JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 22, No. 12, pp. 2129-2137, Dec. 2021

Check for updates

스마트 컨트랙트를 활용한 거버넌스 시스템 설계 및 구현

제 갈 은[1] · 이 수 연[1] · 강 서 진[1] · 강 남 희[2*]
[1]덕성여자대학교 IT미디어공학과 학사과정
[2*]덕성여자대학교 사이버보안전공 교수

Design and Implementation of a Governance System Using the Smart Contract

Eun Jegal[1] · Soo-Yeon Lee[1] · Seo-Jin Kang[1] · Namhi Kang[2*]

[1]Bachelor's Course, Department of IT Media Engineering, Duksung Women's University, Seoul 01369, Korea
[2*]Professor, Department of Cyber Security, Duksung Women's University, Seoul 01369, Korea

[요 약]

국내외 다양한 산업 영역에서 블록체인 기술에 대한 관심이 높아지며 우리 정부에서도 '블록체인 기술 확산 전략'을 발표하며 공공분야 디지털 플랫폼 기획 의지를 제시한 바 있다. 기존의 온라인 서비스의 경우 위□변조가 가능하고 신뢰성 보장이 어려워 공적인 활용에 제한이 있다. 이에 대한 해결 방안으로 블록체인 기술에 사용되고 있는 스마트 컨트랙트를 활용할 수 있다. 본 논문에서는 스마트 컨트랙트를 활용한 거버넌스 모델을 설계하고 구현한다. 해당 모델을 활용한 대표적 예시로서 투표 서비스와 근로 계약서 관리 서비스를 제안하며, 이는 기존 서비스의 무결성 및 신뢰성 문제를 해결할 수 있다. 스마트 컨트랙트는 탈중앙화, 위□변조 방지, 투명성, 익명성과 함께 자동실행이라는 특징을 가지기 때문에 거버넌스 모델에 사용하기 적합하다.

[Abstract]

As interest in blockchain technology is growing in various domestic and foreign industries, the Korean Government has also announced a 'blockchain technology diffusion strategy', suggesting its will to plan a digital platform in the public sector. In the case of existing online services, there is a limit to public use due to the possibility of forgery and alteration and difficulty in ensuring reliability. As a solution to the limitations, the smart contract using in blockchain technology can be used. In this paper, we design and implement a governance system using the smart contract. As representative examples of the system, an online voting service and a labor contract management service are proposed, which can solve the integrity and reliability problems of existing services. Smart contract are suitable for use in governance models because they are characterized by decentralization, prevention of forgery, transparency, and anonymity as well as automatic execution.

색인어 : 블록체인, 스마트 계약, 거버넌스, 투표 시스템. 분산 어플리케이션

Keyword : Blockchain, Smart Contract, Governance, Voting System, Decentralized Application

http://dx.doi.org/10.9728/dcs.2021.22.12.2129

Received 20 November 2021; **Revised** 10 December2021
Accepted 10 December2021

***Corresponding Author; Namhi Kang**

Tel: +82-2-901-8349
E-mail: kang@duksung.ac.kr

Ⅰ. 서 론

블록체인(Blockchain) 기술은 분산화된 디지털 거래원장을 관리하는 기술로 정의할 수 있다 [1]. 블록체인은 중앙서버나 제3의 기관에서 정보를 보관하지 않고 분산된 참여자들이 원장을 저장하는 방식으로 단일 장애점 (SPoF: Single Point of Failure) 문제를 해결할 수 있다. 또한, 분산 저장된 거래 기록은 공개되고 있어 추적이 가능하고 위·변조가 사실상 불가능한 특성으로 거래 양성화가 가능한 장점이 있다 [2]. 초기 블록체인 기술은 암호화폐를 필두로 금융 산업에서 화제가 되었으나, 탈중앙화를 통해 데이터 투명성과 데이터 완결성을 담보할 수 있는 특성을 통해 사회의 공공부문, 즉 '거버넌스(governance)'로의 확산 또한 가능하다.

거버넌스는 공공과 민간영역의 경계가 흐려지고, 기존 정부 및 전문가 집단에 의해 주도되던 형식에서 확장하여 다양한 참여주체의 협력을 통해 정책을 결정하고 집행하는 사회적 협치 시스템이다 [3]. 공공부문의 책임성과 신뢰저하를 포함한 전통적 행적 패러다임의 한계에 기인하여 중앙집중된 대의민주제를 극복할 새로운 대안으로서 블록체인 기술을 활용할 수 있다. 거버넌스에서 가장 중요한 요소인 신뢰를 블록체인이 기술적으로 제공할 수 있기 때문이다.

블록체인 기반 응용의 핵심 기술 중 하나인 스마트 컨트랙트(Smart Contract)는 1994년 암호학자 Nick Szabo가 처음 제안한 방법으로 계약의 협상을 디지털 방식으로 시행하기 위한 프로토콜이다. 이는 특정 조건이 충족되었을 때 제3자의 개입이나 처리를 위한 도움 없이도 계약이 자동 채결되고 동시에 이행될 수 있다는 특징을 가진다. 기존 서면으로 작성하는 계약에 비해 계약의 내용이 명확해지고 조건에 따른 이행이 즉시 가능하다[4].

