이더리움 기반 본인 인증을 통한 투표 플랫폼의 개발

강찬*, 권정*, 김영재*, 박경은*, 박성원*, 박진환*, 송수빈*, 신용호*, 신희평*, 안현준*, 이원빈*, 장희원*, 전유빈*, 조호성*, 최서희*, 최희민**, 김희열**

The development of a voting platform based on Ethereum for identity verification

Chan Kang*, Jung Kwon*, Youngjae Kim*, Kyungeun Park*, Seongwon Park*, Jinhwan Park*, Subeen Song*, Yongho Shin*, Heepyeong Shin*, Hyeonjun An*, Wonbin Lee*, Heewon Jang*, Yubeen Jeon*, Hosung Cho*, SeoHee Choi*, Heemin Choi** and HeeYoul Kim**

요 약

본 논문은 블록체인 기술을 활용하여 현재 투표 시스템의 취약점을 개선하는 방안을 제시한다. 이 시스템은 본인 인증, 중복 투표 방지 및 데이터 보안을 강화하여, 투표 과정의 투명성과 무결성을 보장한다. 또한, 모든 투표 기록을 블록체인에 저장하여 실시간 모니터링을 가능하게 하여 투표의 신뢰성을 높인다.

Abstract

This study develops a blockchain-based voting system that enhances electoral transparency and integrity by implementing a robust identity verification system. By preventing duplicate voting and publicly logging all voting records on the blockchain, the system ensures the authenticity and transparency of each vote. This approach not only strengthens voter confidence by allowing real-time monitoring of the voting process but also maintains voter anonymity while enabling public verification of the results. The application of blockchain technology promises to enhance the accuracy and legitimacy of elections, promoting greater democratic participation across various institutions.

Key words

Blockchain, Identity Verification, Real-time Monitoring, Voter Anonymity

Ⅰ. 서 론

본 논문은 블록체인 기술을 활용하여 현행 투표 시스템의 여러 취약점을 개선하고자 하는 프로젝트를 다룬다. 기존의 투표 시스템은 중복 투표, 부정 행위, 계산 오류 및 과정의 불투명성 등 다양한 문제점을 내포하고 있다. 이 프로젝트는 이더리움 기반의 본인 인증 시스템을 도입해 사용자의 신원을 확인하고 중복 투표를 방지함으로써 투표의 신뢰성을 제고하고자 한다. 또한, 모든 투표 기록을 블록체인에 공개적으로 저장하여 실시간으로 투표 과정을 모니터링할 수 있게 한다.

이 연구는 새로운 시스템이 어떻게 대학 내 민주적 참여를 강화하고 교육 기관의 선거 문화를 혁신하는지에 대해 평가한다. 현재 블록체인 기술은

*경기대학교 컴퓨터공학부,{dhwlddj2,johnk200019,dudwo4345,dolgoraen513,ikaros364125, pjh990925, soorud05, dydghfkrn, tlsgmlvud, 202014953, jhw001013, yubin1203, itskarnel}@kyonggi.ac.kr,
*경기대학교 스포츠과학부 ah0416@kyonggi.ac.kr, *경기대학교 신소재공학과 aryeel@kyonggi.ac.kr,
**경기대학교 컴퓨터공학전공 minco777@kyonggi.ac.kr, heeyoul.kim@kyonggi.ac.kr
※ 지원기관표기(사사표기)

금융, 의료, 부동산 등 다양한 산업에서 활용되고 있으며, 이러한 기술 동향을 바탕으로 투표 시스템에의 적용이 가지는 의미와 잠재적 영향을 심도 있게 분석한다. 본 논문은 또한 프로젝트가 직면할 수 있는 기술적, 사회적, 윤리적 도전 과제들을 다루고, 이에 대한 해결 방안을 모색한다.

