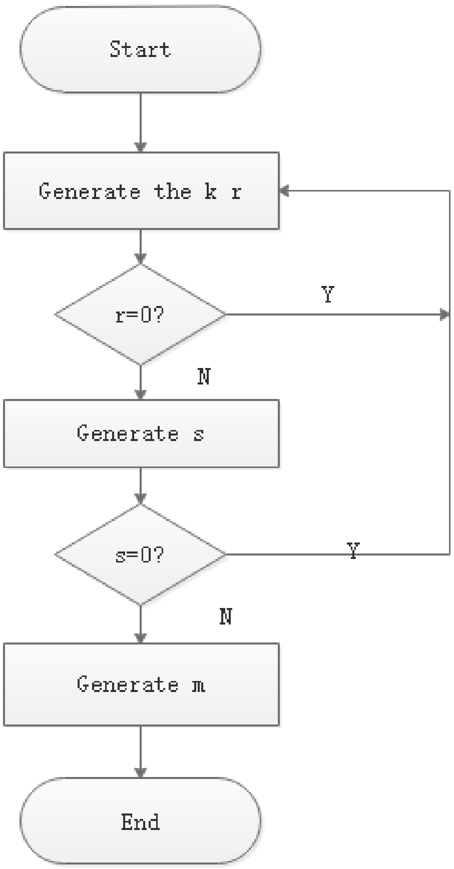

Figure 4. Generate signature flow chart

1) Get the public key (E, P, n, Q)

2) Verify that r and s are integers and are in the interval [1, n-1]

3) Calculate w = s-1 mod n and h(m)

4) Calculate ul = h(m)w mod n and u2 = rw mod n

5) Calculate u1P + u2Q = (x_0, y_0) and v = x0 mod n

6) Signature verification if and only if V = f

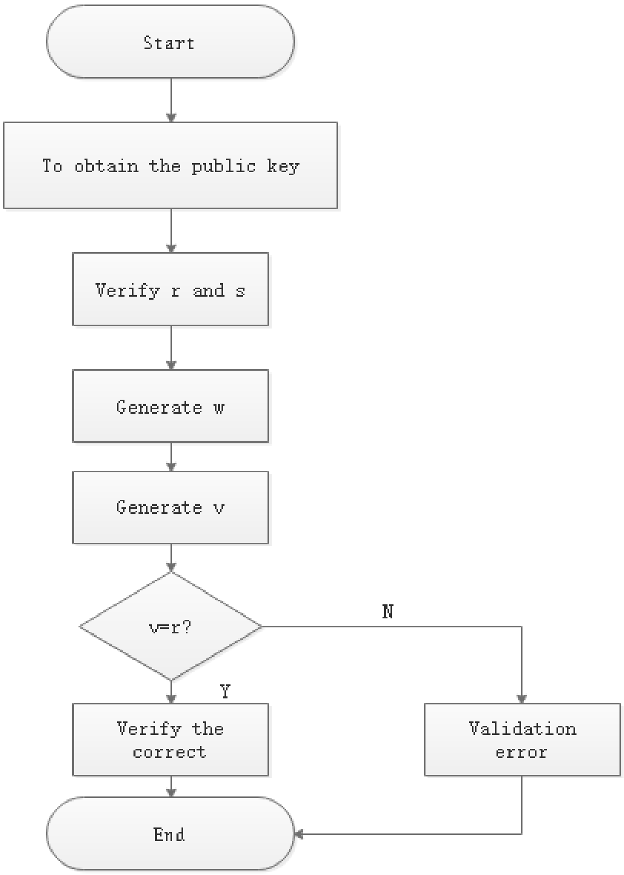

Figure 5. Verify signature flow chart

The core code verification core code is as follows：

public static Boolean verify (byte [] data, ECDSA Signature, byte [] pub) {// Digital signature verification

if (FAKE_SIGNATURES)

return true;

if (Secp256kl Context.is Enabled ()) {

try {return NativeSecp256kl.verify(data, signature.encodeToDER(), pub);}

catch (NativeSecp256klUtil.AssertFailException e) {

return false;}}

ECDSASigner signer= new ECDSASigner ();

