블록체인을 이용한 전자투표 시스템+

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

Electronic voting system using block chain

Chang-Hyun Roh, Im-Yeong Lee
Dept of Computer Science and Engineering, Soonchunhyang University

요 약

블록체인은 분산 원장 기술 중 하나로 여러 개의 노드들이 참여하며, 이 노드들 간의 합의 알고리즘을 통하여 데이터의 위·변조를 막고, 이미 기록된 데이터를 바꿀 수 없는 구조를 장점으로 가진다. 이러한 특성 때문에 블록체인은 신뢰성이 중요시되는 플랫폼에 많이 적용이 되며 많은 플랫폼 중 전자투표의 중요한 기술로서 인식되고 있다. 전자투표는 선거의 모든 과정을 전자화 하여 선거를 관리하는 사람이나 투표자 모두에게 편리함을 제공하는 시스템으로 기술적인 보안성이나 시스템의 안정성이 완벽하게 보장되지 않아 유권자들에게 신뢰를 주지 못해 현실에서 쉽게 적용하지 못하고 있다. 이러한 문제를 해결하기 위해 본 논문에서는 블록체인을 적용하여 투표의 변조를 막고 유권자들의 신뢰와 시스템의 안정성을 제공하는 전자투표 시스템을 제안한다.

1. 서론

블록체인은 여러 노드들로 구성되고 다양한 합의 알고리즘을 적용하여 모든 노드들이 같은 데이터를 가지는 신뢰성이 보장된 네트워크로 구성된다. 블록체인은 비트코인, 이더리움 같은 암호 화폐에서 처음 개념이 등장하였으며, 암호 화폐에서의 블록체인의 역할은 트랜잭션의 모임인 블록들의 무결성과 이전 블록과 트랜잭션을 이용하여 검증하는 투명성이다. 이러한 특징을 가지고 있는 블록체인을 다양한 분야에 적용하려는 움직임이 많이 나타나고 있고, 이 중 대표적인 사례가 블록체인을 적용한 전자투표 시스템을 예로 들 수 있다.

전자투표란 선거의 과정들을 모두 전자화하는 시스템으로 투표자 설정, 신원확인, 투표, 개표, 검표 등의 과정들을 전자적으로 구축하는 시스템이다. 전자투표 시스템에는 여러 가지 요구사항들이 존재하지만, 그 중 가장 중요하게 여기는 것은 완전성과 투명성이다. 완전성은 투표과정과 개표과정이 완전하게 이루어 졌는지에 대한 요구사항이고, 투명성은 자신의 투표가 투표결과에 잘 반영되었는지를 확인할 수 있어야 하는 것이다. 블록체인을 적용할 시 투표와 개표까지의 데이터를 변조 없이 그대로 유지할 수 있기에 전자투표의 완전성을, 이전 블록에 포함된 트랜잭션들을 이용하여 자신의 투표가 투표결과에 잘 적용되었는지 확인할 수 있는 투명성 때문에 이런 두 가지의 요구사항은 블록체인의 특성으로 만족시킬 수 있다[1].

본 논문에서는 분산 원장기술의 하나인 블록체인을 이용하여 Private 블록체인 환경에서 완전성과 투명성을 제공하는 전자투표 시스템을 제안한다.

2. 관련 연구

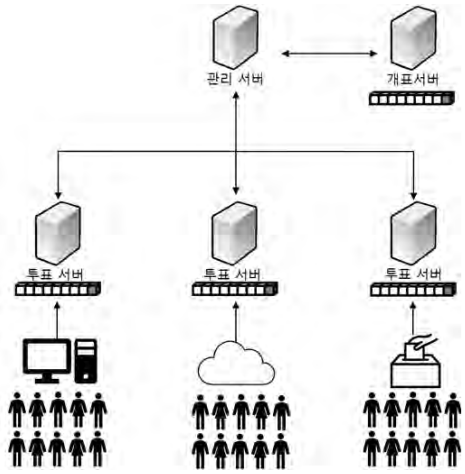
2.1 블록체인

블록체인은 분산 원장 기술 중 하나로써 P2P 방식의 공공 거래 장부라고 이야기 할 수 있다. 블록체인에 참여한 각각의 노드는 서로의 공공 거래 장부를 비교하여 조작되지 않도록 하며, 새롭게 쓰이는 내용은 모든 노드들이 합의 알고리즘을 이용하여 작성되므로 이 또한 조작되지 않는 구조를 가지고 있어서, 데이터에 위·변조를 하려면 블록체인에 참여한 노드들 중 51% 이상을 탈취해야만 가능하다[2]. 블록체인을 이용하는 플랫폼에는 비트코인이나 이더리움과 같은 암호화폐(Cryptocurrency)의 기능을 하는 Public 블록체인, Linux 재단과 IBM이 분산 원장 기술을 중점으로 하는 Hyper Ledger Fabric과 같은 Private 블록체인으로 나뉘며, 블록체인을 다양한 산업 분야에 적용하기 위한 연구들이 계속해서 진행 중이고, 특히 전자투표에 관한 연구들이 계속해서 증가하고 있다.

