Electrical Engineering and Computer Science

# A Review Regarding Electronic Voting Schemes That Utilizes Blockchain For A Higher Security And Confidentiality

Suwhoan Lim[1]

Heung-No Lee[2]

3

[1] Gwangju Institute of Science and Technology (GIST College), S.Korea, suwhoanlim@gist.ac.kr

[2] School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology (GIST College), S.Korea, heungno@gist.ac.kr

# Abstract

Voting is perhaps the most important component that comprises modern-day democracy. By having a secure, trustable voting process, people then can express their opinions anonymously, without the fear of someone realizing to whom the ballot belongs.

A disadvantage that such a traditional paper voting scheme holds is that there must exist a person or a group of people organizing the entire voting process. This is because once a voter expresses their opinion on a paper ballot, the ballot must then be stored, collected, recorded, and announced. Usually, such a process is done by a single organization. For the results of the voting to be clear and reliable, the participants are forced to trust this organization who is doing all the work behind the curtain. This organization is referred to as a Trusted Third Party, and they were often accused of fraud in a vote, whether the fabrication happened or not.

To remove such an entity's existence, people have been trying to incorporate a voting scheme with a blockchain and perform it online. To guarantee that the online ballots are not fabricated a put under a constant watch, people are trying to utilize a blockchain technology when performing electronic voting.

Nevertheless, although blockchain does provide strong immutability and security, it does have a potential risk of getting compromised. Moreover, there are qualifications that an electronic voting scheme must satisfy. One of such qualification is that any information stored on a ballot must remain secret. Nonetheless, a blockchain is a public, distributed ledger. In this review report, we shall discuss the principles of e-voting and look through different pieces of literature to see what kind of research was done by the people to make a blockchain e-voting scheme possible.

# 1. INTRODUCTION

Undeniably, voting and its liability is a crucial component of modern-day democracy. It is not only a means of selecting a representative of the people but also a way to express the commons' opinion on issues varying from 'what to eat for lunch' to 'which regulation should be enforced on the next fall season'. A well-designed voting scheme helps to mitigate unnecessary quarrels between people since it allows people to weigh in on somewhat controversial topics anonymously while keeping their rights to speak up.

One thing that is assumed on most of the voting system is that the participants must believe whoever is conducting the vote will be honest about everything going behind the scene. For instance, picture a small election choosing a classroom representative at an elementary school. The trusted third party, in this case, will be the teacher. In other words, the students will believe that the teacher will not change the ballots, reveal who vote to whom, and more.

Nevertheless, having a Trusted Third Party (TTP) during the voting process naturally, makes people ask this one question; Can we trust this so-called Trusted Third Party? Surely, having such a party lubricates the voting process, but it is also reasonable to argue that the party may be compromised, attempting to fabricate the result. It has been a controversial issue and no matter how clear the voting process was, there is often a dispute among people blaming the Trusted Third Party claiming that a fraudulent act was done during the Korean General Election held in April 2020. [1] To eradicate such protests, people have tried different voting schemes. This is where the blockchain and an idea of a decentralized voting scheme come into play.

Blockchain can be explained as a decentralized ledger, where every participant keeps a record of every transaction done on the network. Since the ledger is distributed and each participant has an exact copy, they can compare the hash value of each block to make sure the ledger is not fabricated by an attacker. Moreover, the consensus algorithm such as Proof of Work (PoW) or Proof of Stake (PoS) allows each node to verify a new block once it's mined. Blockchain combined with several other techniques such as Zero-Knowledge Proof (ZKP) and others, an electronic voting scheme seems like a plausible option that can substitute the classic hand-to-paper voting scheme.

This paper aims to introduce and review some of the blockchain e-voting schemes that has been introduced to the field. The articles are not only limited to a published paper but also varies from a patent to a filed-test report. They will be closely examined based on how well do they satisfy the principles of e-voting. More importantly, this report shall depict some of the possible flaws that may occur in a blockchain e-voting system in advance and then talk about how each article either solves or lacks providing a breakthrough to the issue.

# 2. KEY CONCEPTS

In this section, some key concepts that need to be pondered while reviewing the articles will be introduced. Starting from a brief discussion about an innate limitation of blockchain, we shall be looking deeper into possible problems that may occur from the implantation of the voting scheme into the blockchain. Since each point discussed in this section is intimately linked with any shortcoming of the blockchain e-voting scheme, it will be a good idea to ponder on these issues before reading through each of the articles.

