第八届“认证杯”数学中国

数学建模国际赛

承 诺 书

我们仔细阅读了第八届“认证杯”数学中国数学建模国际赛的竞赛规则。

我们完全明白，在竞赛开始后参赛队员不能以任何方式（包括电话、电子邮件、网上咨询等）与队外的任何人（包括指导教师）研究、讨论与赛题有关的问题。

我们知道，抄袭别人的成果是违反竞赛规则的, 如果引用别人的成果或其他公开的资料（包括网上查到的资料），必须按照规定的参考文献的表述方式在正文引用处和参考文献中明确列出。

我们郑重承诺，严格遵守竞赛规则，以保证竞赛的公正、公平性。如有违反竞赛规则的行为，我们将受到严肃处理。

我们允许数学中国网站(www.madio.net)公布论文，以供网友之间学习交流，数学中国网站以非商业目的的论文交流不需要提前取得我们的同意。

我们的参赛队号为：1651

我们选择的题目是： D 题

参赛队员 (签名) ：

队员 1：卓泽滨

队员 2：徐小圣

队员 3：周欣缘

参赛队教练员 (签名)： 无

卓泽滨

徐小圣

周欣缘

第八届“认证杯”数学中国

数学建模国际赛

编号专用页

参赛队伍的参赛队号：（请各个参赛队提前填写好）：

1651

竞赛统一编号（由竞赛组委会送至评委团前编号）：

竞赛评阅编号（由竞赛评委团评阅前进行编号）：

Bitpoll: an electronic voting system based on blockchain

Abstract: With blockchain technology advancing, it has been applied in various fields. In election for example, blockchain can tackle the root problem of traditional e-voting system insecurity caused by third-party authority. This paper provides a brief review on blockchain and raises an underlying design of blockchain electronic voting system (BEV). Then potential problems of existing BEV systems are evaluated and corresponding solutions are provided. Finally, some extra ideas are proposed in order to reduce the complexity of the system and improve its security.

Key words: Blockchain; Bitpoll; Incentive; Consensus Algorithm; PoW; Public-key cryptography; Security

Summary

The passage mainly discusses on an underlying design of a BEV system, the possible problem of existing BEV model and solution accordingly as well as the optimization and improvement of the complexity and security of the BEV system.

First of all, the article carries out a review on blockchain. Imitating the Bitcoin blockchain techniques, an underlying design of BEV is raised, which turn Bitcoin to Bitpoll. With modification of some protocols and rules, a decentralized voting system is born.

Furthermore, the present paper analyzes the potential problems of the existing BEV system on their incentive mechanism, consensus algorithm and security respectively as well as some innovative solution and novel techniques. From different aspects of the blockchain layers, the article points out several vulnerabilities which might cause extinct danger.

Besides, Optimization on the algorithm and approaches to improve the security of the BEV systems are introduced. Some State-of-the-art methods like Mimic blockchain, PoRA and FORK-256 hash function are also proposed, which are likely to reduce the complexity of the whole network and strengthen the robustness of the systems. Eventually, the passage introduces another model on the basis of smart contract and Ethereum and some future work, existing in other BEV, is illustrated as well.

Technical Note:

The basic techniques deployed in blockchain this paper are as follows:

- Peer-to-Peer Network Technology(P2P)

  P2P network is the underlying layer of the blockchain, as its physical basis, this paper intends to adopt DHT network for shorter network delay.

- Asymmetric Cryptographic Technique

  As a backbone to the blockchain, most of the procedure will employ it for privacy sakes. This passage employs Elliptic Curve Cryptography to generate public key from private, RIPEMD160 to gain public key hash, Base58 Algorithm to deduce the wallet/ballots box address. And finally, SHA256 for calculation of merkle roots and block hash.

- Consensus Algorithm—Proof of Work (PoW)

  Consensus Algorithm is to maintain the consistency of the blockchain copies on all the nodes. The article mainly introduces PoW, the method of verification by workload, also the mainstream of virtual coin.

- Smart Contract

  An automatic-execute code on the platform called Ethereum in essence. It is widely deployed in various fields besides currency.

- Mimic Defense Technology

  Mimic Defense Technology is to adopt a different consensus algorithm with more safety from cyberattacks, whose core is the following techniques DHR.

- Dynamic Heterogeneous Redundancy (DHR)

  A Cryptography that change the algorithm randomly with a key, thus increasing the security.

- Proof-Of-Random-Authority

  A innovative technique as a consensus algorithm, randomly selected nodes among the miners for verification instead of the whole network.

- Difficulty Modifying Strategy Using Electric Load

  To adjust the difficulty according to the electric load of the power grid thus saving the energy resource due to the process of mining as well as maintaining the block size effectively.

- HVC Paralleled Algorithm

  A hash function as to mix various hash algorithm to prevent the blockchain from centralizing by large-scale mining pools

- FORK 256

  A quite state-of-the-art hash has stronger security than SHA256 from cyberattacks like "Rainbows"

Contents

Summary.. 4
Technical Note:... 5
Contents..6
I. Introduction...8
II. The Description of the Problem..8
III. Brief review on blockchain... 9
3.1 The Distributed network...9
3.2 Transaction... 10
3.2.1 Public Key Cryptography [9]... 10
3.2.2 Elliptic Curve Cryptography and Hash Algorithm.............................11
3.2.3 The Data Structure of Transaction Record.. 11
3.2.4 The Verification and Broadcast of Transaction................................. 12
3.3 The Data Structure of the Block...13
Timestamp and Timestamp Server:...13
Block Body:.. 13
Merkle root:...13
Block ID:...14
Nonce:.. 14
Difficulty:... 14
3.4 Procedure of Adding A New Block.. 14
3.4.1 Miners and Incentive...14
3.4.2 Consensus Algorithm.. 15
3.5 General Model of Bitcoin...16
IV. The Underlying Design Models Based on Blockchain.. 17
4.1 Bitcoin to Bitpoll..17
4.1.1 Distribution of Bitpoll... 17
4.1.2 Voting Operation and Bitpoll Structure...18
4.1.3 Protocol to Prevent Bitpoll Reuse... 19
4.2 Miners and incentive.. 20
4.3 Registration... 20
4.4 Consensus Algorithm and Data Structure of Block.................................... 21
4.5 Privacy Protection.. 22
4.6 Difficulty Modifying Strategy..22
4.7 Abstention... 23
4.8 The Entities of Bitpoll Blockchain...23
Registration Server:...23
Eligible voters:.. 24
Miners:... 24
Tallying Authority:.. 24
4.9 Election Stage..24

Registration Phase..24
Initial Distribution Phase..24
Voting Phase...25
Tallying...25
Verification...25
V. Possible Problems of Blockchain Technology in REV and Improvements............25
5.1 Incentive...26
5.2 Consensus Algorithm.. 26
5.3 Security[19]... 26
VI. Optimization and Improvement on Complexity and Security.............................. 27
6. 1Mimic blockchain contribute to the security of blockchain...........................27
6.1.1. Potential Security Issues in Blockchain Technology........................ 27
6.1.2. What is Cryptographic Sortition Technology?..................................28
6.1.3. What is Mimic Blockchain?...28
6.2 PoRA Consensus Algorithm to Reduce the Complexity...............................28
6.3 FORK-256 for Better Security..29
VII. Conclusions... 29
VIII. Future Work..30
8.1 The limitations of the current e-voting systems..30
8.2 The Smart contract in e-voting system..30
VI. References..32
Appendix..33
7.1 The Principle of ECC[8,10]... 33

I. Introduction

When it comes to the secure elections, mounting number of people have come to realize the severity of such an unsettling phenomenon that there are still plenty of room for existing voting systems to improve. It is not surprising to hear remote absentee ballot tampering in a voter fraud incident these days. A latest example is the ballot tampering scandal in the 2019 North Carolina elections

As mail-in votes tend to be nefariously used such as being impersonated, altered or threated, Information Technology has been widely applied to the voting system. However, most of the electronic voting systems design might be poor where online ballots should go through a database administrator, namely a third-party certification authority with poor behavior [1], Since e-voting systems might affect the feeling of the voter for their rights [2,3]. Therefore, it is significant to abandon the third-party authority without risk of system disabled. A novel e-voting system different from the traditional one will be proposed in the present paper.

Similar to Bitcoin blockchain established by Nakamoto in 2009, the present paper comes up with a Bitpoll model where the Bitpoll would be tallied by the whole peer-to-peer network instead of statistics bureau. Supported by a distributed network consisting of large number of interconnected nodes, each of these nodes has their own copy of distributed ledger that contain the full history of voting record. The advantages of using a e-voting scheme on blockchain basis might include the following [4]: i) Greater transparency because of the open blockchain, ii) well protection for voters due to its inherent anonymity, iii) stronger integrity and immutability for voting record with copies of chain on each nodes and consensus algorithm.

The present paper demonstrates an underlying design for e-voting using blockchain technology and discuss the potential problems of REV systems and the corresponding solution and techniques that might benefit to the simplification and safety of the blockchain.

II. The Description of the Problem

In order to design a blockchain electronic voting system (BEV), there are various factors which might affect the results of elections should be considered. Therefore, the present paper concludes following problems that a BEV should be able to solve [4,17]:

Eligibility: Voters could not vote more than command. And to avoid virtual identification abuse, they must pass through the identification.

