Design of Blockchain based e-Voting System for Vote Requirements

Design of Blockchain based e-Voting System for Vote Requirements

Seiwoong Choi [1], Jihun Kang [2] and Kwang Sik Chung [3, *]

[1] Graduate School, Dept. of Information Science, Korea National Open University, Jongno-gu, Dongsung-Dong, Seoul, Republic of Korea
[2] BK 21 Data-Driven Science Future Talent Education Research Group, Dept of Computer Science and Engineering, Korea University, Seoul, Republic of Korea
[3] Dept. Of Computer Science, Korea National Open University, Jongno-gu, Dongsung-Dong, Seoul, Republic of Korea

E-mail: *kchung0825@knou.ac.kr

Abstract. Voting refers to the submission of an election or an opinion on a specific matter by expressing an intention on the ballot to a certain place. The existing voting method has the burden of counting time and cost. For this reason, research has been conducted to introduce an e-voting system. However, despite the advantages of e-voting, it is not widely used due to the risk of manipulation of voting results and various requirements. Recently, in order to reduce the risk of data manipulation, research is being conducted to apply the blockchain, a technology that guarantees data integrity, to e-voting. Blockchain guarantees the integrity of data, but has a weakness in secrecy. This paper applies the critical encryption technique to the blockchain and satisfies the requirements for voting such as verifiability, anonymity, fairness, non-reusability, competence, safety, transparency, and non-ticketing. We propose a system design and implementation method. The proposed blockchain-based e-voting system provides voter anonymity by issuing a voter certificate based on a blockchain address. The e-voting election monitoring committee generates a threshold group encryption key, and the proposed blockchain-based e-voting system guarantees confidentiality by a threshold group encryption algorithm during the voting process. The voting result is encrypted through a homomorphic encryption algorithm and stored in the blockchain. Thus, the released voting results ensure safety, confidentiality, transparency, and non-vote ticketing. In addition, the proposed blockchain-based e-voting system guarantees the unity and competence of voting through the blockchain's smart contract.

1. Introduction

E-voting should be non-changeable, verifiable, and to ensure reliability, provide full transparency to all procedures. Security and safety should be provided through cryptographic algorithms. The blockchain features the user's invariability and verifiability. The characteristics of the blockchain mean that it is used in a variety of areas [1]. These features provide completeness, unity, and verifiability for e-voting, but are vulnerable to secrecy, in that the ledger can be shared by all. Widespread research to apply the blockchain to e-voting is ongoing. However, more research is needed, as no method has yet been proposed that satisfies all of the various requirements of e-voting. In this study, we propose and implement an e-voting system that satisfies the various requirements of voting by applying a blockchain

to e-voting, to provide verifiability and reliability. We introduce various cryptographic algorithms, and thereby verify the proposed system, and present future research directions.

Voting means submitting a ballot to a certain place by expressing one's intention in an election, or deciding on a political opinion. Elections are the essential means of voter participation in politics, as the most essential system for the governance order of modern representative democracies [2]. E-voting systems are under way with the aim of reducing election management costs and increasing voter participation through increased voting convenience. About 40 countries hold e-voting in public officer elections [3]. In the United States, e-voting was held in 2000 in the Democratic primaries in Arizona. In the United Kingdom, e-voting was held in local elections in 2000, such as Burly and Salford. In Japan, e-voting was introduced for the first time in 2002 in the local elections in Okayama [4]. In the case of Korea, the Korea Public Official Election Act in 2005 provided legal grounds for the establishment of an 'Electronic Election Promotion Council' and 'E-voting Test Execution', and in 2005 began the project to establish a pilot system for touch-screen voting [5]. The Korea National Election Commission has established and is operating an online voting system. E-voting was expected to increase representation, including increased voter turnout and reduced invalid votes, along with economic benefits, such as reduced election costs and ballot counting time [6]. Despite its many advantages, the e-voting system has not spread widely because of citizens' trust issues, secret voting issues, security issues, technological proliferation, and problems with voters' ability to use e-voting devices [4].