ECPublicKeyParameters params = new

ECPublicKeyParameters (CURVE.getCurve().decodePoint(pub), CURVE);

signer.init (false, params);

try {return signer.verifySignature(data, signature.r, signature.s); }

catch (NullPointerException e) {

signatures. Those signaturesthread. log.error("Caught NPE inside bouncy castle", e);

return false;}}

3.1.4 Consensus Mechanism

The consensus mechanism provides guarantees for the consistency of data in the blockchain and is the key to maintaining the blockchain's operation. The general model of the consensus mechanism in the computer field is: in a reliable distributed system with channels, how could the system ensure that other nodes are not affected by malicious nodes and could reach a correct consensus on a certain matter in the case of a malicious node? The entire system operates reliably and reliably.

The consensus mechanism in the blockchain is embodied in that when a node collects a certain amount of valid data, multiple nodes package the data into blocks, and how the system assigns the accounting rights in the case that the node may be attacked. Which node reaches a consensus and allows the blockchain to run reliably and reliably. A well-behaved consensus algorithm could select the appropriate node. The node broadcasts its packaged block data to the whole network. After other nodes verify the validity, the block could be stored in the blockchain.

The workload proof mechanism (Proof Of Work, Pow) is simple, easy to implement, and fault tolerant (Allow 50% of nodes in the network to be attacked). It design uses the workload proof mechanism (Proof of Work, Pow). Before the node packs the data into blocks, it requirements to find a random number so that the hash value of each element of the block header is not greater than the target hash (the target hash is generated by a specific algorithm), this raises the threshold for packing blocks. The first node that finds the conditional random number will obtain the accounting rights of the block and broadcast it to the whole network. After most nodes verify the validity, it will be stored in the blockchain. The stronger the computing power, the greater the probability of finding the first random number.

The random number search procedure of the Pow consensus mechanism is as follows：

1) Node verifies data finiteness and stores valid data in the data pool;

2) Calculate the Merkle root of the block data pool, and replenish the block header data, set the random number to zero Add a random number to 1;

3) Calculate the double SHA256 hash of the current block header. If the hash value is not large, find a random number that satisfies the condition, package the data into blocks, and broadcast to the entire network; otherwise, repeat this step. Until you find a random number that satisfies the condition;

4) If a random number that satisfies the condition is not found for a period of time, update the data pool and timestamp, and then calculate the Merkle root and continue to find the random number.