Ⅱ. 본 론

2. 프로세스설계 및 시나리오

2-1 프로세스 설계

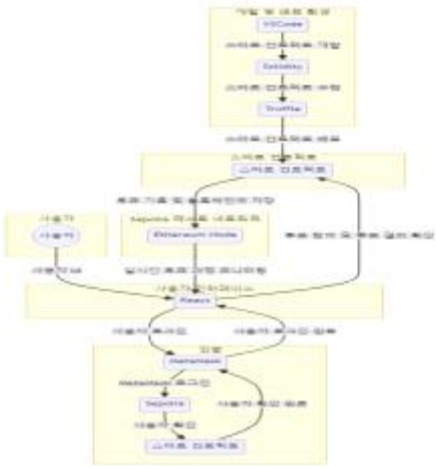

그림 1. 이더리움 기반 투표시스템 구조

사용자는 React 웹에서 로그인후 MetaMask로그인하여 Sepolia 테스트 넷에 주소를 저장, 스마트 컨트렉트에서 본인인증이 진행된다. 그후 사용자 확인이 완료되면 연결된 React 웹에서 투표에 참여한다. 투표 과정은 스마트 컨트랙트를 통해 이루어지며, 이를 VSCode를 통해 Solidity 언어를 이용, Truffle을 사용하여 배포한다. 스마트 컨트랙트는 Sepolia 테스트 네트워크에 투표 기록을 저장하고, 기록이 저장된 Ethereum Node를 통해 실시간 투표 과정을 보여준다. 이 시스템으로 사용자는 React로 개발한 웹을 통해 중복 투표가 방지된 투표참여와 투명성 있는 투표 과정을 실시간으로 모니터링할 수 있다.

2-2 투표자 시행 시나리오 요약

사용자는 웹에 접속하여 학번과 비밀번호를 입력한다. 데이터베이스를 통해 React웹에서 본인인증을 하여 자신의 신원을 확인받고 홈 화면으로 이동하게 된다. 이후, Metamask를 활용하여 이더리움 블록체인에 로그인하게 된다. 이때, 사용자는 기존의 Metamask 계정을 가지고 있을 필요가 있다. Metamask와의 연결이 확인되면 투표 참여 페이지로 이동하게 된다. 사용자는 투표 참여 페이지에서 후보자들의 프로필과 공약을 확인하고 투표에 참여할 수 있다. 투표가 마무리되면, 웹 페이지에서 투표 결과를 확인할 수 있는데 이때 투표 기록이 블록체인에 저장되어 사용자라면 누구든지 열람이 가능하다.

3. 시스템 및 주요 메커니즘

3-1 시스템 설계 및 주의사항

본 시스템은 Solidity 언어를 사용하여 React 웹으로 구현되었으며, 주요 기능으로는 사용자 관리, 본인 인증, 투표 처리, 데이터 보안 등이 있다. 사용자 관리는 웹사이트에 접속한 사용자가 회원가입을 통해 시스템에 등록하고 로그인을 할 수 있도록 하며, 본인 인증 부문에서는 Metamask를 이용하여 사용자의 신원을 확인한다. 투표 처리 부문에서는 스마트 컨트랙트를 활용해 투표를 진행하고, 데이터 보안은 투표 정보와 사용자 정보의 무결성을 유지하기 위해 중요하다. 이러한 각 부문은 시스템의 효율성과 안전성을 보장하도록 설계되었다.

메타마스크를 사용할 때의 주요 단점 중 하나는 사용자가 여러 개의 지갑 주소를 생성할 수 있다는 점이다. 이를 해결하기 위한 방법으로, 각 지갑 주소당 단 한 번의 투표만 허용하는 규칙을 설정한다. 이 조치는 사용자가 여러 주소를 통해 투표하는 것을 방지하며, 각 사용자가 주어진 투표권을 공정하게 사용하도록 보장한다. 추가적으로, 회원가입 시 신원 확인 절차를 도입한다는 가정 하에, 투표를 허락해주는 주소는 신원 확인 후 바로 다음에 생성된 주소로 한정한다.

