블록체인 기반 증명서 인증 서비스의 데이터베이스 구현

권현경*, 백 엘*, 이소영*, 전세희*,최은정*
*서울여자대학교 정보보호학과
e-mail : 17saehee@naver.com, chej@swu.ac.kr

Database Implementation of Certificate Authentication Service based on Block chain

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

요 약

증명서의 위변조를 해결하기 위해 무결성이 보장되는 블록체인 기반의 증명서 인증 서비스 시스템을 제안한다. 블록체인에 증명서를 등록하는 과정에서 데이터베이스와 블록체인의 동작구조를 살펴본다.

1. 서론

기업 채용에 있어 선발과정에서의 내부적 조정, 임직원 관련에 대한 특혜 등은 사실상 관행적으로 이루어져왔다. 하지만 이를 위법하다고 할 만한 법적 근거를 찾기는 어렵다.[1] 이러한 문제를 해결하기 위해 더 안전한 블록체인 기반 증명서 인증 서비스를 제안하고자 한다.

이는 문서형식의 종이 인증서를 발급해주는 기존 인증서 증명 서비스를 대신하여 블록체인에 증명서를 등록한다. 본 논문에서는 블록체인에 증명서를 등록하는 과정에서 특히 데이터베이스와 블록체인의 동작 구조를 살펴보고자 한다.

2. 블록체인 기반 증명서 인증 서비스 설계

본 서비스의 전체 흐름은 다음과 같다. 서비스 이용자(블록체인에 본인의 증명서를 등록하고 싶은 사람)는 블록체인에 증명서를 등록해주는 GUI를 제공해주는 서버에 접속한다. 해당 서버에 접속한 이용자는 발급받고자 하는 증명서를 해당 기관에게 요청한다. 해당 기관은 이용자의 요청에 대해 확인이 된 증명서에 대해서만 블록체인에 등록해준다. 이런 과정으로 블록체인에 증명서가 등록이 된다. 이 후에, 서비스 이용자의 증명서를 확인하고자 하는 기업은 이 서버에 접속하여 해당 사용자를 검색하여 증명서가 등록이 되었는지 확인할 수 있다. 이 과정에서 블록체인의 동작 구조를 다음장에서 살펴보겠다.

3. 데이터베이스와 블록체인 동작 과정

3.1 사전에 준비되어 있어야 할 데이터베이스(DB)

메인 서버의 회원정보 DB는 그림 1과 같다. 서버에서 회원가입을 하면 서버 DB의 회원정보 테이블에 저장이 되고, 개인 Hash 값을 부여해준다. 개인 Hash 값 역시 테이블에 같이 저장된다.

이름	개인 hash	블록이지 id	비밀번호	주민등록번호	생년월일	성별	연락처	본인확인 이메일
강소라	0x6bcf2ace85	sora5454	rjgjwkd@	920324-2015146	03월 24일	여	010-4846-7514	strawberry31@daum.net
권현경	0x7d4f72914c	gyeong97	!sigkekd@	970130-2051743	01월 30일	여	010-5914-3152	apple156@naver.com
민경훈	0x6626ecb804	molla3185	pergkdn%48	960124-1175498	01월 24일	남	010-6615-1892	melon96@naver.com
백 엘	0x7285db89fd	back3746	bkdnvl45!	951012-2275486	10월 12일	여	010-4855-9141	banana67@gmail.com
이민기	0xb845197503	mini1094	!siengkdl69	931214-0196225	12월 14일	남	010-4811-4157	best6898@naver.com
이소영	0xe9f1d7bf4f	gamjae9427	skvmlg38$	940617-1001642	06월 17일	남	010-9648-2552	orange3131@gmail.com
전세희	0x4e0e8aec67	jshi6184	*skble!4865	961130-1578915	11월 30일	남	010-7611-4832	cherry1130@naver.com

그림 1. 메인 서버 DB의 회원정보 테이블

[그림 2]은 한국산업인력공단에서 가지고 있는 DB 중 '정보처리기사 필기' 시험 응시자들의 테이블 예시이다. 이름과 개인을 식별하기 위한 주민등록번호, 시험 내용, 취득 여부, 그리고 취득 일자가 있다. 시험에 합격했을 경우 취득 여부는 Y, 불합격했을 경우 취득 여부는 N으로 표시한다. 또한, 합격했다면 그에 따른 취득 일자를 적어주고, 불합격했을 시 역시 N으로 표시한다.