## 2.1. Byzantium Generals Problem

A group of generals is trying to break down a castle. Nevertheless, the castle stood so firmly that it will fall only if a certain amount of generals all attack at the same time. Spread around the castle, the generals send out messages to one another. ‘Will you join me on an attack on Friday morning?’, or ‘Let’s break them down on Thursday afternoon’. The catch is, there is a spy from the castle eavesdropping onto the message and fabricating the content of the message, say from Friday to Saturday, or not deliver the message at all. In addition to that, some generals have been bribed by the castle defender. They will either initiate an attack on a wrong day, thereby compromising the integrity of the force, or not attack at all. In such a case, can the generals come up with a trustless solution on which message to believe, and decide on a minimum number of honest generals to win a battle? This is the Byzantium Generals Problem, and answering these questions is not easy.

Most of the blockchain networks use a consensus algorithm to solve the Byzantium Generals Problem. That is, they will only accept a new block only if certain conditions provided by the consensus algorithm are met. The significance of resolving the Byzantium Generals Problem comes from the fact that it is closely related to the overall security of the network. For instance, no one will trust the network and the contents stored inside the block if they cannot guarantee the validity of each block. The same goes for the e-voting system. By having a consensus algorithm to prevent the Byzantium Generals Problem, the participants (i.e. voters and candidates) may be relieved from the corruption of the voting results.

## 2.2. Blockchain Trilemma

A blockchain trilemma refers to three key components of a blockchain. Each point is a crucial aspect of blockchain that cannot be sacrificed, but each element makes it hard to fulfill the other element. They are; Scalability, security, and decentralization. Each aspect has something to do with the fact that 1) each block has a finite size, 2) transactions stored inside the blocks are encrypted and finding a proper hash value takes a lot of computational power, and 3) each node must communicate with each other to accept and validate a newly generated block.

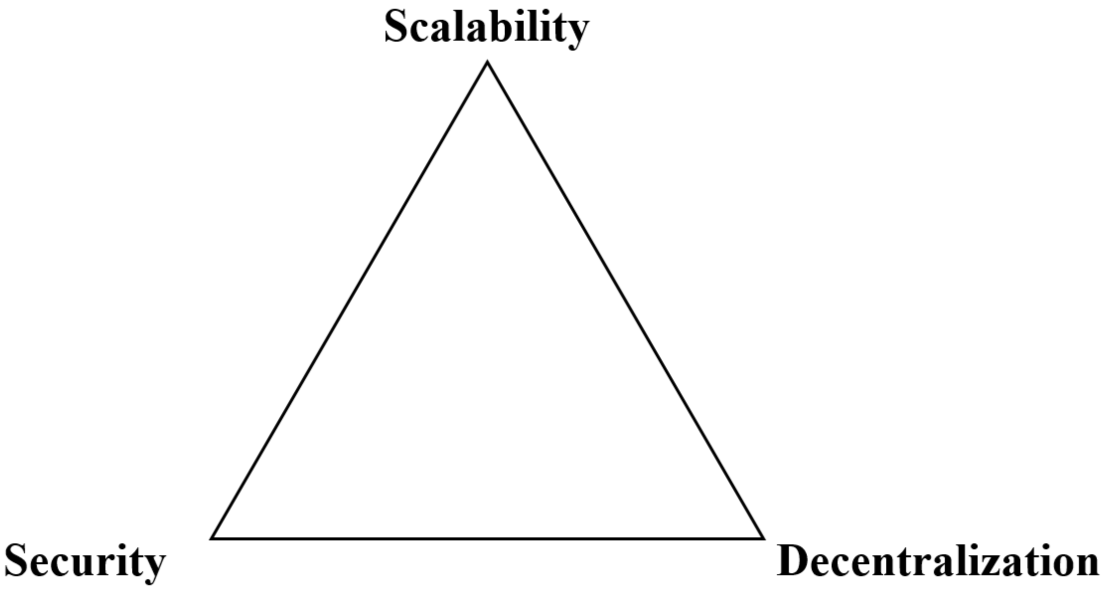

***Figure 1. Blockchain Trilemma. It is widely accepted that it is either extremely hard or even impossible to fulfill the three criteria at the same time.***