과학기술정보통신부는 지난 2020년 6월 대통령직속 4차 산업혁명위원회 제16차 전체회의에서 블록체인 기술을 도입하겠다는 내용을 담은 '블록체인 기술 확산 전략'을 발표했다. 해당 전략에 따르면 중점 추진 과제인 '7대 분야 전면 도입' 내 온라인 투표를 제시하고 있으며, 분산신원증명 서비스 활성화를 통해 '거버넌스 구축' 또한 추진 전략으로 삼고 있음을 명시하고 있다. 즉, 기존의 한계를 극복하는 차세대 블록체인 기술을 확산시켜 국가 차원에서 디지털 신기술 기반의 공공분야 디지털 플랫폼의 기획 및 구축을 지원하겠다는 계획이다.

본 논문에서는 블록체인 기반 스마트 컨트랙트를 활용한 거버넌스 시스템을 구현하여 계약의 위/변조를 방지하고 데이터의 신뢰성과 무결성을 보장할 수 있음을 보인다. 제안 시스템에서 작성한 스마트 계약은 프로그램 상에서 자동으로 이루어지게 한다. 블록체인에 기반한 거버넌스 모델의 대표적 예시로서 투표 서비스와 근로 계약서 관리 서비스를 구현하고 동작 방식을 설명한다. 블록체인 기반 스마트 컨트랙트를 활용한 두 응용 서비스의 기술적 기저와 시스템 동작 구조는 매우 유사하다.

본 논문의 구성은 다음과 같다. 2장에서는 추천 시스템 및 블록체인 기반 거버넌스 모델 중 투표 시스템에 관련된 연구들을 기술한다. 3장에서는 거버넌스 시스템의 공통 모듈로 적용되는 스마트 컨트랙트의 구현 방안을 다룬다. 4장에서는 블록체인 기반 투표 시스템을, 5장에서는 근로 계약 서비스 시스템을 소개하며 각각의 구현 및 동작에 대해 설명한다. 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 관련 연구

박진상 등은 컨소시엄 블록체인 거버넌스 프레임워크에 대한 제안을 하였다 [5]. 해당 연구에서는 기능 및 역할과 책임을 포함하여 의사결정권, 책임성, 보상체계와 같은 '블록체인 거버넌스' 요소 측면에 집중한다.

컨소시엄 블록체인의 두 주체는 거버너(Governor)와 멤버(Member)로 나뉜다. 거버너는 컨소시엄 블록체인의 실질적인 운영 및 관리 주체로서 블록체인의 시스템 개발, 노드관리, 원장관리와 트랜잭션 관리 등의 기능을 담당하며, 각 멤버는 개인키와 공개키를 소유하며 해당 키들을 통해 블록체인 네트워크의 운영주체로 인식되어 블록을 생성하며 검증할 권리를 갖는다.

한성주 등은 기존의 전자투표 방식과 블록체인 기술 기반의 전자투표 시스템과의 비교를 통해 해당 기술의 안정성을 강조한다 [6]. 기존 전자투표의 방식은 PSEV(Poll Site Electronic Voting), Kiosk, REV(Remote Electronic Voting) 등이 있는데, 이 방식들은 각각 투표결과 반영 여부 확인 과정, 전자투표의 완결성, 비밀투표 충족 측면에서 문제점을 가져 투표결과에 불신을 줄 수 있다. 블록체인 기반의 전자투표는 유권자가 노드로 인정받기 위해서 개인 인증 과정을 거쳐야 하기 때문에 가짜 노드를 생성하며 인증받지 못한 투표를 행사하는 것이 불가능하여 안정성과 신뢰성을 향상시킬 수 있다.

이루다 등은 스마트 계약을 구현하기 위한 환경으로 이더리움을 사용한 블록체인 전자 투표 시스템을 제안하였다 [7]. 본 전자투표 시스템은 스마트 컨트랙트로 구현하여 P2P 네트워크를 통해 서비스를 제공하므로 클라이언트와 서버의 구분을 두지 않는다. 투표는 개설 시점에 도달하면 시작되고, 트랜잭션으로 블록체인에 마이닝하여 배포한다. 유권자는 투표할 대상을 선택하며 자신의 전자 지갑(Wallet)을 사용해 후보자에게 투표를 한다. 투표를 실행하는 함수 내에서 유권자를 검증하고 중복투표를 제어하고 있으며, 투표를 하면 sendRawTransaction() 함수를 통해 자신의 전자 지갑을 개인키로 하여 투표 과정을 완료한다. 모든 투표는 블록체인에 기록되고 거래가 승인된 블록은 블록체인에 연결된다.

다만, 해당 연구 내에서는 스마트 컨트랙트의 특징 및 보편적인 구현 환경에 집중하여 실제 스마트 컨트랙트 내 기록되어야 하는 정보와 구현 방식의 설명은 부족하다. 본 논문에서는 스마트 컨트랙트를 직접 설계하여 구조를 설명하고, 거버넌스 서비스 모델에 공통적으로 사용 가능한 모듈을 제안하

여 서비스 구현의 유연성을 높이고자 한다.

염상희 등은 블록체인을 활용하여 비정규 시간제 근로계약 체결 및 관리 시스템을 설계하였다 [8]. 표준근로계약서 양식을 전자 상으로 작성 및 체결하며 열람의 기능이 가능하다. 제안 시스템은 근로자 및 사업주의 사용자, 근로계약서, P2P 네트워크, 계약서 보관용 스토리지로 구성된다. 사업주에 의해 계약서 작성이 시작되며 근로자는 최종적으로 서명검증을 수행한다. 해당 연구는 근로계약서의 작업 증명 및 계약서 검증의 프로토콜에 초점을 맞추고 있다.