Privacy: The voting operation should stand secret, namely it is probabilistically impossible to learn which one deliver the ballots. Moreover, one could not find out the number of the ballots a candidate gains directly.

Coercion-Resistance: A coercer has no way of checking in the BEV whether the victims follow the demand or disobey it.

Transparent Auditability: This property allows the public even without voting rights to download the blockchain of the election and help to audit and verify the results.

System Robustness [20]: The BEV should be able to support a large-scale national election, which requires the high system currency and process ability. Furthermore, the robustness demands the ability of system continuing to run when confronting the malicious attacks.

Receipt-Freeness: A voter could not generate a receipt that allow he or she to demonstrate to a third-party for voting a certain candidate, which could prevent cash-for-votes.

Unreusability: A candidate could not cast the ballots receiving from other voters to another person.

Affordability: the voting fee both for the voters and election holders should be affordable.

III. Brief Review on B lockchain

In order to understand this paper easier, it is necessary to take a review on blockchain. Since blockchain technology is popularized by the digital currency Bitcoin firstly, we take the Bitcoin as an example.

When a transaction takes place, central authority or accounting intermediary keeps track of the transaction with detailed record in traditional system. However, it still suffers from the inherent drawback such as mediating disputes [6]. Hence, in the idea of Nakamoto [7], blockchain serves as a distributed database or joint register of all transaction. When two agents wish to engage in a transaction, they first broadcast this signal to all the self-organized network (often P2P network). Then all the nodes in the network will try to verified and final record it on their ledger if it passes the verification, thus bypassing a central bank to record it. Each individual node contributes to maintaining the public blockchain by updating their own ledger (Fig. 1).

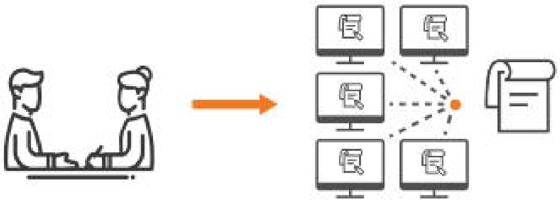


Fig. 1 blockchain maintaining process

3.1 The Distributed network

The physical basis blockchain is peer-to-peer distributed network. Varying from the C/S construction, it is a decentralized network architecture with a higher data transfer rate and security [8]. One of the characteristics of distributed network is that each node equals to one another and there are not nodes owing the privilege to control or manage other nodes. The chart of a general distributed networks are as follows:

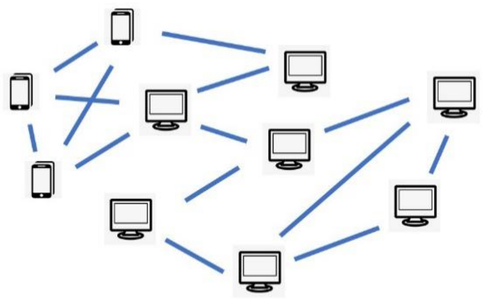


Fig. 2 A general unstructured distributed network

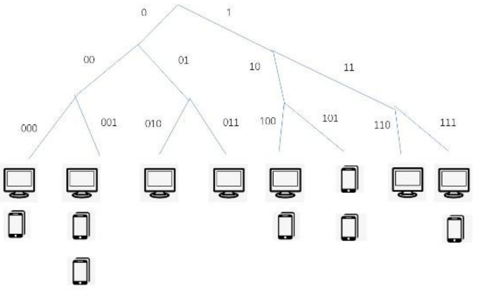


Fig. 3 An DHT based distributed network

However, an unstructured distributed network (see Fig. 1) seems to suffer from signaling flood frequently, hence, to solve this problem, various kinds of structured networks are arisen. A distinguishing feature of DHP based structured network (see Fig. 2) is that it adopts a hash table to map computer resources and address together, hence improving the rate of data transfer and avoid data floods to some extent.

3.2 Transaction

When two agents decide to make a deal, the sender should first encrypt the transaction message using cryptographic techniques in order to protect their privacy.

3.2.1 *Public Key Cryptography* [9]

One of the famous and widely-used cryptographic techniques is public key cryptography. When one wants to convey a message to another through the internet, the sender could encrypt it by the public key of receiver, then, the receiver gets the ciphertext and read it with his private key while the public keys are transparent and private keys are private as the name suggest. Moreover, senders can apply their private key to encrypt the message as digital signature and deliver it with original text. Hence receivers could decrypt the digital signature with the public key of the sender, thus marks the message as genuine by compare the solution with the original text.

In the blockchain model, each node owns both private key and public key. While the public key is open, the private should be strongly preserved. As it is suggested by Huang. Z[8], the public key can be derived from private key employing SECP256K1 algorithm. With the public key, one can deduce the wallet address of the key owner by base58 coding algorithm (Bitcoin for example). The procedure is as follow:

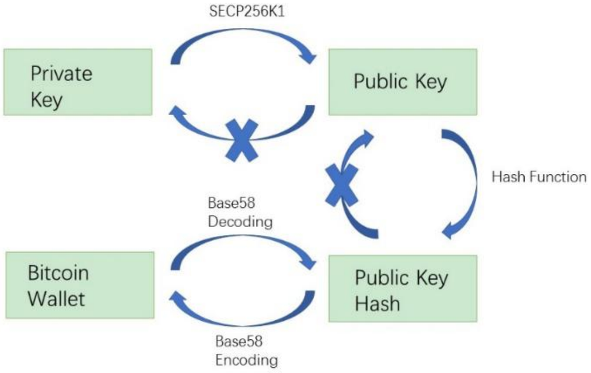


Fig. 4 Private key, public key, wallet address transmitting relationship

3.2.2 *Elliptic Curve Cryptography and Hash Algorithm*

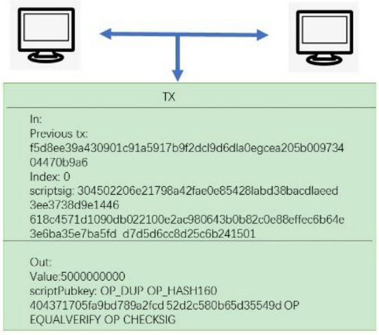
In 1985, Victor Miller and Neil Koblitz employed the Elliptic Curve to the public key cryptosystems which made progress and is adopted by Nakamoto as one of the techniques in blockchain (SECP256K1). As the investigation of Surhone L.M showed that the security of elliptic curve cryptography (EEC) is based on the elliptic curve discrete logarithm problems (ECDLP) which has no sub-logarithmic algorithm to solve, hence results in shorter key lengths than RSA and DSA but same security [10].(For more detail of the principle of EEC, please refer to the Appendix)

One of the most important algorithms for blockchain is hash function. Huang.Z[8] visually compare the hash algorithm to the backbone of the blockchain, that is to say not only is it applied in public key cryptography but also most of procedure in blockchain such as mining.

The hash algorithm used in public key cryptography is SHA256. Designed by NSA, it compresses a string of arbitrary length to a string of fixed length with immense difficulty to invert. As Selvakumar A.L. [11] declared in 2009, SHA256 meets the cryptographic property requirement. It is computationally infeasible to find second two distinct inputs that hash to a same output. Moreover, it has been widely proved as invulnerable to various kinds of cyberattack [11,12].

3.2.3 *The Data Structure of Transaction Record*

During a Bitcoin transaction, the payers first generate a transaction record like Fig.5



```
TX
In:
Previous tx:
f5d8ee39a430901c91a5917b9f2dcl9d6dla0egcea205b009734
04470b9a6
Index: 0
scriptsig: 304502206e21798a42fae0e85428labd38bacdlaeed
3ee3738d9e1446
618c4571d1090db022100e2ac980643b0b82c0e88effec6b64e
3e6ba35e7ba5fd  d7d5d6cc8d25c6b241501

Out:
Value:5000000000
scriptPubkey: OP_DUP OP_HASH160
404371705fa9bd789a2fcd 52d2c580b65d35549d OP
EQUALVERIFY OP CHECKSIG
```

Fig. 5 Bitcoin transaction record

In the above sheet, there are information "In" and "out" that show the origin and destination of the Bitcoins used in transaction.

1. Previous tx means the block ID (usually a hash) where the Bitcoins come from. If the Bitcoins ready to pay has origins more than one, then there must be several number of "In" accordance to the number of the origins.
2. Index: the attribute "index" refers to the index of origin of Bitcoins ready to pay. One can easily backtrack the Bitcoins with index and previous tx.
3. Scriptsig: the digital signature of the payer
4. Value: the total value of the transaction, a Satoshi one unit.
5. scriptPubkey: the public key of payee. The wallet address can be derived from the Pubkey.

3.2.4 *The Verification and Broadcast of Transaction*

As the following figure show, the attribute Scripsig is the script of the digital signature and is convey together with the original data such as the wallet address, the value of the Bitcoin transfer and the public key of the payees et.al (by ciphertext). Then, the digital signature is created by encrypting the above original data with the private key of the payers. Finally, the original data, digital signature and the public key of the payers are delivered together to the distributed network.