Let’s look at some examples to examine how each component hinders each other. To store more data or increase the number of transactions processed per second, one needs to decrease the level of difficulty in computation or reduce the number of participants to speed up the validation process. To make a system more secure, an additional method of block procession or validation must increase, which makes it computationally difficult and consumes more space on a blockchain. To make a blockchain more decentralized, one should reduce the security level so that more people can join the network. Reducing the size of a block might also be helpful since then the blocks can be distributed more efficiently. Although these are just simple illustrations, the trilemma itself has a significance in an e-voting scheme. Since each electronic ballot has its size and adequate encryption, it carries non-negligible size in memory. Moreover, the ballots must be protected from an eavesdropper before the counting. Last but not least, to remove the need of a trusted party and accepted by the participants, it must stay in a decentralized manner. It will be an important factor to see how each literature approach to solve this trilemma.

## 2.3. Trusted Third Party

Perhaps the most important reason why people are trying to incorporate blockchain into the e-voting system is to remove the existence of a trusted party in a voting scheme. Like mentioned in the introduction, having a Trusted Third Party may be a quick and easy solution since they will take care of the works that need to make the result reliable. Nevertheless, it innately yields one critical problem; we need to trust the trusted party! Think about how an untrustworthy party can sabotage the output of the vote. Not only the results may be completely different but also the participants may not even know that there was a fraudulent act done behind the scene. This is where the blockchain and its characteristic of immutability shines.

The Trusted Third Party mainly serves two purposes in a voting process. For one, they collect and keep the data until it is the right time to count. Secondly, they make sure that the ballots are kept unchanged once it leaves the hands of a voter. Blockchain is introduced to serve the second purpose of the Trusted Third Party. Since the contents inside a blockchain cannot be altered in anyways, the voters may rest assured that the results will remain the same.

Providing a breakthrough to the first purposed is a bit more complicated. Since a blockchain is a distributed ledger, everyone who has access to the network can see the contents inside the blockchain which in this case is who votes to whom. Various techniques such as Zero-Knowledge Proof or Homomorphic Cryptography has been used to counteract this problem. After reviewing each literature, we shall be grouping the literature depending on their usage of a different approach to solving the first purpose of the Trusted Third Party.

## 2.4. Principles of Electronic Voting

The National Election Commission of South Korea has announced a guideline that an online voting scheme must follow. Their original words in Korean and an English translation goes like the following. [2]

| Principle Number | Principle | Explanation |
|---|---|---|
| [P1] | Preciseness | All valid ballots must be included in the result. |
| [P2] | Verifiability | A method of verification to distinguish faulty ballots must exist. |
| [P3] | Completeness | An attacker must not be able to sabotage the voting process. Any faulty ballots must not be included in the result. |
| [P4] | Uniqueness | An unauthorized voter must not be able to vote |
| [P5] | Legitimacy | A legitimate voter must have the right to vote once and only once. |
| [P6] | Confidentiality | Relation between a voter and a ballot must remain secret. |
| [P7] | Fairness | A result during the voting must not have an influence to the rest of voting. |

***Table 1. Seven Principles of Electronic Voting asserted by the National Election Commission of South Korea translated in English. Each property is closely related to the conditions an electronic voting scheme must follow.***

The principles represented above are not only the fundamental principles of an election but are also additional conditions that an e-voting scheme must follow to prevent a possible attack. Because an e-voting scheme does not use the traditional method of pen and paper to collect the ballots, it seems plausible that adequate measures must be taken to prevent further problems. Below ideas that must be considered when implementing a new e-voting scheme is introduced. While some of the topics are meant to be applied to a general e-voting system, some portion of the questions are specifically designed to aim at a blockchain e-voting scheme.

| Principle Number | Principle | Possible questions |
|---|---|---|
| [P1] | Preciseness | ➢ Are transactions correctly transmitted to the block generators and stored in a block?<br>➢ Are transactions not omitted during the transmitting phase? |
| [P2] | Verifiability | ➢ Is there a method for miners or any individuals with right authority to validate a ballot to confirm that the ballots are not fabricated in any way? |
| [P3] | Completeness | ➢ Is there a way to prevent an unintentional / deliberate attacks regarding a faulty ballot? |
| [P4] | Uniqueness | ➢ Does the scheme provide a secure method of voter registration?<br>➢ Can the scheme detect and exclude a ballot from an unauthorized voter? |
| [P5] | Legitimacy | ➢ Does the scheme provides each voter with an equal, non-fungible, non-transferable right to vote only once? |
| [P6] | Confidentiality | ➢ Does the scheme guarantee that everyone, whether or not they are a participants of the voting scheme, knows nothing about which ballot belongs to which personnel? |
| [P7] | Fairness | ➢ Does the scheme guarantee that everyone, whether or not they are a participants of the voting scheme, knows nothing about real time vote results before the deadline? |

