November-December 2019
ISSN: 0193-4120 Page No. 1654 – 1661

Smart Contract-Based Electronic Voting System that Provides Fairness

Chang Hyun Roh
Department of Computer Engineering
SoonChunHyang University, Asan, Republic of Korea
Email- rohch@sch.ac.kr

Yong Woon Hwang
Department of Computer Engineering
SoonChunHyang University, Asan, Republic of Korea
Email- hyw0123@sch.ac.kr

Im-Yeong Lee*
Department of Computer Engineering
SoonChunHyang University, Asan, Republic of Korea
Email- imylee@sch.ac.kr

Article Info
Volume 81
Page Number: 1654 – 1661
Publication Issue:
November-December 2019

Article History
Article Received: *5 March 2019*
Revised: *18 May 2019*
Accepted: *24 September 2019*
Publication: *09 December 2019*

Abstract

E-government systems have ensured reliable data and prevented the forgery and modulation of that information, and so far, this role has been carried out in traditional centralized management. However, centralized data management has the disadvantage of single point of failure and bottlenecks. Blockchain technology has emerged to solve this problem. It is characterized by decentralization, which has been considered insecure in the past, to ensure the integrity of data. However, there are many problems in applying general blockchain and smart contracts to e-government electronic voting. In this paper, we propose a scheme to guarantee the integrity of voting data and to automate the process of voting and counting by smart contract by applying blockchain and smart contract to provide integrity and automation function to electronic voting.

Keywords: *e-Voting, Blockchain, Ethereum, Smart contract, Security, Fairness.*

I. INTRODUCTION

Electronic voting refers to the mechanical implementation of existing paper voting schemes. Existing paper voting schemes are more expensive than election ballots, and it is time consuming to count each ballot. Owing to these problems, electronic voting has been proposed as an alternative to paper voting [1].

Conventional electronic voting attempts to provide convenient and secure voting using cryptographic algorithms. However, in a centralized structure, forgery of voting data may occur owing to the authority of the manager. In addition, it has been applied only to fields where a small number of people can use it such that single point of failure can occur [2].

November-December 2019
ISSN: 0193-4120 Page No. 1654 – 1661

Recently, various studies have been conducted to apply blockchain technology to solve the problem of trust and the threat of single point failure [3]. Blockchain refers to ensuring the reliability of having the same data by applying various consensus algorithms in a network of a peer-to-peer environment [4]. Dispersion, which is characteristic of blockchains, can provide stability to the electronic voting system and provide solubility as a property of decentralization. The processing of all voting data as a transaction and storing them in a block renders it impossible for malicious network participants to easily forge data. Furthermore, it uses the smart contracts provided by the blockchain to automate voting and counting and ensures the integrity of the data generated from voting and counting. For this reason, many schemes for electronic voting with blockchain have been proposed. However, a scheme of ensuring all the basic security requirements of electronic voting has not been proposed yet. In electronic voting, the proposed scheme encrypts the contents of voting to ensure confidentiality and hinders the voter from linking such that the voter cannot be determined by the voting contents. In addition, we propose an electronic voting system using a blockchain that provides fairness by not counting in real time using a counting server. This proposal consists of the following: Section 2 discusses electronic voting, blockchain, and the electronic voting schemes that apply blockchain. Section 3 describes the electronic security requirements and system goals. Section 4 describes the proposed blockchain electronic voting scheme. Section 5 analysis the security requirements of the proposed scheme of electronic voting.

II.RELATED RESEARCH

2.1 E-Voting –

Electronic voting implies electronicizing all voting procedures. The voting process comprises the establishment of candidates and voters, identification, voting, counting of votes, verifications, etc., and all these processes must be performed with credibility such that an election can be regarded as legal [5]. With the development of various technologies, schemes, such as short message service electronic voting using a smartphone or a phone, voting by logging into a general server, and a mobile voting using a smartphone or tablet, Personal Computer have been proposed [6]. Electronic voting affords the advantages of low time and space constraints, low voting costs, and quick and convenient ballot counting [7]; however, it cannot be used owing to lack of system reliability and data forgery and alteration. Hence, many researchers have recently proposed an electronic voting system using a blockchain.

