Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 129 (2018) 234–237

Procedia Computer Science

www.elsevier.com/locate/procedia

2017 International Conference on Identification, Information and Knowledge in the Internet of Things

Large-scale Election Based On Blockchain

Baocheng Wang[a,*], Jiawei Sun[a], Yunhua He[a], Dandan Pang[a], Ningxiao Lu[a]

[a]*North China University Of Technology, No.5 Jinyuanzhuang Road, Shijingshan District Beijing, Beijing 100144 , China*

Abstract

Based on the blockchain, homomorphic ElGamal encryption and ring signature, an electronic voting scheme based on blockchain is proposed for large-scale voting, which has the properties of decentralization, self-management, non-interactive and free-receipt, furthermore the one-time ring signature ensures the anonymity of the vote trading in the blockchain. The public verifiable billboards guarantee the voting fair, and the miner nodes provides ciphertext ballot counting service makes large-scale voting feasible. Finally, we analysis the security of the blockchain voting system and present the performance in large-scale nodes.

Selection and peer-review under responsibility of the scientific committee of the 2017 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI2017).

Keywords: blockchain, electronic voting, large-scale voting, ring signature;

1. Introduction

As an increasing number of votes appear in the real life, people are aware of the importance of electoral system gradually. At present, most schemes are centralized (including voting schemes based on the mix-net, blind signature FOO and homomorphic encryption technology), these schemes are recorded, managed, calculated and checked by the central agency. However, it is necessary to assume that there is a credible bulletin board and the corresponding credible counting agencies. The single central institutions and intensive data cause the vulnerability of the electronic voting security.

Recently, the distributed electronic voting scheme based on blockchain is a hot spot of the research. There are already some blockchain-based voting systems or schemes. But most of them just use blockchain as storage media for voting data, and only apply to small-scale voting, and public key address scheme in the original bitcoin program is simply used in the user privacy protection. By means of some social engineering methods, it is possible that the physical address of a bitcoin currency wallet is exposed; accompanied by big data analysis, the anonymity and no receipt is difficult to guarantee.

* Baocheng Wang. Tel.: +0-108-880-1530 ; fax: +0-108-880-1530.
E-mail address: wbaocheng@ncut.edu.cn

Selection and peer-review under responsibility of the scientific committee of the 2017 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI2017).
10.1016/j.procs.2018.03.063

Considering above problems, this paper proposed a free-receipt electronic voting scheme based on blockchain. In this scheme, the management node publishes the smart voting contract in the blockchain and uses it to accomplish the recording, management, calculation and inspection. Through the transaction ballot, voter nodes transfer and record the ballot ticket by means of the blockchain; Using the computing ability of the miner node as the support of multipartite secure calculation to ensure the feasibility of large-scale voting; One-time ring signature and homomorphic encryption protect the privacy and free-receipt of voters. Blockchain greatly increases the transparency between the public and the government, and anyone could see what is happening in the chain. In contrast, the blockchain system is more overt and transparent. This method not only guarantees the anonymity and verifiability of the electronic voting scheme, but also ensures the distributed credibility of the blockchain. As the contract-operated voting program, it is capable of the features of decentralization, self-management and self-running.The contributions are listed as follows:

- We proposed the electronic voting based on blockchain to apply for large-scale voting circumstances.
- We intensified the privacy protection of voting schemes based on the architecture of blockchain.

2. The blockchain based electronic voting scheme

2.1. Consensus algorithm

Based on Ethereum architecture, we post the voting task through smart contract. Because of the need to support large-scale elections, the mechanism of original network consensus is not appropriate for large-scale voting. The consensus algorithm should be an effective method to ensure the consistency of data in the distributed computing system.

As the POW workload consumes too much energy, causes a vast of waste of resources, leading to mining center and slow transaction. DPOS can significantly reduce the number of participating in verification and billing nodes to accelerate the transaction speed. Therefore DPOS is applied for high-demanded public chain similar to the election chain , and the confirmation time of transaction is very fast.

For large-scale voting, the workload of the cryptographic calculation is also large, so the miner nodes designed in the scheme not only need to complete the accounting work through the DPOS consensus, but also require to use the calculation of the miners to ensure the support of large-scale elections. Moreover, the system stimulates its electronic money through the workload of miner nodes.

2.2. The procedure of voting

The voting scheme consists of the following stages (**Setup, Register, Vote, Valid, Append, Publish, VerifyVote**). The smart contract is created by the electoral administrator in the blockchain. Randomized nodes and miner nodes are registered in smart contracts.

