블록체인 기반 증명서 인증 서비스 설계

권현경, 백엘, 이소영, 전세희, 최은정
서울여자대학교 정보보호학과
e-mail : silviakwon@naver.com, chej@swu.ac.kr

Certificate Authentication Service Design based on Block Chain

Hyeon-Gyeong Kwon, El Baek, So-Young Lee, Sae-hee Jun, Eun-Jung Choi
Dept of Information Security, Seoul Women's University

요 약

4 차 산업혁명의 핵심 기술로 선정된 블록체인은 비트 코인(금융권)을 포함하여 물류·유통 등을 중심으로 기존의 비즈니스 프로세스를 바꿀 새로운 패러다임으로 부상하고 있다. 이 글에서는 블록체인의 원장 공유 성격을 이용하여 기업과 지원자 간의 원하는 부분을 충족시켜 줄 수 있는 플랫폼 서비스 CUTnnect 에 대해 기술하고 있다.

1. 서론

민간기업 채용에 있어 제 3 자의 추천, 선발과정에서의 내부적 조정, 임직원 관련에 대한 특혜 등은 사실상 관행적으로 이루어져 왔고, 채용 권한이 있는 자가 그렇게 뽑겠다고 하는 경우 이를 위법하다고 할 만한 법적 근거를 찾기는 어려웠다[1]. 이러한 문제를 해결하기 위해 더 안전한 증명서 인증 서비스를 제안하고자 한다.

블록체인은 퍼블릭 혹은 프라이빗 네트워크에서 일어나는 거래정보가 암호화되어 해당 네트워크 구성원 간 공유되는 디지털 원장(ledger)를 의미한다[2]. 블록체인의 거래정보는 임의로 변경이 불가능하기 때문에 거래의 신뢰성이 높아지고 정보 추적이 용이하기 때문에 인증서 내용을 투명하게 관리할 수 있다. 또한 분산원장 기술은 암호화된 데이터와 암호화된 키 값으로만 거래가 이루어지므로 보안성을 높일 수 있다. 그리고 거래 정보와 인증을 위한 중앙 서버와 집중화 된 시스템이 필요 없기 때문에 비용이 적게 들어 채용 비용을 절감할 수 있다.

본 논문은 앞으로 우리나라의 채용비리 근절에 기여할 수 있는 새로운 플랫폼인 블록체인 기반 증명서 인증 서비스를 제안하고자 한다.

2. 관련연구

2.1 서비스 구성

본 시스템은 성적, 자격증, 학력 등 다양한 증명서비스에 활용될 수 있으며, 아래의 시나리오는 자격증 증명 서비스이다. 관련된 액터는 [그림 1]와 같다. 지원자와 기업은 CUTnecct 에 접속 및 가입하고, 이때 설정한 정보를 토대로 기관은 각종 이력들을 검증해 줄 수 있는 증명서를 블록체인에 올려준다. 웹 API 의 동작은 [그림 2]과 같으며, 이더리움 마이너 노드는 RPC 통신을 제공하고 서버 사이드 언어에서 마이너 노드의 RPC 통신을 통해 블록체인 데이터를 질의하면 블록체인 데이터를 웹으로 표현한다.

