ISSN 2616-5775 Vol. 4, Issue 4: 30-34, DOI: 10.25236/AJCIS.2021.040405

Improved Voting System Based on Blockchain

Yueren Sun, Dandan Xu, Haoqi Wang

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

Abstract: *In the operation of the voting system, this paper found that the system had the problem of no counting tickets and data redundancy. Although the system has carried on the statistics to the voting information, but has not completed the counting publicity very well. In view of this problem, we have optimized the counting item. In order to solve the problem of data redundancy in the operation of the system, we choose an improved homomorphic encryption algorithm based on ECC, which effectively improves the operation efficiency. After comparing with other models, we find that there are risks in private key storage. We cooperate with the external database and propose a scheme to reduce the risks by associating private key, security problem and password.*

Keywords: *blockchain, voting system, ECC, private key*

1. Introduction

Due to the interoperability and convenience of today's network, there are many security and privacy issues. Such as counting people or counting institutions can be fair statistics, hackers malicious attacks on the system, whether the internal members for the benefit of undercover operation.....There is a great deal of debate about this, and we urgently need a new technology to solve these problems. The rapidly developing block chain technology just meets the requirement of security and reliability.

Blockchain is created through a series of cryptography methods associated data blocks, each block contains all the information before trading, can be used to verify the authenticity of information and generates the next block, and all the data is open and transparent. Blockchain technology can be applied to voting systems.

2. Optimization Model

2.1 Optimization of the Counting Phase

The public and private keys generated in the process of encryption are used by the counting system to deduce the voting choices made by voters and make statistics (as shown in figure 1). The system generates voting records, records user ID, user voting time and candidate ID, and generates voting certificate packets encrypted.

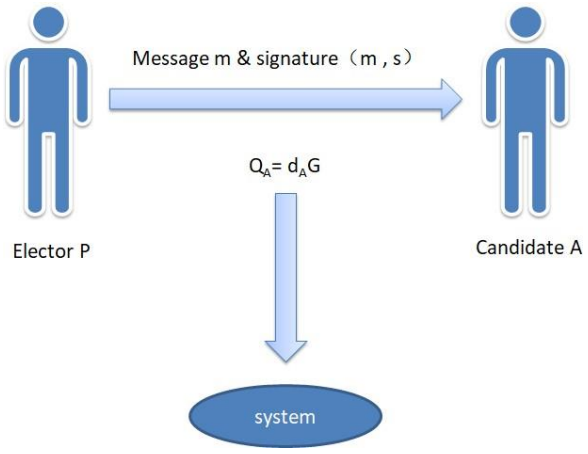

Figure 1: The Process of Obtaining Voting Information

Voters can view their voting records in a specific interface.

ISSN 2616-5775 Vol. 4, Issue 4: 30-34, DOI: 10.25236/AJCIS.2021.040405

The whole voting process is improved as follows:

1) Voters check whether they are the only legal ID when they register, and adopt zero-knowledge proof to protect voters' privacy in this process.

2) Voters make their own ballot choices and protect the real intention of voters through ECDSA algorithm. Voters' ballot choices are sent to the designated candidates.

3) Voters' choices are tested and then approved through region-wide broadcasts, and approved messages are recorded as a node.

4) The system translates and statistics voters' choices through the private and public keys used by voters, and voters' choices are generated and stored by credentials.

2.2 Optimization of Data Redundancy

From a technical perspective, the consensus of all block chain agreement has a challenging restrictions: each fully participate in the node in the network must verify every transaction, and these nodes must be consistent with other nodes, it is part of the block chain technology, it by creating a distributed books to ensure the safety of chain block. But this approach comes at the cost of reducing scalability. As these public blockchain get bigger, it will need more and more processing power to validate them. This could create bottlenecks in these blockchain networks, slowing down the creation of new applications. This means that as more and more people vote in elections, it slows down their voting speed. Therefore, we hope to find a method that can improve the efficiency. After discussion, we choose to use an improved homomorphic encryption algorithm based on ECC to effectively improve the operation efficiency.