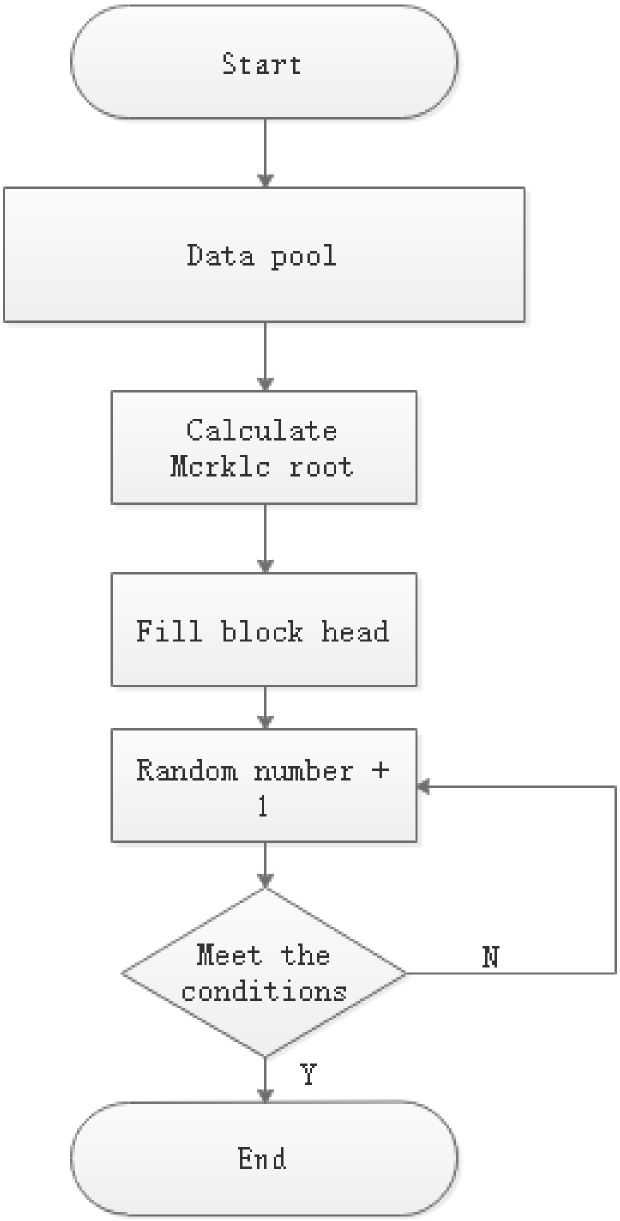

Figure 6. Random number search flow chart

3.2 Blockchain Storage Layer Design

3.2.1 Data Blocks

In order to realize the chain structure storage of the data base time stamp and to quickly verify the validity of the data, the data block adopts the structure as shown in the figure, and each data block is divided into a block header

DOI: https://doi.org/10.30564/jcsr.v3i2.2797

and a block body. The version number is included in the block header, the previous block hash value, timestamp, random number, this block target hash value (Bits) and Merkle root. The valid data and corresponding quantities generated during the block creation procedure is saved in the block body. Valid data is generated by the hash of the Merkle tree to produce a unique Merkle root, which is stored in the block header.

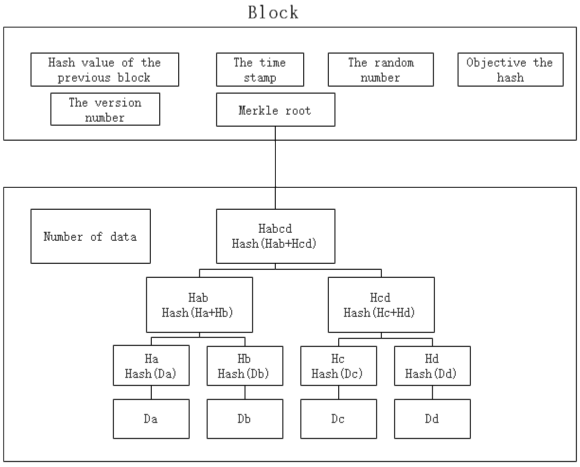

Figure 7. Block structure diagram

The data block corresponding class should contain relevant information, and could implement functions such as creating new blocks, adding valid data, verifying data, and verifying the Merkle root.

3.2.2 Timestamp

Using time stamping techniques in digital information, you could verify the exact time at which digital information is generated. Time stamping techniques provide reliable verification of the integrity and presence of digital information over a certain period of time or before a certain point in time.

In order to prove the existence of data in the blockchain, it is necessary to know the exact time of data block generation. Therefore, the node that first finds the random number and obtains the accounting right must add the timestamp to the block header, and record the data block write. The exact time of the blockchain. By using the timestamp technique, data blocks arranged in chronological order are formed in the blockchain. The time stamp technology itself is not a new technology, but its application in the blockchain technology could be used as a proof of the existence of data blocks, forming a basis for realizing the irreversible change of blockchain data.

3.2.3 Hash Function

Hash functions are characterized by unidirectionality, timing, fixed length, and randomness, making them ideal for validating data. The system will use digital signature algorithm and encryption technology to ensure that the data cannot be tampered. The selection of the hash function will affect the safety of the system. SHA256 and RIPEMD160 are based on MD4's improved hash function, which is more complex than the MD4 and MD5 algorithms and therefore more secure. It design will use two hash functions, SHA256 and RIPEMD160. Among them, SHA256 is used more, with thousands of block header hash values, block data, blockchain address generation, etc., while RIPEMD160 uses only 1000 to generate blockchain addresses. The blockchain layer will use the SHA256 hash function to procedure the data, that is, the SHA256 hash function is used twice to generate a 256-bit (32-byte binary value).