2.2. Blockchain –

Blockchain was first introduced as an application called Bitcoin by an anonymous developer named Satoshi Nakamoto. Bitcoin has no structure for issuing and managing money like a central bank. In a P2P network, all participants form a network using a distributed database with the same ledger [8]. Blockchain is a list of data records that is constantly growing as a form of distributed database and is designed to be free from arbitrary manipulations by the operators of distributed nodes. The characteristics of such a blockchain are as follows [9]:

- Decentralization: Blockchain operates in a P2P distributed network, and everyone creates a blockchain by sharing data with equal conditions without management.
- Difficult to forge: Because data are shared through a consensus algorithm in a distributed network, it is difficult to forge a consensus algorithm without seizing more than half of the network.
- Traceable transaction: A transaction is where owners of private and public keys are shared across all networks through signatures; therefore, a feature that can reliably connect and track the movement of transactions exists.

As a characteristic of the blockchain, it affords decentralization and a distributed network through a P2P network, and the ledger of the blockchain is transparent as it can be verified by anyone. In addition, the voter and voter information are not mapped, thus providing anonymity. Furthermore, blockchain networks are guaranteed to be accessible anywhere and anytime.Blockchain is divided into public blockchain and private blockchain according to the characteristics of participants. Public blockchain is a structure that anyone can participate in the blockchain network so that anyone can read and write data. Private blockchain is a structure where only designated blockchain nodes and designated users use the blockchain, so only trusted and guaranteed users can participate in the blockchain network. Private blockchain is more suitable for electronic voting because public blockchain is mainly communication between untrusted network participants. Electronic voting is conducted through trusted institutions such as governments.

2.3.Blockchain-based e-voting system –

In 2015, Zhao and Chan first applied electronic voting to the Bitcoin blockchain platform [10]. Based on the Lottery algorithm, candidates were selected, and voters voted by sending Bitcoins to their preferred people. In addition, the voter's behaviour is represented using random numbers to hide the voter's relationship, and it has a function to determine the authenticity of the vote by

November-December 2019
ISSN: 0193-4120 Page No. 1654 – 1661

calculating that the total number of random numbers is zero. However, the Lottery algorithm does not encrypt the voting data; therefore, the voting flow is revealed in real time. Subsequently, L. Kibin presented an electronic voting model by storing voting data in Bitcoin and identifying voters via TTP(Trusted Third Party). In voting by sending Bitcoins, the content of the vote is displayed in real time, which may affect the next voter [11]. Most recently, Friðrik Þ. Et al. proposed an electronic voting protocol using Ethereum and smart contracts [12]. The election manager pre-registers the election and selects the candidates. After the selected candidates execute a voting contract to vote in a predetermined election, the voting data are stored in the blockchain to be recorded and counted in real time. However, even in this study, the content of the voting contract is not encrypted; thus, the contents of the voting can be viewed in real time and may affect the subsequent voters.In this paper, the process of voting and counting is composed of smart contracts in the electronic voting system operating on the blockchain, so that administrators cannot participate in the voting and counting process. In addition, there is a process that stores the results of voting and counting in the smart contract code stored in the blockchain and executed in the smart contract code.

III.SECURITY REQUIREMENT AND GOALS

3.1. Security Requirement –

Electronic voting is constructed by applying the appropriate cryptographic algorithm and uses the applied cryptographic techniques to satisfy the attributes of voting [13]. First, all the contents compiled during voting must be correctly processed and counted, and the voting must not be interrupted by unjust users. In addition, a voter must not be able to prove his vote, and the voter can vote only once. Additionally, only those who have the right to vote can vote, and the voting system shall not affect the voting. Finally, anyone should be able to verify the count of the ballot results. Therefore, the requirements of electronic voting are as follows[14].

- Completeness: All contents counted in the ballot must be processed correctly.
- Soundness: Votes must not be interrupted by unjust voters.
- Privacy: No one else should know who a voter has voted for.
- Unreusability: Voters must be able to vote only once.
- Eligibility: One has the right to vote and one can vote.
- Fairness: A vote should not be affected in any situation.
- Verifiability: Anyone should be able to verify the results of the vote.

3.2. Token Freeze –

In this proposed scheme, a token is sent to registered voters and then the token is sent to the candidates. However, all transactions in the blockchain are public, which may cause unfairness. Hence, we use token freeze, which sends tokens to intermediate smart contract addresses and subsequently to candidates when voting ends. For voting fairness, data are encrypted using multi-signature and hierarchical wallets, and a freeze design using multi-signatures is used.

