Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.4, Aug. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.4.779

블록체인 기반 교내 전자투표 시스템*

성 기 정,† 정 채 린, 조 은 아, 이 종 호, 김 희 영, 김 영 우, 이 경 현‡
부경대학교 IT융합응용공학과

An Intramural Electronic Voting System Based on Blockchain*

Ki-jeong Sung,† Chae-rin Jeong, Eun-a Cho, Jong-ho Lee, Hee-young Kim, Young-woo Kim, Kyung-hyune Rhee‡
Dept. of IT Convergence and Application Engineering, Pukyong National University

요 약

오랫동안 시행되어 온 종이 투표가 보안상의 문제점이 계속해서 거론되면서 안전성과 편리성을 높인 전자투표가 몇몇 국가에서 도입되었다. 하지만 기존 전자투표는 상호의존성 및 절차상의 보안상 결점으로 인해 대부분 국가에서 도입되지 못하였다. 한편 블록체인 기술은 중앙기관 없이 P2P 방식을 이용해 블록을 독립적으로 검증하고 보유하기 때문에 높은 신뢰성을 가지며 각 블록이 이전 블록의 해시를 참조하기 때문에 한 블록을 변경하고자 한다면 모든 블록을 변경해야 하므로 위변조가 매우 어렵다. 이를 전자투표시스템에 적용 시 무결성과 투표결과에 대한 투명성이 확보된다. 본 논문에서는 기존 전자투표시스템의 상호의존성 및 과도한 TTP의 신뢰문제와 단일 실패지점 문제를 개선한 블록체인 기반의 교내 투표 시스템을 제시하고 구현한다. 추가로 시스템 안전성 및 기존 비트코인 기반 전자투표 시스템과 비교 장점을 제시한다.

ABSTRACT

As security problems of the paper ballot have been emerged on and on, electronic voting with enhanced security and convenience has been introduced in several countries. However, it has not been adopted most of countries because of the problems that come from interdependence and security flaws. Meanwhile, the blockchain technology has high reliability due to the mechanism of mining that miners verify and preserve blocks independently by using P2P formation which does not have a central authority. Furthermore, because each block refers to the hash of the previous block. if any one block is changed, it is very difficult to forge and modify the blockchain because all blocks must be changed. If this technology is applied to the E-voting, integrity, and transparency about the result of the ballot is guaranteed. In this paper, we propose and implement an electronic voting system based on blockchain that improves interdependence, the reliability of excessive TTP and single point of failure come from original electronic voting. Also, we analyze the security and advantage of the proposal system compared with the existing bitcoin-based electronic voting system.

Keywords: E-voting, Ethereum, Blockchain

I. 서 론

2016년 미국 대선 2개월 전, 애리조나와 일리노이주의 투표 기계가 해외 해커들로부터 해킹된 사실이 공론화되었다. 이는 당시 해당 주의 유권자들에게 투표결과의 무결성에 대한 의구심을 불러일으키며 전

Received(03. 15. 2018), Modified(07. 09. 2018), Accepted(07. 09. 2018)
* 본 논문은 2017년도 동계학술대회에 발표한 우수논문을 개선 및 확장한 것임
† 주저자, 12eeea@naver.com
‡ 교신저자, khrhee@pknu.ac.kr(Corresponding author)

자투표 시스템 개선의 필요성을 야기했다[1]. 기존의 종이 투표와 비교했을 때, 전자투표는 실시간 집계 처리가 가능할 뿐만 아니라 오류의 발생도 적어 실제 에스토니아에서는 2005년부터 전자투표를 도입하여 시행 중이다. 하지만 전자투표에서는 상호의존성이라는 특징 때문에 시스템의 한 지점에서 오류가 발생하더라도 시스템의 다른 부분들이 서로 의존하기 때문에 상호 영향을 받으며 오류의 발생 지점을 정확히 식별하기 어렵다[2]. 또한 몇몇 전자투표 시스템은 신원 검증 및 투표 신뢰성 확보 등을 위해 Trusted Third Party(TTP)를 포함하지만 TTP의 포함은 단일 실패지점(SPoF) 문제와 TTP의 권한 남용 문제가 발생한다. 따라서 언급한 문제점을 해소하기 위해 TTP를 최소한으로 구성한 P2P 방식의 분산 원장 기술인 블록체인을 결합한 전자투표 시스템이 최근 제안되었다. 블록체인은 투명성, 비가역성, 부인방지 등의 특성을 가지며[3] 이를 전자투표 시스템에 적용 시 투표과정의 안전성을 높여준다. 이와 관련하여 최초로 비트코인 기반의 전자투표시스템이 2015년 Zhao와 Chan에 의해 제안되었다[4]. 본 논문에서는 이더리움 블록체인 기반의 전자투표 시스템 요구사항을 제시하고 이를 구현하였다. 또한, 이에 따른 안전성과 기존 비트코인 블록체인 기반 전자투표 시스템과의 비교 장점을 분석한다. 추가적으로 투표과정에서 강압에 의한 매수 매표 문제를 완화하기 위한 재투표 방법을 제시한다.