3-2 본인 인증 메커니즘 및 데이터 보안

본인 인증 시스템의 구축은 사용자가 누구인지 확인하고 제공된 정보의 진위를 검증하는 필수적인 요소를 포함한다. 이 시스템을 선거 과정에 적용하면, 시스템상에서 본인 인증 절차를 거쳐 선거권을 가진 사람만이 투표할 수 있으며, 모든 유권자는 한 번만 투표가 가능하다. 또한, 중복

투표는 시스템상에서 자동으로 차단되어 투표의 신뢰성을 높이는 데 기여한다.[1] 이러한 시스템은 투표 과정에서의 정확성과 공정성을 보장하며, 유권자 신원의 정확한 검증을 통해 무효표 및 부정 투표의 위험을 줄인다. 본인인증 프로세스는 사용자가 웹사이트에 접속하여 MetaMask를 통해 자신의 이더리움 지갑 주소를 제공하는 과정에서 시작된다. 이 지갑 주소는 사용자의 디지털 신원을 대표하는 키로 기능하며, 사용자는 추가적으로 이름, 이메일 등의 개인 정보를 입력하여 스마트 컨트랙트에 저장한다. 이 정보는 블록체인 노드에 안전하게 기록되며, 초기 신원 확인을 위한 것으로 스마트 컨트랙트에 의해 검증된다.

로그인 시도 시, MetaMask는 사용자의 지갑 주소를 통해 인증을 요청한다. 스마트 컨트랙트는 블록체인 노드에 기록된 회원 정보를 조회하여 해당 지갑 주소와 연결된 데이터가 있는지 확인한다. 등록된 정보가 없을 경우, 사용자는 회원 가입 페이지로 리다이렉트되어 추가 정보를 제공해야 한다. 반면 정보가 존재할 경우, 사용자는 투표 등의 추가 권한을 부여받아 시스템을 이용할 수 있다.

데이터 보안 측면에서, MetaMask와 스마트 컨트랙트는 이더리움 블록체인의 강력한 암호화 기술을 활용하여 사용자 정보의 안전성을 보장한다. 모든 데이터는 변조가 불가능한 형태로 블록체인 노드에 기록되며, 개인 키를 이용한 디지털 서명을 통해 정보의 진위를 검증할 수 있다. 이러한 접근 방식은 데이터의 무결성을 유지하는 동시에, 사용자 인증을 위한 안전한 방법을 제공한다.

3-3 투명성 구현

투표에 있어서 투명성을 강화하기 위해 로그 공개가 필수적이다. 즉, 투표 참여에 대한 모든 기록이 공개되어 실시간 모니터링이 가능하게 함으로써, 모든 유권자가 선거 과정을 신뢰할 수 있도록 하는 방법이다.

블록체인은 분산형 원장 구조로서, 네트워크에 참여한 모든 사람이 거래에 대한 원장을 소유하고 모든 거래장부를 기록함으로써 거래의 투명성을 높인다.[2] 이러한 구조를 통해 기록된 데이터는 변경 불가능하고, 모든 투표 참여에 대한 로그를 홈페이지에 공개하여 사용자가 실시간으로 투표 참여를 모니터링할 수 있도록 한다. 이는 투표 과정에서 데이터의 무결성과 투명성을 보장하며, 유권자의 익명성을 유지하면서도 공개적인 검증 가능성을 제공하여, 투표의 신뢰성을 높이는 데 기여한다.

4. 시스템 상세

4-1 예상 웹페이지 상세 설명

1) 회원 가입 페이지

사용자는 웹사이트에 접속 후 로그인 화면에서 '회원 가입' 버튼을 클릭하여 이동한다. Metamask 계정이 필요하며, 계정 인증 후 사용자의 이름, 이메일 등 개인 정보를 입력하여 스마트 컨트랙트에 저장한다. 이 과정을 통해 회원 가입이 완료된다.

2) 로그인 페이지

회원 가입을 완료한 사용자는 Metamask를 이용해 투표자 권한을 부여받아 시스템을 이용할 수 있다.