Ⅲ. 시스템 공통 모듈

블록체인 시스템에서는 참여자들 간의 거래가 저장되며 거래에서 발생하는 다양한 정보는 블록체인에 담기게 된다. 블록체인은 암호학적으로 안전한 해시(Hash) 함수를 사용한 데이터 연결 구조와 모든 참여자들의 합의에 의해 관리가 이루어지기 때문에 데이터의 위/변조가 어려워진다는 특성을 가진다 [9]. 이러한 무결성과 신뢰성의 제공은 거버넌스 모델의 필수 요구조건에 해당한다.

또한 거버넌스 모델에서 중요한 점은 조건에 따른 거래의 이행이다. 스마트 컨트랙트는 프로그램(코드)에 거래의 조건을 담아 거래가 자동적으로 이행되도록 하는 것이다[10]. 한번 작성된 계약은 조건이 충족된다면 진행이 자동으로 이루어진다. 거래가 자동으로 수행되기 때문에 중개자의 개입 없이 사용할 수 있다. 모든 참여자가 같은 형식의 스마트 컨트랙트를 전달받기 때문에 다른 참여자의 거래 조건과 이행 여부를 감시할 필요가 없다. 또한 스마트 컨트랙트를 활용하여 거래의 조건들을 체계적으로 관리할 수 있다.

본 장에서는 제안 시스템에서 공통 모듈로 사용 가능한 블록체인 기반 스마트 컨트랙트 설계를 제안한다. 블록체인 기반 스마트 컨트랙트는 탈중앙화, 위/변조 방지, 투명성, 익명성과 함께 자동실행이라는 특징을 가지기 때문에 거버넌스 모델에 사용하기 적합하다고 판단하였다 [11].

본 논문에서 제안하는 투표 시스템과 근로 계약 시스템은 본장에서 설계한 스마트 컨트랙트를 공통으로 활용하여 구현된다. 이를 위해 본장에서는 스마트 컨트랙트를 활용하여 구현되는 투표 시스템과 근로 계약 시스템의 주요 요구 사항들을 기술한다. 설계 및 구현하는 시스템의 경우 이더리움 기반 블록체인을 사용한다.

3-1 공통 모듈 스마트 컨트랙트 설계

제안 시스템에서는 다양한 응용에서 이행되어야 할 조건들을 함수로 구성하여 스마트 컨트랙트에 저장한다. 제안 시스템은 서비스 진행을 위해 스마트 컨트랙트를 배포하여 사용한다. 해당 함수 사용 시 트랙잭션을 생성하여 함수를 사용하는 정보를 블록에 저장한다. 해당 스마트 컨트랙트는 사용자들의 상이한 요구사항이 저장되며 블록체인의 특성으로 위/변조가 불가능하다.

그림 1은 공통 모듈 스마트 컨트랙트 설계와 동작 방법을 나타낸다.

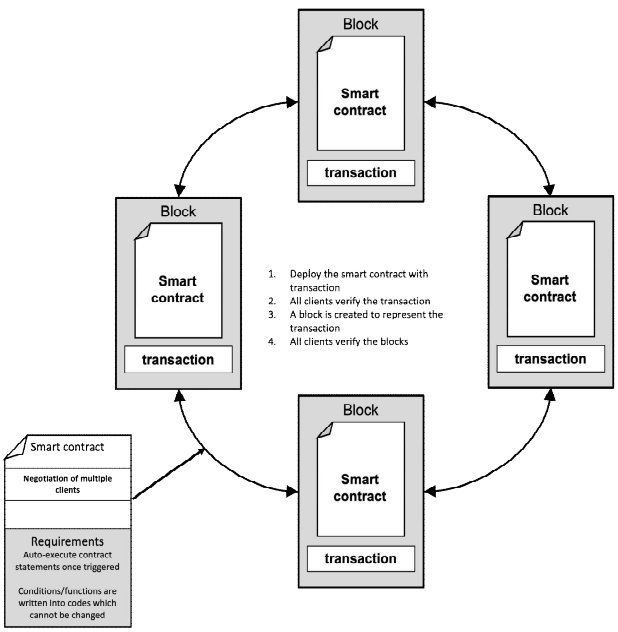


그림 1. 공통 모듈 스마트 컨트랙트 설계와 동작 방법
Fig 1. Design of smart contract and deployment

스마트 컨트랙트를 이용한 서비스가 진행 시 바뀌지 않아야 하는 조건이 담긴 컨트랙트를 설계하고 배포한다. 배포된 컨트랙트는 해당 컨트랙트를 이행하는 모든 사용자가 전달받는다. 사용자가 전달받은 스마트 컨트랙트를 이용할 때 발생하는 모든 트랜잭션은 블록에 저장되고 모든 사용자들은 이를 공유한다.

3-2 투표 시스템 요구 사항

투표 시스템은 선거장 등록 단계, 후보자 등록 단계, 유권자 확인 단계, 투표 단계, 개표 단계로 구분할 수 있다. 모든 단계들이 스마트 컨트랙트에서 관리된다. 다음은 각 단계의 과정을 간단하게 설명한다.

1) 선거장 등록 단계

선거관리위원회에게 입력(Input)으로 받은 선거장 정보를 확인 후 선거장의 ID와 투표 시작 값을 'False'로 초기화 후 선거장 리스트에 저장한다. 저장 후 선거장의 ID를 사용자에게 전달한다.

2) 후보자 등록 단계

선거관리위원회에게 입력으로 받은 후보자의 정보를 확인 후 해당 후보자가 속한 선거장의 ID, 후보자의 ID, 득표수를

0으로 초기화 후 후보자 리스트에 저장한다. 저장 후 후보자의 ID를 사용자에게 전달한다.