The remainder of the paper is structured as follows: Section 2 reviews related works, including e-voting and previous e-voting services worldwide, e-Voting system requirements, and the blockchain based e-voting system. Section 3 presents the service flow and system architecture of the proposed Blockchain based e-voting System for e-voting Requirements. Section 4 concludes the paper by describing how the seven e-voting system principles and two e-vote Requirements are satisfied by the proposed blockchain based e-voting System for e-voting Requirements, mentioning the limitations of the study, and indicating future research directions.

2. Related Works

[7] uses Ethereum, a public blockchain, and shows the efficiency of an e-voting system. However, there is a lack of debate on how to resolve the requirement factors for an e-voting system. [8] implements confidentiality by encrypting the voting contents in a homogeneous cryptography, and stores the hashed vote results in an IPFS, and the hash values of the IPFS in the blockchain. [9] proposes a solution using a blockchain for the various requirement factors for an e-voting system. In implementation of this e-voting system, the actual voter cannot confirm that his or her vote was normally reflected in the results, because the voter's voting result is not stored in the blockchain; rather, an encrypted voting result is sent to the calculator by using a homogeneous password. [10] generates a unique key to be used for signature based on voter biometric authentication. If the voter's biometric information is exposed, the encryption key is likely to be exposed. Voting is done by sending transactions to each candidate's address, using a separate address. [11] provides confidentiality by encrypting the voting content included in the transaction. After generating a voting transaction by encrypting the contents with the public key of the ballot counting center by encrypting the contents of the ballot counting center, a method should be taken to encode the encrypted voting contents with the private key of the ballot counting center. At this time, the asymmetrical key pairs of counting stations are created simultaneously before the election, so if the individual keys of counting stations are exposed during the election period, the stability of the vote will be challenged.

3. Proposed Blockchain based e-Voting System for Vote Requirements

The proposed blockchain based e-voting system provides anonymity for voters by issuing voting certificates based on blockchain addresses. The election supervisory committee, composed of people with conflicting interests, creates a critical group encryption key, giving confidentiality by the critical encryption algorithm during the voting process. The voting content is encrypted through a homomorphic encryption algorithm and stored in the blockchain, and the public voting content of proposed blockchain

based e-voting system satisfies safety, confidentiality, transparency, and non-ticketing. Blockchain's smart contract provides the unity and competence of voting in figure 1.