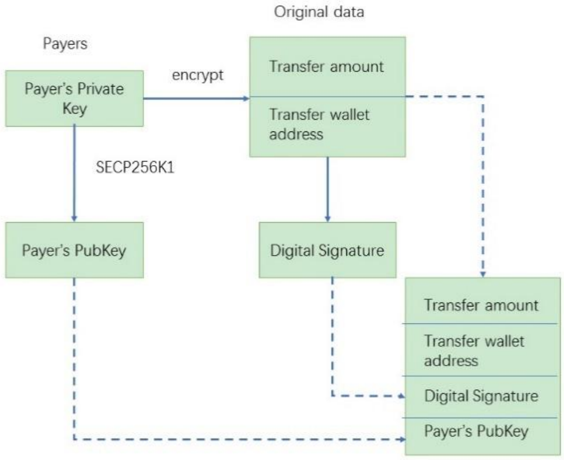


Fig. 6 The procedure of creating a transaction

The closet nodes in the network will first gain the transaction record and then verify it using the digital signature, original data and the public key. By decrypt the digital signature with the public key and compare the original data to the plain text solved above. If both are the same, then the node finishes the first verification phase.

Secondly, the nodes receiving the transaction will verify the feasibility of the transaction. As it is mentioned above, the origin and destination of each transaction is recorded in the "in" and "out", hence, the node could track back in "in", and check whether there are enough Bitcoins for the payments in the last transaction where the Bitcoins ready to pay come.

If all these verifications are done, then the nodes gaining the transaction will help to broadcast it to other nodes next to them who would do the same examinations above and broadcast it in the same way unless more than 51% of the whole nodes confirm it.. Otherwise, the transaction would be sent back to the payer node with a error notification and the request of broadcast will be rejected.

3.3 The Data Structure of the Block

If compare the Blockchain to a ledger, then a block was one page. A general view of blockchain and block structure is described as Fig.7

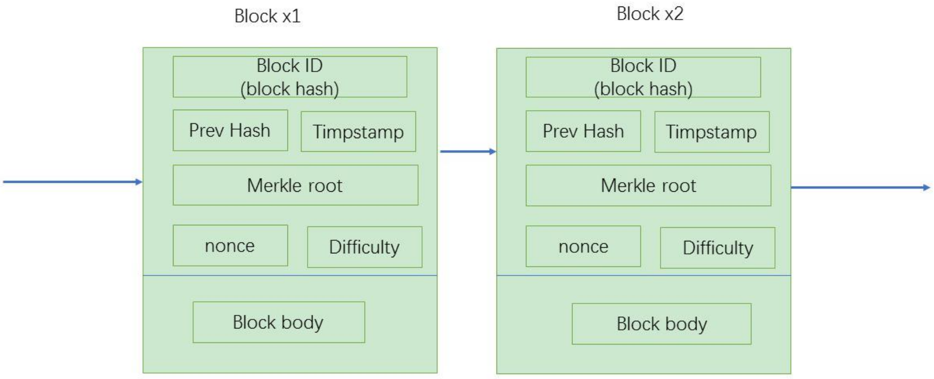


Fig. 7 the data structure of the block

Nodes on the network regularly consider the longest chain to be the correct one and will maintain a copy on the disk and keep working on it. Since it is so impractical to keep all the data of every block in a PC, some users of nodes only need to keep the copy of the block headers of the longest chain. Although it is possible that there are two chain with same length in the net Simultaneously, the nodes will work on the chain they received first and keep a copy of another. The tie will last until another block is created and one of the branches become longer [6].

Timestamp and Timestamp Server:

Timestamp as one of the authentications of the data in every block is produced by a timestamp server. The timestamp proves that the data have existed in a certain time[6].

Block Body:

The Block Body is mainly composed of the transactions collected from the networks.

Merkle root:

Derived from the transactions collected in the block, the Merkle root includes all the information of the transactions. The computation process of Merkle root is a Merkle tree: Firstly, every transaction in the block will turn to a hash by the hash algorithm (usually the SHA256), Then the hashes produced above will be hash once again two by two until there is only two hashes leave. Finally the Merkle root is hashed from the final two hash [6]. An example of a computation process of the Merkel from four transactions block is as Fig.8:

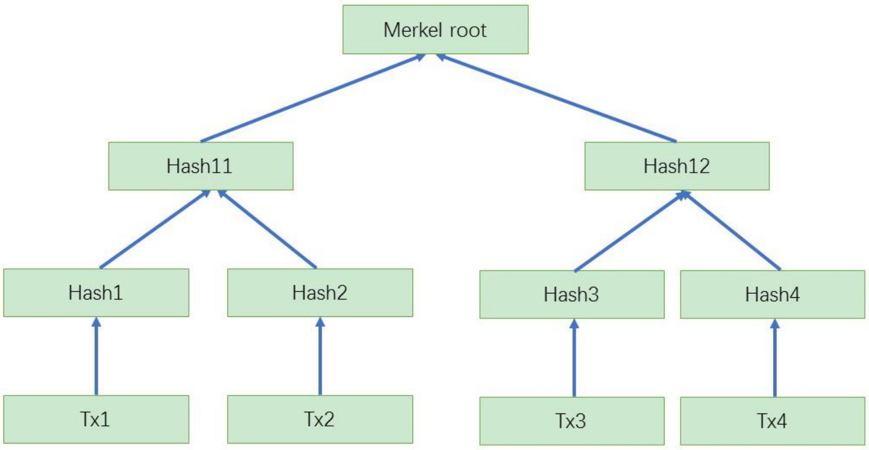


Fig. 8 The Computation Procedure of Merkle root

Furthermore, the Merkle root, as proposed by Nakamoto, is applied to compact the size of the block. When the latest transaction in a coin is buried under adequate blocks, then the spent transaction before it can be discarded to save the disk space. With Merkle, the block hash (block ID) would not change even some transaction with less necessity.

Block ID:

The block ID, block hash as well, is calculated from the Timestamp, block hash of previous block, Merkle root and a nonce by hash them together in a hash function. When a miner in the network pass the consensus algorithm successfully, then a new block is created with the block hash calculated before.

Nonce:

A Nonce is a random number, generated during the process of producing a block, to create a qualified block hash. When a miner successfully passes the PoW (a consensus algorithm), then it must broadcast the block it created exactly to all the node to verify it. The node gains the result will use the nonce to create a block ID and check whether it meets the target [2].

Difficulty:

In order to maintain the generation circulation of blocks to ensure each block owns almost the same size, the Bitcoin blockchain introduces difficulty based on the average computing power of the network. Bitcoin blockchain adjusts the degree of difficulty whenever 2016 blocks have been established, hence ensuring the circulation of creating a block is 10 minutes approximately. The difficulty is adjusted according to the following formula:

$$New\ Difficulty = \frac{Old\ Difficulty \times Actual\ time\ cost\ of\ last\ 2016\ blocks}{2016 \times 10\ min} \qquad (1)$$

3.4 Procedure of Adding A New Block

3.4.1 *Miners and Incentive*

All the nodes participant in adding new block to the existing blockchain owns a reserve blocks themselves. They sniffs the whole network for transactions and then put the transactions they collected in their reserve blocks, calculating the Merkle roots Simultaneously as well as block hash until the reserve blocks is full, then miners will continue calculating the block hash unless the block hash meets the target or other nodes successfully reach the target[8] (see Fig.9).

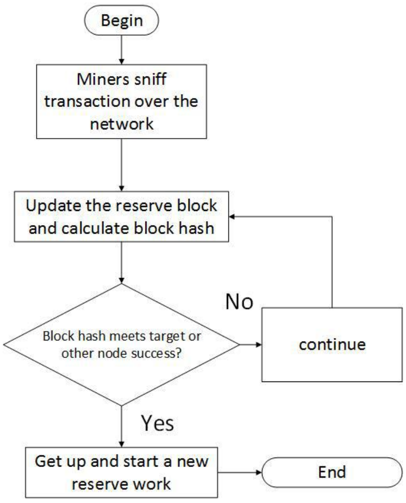

Begin
Miners sniff transaction over the network
Update the reserve block and calculate block hash
Block hash meets target or other node success?
No
continue
Yes
Get up and start a new reserve work
End

Fig. 9 The procedure of miners and the way block creating

Every node succeeds in adding a node to the blockchain will gain a certain number of Bitcoins. Hence there are always passion for some nodes to devote in the above work, which are vividly mentioned as mining.

3.4.2 *Consensus Algorithm*

In order to prevent inconsistency of the copies on the whole network, it is necessary to establish a mechanism to ensure that the establishment of blocks is agreed by the whole network. In numbers of cryptographic protocols, provers tend to convince verifiers that they possess knowledge of a secret or that a certain mathematical relation holds correct. On the contrary, in the proof of work mechanism employed by the Bitcoin Blockchain to guarantee a unique ledger (blockchain), provers demonstrate to the verifiers that they have finished certain amount of work in specified interval of time [13].

