International Journal of Control and Automation
Vol. 10, No. 12 (2017), pp.121-130
http//dx.doi.org/10.14257/ijca.2017.10.12.11

A Study on Ways to Apply the Blockchain-based Online Voting System

Hye Ri Kim[1], Kyoungsik Min[2,*] and Seng-phil Hong[3]

[1]*Dept. of Computer Science, Graduate School, Sungshin Women's University*
[2]*Korea Internet & Security Agency*
[3]*Dept. of Convergence Security Engineering, Sungshin Women's University*
[1, 3]*{hrkim,philhong}@sungshin.ac.kr,* [2]*kyoungsik@kisa.or.kr,*

Abstract

The blockchain is a technology designed to verify whether online financial transaction data has been tampered with or not. It has been proven to be reliable as it has been introduced into various fields requiring reliability as well as financial institutions around the world. As the introduction of blockchain technology is expected to bring about a lot of changes in the public service sector, technology adoption is also being reviewed in many countries around the world. In particular, the introduction of blockchain technology in the online voting sector has the advantage of enhancing the reliability, transparency and efficiency of voting. Therefore, in this paper, we analyze the institutional and technical problems that may occur when applying the blockchain technology to online voting system, and suggest ways of using it.

Keywords: *Blockchain, Distributed Ledger, Online voting*

1. Introduction

Major countries around the world have been adopting electronic voting since the mid-1990's, and currently about 50 countries are using electronic voting in elections for public offices. As for electronic voting in Korea, Internet voting was used for the Democratic presidential nomination in 2002. In 2003 it was selected as the core project of the 'increasing citizens' online participation' task, one of the 31 electronic government roadmap tasks of the Participatory Government. Accordingly, the National Election Commission began to develop the electronic voting system in 2006, and it was used in various commissioned elections on a pilot basis. Electronic voting has been advancing gradually [1]. However, using electronic voting in elections for public offices does not mean simply changing the election management method from paper voting to digital voting. It needs to be evaluated as a very political public policy with big repercussions on national policies. Accordingly, for this electronic voting system to win the trust of voters, technical security and stability must be perfectly guaranteed.

Recently there is a movement for utilizing the "blockchain" method, which is emerging as a future technology, to reinforce security. Blockchain is a distributed open ledger management technology that commonly records and stores the information and values produced by network participants, and it can be said to be a storage platform designed to make it difficult to arbitrarily fabricate data as all participants verify and store the data on the network [2]. Therefore, if this blockchain technology is applied to the online voting system, it is possible to implement electronic management, *e.g.*, recording the right to vote in the blockchain, and if it is used to check whether voters voted or count votes, it will improve efficiency. Also, as it has various advantages, *e.g.*, time and cost reduction,

Received (September 6, 2017), Review Result (December 1, 2017), Accepted (December 7, 2017)
[*] Corresponding Author

increased voter participation, and increased security and reliability, there is a movement to utilize the blockchain method in voting. Therefore, this paper will summarize the issues that must be considered when the blockchain technology is applied to the online voting system to increase reliability, transparency and efficiency, and suggest ways to utilize it.

2. Theoretical Background and Case Studies

2.1. Blockchain

Bitcoin appeared in the world in 2008 when a developer using a pseudonym Satoshi Nakamoto published a report titled <Bitcoin: A Peer-to-Peer Electronic Cash System>, and the blockchain originated from the success of the virtual currency called bitcoin [2]. The Bank of Korea defined blockchain as ‘a technology that makes it possible for participants to commonly record and manage transaction information by distributing the ledgers containing transaction information on the P2P network, not in the server of a certain institution,’ and as all users on the network jointly own the ledgers, even if part of the network has a problem, the entire block will not be affected, and as it does not go through a third party, fees and maintenance costs can be reduced. [3]

As the blocks of all transactions that network participants agreed on and verified as valid are linked to the most recent block at the genesis block, hence the name blockchain. And the blockchain serves as the single access path to the absolutely perfect original data, and the members of the blockchain network can view only those transactions which are related to them [4].