- **Setup**$(1^\lambda, 1^k)$**:**
  The security parameters are input as 1^λ,1^k,the private/public key pair to encrypt and decrypt is calculated as $(pk, sk) \xleftarrow{\$} EKeyGen^{(x)}(1^\lambda, 1^k)$, then Fiat-Shamir zero knowledge proof is generated,and return $(pk^* = (pk, \Pi_\sigma), sk)$
- **Register(***id***):**
  The identify logo and pk are iuput as id and $pk = (pp, crs, h, P)$ respectively, and the private/public key is output as $(usk_{id}, upk_{id}) \xleftarrow{\$} SKeyGen(pp)$.
- **Vote(***id*, *upk*, *usk*, *v***):**
  Voters create voters v, calculate the ciphertext $c \leftarrow Encrypt_+(pk, upk, v)$ and the corresponding signature $\sigma \leftarrow Sign_+(usk, pk, c)$, and returns $b = (id, upk, c, \sigma)$.
- **Valid(***BB*, *b***):**
  First of all, we need to verify the validity of the ballot in the ballot box BB (voting server) to select the ballot as input and confirm the legitimacy of the ballot (such as protocol format and signature correctness). After verification, verification result $\perp$ or $\top$ is returned.

- **Append:**
  Vote b = (id, upk, c, σ) is randomized and then updated(c, σ) to the ballot box $BB(C', \sigma') \leftarrow b' = Random_+(upk, pk, c, \sigma)$ and appends to BB a randomized version $b' = (id, upk, c', \sigma')ofb$
- **Publish(BB):**
  For each vote $b = (id, upk, c, \sigma)$, the corresponding $id, c_3, C_T, \pi_T and \pi_v$ are removed, and $\hat{b} = (upk, (c_1, c_2, C_m, C_r, \pi_r, \pi_m), (\sigma_1, \sigma_2, \sigma_3, \sigma_4))$ is built. Then b^* is added to the polling box in the public view PBB, and returns PBB.
- **VerifyVote:**
  After the voting stage, the voters could inquiry their own votes in the smart contract during the voting publicity period, and verify the return results by entering the polling box public view PBB, ballot b, voter status and privacy information id, usk, upk. For entry $\hat{b} := (upk = (pp, X_1, X_2), (c_1, c_2, C_m, C_r, \pi_r, \pi_m), (\sigma_1, \sigma_2, \sigma_3, \sigma_4)))$
  If π_r, π_m are valid and below could hold.
  $e(\sigma_1, g_2) = e(c_1, \sigma_4)e(\sigma_2, g_2) = e(z, X_2) \cdot e(c_2, \sigma_4)$
  $e(\sigma_1, g_2) = e(c_1, \sigma_4)$
  Then return $\perp$, otherwise return $\top$.
- **Tally:**
  We enter the voting box BB and the private key sk, output the counting result r and the corresponding publicity proof result $TAB2$, and return the election verification result. If the election result is invalid, the counting result should be $FALSE(r := \perp)$.
- **Verify:**
  Π_d is proved by the input of the public polling box view in the publicity stage PBB, the count result r and result. And it is verified to be a valid and correct voting result. verifies Π_σ w.r.t. crs and Π_d w.r.t.PBB and result r.

3. Anonymous voting scheme

All transactions among the participants in the blockchain are publicly visible, and any transaction can be traced back to a unique origin and the final recipient. But as for the voting system, it is necessary to ensure its anonymity, that is, the voter status corresponding to the votes is anonymous.To solve this problem, this paper use a one-time ring signature technique [8] to protect the anonymity in the voting scheme based on the blockchain. Unlinkable signature is used to protect the receiver of transactionanonymity, while ring signature could help keep the anonymity of sender.

3.1. Un-linkable signatures

A solution in the literature [9] allows the user to publish an address which not traded by multiple transactions. By default, the target of each transaction output is a public key that derives from random data from the recipient address and senders random data. The main advantage against bitcoin addresses is that each recipient address is unique (unless each time the sender uses the same random number for the same recipient). Thus, there is no problem to design the 'address reuse', and no observer can determine whether the transactions are sent to a particular address or two addresses are associated.