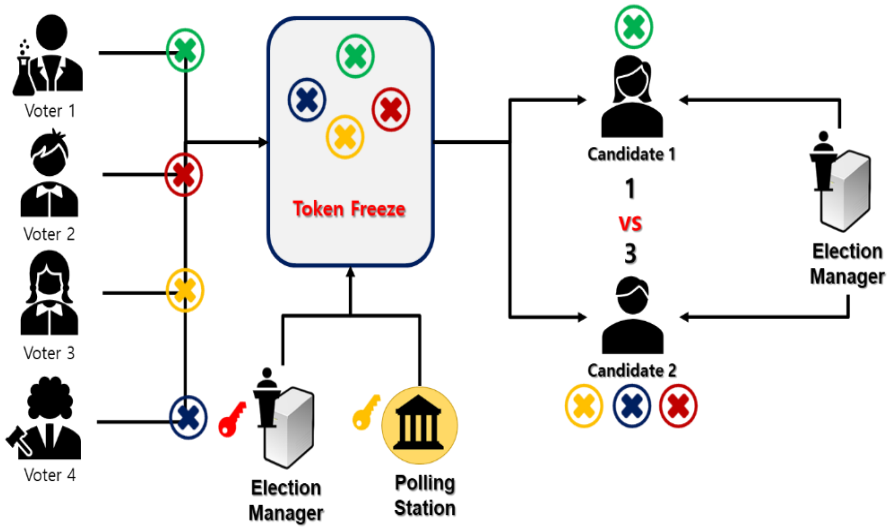

Figure 1. Token Freeze

November-December 2019
ISSN: 0193-4120 Page No. 1654 – 1661

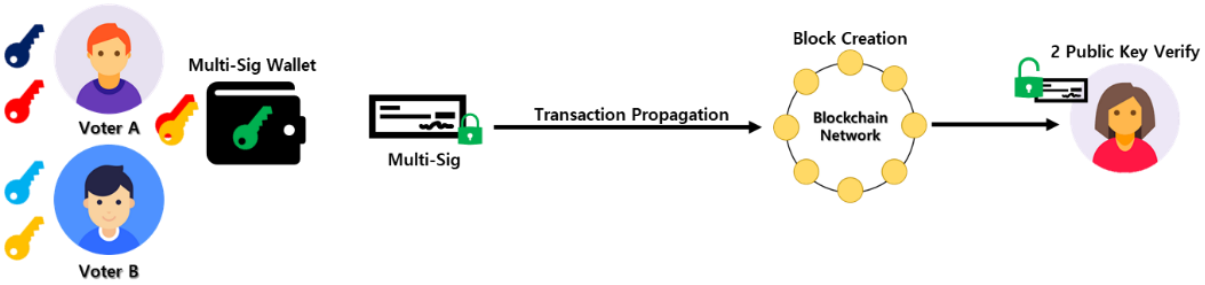

Figure 2. Multi-Signature

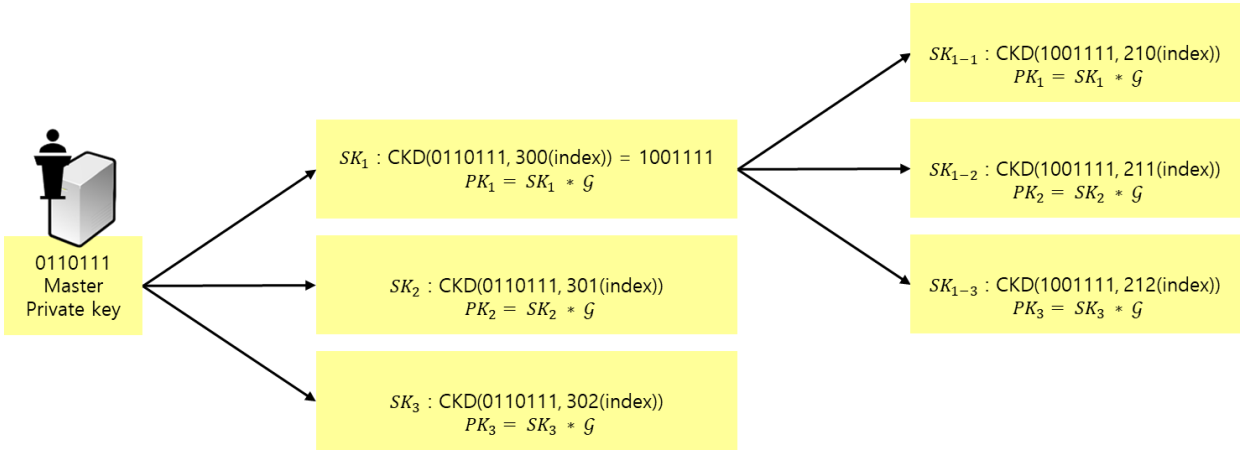

Figure 3. Hierarchical Deterministic Wallet

- Multi-signature
  Multi-signature refer to a scheme of transmitting a specified number of keys among multiple keys. In the past, a signature is sent with the private key of the sender who created the transaction (Shown in Figure 2). However, the multi-signature is composed of a structure that can generate a transaction only with the consent of several people. This is called an m-of-n transaction and is a function provided by the Wallet program in Bitcoin.
- Hierarchical Deterministic Wallet
  Hierarchical deterministic wallets simplify the backup of private keys used in wallets significantly and are key management tools that do not require repeated communications in multiple programs using the same wallet. They are used to derive the lower private key and public key from the upper private key, and the upper key private key has a feature that can control the lower layer and divide it into restricted accesses (Shown in Figure 3). The wallet was first proposed as an application on the blockchain in 2012 under the code name BIP0032 in the developer proposal of Bitcoin; additionally, it can generate and derive a key based on ECDSA, a key generation algorithm of Bitcoin or Ethereum.

IV.PROPOSED SCHEME

This chapter proposes a scheme of voting on the blockchain that satisfies various security requirements of electronic voting by using smart contracts in the private blockchain. This proposal consists of managers, polling server and counting server. Participating polling servers and counting server form a blockchain network.

This proposal is divided into preparation phase, voting phase, block generation phase, and counting phase. In the preparation phase, votes are established by generating election keys for the counting server and managers. They then have a process of registering voters to prepare for elections. At the voting phase, registered voters are checked and voting proceeds. The process by which the voter selects the candidate data is encrypted with the public key of the counting server and the manager and inserted into the transaction. In the block generation phase, the transaction creator checks whether the vote

November-December 2019
ISSN: 0193-4120 Page No. 1654 – 1661

has been duplicated and generates a block. Lastly, in the counting phase, the manager and the counting sequentially decrypt the encrypted voting data and proceed with the counting.

4.1. System Parameters –

* : Participating object (M: Manager, P: Polling server, C: Counting server, V : Voter)

pk, sk: Public / Private key pair
E_{pk}: Encrypt with public key
D_{sk}: Decrypt with private key
I_L : Left bit of I
I_R : Right bit of I
mk: Master key used to derive subkey
esk: Child private key for election derived from master key
epk : The public key for election generated from the derived private key
$Index$:Parameters for deriving subkeys
$H()$: Hash function
tx: Transaction
$Block$: Block
ci_i: Candidate info
vi_i: Voter info
vl: Voter list
CKD: Child key derivation function
sig_{sk}: Signature of private key

4.2. Preparation Phase –

The preparation phase includes a step-in which M sets up a voting, registers a user, and registers a smart contract before each participating object proceeds to vote. The contents of the smart contract will include voting topics, content, time, and voter information(Shown in Figure 4).

Step 1. The voter randomly selects a random integer value sk_v included in Z^p on the elliptic curve, calculates the point G on the elliptic curve, and generates a public key pk_v.

Step 2.M and C generate master key using CKD

Step 3. The M and P derive a child private key using mk and cc created in Step 2 and generate the child public key by calculating this private key with the point G on the elliptic curve.

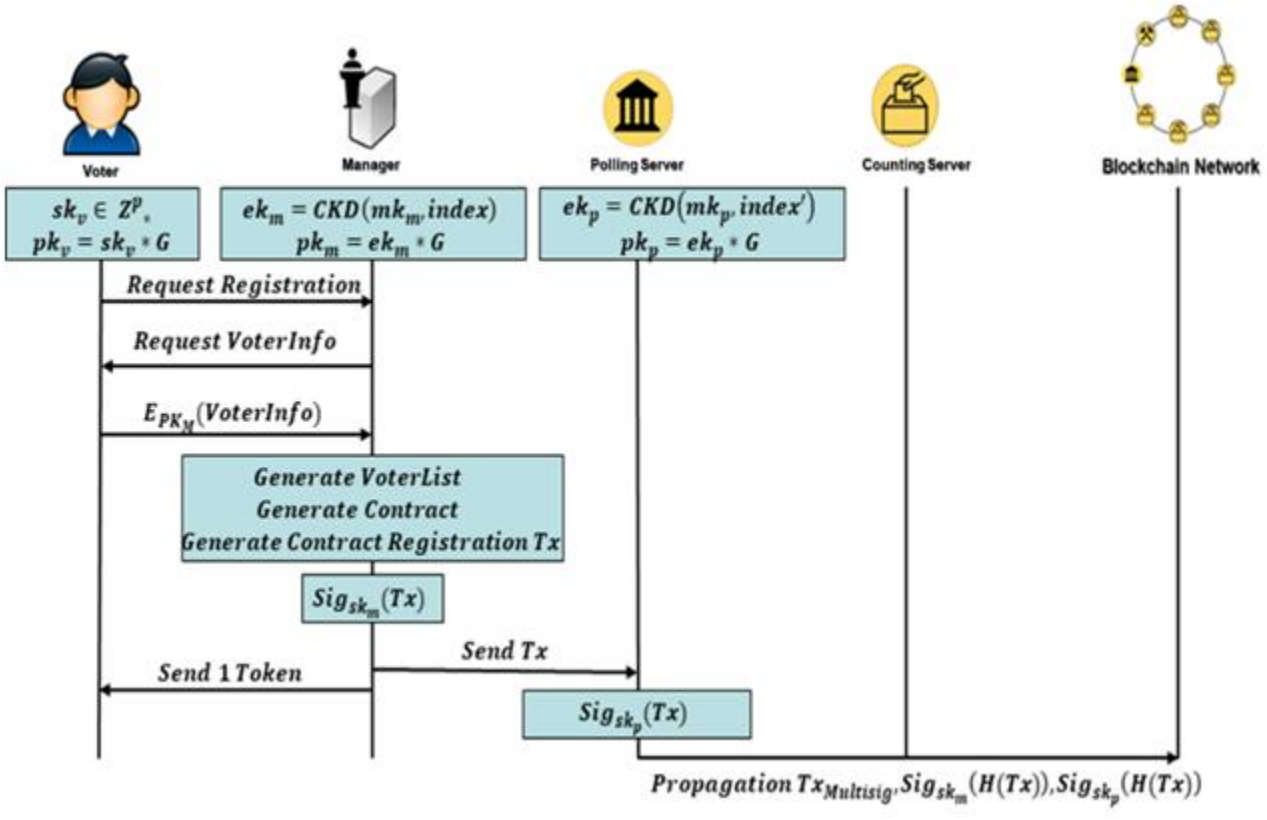

Figure 4. Preparation Phase

November-December 2019
ISSN: 0193-4120 Page No. 1654 – 1661

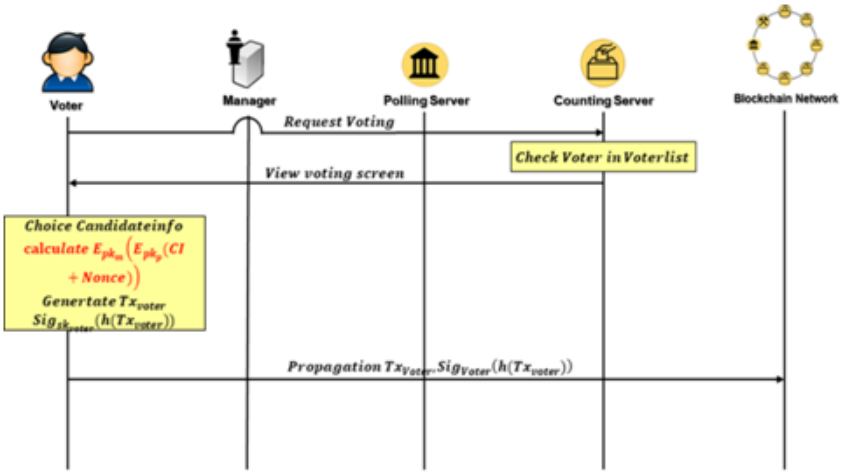

Figure 5. Voting Phase

Step 4. The voter encrypts his / her personal informationvi to be registered in the election with the M's election public key and sends it.The M then createsvl.

Step 5. The M creates the election contract and inserts it into the transaction. Signed with esk_m and delivered to C.

Step 6.P signs the received transaction with esk_c and creates a multisignature transaction with C's signature and P's signature in the transaction.

Step 7. The M sends one token to the registered voters.

4.3. Voting Phase –

In the voting Phase, V executes P's voting contract, passes the voter authentication process, receives candidate information, selects a candidate, associates the selected data with the voting time, encrypts it, and inserts it into a transaction(Shown in Figure 5).

Step 1.V accesses smart contracts on blockchain network

Step 2.V selects the candidate and generateci_i. Then ci_i is encrypted using P's and C's election public keys esk_p and esk_c.

Step 3. V selects the voter, encrypts it with the election public key of the P and the C, and creates a transaction.

4.4. Block Generation Phase–

In the block generation Phase, V transmits a transaction in which the encrypted data is inserted to P who voted. P then validates the transaction with another P. The blockchain network collects transactions, creates blocks, sends them to all Ps and Cs, and connects them to the blockchain.

Step 1. Miner receives alltx.

Step 2. Check that the user first created tx. If a user creates more than one tx, $tx$is not accepted.

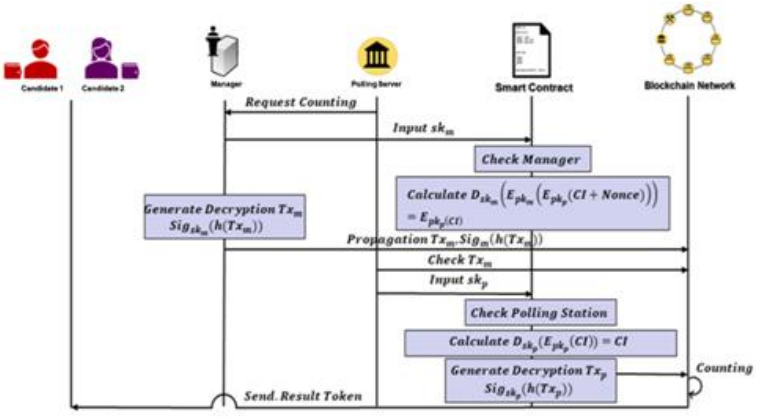

Figure 6. Counting Phase

November-December 2019
ISSN: 0193-4120 Page No. 1654 – 1661

Step 3. Miner validates tx received from another node.
Step 4. When the validation is complete, the miner collects tx to create a block.
Step 5. Miner propagates $Block$ to all nodes of blockchain network

4.5. CountingPhase –

The counting phase proceeds by P sending a counting message to M. P enters the election private key into the counting contract and performs the first decryption. Thereafter, the Pperforms the second decryption with the election private key of the Pand transmits the tokens to the wallet addresses of the candidates who generated the tokens as the M's subkeys according to the voting result (Shown in Figure 6).

Step 1. After checking the voting time, P sends to M if it is finished.
Step 2. M executes the counting contract and enters epk_m to proceed with the first decryption.
Step 3. After the first decryption, the Penters epk_p into the contract to proceed with the second decryption.
Step 4. Countci_i after decryption

V. SECURITY REQUIREMENT ANALYSIS

This proposal satisfies the security requirements der ived in Section 3 as follows. In particular, the propo sed scheme can provide fairness. When voting using the proposed scheme, the voting data ci and nonce are encrypted with epk_m and epk_c, which are the p ublic keys of the polling server and manager, respec tively, and encrypt data is inserted into the transacti on. This prevents the nodes participating in the bloc kchain from verifying the voting data, which provid es confidentiality to the voting data, thereby providi ng fairness to the voting system. For this protocol a nd implementation, the attributes can be described a s follows.

