블록체인에서의 스마트 컨트랙트 기반의 전자투표 시스템+

노창현*, 이임영**
*,**순천향대학교 컴퓨터학과
e-mail : *rohch@sch.ac.kr, **imylee@sch.ac.kr

Smart Contract Based Electronic Voting System in Blockchain

Chang-Hyun Roh*, Im-Yeong Lee**
*,**Dept of Computer Engineering, SoonChunHyang University

요 약

전자 정부의 시스템들은 공신력 있는 데이터를 보장하고 그 정보의 위·변조를 막아왔으며, 지금까지 이러한 역할을 전통적인 중앙집중형 관리 방식으로 진행되어 왔다. 하지만, 중앙집중형의 데이터 관리 방식은 단일 오류점의 문제와 병목현상의 단점을 가지고 있다. 이러한 문제를 해결하기 위해 블록체인 기술이 등장하여 그동안 안전하지 못하다고 생각되어 왔던 탈중앙화를 특징으로 하여 데이터의 무결성을 보장한다. 하지만, 일반적인 블록체인과 스마트 컨트랙트를 전자 정부의 전자투표에 그대로 적용하기에는 많은 문제점들이 존재한다. 본 연구에서는 전자투표에 무결성과 자동화 기능을 제공하기 위해 블록체인과 스마트 컨트랙트를 적용하여 투표 데이터의 무결성을 보장하고 투표와 개표의 과정들을 스마트 컨트랙트로 자동화하는 방법을 제시하고자 한다.

1. 서론

전자투표란 기존의 종이 투표의 방법들을 기계적으로 구현한 것을 의미한다. 투표는 민주주의의 꽃으로 불리며 유권자가 자신의 의견을 직접 표현하는 것을 의미한다. 투표는 오랫동안 진행되어 왔고, 현대에 이르러 투표의 과정들을 모두 전자화 하여 우리 생활에 적용하려는 움직임이 늘어나고 있다. 기존의 종이투표 방식은 선거 운용비용이 전자투표에 비해 많이 비싸며 집계를 진행할 때에는 일일이 투표지를 확인하여 진행하기에 개표에도 많은 시간이 걸린다. 이러한 문제점으로 인해 종이투표의 대안으로 전자투표가 계속해서 제안되었다[1].

기존의 전자투표는 암호학적 알고리즘을 사용하여 편리하고 안전한 투표를 제공하려 했다. 하지만, 중앙 집중형 구조에서는 관리자의 많은 권한으로 인해 투표 데이터를 위·변조할 수 있는 가능성이 있다. 또한, 단일 지점 공격에 대한 가능성을 제공하기에 현재까지도 소규모의 적은 인원이 사용할 수 있는 분야에만 적용하여 사용되었다[2]. 이런 문제로 최근에는 신뢰의 문제와 단일 지점 공격에 대한 위협을 해결하고자 블록체인 기술을 적용하는 다양한 연구들이 진행되고 있다.

블록체인(Blockchain)이란 P2P(Peer to Peer)환경의 네트워크에서 모든 참여자들이 다양한 합의 알고리즘을 적용하여 같은 데이터를 가지는 신뢰성을 보장하는 것을 말한다. 이러한 특징을 전자투표에 적용하여 모든 투표 데이터를 트랜잭션처럼 처리하여 블록에 저장할 경우 악의적인 네트워크 참여자가 데이터를 쉽게 위·변조 할 수 없는 구조가 되며, 분산 네트워크를 통해 이루어지는 투표로 인해 관리자의 권한도 축소시켜 신뢰성을 얻을 수 있다. 또한, 블록체인에서 제공하는 스마트 컨트랙트를 이용하여 투표와 개표의 과정들을 자동화하고, 투표와 개표의 진행사항에서 생성된 데이터들의 무결성을 제공한다.

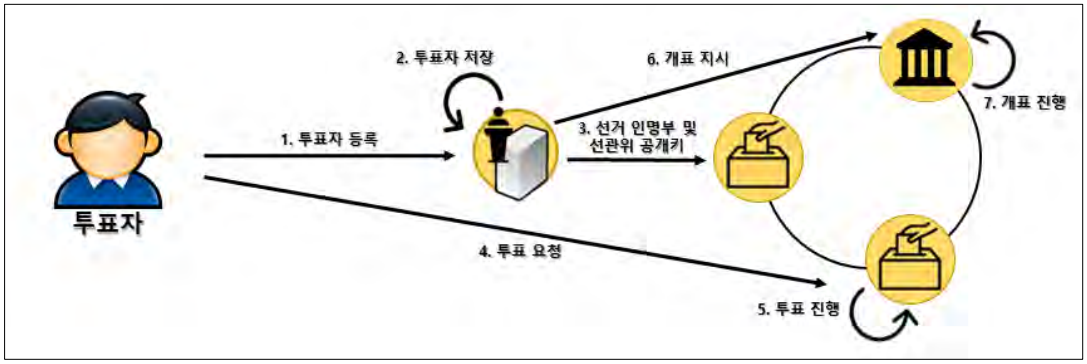
본 논문에서는 스마트 컨트랙트와 블록체인을 이용하여 전자투표에 투표 데이터의 무결성과 투표와 개표에 투명성을 보장하는 시스템을 제안한다.

