

# 블록체인 기반 인증 서비스 구현을 위한 블록체인 필드 설계 및 인증구현

권현경, 백엘, 이소영, 전세희, 최은정  
서울여자대학교 정보보호학과  
e-mail : bel516@hanmail.net, chej@swu.ac.kr

## Block Chain Field Design of Certificate Authentication Service 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

### 요약

만물의 디지털화로 정보를 더 빠르고 정확하게 공유하고자 하는 세상에 블록체인은 그 중심에 서 있다. 블록체인의 완전한 투명성 보장의 성질을 이용하여 구축한 증명서 인증 서비스는 기존 채용 시장의 채용비리 문제를 근절하는 서비스를 제공한다.

### 1. 서론

민간기업들은 관행적으로 채용에 있어 타인의 추천, 선발과정에서의 내부 조작, 임직원 관련 특혜 등의 부조리가 이루어졌으며, 채용 권한이 있는 자가 뽑겠다고 할 경우 이를 법적 증거에 근거하여 위법한다고 하기 어렵다[1]. 이러한 문제를 해결하기 위해 더 안전한 증명서 인증 서비스를 제안하고자 한다.

블록체인은 과거 블록의 내용을 조작하는 것이 불가능하다. 따라서 신뢰성이 높아지며 거래 시점을 객관적으로 알기에 투명성도 보장된다. 탈중앙화 시스템으로 인해 채용 비용 역시 절감한다.

본 논문은 분산원장에 올릴 블록체인 필드를 구성하고, 상세 내용에 대해서 서술한다. 이를 바탕으로 등록된 블록이 시스템 사용자의 UI 에서 어떻게 보여지는가와 인증된 내역 조회 원리에 대해 살펴보겠다.

### 2. 관련연구

#### 2.1 블록체인 필드 구성과정

##### 1) 회원 기본정보 및 자격증 정보

지원자가 CUTnnect 시스템에 회원가입을 하면, 가입 시 입력한 개인정보와 ID로 쓰일 발급받은 개인 Hash가 회원 DB에 저장된다. 이 후 기관 DB에서 합격자 정보를 주려낸 후, 회원 DB에서 개인 Hash를 얻어내 개인 정보에 민감한 주민등록번호는 삭제한 후 이를 블록체인에 올린다. 자격증 정보를 올리게 되면 블록체인에서 트랜잭션 Hash를 발급한다.

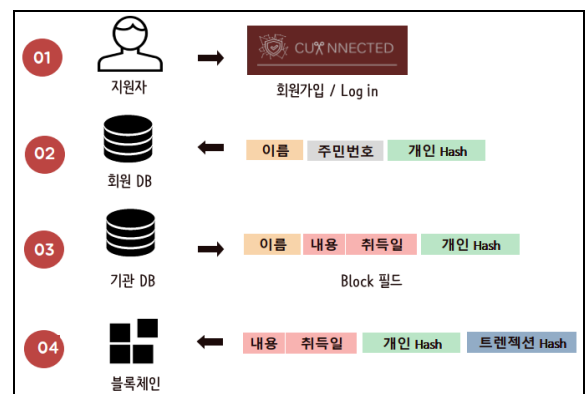


Figure 1. 블록체인 등재 과정

##### 2) 블록체인 필드 상세 내용

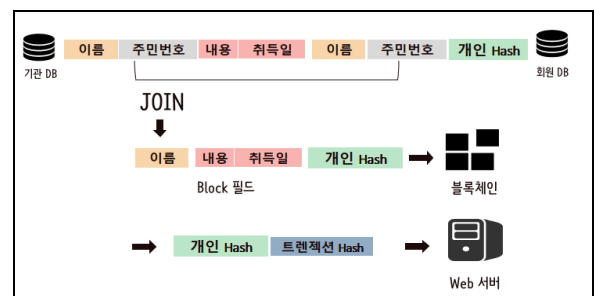


Figure 2. 블록체인 필드 구성과정 (Figure 1 상세)

기관과 회원 DB의 주민등록번호를 외래키로 사용하여 두 테이블을 조인해준 뒤 주민등록번호를 제외한 내용을 블록체인에 올린다. 그 후 개인 Hash와 블록체인에서 부여된 트랜잭션 Hash가 웹 서버에 저장된다.