3) 유권자 확인 단계

유권자에게 입력으로 받은 유권자의 정보를 확인 후 해당 유권자가 투표 가능한 유권자인지 확인한다.

4) 투표 단계

선거관리위원회가 투표를 시작하면 선거장의 투표 시작 값이 'True'로 변환된다. 이 과정에서 앞서 인증된 유권자들에게 지갑을 생성하고 스마트 컨트랙트를 전달한다. 유권자들이 투표권을 행사할 때 먼저 유권자의 ID가 투표자 리스트의 존재하는지 여부를 확인한다. 투표자 리스트에 해당 유권자의 ID가 존재하지 않을 경우 투표권을 행사할 수 있다. 유권자가 투표권을 행사 시 유권자의 ID와 선택한 후보자가 있는 선거장의 ID를 투표자 리스트에 저장한다. 또한 유권자가 선택한 후보자의 ID를 해당 선거장 내에서 확인 후 같은 값이 있다면 해당 후보자의 득표수를 1 증가 한다. 해당 유권자의 ID는 투표자 리스트에 저장되었기 때문에 재투표 진행 시 'True'를 반환하여 중복투표를 제어한다.

6) 개표단계

선거관리위원회는 종료된 투표장을 확인 후 개표를 진행한다. 개표 진행 시 입력받은 선거장의 ID를 확인한 후 해당 선거장의 ID, 선거장에 속한 후보자들의 ID, 해당 후보자들이 받은 득표수를 사용자에게 전달한다.

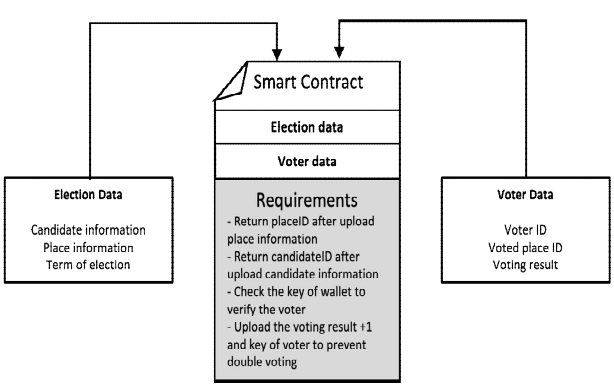


그림 2. 투표 시스템 스마트 컨트랙트 설계
Fig. 2. Design of smart contract for voting system

모든 단계에서 발생하는 사용자들의 요구 사항을 기반으로 그림 2와 같이 스마트 컨트랙트를 설계한다. 스마트 컨트랙트를 전달받은 사용자가 요구 사항을 입력하고 전달할 때 마다 발생한 정보들은 블록에 저장하여 안전하고 공정한 투표 시스템을 구축한다[12].

3-3 근로 계약 시스템 요구 사항

근로 계약 시스템은 사업자 채용공고 등록 단계, 지원자 등록 단계, 지원자 확인 단계, 지원자 채용 단계, 지원자 협상 단계로 구분할 수 있다. 다음은 각 단계의 과정을 설명한다.

1) 사업자 채용공고 등록 단계

채용을 진행하는 사업장에게 입력(Input)으로 해당 사업장의 공고 정보를 받는다. 해당 사업장의 정보를 확인 후 사업장의 ID와 채용 시작 값을 'True'로 초기화 후 사업장 리스트에 저장한다. 저장 후 사업장의 ID를 사용자에게 전달한다.

2) 지원자 등록 단계

지원자는 자신이 지원하고자 하는 사업장을 확인 후 자신의 정보를 입력(Input)한다. 입력받은 정보를 확인한 후 해당 지원자가 속한 사업장의 ID, 지원자의 ID, 채용 여부를 false로 초기화 후 지원자 리스트에 저장한다. 저장 후 지원자의 ID를 사용자에게 전달한다.

3) 지원자 확인 단계

공고 진행 중인 사업장은 자신의 사업장으로 지원한 지원자들의 정보를 확인할 수 있다.

4) 지원자 채용 단계

해당 공고가 마감되면 사업장의 채용 시작 값을 'False'로 변환한다. 해당 공고장은 자신의 공고장 ID를 확인한 후 지원자 리스트를 확인하고 지원자 채용을 시작한다.

5) 지원자 협상 단계

채용 예정의 지원자들과 해당 사업장은 근로 계약서에 담길 정보들을 협상한다. 최종적으로 협상이 완료된 지원자의 채용 여부는 'True'로 변환된다. 협상된 정보를 스마트 컨트랙트에 저장한다.

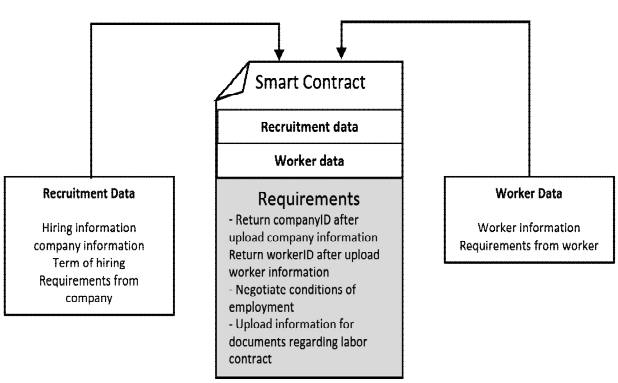


그림 3. 근로 계약 시스템 스마트 컨트랙트 설계
Fig. 3. Design of smart contract for lobor contract system

모든 단계에서 발생하는 사용자들의 요구 사항을 기반으로 그림 3과 같이 스마트 컨트랙트를 설계한다[12]. 스마트 컨트랙트를 전달받은 사용자가 요구 사항을 입력하고 전달할

때 마다 발생한 정보들은 블록에 저장한다. 또한 근로계약서 조건에 맞춰 사용자들에게 입력받은 조건을 저장하여 안전하고 투명한 근로 계약 시스템을 구축한다.