2.2 전자투표

전자투표란 온·오프라인의 투표소를 이용하고 안전성이 확보된 암호 알고리즘으로 프로토콜을 구성하여 선거과정들을 전자적으로 구현한 선거 행위로 투표의 비밀성,

+ 이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00156, 블록체인의 정보보호 프레임워크 및 평가 방법 개발)



(그림 1) 전체 시나리오

완전성, 공정성, 검증성 등이 보장되는 방식을 이야기한다 [3]. 전자투표의 구성요소에는 선거기관, 투표자들이 있고, 선거기관은 투표자를 지정하고, 투표 시작 시 투표자들을 인증하고 비밀을 보장한다. 투표가 완료된 후에는 투표를 취합하고 유효한 투표를 집계하여 결과를 발표하게 된다. 이러한 과정들을 가지고 있기에 비밀성, 완전성, 공정성, 검증성 등이 보장되어야 하며, 이는 블록체인의 특성과 부합하므로 블록체인 적용 시 많은 특성들을 TTP (Trusted Third Party)를 적용하지 않고 보장할 수 있다.

3. 제안방식

본 장에서는 전자투표에 Private 블록체인 환경을 적용한 시스템을 (그림 1)과 같이 제안한다. 제안된 시스템은 크게 선거 등록단계, 투표 단계, 블록 생성단계, 개표 단계로 구성된다.

3.1 선거 등록단계

선거 등록 단계에서는 투표 관리자가 선거 내용, 선거 진행 시간, 투표용지, 투표자 명부, 개표서버의 공개키를 등록하고 투표서버에 전송한다.

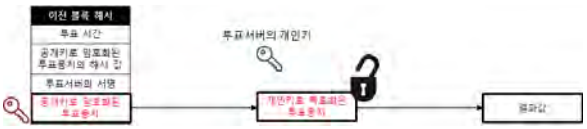
3.2 투표 단계

투표 단계는 투표 서버에서 진행되며 지정된 투표자가 투표를 시작할 때, 투표 서버는 투표자 명부를 이용하여 지정된 투표자인지 인증하는 과정을 가진다. 투표자 인증 후 투표용지를 발급하여 투표를 진행하게 되며, 투표용지는 투표가 끝나자마자 개표서버의 공개키로 암호화 되고 투표 서버는 암호화된 투표용지와 투표자의 ID를 이용하여 서명을 생성하고, 트랜잭션을 생성한다.

3.3 블록생성 단계

투표 단계에서 생성된 트랜잭션을 다른 투표서버에 Broadcast하여 정상적인 트랜잭션인지, 이전 블록에서 투표가 존재하는지, 투표자 명부에 존재하는 사람인지를 확

(그림 2) 블록체인 구성



(그림 3) 개표 과정

인하고 정상적인 트랜잭션일 경우 자신의 서명을 첨부하여 트랜잭션을 생성한 투표 서버로 회신한다. 트랜잭션을 생성한 서버에서는 모든 투표 서버의 인정을 받은 트랜잭션을 관리서버로 보내고 관리서버는 트랜잭션들을 모아서 블록을 만들고 블록을 모든 서버에 전송하게 된다(그림 2).

3.4 개표 단계

개표 단계에서는 관리 서버가 투표가 종료되었다는 것을 확인 후 개표 서버에 개표 시작 메시지를 보낸다. 개표 메시지를 받은 개표 서버는 블록체인에 저장된 트랜잭션들을 모두 개표 서버의 개인키로 복호화하여 (그림 3)처럼 계산을 진행한다. 개표를 모두 진행하게 되면 관리서버에 개표 결과를 전송하고, 관리 서버에서는 개표 결과를 공표한다.

4. 결론

본 논문에서는 블록체인을 이용한 전자투표에 대한 구성 방법을 제안하였다. 기존의 전자투표는 비밀성, 완전성, 공정성, 검증성 등의 요구사항들을 중앙 기관을 이용하여 제공하였다. 하지만, 전자투표의 투표용지를 블록체인으로 블록화 하여 저장함으로써 완전성, 공정성을 제공하고, 개표 서버에도 블록을 함께 저장해서 검증성을 제공한다.

향후 연구 방향으로는 다양한 블록체인 환경에서 전자투표를 적용할 수 있는지 검토하고, 다양한 암호학 기법을 추가하여 익명성을 강화하여 투표, 개표 서버에서도 기밀성을 제공하는 전자투표를 제안할 것이다.

참고문헌

[1] 하현수, 이선준, 정구익, 신용구, 김명호, 김영종 “Public Blockchain 기반의 익명성 전자투표 블록체인 프랫폼 모델”, 한국소프트웨어종합학술대회 논문집, 2017.

[2] S. Nakamoto. “Bitcoin : A Peer-to-peer Electronic Cash System” bitcoin.org, 2009.

[3] 허원근, 김희선, 김광조 “전자선거 프로토콜의 요구사항 연구”, 정보보호학회지, 2000.