이름	주민등록번호	내용	취득 여부	취득 일자
강소라	920324-2015146	정보처리기사 필기	N	N
권현경	970130-2051743	정보처리기사 필기	Y	2018-03-16
민경훈	960124-1175498	정보처리기사 필기	N	N
백 엘	951012-2275486	정보처리기사 필기	Y	2018-03-16
이민기	931214-0196225	정보처리기사 필기	N	N
이소영	940617-2001642	정보처리기사 필기	Y	2018-03-16
전세희	961130-2578915	정보처리기사 필기	Y	2018-03-16

그림 2. 기관 DB의 응시자 정보 테이블

[그림 3]은 [그림 2]의 응시자 테이블에서 합격자들만 추려서 기관 DB에 합격자 정보를 따로 저장한 테이블이다.

이름	주민등록번호	내용	취득 여부	취득 일자
권현경	970130-2051743	정보처리기사 필기	Y	2018-03-16
백 엘	951012-2275486	정보처리기사 필기	Y	2018-03-16
이소영	940617-2001642	정보처리기사 필기	Y	2018-03-16
전세희	961130-2578915	정보처리기사 필기	Y	2018-03-16

그림 3. 기관 DB 의 합격자 정보 테이블

3.2 동작 순서

[그림 1]의 메인 서버 DB 의 회원정보 테이블과 [그림 3] 기관 DB 의 합격자 정보 테이블을 조인하여 블록체인 필드를 구성한다. (그림 4)

이름	개인 hash	내용	취득 일자	발행처
권현경	0x7d4f72914c	정보처리기사 필기 합격	2018-03-16	한국산업인력공단
백 엘	0x7285db28fd	정보처리기사 필기 합격	2018-03-16	한국산업인력공단
이소영	0xe9f1d7bf4f	정보처리기사 필기 합격	2018-03-16	한국산업인력공단
전세희	0x4e0e8aec67	정보처리기사 필기 합격	2018-03-16	한국산업인력공단

그림 4. 조인 후 블록에 올라갈 트랜잭션의 틀

[그림 4]와 같이 정리된 테이블을 블록체인 트랜잭션에 올린다(그림 5). 트랜잭션에는 이름, 개인 Hash 값, 취득 내용, 취득 일자, 발행처 순으로 등록되며, 이 트랜잭션의 Hash 값은 따로 저장해둔다. 동일한 방법으로 나머지 정보들 역시 트랜잭션에 올린다(그림 6).

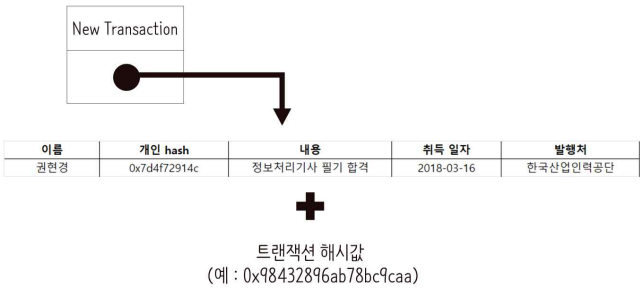

그림 5. 블록체인 장부에 등록하기

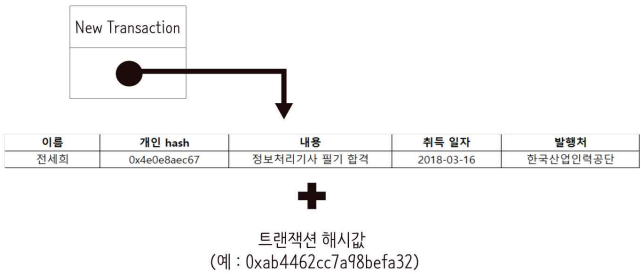

그림 6. 블록체인 장부에 등록하기 (2)