***Table 2. Seven Principles of Electronic Voting asserted by the National Election Commission of South Korea and possible questions to consider when implementing an e-voting scheme.***

Looking closely into each of the components, one can see that the traditional paper voting scheme does a pretty good job of satisfying the last four elements. Nevertheless, since each ballot from the traditional method is put in a box where the ballots become indistinguishable, the traditional methodology fails to meet the first three criteria. In other words, there is no way anyone can track down which ballot was from who from the vote-counting phase. This adds strong security in terms of [P6] and [P7].

On the other hand, an e-voting scheme using blockchain may provide a breakthrough in providing numbers [P1] to [P3] a solid foundation. Immutability of a blockchain will not only be a clear guarantee that the contents stay intact but also a digital signature appended on the ballots will be a good aid against [P2] and [P3].

# 3. Literature Review

## 3.1. Literature introduction

To check upon the development of the blockchain e-voting scheme after the introduction of blockchain technology, a few articles have been selected and will be introduced in this section. To maximize the report's purpose, which is to show the flow of the development of blockchain e-voting technology, the literature was selected from various sources. The sources include published paper, blog article, and patent. Anything that is outdated, lacks novelty or theoretical background has been removed from the list.

| Authors | Ref. No. | Literature No. | Title | Publication type | Research Process Stage |
|---|---|---|---|---|---|
| McCorry et al. (2017) | [3] | [L1] | A Smart Contract for Boardroom Voting with Maximum Voter Privacy | Conference Paper | Prototype |
| Rifa Hanifatunnisa et al. (2017) | [4] | [L2] | Blockchain Based E-Voting Recording System Design | Conference Paper | Concept |
| Sandberg-Maitland et al. (2020) | [5] | [L3] | Threshold secret share authentication proof and secure blockchain voting with hardware security modules | Patent | System Architecture |
| Ryan Uhr et al. (2018) | [6] | [L4] | Method for providing secret electronic voting service on the basis of blockchain with merkle tree structure by using zero knowledge proof algorithm, and voting coin minter server, voting token distributor server and voting supporting server using the same | Patent | System Architecture |
| City of Zug (2018) | [7] | [L5] | Evaluation of the blockchain vote in the city of Zug | Report | System Architecture |
| DongHeon Lee (2019) | [8] | [L6] | Blockchain based E-Voting System Suggestion for a Fairer Election | Blog Article | System Architecture |

***Table 3. Total of six literatures from four different sources will be discussed in this report. The***

***selection of the literatures was made based on novelty, depth of theoretical background, and feasibility of the scheme introduced in each of the paper.***

Given these pieces of literature, we shall be looking through which specific problem did they tried to solve and what key elements have they adopted to solve the problem. The analysis will be followed by a deeper exploration of which principles of electronic voting did they solved and which they did not.

## 3.2. Literature Analysis

In this section, we shall be diagnosing each of the literature, especially looking closely at 1) Problem they aimed to solve, 2) their solution on solving the particular problem, 3) principles of electronic voting they have solved, and 4) principles of electronic voting that they did not quite manage to fulfill. The below table discusses the points just mentioned.

| Literature No. | Problems | Solution / Key Technology | Solved Principles | Unsolved Principles | Unanswered Principles |
|---|---|---|---|---|---|
| [L1] | Scalability, Confidentiality | Self-tallying protocol, Open vote protocol, Non-Interactive Zero Knowledge Proof (ZKP) | P1, P2, P3, P5 | P6, P7 | P4 |
| [L2] | Immutability, Security | Blockchain | P1 | P6, P7 | P2, P3, P4, P5 |
| [L3] | Confidentiality | Threshold Secret Sharing Scheme | P1, P4, P5, P7 | | P2, P3, P6 |
| [L4] | Immutability | PU/PR Key Pair Encryption, Zero Knowledge Proof | P1, P2, P6, P7 | | P3, P4, P5 |
| [L5] | Security, Confidentiality | Homomorphic Encryption, Digital Signature, Client-side Encryption, Zero Knowledge Proof | P1, P2, P3, P6 | P7 | P4, P5 |
| [L6] | Confidentiality | Receipt | P1, P5, P6 | P2, P3, P4, P7 | |

***Table 4. An analysis of each method based on their target problems, key solution to the problems, principles they have managed to solve, principles that cannot be solved by the suggested solution, and principles that are either not clearly mentioned or are not incorporate in the literature.***

A deeper explanation of the tables and things that must be emphasized will be discussed in the Literature Discussion section. Below are the figures illustrating the different types of technology used and how frequently have they been used. Figure 2 shows the frequency of each technology’s usage, and figure 3 shows which principle of electronic voting the technology was used.

