International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

A Decentralized E-Voting System Based on Blockchain Network

Hee-Dong Park

Abstract: ***This paper describes a decentralized electronic voting system using blockchain technology with peer-to-peer network rather than the centralized voting system of server-client structure. In the proposed system, an Ethereum-based private blockchain network is configured and decentralized applications are implemented to store and distribute voting data to all nodes participating in the network to create secure and reliable electronic voting system. Smart contracts for electronic voting are implemented using the Solidity language and distributed to a configured network so that all users can view and vote on elections, and voting data are shared and contrasted by all users in the network, which makes it possible to build a safer and more reliable electronic voting system without third party involvement.***

Index Terms**: electronic voting system, blockchain, peer-to-peer network, Ethereum, decentralized applications.**

I. INTRODUCTION

Electronic voting refers to a method of voting with quick counting and high accuracy, using electronic technologies such as the Internet and mobile to replace traditional paper voting methods [1, 2]. However, voters are nervous about security issues. Security issues of electronic voting systems include the vulnerability to the safety of the Internet itself and the possibility of election fraud, especially when it comes to serious concerns about safety, such as hackers invading websites or spreading computer viruses [3].

In order to overcome these problems, server-free and non-centralized blockchain-based electronic voting systems are being introduced [4-7]. Blockchain-based electronic voting systems are employed basically with peer-to-peer (P2P) networks rather than server-client structure of existing electronic voting systems. Blockchain technology has a distributed database where all users share data and directly update data without a central server. Storing voting data in a block reduces the likelihood of data loss by sharing the data block with all users in the network, summarizing the data record through the hash function, and using the hash function as the input value. The next block contains the hash value, which makes it difficult to forge and falsify the voting value.

This paper proposes a de-centralized electronic voting system based on a blockchain network using Ethereum platform, rather than the server-client method of conventional electronic voting systems.

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author
Hee-Dong Park*, Associate Professor, School of IT Convergence, Korea Nazarene University/ Cheonan-city, Korea.

II. RELATED WORK

Blockchain is a computing technology-based data forgery and alteration prevention technology that stores chain-type blocks in which small-scale data called 'block' are managed based on P2P methods in a distributed data storage environment. It is called public ledger or distributed ledger. All participants in the blockchain network jointly verify, record and archive transaction information to ensure the integrity and reliability of transaction records without an authorized third party.

The block consists of six pieces of information: version, previousHash, merkleHash, timestemp, difficulty, and nonce. The block hash, which serves as an identifier of each block, is calculated by applying the SHA256 hash function as the input information. Each block is chained together by including the hash value of the previous block.

A. Blockchain Consensus Algorithm

PoW (Proof of work) is a consensus algorithm adopted by many blockchain-based technologies, starting with Bitcoin [8]. After creating and distributing a block, it defines what is used by many participants as the correct block, so it can increase the number of participants without affecting the number of participants. On the other hand, if there are inconsistencies in some parts of the network, the result can be uncertain or the performance is not guaranteed.

PoS (Proof of Stake) is an algorithm adopted by Ethereum [9]. It is characteristic that an authorized person who owns more money can create a block first. It is based on the premise that “Participants who own a large currency will not lose the credibility of the system in order to protect its value.” The basic structure is not different from PoW, but the difficulty of calculating the hash depends on the amount of money, which has the advantage of lower resource consumption compared to PoW.

PBFT (Practical Byzantine Fault Tolerance) solves the uncertainty and performance issues of PoW and PoS [10]. Unlike PoW or PoS, blockchain branches are not created because they are made by majority decision making and block making. As a result, the blocks that are determined once will not be changed, so you can get the final results. And it works very fast because you don't have to repeat the calculation until you meet the conditions, like PoW.

B. Ethereum Platform

Ethereum Platform is a distributed computing platform for implementing smart contract functions based on blockchain technology [9].

Ethereum platform provides scalability to operate various applications besides decentralized trading and settlement. That is, it can be used not only as crypto currency but also for various purposes.

An application for blockchain-based distributed data technology, in which all participants share data in the blockchain network, is called a decentralized application or a DApp. It supports various programming languages such as C ++, JAVA, Python, and Go languages.

Ethereum networks can be classified into two types: live network and test network. Live networks are open networks with nodes (participants) from all over the world. Anyone can join and access the blockchain and send transactions. The test network is a network for testing. It is a private network, where only one node or a limited number of nodes can join. It is often used to implement decentralized applications.

C. Smart Contract

Smart contracts refer to various types of blockchain-based contracts, such as financial transactions, contracts and notaries [3]. Developers can code the contract terms and contents directly, and in principle, all kinds of contracts can be implemented using the Ethereum platform.