블록에는 트랜잭션의 Hash 값과 이전 트랜잭션의 Hash 값, 그리고 트랜잭션 내용들이 함께 포함되어 있다. 트랜잭션 내용은 이름, 개인 Hash 값, 취득 내용, 취득 일자, 그리고 발행처를 담고 있다. 이는 [그림 7]와 같다.

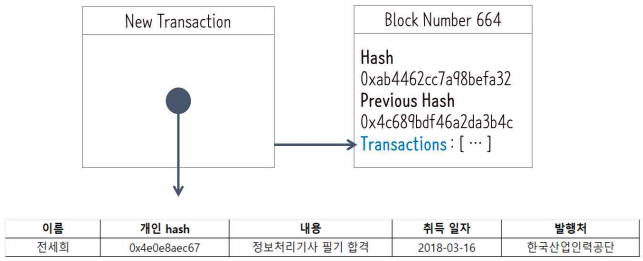

그림 7. 블록에 올라간 내용

[그림 8]의 왼쪽 상단에 있는 664 번 블록이 가장 마지막으로 올라온 블록이고, 오른쪽 하단에 있는 661 번 블록이 해당 트랜잭션을 올릴 때 가장 처음으로 올린 블록이 된다.

각 트랜잭션에는 이전 Hash 값을 가지고 있으며, 이를 화살표로 표현해보면 [그림 9]과 같다. 데이터를 위/변조하기 위해서는 이 Hash 값을 모두 변경해야 하는데, 블록은 시간대별로 정렬되어 있기 때문에 사실상 불가능에 가깝다.

한 블록에는 앞의 블록과 뒤의 블록과 연결되는 연결정보가 포함돼 있으며, 앞 블록의 내용을 변경하면 뒤에 이어지는 모든 블록을 다시 생성해야 한다. 따라서 과거 블록의 내용을 조작하는 것은 어렵다.

즉, 과거에 등록된 기록이 존재한다면 그것은 그 시간에 등록이 완료되었음을 객관적으로 알 수 있으며, 데이터의 무결성을 증명할 수 있다.[2]

