ISSN 2616-5902 Vol. 3, Issue 6: 95-99, DOI: 10.25236/AJBM.2021.030615

Blockchain: A Method to Improve Voting System

Yueren Sun, Haoqi Wang, Dandan Xu

Xi'an International Studies University, Xi'an, Shaanxi 710128, China

Abstract: *In order to overcome the disadvantages of poor security and lack of trust in the traditional electronic voting system and improve the reliability of the election system, this paper proposes an electronic voting system based on blockchain. This system is divided into voting module and blockchain management module, which mainly aims at the credibility of voting data and the protection of voters' privacy. The voting module begins with the verification of voter's identity, uses Zero Knowledge Proof algorithm to prove that the entrant is the legitimate owner of part of the rights and interests, uses ECDSA to encrypt the data, and uses Digital Signature to verify the security and integrity of the data. The main purpose of the blockchain management module is to update the data in real time, make the newly added nodes complete data synchronization, check the consistency of the data, and provide the user with historical records.*

Keywords: *blockchain, voting system, ECDSA*

1. Introduction

There are many times in life when public opinion needs to be expressed, and people participate by voting offline. With the development of science and technology, the advantages of electronic voting through the network and computer greatly reduce the labor cost and organizing cost, compared with offline voting, has great advantages.

Block chain technology is the core advantage of decentralization, to be able to use data encryption and timestamp, distributed consensus and economic incentives, in the node without mutual trust in the distributed system implementation is based on decentralized credit point-to-point transaction, coordination and cooperation, thus to solve the centralized organization the prevalence of high cost, low efficiency and provides a solution to data storage uneasy congruent problem. There is no doubt that this decentralized and mutually trusted technology is suitable for voting systems.

2. Basic Model

In order to meet the most basic voting requirements and ensure the security of voting progress, the basic model (as shown in Figure1) includes the following two parts: vote module and blockchain management module.

In the first part, the basic model has made two major contributions to the protection of privacy. The first contribution is to ensure the legitimacy of the registration while not revealing their real identity. The second contribution is to encrypt and protect voters' election intentions, ensuring that the protection of voters' privacy is met when broadcasting to all nodes.

In the second part, the blockchain management module is mainly responsible for background management, timely sharing and updating of data generated by each voter node, so as to ensure that each voter node stores the longest chain in the block chain.

2.1 Vote module

2.1.1 Authorization Stage -- Zero Knowledge Proof

In our life, not everyone has the right to vote. In the United States, only American citizens over the age of 18 have the right to vote. Therefore, the electronic voting system needs to meet such a requirement: only legitimate users have participation, illegal users can not vote. Through the issuance of a unique registration ID and elector self-certification registration ID, to achieve the purpose of voting is based on legitimate users.

ISSN 2616-5902 Vol. 3, Issue 6: 95-99, DOI: 10.25236/AJBM.2021.030615

Prior to Election Day, electors' RFID CARDS are prepared and distributed by the government to electors prior to the election, and the legality of electors' identity is uniquely determined by the RFID card information.

On Election Day, electors submit registration requests to the government, which USES a smart contract to verify that the elector's registration ID is a match, so that qualified electors can proceed to the next step of the voting process. In order to protect electors' privacy, we adopt zero-knowledge proof method.

Zero-knowledge proof is a probabilistic verification method, which consists of two parts: the first part is the one who claims that a certain proposition is true, and the second part is the one who confirms that the proposition is true. Therefore, the zero-knowledge proof can fully prove that the certifier is the legal owner of some rights and interests, and does not leak out the relevant information.