3-4 스마트 컨트랙트 구현 및 활용

그림 4는 본 장에서 제안하는 스마트 컨트랙트를 활용한 시스템의 동작 과정 및 순서를 다이어그램으로 나타낸 것이다.

제안하는 시스템 구현은 이더리움 시험 환경인 Ethereum tesetRPC를 활용했다. 또한, 블록체인 기반 웹서비스와 스마트 기기용 앱서비스 개발을 위해 Express.js와 web3.js를 활용했다. 웹 및 앱 서비스를 통해 스마트 컨트랙트 내에 함수가 사용될 때 발생되는 데이터들은 블록체인에 저장된다.

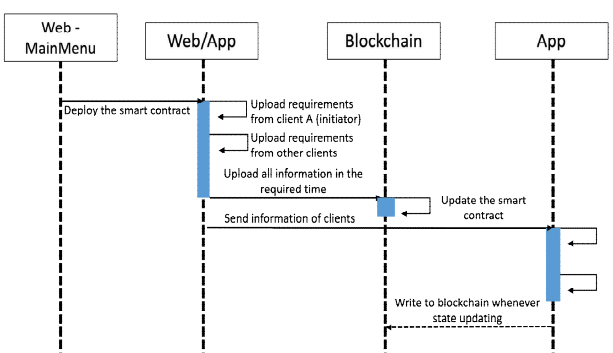


그림 4. 블록체인 기반 시스템 시퀀스 다이어그램
Fig. 4. Sequence diagram of blockchain-based system

Ⅳ. 전자 투표 시스템 구현 및 시험

표 1은 전자투표 시스템을 구현하기 위해 적용한 개발 환경을 나타낸다.

표 1. 개발 환경
Table 1. development environment

Development Language	Solidity, Node.js, web3.js, Java, MySQL
Hardware	3 Computers (i5 2.3GHz CPU)
Operating Systems	Linux Ubuntu
Network	P2P Ethereum Network

4-1 사전 준비

제안 시스템에서는 선거관리위원회가 선거장을 사전에 생성해야 한다. 선거관리위원회가 웹 사이트에 선거장 이름, 선거기간, 투표 시작 및 종료 시간, 선거 내용, 선거장 포스터를 첨부하여 작성한 뒤에 등록한다. 선거장을 등록한 후 '투표 시작' 버튼을 눌러야 투표가 개시된다. 선거장을 등록하면 데이터베이스의 선거장의 상태(isStarted)가 0이 되고 투표가 시작되면 상태는 1로 바뀐다.

선거관리위원회는 후보자도 사전에 생성해야 한다. 선거장 번호, 후보자 번호, 후보자 이름, 선본명, 구호, 후보자 사진, 공약, 지원하는 선거를 선택하여 후보자를 생성한다. 예비 후보자를 등록할 때는 데이터베이스에 저장되고 블록체인에는 따로 배포되지 않는다. 예비 후보자에서 '등록'버튼을 누를 때만 블록체인에 배포된다. 예비 등록 후보자일 때는 상태(state)가 0이고, 등록된 후보자일 때는 상태(state)가 1로 변경된다.

4-2 트랜잭션

선거장 관리 카테고리에서 만든 선거장을 확인할 수 있다. '시작'버튼을 누르면 선거가 시작되며 상태(isStarted)가 1로 바뀐다. 또한 '종료' 버튼을 누르면 선거장의 상태(isStarted)가 2로 바뀌며 선거가 종료된다. 종료되면 개표 결과를 확인할 수 있다. 선거가 시작 및 종료될 때마다 트랜잭션이 생성되어 블록체인에 배포된다.

그림5에서 트랜잭션의 모습을 확인할 수 있다.

그림 5. 선거장 생성 및 종료 트랜잭션
Fig. 5. Election Field Creation and Closing Transactions

투표도 마찬가지로 블록체인에 기록이 되는데, 유권자는 투표할 후보자를 선택하고 자신이 부여받은 지갑을 이용해서 투표한다. 선거장 번호, 후보자 번호와 유권자의 아이디는 스마트 컨트랜트에 저장되며 블록체인에도 기록된다. 배포된 블록에는 트랜잭션 주소, Gas 비용, 블록 번호, 타임스탬프가 저장된다. 선거장 등록 및 후보자 등록할 때 부여받은 지갑으로 sendTransaction()함수를 사용하여 Gas 비용을 지불한다.

4-3 투표 서비스 동작

유권자는 투표권을 행사하기 위해 애플리케이션에 회원가입을 한다. 회원가입 시 중복 회원가입을 방지하기위해 아이디를 확인하는 절차를 수행하고, 아이디를 기본 키로 지정하였다. 회원가입 후에 로그인하여 투표를 진행할 수 있다.