2. 관련 연구

2.1 전자투표

전자투표는 투표를 진행하는 모든 절차를 전자화하는 것을 의미한다. 투표 과정은 후보자 설정, 투표자 설정, 신원 확인, 투표, 개표, 검표 등의 과정으로 진행되며 모든 과정들이 신뢰성을 가지고 진행되어야 선거로써의 법적인

+ 본 연구는 과학기술정보통신부 및 정보통신기기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2019-2015-0-00403)



<그림 1> **전체 시나리오**

효력을 얻을 수 있다. 다양한 기술의 발전에 따라 스마트 폰이나 전화기를 이용한 모바일 투표 방식, 일반적인 서버를 이용한 투표 방식 등 여러 방법들이 제시되었다.

2.2 블록체인

블록체인은 2009년 Satoshi Nakamoto가 처음 비트코인이라는 암호화폐로 제안하였다. 비트코인은 P2P 네트워크에서 모든 참여자들이 같은 장부를 가지는 분산 데이터베이스를 이용하여 네트워크를 구성한다[3].

블록체인의 가장 큰 특징은 분산 데이터베이스의 형태로 모든 참여자들이 같은 데이터를 갖는 것이다. 주기적으로 생성된 블록은 블록 순서대로 연결되어 데이터를 쉽게 위·변조하지 못하는 장점을 갖는다.

2.3 스마트 컨트랙트(Smart Contract)

스마트 컨트랙트는 블록체인 기술을 기반으로 금융 거래나 부동산 계약 등 다양한 형태의 계약을 체결하고 자동으로 실행할 수 있는 기능을 제공하는 프로그램이다. 이 개념을 처음 제안한 사람은 1994년 전산학자인 닉 자보(Nick Szabo)다. 닉자보의 스마트 컨트랙트는 그동안 보안 문제들과 기술적 제약으로 인해 주목받지 못하였으나, 블록체인 플랫폼 중 하나인 이더리움(Ethereum)의 등장으로 구현이 가능하게 되었다.

3. 제안방식

본 장에서는 Private 블록체인에서의 스마트 컨트랙트를 이용하여 블록체인과 스마트 컨트랙트로 투표를 진행하는 방식을 제안한다. 본 제안방식은 한국에서의 현 상황에 맞게 선거관리위원회(이하 선관위), 투표소, 개표소로 구성되며 참여하는 투표소와 개표소는 블록체인 네트워크를 구성한다.

3.1 준비 단계

준비 단계는 각 참여 객체들이 투표를 진행하기에 앞서 선관위는 투표를 설정한다. 설정은 투표 주제, 내용, 시간 등이 들어가게 된다. 선관위는 공개·개인키 쌍을 생성하여 공개키를 투표소에 전송하는 단계를 가진다.

3.2 등록 단계

등록 단계는 선관위가 후보자와 투표자를 등록하고 후보자는 자신의 정보를 전송하여 후보자 리스트를 생성하며, 투표자는 신원 인증 후 공개키·개인키 쌍을 생성하고 공개키를 선관위로 전송하여 투표자 리스트를 생성한다.

3.3 투표 단계

투표 단계에서는 투표자가 가 투표소의 투표 컨트랙트를 실행하고 투표자 인증 과정을 거친 후 후보자 정보를 전송받고 후보자를 선택 후 선택된 데이터와 투표 시간을 연접하여 선관위의 공개키로 암호화한 후 트랜잭션에 삽입하여 전송하는 과정을 가진다.

3.4 개표 단계

개표 단계는 선관위가 개표소에 개표 매시지와 선관위 개인키를 전송하여 개표 컨트랙트를 실행한다. 개표소는 블록에 저장된 트랜잭션을 추출하고 암호화된 데이터를 선관위의 개인키로 복호화하여 개표를 진행한다.

4. 결론

본 논문에서는 트랜잭션에 투표 데이터를 암호화하여 전송하기에 투명한 투표 결과를 기대할 수 있다. 또한, 스마트 컨트랙트를 이용한 투표, 개표방법을 이용함으로써 중앙 관리자나 선관위가 한 번 투표를 설정한 후 관여하는 일 없이 자동으로 진행할 수 있도록 하였다. 이러한 방법으로 전자투표 시스템이 개발되고 상용화된다면, 투표 진행비용 감소와 투표율 증가 등의 효과를 기대할 수 있을 것이다.

참고문헌

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