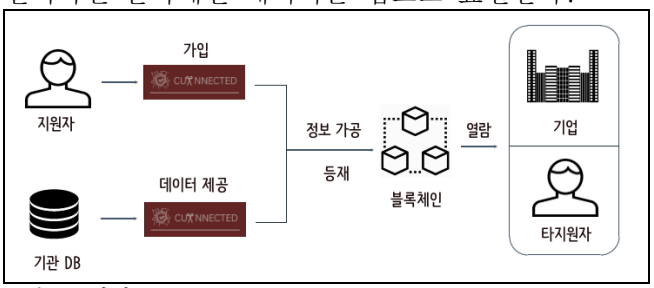

그림 1. 전체 흐름도

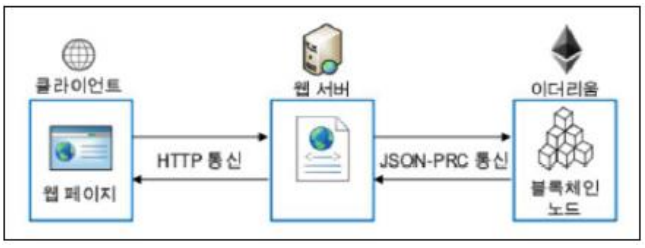

그림 2. 웹 API

2.2 네트워크 동작 구조

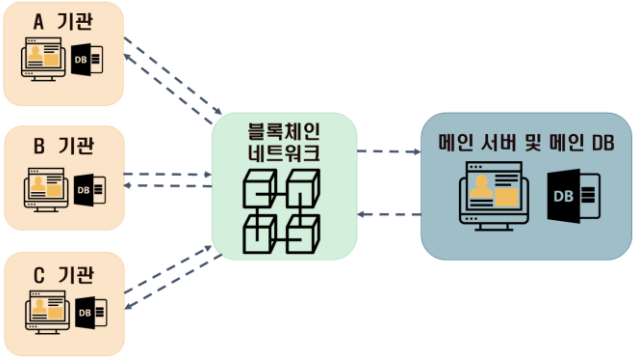

그림 3. 네트워크 동작 구조

네트워크 동작 구조에서 블록체인과 통신하는 객체를 나누면 크게 2 가지가 있다. 먼저 기관과 블록체인, 그리고 블록체인 네트워크와 CUTnnect 메인 서버 및 DB 끼리의 통신이다(그림 3).

컨트랙트는 geth 내부의 EVM(Ethereum Virtual Machine)이라는 환경에서 동작한다. EVM 은 자바의 가상 머신(JVM:Java Virtual Machine)처럼 운영체제에 종속되지 않고 고유의 코드를 구동할 수 있다.

[그림 4]는 위의 동작을 조금 더 로우 레벨에 대한 설명이다. 먼저 블록체인에서 스마트 컨트랙트는 솔리디티 언어로 작성된다. 이는 바이트 코드가 되어 이더리움 클라이언트에서 돌아가게 된다. 또한 이는 p2p 네트워크를 통해 배포된다. 이 블록체인 네트워크와 각 기관, 그리고 CUTnnect 와의 통신을 JSON-RPC 호출을 통해 이루어진다. Web3 라이브러리를 사용해 JSON-RPC 를 래핑하기 쉽게 호출할 수 있다. 또한 콘솔을 통한 명령어 조작으로 통신도 가능 하도록 한다.

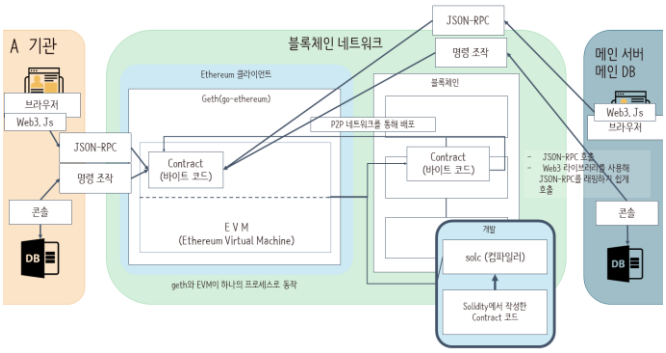

그림 4. 로우 레벨 네트워크 동작 구조

3. 결론

본 논문에서는 기업과 지원자 간의 효율적인 소통을 위해 보다 나은 플랫폼에서, 기업은 확실하게 이력이 보장된 지원자를 얻고, 지원자는 온전히 자신의 실력을 드러낼 수 있도록 한 서비스를 설계하였다. 기업, 지원자, 기관 DB 를 따로 두어 각각의 트랜잭션 필드를 상이하게 구성함으로써 사용자가 후에 이력서로 취합 시 열람을 쉽게 할 수 있도록 한다. 또한 각종 연고주의 문화, 비리로 인한 채용 문제는 사라지게 되며 이는 사회적으로 명확한 실력주의 사회를 만들어 나가는데 도움이 될 것이다.

감사의 글

본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW 중심대학 지원사업의 연구결과로 수행되었음 (2016-0-00022)

참고문헌

[1] 신권철. (2018). 채용의 공정. *노동법학*, (67), 13

[2] McKinsey&Company(2015.12.). 「The future of financial infrastructure」

[3] 이제영(2017), "블록체인(Blockchain) 기술동향과 시사점", 과학기술정책연구원