3.2.4 Merkle Tree

When performing block verification, if the data in the current block are verified one by one, the efficiency is very low. To do this, you could use Merkle Tree to quickly verify the block data. The Merkle Tree is a Hash Tree that verifies the integrity of block data in a short period of time, ensuring that data in the blockchain network are not lost and modified, and that nodes are not sending fake blocks. The Merkle tree usually consists of block data, the Merkle root, and all subtrees from the block data to the Merkle root. The procedure of generating a Merkle Tree is as follows:

1) Block data generates a hash value under the action of a hash function;

2) Combine two adjacent hashes into one string and generate a hash value under the hash function;

3) It recursion until only the last Merkle root remains.

Merkle Tree is mainly used to verify the integrity of block data in a short time. The Merkle root is the only feature of all leaf node values (block data). As long as you verify that the Merkle roots are equal, you could know if the block data have changed. If the block has N block data, the algorithm complexity of locating the tamper data is only logN.

The core code for generating the Merkle Tree is as follows:

```
    private List<byte []> constructMerkleTree()
            {ArrayList<byte[]> tree = new ArrayList<>O;
            for (Transaction t: transactions)
            {tree.add(t.getHash().getBytes());}
            int levelOffset = O; // Offset
            for (int levelSize = transactions.size(); levelSize >
1; levelSize = (levelSize + 1) / 2)
                {for (int left= O; left< levelSize; left+= 2)}//
When it is singular, the left child and the right child are the same
            int right= Math.min(left + 1, levelSize - 1);
                byte[] leftBytes = Utils.reverseBytes(tree.get(levelOffset + left));
                byte[] rightBytes = Utils.reverseBytes(tree.get(levelOffset + right));
              tree.add(Utils.reverseBytes(hashTwice(leftBytes, 0, 32, rightBytes, 0, 32))); }
    levelOffset+= levelSize;}
    return tree;}
```

3.2.5 Chain Structure

In order to provide traceability and verification of blockchain data, blocks could be stored in a chained structure of Figure 8. The current block contains the hash value of the previous block. If the node does not know the hash value of the previous block, it cannot generate a new block. All data blocks in the blockchain are chained into a chain by block hash values, and the longest chain (main chain) is always stored in the blockchain, from the creation block to the newly generated block. When a new block is stored in the blockchain, it will be linked behind the main chain.

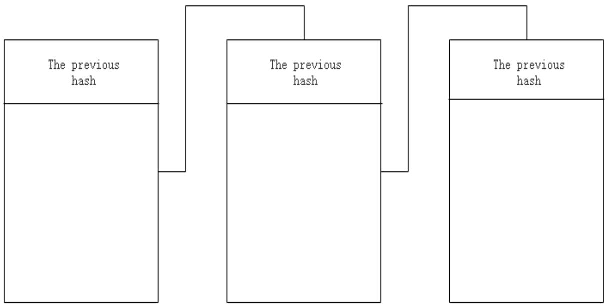

Figure 8. Chain structure diagram

The blockchain stores the data blocks in a chain structure on a blockchain with timestamps in the data blocks. It increases the time dimension of the data and makes it easy to trace and validate the data. With the previous block hash value, you could locate the previous block and verify that the previous block was modified. Through the "block ten chain structure", the blockchain could detect the tampering of any data in time. The blockchain provides a time-series, recordable record that could be viewed as a database that is not tamper-proof and authentic.

3.2.6 Asymmetric Encryption

For data safety and ownership verification, the system uses asymmetric encryption. Asymmetric encryption technology will play an important role in application scenarios such as digital signature and information encryption at the blockchain layer. In the digital signature scenario, the sender in the blockchain encrypts the information with its own private key, and sends the public key together with the private key to the blockchain network. The node decrypts the information with the public key, thereby verifying the information. ownership. In an information encryption scenario, the sender in the blockchain will encrypt the information with the recipient's public key, and the recipient decrypts the information with the private key. RSA relies on thousands of prime factorizations, so it is impossible to theoretically measure the confidentiality of RSA. The RSA key is too long, and the large number operation causes the encryption and decryption procedure to be slow. The elliptic curve encryption algorithm provides a shorter key than RSA, which is characterized by higher safety and faster procedureing. Therefore, this design will use an elliptic curve encryption algorithm, and the mechanism for generating asymmetric cryptographic public and private keys is shown in the figure.

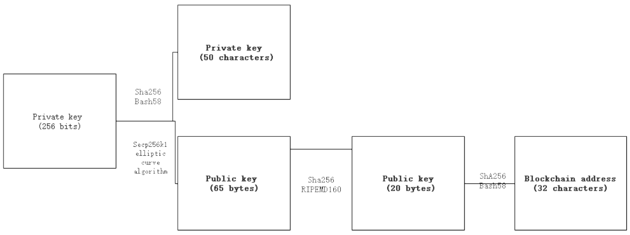

Figure 9. Asymmetric encryption

The procedure of generating the public and private key and the blockchain address is as follows：

1) Generate a 256-bit binary-shaped random number as the private key. The number of private keys will be as high as 2^{256}, making it impossible to traverse the private key. It could be generated by calling the random number generator of the base operating system.

2) For ease of memory, use the SHA256 hash function and Base58 encoding to convert a 256-bit binary private key into a private key of 50 characters, such as 6KXl j299sB bbwGnAbz3FPUDJ47r5 z2SCC Td7ytuX2QNPyrnWjss

3) A public key of 65 bytes in length is generated by a private key of 256-bit binary form by the Secp256kl elliptic curve algorithm. Such as 075ab939e3aa7a4a9aa03c5bdf22ca2dea249366c0fa88dec78aclcc2c335a72245a306218bee3c692fc540b5277c02552b8b5626db790526e4109c4e5934b

4) Use the SHA25 hash function and the RIPEMD 160 hash function to compress a 65-byte public key into a 20-byte hash.

5) For ease of memory, a hash value of 20 bytes is

DOI: https://doi.org/10.30564/jcsr.v3i2.2797

converted to a 33-character blockchain address using the SHA256 hash function and Base58 encoding. Such as 1HwgZoSa4ffzDijk5eaExNo6aKkZJ xpkw.

It is important to note that the procedure of generating a public key from a private key is irreversible, that is, the private key cannot be reversed by the public key. The procedure of generating a blockchain address by a public key is also irreversible. The role of the blockchain address is that the blockchain address could be used for reception when the user does not want to expose their public key.

4. Conclusions

4.1 Conclusions of the Matter

Blockchain has the advantages of decentralized, secure and reliable, and data cannot be tampered with. It paper studies the principle of block chain and use of P2P network technology, the consensus algorithm, timestamp technique, the chain structure, the digital signature algorithm and the encryption technology to construct the underlying block chain, on the basis of general block chain technique is applied to voting scenario, implements a data safety of the voting system, to ensure its vote fair, fair and credible [8].

4.2 Methods Used in Our Models

1) Hash function

Hash function is a kind of mathematical function, which is widely used in computer science and cryptography. In the field of cryptography, Hash functions could compress any length of input into a short, fixed output, known as a Hash value. Hash function has the characteristics of underactivity, timing, length and randomness. Cryptography has a wide range of applications, through a single hash function to compress arbitrary length of digital information into a fixed length digital digest. Digital digest is also known as digital fingerprint. Digital abstract has the characteristics of fixed length, same information abstract and different information abstract. Therefore, the digital digest could be used to verify whether the data have changed, that is, data integrity.

2) Asymmetric encryption

Encryption and decryption use the same secret key. Encryption method is called symmetric encryption. The encryption method is called asymmetric encryption. The secret keys of asymmetric encryption are produced in pairs. The public secret key is called public key, while the private key is called private key. If you encrypt the information with a private key, you could only decrypt the information using a public key. If the message is encrypted with a public key, only the private key could be used to decrypt the message. The safety of asymmetric encryption is guaranteed by the algorithm and the secret key. The strength of the algorithm is high and the secret key is highly confidential (unlike symmetric encryption, which requires the exchange of secret keys), so the safety of asymmetric encryption algorithm is more guaranteed. However, the speed of asymmetric encryption algorithm is relatively slow, which is not suitable for scenarios that need to encrypt halo data, including digital signature or secret key negotiation. Common asymmetric encryption algorithm RSA, ECC (elliptic curve encryption algorithm) knapsack algorithm, Ellamae, Rabin, Diffie - Hellman [. RSA is dependent on the quality of large number factorization, how to measure the confidentiality of the RSA in theory. The RSA key is too long, a large operation and lead to the encrypted the decryption procedure is slow. Elliptic curve encryption algorithm, and secret key provided by the shorter than RSA, has the characteristics of higher safety and faster procuring speed.