In this case, we need to verify that the elector has a valid ID and that the elector's real identity will not be revealed in this verification. The specific authentication process is as follows(As shown in Figure 1):

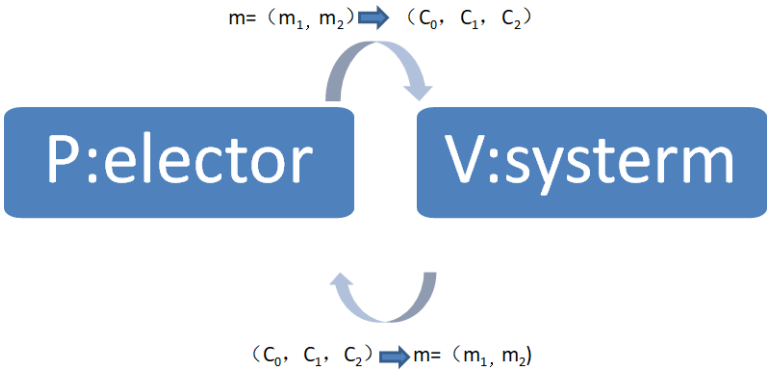

Figure 1: Zero Knowledge Proof Diagram

(1) Before issuing the private key, system V randomly selects a module n, which is the product of two large prime Numbers. To generate public and private keys for elector P, select k different Numbers first: v_1, v_2, ..., v_k. v_i here is the quadratic residual of modulus n. In other words, $x^2=v_i \bmod n$ has a solution, and v_i^{-1}modn exists. String of v_1, v_2, ..., v_k as the public key. Finally, calculate the smallest si that conforms to $s_i= v_i^{-1/2} \bmod n$. String $s_1,s_2,\ldots s_k$ as the private key.

(2) Select a random number r by elector P, r < n, calculate $x=r^2 \bmod n$, and send x to system V.

(3) System V assigns a k-bit random binary string $b_1,b_2,\ldots,b_k$ to elector P.

(4) $y=r*(s_1^{b2}*s_2^{b2}*\ldots*s_k^{bk}) \bmod n$, which is to multiply the s_i values corresponding to $b_i=1$. Elector P sends the result y to system V.

(5) System V verification $x=y^2*(v_1^{b2}*v_2^{b2}*\ldots*v_k^{bk}) \bmod n$.

When elector P and system V can verify each other, it means that elector P's ID is true and valid, and elector P's ID will be added to the list of eligible electors.

2.1.2 Voting Stage -- ECDSA

Qualified electors who pass the test will be able to choose their preferred candidate after registration. Based on the fact that all data in blockchain is distributed and open and transparent, it is necessary to protect the privacy of citizens' election choices in order to protect the privacy of citizens' election content. Compared with other public key cryptography, elliptic curve digital signature algorithm can provide higher security performance and save storage space, so we adopt elliptic curve digital signature algorithm to encrypt. The specific encryption process is as follows(As shown in Figure 2):

ISSN 2616-5902 Vol. 3, Issue 6: 95-99, DOI: 10.25236/AJBM.2021.030615

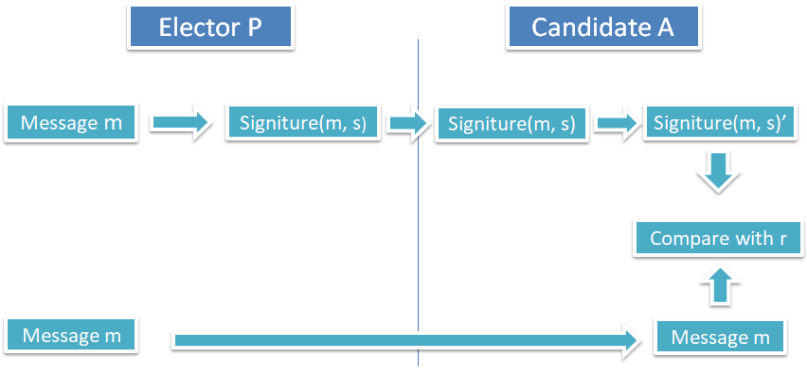

Figure 2: ECDSA Diagram

(1) Input of parameters in elliptic curve domain

Suppose that the parameters of the elliptic curve domain are T=(q,a,b,G,n,h) domain parameters are defined as follows :q represents the size of the domain;

Based on elliptic curve $E(F_q)$ on F_q; base point G; G order n; Message m; $\#(F_q)$ represents the order of the elliptic curve; The integer $h=\#E(F_q)$ is a cofactor.