II. 관련 연구

2.1 기존 전자투표 사례

전자투표는 현재 몇몇 국가에서만 시행되고 있으며 에스토니아는 인터넷을 이용하여 투표시스템을 국가적인 규모에 적용 시킨 첫 번째 국가이다. 기존인터넷 기반 전자투표인 I-voting 시스템의 구조는 E2E 암호를 사용하여 투표를 수행하지만, 에스토니아의 전자투표 시스템은 블라인드 서명 기술을 활용한다[5-6].

에스토니아의 전자투표 시스템은 국가에서 발행한 ID 카드와 그 카드들이 갖는 키를 사용하여 투표한다. 투표를 위해 에스토니아의 유권자는 카드 리더기와 클라이언트 소프트웨어를 사용하여 전자투표를 위한 웹사이트에 접근할 수 있으며 법적 효력이 있는 서명을 만든다. 투표 과정에서 두 개의 RSA 키 쌍이 생성되며 하나는 인증을, 다른 하나는 디지털 서명을 위해 사용된다. 하지만 기술적인 수단보다는 절차적 통제를 설정하여 무결성을 제공하고자 하였으나 절차상의 취약점으로 인해 시스템의 무결성이 훼손되었다[5]. 또한 에스토니아[7]뿐 아니라 캐나다[8], 오스트레일리아[9]의 전자투표 시스템에서도 안전성에 관한 분석 결과로 다양한 결함이 발견되어 대부분 국가에 전자투표 시스템이 도입되지는 않았다.

2.2 블록체인 기반 전자투표 사례

FollowMyVote는 온라인상에서 구현되는 블록체인 기반의 전자투표 시스템으로 투표자와 감시자에게 투표함에서 표가 없어지지 않았다는 것을 증명하기 위해 블록체인을 이용한다. FollowMyVote 시스템은 응용 프로그램을 다운받고 그들의 신원을 인증 받으면 투표권을 얻는 방식을 채택하였다. 이 시스템은 투표자 익명의 유지를 위해 타원-곡선 암호화 방식을 사용하여 두 개의 키 쌍을 사용한다. 하나는 신원 증명을 위한 것이고, 나머지는 투표를 위해 사용된다[10-11].

이후 Zhao와 Chan은 비트코인 lottery 기반의 시스템을 제안하였다[4]. 이는 선거기간 이후 표를 복호화하는 중앙기관에 대한 필요성을 없애 투표를 암호화할 필요가 없는 새로운 접근법으로 난수 값을 이용해 투표 행위와 투표자의 관계를 숨기는 방식을 사용하였으며 투표자의 난수 값의 총합이 0임을 증명을 통해 투표의 진위성을 판별하였다[10]. 이후 Takabatake[12]도 유사한 영지식 증명을 사용한 투표시스템을 제안하였다.

가장 최근에는 Bistarelli 등이 비트코인을 이용하여 전자투표 프로토콜을 제안하였으며[13-14] 이는 선거 조직을 두 개 주체로 분리하여 하나는 인증기능을, 다른 하나는 투표권을 부여하는 토큰 분배기능을 수행하였다. 이를 통해 투표과정에서 유권자의 프라이버시를 보호하였으나 이 프로토콜에서는 별도로 분리 구성된 두 개 주체의 행위에 대해 행동을 감시하기 어려우며 투표 규모를 확장함에 있어 한계점을 지녔다[6].