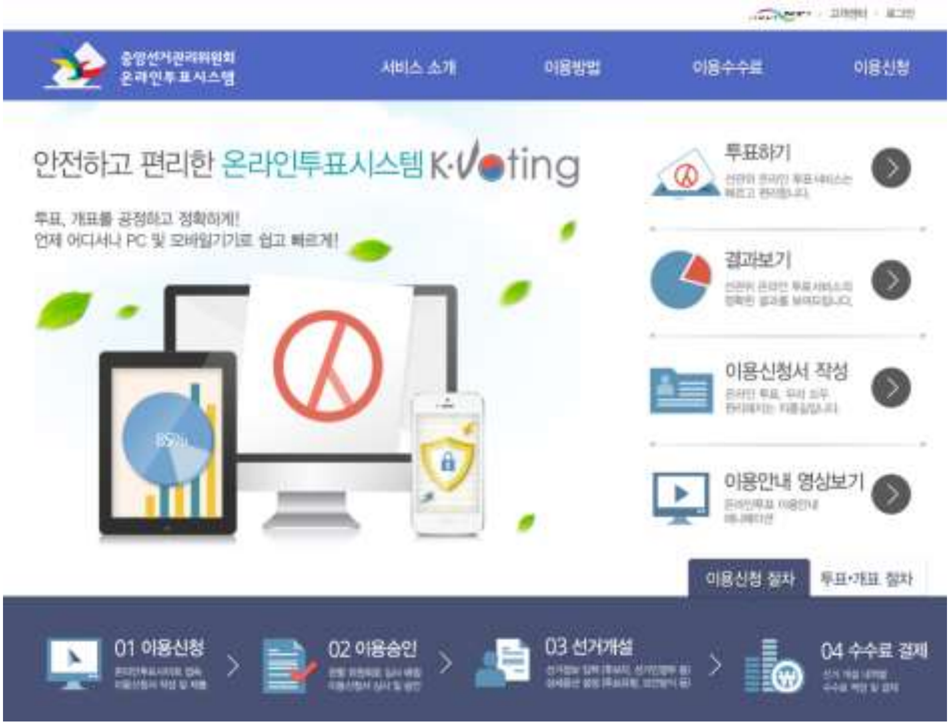
2.2. Case Studies

2.2.1. Domestic Online Voting System K-Voting

The online voting system replaces the existing voting method, *i.e.*, visiting the polling place in person, going through the identification process, filling out the voting paper, and putting it in the ballot box, and helps voters use PCs and mobile communication terminals to express their opinions and elect representatives in the web and mobile environment anytime and anywhere [5]. It also makes it possible to hold various ballots, *e.g.*, general preferential voting and aye and no votes, efficiently and safely so that people’s intentions can be correctly reflected in selection of board members, revision of the articles of incorporation and making decisions on agendas. Like the conventional election method, voters’ basic rights, *i.e.*, the principles of universal suffrage, equal suffrage, direct vote and secret vote, must be guaranteed throughout the voting process.

The National Election Commission has been operating the online voting system K-Voting since October 2013, and K-voting is utilized not only to elect the representatives of communities like schools, apartments, villages and cooperatives, but also to gather opinions on certain agendas and make policy decisions [6]. Also, the National Election Commission supports the online voting system in election of representatives of political parties and nomination of presidential candidates.

Online voting provides the convenience of voting regardless of time and place, and has a big advantage, *i.e.*, cost reduction. But nevertheless, it is not widely used in Korea yet.



안전하고 편리한 온라인투표시스템 K-Voting

투표, 개표를 공정하고 정확하게!
언제 어디서나 PC 및 모바일기기로 쉽고 빠르게!

Figure 1. Online Voting System ‘K-Voting’[6]

2.2.2. Republican Presidential Nomination in Utah, US

The online voting system of the blockchain method was used in the process of nominating the presidential candidate for the Libertarian Party in Texas, US and nominating the presidential candidate for the Republican Party in Utah, US in 2016. It was announced that more Republicans of Utah registered online to exercise their right to vote because of the convenience of the blockchain technology. In the past, citizens living overseas, e.g. overseas travellers, missionaries and soldiers, used to receive ballots in the mail, but online voting utilizing the blockchain is said to have simplified the registration to vote and the voting process. As for the voting method, voters can visit the polling place to vote as previously, or visit the website of the Republican Party (utah.gop) and vote between 7:00am and 11:00am (local time), and if voters preregister for the online voting system, a unique PIN code will be sent to the voters’ cell phone or e-mail on the day of system election. UK-based Smartmatic, which provides online voting solutions, used end-to-end encryption and the private blockchain to provide the online voting infrastructure [7].