Smart contracts on the Ethereum platform are implemented with the Solidity language, a Java-based independent language. Solidity is a language similar to JavaScript and is currently the most commonly used language for implementing contracts on Ethereum. The created smart contract is distributed to the blockchain network by the Ethereum Virtual Machine (EVM) compiler and stored in the block as EVM bytecode. Since all participants in the blockchain network have the same block, they can share the contract while holding and executing the EVM bytecode.

III. THE PROPOSED E-VOTING SYSTEM

The proposed e-voting system uses Ethereum platform and a semi-permissioned blockchain, which discloses information about validators to establish legal grounds and guaranties anonymity of voters. Thus, voters can participate autonomously, but the validator nodes need to be identified in advance to participate in blockchain networks.

A. Smart Contract for E-Voting

The proposed system creates a smart contract for electronic voting using Solidity language as shown in Fig. 1. The contract details define the election title, subtitle, voting start and end dates, and a structure to store information about candidates running for that election. The structure consists of the candidate's identification value (ID), name (candidateName), capture (candidatePledge), and votecount (voteCount).

When voting is performed, the blockchain network participant's account address is used as a key value, and whether the vote is participated in (true) or not (false) is stored. The proposed e-voting system prevents re-voting from occurring in the accounts that have already participated by using account address as a parameter of mapping function of Solidity language.

```
pragma solidity ^0.4.2;

contract Election {
    string public electionMainTitle;
    string public electionSubTitle;
    string public electionStartDay;
    string public electionEndDay;
    uint public votersTotalCount;

    struct Candidate {
        uint candidateId;
        string candidateName;
        string candidatePledge;
        uint voteCount;
    }

    uint public candidatesCount;
    uint public votersCount;
    mapping(address => bool) public voters;
    mapping(uint => Candidate) public candidates;


    function addCandidate( string _candidateName, string _candidatePledge ) {
        candidatesCount++;
        candidates[candidatesCount].candidateId = candidatesCount;
        candidates[candidatesCount].candidateName = _candidateName;
        candidates[candidatesCount].candidatePledge = _candidatePledge;
    }

    function addElection( string _electionMainTitle, string _electionSubTitle, string _electionStartDay, string _electionEndDay) {
        electionMainTitle = _electionMainTitle;
        electionSubTitle = _electionSubTitle;
        electionStartDay = _electionStartDay;
        electionEndDay = _electionEndDay;
        votersTotalCount = 0;
    }

    function getCandidate(uint i) public constant returns( uint, string, string, uint ) {
          return (candidates[i].candidateId, candidates[i].candidateName, candidates[i].candidatePledge, candidates[i].voteCount);
    }

    function castVote( uint _candidateId ) public  {
        require(!voters[msg.sender]);
        require(_candidateId > 0 && _candidateId <= candidatesCount);

        votersTotalCount++;

        voters[msg.sender] = true;

        candidates[_candidateId].voteCount++;
    }
}
```

Fig. 1. Smart contract for the proposed e-voting system.

B. Configuration of Blockchain Network

To implement the decentralized application for electronic voting using blockchain technology, the proposed system configures a private network, a test network of the Ethereum network.

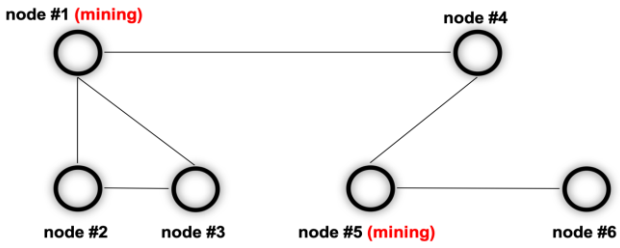

Fig. 2. Configuration of the proposed blockchain network.

Fig. 2 shows the configuration of the proposed private blockchain network for electronic voting. In order to use a private network, the proposed system runs one node (node #1) by using Geth (Go-Ethereum) and distribute the e-voting smart contract, while registering the election contents (title, subhead, candidate, start date, end date). In the same way, there are six nodes running in the network and they are divided into two categories for mining and voting. Node #1 and #5 are for mining and the others (node #2, #3, #4, #6) includes accounts of voters. The 6 nodes shares blocks and contracts created by miners.