앞서 언급한 비트코인 블록체인 기반의 전자투표는 비트코인이 갖는 튜링 불완전성의 특징 때문에 투표자에 대한 정당성 검증과 관리적 접근제한 등 완전한 투표 시스템의 기능을 구현할 수 없었으며 대신 부분적으로 블록체인을 이용하였다. 반면 튜링 완전

언어를 지원하는 이더리움의 경우 스마트 컨트랙트를 [3] 이용하여 투표자에 대한 검증 및 투표 시스템 전체에 대한 완전한 구현이 가능하다.

이후 3장에서는 전자투표 및 제안하는 시스템의 보안 요구사항을 제시하며 4장에서는 제안 시스템 동작절차를 신원 인증과정 및 전단부와 후단부로 나누어 설명한다. 5장에서는 3장에서 언급한 요구사항에 대해 안전성을 분석하며 기존 비트코인 기반의 시스템과 비교 장점을 제시한다.

III. 요구사항

3.1 전자투표 보안 요구사항

일반적인 전자투표 보안 요구사항을 다음과 같이 표로 제시한다[16].

Table 1. Requirements for implemented system

Privacy	There must not be any connections between voter and vote. Privacy must be provided so that voter can vote freely without coercion
Accuracy	Every voting value must be reflected accurately in the result of a vote. Only valid voting value can be included.
Fairness	E-voting should be fair so that there are not some candidates or some voters who have unlawful effects at the voting stage. It may affect a judgment of voters if some results are published before the end of the election
Eligibility	Only voters who are entitled to vote can vote. To do this, the list of voters should be published in advance and managed on the database
Prevention of double voting	There must not be any cases in which one person who vote more than twice.
Receipt Freeness	A voter cannot verify one's choice to the third party. If a voter can prove his or her vote to the third party, there may be a vote with coercion or for money.
Verifiability	We need a function to verify that the voting process is operating and counted correctly. This function can increase credibility about the whole system since voter does not have to trust the organizer of an election.
Robustness	A management of whole voting system must not be influenced by an error which occurred by the organizer or some system.
Soundness	There should be no obstruction of the coercion by dishonest voters. In the final count, an illegal vote should be disclosed so that the election must not be affected.

3.2 제안 시스템 보안 요구사항

제시 및 구현하는 시스템의 경우 이더리움 기반의 블록체인을 사용하며 보안 요구사항을 다음과 같이 정의한다.

1) 투표권을 의미하는 토큰의 부여 및 전송, 회수 등의 절차는 투명하게 검증될 수 있어야 한다.

2) 투표의 최초 게시자 및 관리자에 대한 과도한 권한이 제한되어야 한다.

IV. 구현 시스템

4.1 사용자 인증절차

해당 시스템에서 참여자는 학생(유권자, 후보자) 및 인증기관(신원 인증 수행기관)이며 모든 투표시스템은 이더리움 블록체인의 스마트 컨트랙트 형태로 동작한다. 또한 언급되지 않은 사항과 합의 및 블록의 채굴 메커니즘은 기존 이더리움 환경과 동일하게 동작한다.

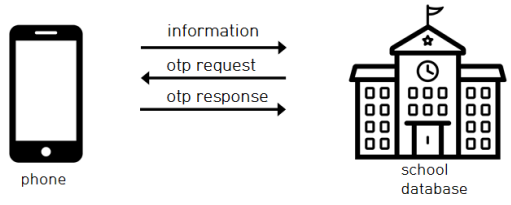

Fig 1. Authentication process

투표 전 신원 인증과정에서 가정사항은 첫 번째로, 휴대폰은 개인에게 귀속되며 두 번째로, 인증기관은 기존의 안전성이 검증된 데이터베이스를 운용중이고 학생들의 학번과 비밀번호의 해시값만을 저장중이며 세 번째로, 휴대폰에서 Seed로부터 파생된 블록체인의 주소를 구성하는 개인키는 사용자에 의해 유출 및 훼손될 수 없도록 보호된다고 가정한다.

인증절차에서 "Fig.1"과 같이 유권자의 신원 인증을 위해 교내 인증기관을 두고 인증기관이 보유한 안전한 데이터베이스에 저장된 학생 정보를 이용하여 OTP 인증절차를 수행하며 이는 다음과 같다.

1) 유권자가 투표를 위해 "Fig.2"와 같은 모바일 앱에 자신의 학번 및 비밀번호를 입력하면 해당 정보가 해싱되어 교내 인증기관으로 전송된다.