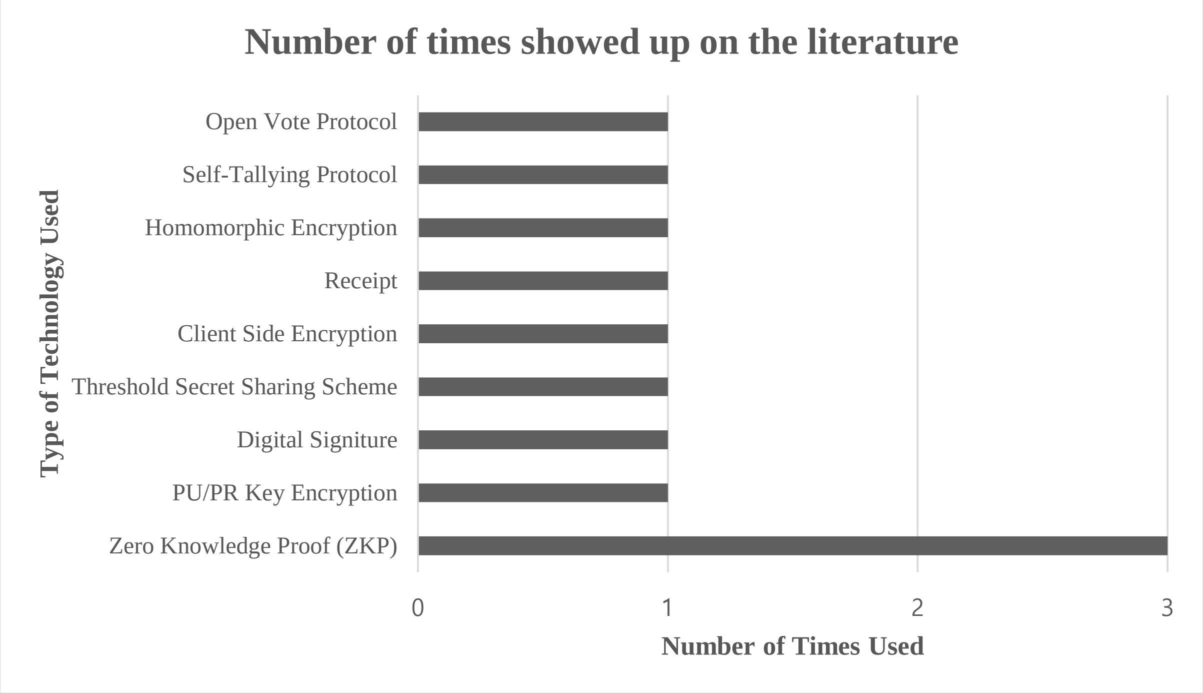

***Figure 2. Analysis of different types of technology and their number of appearance in the literatures. The technologies shown in this figure is introduced in Table 4.***