로그인하고 투표를 진행할 선거장을 선택한다. 후보자를 선택하기 전에 본인을 증명하기 위한 이메일 OTP 인증 절차를 거친다. 해당 이메일로 인증번호가 전송되고 번호를 맞게 입력하면 인증에 성공한다. 인증에 성공하면 후보자를 선택할 수 있다. 후보자를 선택한 후 투표를 하면 유권자의 투표 여부를 확인한다. 유권자가 투표했을 때 스마트 컨트랙트에 유권자의 아이디를 저장하도록 구현하였다. 따라서 다음 투표권을 행사할 때 해당 학번이 스마트 컨트랙트에 존재하면 투표할 수 없다.

선거관리위원회가 웹을 통해 선거를 종료하면 개표를 할 수 있다. 개표 시 블록을 암복호화를 통해 개표 과정을 거쳐야 하나 이는 네트워크 오버헤드가 야기될 수 있다. 따라서 투표하면 데이터베이스에 후보자 득표수가 저장될 수 있게 구현하였다. 개표 시에는 데이터베이스에서 후보자 득표수를 가져와 빠른 개표가 가능하다.

4-4 시스템 평가

본 절에서는 제안하는 투표 시스템이 안정성과 신뢰성을 보장할 수 있는지 평가한다. 해당 평가를 수행하기 위해 정부의 중앙선거 관리 위원회가 제시하고 있는 온라인 투표의 기준(표 2 참조)을 충족하는지 분석한다.

표 2. 온라인 투표 기준
Table 2. Online Voting Criteria

Category	Contents
Accuracy	Every voting value must be reflected accurately in the result of a vote. Only valid voting value can be included.
Verifiability	We need a function to verify that the voting process is operating and counted correctly.
Soundness	There should be no obstruction of the coercion by dishonest votes. in the final count, an illegal vote should be disclosed so that the election must not be affected
Eligibility	Only voters who are entitled to vote can vote.
Prevention of double voting	There must not be any cases in which one person who vote more than twice.
Privacy	There must not be any connections between voter and vote.
Fairness	E-voting should be fair so that there are not some candidates or some voters who have unlawful effects at the voting stage.

1) 정확성

제안 시스템에서는 투표 행위에 유관한 정보들이 블록체인에 저장되기 때문에 유권자의 투표 데이터의 무결성을 제공할 수 있다. 리를 합산한 결과를 도출하기 때문에 투표의 정확성이 보장된다.

2) 확인성

선거장 생성 및 종료, 후보자 생성, 투표마다 트랜젝션(transaction)으로 배포되어 블록체인에 저장되기 때문에 기록을 확인할 수 있다. 즉 트랜젝션의 수로 투표의 과정에서 위조가 되었는지 확인할 수 있기에 보장할 수 있다.

3) 완정성

블록체인의 모든 블록은 암호학적 해쉬함수로 처리되어 사슬처럼 연결되어 있으며, 현재의 컴퓨팅 자원으로는 각 블록에 사용된 해쉬함수의 역산이 사실상 불가능하므로, 기존 블록에 문제가 있더라도 이미 생성되어있는 블록의 내용을 수정하거나 무효로 할 수 없다[13]. 이처럼 투표하면 Smart Contract에 저장되어 블록체인에 배포되기 때문에 투표 데이터를 임의로 조작하는 것은 불가능하여 완정성이 보장된다.

4) 단일성

투표를 진행하기 전, 유권자는 본인 인증을 위해 two-factor 인증 방안으로 이메일 인증 절차를 수행한다. 인증을 완료한 이용자에게 지갑이 생성되고, 지갑을 가지고 있어야 투표할 수 있다. 따라서 인증절차를 거치지 않은 이용자는 투표할 수 없다.

5) 합법성

회원가입 시 유권자의 아이디를 기본 키로 정하고 데이터베이스의 회원 존재 유무를 확인하는 절차를 거친다. 데이터베이스 이외에도 스마트 컨트랙트에서 setVote() 함수를 통해 중복된 유권자가 블록에 저장되어 있는지 검사한다. 따라서 동일한 사람이 여러 계정으로 투표하는 부정투표를 방지할 수 있다.

6) 기밀성

투표를 하는 과정에서 후보자의 득표와 유권자의 투표 결과를 분리하여 저장한다. 블록체인의 특성으로 투표 결과는 투명하게 공개될 수 있으나 투표결과와 유권자를 매핑할 수 없도록 하여 기밀성을 보장한다.

7) 공정성

선거운영의 주체인 선거관리위원회가 선거를 종료시켜야만 개표할 수 있도록 구현했다. 즉 유권자가 선거 도중에 투표 결과를 추론할 수 있는 방법이 없기에 공정성이 보장된다.

8) 블록체인 계정 노출로 인한 신뢰성 향상

제안 시스템의 차별점은 블록체인 계정의 노출이다. 기존 온라인 투표의 문제점은 비밀투표의 보장이었다. 이에 대한 방안으로 사용자가 본인의 투표지가 블록체인에 의해 안전하

게 보호되고 있다는 사실을 보여주는 것이다. 블록체인의 계정 10개를 임의로 가져와 노출함으로써(그림 8 참조) 가능하게 했다. 사용자에게 간접적으로 블록체인 사용 여부를 알려주어 신뢰감을 높일 수 있다. 해당 노출되는 계정은 유권자의 계정과 연결되어 있지 않아 기밀성이 보장되며 비밀투표에 관한 사용자의 불안감도 감소시킬 수 있다.