(2) Generation steps of ECDSA signature of voting intention m of elector P:

Suppose the secret key dA of elector P, $dA \in [1, n-1]$, and the public secret key $Q_A= d_AG$;

1) represent the message m as a binary string;

2) hash value e=SHA1(m) of message m generated by hash algorithm;

3) select a random integer $k \in [1, n-1]$;

4) calculate the point $R_1=kG=(x,y)$, and set r=x mod n, where x is the whole point on the Xcoordinate;

5) calculate k^{-1}mod n;

6) use the secret key d_A of elector P to calculate $s= k^{-1} (e+d_Ar)$ mod n; Get the signature (r,s);

7) send the signature (r,s) with message m to candidate A.

(3) Steps to verify the ECDSA signature of message m:

1) find the sender's public key Q_A;

2) calculate the hash value of message m, e=SHA1(m); Calculate u=ewmod n and v=rwmod n;

Calculation point $R_2=(x_1,y_1)=uG+vQ_A$mod n;

Calculate r'= xmod n, if r' =r, then elector P's signature is valid.

Through rigorous algorithm encryption, electors' voting intentions are effectively protected.

2.1.3 Counting phase – verification

The verified eligible electors choose their own intention in the voting system, and the system encrypts it through ECDSA algorithm after the selection. For other elector nodes, they can only see the increase of the number of votes, but cannot see the specific content of the votes. The system will broadcast and share each elector's choice, and the elector node receiving the message will update its own blockchain.

2.2 Blockchain Management Module

Through the block chain management module, we determined the consistency and integrity of voting information, so that the block chain data of each node could be updated in the same way and resources could be fully shared.

2.2.1 Data Sharing

The successful transmission of the information and the transmission of the information at the candidate node to the nearby node through the P2P network, each node to the surrounding dissemination,

ISSN 2616-5902 Vol. 3, Issue 6: 95-99, DOI: 10.25236/AJBM.2021.030615

and so on to achieve public broadcasting.At the same time, all the nodes in the system get the propagated information.

2.2.2 Test Consistency

Each block in a blockchain is made up of a block header and block body. The block header stores the relevant properties of the block, such as hash value, version, timestamp and Merkle root of the previous block. Merkle root is the top layer of Merkle Tree (As shown in Figure 3). Before downloading the p2p network, obtain the Merkle root of the file from the trusted source. Once you have the Merkle Root you can get the Merkle tree from other untrusted sources. If the Merkle Tree is corrupted or false, get another Merkle Tree from another source until you get a Merkle Tree that matches the Merkle Root. Therefore, it can be used to determine whether the blocks are the same between nodes. If each hash value cannot correspond to one to one, the message is discarded. If so, the information is consistent. When more than 50% of the nodes match the local blockchain, the local blockchain is considered correct, otherwise the local data is deleted.