3) Digital signature

Digital signature is a combination of digital digest technology and asymmetric encryption technology, which provides a strong guarantee for the integrity of digital information and the authenticity of sender's identity.

4) Timestamp technology

Timestamp technology is the application of authoritative time source and digital signature technology. Using the timestamp technique in digital information could verify the exact time when the digital information was generated. Timestamp technology could provide reliable verification of the integrity and existence of digital information in a certain time period or before a certain time point.

5) Merkle tree

Merkle tree is a Hash tree, usually a binary tree. The hash value of Merkle tree leaf node data, the non-leaf node is the hash value of two adjacent hash values merged into a string, and the Merkle root is finally generated. Merkle tree could verify the integrity of the data in a short time, that is, if the data have been changed. The Merkle root is the unique characteristic of all leaf nodes. By verifying that the Merkle root is equal, you could know whether the data of the leaf node has been changed. In a distributed system, Merkle tree could quickly verify whether the data changes during transmission, greatly reducing the computational complexity.

6) P2P network

Peer-to- Peer (P2P) [25l, is a network formed in the application layer.

DOI: https://doi.org/10.30564/jcsr.v3i2.2797

P2P network is different from client/server model. There is no concept of client or server in P2P network. There is no central node, only peer nodes. Each node seeks both the service and the provider of the service. A node in a P2P network acts as both a client and a server. There are no limits on the number, scope, time, or space of nodes in a P2P network, and each node is free to join or leave.

All nodes in P2P network share the pressure of server in traditional way. The more nodes join the network, the more stable the whole network will be, providing higher quality services. P2P networks return power to users and decentralization.

7) Distributed storage

Traditional storage systems generally store data centrally in centralized storage servers, but the storage resources of centralized storage servers are very limited and cannot meet the requirements of storing large-scale data. But the distributed storage system adopts the expandable system structure, and stores the data in several nodes, so that the capacity, stability and expansibility of the system are greatly improved.

8) Consensus mechanism

In any decentralized distributed system, the nodes of the participating system are equal in status and lack of trusted central nodes. When decisions are divided, the matter of how the nodes could reach consensus arises. Consensus on transactions is one of the core challenges of distributed systems.

9) Blockchain

There are many definitions of blockchain. It is difficult to intuitively understand the real meaning of blockchain from the definition alone. We could first understand the general meaning of blockchain from the perspective of application.

Traditional network storage system could adopt centralized storage or distributed storage to store data. Distributed storage system could solve the matter of limited space of centralized storage system. However, no matter centralized storage or distributed storage system, such as the storage system is attacked by hackers or improper right management, it will cause the modification or loss of data. Blockchain is a real and reliable database that cannot be tampered with. Once the data are stored in the database, it cannot be tampered with. Blockchain is a distributed database based on P2P network. There is no central node, and each node in the P2P network stores exactly the same data. Any malicious modification of data by any node will not affect the correctness of the entire network data. One of the important features of blockchain is that data cannot be tampered with.