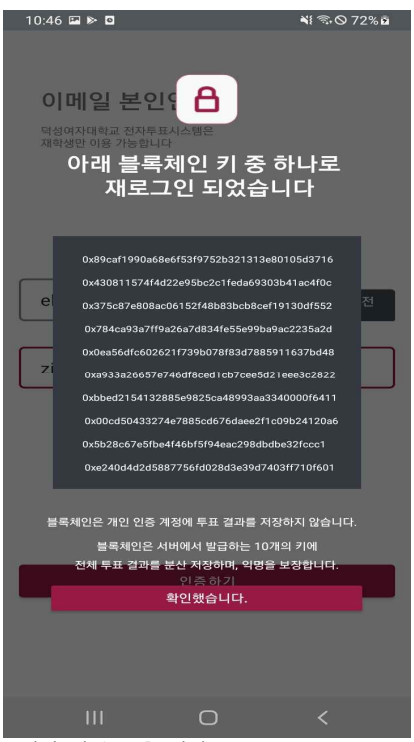


그림 6. 블록체인 계정 노출 화면
Fig. 6. Screen Shot of Blockchain Account Exposure

Ⅴ. 근로 계약 서비스 시스템 구현 및 동작

5-1 고용 서비스 동작 개요

제안 시스템은 고용주가 사업장 공고를 사전에 생성하도록 한다. 고용주는 근로 계약 서비스에 해당 사업장 이름, 공고 기간, 공고 내용을 작성한 뒤 등록한다. 등록하면 데이터베이스에 사업장 정보가 저장되며 트랜잭션으로 배포되어 블록체인에 저장된다.

공고를 등록한 후 '공고 시작' 버튼을 눌러야 공고가 사용자에게 공개된다. 근로 희망자는 공고를 보고 본인 이력서를 등록한다. 고용주는 공고 기간 내에 예비 근로자와 면접을 진행하고 애플리케이션으로 고용할 근로자를 선택한다. 근로자를 선택하면 근로계약서가 스마트 컨트랙트에 작성되고 블록에 저장된다. 공고 기간이 지나면 고용주는 '공고 종료' 버튼을 누른다.

5-2 근로 계약 관리 서비스

근로 희망자는 공고 기간 내에 이름, 사진, 경력, 지원하는 공고를 선택하여 이력서를 생성한다. 생성한 이력서는 애플리케이션으로 확인할 수 있으며 고용주는 회원가입을 해야 확인할 수 있다. 회원가입 시 사업자 번호를 입력하고 정상 등록된 사업자인지 확인하는 절차를 거친다.

로그인하면 자신이 등록한 공고와 지원한 근로자를 확인할 수 있다. 면접을 진행한 후 최종적으로 고용할 근로자를 투표하면 근로계약서가 스마트 컨트랙트로 배포되면서 블록체인에 저장한다. 그림 7은 근로 계약서 앱 서비스 화면을 보여준다.

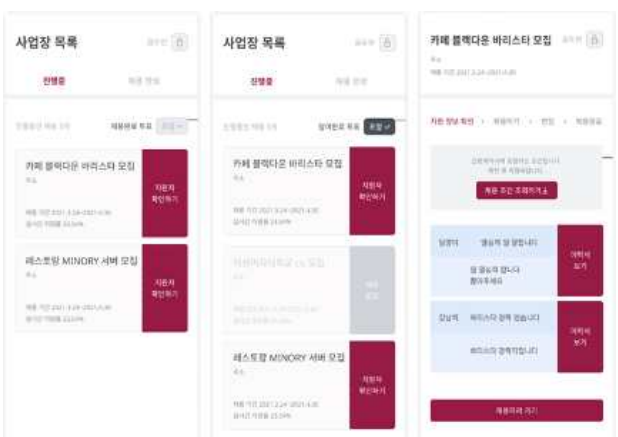


그림 7. 근로 계약서 앱 서비스 화면
Fig. 7. Screen Shot of Labor Contract App Service

5-3 기존 채용서비스와의 비교

현재 애플리케이션과 웹 서비스를 통해 근로자-고용자와의 대면과 채용이 이루어지고 있다. 근로계약서 작성은 대부분 서면으로 진행되고 있다. 하지만 근로계약이 체결되지 않은 근로자가 있으며 작성의 번거로움이 존재한다. 서면 근로계약서는 고용주가 근로자 동의 없이 변경할 수 있으며 근로자 서명까지 날인할 수 있다.

본 논문은 블록체인을 활용한 전자 근로계약서를 제안한다. 애플리케이션으로 입력한 근로계약서는 스마트 컨트랙트에 저장이 되어 블록체인에 저장된다. 애플리케이션으로 작성한 전자근로계약서는 국내 전자문서법 제4조 제1항에 의해서 서면 근로계약서와 동일한 법적 효력을 갖게 된다. 또한 블록체인에 근로계약서를 저장하면 고용주-근로자 간의 합의 내용에 관해 위□변조가 불가능하기에 안전성과 신뢰성이 보장된다. 전자 근로계약서는 서면 근로계약서와 달리, 근로계약서의 작성과 보관이 편리하다. 본 시스템은 전자근로계약서를 반드시 작성해야 근로자를 선택이 완료되기 때문에 근로계약서 체결률을 높일 수 있다. 블록체인과 스마트 계약을 도입해 근로자의 권익을 강화할 수 있다.