## 2.2 블록체인 내의 인증 내용 조회

등록된 블록은 지원자 A와 회사, 타지원자 등 블록체인에 참여한 모두가 열람할 수 있다. 지원자 A는 발급받은 고유의 ID인 개인 hash를 통해 트랜잭션 hash를 확보하여 Etherscan을 통해 블록을 검색하여 렌더링 해준다. 이를 시각화 하면 그림 [Figure 3]과 같다. 해당부분 UI는 [Figure 6]과 같다. 상단 좌측에 이름과 개인 hash가 담긴 기본 정보, 상단 우측에는 인증 받은 내역이 있다. 하단에는 열람한 사람에 대한 기록(Log Record)을 남김으로써, 투명성을 보장한다.

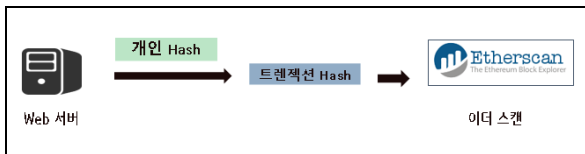


Figure 3. 지원자 측 블록 열람과정

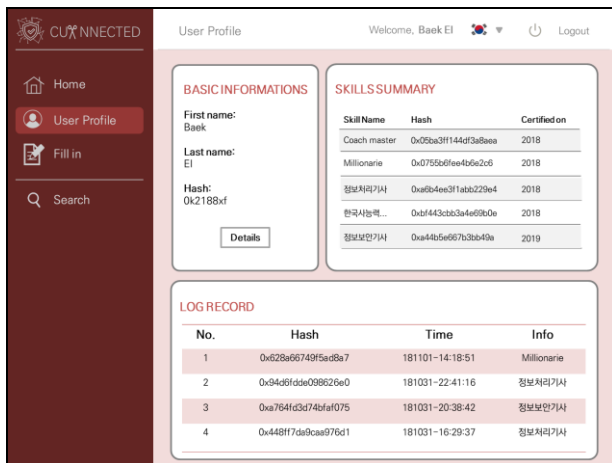


Figure 4. 지원자 측 UI (User Profile)

기업과 타 지원자 역시 트랜잭션 hash를 통해 Etherscan으로 지원자 A의 트랜잭션 외 지원자들의 트랜잭션 검색이 가능하다. 이 역시 시각화 하면 그림 [Figure 5]과 같다. 해당 UI는 [Figure 6]과 같다. 상단에 있는 부분에 트랜잭션 hash를 입력하여 검색하면, 하단에서 등록된 자격증 내용을 보여준다.

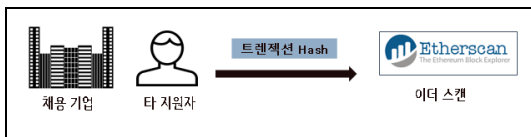


Figure 5. 회사 및 타 지원자의 블록 열람 과정

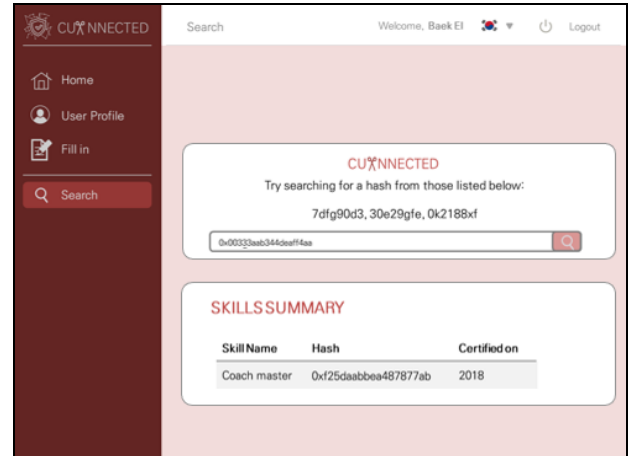


Figure 6. 회사 및 타 지원자의 검색 페이지 UI

## 3. 결론

본 논문에서 제안한 서비스는 개개인이 발급 받은 hash 값을 이용해, 구성되어진 필드 값들을 chaining하여 자신의 개인 이력서를 만들어낸다. 기업, 지원자, 기관 3개의 DB가 연동되어 있으며, 필요 시 조인하여 이후 열람 또한 쉽게 할 수 있도록 하였다. 이로써 지원자가 이력을 내고, 기업은 열람하고, 기관과 타 지원자까지 이 네트워크에 참여할 수 있게 되어 모든 과정에서 투명성을 보장하게 된다.

## 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
- [4] 아카하네 요시하루, 아이케이 마나부, 「블록체인 구조와 이론」, 위키북스(2017)
- [5] 가사키 나가토, 시노하라 와타루, 「처음 배우는 블록체인」, 한빛미디어(2018)