About 10,000 out of 40,000 Utah residents, who voted online on the day of voting, said they had difficulties in the authentication stage. It turned out that most voters received the PIN code as a spam message, or they were not pre-registered properly in the pre-registration stage, but thought they completed pre-registration.

2.2.3. Estonia

Among the 40 or so countries around the world that are practicing electronic voting, Estonia is a country that is practicing the most advanced Internet voting. Estonia is a small country with a population of 1.34 million. As a result, Estonia can manage and carry out government policies more easily than other countries. It is a powerhouse in not only Internet voting, but also in electronic democracy. It is carrying out various electronic democracy programs and attracting global attention.

Estonia implemented the web-based voting system, which allows Internet voting, back in 1999, and made it possible to do the early voting on the Internet. In the past, as it was likely that only young voters can participate in Internet voting due to digital divide, people raised an issue of violation of equal suffrage. And other issues were raised as well, *e.g.*, hacking and violation of the principle of secret election, but in Estonia there are fewer voters who are not familiar with digital methods due to the high level of informatization than in other countries. Therefore, despite the issues raised above, electronic voting is introduced due to its positive effects on increasing voter turnout and democracy [8].

As most citizens have an ID card with the digital certificate, Estonia could implement the blockchain-based voting system. The block diagram of Estonia's online voting system is shown below.

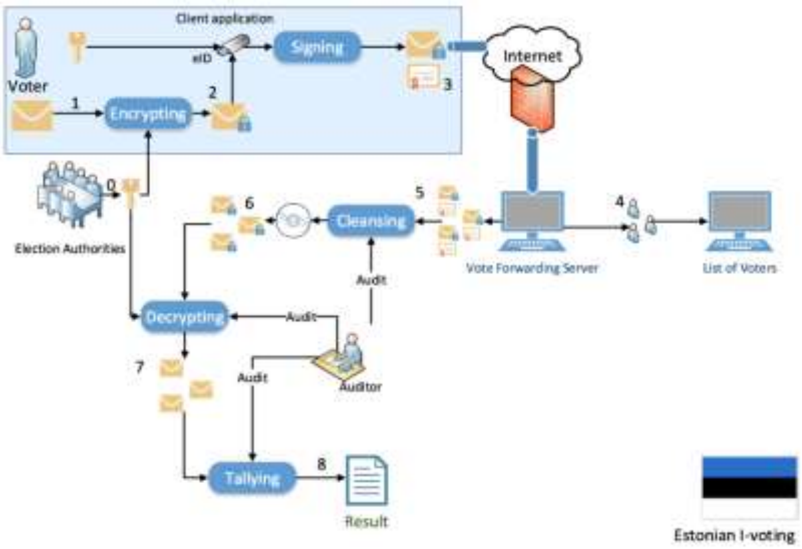


Figure 2. Block Diagram of Estonia's Online Voting System [8]

2.3. Advantages of the Online Voting System using the Blockchain Method

If the blockchain method is applied to the online voting system, it will be possible to implement electronic management, *e.g.*, recording and storing the right to vote in the blockchain. It can also be used to check whether voters voted or count votes, making election management more efficient. The advantages of the blockchain-based online voting system are as follows:

- Time and cost reduction

The blockchain-based online voting system can reduce time and cost compared to conventional voting. According to the existing voting method, it takes some time before the ballot counter counts all the votes, but if the voting is done on the blockchain server, it will be possible to see the voting result immediately after voting. So it is not necessary to wait for the voting result to come in after a certain time. As a matter of fact, the blockchain-based online voting system was used in the Republican presidential nomination in Utah, US, which was examined above, and it was confirmed that the voting process was simplified. Also, due to the simplified voting process, voting costs can also be expected to be reduced. The blockchain-based online voting system can reduce the cost of voting and ballot counting compared to that of the conventional voting method, and unlike the existing online voting system, the blockchain-based online voting system can also reduce the cost of implementing the central server and the security system.