The principle of Pow is as follow:

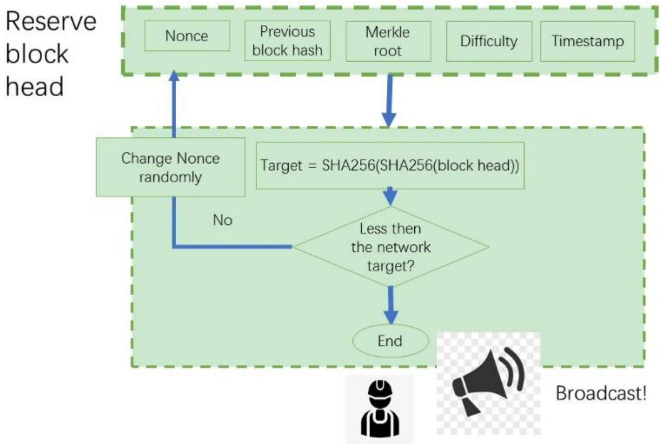


Fig. 10 The principle of PoW

When a miner has created a reserve block, what he wants to do is to demonstrate his reserve block to other nodes and thus have a chance to add the blockchain with his reserve block so as to gain his reward, which might results in multiple versions of blockchain. Hence, the PoW is applied in the Bitcoin to solve this problem. As Fig.10 shown above, after specify numbers of blocks (2016 for Bitcoin) have been added, the network target will change corresponding to the difficulty which will change as the formula (1) shown before.

By modify the nonce in the head of reserve block randomly, the requirement that target must less then network target will be met with a certain nonce. Hence, a node with more computing power could be faster to meet the requirement because it tests more nonce in same interval of time. When a node succeed in gaining a solution, it will first delivered the block head and nonce to other nodes next to it who will stop mining to check whether the nonce with the block head accordingly is qualified by just doing a hash algorithm to the above two data and comparing the result to the network target.

With most of the node confirm the qualification of the nonce, the reserve block will then be added to the blockchain.

3.5 General Model of Bitcoin

All above, blockchain is physically based on distributed network. Each node in the network will generate transactions which encrypted as ciphertext and broadcast to the whole network. Each node getting the transaction will check its credibility and contribute to transfer it or stop it. Miners, playing a role in packing the transactions to a block and adding to the blockchain, never stop sniffing the information transmitting in the network and struggling to colliding a nonce to meet the consensus algorithm to makes their fortune.

There are some points worth paying attention. New transaction do not necessary to transfer to every node. As long as they reach many nodes, they will eventually get into a block before long. Nodes always account for the longest chain and keep it. If there are different versions of blockchain, the nodes will stick to the first one they got, and keep a copies of other versions until the longest blockchain takes place [6].

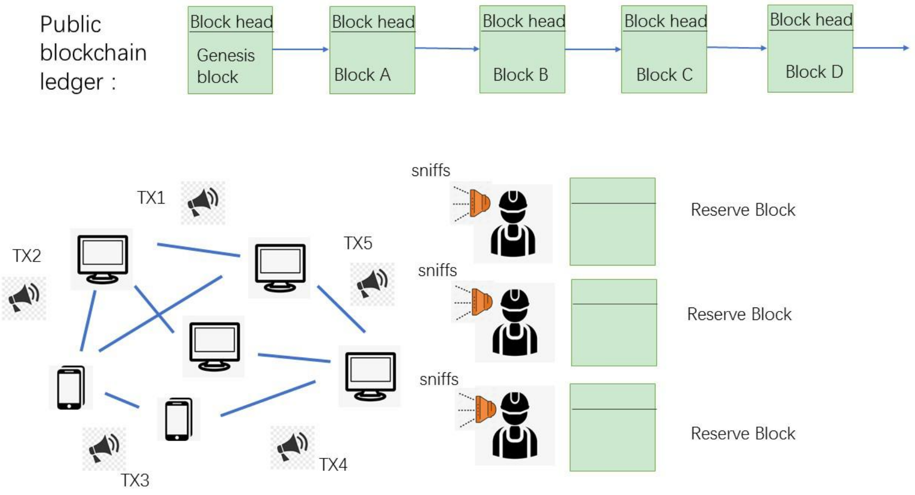


Fig. 11 General Model of Bitcoin

IV. The Underlying Design Models Based on Blockchain

Each ballot must go through a third-party authority like auditing bureau to record it on the traditional remote e-voting systems (REV). Hence compared to the currency system, this paper proposes a blockchain-enabled voting (BEV) system mainly similar to Bitcoin technology despite some disputes.

4.1 Bitcoin to Bitpoll

supposing that the procedure of voting as a transaction, namely one votes for somebody is to give the Bitpoll he owns to the person he votes for. Then we can adhere mainly to the construction of Bitcoin.

4.1.1 Distribution of Bitpoll

Different from the Bitcoin which generated by mining, the Bitpolls must be delivered to all the voters when the election begins. Hence, in this paper, the first block of the blockchain is not created by a miner but the authority. In the first block, there are operations in the block body that give every voter a Bitpoll.

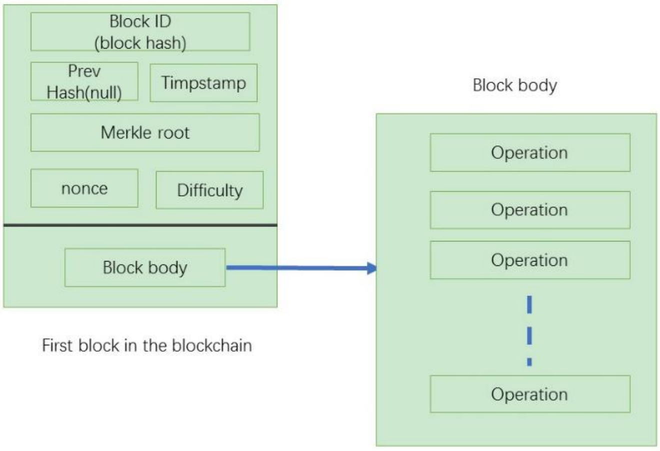


Fig. 12 The initial distribution of Bitpoll

In the above figure, the operations in the first block is to deliver a Bitpoll to every electors.

4.1.2 Voting Operation and Bitpoll Structure

The payments of Bitcoins are not so much based on the balance as the records of previous transactions of the Bitcoins to pay [8]. Every Bitcoin can date back to its original block where there is a record noting how the Bitcoin is born (always generates as a reward for miners). Suppose there is a transaction which is created by the activity that A pays B 10 Bitcoins:

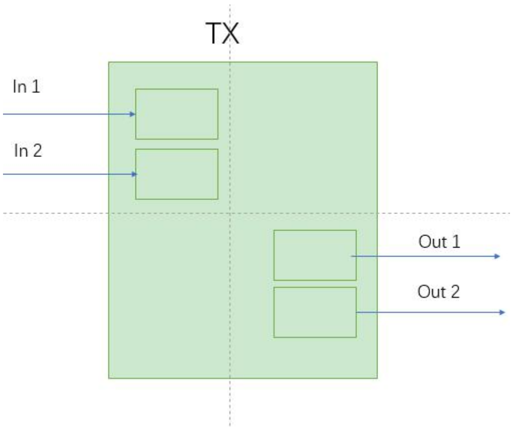


Fig. 13 A transaction record created by a payment

Suppose A has 12 Bitcoins totally. 9 coins comes from "In 1" where one can track back to the last transaction of the coins and the original block if he or she likes. The other 3 could be dated from "In 2". Since 9 coins absolutely not enough to pay B, the transaction must be composed of both "In". The transaction must consist of two "Out" one for B while another for changing for the sake of maintaining the continuities of these Bitcoins.

Therefore, it is significant to describe the voting operation since Bitpoll is similar to Bitcoin.

This paper proposes the data structure of voting operation as follow:

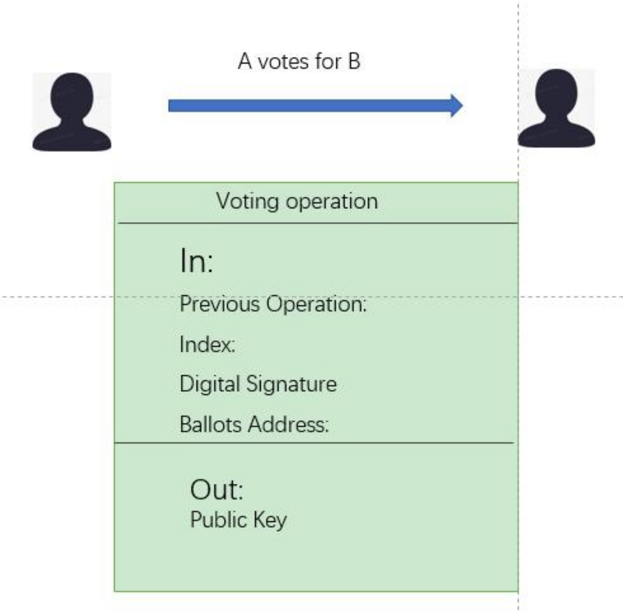


Fig. 14 voting operation structure

Similar to Bitcoin transactions, the meaning of attributes are as follows:

Previous Operation: the block hash of the last operation of Bitpoll (usually the first block)

Index: to locate the exact position of the last operation in the block.

Digital Signature: with the same cryptography, it is generated by encrypt the original data of the operation with the private key of the voter.

Public Key: the public key of candidate, one can deduce the ballots box address (namely wallet address for Bitcoin) using base58 algorithm.

4.1.3 Protocol to Prevent Bitpoll Reuse

Unlike the Bitcoin, Bitpoll once be delivered to a person, it can not be sent to other by the person receiving it.