그림 2.로그인 페이지에 Metamask인증을 도입한 모습

3) 홈페이지

로그인한 사용자는 투표자 권한을 받은 후 홈 이지에 접근한다. 이 페이지에는 투표 리스트와 투표 로그 페이지 열람 버튼이 제공된다. 사용자는 원하는 투표 주제를 선택하여 참여할 수 있다.

4) 투표 참여 페이지

사용자가 홈페이지에서 선택한 투표 주제에 따라 접근가능한 투표 참여 페이지에서는 후보자의 프로필과 공약을 확인할 수 있다.

1) 김도훈, 「블록체인 기반 온라인 투표 시스템 개발」, 『한국정보과학회 학술발표논문집』, 2023, 2,013 - 2,015

2) 안규황, 서화정, 「블록체인 기반 기부 시스템 개발」, 『 한국정보통신학회논문지』, 2018, 812-817.

그림 3. 예상 투표 참여 페이지

5) 관리자 페이지

특정 ID를 사용하여 로그인한 관리자만 접근할 수 있는 페이지로, 투표 등록 작업이 이루어진다. 관리자는 후보자의 사진, 프로필, 공약 등을 등록할 수 있다.

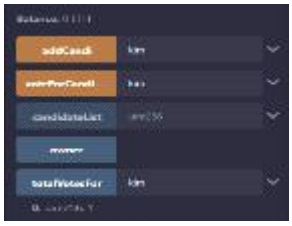

그림 4. Solidity로 구현된 후보자 등록 기능

6) 로그 페이지

홈 페이지에서 접근할 수 있는 로그 페이지에서는 스마트 컨트랙트를 통해 Ethereum Node에 저장된 투표 기록을 일부 사용자가 열람할 수 있도록 하여 시스템의 투명성을 유지한다. 이 페이지는 실시간으로 투표 과정을 모니터링하는 기능을 제공한다.

그림 5. 투표 기록을 나타내는 예상 로그 페이지

이 시스템 설계는 투표 시스템의 효율성과 보안을 강화하며 사용자가 쉽게 투표에 참여하고 투표 결과를 신뢰할 수 있도록 설계되었다.

Ⅲ. 결 론

5. 결론 및 기대효과

본 연구에서 제안된 블록체인 기반 투표 시스템이 실제로 구현된다면, 여러 중요한 기대효과와 이점이 있을 것이다. 먼저, 모든 투표 기록이 블록체인에 저장되어 불변성을 갖기 때문에 투표 과정의 투명성과 신뢰성이 크게 향상된다. 이러한 시스템은 유권자들에게 보다 안전하고 공정한 투표 환경을 제공함으로써 참여율을 높이고, 투표에 대한 신뢰감을 증진할 수 있다.

또한, 중복 투표를 방지하고 실시간으로 투표 과정을 모니터링할 수 있는 기능은 선거 과정에서의 부정 행위를 크게 줄일 수 있다. 점에서 큰 장점이다.

또한 전통적인 투표 시스템과 비교했을 때, 물리적인 투표소 설치나 운영에 드는 비용을 줄일 수 있으며, 장기적으로는 더 많은 자원을 선거의 다른 중요한 측면에 할당할 수 있다.

이 연구는 또한 투표 시스템에 블록체인 기술을 적용하는 것이 교육 기관, 지방 자치단체, 기업 내부의 선거 등 다양한 영역에서 실제 적용될 수 있는 가능성을 시사한다. 이를 통해 블록체인 기술이 단순히 금융 분야에 국한되지 않고, 사회의 다양한 분야에서 실질적인 변화를 가져올 수 있는 기술로 자리 잡을 수 있을 것이다.

Ⅳ. 참고 문헌

1) 김도훈, 「블록체인 기반 온라인 투표 시스템 개발」, 『한국정보과학회 학술발표논문집』, 2023, 2,013 - 2,015

2) 안규황, 서화정, 「블록체인 기반 기부 시스템 개발」, 『한국정보통신학회논문지』, 2018, 812-817.