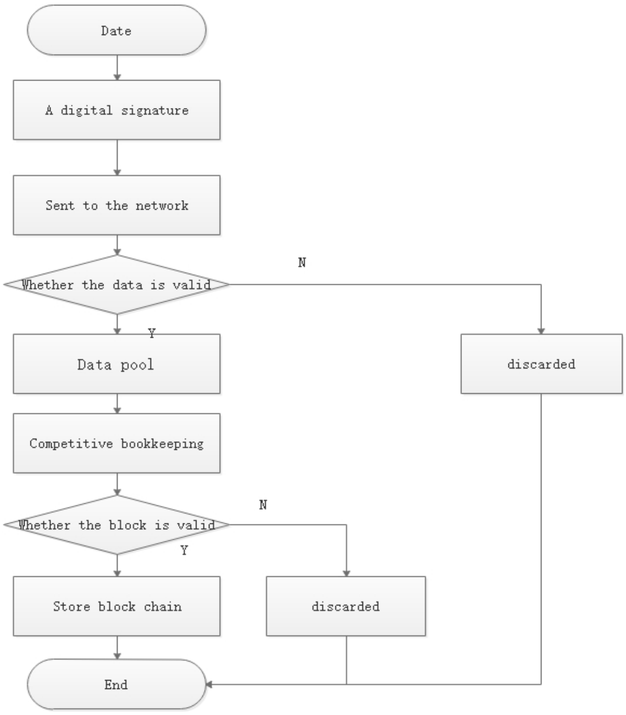

Figure 10. Blockchain data storage flow chart

4.3 Application of Our Models

On the basis of completing the design of the underlying blockchain, the application layer adopts the BIS architecture, and the web application layer mainly implements the system functions. According to the analysis of the system function, the registration module, the homepage module, the voting module, the new voting module, the voting result query module, and the voting history query module are designed. The web application layer will be developed using the framework of Spring + Spring Boot + My bits, and the database is MySQL.

The application layer adopts the MVC (Model View Controller) design pattern and is divided into a view layer, a business logic layer, and a data access layer. As shown.

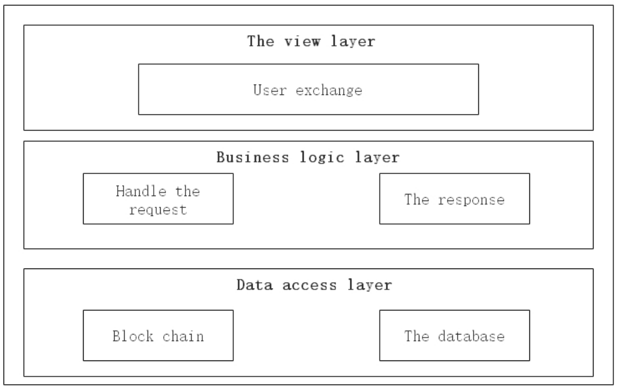

Figure 11. Web application layer architecture

DOI: https://doi.org/10.30564/jcsr.v3i2.2797

1) View layer: The view layer provides the ability to interact with the user. A good user experience is an important indicator of system design. It design uses the Free Marker template engine, which uses a "template + data = output" model with no business logic. The template is only responsible for populating the data in the page, and finally the combination of the template and the data is presented in front of the user. Separate the view layer from the business logic to improve development efficiency. The front-end framework uses bootstrap, which provides comprehensive documentation, rich components, and ease of use to quickly and easily customize the pages you need.

2) Business logic layer: The business logic layer is the key to implementing system functions, procuring requests from the view layer and returning responses. For example, store the information entered by the user into the database. The ajax technology enables the view layer and business logic to asynchronously interact with data, providing a better user experience.

3) Data access layer: The data access layer is responsible for data access. Normal data (such as user name, password, etc.) are directly stored in the database, and blockchain data (voting records) are stored in the blockchain. When accessing normal data, you need to design the database and write sq. statements. When accessing the blockchain data, the underlying blockchain interface requirements to be called to implement access in the blockchain of data.

5. Future Work

5.1 Model Advantage

Voting is the preferred democratic expression in any situation where multiple people are required to make decisions. But when the voting system rises to the national level, its disadvantages gradually appear. Where power struggles exist, fraud and corruption are hard to root out. In addition, in the United States and other western countries with a large population and a large number of votes, the existing paper voting method has disadvantages such as low efficiency, high cost and low transparency. Blockchain offers voters an updated system to address these issues.

Since the emergence of blockchain technology, many people believe that it has the potential to reform the voting system because of its features such as non-tampering and high transparency. Citizens could vote through smart devices and record the data on the blockchain, which cannot be tampered with, so as to ensure safety and save time and capital cost. The characteristics of distributed and distrust could guarantee the personal privacy of voters and the full realization of public opinion [7].

5.2 Limitations of the Model in the Voting Domain

First, safety. Skepticism about the nascent blockchain technology is also based on distrust of electronic voting systems. Voting through blockchain still requires electronic devices, which poses the risk of hacking and affects confidentiality and fairness.

Second, unnecessary. Blockchain technology does have big advantages in voting, but these advantages are not irreplaceable. Opponents of blockchain voting still insist that paper ballots have irreplaceable advantages, and that blockchain technology's advantages in voting could be replaced by other ways.