- Increased participation of citizens

The blockchain-based online voting system can increase citizens' participation in voting. Everyone finds it difficult to participate in the current direct voting, but if the blockchain is used for voting, it will be possible to overcome physical limitations, and more people can participate in the policy-making process. In the Utah case examined above, most Utah residents are Mormons (the Church of Jesus Christ of Latter-day Saints), and many of them are living overseas for missionary work. So they relied on mail voting. However, registered voters, who have a smartphone, tablet or PC, could access the platform and vote online easily regardless of their actual location. Also, as the online ballot paper provided a link to the information on each candidate, they could get information more easily and faster than in the conventional voting.

- Security and reliability

With regard to the online voting system, there are concerns about the secrecy of voting, the personal information security issue and the abuse and fabrication of the right to vote. However, the decentralized information sharing system of the blockchain can secure integrity and security on its own. In the conventional online voting system, as the central server and the central database manage and process voting values, there is a high risk of fabricating voting result. In the blockchain-based online voting system, not all voting values are stored in the central server and the central database, but they are disclosed to everyone participating in the voting on the P2P (Peer to Peer) distributed network. So voting can be done transparently.

Also, in the blockchain-based online voting system, voting values are connected together using the keys and hash functions of other voting values. So it is impossible to arbitrarily modify or omit them. Since one-way calculation, i.e. obtaining the hash value from data, is easy, but inverse calculation is very difficult, the input value cannot be inferred or calculated no matter what method is used. In other words, as for the connection of blocks of voting details, the current block includes the hash value of the previous block. So it is difficult to forge or alter them, and voting can be conducted transparently

3. Analysis of Issues when Blockchain is Applied to the Online Voting System

3.1. Problems of the Old Online Voting System

Online voting brings to voters the convenience of voting without any restriction in time and place, and reduces costs. Despite these advantages, it is not widely used in Korea yet. Online voting goes through the following processes: 1) voter registration after identification 2) viewing agendas 3) voting and 4) viewing the voting result [9].

For people to trust the voting method, the method must be safer and correct. And it must be proven that the voting results correctly reflected the intentions of the voters. The following problems may occur in online voting. For starters, in the identification process, problems occur during non-face-to-face authentication to see if the voter is a registered voter. There are other problems, such as the forgery and alteration of voting results due to cyber attacks during the voting process, and system shutdown due to power failure or natural disasters. There also may be a problem with guaranteeing the secrecy of voting details to voters. If voting is carried out in an online environment in which personal information can be leaked, others' personal information may be stolen, and used for voting by proxy and repeated voting, and there may be a security problem with regard to guaranteeing the secrecy of voting. Lastly, voting results may be fabricated, and if there is distrust of security, trust in voting results cannot be guaranteed either.

3.2. Domestic Laws and Institutions Issues when the Blockchain Technology is Utilized

In most democratic countries, elections abide by the 4 basic principles, *i.e.*, universal suffrage, equal suffrage, direct vote and secret vote. Universal suffrage is a principle that gives the suffrage to all citizens who are a certain age or older. In Korea, all adults aged 19 or older can participate in election. Equal suffrage is a principle that one man can cast one vote regardless of conditions, e.g. status, property, gender and academic background (one man, one vote). Direct vote is a principle that other cannot vote by proxy, and voters themselves must vote in person. People identify themselves at the polling place before receiving the ballot paper. This is an example of direct vote. These five principles of election and the legal and institutional issues that may occur if the blockchain-based online voting system is used in Korea can be summarized as follows:

- The issue of the direct vote principle

Examining overseas examples of introducing the blockchain-based voting system, the procedure for identifying voters is complicated. Public certification ID cards, containing voters' unique information, are recognized by designated readers, or PIN number authentication and bank information are used for identification. According to the Public Official Election Act of Korea, however, electors must show their ID cards, passports, driver's license or public official ID cards to voting witnesses at the polling place, and go through the fingerprint recognition process or affix their digital signature. If remote voting is carried mobile or on the tablet, however, it may be impossible to check if voters have their own ID cards, or others have it.

- Issues of the secret vote principle

If remote voting is carried out, there are a few problems that are more likely to violate the principle of secret vote than the existing voting method. As there is no voting witness, it is difficult to control the behavior of electors. Therefore, it is difficult to check what is described in Article 166-2 and Article 167 of the Public Official Election Act. When voting using electronic media, electors can be prevented from capturing the screen technologically, but it is difficult to check if they photograph the screen itself. Also, as a voting booth is not separately installed as in the existing polling place, there is no checking whether voting secrecy is guaranteed or infringed by others. If people are forced to vote by others, the one-man one-vote principle will be violated. So it may violate the equality principle as well as the secrecy principle.

- Issues of ballot counting

According to the Public Official Election Act, when ballots are counted, the number of votes received by each candidate cannot be reported before official announcement. In the blockchain-based voting system, however, the voting process itself is done electronically. So as soon as ballot counting starts, the rate of votes earned and results may be exposed.

3.3. Technical Status and Issues when the Blockchain Technology is Utilized

In the online voting system, users vote freely in the space they desire without any monitoring agency. So checking whether the person identified on the network is actually the same person as the voter and ensuring that voters are voting by their own free will are important factors. Also, voters' voting information must be correctly delivered to the ballot counting process without any error, and votes must be counted correctly and quickly. The following issues may be raised when the blockchain technology is applied to the online voting system:

- The blockchain-based voting technology as examined by way of overseas cases

If the voting system is implemented on public networks that already exist, the elector authentication system and the information protection system must be implemented separately. So most voting systems are implemented on private networks. In overseas cases, we analyzed what kind of technology was used in the voting process, and how the blockchain is introduced is examined below.

(Identification of electors) In most countries, electors are identified using their name, birthdate, unique ID number and certified electronic ID card. Uses are identified using the multi-factor identification method, not a single factor, to increase trust in voting. As the electronic identification method is relatively less trustworthy, voting witnesses directly identify voters as in the existing polling place.

(Voting) Voting is carried out using digital medias, e.g. using mobile devices and PCs. Voting details are stored in the blockchain after they are encrypted with electors' digital signature, the ballots are scanned, and recorded in the blockchain. It can be referenced as a case of overcoming the weaknesses of conventional online voting and remote voting.

(Ballot counting) In the ballot counting process, ballot counting qualifications are verified before voting. Once confirmed, the key of the manager (national and regional) used for decryption and the voting results are checked. In most countries, the chain is divided into two. One is the chain for calculating the voter turnout, and the other is a chain containing the information on which candidates they voted for. This technology was devised to guarantee the anonymity of electors.

- The problems of anonymity

In small and medium-sized civilian election and political party voting in which secret voting is not an issue, the blockchain-based voting system may not be a problem. But on a national scale, *e.g.*, general elections and presidential elections, it can be tracked. So the secret vote principle may be violated.

In the blockchain, as personal information is not linked to the public key or personal key, anonymity can be guaranteed. As all participants share the ledger in the blockchain, however, if electors' personal information is used for authentication, elector information and voting details may be estimated, which may be a problem.

- Key management problems

As in the existing public certificate system, the blockchain uses the private key for digital signature when using the asymmetric key encryption system to upload transactions to the blockchain. To prove that electors themselves voted in the voting system, electors' personal key is used. In the process of generating encryption keys used in voting, or in the process of providing them, there is a key management issue. It will be necessary to safely manage keys by deciding whether electors themselves should manage keys, or an official institution like the National Election Commissions should manage keys.

3.4. Implications

This study confirmed that there are institutional and technical disputes in Korea with regard to introducing the blockchain-based voting system. Examining the cases of countries or enterprises that already introduced the blockchain technology, they were introducing many technologies to ensure the reliability of the identification procedure or the voting procedure. As the blockchain technology supports integrity, it was expected that it could enhance the reliability of voting. However, it cannot solve the issue of the anonymity of election, forced voting, which was an issue with conventional electronic voting, and digital divide. Also, there are a few legal and institutional issues. Even if these issues can be solved technologically, introducing the distributed technology may be a problem according to the current laws. To introduce a safe voting system, it seems necessary to revise and enact the laws.

