

이더리움 블록체인 네트워크를 활용한 투표 시스템

허태성*, 김가겸^o, 한석현*
인하공업전문대학, 컴퓨터정보과^o
인하공업전문대학, 컴퓨터정보과*

e-mail: tshur@inhac.ac.kr*, rkrua5283@gmail.com^o, tjrqhd121@naver.com*

Voting system using Ethereum block-chain network

Tai-Sung Hur*, Ga-Gyeom Kim^o, Seok-Hyeon Han*
Dept.of Computer Science, Inha Technical College^o
Dept.of Computer Science, Inha Technical College*

● 요약 ●

현실 세계에서 진행되는 투표는 시간과 공간이라는 자원들을 낭비하면서 진행이 된다. 그에 따른 보완책으로 온라인 투표 시스템을 제안할 수 있지만, 이 경우 데이터를 저장한 중앙 서버가 해킹당할 경우 데이터의 무결성이 훼손되는 문제점을 야기할 수 있다. 본 논문에서는 이러한 문제점을 보완하기 위하여 블록체인 네트워크를 활용한 투표 시스템을 제안한다. 블록체인 투표 시스템을 응용하면 온라인으로 투표를 진행하여 시간과 공간이라는 자원을 절약할 수 있고 보안의 3요소 중 하나인 데이터의 무결성을 유지하여 투표 시스템의 투명성을 향상시킬 수 있다.

키워드: 블록체인 네트워크(Block chain network), 투표 시스템(Voting system), 무결성(integrity)

I. 서론

기존의 투표 시스템은 현실 세계에서 투표를 하기 위해서는 투표장에 투표자가 직접 방문하여 자신의 신분을 증명한 후 투표용지를 수령하여 투표장 내부에서 자신이 지지하는 후보자를 선택 후 투표용지를 투표함에 제출한다. 그리고 투표 기간이 종료되면 각 투표장에 있는 투표함의 투표용지를 수거하여 물리적인 방법으로 개표를 진행한다.

위와 같은 방식으로 진행하게 된다면 투표 기간 동안 투표장이라는 물리적인 자원을 사용하여야 하며 투표 결과를 원시적인 방법인 투표지 분류기 또는 수작업으로 집계를 하면서 투표를 진행하는 동안 공간적 또는 시간적 자원 낭비를 초래하게 된다.

이러한 문제점을 해결하기 위해 온라인상에서 투표를 진행하는 온라인 투표 시스템을 제안할 수 있다 그러나 기존의 온라인 투표 시스템의 방식으로는 서버에 투표 결과를 저장하게 되며 악의적인 사용자가 서버에 접근하여 임의로 데이터를 조작할 경우 데이터의 무결성이 위배되어 투표 결과에 대한 신뢰성을 떨어뜨리는 위험성이 존재한다.

본 논문은 온라인상에서 투표를 진행하면서 현실 세계의 자원을 절약하고, 데이터의 무결성을 지키므로서 투표 결과에 대한 신뢰성을 높일 수 있는 이더리움 블록체인 네트워크를 활용한 온라인 투표 시스템을 제안한다.

II. 본론

1. 관련연구

본 논문에서는 이더리움 방식의 블록체인 네트워크를 활용하여 투표 시스템을 구현한다. 이더리움 방식을 사용한 블록체인 네트워크의 중요 특징으로 비트코인 블록체인 네트워크와는 달리 화폐로서만 동작하는 것이 아닌 사용자의 목적에 따라서 자유로운 용도로 사용이 가능하다는 튜링의 완전성[1]이 있다. 또한 이더리움 블록체인 네트워크에서 사용자가 지정한 특정 조건을 만족할 경우 계약 조건을 이행하는 스마트 컨트랙트(Smart Contract)[2]를 사용할 수 있다.

2. 제안 환경

기존 온라인 투표 시스템은 투표 결과를 서버에 저장하여 데이터를 관리하는 방식이라면 이더리움 블록체인 네트워크를 활용한 투표 시스템은 해당 투표 시스템이 사용한 블록체인 네트워크의 사용자 전부가 해당 데이터를 저장하여 데이터의 무결성을 지키는 방식이다.