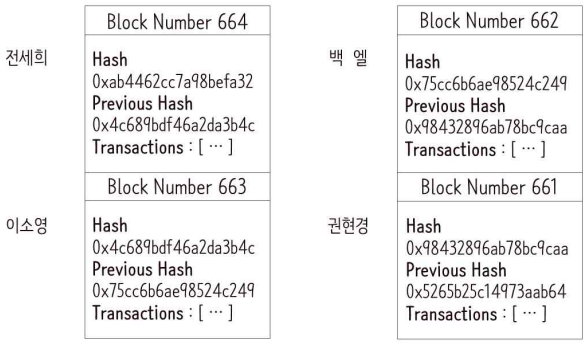

그림 8. 블록체인 장부

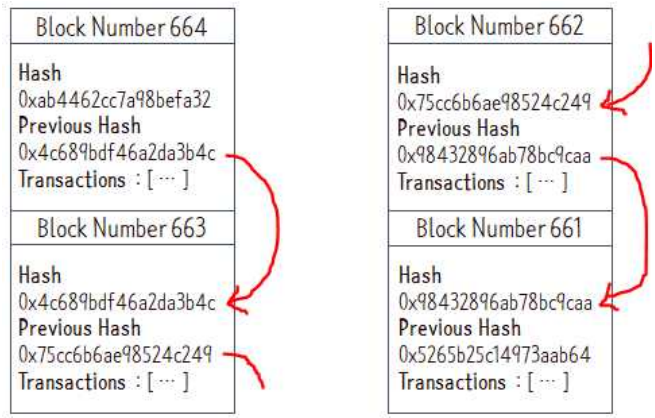

그림 9. 블록체인 원리

[그림 10]은 블록체인에 등록하면서 얻은 트랜잭션의 Hash 값과(그림 5, 그림 6) 메인 서버 DB 의 개인 Hash 값(그림 1)을 조인하여 새로운 테이블이다. 이 정보를 메인 서버에 전송하여, UI 에서 렌더링(rendering)해준다. 그러면 마이페이지에서 개인 이력들이 어떤 블록에 저장되어 있는지 트랜잭션 Hash 값을 확인할 수 있으며, [그림 11]가 이를 나타낸다.

이름	개인 hash	내용	취득 일자	발행처	트랜잭션 해시값
권현경	0x7d4f72914c	정보처리기사 필기 합격	2018-03-16	한국산업인력공단	0x98432896ab78bc9caa
백 열	0x7285db28fd	정보처리기사 필기 합격	2018-03-16	한국산업인력공단	0x75cc6b6ae98524c249
이소영	0xe9f1d7bf4f	정보처리기사 필기 합격	2018-03-16	한국산업인력공단	0x4c689bdf46a2da3b4c
전세희	0x4e0e8aec67	정보처리기사 필기 합격	2018-03-16	한국산업인력공단	0xab4462cc7a98befa32

그림 10. 트랜잭션 Hash 값이 포함된 테이블

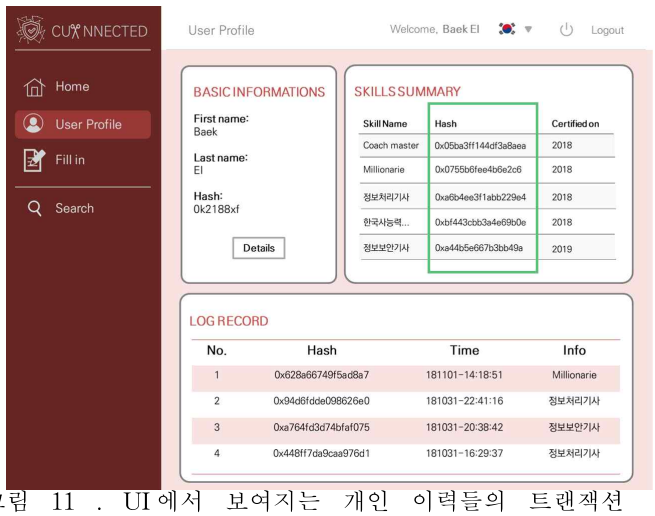

그림 11 . UI에서 보여지는 개인 이력들의 트랜잭션 Hash 값

4. 결론

본 논문에서는 기존의 인증서 서비스를 대신하여 블록체인을 기반을 둔 인증서 서비스의 모델과 서비스 안에서의 데이터베이스 동작 과정을 살펴보았다. 본 서비스는 블록체인의 특징으로 블록체인에 올라간 데이터의 무결성이 보장된다. 이로써 지원자의 블록 내의 단 한 번의 지원으로 모든 기업으로 본인의 이력을 보일 수 있게 되고, 기업 입장에서는 채용에 대한 투명성을 증명할 수 있음과 동시에 요구하는 인재상에 걸맞는 인력을 충원할 수 있게 된다. 또한 기존 증명서 인증 시스템에 비해 재확인 절차가 필요하지 않으므로 비용과 시간이 줄어든다. 본 서비스는 인증서 서비스 이외의 다른 무결성이 보장되어야 하는 데이터에 적용 할 수 있는 플랫폼이다.

감사의 글

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

참고문헌

[1] 서종천, 김종렬, 양동규, “악교정 수술환자에서 술전 후의 교합력변화에 관한 연구,” 대한구강악안면외과학회지, 제22권, 1호, pp. 121-129, 1996.

[2] 아카하네 요시하루, 이어케이 마나부, 『블록체인 구조와 이론』, 위키북스, 2017, 31p