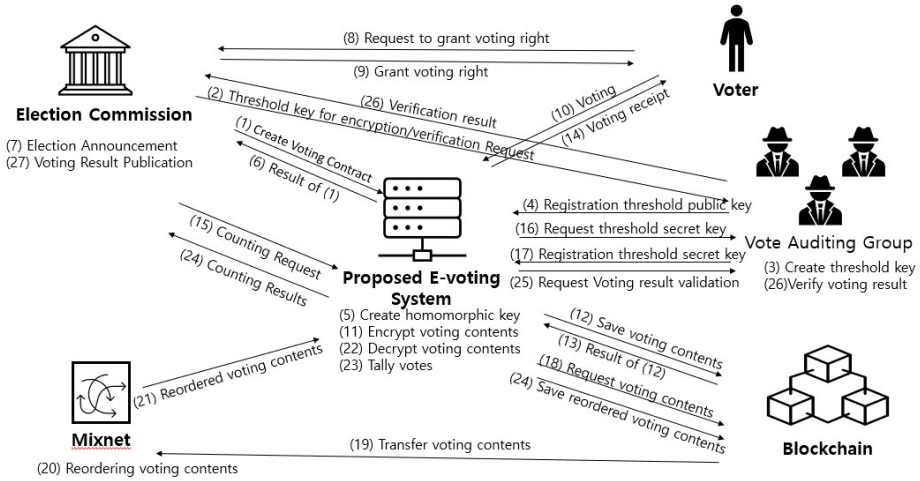

Figure 1. Proposed Blockchain based e-Voting System

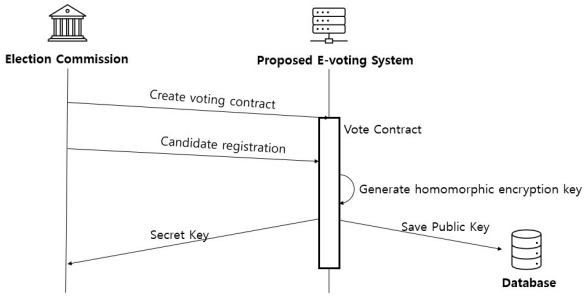

Figure 2. Process of Voting Contract Creation

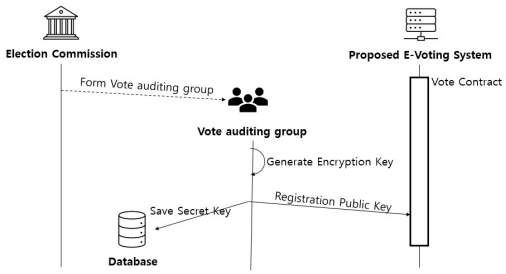

Figure 3. Process of Vote Auditing Group

Process of voting contract creation is presented in figure 2 and each stage messages flows are depicted in bellows.

① The election commission committee generates election contracts.

② The election commission committee registers candidates in the election contract. At this time, the unique number of each candidate to be used for the aggregation shall be registered together.

③Election contracts generate homomorphic cryptographic asymmetric keys, store public keys in a system, and deliver secret keys to the Election Commission.

Process of composition of Vote Auditing Group and enrolment of cryptographic keys is presented in figure 3 and each stage messages flows are depicted in bellows.

① The election commission committee forms a vote auditing group and requests the enrolment of encryption keys.

② The vote auditing group generates a key for encrypting and validating voting contents, enrolments the public key in the vote contract, and keeps the secret key individually.

Process of grant voting right to wallet is presented in figure 4 and each stage messages flows are depicted in bellows.

① Voters generate a blockchain wallet for e-voting.

②Voters ask for voting authority by presenting the proposed e-voting block wallet address created by the election commission committee.

③ After confirming the requester's voting authority, the election commission committee grants voting right to the wallet presented.

Process of voting is presented in figure 5 and each stage messages flows are depicted in bellows.

① Voter requests list of candidates.

② The election contract confirms the address presented and sends the list of candidates.

③Voters enter candidate numbers manually.

④ The election contract extracts the voting content from the voters' hand-written images and presents the voting content to the voters.

⑤Voters check the voting details extracted by the voting system, sign their own secret keys on the hand-written images and extracted voting contents, and register their handwritten images with their own public key again as evidence of voting.

⑥Election contracts prevent double voting by scrapping voting rights granted to a block change box of a voter's proposed e-voting system.

⑦Electoral contracts store voter encrypted voting evidence separately.

⑧Voting data and verification data are created and stored in the blockchain, respectively, using the location where the voting evidence is stored and the extracted voting details.

⑨Stored voting evidence is used to check whether or not the contents of the vote are reflected properly after the voting is completed.

⑩When stored in a blockchain by election contract, the generated transaction key is distributed to the voters as a receipt. This transaction key allows voters to verify that their voting is recorded in the blockchain.

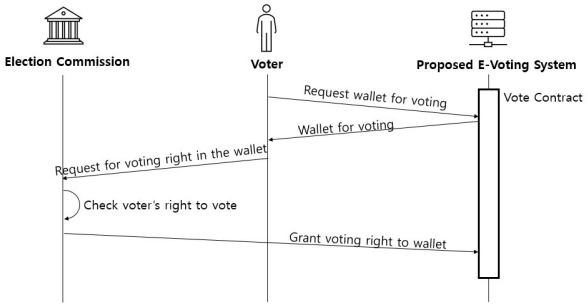

Figure 4. Process of Grant voting right to wallet

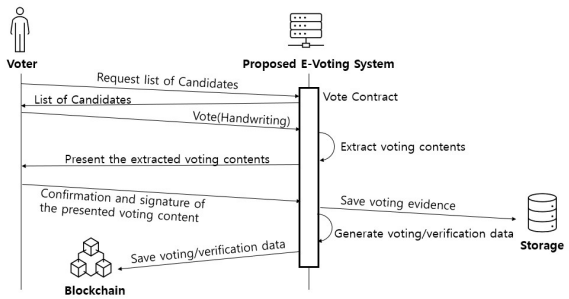

Figure 5. Voting

Process of Tally is presented in figure 6 and each stage messages flows are depicted in bellows.