Third, high costs. Blockchain technology is still in the early stage of implementation. If blockchain technology really wants to completely overturn the voting method, it will need a lot of promotion costs.

References

[1] Yuan Yong, Wang Feiyue. Current situation and Prospect of blockchain technology[[J]. Acta Automatics Sinica,2016,42(4):481-494.

[2] Swan M. Blockchain: Blueprint for a New Economy. USA:O'Reilly Media Inc., 2015.

[3] Ding Wei. Block chain based instrument data management system. China Instrumentation, 2015, (10): 15-17.

[4] Zhao He, Li Xiao-Feng, ZhanLi-Kui, Wu Zhong-Cheng. Data integrity protection method for microorganism sampling robots based on blockchain technology. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2015, 43(Zl): 216-219.

[5] Swan M.Blockchain thinking: the brain as a decentralized autonomous corporation.IEEE Technology and Society Magazine, 2015, 34(4): 41-52.

[6] Sarr Idrissa, Naacke Gueye Ibrahima. Blockchain-based model for social transactions procedureing[C]. DATA 2015-4th International Conference on Data Management Technologies and Applieations. 2015:309-315.

[7] H.Watanabe, S. Fujimura, A. Nakadaira, etc. Blockchain contract: Securing a blockchain applied to smart contracts[C]. IEEE International Conference on Consumer Electronics (ICCE)□2016:467-468.

[8] Zhu Yan, Gan Guohua, Deng Di and other key technologies of blockchain security research [J]. Infor-

DOI: https://doi.org/10.30564/jcsr.v3i2.2797

mation security research□ 2016,(12):1090-1097.

[9] Shen Xin, Pei Qingqi, Liu Xuefeng. Overview of blockchain technology [J]. Journal of network and information security， 2016,(11) :11-20.

[10] Jia Liping. Theory, practice and influence of bitcoin [J] international financial research, 2013, (12) :14-25.

[11] National Institute of Standards and Technology (NIST), Secure hash standard. Federal Information Procuring Standards Publication (FIPS PUB)180, May 1993.

[12] National Institute of Standards and Technology (NIST) Computer Systems Laboratory, Secure hash standard. Federal Information Procuring Standards Publication (FIPS PUB)180-1, April 1995.

[13] National Institute of Standards and Technology (NIST) Computer Systems Laboratory, Secure Hash Standard. Federal Information Procuring Standards Publication (FIPS PUB)180-2, August 2002. http://csrc.nist.gov/publications/fips/fips 180-2/flips 180-2.pdf.

[14] Rivets R. The MD4 message digest algorithm. In Advances in Cryptology, Crypto'90 volume 537 of LNCS, pages 303-311.Springer-Verlag, 1991.

Technical Report

We focus on the design of P2P network design, node block synchronization, data and block verification mechanism and ensure the consistency of data consensus mechanism. Then the time stamp, Merkle tree and asymmetric encryption are used to design the data block.

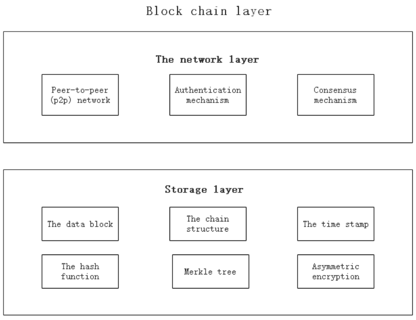

Figure 12. Blockchain layer

In order to satisfy the system centralization, the information cannot be tampered. Open and transparent requirements, combined with the underlying block chain to store data characteristics. We divide the system into view layers. Business logic layer and data access layer. Combined with the block chain characteristics of the business layer architecture design.

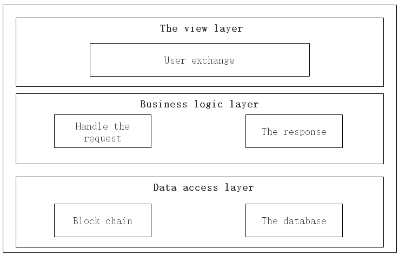

Figure 13. Application layer architecture design

A data secure voting system is designed by taking full advantage of the decentralized blockchain, untamable data, and secure and reliable data.