The majority of ECC is binary, where the scalar t is used instead of decimal to serialize the binary to reduce computation time.

ECC algorithm mainly includes the generation of key, encryption data, decryption data three parts. The details are as follows:

1) Select a random integer d and solve Q=dG

2) Map plaintext to element m, and randomly select integer k, calculate $(x_1, y_1)=kG$ $(x_2, y_2)=kG$, $C=m*x_2$, and then obtain the encrypted data as (x_1, y_1, C).

3) Using the private key d, calculate $(X_2,Y_2)=d(X_1,Y_1)$ and $m=C*X_2^{-1}$.

The improvements we prepare are as follows:

In the improved algorithm, we extend random binary string S with unfixed digits to obtain random number k.

Let w be the digit of base-point order n, and get S at random, whose digit u satisfies 1.

Because k is the extension of S, k is the concatenation of SN and ST.Through k and S, the integer part n=w/u is obtained. N represents the number of times S needs to be extended.

Since it is not clear whether ST is to the left or right of S, there are two calculation methods. Let's take the left to the right as an example:

1) If M = 0;i = 0

2) Calculate Q=S*P and get R=ST*P in the process

3) If $K_i=1$. Then M=M+Q

4) M = 2 ^{u}m

5) I = I + 1

6) Then return to step (3).Repeat n times, no more steps 4 after the last step 3

7) M =2 vm

8) M=M+R ,gives M

Through subsequent aging calculation, it can be concluded that with the increase of the value of parameter m, the efficiency of improvement will be higher. The processing speed of the block

ISSN 2616-5775 Vol. 4, Issue 4: 30-34, DOI: 10.25236/AJCIS.2021.040405

chain system has been improved, especially in the counting of votes.

3. Comparison with Other Model

3.1 The Problem of Private Key

In the operation of voting system, we realized that the blockchain has Asymmetric Encryption, Merkle Tree, Digital Signature etc. to ensure the security and consistency of information, but the user's private key is not protected by above-mentioned technologies. Once the private key is lost or leaked, it will cause a serious negative impact.

For example:

1) On February 24, 2014, Mt. GOx, the world's largest bitcoin exchange operator, announced that 850000 bitcoins on its trading platform had been stolen, which caused it immediately went offline and applied for bankruptcy protection.
2) In the early morning of August 3, 2016, Bitfinex, the largest US dollar bitcoin trading platform, posted a notice on its official website: Due to a security vulnerability on the website, the bitcoin held by users was stolen, with a total of 119756 stolen bitcoins, at that time the total value of which was about 65 million US dollars.

These malignant events make us pay more attention to the security of users' private keys.

3.2 The Solution of Problem

Based on this, we have consulted many materials and learned that there are several solutions at present:

1) Mnemonic, backup mnemonics in advance, and decide the backup method by voters themselves.
2) Secret sharing, which distributes a secret encryption to multiple participants. Only when a certain number of participants work together can they spell out the original secret.
3) Standard KYC (know your costumer) program, users provide identity information to KYC suppliers, and need to perform a set process to make the identification behind the address be known.

But the above methods have disadvantages: high cost or complex operation.

So we came up with a more appropriate solution:

1) Use platform password to encrypt private key, named EPK1;
2) At the same time, use security issues and public key named EPK2 to encrypt recoverable content, and save information in system database.