4. Suggestions for Introducing the Blockchain-based Online Voting System

As examined above, to apply the blockchain technology to the online voting system, institutional and technological issues must be solved first. This paper makes institutional, technological and policy proposals for introducing the blockchain-based online voting system to Korean elections to solve these problems.

4.1. Systematic Suggestions

- Reviewing alternative means of identification

The biggest problem of the online voting system is the identification procedure, e.g. whether the voter directly voted and whether the voting process was carried out secretly. The Public Official Election Act stipulates that the voter should submit his/her ID card to the voting witnesses and have it confirmed by the voting witness. As the online voting system has technological limitations in complying with this provision, however, Paragraph 2 of Article 152 of the Public Official Election Act needs to be amended. That is, it seems necessary to revise the legal provision that “the voting manager may issue the electoral register number to electors who identified themselves and signed or sealed the electoral register and allow them to vote,” and review a non-face-to-face identification procedure or a system that can replace it.

If online voting is still believed to be unstable, alternatively the blockchain voting system, which allows voters to visit the polling place in person as now, and makes sure that voting results are recorded in the blockchain at the site, can be implemented.

- Reviewing the digitalization of the voting and ballot counting system

As elections for public offices must comply with the Public Official Election Act, to introduce the blockchain technology to the election system, the Public Official Election Act needs to be amended. As described in Article 278 of the Public Official Election Act (Voting and Counting of Votes by Computer System) introducing the online system to voting is not prohibited. Chapter 16-2 Special Cases of Electronic Voting and Ballot Counting of the Elections for Public Offices Management Rules mentions that electronic voting requires an electronic voting machine in elections for public offices. To implement a safer voting system, the law requires that the requirements of the online voting system must be more specific.

4.2. Technical Suggestions

- Implementing the blockchain platform for public service

To carry out public official voting systematically, a stated public service platform must be implemented first. Security and trust are more important than anything else in public service as well as elections. Therefore, it is proposed to use the core blockchain technology to implement a standard platform for the government and public service. It is necessary to develop it into an open platform, and help public institutions, which want to introduce the blockchain technology, easily develop service. It is proposed to gradually expand the blockchain as a national infrastructure to various government systems.

In particular, as the online electronic voting system violates the secret vote principle, it is a good idea to implement the voting system separately. It is known that the blockchain can guarantee anonymity with the current technology, but as everyone shares voting details, secrecy is not fully guaranteed. Accordingly, when the blockchain is implemented for the first time, it will be a good idea to separate electors and voting results so that they cannot be matched.

- Designing the agreement structure for public service

The agreement structure in the blockchain is the most important. Here, the agreement structure can be largely divided into two. The first is the agreement structure that goes into action when we determine which information will be stored in the block in the process of creating blocks. Bitcoin has a structure in which if information is recorded in 51% of the server currently participating in the bitcoin network, that information is confirmed as authentic. The second is the agreement structure related to modifying the logic applied to the blockchain and the policy task, *i.e.*, the code of the blockchain itself. In most cases, there is no clear rule as to how to reach an agreement about the operational problems of most blockchain projects in existence, including bitcoin, addition of functions and policy changes. Accordingly, to apply the blockchain technology to public service, especially the voting system, it is necessary to implement the decision-making structure with regard to the operations in the design process.

4.3. Policy Proposals

- Pilot projects led by the public sector

As the blockchain technology can be expected to be very effective in terms of transparency of transactions, if it is applied to voting, the characteristics and advantages of the blockchain can be put to good use. Furthermore, as voting results can be checked immediately after voting is completed, voting management expenses will be drastically reduced, and controversies over corruption or fabrication in voting can be resolved. So unnecessary wasteful arguments can be reduced. In that voting must be fair and reliable, however, it is necessary to secure infrastructure that everyone can trust. Therefore, the state, not enterprises or the private sector, must build a reliable infrastructure. After the infrastructure is built, best practices must be secured through pilot projects. Public service requires a high level of security and stability. As it is more so when it comes to voting, the private sector may have some difficulties building this infrastructure. It is necessary to utilize the core blockchain technology to build a standard platform for the government and public service, and apply technologies that can satisfy various compliance schemes at home and abroad.

Furthermore, it is necessary to enter into an MOU with the US, Canada, Germany and Estonia, which have many cases. In particular, it will be necessary to share best practices with countries which has many cases of advanced blockchain service based on public service projects, and develop them in a way fit for the domestic environment.

- Utilizing the conventional K-voting service

K-voting service is not used in elections for public offices, but small organizations are benefiting from it. It makes it possible to participate in apartment building representative elections and the voting to elect representatives of various organizations anytime and anywhere.

The blockchain makes sure that individuals' voting participation records and voting results are not matched. As the server is located at the center in the conventional online voting system, the possibility of fabricating or altering voting results is raised. Therefore, to implement a safer online voting system, the introduction of the blockchain technology may be introduced to enhance security.

As K-voting currently provides services necessary for online voting, *e.g.*, making the electoral register, candidate information collection, voting media determination, authentication method, voting preparation, election ballot counting, and viewing the result of ballot counting, it is proposed to introduce the blockchain to existing processes on a pilot basis.

5. Conclusion

As examined above, the blockchain-based voting system has several advantages. Above all, its biggest advantage can be the fact that voting results cannot be forged or altered. Also, as it is possible to check voting results immediately after voting is completed, management costs can be drastically reduced. It can reduce unnecessary wasteful arguments by eliminating controversies over corruption or fabrication of voting.

If the blockchain technology is utilized, it is possible to implement a system that you like, *e.g.*, online voting and secret voting. In other words, another advantage of the blockchain is provision of a flexible method fit for the purpose of voting. If you find voting results being disclosed in real time, and affecting voting result to be burdensome, it is possible to disclose results at the closing time if necessary.

The introduction of blockchain to the online voting system means that the blockchain-based online voting system can perform more functions than existing online voting system. The blockchain basically has fairness, transparency and certainty. Therefore, if you start with small and medium-sized voting, and further expand it, it will be actively used in elections, which requires trust and transparency most frequently. The authors will study methods of applying technology and infrastructure so that the blockchain technology can be applied to the online voting system.

References

[1] Heon Woo Yoo, “A Study on Performance Improvement and Implementation of Electronic Voting System using Blockchain”, Master’s thesis on information protection, Graduate School of Information technology, Ajou University, **(2016)**.

[2] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, http://bitcoin.org/bitcoin.pdf, **(2008)**.

[3] Security Technology Team, Security Research Department, Financial Security Institute, “Blockchain and Bitcoin Security Technology Report,” Security Research Department-2015-029 **(2015)**.

[4] Lee, Jong-Ki, “An Exploratory Case Study of Distributed Ledger Processing Using IBM Bluemix Blockchain,” Korean Computers and Accounting Review, Vol.15 No.1, pp. 25-38**. (2017)**.

[5] Cho Hee-jeong, “Electronic Democracy and Internet Voting: with focus on the case of Estonia,” Korean Association of Party Studies Journal Volume 7 Issue No. 2 Serial No. 12 **(2008)**.

[6] National Election Commission Online Voting System (http://www.kvoting.go.kr).

[7] National Information Society Agency, “Major Cases of Electronic Voting Utilizing the Blockchain and Implications,” National Information Society Agency Special Report **(2017)**.

[8] Andrew Barnes, Christopher Brake and Thomas Perry, “Digital Voting with the use of Blockchain Technology,” Computing with Plymouth University (https://www.economist.com/sites/default/files/plymouth.pdf).

[9] Lee Roo-da, “Implementing the Electronic Voting System Utilizing the Blockchain,” Master’s thesis, Department of Computer Science, Graduate School, Sangmyung University,” **(2017)**.

[10] The Public Official Election Act, National Law Information Center (http://www.law.go.kr/lsInfoP.do?lsiSeq=195320&efYd=20170726#0000).

[11] Jeon Myeong-san, “Blockchain Government,” Alma Publishing Company **(2017**).