As shown in the Fig. 3, node #1 and #5 collects transaction data originating from other nodes, create a new block, and propagate it to each participating node of the blockchain network

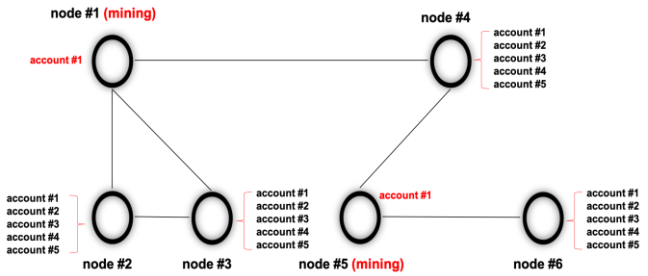

Fig. 3. Data block creation and propagation.

C. Decentralized Application

The proposed system provides a decentralized application using web3.js. The application confirms the voting contents and provides web pages to check the voting participation, the aggregate status, and the voting results. It can distinguish ongoing and closed votes by comparing the start and end dates of the votes with the current time. In case of ongoing votes, the application pages provide information of vote participation and counting status. On the other hand, in case of closed votes, the application only provides information of voting results.

IV. IMPLEMENTATION AND VERIFICATION

The proposed e-voting system is implemented to verify operation. Voting data of voters who participated in the voting are stored in blocks created by node # 1 and node # 5 (shown in Fig. 2), which are miners who collect data records and create new blocks. The voting data blocks are linked with previous blocks to form a block structure. All nodes participating in the network store the same block data.

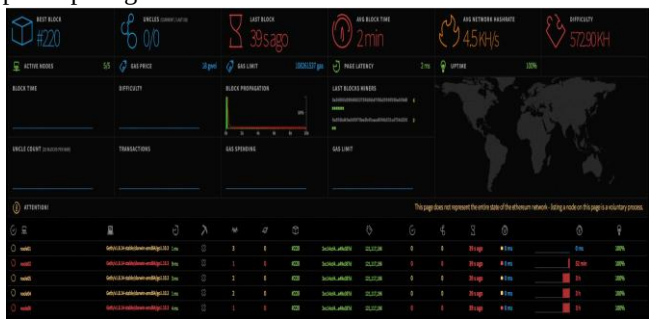

Fig. 4. Block information of a node participating in the proposed block chain network.

Fig. 4 shows block information of a node participating in the implemented blockchain network. After participating in the network through a P2P connection with an existing node, the newly added node was also able to take part in the vote and see the results of the vote. In addition, even after disconnecting the intermediate node and connecting with other nodes, the voters' accounts that already participated could not be re-voted, and the same voting data could be confirmed by propagating the blocks shared by the existing nodes.

V. CONCLUSION

This paper proposes and implements a decentralized electronic voting system based on P2P blockchain network without a central server to overcome the shortcomings of the existing server-client based electronic voting system. Through the proposed e-voting system, all voters can store and share the voting data. The proposed system could reduce the likelihood of vote data manipulation through distributed storage and management and comparison and confrontation. Implement results show that the proposed e-voting system operates very well.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(2017R1D1A3B06035024). This research was also supported by Korea Nazarene University Research Grants.

REFERENCES

1. Nir Kshetri, Jeffrey Voas, “Blockchain-Enabled E-Voting,” *IEEE Software*, Vol. 35, Issue 4, 2018.
2. https://steemit.com/blockchain-voting/@swu/4qkhpj.
3. F. Ciazzo and M. Chow, “A Blockchain Implemented Voting System,” Dec. 2016.
4. Friorik P. Hjalmarsson, Gunnlaugur K. Hreioarsson, Mohammad Hamdaqa, Gisli Hjalmtysson, “Blockchain-Based E-Voting System,” *IEEE 11 international Conference on Cloud Computing (CLOUD)*, July 2018.
5. Emanuele Bellini, Paolo Ceravolo, Ernesto Damiani, “Blockchain-Based E-Vote-as-a-Service,” *IEEE International Conference on Cloud Computing (CLOUD)*, July 2019.
6. S. Han, M. Bae, G. Hwang, “Development of Electronic Voting System Based on Blockchain using Homomorphic Encryption,” *The Journal of Korean Institute of Communications and Information Sciences*, Vol. 44, no 1, Jan. 2019.
7. David Khoury, Elie F. Kfoury, Ali Kassem, Hamza Harb, “Decentralized Voting Platform Based on Ethereum Blockchain,” *IEEE International Multidisciplinary Conference on Engineering Technology* (IMCET), Nov. 2018.
8. Satoshi Nakamoto, “Bitcoin: A Peer-to-peer Electronic Cash System,” 2018.
9. Go Ethereum, https://geth.ethereum.org/.
10. Miguel Castro, Barbara Liskov, “Practical Byzantine Fault Tolerance,” *Proceedings of the Third Symposium on Operating Systems Design and Implementation*,” Feb. 1999.