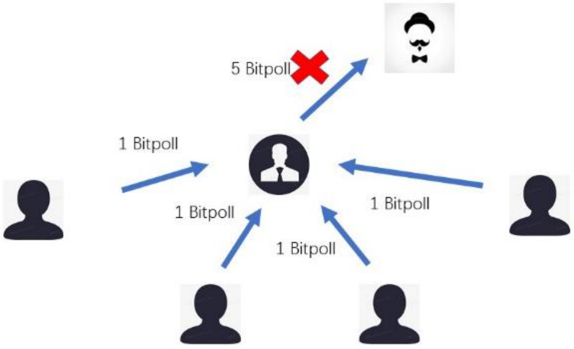


Fig. 15 Ban If there are candidates reusing other voters' ballots.

This rule could be realized by demanding that the Bitpoll convey to a certain ballots box must check it "in" first. Nodes close to the voter node receive the voting operation broadcast will check whether this Bitpoll is from the first block of the blockchain. If not, then the nodes refuse to broadcast the operation and send a error information to the voters (see Fig. 16)

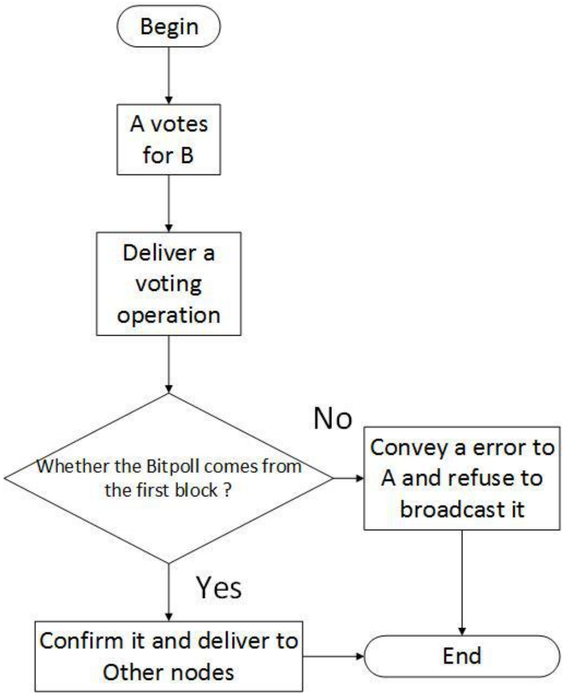

Begin
A votes for B
Deliver a voting operation
Whether the Bitpoll comes from the first block ?
No
Convey a error to A and refuse to broadcast it
Yes
Confirm it and deliver to Other nodes
End

Fig. 16 Procedure Diagram on preventing Bitpoll abuse

4.2 Miners and incentive

Be opposed to Bitcoin, there seems to be no one being volunteered to practice complex calculations to create block and add it to the blockchain of Bitpoll which will results in poor recording of voting operations. Therefore, on the condition of adopting the PoW as the consensus algorithm, the present paper proposes that, since Bitpoll do not have the property of consuming, the reward for block creator relies on the government with cash. Thus, add an incentive for nodes to support the blockchain.

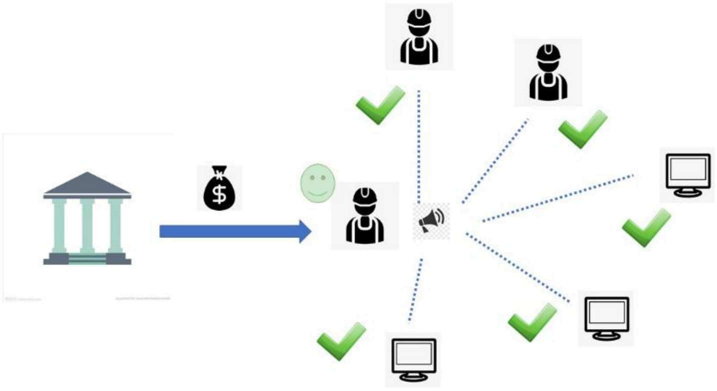


Fig. 17 The Incentive

4.3 Registration

While the owners of Bitcoin might have several virtual wallet addresses, the ballots box address for Bitpolls must be only one, that is only the eligible nodes can vote.

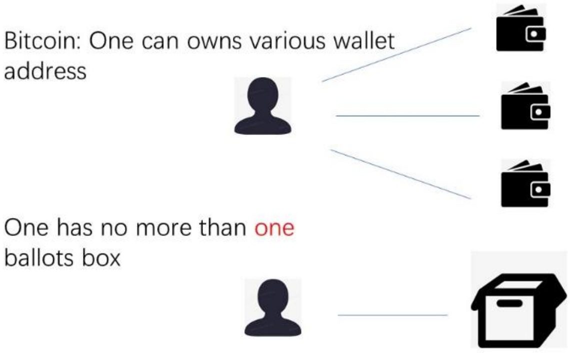

Bitcoin: One can owns various wallet address
One has no more than one ballots box

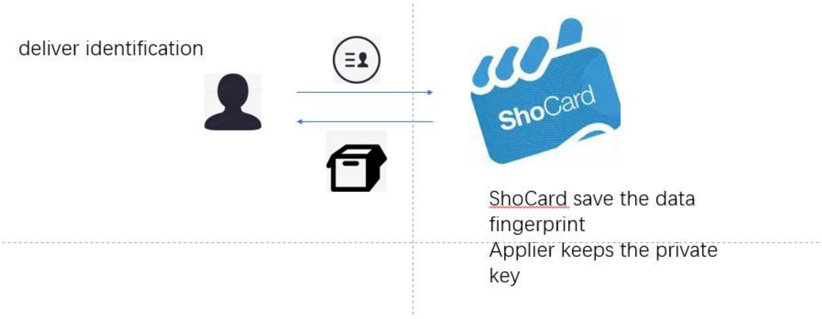
Fig. 18

In order to prevent duplicate application for ballots boxes, there seems to be necessity of the help of a Credit Management Agency to collect the identical of voters, which goes against decentralizing as the paper recommends.

One of the solutions is that we can turn to existing identical management based on Blockchain to help us such as ShoCard, BitID, ID.me, and IDchainZ.[15]. In the run-up to the election, voters should deliver their identification to the ShoCard to gain a ballots boxes address.

The process of gaining a ballots boxes address is as follows (see Fig.: take ShoCard as example)

During the run-up to the election, voters transmit their physical identity cards data (by scanning) to the ShoCard which save the data fingerprints in the blockchain and send back an encrypted identity information to the local disk of the voters using smart contract techniques [8,15]. No one (including ShoCard itself) is not able to alter it without the private of the owners. Thus, the duplicate application would be avoided thanks to the fingerprints in the ShoCard blockchain. And if one tries to reapply for two address, the application would be refused due to the identity record that already exists in the ShoCard.


deliver identification
ShoCard
ShoCard save the data fingerprint
Applier keeps the private key

4.4 Consensus Algorithm and Data Structure of Block

Like Bitcoin blockchain, the data structure of block in the blockchain has block head and block body. While the block body collects the voting operations from the network, block head contains previous block hash, timestamp, version, Merkle root and nonce et.al. The block structure is described as Fig.19:

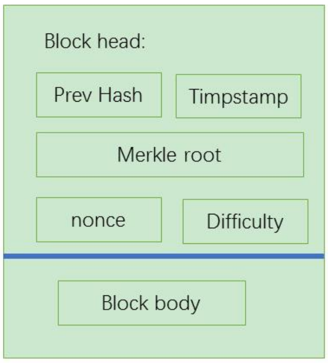


Fig. 19 Block Structure

Similar to Bitcoin as well, the Consensus Algorithm is PoW to address the inconsistency problem in the distributed system. The difficulty will automatically be modified. Every miner who wishes to gain the money from the government must struggle to add his or her reserve block to the blockchain and broadcast it to the whole network to verify it.

4.5 Privacy Protection

Although the Blockchain is open and transparent to the network, one is unable to recognize the identity of both voters and candidates for every voting operation is encrypted with EEC and hash function cryptography. A public key or ballots address of voters and candidates have nothing to do with the real identify. Therefore, both the voting activities and the identity of the voters will not leak to the network.

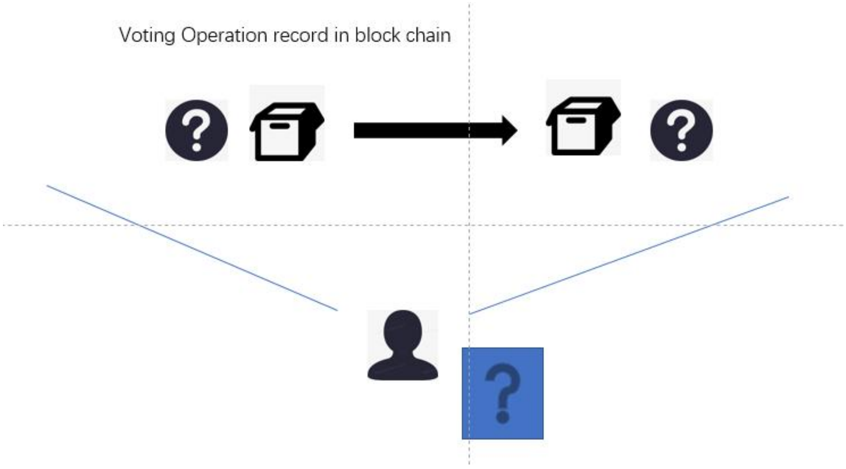


Fig. 20 The other node could not recognize the exact identity in the open blockchain

4.6 Difficulty Modifying Strategy

To the contrary of Bitcoin, the difficulty of adding a block to blockchain is adjusted with the computing power of the whole network to maintain the interval of time of adding a block. However, it might be necessary for our blockchain to behave this way. The interval of time could be adjusted to suit human schedule. Considering fewer voting operation would takes place in the middle of the night, the interval of time could be increased by enhancing the difficulty. The present paper demonstrates a method to adjust the difficulty by change the interval of the time for creating block with the national/local electrical load.