3.2. Ring signature

The ring signature is a special group signature, there is no trusting center, no group establishment process. For the verifier, the signer is completely anonymous. The name reflects its unique ring structure, the real signer generates a ring with a fracture using the public key produced by other possible signers, and connects the fracture to form a complete ring with his own private key. Any verifiercan verify who generates the ring signature by the public key of the ring member. According to the result of the calculation, the validity of the signature is judged, and then the signature will be accepted or rejected.The one-time ring signature contains four algorithms: (**GEN, SIG, VER, LNK**)

- **GEN**: Getting public parameters and output key pair (P, x) and public key index I.
- **SIG**: For message m, using a set s' of public keys $P_{i(is)}$, a pair (P_s, x_s) and outputs a signature σ and a set of $S = S' \bigcup \{P_s\}$.

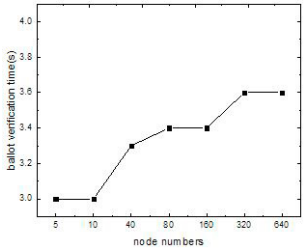

Fig. 1. Cost time in different node number

Table 1. cost time in different number of candidate

Number of candidates	CPU I7	CPU I3
K=1	1s	1.49s
K=5	2.43s	3.46s
K=10	4.02s	5.92s
K=25	9.24s	13.62s

- **VER**: takes a message m, the set S, the signature σ and output the extension result "true" or "false".
- **LNK**: Using $I = \{I_i\}$, a signature σ to verify whether the ring signature has been used or not, and outputs "linked" or "indep".

4. Experiment

Since relatively sophisticated cryptographic calculations are used in the voting scheme, especially the Groth-Sahai non-interactive zero-knowledge proof. For the homomorphic counting ballot, when $k = 1$, 5, 10 and 25, the time consumption of a single node is counted. As shown in the table 1, when k is small, the cryptographic calculation required for voting can be accomplished by a single node within a reasonable time.

As shown in the figure 4, the time of ballot verification time is in a acceptable time while the number of voter node increases. On the smart contract, a large number of randomized work and counting work are assigned to all miner nodes, the network of computing resources are rationally used, thus handling large-scale electoral voting work.

5. Conclusion

Based on smart contract, one-time ring signature and homomorphic encryption this paper proposed a non-interactive and non-receipt electronic voting method. The smart contract is used to accomplish recording, managing, calculating and checking during the voting work; In order to protect the privacy of electronic voting scheme, ring signature is employed to ensure that the registration and voting is anonymous; For large-scale voting in the blockchain, we use DPOS for distributed consensus and miners node to randomize the votes and count the ballots.

References

[1] Adida, Ben (2008) "Helios: Web-based Open-Audit Voting." *USENIX security symposium* **17**: 335-348.
[2] Adida, Ben and De Marneffe, Olivier and Pereira, Olivier and Quisquater, Jean-Jacques and others (2009) "Electing a university president using open-audit voting: Analysis of real-world use of Helios." *EVT/WOTE* **9** (10).
[3] Cortier, Véronique and Galindo, David and Glondu, Stéphane and Izabachene, Malika (2014) "Election verifiability for Helios under weaker trust assumptions." *European Symposium on Research in Computer Security* : 327-344.
[4] Chaidos, Pyrros and Cortier, Véronique and Fuchsbauer, Georg and Galindo, David (2013) "BeleniosRF: A non-interactive receipt-free electronic voting scheme." *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* : 1614-1625.
[5] Cortier, Véronique and Smyth, Ben (2013) "Attacking and fixing Helios: An analysis of ballot secrecy." *Journal of Computer Security* **21** (1): 89-148.
[6] Fuchsbauer, Georg and Pointcheval, David (2009) "Proofs on Encrypted Values in Bilinear Groups and an Application to Anonymity of Signatures." *Pairing* **5671** 132–149.
[7] McCorry, Patrick and Shahandashti, Siamak F and Hao, Feng (2017) "A Smart Contract for Boardroom Voting with Maximum Voter Privacy." *Theoretical Computer Science* 110.
[8] RL Rivest, A Shamir, Y Tauman (2006) "How to Leak a Secret: Theory and Applications of Ring Signatures." *Theoretical Computer Science* **22** (11): 164-186.
[9] Chaum, David L. (1981) "Untraceable electronic mail, return addresses, and digital pseudonyms." *Communications of the ACM* **24** (2): 84–90.
[10] J Groth, A Sahai. (2008) "Efficient Non-interactive Proof Systems for Bilinear Groups." *EUROCRYPT 2008* **41** (5): 415-432.