2) 해싱된 개인정보와 교내 DB에 저장된 학생의 신원 정보가 일치한다면 인증기관에서 해당 학생의 휴대전화로 OTP 인증을 요청한다.

3) 유권자는 본인의 휴대전화에서 OTP에 대한 응답을 인증기관으로 전송하며 인증기관은 이를 검증 후 성공여부를 유권자의 휴대폰으로 전송한다.

4) 유권자는 인증기관의 인증 성공 응답을 받았는지를 전단부에서 안전한 방식으로 검증하며 이후 랜덤한 Seed를 생성하고 이로부터 개인키 및 공개키와 이더리움 블록체인의 주소(address)를 생성하며 이는 자동적으로 전단부의 인증과정 후 스마트 컨트랙트에 등록된다.

4.2 전단부

구현하는 시스템의 전단부는 모바일 응용 프로그램이며 실행 화면은 "Fig.2"와 같다. 앱 접속 시 "Fig.2"와 같은 화면이 나타나고 학생의 고유 식별번호인 학번과 투표자가 설정한 패스워드가 일치하면 본인의 신원이 인증되며 이후 OTP 인증절차를 모두 거치면 휴대폰에 저장된 Seed로부터 파생된 블록체인의 주소가 스마트 컨트랙트에 등록된다.

4.3 후단부

전자투표 시스템의 후단부에서는 이더리움 기반의

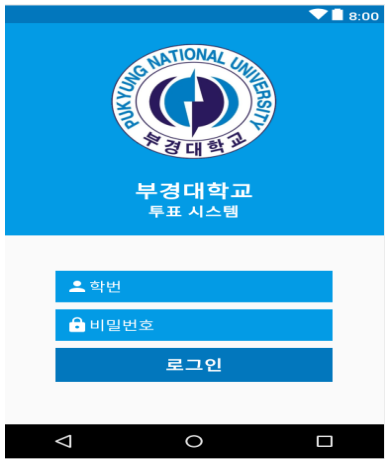

Fig. 2. The mobile app interface for user authentication

솔리디티 언어를 사용하여 스마트 컨트랙트를 구현하였으며 이더리움 테스트 네트워크에 컨트랙트를 배포한다. 또한 테스트 네트워크 환경에서는 투표 트랜잭션 전송을 위한 가스 및 이더는 각 유권자에게 일정량 faucet 서비스를 이용하여 공급하였으며 각 절차에서 함수 실행 전 조건을 검사하는 수식자인 Modifier와 예외 처리를 위한 Require를 사용하여 접근제어 및 완전한 투표시스템을 구현하였다. 또한 해당 시스템에서는 ERC20 토큰의 표준을 사용한다.

블록체인 트랜잭션의 공개성을 고려하여 사용자에게는 후보자의 블록체인 주소와 발행되는 토큰의 종류를 감추며 단지 후보자의 기호번호만 모바일 앱에 공개하여 공개형 블록체인 환경에서도 추적할 수 없도록 한다. 또한 매 투표시기별로 새로운 토큰을 생성하여 투표를 진행한다. 다음은 스마트 컨트랙트 상 구현된 주요 기능 및 사용된 보안 메커니즘에 대해 제시한다.

1) 유권자 및 후보자 등록 및 조회 컨트랙트

해당 기능은 수식자 onlyOwner를 통해 관리자만 접근 가능한 특정 함수에 대해 접근제한을 두며 최초 컨트랙트 배포자인 관리자만 유권자 등록을 수행할 수 있다.

setTime 함수는 타임스탬프를 투표 시작 시간으로 설정하며 생성자 Register는 투표권을 의미하는 토큰을 생성한다. 토큰은 투표 관리자가 소유하며 토큰을 전송하는 함수인 transfer을 이용하여 registerVoter에서 등록된 주소에게 투표권을 부여

할 수 있다.

또한 check 함수를 통해 중복된 블록체인 주소가 투표자로 저장되어 있는지를 검사한다.

registerVoter 함수는 유권자를 저장할 수 있으며 관리자가 이 함수를 실행하여 check 함수 등 몇 가지의 검증을 거치며 OTP로 인증된 유권자만 등록된다.

registerCandidate 함수는 유권자 등록과 유사한 방식으로 후보자를 저장하며 중복되거나 공백인 정보를 입력한 후보자의 등록은 에러를 반환한다.

getNumberOfVoter 함수는 등록된 유권자의 수를 반환하며 getCandidateInfo 함수는 컨트랙트에 저장된 후보자의 주소를 반환하는 함수로써 잘못된 기호 번호를 입력하면 컨트랙트는 종료된다.