- Completeness: All ballots can be calculated correctly. All data stored in the blockchain are difficult to forge and alter; therefore, the voting data can be calculated completely.
- Soundness: Registered voters go through the manager and receive the public key through voter registration; therefore, soundness is guaranteed because it is a structure that cannot interfere with unjust voting.
- Privacy: Encrypts the voting data with the public key of the manager, such as $E_{pk_m}(E_{pk_c}(C_i \parallel nonce))$; therefore, one can hide the votes, thus ensuring privacy.
- Unreusability: Even if a voter had registered on the blockchain votes multiple times, it provides unreusability because only the first data are recognized as the voting data. (Apply in step 2 in 4.3)
- Eligibility: Only registered persons can vote through the registration process and provide eligibility because the interferer can confirm whether the registered person is registered even if they created and added a transaction.
- Fairness: Provides fairness by encrypting voting data such that voting proceeds and does not affect the next voter.
- Verifiability: Data are always stored correctly in the blockchain; therefore, if verification requests occur, the data can be verified with the private key of the manager.

VI.CONCLUSIONS

In order to secure voter credibility for the voting pro cess and results in the online environment, research es are being conducted to solve the security threats caused by electronic voting using blockchain techno logy. Electronic voting using the existing blockchai n platform was a problem in which the voting data was disclosed and voted to each candidate, so that a nyone could know the current status of voting. To s olve this problem, we proposed a system that satisfi es all the security requirements in the electronic voti ng system using blockchain through the encryption of voting data. In particular, the blockchain network was limited to the polling server and counting serve rs. The powers of the manager and voting and count ing servers are distributed, and the registration proc ess is performed separately for a better process. In a ddition, because the voting data are encrypted and tr ansmitted in the transaction, transparent voting resul ts can be expected through collecting the transaction s from the manager to prevent negation when gener ating the block. Furthermore, the smart contract voti ng and counting schemes enable the central manage r or the manager to set up a voting poll once and pro

November-December 2019
ISSN: 0193-4120 Page No. 1654 – 1661

ceed automatically without any involvement.
In the future, it is necessary to study from the ineffi cient scheme of applying encryption twice to the sc heme of efficient encryption between the manager a nd the Counting server.If the electronic voting syste m is developed and commercialized as such, the vot ing cost can be reduced, and the turnout rate can be increased. Hence, safe voting and counting services can be realized in electronic voting.

ACKNOWLEDGEMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2019R1A2C1085718) and the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2019-0-00403) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation)

REFERENCES

1. F. Ciazzo and M. Chow, “A block- chain implemented voting system,” Dec. 2016.
2. Government Accountability Office, “Federal efforts to improve security and reliability of electronic voting systems are under way, but key activities need to be completed,” Sep. 2005.
3. Ourad, Abdallah Zoubir, Boutheyna Belgacem, and Khaled Salah. "Using blockchain for IOT access control and authentication management." International Conference on Internet of Things. Springer, Cham, 2018.
4. PILKINGTON, Marc. 11 Blockchain technology: principles and applications. Research handbook on digital transformations, 2016, 225.
5. Tschorsch, Florian, and Björn Scheuermann. "Bitcoin and beyond: A technical survey on decentralized digital currencies." IEEE Communications Surveys & Tutorials 18.3 (2016): 2084-2123.
6. NEFF, C. Andrew. A verifiable secret shuffle and its application to e-voting. In: Proceedings of the 8th ACM conference on Computer and Communications Security. ACM, 2001. pp116-125.
7. Ofori-Dwumfuo, G. O., and E. Paatey. "The design of an electronic voting system." Research Journal of Information Technology 3.2 (2011): 91-98.
8. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system.”2008.
9. Yeboah, A. "Electronic Voting in Ghana: Is It The Solution To Ghana’s Perceived Electoral Challenges After Biometric Registration?" Journal of Information Engineering and Applications 3.1 (2013).
10. Z. Zhao and T-H. Hubert Chan, “How to vote privately using bitcoin, “International Conference on Information and Communications Security, pp82-96, Dec 2015.
11. LEE, Kibin, et al. Electronic voting service using block-chain. Journal of Digital Forensics, Security and Law, 2016, 11.2: 8.
12. Hjálmarsson, Friðrik Þ., et al. "Blockchain-based e-voting system." 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). IEEE, 2018.
13. Bernhard, David, and Bogdan Warinschi. "Cryptographic voting—a gentle introduction." Foundations of Security Analysis and Design VII. Springer, Cham, 2013. 167-211.
14. Okamoto, Tatsuaki. "Receipt-free electronic voting schemes for large scale elections." International Workshop on Security Protocols. Springer, Berlin, Heidelberg, 1997.