The relationship between time and electric load is as follows:

$$t = e^{4(L-1)^2} \tag{2}$$

where t is the interval of time, L is the electric load of the power grid. L equals to 1 means full load while 0 means no power usage.

The formula (2) is described as

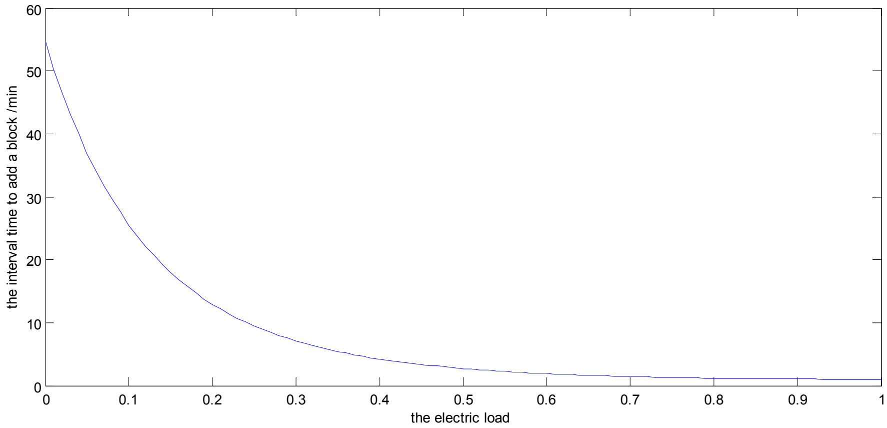


Fig. 21 The relationship between time and electric load of power grid

The curve above show that when the local/national power grid is full load, then in order to catch up with the soaring voting operation to maintain the block size, the interval of time should be adjusted to 1 minute.

Suppose n is new block during the update circulation of the difficulty, ND is the new difficulty, and OD the previous, and t_0 refers to the actual time of creating n blocks, then the adjust formula of the difficulty is as follows:

$$ND = \frac{OD \times t_0}{nt} \tag{3}$$

4.7 Abstention

While there might be some one abstains from voting, it is necessary to set an abstention method. We command if voters do not cast away their ballots, then it is regarded as abstention automatically.

In order to avoid counting the Bitpoll left due to abstention, this paper declares that the tallying organization could only count the Bitpoll whose "in" does not come from the first block of the blockchain.

4.8 The Entities of Bitpoll Blockchain

***Registration Server*:**

The roles of registration server is to register eligible voters and prevent duplicate registrations of voters. In order to decentralize, this paper proposes to work with the identity management blockchain like Shocard.

Eligible voters:

Each voter owns a ballots box with a initial Bitpoll distributed by the first block. They have the rights to cast their initial Bitpolls to other ballots box address.

Miners:

The miners play an important role in supporting the network. They never stop collecting the voting operations and pack it to a reserve block. Then tempted by the incentive, they will struggle to do hash calculations and add their reserve block to the blockchain.

Tallying Authority:

With the transparent and open blockchain, one could easily find out which is the finalist. While it is time impractical for a person to do all the statistic work, hence there must be some organization to do the jobs. Although it seems go against the principle of decentralization, the tallying authority could not practice fraud because of the open and transparent blockchain. The Tallying Authority could be trusted third-party authorities, other organization work for social interest or the modest or large scale parties.

4.9 Election Stage

Registration Phase

This phase takes place in a registration server which mentioned above. A voter would gain ballots box address, public key and private key from the identify management blockchain like Shocard after verifying his or her legitimacy by scanning his identification like ID cards.

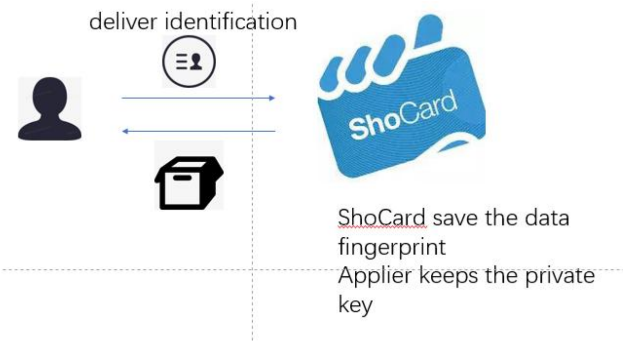

deliver identification
ShoCard
ShoCard save the data fingerprint
Applier keeps the private key

Fig. 22 The sketch of registration phase

Initial Distribution Phase

As soon as the voters register successfully, they broadcast a information to all the network. Different from the voting operation, this information is to create a Bitpoll to their ballots box address. The information will finally reach to the miners. Different from other block as well, this block must be created at the time the voter registration is over, which can make sure most of the information is pack by the miner. Then the first block of the blockchain generates.

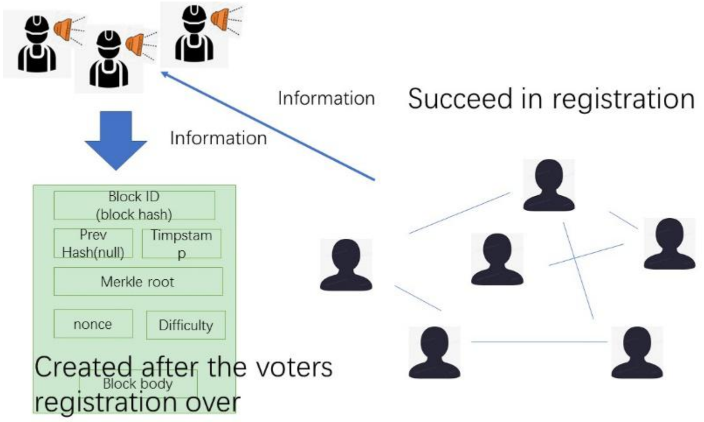


Fig. 23 The first block creation phase and distribution of Bitpoll

Voting Phase

During the election, voters can transfer their Bitpoll to the candidates broadcasting the voting operation to the closet nodes. After passing the verification like Bitcoin mentioned in 3.2.4, the voting information will reach to miners who will pack it to the reserve block. After competing for adding their block, miners will contribute to save the voting operation record to the blockchain (3.4.1/3.4.2).

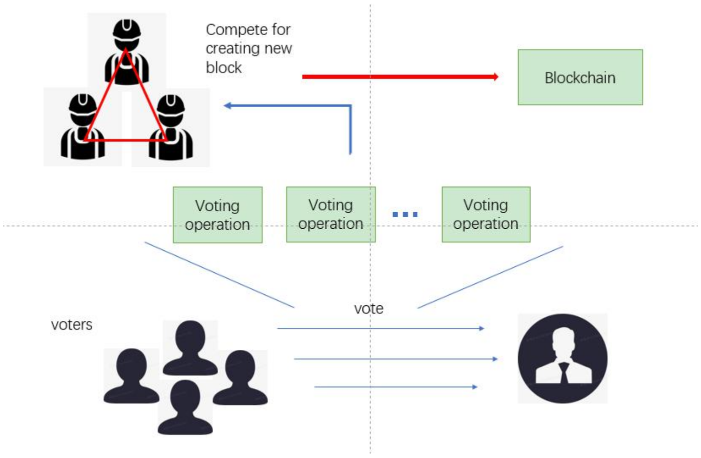


Fig. 24 the sketch of voting phase

Tallying

The tallying organization take charge of counting the amount of Bitpoll of every ballots box address.

Verification

After selecting the ballots box address with most amount of Bitpoll, the candidates should use its private key to verify it. And finally end the election.

V. Possible Problems of Blockchain Technology in REV and Improvements

5.1 Incentive

Due to the huge financial cost, monetary incentive systems are impractical for large-scale national elections [4,16]. Some other BEV systems like VYV [17], Mc Corry, et.al.[18] based on Ethereum charge both voters and the election holders with ETH, which might be an enormous number for a large-size election. However, without incentive, there seems to be few computers packing the voting operation into a reserve block and trying to add it to the blockchain after solving some complex mathematical calculation, which might consume amount of electrical resources.

In order to solve it, the present paper consider to turn the incentive into an obligation, that is to command the election parties to work as miners the without pay.

5.2 Consensus Algorithm

Creating a block based on proof-of-work, one has to finish a certain number of calculations, which seem to waste energy resources. Another problem arose by PoW might be that if there are some cooperating groups of attacker nodes whose computing power is more than 51% of the average of the network, then they might change the block as they like. Moreover, the PoW consensus Algorithm might contribute to expanding the powerful mine pools and eliminating the pools with poor mining power, which tend to go against the decentralization [6,14,19].