Ⅵ. 결 론

본 논문에서는 블록체인 기술의 스마트 컨트랙트를 활용하여 전자 투표 시스템과 근로계약서 관리 시스템을 설계하고 구현하였으며 시스템 평가 및 기존 서비스와의 차별점을 분석하였다. 해당 시스템을 개발하기 위해 Solidity 기반의 스마트 컨트랙트를 개발하였고 블록체인에 해당 컨트랙트를 배포하였다. 스마트 컨트랙트가 배포된 후에는 데이터 위□변조가 불가능하여 시스템 무결성 문제를 해결하였다. 제시된 투표 시스템은 블록체인의 계정을 사용자에게 노출시킴으로써 간접적으로 블록체인을 사용하고 있다는 느낌을 주어 신뢰감을 높였다. 제시된 채용 시스템은 기존의 서면 근로계약서에서 벗어난 전자 근로 계약서를 제안함으로써 얻는 이점을 분석하였다. 두 시스템은 스마트 컨트랙트의 내용만 다를 뿐 기술적 기저와 시스템 동작 구조는 매우 유사하다.

감사의 글

본 논문은 덕성여자대학교 2021년도 교내연구비 지원에 의해 수행되었습니다.

참고문헌

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *Decentralized Business Review*, White Paper, 2008. https://bitcoin.org/bitcoin.pdf

[2] J. Y. Kim, “A Study on the Public Legal Issues and Legislation on the Utilization of Block Chain Technology,” *Hannam Journal of Law&Technology*, Vol. 24, No. 2, pp. 43-79, June 2018. http://doi.org/10.32430/ilst.2018.24.2.43

[3] A. S. Kim, Y. J. Yoon, K. J. Joo, C. K. Park. "Blockchain and governance innovation," *KCERN 30th Forum Report*, pp. 1-119, 2016.

[4] Nick Szabo, "Smart Contracts: Building Blocks for Digital Markets", http://www.fon.hum.uva.nl, 1996, retrived 19 December 2017.

[5] J. S. Park, J. D. Kim, “A Study on the Development of Consortium Blockchain Governance Framework,” *Journal of Digital Convergence,* Vol. 17, No. 8, pp. 89-94, August 2019. https://doi.org/10.14400/JDC.2019.17.8.089

[6] C. Z. Han, H. Chang, “The Electronic Voting System Based on Block Chain Technology,” in Proceeding of 2019 Korea Computer Science Conference, *The Korean Institute of Information Scientists and Engineers*, pp. 1990-1992, June 2019.

[7] R. D. Lee, J. S. Lim, “Electronic Voting Systems Using the Blockchain,” *Journal of the Korea Institute of Information and Communication Engineering*, Vol. 23, No. 1, pp. 103-110, January 2019. http://doi.org/10.6109/jkiice.2019.23.1.103

[8] S. H. Yeom, S. Y. Choi, S. Y. Park, “Development of Part-time Employment Contract Managing System based on the Blockchain Technology,” in Proceeding of 2019 Korea Software Symposium, t*he Korean Institute of Information Scientists and Engineers*, pp. 1657-1659, December 2019.

[9] D. Lee, J. Park, J. Lee, S. Lee, S. Park, “Blockchain Core Technology and Domestic and Foreign Trends”, *Communications of the Korean Institute of Information Scientists and Engineers,* Vol. 35, No. 6, pp. 2-28, June 2017.

[10] U. Kim, M. Kim, T. Kim, J. Hong, “Used Car Trading Platform Using Block Chain and Smart Contract”, *in Proceedings of KIIT Conference*, pp. 76-79, 2018

[11] H. Kim “Blockchain-based Smart Contracts and Legal Issues,” *Dankook Law Review*, Vol. 44, pp.171-192, 2020.

[12] J. Shin, K. Kim, H. Youm, “Design for the Applications distributed payment system using the Smart Contract,” *in Proceedings of Symposium of the Korean Institute of communications and Information Sciences*, pp. 1188-1189, June 2018.

[13] D. M. Kim, “A Study on the Structure and Characteristics of Smart Contracts Using Blockchain Technology”, *The Korean Association Of Comparative Private Law,* Vol. 28, No. 3, pp.75-112, August 2021. https://doi.org/10.22922/jcpl.2021.28.3.75

제갈은(Eun Jegal)

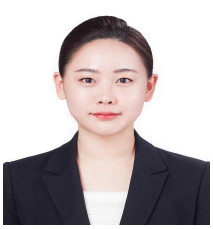
2017년～현 재: 덕성여자대학교 IT미디어공학과

2017년～현 재: 덕성여자대학교 공과대학 IT미디어공학과 (학사과정)
※관심분야 : 블록체인, 공공데이터, 정보보호, 빅데이터

이수연(Soo-Yeon Lee)

2017년～현 재: 덕성여자대학교 IT미디어공학과

2017년～현 재: 덕성여자대학교 공과대학 IT미디어공학과 (학사과정)
※관심분야 : 블록체인, 공공데이터, 정보보호, 인공지능



강서진(Seo-Jin Kang)

2017년～현 재: 덕성여자대학교 IT미디어공학과

2017년～현 재: 덕성여자대학교 공과대학 IT미디어공학과 (학사과정)
※관심분야 : 블록체인, 공공데이터, 디지털정부, 거버넌스

강남희(Namhi Kang)

1999년 : 숭실대학교 정보통신공학과 (공학사)
2001년 : 숭실대학교 정보통신대학원 (공학석사)
2005년 : University of Siegen 컴퓨터공학과 (공학박사)
2009년～2019년: 덕성여자대학교 공과대학 IT미디어공학과 교수
2020년～현 재: 덕성여자대학교 과학기술대학 사이버보안전공 교수
2006년～현 재: 덕성여자대학교 학교기업 DCS 대표
※관심분야 : 유무선 인터넷통신, 시스템 보안, 사물인터넷 보안, 인공지능 보안