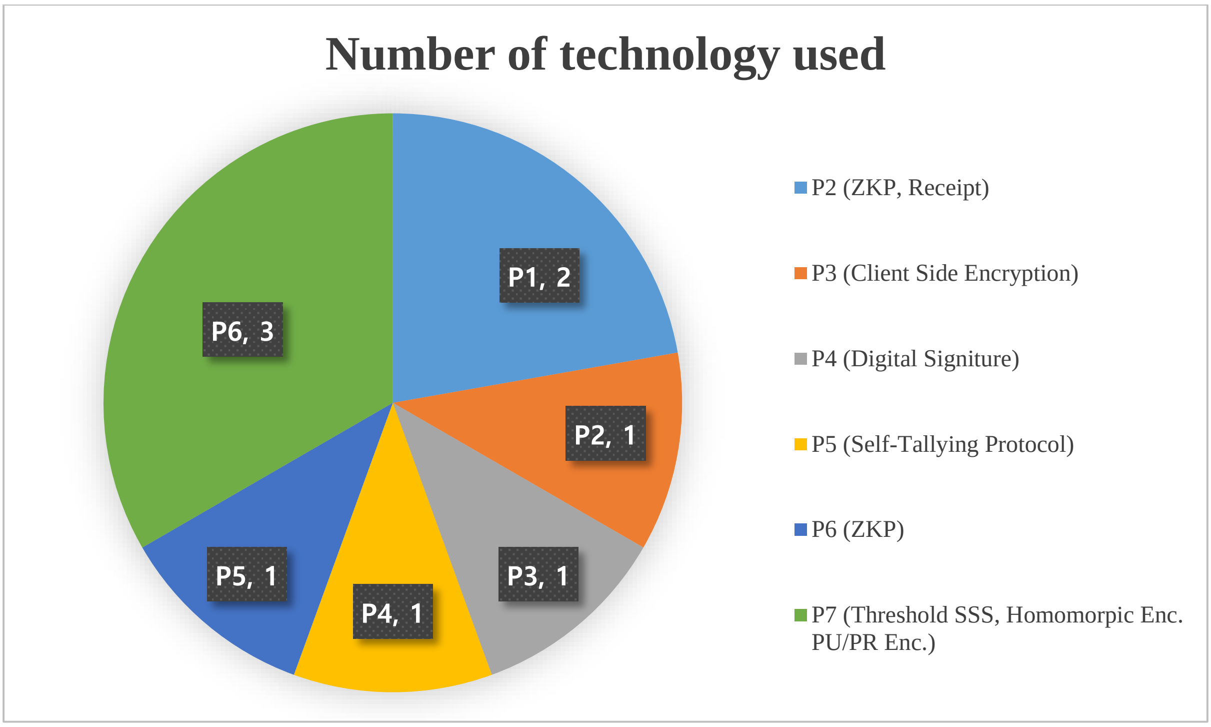

***Figure 3. A pie graph showing the number of technologies used to solve a particular principle of electronic voting. [P1] is omitted from the graph since it is believed that no clear technology was used solely to achieve it. Specific names of the technologies has been introduced in the legend section. The technologies shown in this figure was introduced in Table 4.***

A further discussion regarding the graphs will be done on the following section.

## 3.3. Literature Discussion

The schemes introduced in the previous section use the blockchain technology as a key part of maintaining preciseness and verifiability of a voting process. Blockchain technology does an excellent job in this area that people take it for granted when it comes to a blockchain e-voting scheme. Nevertheless, the human part of the scheme is seemed to be underrated. As shown in Table 4, 4 out of the 7 works of literature do not mention anything about the uniqueness of the ballot. Also, 3 out of the 7 pieces of literature do not provide a clear explanation about the Completeness of the scheme. Given these statistics, it seems plausible to argue that an important part of the scheme is currently not discussed enough. Although the blockchain technology may be solid and profound, it will be the human part where the most problem occurs if not addressed carefully.

One thing that is also shown in common among the literature is that they do not discuss in depth about producing and distributing a digital ID that is used to verify a voter. Although this is not directly linked to using blockchain, it should not be underestimated since having a valid ID to identify individuals is critically linked to verifiability, which is one of the key principles of an electronic voting scheme.

Moving onto the different types of technologies used to aid the blockchain voting scheme, we had Zero Knowledge Proof (ZKP) appearing in the 3 works of literature among the 7 pieces of literature, while the other techniques only appeared at most once. Combined with being applied to serve 2 different principles, as shown in figure 3, ZKP can be recognized as the most famous technology apart from the blockchain. Such a tendency is believed to have been driven by the fact that ZKP can not only successfully verify that the ballot has come from the right voter without revealing their identity.

# 4. Final Remarks

Voting has been an important measurement in a democratic society to express one’s opinions and gather knowledge about a certain issue. Back in the days when the population wasn’t so high, such a voting process could be done within a few hours. Nevertheless, as more and more people gather to voice their arguments, it became increasingly important that the process and results are kept more securely. To make things more efficient with a greater level of confidentiality, electronic voting schemes that utilize blockchain has recently emerged.

Blockchain e-voting system has an advantage compared with current paper voting in a way that it can eliminate the Trusted Third Party within a voting scheme. Although the existence of the Trusted Third Party does make things easier by delegating all the necessary work to the party and trust them that they will do the job properly, it is also a victim to be blamed when it goes rogue and therefore the results of the voting are sabotaged.