Considering the problems caused by PoW, one of the solutions is to adopt another consensus algorithm. Like Proof-of-Share, one who owns Bitpolls more and longer than other would be easier to add his or her reserve block to the blockchain, which could reduce waste of computing power and prevent centralize to some extent.

On the other hand, we can adjust the hash function used in calculating the block hash[14] to restrain the ASIC mining pools, the mainstream of mining machines, designed by specify circuit. One of the modified algorithms is HVC paralleled algorithm, which can reduce the computing ability of ASIC mining pools because this algorithm is hard to be solve using ASIC mining machines. The Scrypt algorithm which relied mainly on RAM could prevent the existing mining pools as well [19].

5.3 Security [19]

According to the technical feature of blockchain, we can divide the blockchain security model into seven layers described in Fig.25

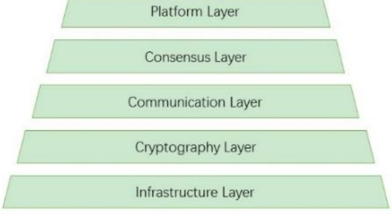


Fig. 25 Seven layers of blockchain for security analysis

The infrastructure layer is the underlying systems of the network. Although the blockchain technique could resist the damage caused by malicious control of few nodes, if network vulnerability makes hackers easy to control the majority, then the whole blockchain would still suffer from danger.

The Cryptography layer plays an important role in keep the integrity, availability and confidentiality of a blockchain system. Blockchain technique, strongly depends on cryptology such as asymmetric algorithm and hash algorithm, which are relatively safe but not absolutely. The method to protect this layer is to update the cryptograph to catch up the hardware.

A blockchain system can be attacked on the communication layer because the P2P network is so open that it may cause some security problems. Attackers can launch eclipse attack, hacking attack and DDoS attack, etc. on some nodes in a P2P network and them pollute the whole network.

Blockchain systems can be grouped into two categories: public chain and license chain. Both need corresponding consensus mechanism to make sure that the last block in the chain could illustrate the state of the total network. Bitcoin system, stands for public chain, applies proof of work (PoW) as its consensus mechanism. However, once the total computational power is too small that attackers can easily hijack the network, according to 51% principle.

Smart contract virtual machines, where smart contract of blockchain runs on, may have some flaws that could be attacked, which would cause serious security problems on platform layer.

Smart contract actually is a piece of code that runs in the blockchain network, so it may have bugs that bring safety risk. Nowadays attack aiming at smart contract is reentrancy attack, transaction sequential dependency attack and time stamp dependency attack, etc.

Various kinds of conventional security problems happen in the application layer because it is involved into different industries and has many interfaces. In fact, most risks in this layer have no relationship with blockchain itself, but the weakness of algorithm, application and platform. Therefore, while improving the safety level of blockchain, it is also important to enhance the infrastructure and the acknowledges of the cyber manager and coders.

VI. Optimization and Improvement on Complexity and Security

6. 1Mimic blockchain contribute to the security of blockchain

6.1.1. Potential Security Issues in Blockchain Technology

The current blockchain can be understood as simple isomorphic redundancy, where each node stores the same data [24], adopts the same consensus algorithm in each census round, and the same signature algorithm. This isomorphic static structure provides convenience for attackers and is the fundamental reason why blockchain is facing security threats at present.

6.1.2. What is Cryptographic Sortition Technology?

Cryptography sortition is a kind of trusted and authenticated balloting in distributed network by means of decentralized method [24]. Turing prize winner Sivio Micali's Algorand Blockchain protocol applies the cryptographic sortition technology to the blockchain, where the system creates and updates a parameter called “seed” that cannot be predicted or controlled by an attacker. Sivio Micali publishes a verifiable random function (VRF) according to the seed during each round of consensus process. Each user performs the VRF with his or her private key to obtain a corresponding credential. Users whose credentials meet certain criteria are identified as validators of this consensus round, and each validator completes a block and publishes it with his credentials. In this round, the verifier with the smallest dictionary order of credentials is identified as the leader. Finally, all verifiers run the Byzantine protocol against the leader's block

6.1.3. What is Mimic Blockchain?

Mimic defense [25] is a new network security defense technology, whose core is dynamic heterogeneous redundancy (DHR), aiming at solving uncertain threats based on unknown loopholes, back donors or virus on the relevant application levels of network space. In the DHR consensus mechanism, each consensus node determines the consensus mechanism to be adopted and completes the consensus in each round of consensus by means of cryptographic sortition. Finally, the final consensus node of this round should be determined according to the voucher of the cryptographic sortition. That is to say, DHR adopts dynamic signature algorithm. Even if an attacker can forge a signature algorithm, the system can change it into another consensus mechanism at any time, the DHR is described as follows:

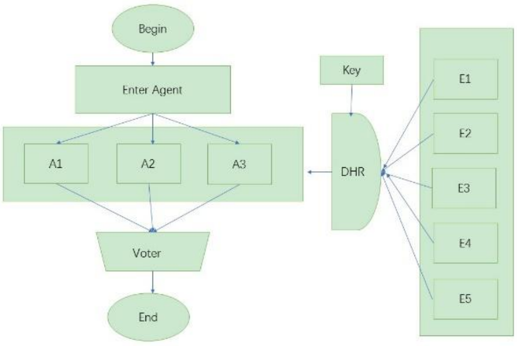


Fig. 26 the principle and process of DHR

Mimic blockchain takes advantage of this latest technology, which might be the solution to the security of blockchain.

6.2 PoRA Consensus Algorithm to Reduce the Complexity

To reduce the complexity of blockchain technology, a new consensus mechanism named proof-of-random-authority (PoRA) is designed. Different from PoW, which requires every node in the network to verify the information broadcast by the first miner who solves the puzzle, the verification process in PoRA is carried out by randomly chosing online nodes with a dynamic probability. The other nodes supervise the selected nodes to guarantee they are credible to some extent. Extra rewards are allocated to these chosen nodes so that spare computation power will not be totally wasted and prevent some malicious nodes from keeping online for being selected multiple times.

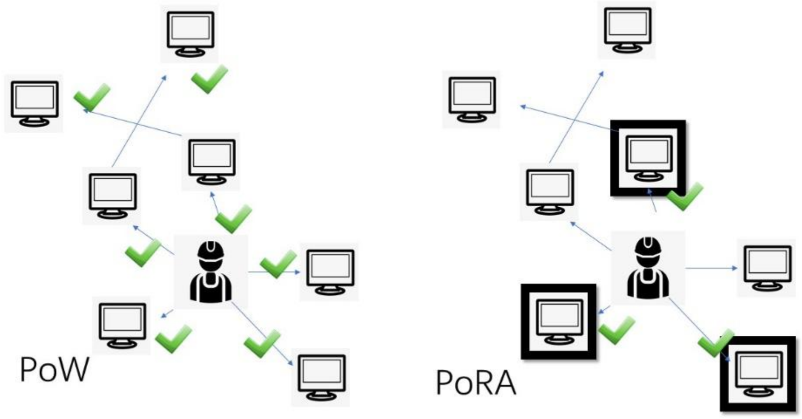


Fig. 27 PoRA vs PoW

Compared with PoW and PoS, PoRA proposed by the article may seem to loss the property of decentration of a blockchain system since the voting result in a period is not verified by every voter but a part of them, but the randomness does compensate the loss. However, the computation power for operating PoRA is less than that for running PoW and PoS because PoRA is not dense and the time cost for PoRA is less as well. From this point of view, PoRA finds a balance between decentration and computation efficiency and it simplifies the conventional blockchain system.

Besides, the time interval and difficulty adjusting based daily electric load technique, used to design the blockchain election system for task 1, can make the cost to run a blockchain election system lower without doing harm to the security.

6.3 FORK-256 for Better Security

To improve the security of blockchain election technology, some new hash function may be adopted. A function named FORK-256 is introduced in [26] in order to defense against any known attacks on hash functions. Like SHA-256, FORK-256 also has a 256-bit output by inputting a word but it is generated by four parallel branches, which can be implemented in hardware but difficult to analyze the branches simultaneously. With the hardware advancing and computation power increasing, SHA-512 and FORK-512 will launch in the coming future.

VII. Conclusions

Although BEV system has drawbacks, it still has a tendency to develop and enhance despite many disputes. Varying from the traditional remote e-voting system, the e-voting system based on blockchain is similar to a decentralized distributed database managed by the whole network, which could eliminate the fraud by the third-party authority. Besides, due to its inherent property of anonymity and transparency, it is widely deployed in soaring numbers of voting protocols.

The design proposed by the present paper almost solve the risk of reliance on the so-call trusted third-party authority. Even if there are still tallying organizations to do the statistic work, it is impractical to practice fraud because every node on the network owns a copy of the transparent and open blockchain.

While there is still some problem like energy consuming and wastes of computing power, the article there come up with some useful techniques that might help to solve it. Moreover, there are some novel idea such as the difficulty modifying strategy and PoRA consensus algorithm, which could be taken into practice after adequate theoretical tests.

All above, there are still plenty of room left for enhancement and improvement for BEV system, undoubtedly, it will be the mainstream technique in remote e-voting system in the future.

VIII. Future Work

8.1 The limitations of the current e-voting systems

Most of the e-voting systems that employ blockchain technology to conduct online voting rely on trusted third-party to perform the auditing and managing duties during the election. For example, in 2016, Lee, James, Ejeta and Kim et al [22]. turn to a third-party in the BEV system to protect the ballots of voters. In 2017, Cruz et.al.[23]. came up with a BEV system applying blind signature technique, which also introduced a third-party counting mechanism to count the voting results.