The relationship between EPK1, EPK2 and EPK 'ensures the security of the private key, as shown in the figure 2:

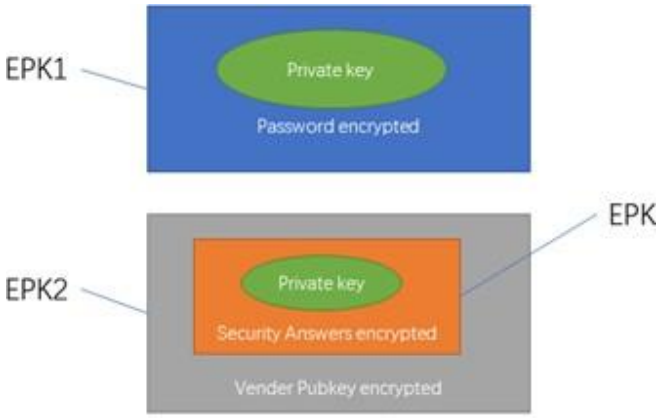

Figure 2: The Relationships between EPKs

ISSN 2616-5775 Vol. 4, Issue 4: 30-34, DOI: 10.25236/AJCIS.2021.040405

After the user registers successfully (the registration flowchart is shown in figure 3), the system generates the public key and private key, and then performs the following operations:

1) The private key is processed by EPK1 and saved locally.
2) Save the password after local encryption.
3) Encrypt the security questions and answers in EPK ', and then encrypt and save them in EPK2.
4) Save Secret Question.
5) Save platform public key.

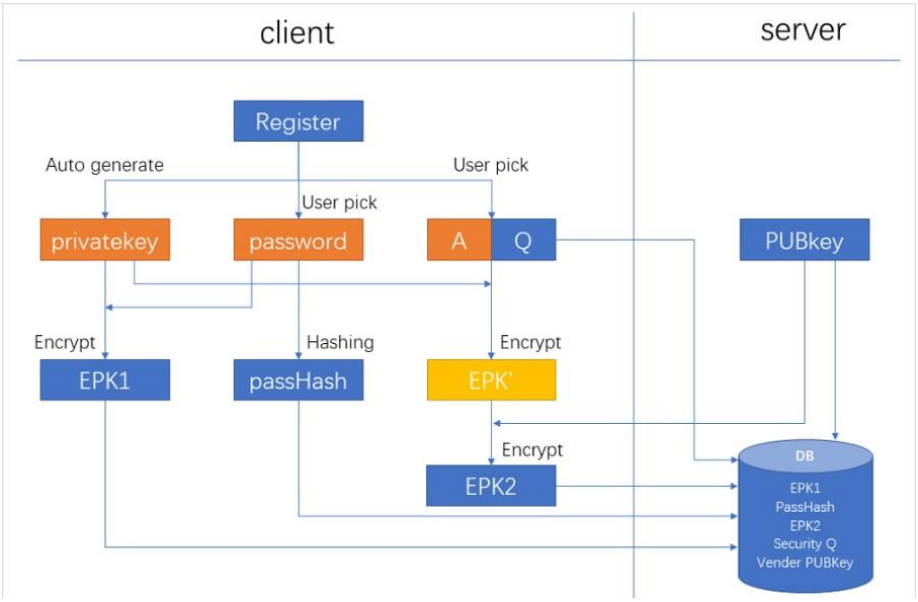

Figure 3: User registration flowchart

Then the normal login steps are(as shown in Figure 4):

1) Enter password to get passhash.
2) Compare the passhash which is saved in the database before, and if it is the same, return to EPK1.
3) Decrypt the private key from EPK1 with password.
4) Use private key for digital signature and send information to blockchain system.