2) 투표 컨트랙트

해당 기능은 수식자 onlyVoter를 통해 등록된 유권자만 투표를 수행할 수 있다.

컨트랙트에서 start 함수를 통해 후보자에게 투표할 수 있으며 투표권은 투표 기간 내에만 행사할 수 있다. 실제 동작에서 투표는 투표 게시자에게 후보자의 정보와 함께 다시 1 토큰(투표권)을 반환하여 관리자 컨트랙트에서 집계하는 방식으로 진행된다.

update 함수는 1번 이상 투표를 시도했을 때 실행되며 재투표를 할 수 있다.

getParticipation 함수는 투표 참여자 수를 반환하며 getCount 함수는 각 후보자별 득표수를 반환하여 최종적으로는 getResult 함수를 통해 투표 결과를 반환하여 당선자를 알려준다.

V. 안전성 분석

5.1 요구사항에 따른 안전성 분석

3장에서 언급한 전자투표 및 제안시스템의 보안 요구사항에 대해 다음과 같은 안전성 분석을 제시한다.

1) 프라이버시(Privacy)

유권자의 신원과 블록체인의 주소는 연관성이 존재하지 않으며 인증 및 투표권 부여 절차에서 인증기관은 랜덤한 Seed로부터 파생된 투표자의 블록체인 주소와 유권자의 신원을 연결할 수 없다. 따라서 유권자의 투표 결과를 추적할 수 없어 유권자의 프라이버시가 보호된다.

2) 정확성(Accuracy)

투표 컨트랙트의 start 함수는 투표 기간에만 실행할 수 있으며 투표기간 내에 투표된 건만 블록체인에서 집계된다. 또한 토큰을 가지고 있지 않으면 투표에 참여할 수 없으며 토큰 전송을 위해 사용하는 transfer 함수는 2개의 require 함수를 이용해 토큰의 부정 전송을 방지하여 투표의 정확성을 보장한다.

3) 공정성(Fairness)

setTime 함수를 통해 정의된 시간이 지나야만 투표 결과를 조회할 수 있으며 종료 시간 이전에 getCount, getResult 함수를 실행할 경우 require 함수가 실행되어 컨트랙트가 종료된다. 이를 통해 권한있는 자의 투표 중간 결과 유출을 방지하여 투표의 공정성을 보장한다.

4) 적임성(Eligibility)

컨트랙트에 저장되지 않아 토큰을 가지고 있지 않는 유권자의 주소는 투표에 참여할 수 없다.

5) 검증성(Verifiability)

퍼블릭 블록체인인 이더리움을 통해 컨트랙트를 배포하므로 누구나 트랜잭션을 검증할 수 있으며 블록체인의 특징으로 인해 데이터 위변조가 어렵다.

6) 강인성(Robustness)

블록체인을 통해 해당 시스템에서는 이더리움의 채굴자들이 독립적으로 블록을 검증하며 블록안에 포함된 스마트 컨트랙트로 구성한 투표 시스템의 경우 블록체인의 특징으로 인해 위변조 되기 어렵다. 또한 투표 관리자에 의해 투표 기간은 단 한번만 설정할 수 있으며 투표가 진행되는 도중에는 투표 기간 검증을 통해 관리자는 투표 결과를 조회 및 변경하는 등 투표 시스템에 영향을 줄 수 있는 행위는 할 수 없다.

7) 건전성, 중복투표, 강제 매표에 대한 안전

변수 doubleVote를 통해 이미 투표에 참여한 사람이 투표를 하려 한다면 재투표를 할 수 있는 update 함수가 실행된다. 이는 2명의 후보자에게 투표가 불가능하며 재투표시 기존 후보자에게 행사한

표는 감소시키고 새롭게 선택한 후보자의 득표수를 증가시킨다. 이에 따라 강압에 의해 매표를 하더라도 재투표한 결과만이 최종 반영된다. 또한 재투표 시도는 블록체인에 기록되며 향후 감사를 통해 적발될 수 있다.

8) 투표 주장(Receipt Freeness)에 대한 안전

블록체인 주소를 구성하는 개인키를 유출 및 훼손할 수 없도록 구성하여 공개된 블록체인 주소와 특정 유권자의 정보만으로는 유권자가 해당 후보자에 대한 투표 사실을 주장할 수 없어 투표권 주장 문제에 대해 안전하다.

5.2 기존 시스템과의 비교

본 절에서는 제안한 전자투표 시스템과 기존 E-Voting 및 비트코인 기반의 전자투표시스템을 비교 분석하여 다음과 같이 제시한다.

표와 관련하여, 암호복잡도 및 기밀성의 경우 기존 E-Voting 시스템은 영지식 증명과 암호기법 및 다양한 서명기법을 통해 유권자의 투표에 대한 증명 및 기밀성을 보장하며 비트코인 기반 전자투표의 경우 영지식 증명과 동형암호등의 기법을 비트코인 트랜잭션에 적용하여 기밀성을 보장한다.

따라서 기존 시스템의 높은 암호학적 복잡도에 비해 상대적으로 제안 시스템에서는 단순히 블록체인상 Ecdsa의 서명 검증과 해시 함수만을 사용하여 낮은 복잡도를 유지한다. 또한 토큰 기반의 유권자 증명 및 함수에 의한 접근제어와 모바일 앱에서 토큰과 유권자의 블록체인 주소를 사용자에게 공개하지 않으며 투표과정에서도 토큰을 관리자에게 회수하는 방식으로 진행하므로 개별적인 후보자에 대한 실시간 득표 사항을 공개형 블록체인을 통해 확인하기 어렵다. 이처럼 실제 신원과 유권자의 블록체인 주소 간 비 연결성이 확보되며 공개형 블록체인을 통해서도 실시간 투표 결과를 확인하기 어려우므로 별도 기밀성에 대한 고려가 필요하지 않다.

Table 2. Comparison with existing model

	E-Voting [5-9]	Bitcoin-based model [10-15]	Proposal model
Cryptographic Complexity	High	Middle	Low
Confidentiality	High	High	Don't need
Extendability	Low	Middle	High
Anonymity	High	High	High
Integrity	Middle	High	High
Functionality	High	Middle	High
Acess control	High	Middle	High
Receipt Freeness	Low	Low	Middle

확장성의 경우 기존 E-Voting 시스템은 증가하는 유권자에 대한 관리서버 및 TTP 수의 증가로 인해 SPoF 및 상호의존성 문제가 발생하여 확장성이 제한되며, 비트코인 기반 시스템의 경우 별도 비트코인 블록체인과 호환되지 않는 암호 기술의 사용으로 인해 모든 참여자는 별도의 프로그램 설치가 필요하므로 확장성에 대한 제한이 있다.

표 2에서 제시한 바와 같이 기존 E-Voting의 경우 절차상 문제 등으로 인해 시스템의 무결성이 훼손될 수 있으나 블록체인 기반 시스템의 경우 블록체인 합의와 해시함수의 특징으로 인해 시스템의 무결성을 보장받을 수 있다.

접근제어 및 기능적 특성 부분에서 기존 제시된 비트코인 기반 시스템의 경우 접근제어 기능 및 투표 시스템에 필요한 투표 집계와 같은 기능들은 제공하지 않았으나 제안하는 이더리움 기반의 시스템에서는 튜링 완전성을 통해 다양한 기능들이 구현 가능하다.

추가적으로 제안 시스템에서는 강압에 의한 매수매표 문제에 대해 재투표 기능을 도입하였으며 이러한 기록을 별도로 두어 투명하게 감사할 수 있는 시스템을 제안하였다.

VI. 결 론

본 논문에서는 이더리움 블록체인과 스마트 컨트랙트 및 토큰을 사용한 이더리움 기반의 교내 전자투표 시스템을 제시하고 구현하였으며 이에 대한 시스템의 안전성 및 기존 시스템과의 비교 장점을 분석하였다. 기존의 전자투표 시스템이 갖는 상호 의존성과 TTP의 과도한 권한 문제 및 시스템 무결성 문제를 해결하기 위해 이더리움 블록체인을 사용하였으며 제안된 시스템에서는 기존 비트코인 시스템에 비해 접근제어 등의 기능 구현이 용이하였으며 강압에 의한 매수매표 문제에 대해 재투표 기능을 구현하여 해당 문제를 완화하였다. 제안 모델은 공개형 블록체인

과 토큰을 사용하였으며 이러한 특징 때문에 향후 추가적인 보완을 통해 확장성 있는 전자투표 시스템 구축이 가능할 것으로 판단된다.