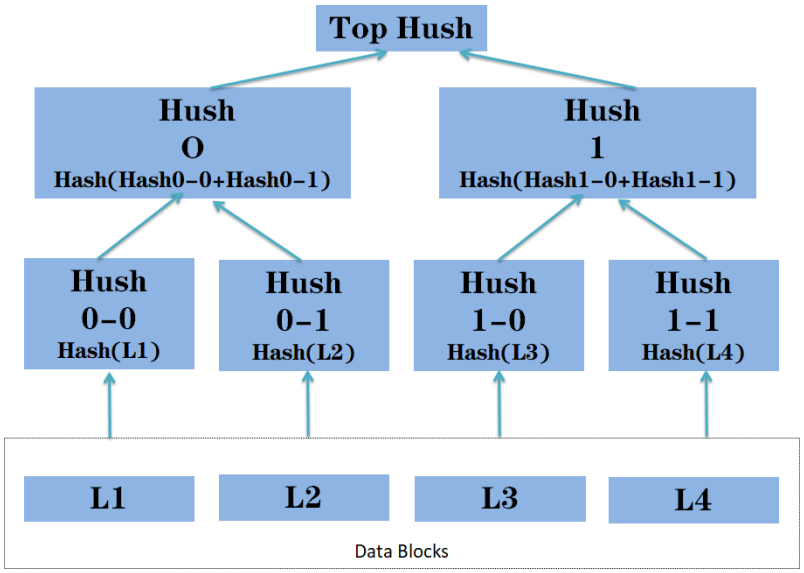

Figure 3: Merkle Tree

2.2.3 Refresh Data

If there is no previous block chain information locally due to other reasons, the P2P network will send requests to all nodes and wait for a certain time to receive data from other nodes. Based on the first received data information, the local block chain will be updated to realize the integrity of the block chain. The wait time should be less than the system update time.

2.2.4 Query Log

The user enters the time range to query, sends the request to all nodes, and the node finds the target data as required, generates a history in chronological order, and then returns to the page.

2.3 The Result of Basic Model Analysis

2.3.1 No Vote Counting System Analysis

The basic model describes in detail the foreground voting stage and the background voting information sharing stage of the entire voting system and data protection. However, the basic model does not elaborate on how to organize the voters' voting information statistics, and does not mention the method and process of voting information statistics. And it is very important for voters to verify the results of their voting. Voters need a proper platform to test their voting behavior.

2.3.2 Data Redundancy

The security of a blockchain with no central node depends on a large amount of data redundancy. Even if an attacker has the ability to control a node and forge, tamper or delete the effective data of the node, it is very difficult to attack many network nodes at the same time. A major feature of blockchain is that each node stores the longest chain in the blockchain. If the node does not store the longest chain, the

ISSN 2616-5902 Vol. 3, Issue 6: 95-99, DOI: 10.25236/AJBM.2021.030615

node will update the information to reach the state of the longest chain. However, this means that when applying blockchain to the election system, each voter node has to store all the election information of all the people, and the whole data storage is too huge.

2.3.3 Storage Risk of Private Key

The basic model uses zero-knowledge proof in voter registration ID to ensure that voters are eligible voters without revealing voters' unique ID. The basic model also encrypts voters' voting intentions before voters broadcast data and protects voters' privacy. In these effective protection processes, the necessary private and public keys are generated. However, the storage risk of private key is high, which needs to be improved in the next optimization model.

3. Evaluation

3.1 Advantages of the model

1. Decentralization: the verification, bookkeeping, storage, maintenance and transmission of block chain data are all based on the structure of distributed system. The trust relationship between distributed nodes is established by pure mathematical method instead of central organization, so as to form decentralized and trustworthy distributed system.

3.2 Disadvantages of the model

1) Each synchronous update of the block chain will increase the storage, which requires high performance of the computer.

2) Tamper and undo are both advantages and disadvantages of blockchain. We lack the option to repeat the confirmation without considering the possibility of misoperation.

References

[1] Zhang Xinwei, Zhang Hua, Guo Xiaowang, et a1.Research and analysis of electronic voting system based on block— chain [J]. Application of Electronic Technique, 2017, 43(11): 132-135.
[2] Han Jindong, Cui Zhe. Data integrity verification method of election system [J]. Computer application, 2017, 37s2: 52-56.
[3] Yan Chunhui, you Lin. design and implementation of secure voting system based on blockchain [J]. Communication technology, 20185108: 1979-1989.
[4] Li Bei. Electronic election system based on homomorphic encryption strategy [J].Computer application, 2015, 35s1: 66-68 + 88.
[5] Bai Yongxiang. Design and implementation of blind signature scheme based on ECC and zero knowledge proof [J]. Communication technology, 20154810: 1174-1178.