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.