References

[1] F. Ciazzo and M. Chow, "A blockchain 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] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum White Paper, 2014.

[4] Z. Zhao and T-H. Hubert Chan, "How to vote privately using bitcoin," International Conference on Information and Communications Security, pp. 82-96, Dec, 2015.

[5] D. Springall, T. Finkenauer, and Z. Durumeric, "Security analysis of the Estonian internet voting system," Proceeding of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 703-715, Nov, 2014.

[6] Y. Liu and Q. Wang, "An e-voting protocol based on blockchain," IACR Cryptology ePrint Archive 2017: 1043.

[7] R. Krimmer, "Electronic voting 2006," GI Lecture Notes in Informatics, P-86, Bonn, 2006.

[8] N.J. Goodman, "Internet voting in a local election in Canada," The Internet and Democracy in Global Perspective. Springer, Cham, 2014. 7-24.

[9] I. Brightwell, J. Cucurull, D. Galindo and S. Guashch, "An overview of the ivote 2015 voting system." available through https://www. elections. nsw. gov. au, 2015.

[10] I. Kubjas, "Using blockchain for enabling internet voting," Jan. 2017.

[11] C.R. Jeong, J.H. Lee, Y.W. Kim, E.A. Cho, K.J. Sung, H.Y. Kim, and K.H. Rhee, "Analysis of requirements for construction of electronic voting system based on blockchain," CISC-W' 17, pp. 31-34, Dec. 2017.

[12] Y. Takabatake, D. Kotani, and Y. Okabe, "An anonymous distributed electronic voting system using zerocoin," Institute of Electronics, Information and Communication Engineers(IEICE), Technical Report IA2016-54, pp. 127-131, Nov. 2016.

[13] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system." 2008.

[14] S. Bistarelli, M. Mantilacci, P. Santancini, and F. Santini, "An end-to-end voting system based on bitcoin," Proceedings of the Symposium on Applied Computing. ACM, pp. 1836-1841, 2017.

[15] S.S. Kim, J.S. Lee, and S.K. Lee, "A proposal for the practical and secure electronic voting protocol," Journal of the Korea Institute of Information Security and Cryptology, 10(4), pp. 21-32, 2000.

[16] B.C. Lee, "Analysis of issues for a e-voting introduction," Journal of the Korea Institute of Information Security and Cryptology, 12(4), pp. 33-45, 2005.

〈저자소개〉

성 기 정 (Ki-jeong Sung) 학생회원
2015년 3월~현재: 부경대학교 IT융합응용공학과 재학
〈관심분야〉 정보보호, 암호학, 블록체인

정 채 린 (Chae-rin Jeong) 학생회원
2014년 3월~현재: 부경대학교 IT융합응용공학과 재학
〈관심분야〉 보안, 네트워크, IT융합

조 은 아 (Eun-a Cho) 학생회원
2014년 3월~현재: 부경대학교 IT융합응용공학과 재학
〈관심분야〉 정보보호, 전자공학, IT융합

이 종 호 (Jong-ho Lee) 학생회원
2012년 3월~현재: 부경대학교 IT융합응용공학과 재학
〈관심분야〉 정보보호, 블록체인, IT융합, IoT

김 희 영 (Hee-young Kim) 학생회원
2013년 3월~현재: 부경대학교 IT융합응용공학과 재학
〈관심분야〉 정보보호, 프로그래밍

김 영 우 (Young-woo Kim) 학생회원
2013년 3월~현재: 부경대학교 IT융합응용공학과 재학
〈관심분야〉 정보보호, 네트워크보안, 임베디드

이 경 현 (Kyung-hyune Rhee) 종신회원
1982년 2월: 경북대학교 수학교육과 졸업
1985년 2월: 한국과학기술원 응용수학과 석사
1992년 8월: 한국과학기술원 수학과 박사
1985년 2월~1993년 2월: 한국전자통신연구원 연구원, 선임연구원
1993년 3월~현재: 부경대학 IT융합응용공학과 교수
〈관심분야〉 정보보호, 암호이론, 암호 프로토콜, 통신보안, 블록체인 기반 기술 및 응용