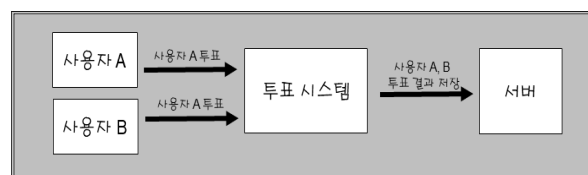


Fig. 1. Existing Online Voting System

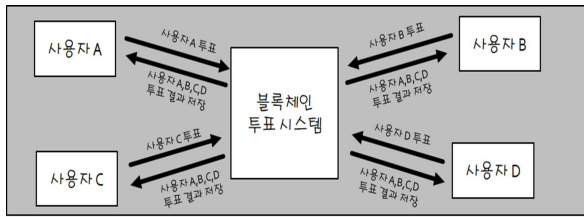


Fig. 2. Ethereum Block Chain Voting System

기존 온라인 투표 시스템의 진행 방식은 그림 1에서 보는 바와 같이 진행된다. 이 경우 서버에 저장된 투표 내용이 악의적인 사용자에게 의하여 데이터가 변조될 경우 투표에 대한 신뢰성이 깨지게 된다.

그러나 이더리움 블록체인 투표 시스템의 진행 방식은 그림 2에서 보는 바와 같이 진행되며 해당 투표 결과의 신뢰성을 깨뜨리기 위해서는 51% 이상의 이더리움 블록체인 네트워크 사용자의 데이터를 변조시켜야 하므로 기존 온라인 투표 시스템과 비교하여 투표 결과의 신뢰성을 높일 수 있다.

3. 제안 시스템

개발환경의 블록체인 투표 시스템을 구현 및 테스트를 진행하기 위하여 로컬 네트워크상에서 가나슈(Ganache)[3]를 이용하여 블록체인 네트워크를 구성하고 스마트 컨트랙트(Smart Contract)를 구현하는 언어로는 솔리디티(Solidity) 0.4.23[4]를 사용하며 해당 스마트 컨트랙트(Smart Contract)의 테스트를 위하여 node.js[5]를 사용한다.

4. 결과 화면

본 논문에서 구현할 블록체인 투표 시스템의 테스트 결과 화면은 다음과 같다.

후보자	투표수
김철수	2
이영희	0
박복희	1

김철수 [선택] 투표하기

Fig. 3. Block Chain Voting System

```
> deployedContract.address
'0xe271ce2bd44cc96e22f15cf26057e1643c769020'
```

Fig. 4. Address of Smart Contract

그림 3에서 보는 바와 같이 '김철수 후보에게 투표한다'는 조건을 그림 4의 주소로 전송할 경우 스마트 컨트랙트의 조건을 만족 시키면서 해당 데이터를 이더리움 블록체인 네트워크에 참가한 모든 사용자에게 데이터를 전송하여 투표 결과를 관리 보관하게 한다.

IV. 결론

본 논문에서 제안한 이더리움 블록체인 네트워크를 활용한 투표 시스템을 활용할 경우 원본 데이터를 모든 사용자가 소유하면서 보안의 3대 요소[6] 중 하나인 데이터의 무결성을 지킬 수 있게 되어 기존 온라인 투표 시스템의 문제점인 투표 결과의 신뢰성에 대한 문제점을 해결할 수 있으나 투표 결과의 기밀성을 지키는 것이 힘들어진다. 그러므로 해당 특성을 보완할 방법에 관한 연구가 필요하다.

REFERENCES

- [1] <https://github.com/ethereum/wiki/wiki/%5BKorean%5D-White-Paper>
- [2] https://en.wikipedia.org/wiki/Smart_contract
- [3] <https://www.trufflesuite.com/ganache>
- [4] <https://solidity.readthedocs.io/en/v0.4.23/>
- [5] <https://nodejs.org/ko/>
- [6] <https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA>