하이퍼레저 패브릭을 이용한 전자 투표 시스템

박찬형, 김재훈
아주대학교

{fetch,jaikim}@ajou.ac.kr

Electronic Voting System Using Hyperledger Fabric

Chan Hyeong Park, Jai-Hoon Kim
Ajou University

요 약

블록체인 기술은 현재 신뢰를 필요로 하는 다양한 분야에서 사용하려는 시도가 늘고 있다. 특히 전자 투표에 활용하기 위해 활발하게 연구되고 있다. 블록체인은 네트워크에 참여하는 모든 사용자가 모든 거래 내역 등의 데이터를 분산 저장하는 기술로, 탈중앙화, 투명성, 불변성, 가용성 등 다양한 장점을 가졌다. 본 논문에서는 허가형 블록체인인 하이퍼레저 패브릭을 이용해서 전자 투표 시스템을 구축하고, 구축한 시스템이 전자 투표 시스템이 갖춰야 할 요구사항을 항목별로 만족하는지 비교하여 상용화할 수 있는 모델을 제안하였다.

Ⅰ. 서 론

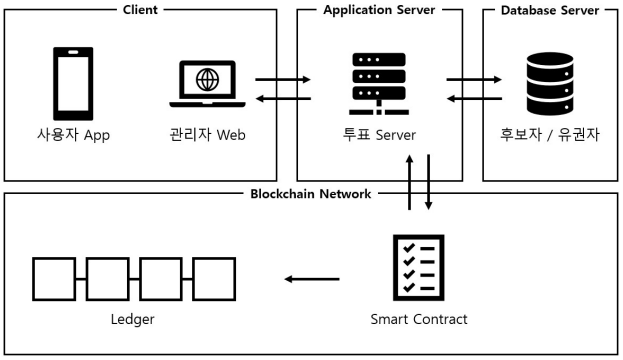

그림 1. 블록체인 전자 투표 시스템 구성도

블록체인은 4차 산업혁명의 주요 기술 중 하나로 세계적으로 주목받는 기술 중 하나이다.[1] 블록체인의 탈중앙화, 투명성, 불변성, 가용성 등 다양한 장점 때문에 신뢰성을 필요로 하는 다양한 분야에서 사용하려는 시도가 늘고 있다.

특히 블록체인 온라인 투표는 블록체인을 이용한 수많은 비 금융 서비스 분야의 성공적인 사례 중 하나이다.[2] 전자 투표는 편리성과 투표율 증가, 투표 비용의 감소 등 다양한 이점이 있기 때문에 활발하게 연구되고 있다.

그림 1은 본 연구에서 구축한 블록체인 전자 투표 시스템의 구성도를 나타낸다. 본 연구에서는 Hyperledger Fabric[3]을 이용하여 블록체인 기반 전자 투표 시스템을 구축하고, 전자 투표 시스템이 갖춰야 할 보안 요구사항을 모두 만족하는지 항목별로 비교해보았다.

Ⅱ. 본론

2.1. 블록체인

블록체인(분산원장기술, DLT)은 P2P 기반으로 중복된 데이터를 분산 처리 및 저장하는 기술이다. 즉, 네트워크에 참여하는 모든 사용자가 모든 거래 내역 등의 데이터를 P2P 네트워크에 중복하여 분산 저장하는 기술을 지칭하는 말이다. 블록체인에서 '블록'은 개개인(P2P)의 거래 데이터(Transaction)가 기록되는 장부가 된다. 이런 블록들은 형성된 후 시간의 흐름에 따라 순차적으로 연결된 '사슬(체인)'의 구조를 가지게 된다. 같은 네트워크 안에 있는 모든 사용자가 거래 내역을 중복으로 보유하고 있어 거래 내역을 확인할 때는 모든 사용자가 보유한 장부를 대조하고 확인해야 한다. 따라서 위·변조가 어려우며 중앙 관리자가 필요 없다는 특징이 있다.

2.2. 관련 연구

블록체인 기반의 온라인 투표가 투표 결과에 대한 신뢰를 유지하면서 투표율을 끌어올리는 데도 긍정적이라는 분석이 나오고 있다.[4] 하지만, 본격적인 블록체인 투표 도입을 위해서는 아직 남아있는 보안 위협에 대한 대응 방안이 필요하다.

전자 투표 시스템에는 기본적으로 갖춰야 할 요구사항으로 정확성, 비밀성, 단일성, 공정성, 적임성, 확인성, 완전성, 위조 불가능성, 투표권 매매 방지 항목이 있다.[2]

2.3. 전자 투표 시스템 구현

본 연구에서는 하이퍼레저 패브릭을 이용해 표 1에서 제시한 보안 요구사항을 만족하는 전자 투표 시스템을 제안한다. 시스템은 그림 2와 같은 순서로 동작한다.

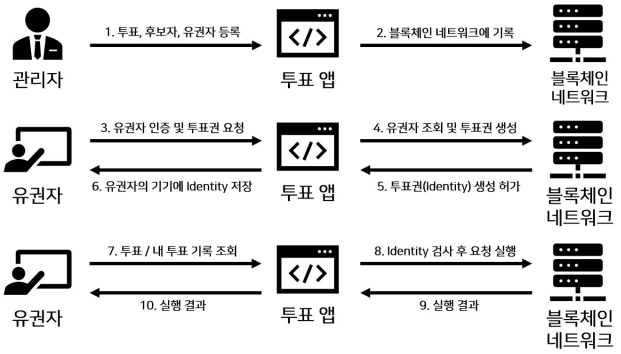

그림 2. 전자 투표 시스템 흐름도

관리자는 투표 앱(관리자용 웹앱)을 통해 새로운 투표를 등록한다. 새로 등록한 투표는 블록체인 원장(Ledger)에 기록한다.

해당 투표에 참여하는 후보자와 유권자 목록은 신뢰할 수 있는 데이터베이스 서버에 기록하고, 후보자 목록은 블록체인 원장에 함께 기록한다.

데이터베이스에 기록된 유권자 정보는 본인 확인이 가능한 정보(이름, 휴대전화 번호 등)로 구성되며, 유권자가 투표에 참여하기 위해 본인 인증 과정을 수행하면 인증에 사용한 모바일 기기에 투표권 역할을 하는 Wallet Identity 파일이 저장된다.

유권자는 지급받은 투표권을 이용해서 투표에 참여하거나, 본인이 투표한 기록을 조회할 수 있다.

2.4. 연구 결과

제안한 시스템이 보안 요구사항을 만족하는지 각 항목별로 비교한 결과는 표 1과 같다. 통신 과정에서 발생할 수 있는 문제점에 대해서는 본 연구에서 고려하지 않았다.

표 1. 구축한 시스템의 보안 요구사항 평가

요구사항	평가
정확성	인증된 Identity에 한해서 1회 투표할 수 있고 모든 기록이 네트워크 내부에 변조할 수 없는 상태로 저장되기 때문에 완전성이 보장된다.
비밀성	유권자의 인증 정보와 관련 없이 랜덤 해시로 투표권 역할을 하는 Identity를 생성하고, 생성한 개개인의 Identity는 유권자 본인만 접근할 수 있기 때문에 비밀성이 보장된다.
단일성	같은 Identity값으로 중복 투표하는 경우 그 요청(Proposal)은 반영되지 않는다.
공정성	모두 독립된 환경에서 투표를 진행하기 때문에 공정성이 보장된다.
적임성	인증된 Identity에 한해서만 투표에 참여할 수 있기 때문에 적임성이 보장된다.
확인성	본인의 투표 기록과 투표 결과를 확인할 수 있다.
완전성	인증된 Identity에 한해서 1회 투표할 수 있고 모든 기록이 네트워크 내부에 변조할 수 없는 상태로 저장되기 때문에 완전성이 보장된다.
위조 불가능성	하이퍼레저 패브릭의 CA에 의해서 인증 과정을 거치기 때문에 위조할 수 없다.
투표권 매매 방지	확장 모델로, 투표권을 받는 기기의 ID를 저장한다면 그 기기로만 이용할 수 있기 때문에 매매를 방지할 수 있다.

Ⅲ. 결론

현재 전자투표는 투표관리업무의 생산성 증대, 투표율 제고 및 참여 민주주의 발전, 투표 비용의 감소, 해외거주자 투표문제 해결 등 다양한 이점을 가지고 있어 오프라인 투표의 한계를 보완할 대안책으로 등장하며 전 세계적으로 도입을 시도하고 있다. 그러나 시민의 신뢰 확보 문제나 여러가지 보안 문제 등 해결해야 할 문제가 아직 많이 남아있기 때문에 쉽사리 도입하지 못하고 있는 실정이다.[5] 본 논문에서는 전자투표 시스템이 갖춰야 할 보안 요구사항을 만족할 수 있도록 허가형 블록체인인 하이퍼레저 패브릭을 이용해서 전자 투표 시스템을 제안하고 프로토타입을 구축하였다. 이후 구축한 전자 투표 시스템이 올바른 투표의 기능을 수행할 수 있는지 보안 요구사항을 항목별로 비교해보고 상용화할 수 있는 모델임을 확인하였다. 향후 연구과제는 본 논문에서 고려하지 않은 물리적인 위협 관련 대책 또한 연구함으로써 블록체인 기반의 전자 투표 시스템에 대한 활용이 활발하게 이루어 질 수 있도록 도움이 되고자 한다.

ACKNOWLEDGMENT

이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업과(NRF-2018R1D1A1B07040573) 2020년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임 (P0008703, 2020년 산업전문인력역량강화사업).

참 고 문 헌

[1] 유성민. (2020). CES 2020에서 살펴보는 탈중앙 화폐와 블록체인 현황. 한국통신학회지(정보와통신), 37(2), 64-70.

[2] 박근덕. (2017). 분산 원장 기술을 활용한 온라인 투표에 대한 보안 위협과 대응 방안. 한국정보보호학회논문지, vol.27, no.5, pp. 1201-1216. https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do?cbIdx=82618&bcIdx=18560&parentSeq=18560

[3] "A Blockchain Platform for the Enterprise" Hyperledger Fabric Docs. 2020년 1월 29일 수정, 2020년 5월 17일 접속, https://hyperledger-fabric.readthedocs.io/en/release-2.0/

[4] 황치규, "블록체인 기반 투표 시기상조… 아직 리스크 크다", THEBCHAIN, 2019.10.25, https://www.thebchain.co.kr/news/articleView.html?idxno=5972

[5] 김정숙. (2018). 블록체인 기반의 서비스 현황 및 문제점 분석. 융복합지식학회논문지, 6(1), 135-140. https://kpc4ir.kaist.ac.kr/index.php?document_srl=949&mid=kpc4ir_03_01_01