① The election commission requests the secret key registration to the election auditors

② The election auditors register the secret key in the election contract.

③Election contracts read the voting tables stored in the blockchain in a rearranged voting order through the Mix-net.

④Election contracts use secret keys of election watchdogs to duplicate voting tables.

⑤Election contracts re-save the vote data in the blockchain.

⑥Election contracts aggregate voting data.

Process of verification is presented in figure 7 and each stage messages flows are depicted in bellows.

① The election auditor uses the verification data to determine the exact number of votes counted for each candidate.

②Results of the verified tally is notified and published to the Election Commission.

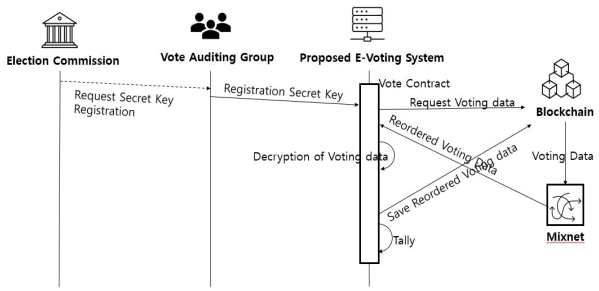

Figure 6. Process of Tally

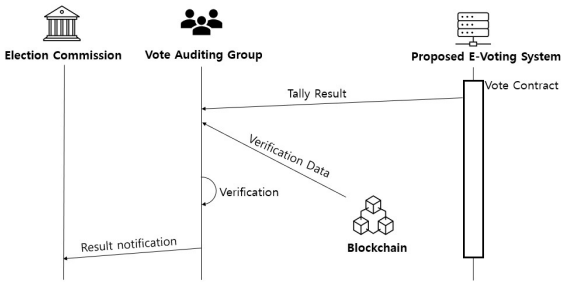

Figure 7. Process of Verification

Process of Voter's ballot Verification are depicted in bellows.

① Voters who wish to verify the voting results submit their ballot receipts and secret keys of the voting block wallet to the Election Commission.

② The Electoral Commission takes the voting evidence recorded on the submitted ballot receipt from the repository.

③The secret key of the submitted voting blockchain wallet will be sublime.

④Confirm that the image and signature are voters'.

⑤The voting data is generated with the voting content, and it is verified that it is the same as the contents stored in the blockchain.

4. Conclusion

Research on the existing e-voting system has targeted only some of the requirements for e-voting, and not all e-voting requirements have been satisfied. In particular, the encryption of data stored in the blockchain was used for voting results, and there was a problem in verifying the voter's voting results.