There is no right standard so far and the technology is still subject to change. As new techniques armed with state-of-the-art encryption and trustless consensus protocol are introduced, it will be a matter of time before a reliable e-voting scheme using blockchain is solidly founded. Nevertheless, as of now, it can be argued that there is no concrete scheme that meets the demand of 7 principles of electronic voting.

Returning to the study of the current stage of blockchain e-voting, it seems plausible to argue that the Zero Knowledge Proof provides a key breakthrough in solving some important aspects of the e-voting scheme. This works in a way that Zero-Knowledge Proof allows people to hide their identity while providing the validators information that the voters indeed have the right to vote. Such a tendency shows that Zero-Knowledge Proof shall continue to be a critical component of a blockchain e-voting system.

## 5. Future Suggestions

Apart from issuing a valid ID, the principles of electronic voting can be summarized into these questions, each accounting for several important aspects an e-voting scheme must follow.

| **Question Number** | **Key Principles** | **Question** |
|---|---|---|
| [Q1] | Verifiability,<br>Uniqueness,<br>Confidentiality | ➢ When an ID is issued, everyone, whether they participate in the voting scheme or not, must not be able to track down the identity of the voter. |
| [Q2] | Fairness | ➢ Everyone, whether they participate in the voting scheme or not, must not know the result before the due time is over. |
| [Q3] | Confidentiality | ➢ A voter must not be able to show or prove to a third person that a certain ballot belongs to the voter. |
| [Q4] | Verifiability | ➢ A voter may track one’s own ballot to check whether the contents has been securely and correctly uploaded to the network. |
| [Q5] | Verifiability,<br>Legitimacy | ➢ A verifier must be able to verify that a ballot has come from a legitimate voter |

***Table 5. Key concepts that a blockchain e-voting system must follow. Each questions are designed based on the principles of e-voting suggested in the Table 2.***

In this report, different kinds of literature regarding an electronic voting system that uses blockchain has been discussed. As various articles are addressed, it seems clear that there does not exist a solid scheme that can accompany all the basic requirements given by the National Election Committee of South Korea. Like such point implies, research regarding blockchain is mostly new. This factor may make things harder to conduct new research. Nevertheless, on the bright side, it means there are lots of new fields that can be discovered.

Just because no solid scheme exists does not necessarily imply that one cannot exist. It will only be a matter of time before a breakthrough is introduced to the area and a new, profound blockchain e-voting scheme is introduced to the public. All it remains between now and then will be the effort people put into this research topic.

## 6. REFERENCES

[1] 김형수, "세계가 대한민국 부정선거를 주목하다." https://www.lkp.news/news/article.html?no=9320 (accessed Aug. 12, 2020).

[2] "서비스소개(온라인투표시스템) | 온라인투표시스템." http://pub.kvoting.go.kr/html/service/service_01_01.jsp (accessed Aug. 14, 2020).

[3] P. McCorry, S. F. Shahandashti, and F. Hao, "A Smart Contract for Boardroom Voting with Maximum Voter Privacy," in *Financial Cryptography and Data Security*, Cham, 2017, pp. 357–375, doi: 10.1007/978-3-319-70972-7_20.

[4] R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," in *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, Oct. 2017, pp. 1–6, doi: 10.1109/TSSA.2017.8272896.

[5] W. Sandberg-Maitland and B. G. Tregub, "Threshold secret share authentication proof and secure blockchain voting with hardware security modules," US10673626B2, Jun. 02, 2020.

[6] 어준선, 홍재우, and 송주한, "영지식 증명 알고리즘을 사용하여 머클 트리 구조의 블록체인 기반 비밀 전자 투표 서비스를 제공하기 위한 방법, 및 이를 이용한 투표 코인 발행 서버, 투표 토큰 분배 서버 및 투표 지원 서버," KR101837169B1, Mar. 09, 2018.

[7] "Evaluation of the blockchain vote in the city of Zug", Luxoft, Zug, Switzerland, Rep. Final, Nov. 30, 2018

[8] DongHeon Lee, "공정한 선거를 위한 블록체인 기반 전자투표 시스템 제안", https://medium.com/decipher-media/공정한-선거를-위한-블록체인-기반-전자투표-시스템-제안-f9c1cb86ca0, (accessed Jul. 14, 2020).