However, no one cannot exclude the possibility of the third-party counting institutions and the managers to attack the system, which results in the tampering of voting results, or the possibility that counting institutions leaked the voting results in advance to control the change of the entire voting results. In addition, the restriction of the storage of bitcoin transactions also makes the existing BEV systems imperfect.

8.2 The Smart contract in e-voting system

Smart contract, consisting of self-verification and automatic execution of contract terms, is a computer transaction protocol without intermediary, based on distributed architecture and consensus algorithm in blockchain technology, smart contract allows population without trust to complete transactions bypassing any third-party intermediary or authority. The emergence of Ethereum (a smart contract development platform) has changed the application pattern of blockchain and smart contract, making it no longer limited to digital currency, and starting to have the opportunity to build a broader financial system and apply it to other social fields.

The smart contract has the characteristics of protecting the privacy of voters and can realize self-counting when used in online voting systems. General process can be simplified as: Voting promoters verify the voters through the smart contract qualification, only those who have passed the certification can be included in the voting protocol. During the voting process, smart contracts automatically submit encrypted votes to the blockchain. When the vote is completed, the voting promoter notifies the smart contract to enter the counting stage (the method of counting the votes written in the intelligent contract is invoked, without any third-party participation). Finally, the statistical results corresponding to each candidate are published in the whole system and can be verified by anyone.

The smart contract on the blockchain can realize a voting scheme with self-counting function. In addition to the fact that there is no participation of third-party counting institution, it can also achieve the characteristics of public verifiability and data tamper-proof during the voting process. In the future, there will be considerable space for smart contract to develop.

VI. References

[1] Benaloh J , Fischer M J . A Robust and Verifiable Cryptographically Secure Election Scheme[C]// Symposium on Foundations of Computer Science. IEEE, 1985.

[2] Xenakis A , Macintosh A . Trust Analysis of the U.K. e-Voting Pilots[M]. Sage Publications, Inc. 2005.

[3] Brewer P R , Sigelman L . Trust in Government: Personal Ties that Bind?[J]. Social Science Quarterly, 2002, 83(2):624-631.

[4] Zhang, S. , Wang, L. , & Xiong, H. . (2019). Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. *International Journal of Information Security*(2).

[5] Jianshe, Z. , Peng, S. , & Qing, W. U. . (2008). Research on data information indexing and searching algorithm based on DHT. *Computer Engineering & Applications*, 44(31), 159-163.

[6] Nakamoto S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[7] Pieters, G. C. , & Koch, C. . (2017). Blockchain technology disrupting traditional records systems. *Economic review (Federal Reserve Bank of Dallas)*, 6(2), 1-3.

[8] Huang, Z., Lv. K., & Li, H.. (2017). *Learn the blockchain from scratch: Digital currency and new pattern of Internet finance*. Qinghua University Press.

[9] Whitfield Diffie, & Martin E. Hellman. (1976). Multiuser cryptographic techniques. American Federation of Information Processing Societies: 1976 National Computer Conference, 7-10 June 1976, New York, NY, USA. ACM.

[10] Surhone, L. M. , Tennoe, M. T. , Henssonow, S. F. , & Transform, A. O. N. . (2010). Elliptic curve cryptography. *Ubiquity, 2008*(May), 1-8.

[11] Selvakumar, A. L. , & Ganadhas, C. S. . (2009). The Evaluation Report of SHA-256 Crypt Analysis Hash Function. *International Conference on Communication Software & Networks*. IEEE.

[12] He R.M., & Ma J.. (2014). Sha-256 Algorithm security analysis. *Electronic Design Engineering*,22(03), 31-33.

[13] Jakobsson, M. , & Juels, A. . (1999). Proofs of Work and Bread Pudding Protocols. *Secure Information Networks: Communications and Multimedia Security, IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS '99), September 20-21, 1999, Leuven, Belgium.* Kluwer, B.V.

[14] Du. J. (2018). Discussion On Hasche Algorithm in block chain proof-of-work system mechanism. *Computer programming skills and maintenance*(4), 40-42.

[15] Paul, D. , & Petitcolas, F. A. P. . (2018). A first look at identity management schemes on the blockchain. *IEEE Security & Privacy, 16*(4), 20-29.

[16] Heiberg, S., Kubjas, I., Siim, J., Willemson, J. (2018). On trade-offs of applying block chains for electronic voting bulletin boards. *E-Vote-ID* 2018, p. 259

[17] Chaieb, M. , Yousfi, S. , Lafourcade, P. , & Robbana, R. . (2018).

Verify-your-vote: a verifiable blockchain-based online voting protocol.

[18] Mccorry, P. , Shahandashti, S. F. , & Hao, F. . (2017). A Smart Contract for Boardroom Voting with Maximum Voter Privacy. *Financial Cryptography and Data Security. Springer*, Cham.

[19] Ye. Z. Z, Pan. J, Zhao. Y. H. et.al. (2019) *ANNUAL REPORT ON CHIAN'S BLOCKCHAIN APPLICATION AND DEVELOPMENT*. Social Sciences Academic Press. No.1

[20] Ryan, P. Y., Bismark, D., Heather, J., Schneider, S., Xia, Z(2009).: Prêt à voter: a voter-verifiable voting system. *IEEE Trans. Inf. Forensics Secur. 4*(4), 662–673.

[21] Tan. S. B. (2019) *Ethereum Development Practice of Smart Contract. China Machine Press*. No.4

[22] Lee K,James J I,Ejeta T G,et al. (2016). Electronic Voting Service Using Blockchain.*The Journal of Digital Forensics,Security and Law:JDFSL*,11(02):123.

[23] Jason P. C, Yuichi K. (2017) E-voting System Based on the Bitcoin Protocol and Blind Signatures. *Transactions on Mathematical Modeling and Its Applications*,10(01):14-22.

[24] Xu M.X. Yuan C. Wang Y.J. et.al.(2009)Mimic blockchain--Solution to the security of blockchain. Journal of Software,30(6)

[25] Si X.M. Wang W. Zeng J.J. et.al. (2017). A review of the basic theory of mimic defense. *Strategic Study of CAE, 18*(6) :62—68

[26] Selvakumar, A. L. , & Ganadhas, C. S. . (2009). The Evaluation Report of SHA-256 Crypt Analysis Hash Function. *International Conference on Communication Software & Networks. IEEE.*

Appendix

7.1 The Principle of ECC[8,10]

In order to define a specify elliptic curve field, we should define the following six parameters:

T = (p, a, b, G, n, h)

p : represents prime number of finite field F_p

a, b: the parameters of elliptic equation.

G: an arbitary base point in elliptic equation $G = (x_G, y_G)$

n: a prime number. the position of the base point G in the elliptic equation.

h: a cofactor which controls the dense of the selected points.

$$h = \frac{total\, number\, of\, points\, in\, the\, elliptic\, equation}{n}$$

Take the SECP256K1 for example, the value of all the parameters are as follow:

p = $2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$

a = 0, b=7

G=0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F28

15B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8(G=0279BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798 when compressed)

n=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141

h = 01

The detail of encrypting process is as follow:

1. Client A selects a elliptic curve E(a, b), then select a base point on the elliptic curve.
2. Select an arbitrary point k on the curve also, where k a is integer less then n. And regard k as the private key of A. One can find a point Q which satisfies the equation: Q=k*G and take it as public key.
3. Client A conveys the point E(a, b) and K, G to the client B.
4. Client B receives the information such as public key from A, and then encode the plaintext to the elliptic curve as a point M, and generating a random integer r.
5. Client B computes points : C_1= M+rK; $C_2 = rG$
6. Client B conveys the points C_1, C_2 to A
7. A computes the results $C_1 - kC_2$ once receiving the information

$$C_1 - kC_2 = M + rK - k(rG) = M + rK - r(kG) = M$$

Then, decrypting the point M again to gain the plaintext and the encrypted communication process is fulfilled.

If there are sniffers intercept the message between A and B, they can only gain the point E(a, b), K, G, C_1, C_2. But they are unable to derive k or r from the above information. Thus they have no way of learning the plain text between A and B. The process is described as Fig.

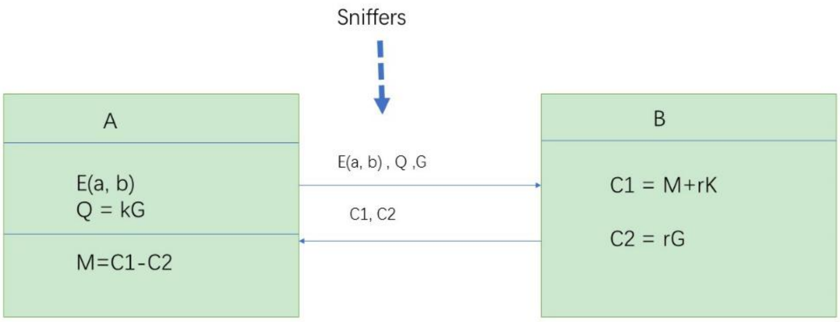


Fig. 28 The secrecy process of Elliptic Curve Schematic diagram