In this study, we designed a blockchain-based e-voting system that includes the process of encryption and verification of voting results. The proposed blockchain-based e-voting system satisfies the requirements of e-voting as follows: First, the proposed blockchain-based e-voting system stores voting results in a blockchain that cannot be altered. The stored voting results are homogeneously encrypted, and the voting results are opened to the public. Therefore, anyone can check the accuracy of the vote count results. Voters can check and approve their vote results; thereby, the proposed blockchain-based e-voting system prevents voters from a voting result that is different from their intentions. Therefore, the proposed blockchain-based e-voting system guarantees stability. Second, the proposed blockchain-based e-voting system uses the poll site voting method, and builds an independent environment that is separate from the general network. Therefore, the proposed blockchain-based e-voting system guarantees integrity by removing external risk factors, such as hacking. Third, there is no direct connection between the voter with voting authority and the voter's blockchain wallet used in the voting process, and voters cannot be inferred from the blockchain wallet. The order of the voting results released after the voting counting is changed through MixNet, and the voting results of the voters cannot be grasped using the voting order. When a vote is made, the voter creates a new blockchain wallet. Since the address of the blockchain wallet used for voting is changed every time, it is impossible to predict from the past voting history. Through this, the proposed blockchain-based e-voting system guarantees confidentiality. Fourth, each voter receives the blockchain wallet address information, and stores the voting result in the blockchain wallet address. Using the smart contract of the blockchain, the smart contract checks whether the address of the blockchain wallet is voting, and one vote is allowed. Through this, the proposed blockchain-based e-voting system guarantees unity and competence. Fifth, during the voting process, the voter's voting results are critically encrypted. Through critical encryption, the voting results are made impossible to decrypt by a specific group. Through this, the proposed blockchain-based e-voting system ensures fairness by preventing previous voting from affecting the remaining voting. Sixth, after voting, the voter can use the voting receipt to confirm that his or her vote is stored in the normal blockchain. After counting the voting results, voters can check the reflection of the voting results

through the Election Commission. The proposed blockchain-based e-voting system creates both voting count data, and voting verification data. The voting count data and the voting verification data use a separate encryption key, and the proposed blockchain-based e-voting system guarantees verification. Seventh, after counting the votes, it is impossible for a voter to independently check the results of his or her vote. This disallows the act of voting through the disclosure of the voter's voting results.

This study confirms that when applying a blockchain and cryptographic algorithm, a system that satisfies the requirements of e-voting is possible.

Acknowledgments
This work is supported by 2020 Korea National Open University Research Fund (202000730001).

References

[1] Huh Won-geun, Kim Hui-seon, Kim Gwang-jo. A Study on the Requirements of Electronic Election Protocol, Korea Institute of Information Security and Cryptology, 2000, 10(1): 63-67
[2] Korea National Election Commission (http://law.nec.go.kr)
[3] Cho Hee-jung. Electronic Democracy and internet Voting – Focusing on Estonian Cases, Korean Political Parties Association, Korea Political Parties Association, Journal of the Korea Political Parties Association, 2008, 7(2): 159-188(In Korean).
[4] Jeong Jin-woo. Exploring Research on the Effect and Problems of E-voting, Seoul National University Graduate School of Public Administration, General Assembly, 2003, 44(4): 107-126.
[5] Ryu Seok-jin and Kim Yong-bok. The Issue and Reality of E-voting Discussion: Comparison Between Korea and Japan", Seoul National University's Korean Political Research Institute, 2009, 18(2): 127-158.
[6] Hong Seung-pil, Min Kyung-sik, Kim Hye-ri. Research on the Applicability of Online Voting System Using Blockchain Method, Korea Internet Information Association, 2017 National Election Training Institute Research Service Report, 2017.
[7] Park Tae-jin. Design and Implementation of Online Voting System using BlockChain, Hanyang University Graduate School of Engineering, Diploma (Master) Hanyang University Graduate School of Engineering: Computer Engineering major, 2019.
[8] Han Sang-woo, Bae Min-soo, and Hwang Kyung-ho. Development of Blockchain based E-voting System Using Homomorphic Cryptography, Korea Telecommunications Association, Journal of the Korea Telecommunication Association, 2019, 44(1): 171-174.
[9] Kang Hee-jung. Designing and Implementing a Reliable Blockchain Based E-voting System, Sunghin Women's University Graduate School, Diploma (Master), Sungshin Women's University Graduate School: Computer Science, 2019.
[10] Ha Hyun-soo, Lee Seo-joon, Jung Gu-ik, Shin Yong-gu, Kim Myung-ho, Kim Young-jong. Anonymous E-voting Blockchain Platform Model Based on Public Blockchain, Korea Information Science Association, A collection of papers published by the Korea Information Science Association, 2017, 12(2): 1176-1178.
[11] Roh Chang-hyun. A Study on E-voting System using Blockchain", Soonchunhyang University Graduate School, Diploma (Master), Soonchunhayung University Graduate School: Computer science, 2020.