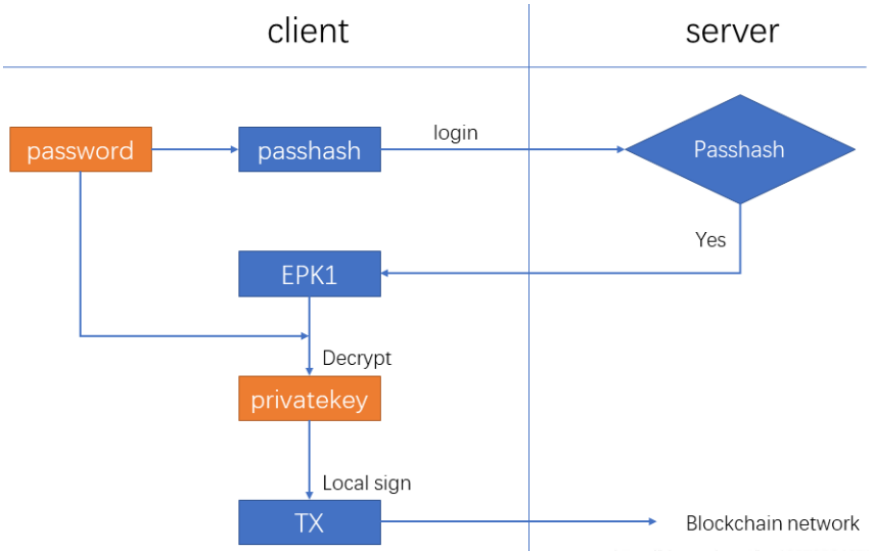

Figure 4: Load Steps

ISSN 2616-5775 Vol. 4, Issue 4: 30-34, DOI: 10.25236/AJCIS.2021.040405

Main actions when password is lost or resetted (as shown in Figure 5):

1) When logging in, enter the new password to get the passhash.
2) Compare the passhash saved before. If it is different, apply to save it again and get the platform private key.
3) Get EPK2, decrypt with platform private key, and get EPK '.
4) The user answers the security question and recovers the private key from EPK '.
5) Generate a new EPK1 and update the database.

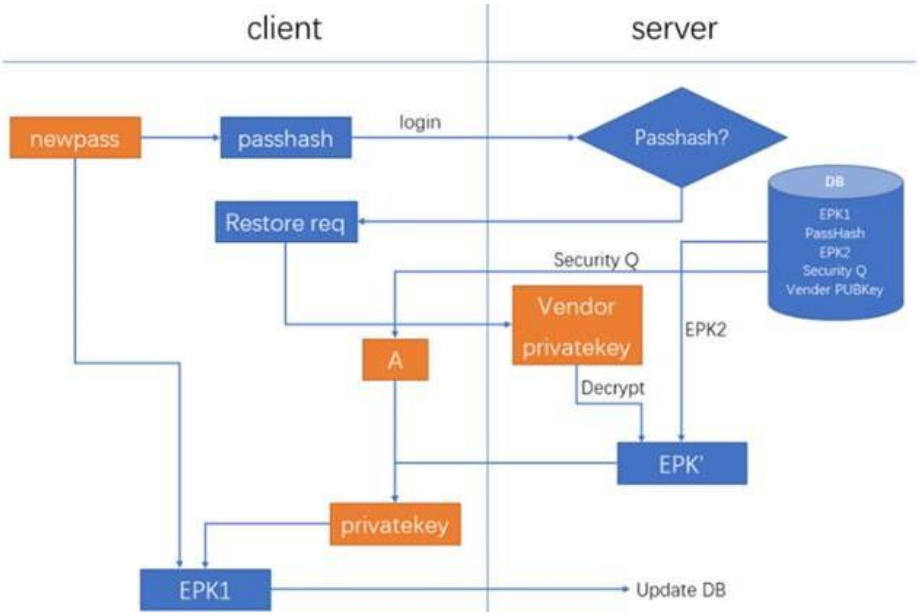

Figure 5: Operation steps when password is lost or reset

4. Evaluation

4.1 Advantages of the model

Timing data: blockchain adopts chain block structure with time stamp to store data, which adds time dimension to the data and has strong verificability and traceability.

4.2 Disadvantages of the model

Transactions in blockchain are delayed, and there may be conflicts between the cut-off time and the arrival time of information.

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] Huai Fanli, Wang Gaiyun, Yang Fan, Yan Jihong. Development and implementation of election system based on secure multi-party summation [J]. Network security technology and application, 2011,09: 43-44 + 48.
[5] Wang Quanfu. Research and improvement of homomorphic encryption algorithm based on ECC [D]. Zhongbei University, 2017.