수정 가능한 스마트 컨트랙트 기반의 학력인증서비스1)

전세희*, 김형종**
*서울여자대학교 정보보호학과
**서울여자대학교 정보보호학과
17saehee@naver.com

Academic Certification Service Based on Modifiable smart contract

Sae-Hee Jun*, Hyung-Jong Kim**
*Dept of Information Security, Seoul Women's University
**Dept of Information Security, Seoul Women's University

요 약

기존의 학력인증 서비스는 학교에 직접 방문하거나, 온라인을 통해 종이 증명서를 발급받는다. 하지만 학력인증을 블록체인에 기록하여, 인증 서비스의 비용을 줄이고 절차를 간소화하고자 한다. 더불어, 디지털 증명서를 블록체인에 등록하여 발급해온 증명서의 진위 여부를 확인하는 체제가 잘 갖춰지지 않은 곳에서도 재확인이 필요 없는 서비스를 제공하고자 한다. 블록체인에 증명서를 등록하는 중요한 기능은 '스마트 컨트랙트'를 통해 이루어진다. 매년 졸업요건이 변경된다는 점을 고려하면 스마트 컨트랙트에서 블록체인에 학력인증이 등록되는 조건의 업데이트는 필수불가결이다. 하지만 새로운 스마트 컨트랙트를 배포하는 식의 컨트랙트 업데이트는 여러 문제점들이 있다. 이를 해결하고자 본 논문에서는 proxy contract를 이용한 학력인증 서비스 시스템의 설계를 다루고자 한다.

1. 서론

기존의 학력인증 서비스는 발급하고자 하는 사람이 직접 학교에 방문하거나, 온라인에서 여러 절차를 통해 종이 증명서(문서 형태)를 발급한다. 후에 이를 학력인증을 요구하는 기관에 제출한다. 증명서를 받은 기관에서는 이 증명서가 위조되거나 변조된 것이 아닌지 확인을 한 후에야 한 사람의 학력이 인증된다. 또한 발급받은 증명서의 진위 여부를 판단하는 환경이 갖춰지지 않으면 기존의 학력인증 서비스 시스템은 무의미해진다.

블록체인기반의 학력인증 서비스를 통해 디지털 증명서를 발급하여(블록체인에 등록하는 것을 말함), 기존 서비스의 복잡한 절차를 간소화하고 비용을 줄이고자 한다. 또한 한번 발급된 증명서는 블록체인 특징인 무결성과 투명성에 의해 진위여부를 재확인할 필요가 없다.[1]

블록체인에서 학력인증 증명서를 입력해주는 역할은 스마트 컨트랙트가 한다. 하지만 매년 졸업요건이 변경되는 점을 고려하면 스마트 컨트랙트의 업데이트는 필수불가결이다. 하지만 스마트 컨트랙트도 블록체인의 하나의 데이터로 들어가는 것이기 때문에 이미 배포된 스마트 컨트랙트를 다시 수정하기는 불가능하다. 다른 방법으로 새로운 스마트 컨트랙트를 작성해서 배포한 후 그 컨트랙트를 사용하는 방법이 있다. 하지만 이러한 경우 몇 가지의 문제점이 나타난다. 이 문제점은 다음 목차에서 살펴보고자 한다. 본 논문에서는 문제점 없이 컨트랙트를 업데이트 시킬 수 있는 proxy contract를 이용한 학력인증 서비스 시스템의 모델을 설계하고자 한다.

2. 배경지식

2.1 블록체인

2.1.1 정의[2]

블록체인은 중앙시스템 없이 자율적으로 동작하는 분산 시스템 기술을 통칭한다. 거래 내역 등을 '블록'이라는 데이터 단위로 저장한 후 해당 블록의 해시 값을 다음 블록에 저장 시켜 블록과 블록 사이에 체인 형태의 연결고리를 만든다.

2.1.2 특징[1]

블록은 시간별로 정렬되어 있다. 블록에는 고유의 해시 값이 존재한다. 이 해시 값은 이전 해시 값을 이용해서 만든 해시 값이기 때문에, 하나 블록의 내용을 변경하려면, 그 블록 이전 모든 블록의 해시 값을 변경해야한다.

1) "본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음"
(IITP-2019-2018-0-01799)

따라서 과거 블록 내용을 조작하는 것은 어렵다.

블록체인은 분산형 원장 구조다. 즉, 그 블록체인 네트워크에 참가한 모든 사람이 모든 거래 기록을 기록한 원장을 소유한다. 그렇기 때문에 거래의 투명성도 높아지는 것이다.

2.2 스마트 컨트랙트[2]

스마트 컨트랙트는 IT 기술을 이용해 계약 내역을 자동으로 실행하는 것이다. 예를 들어, 전자화폐의 잔액이 일정 액수 이상이면 적금통장으로 자동으로 저축되는 서비스도 스마트 계약의 하나이다.

2.3 프록시(proxy)

프록시란 '중개자' 혹은 '대리'라는 의미로, 주로 네트워크 기술에서 사용되는 개념이다. 즉, 네트워크 기술에서는 통신하고자하는 두 지점 사이에 위치하여 중계 기능을 하는 것이다.

3. 이론적 배경

스마트 컨트랙트를 배포 한 이후, 기존 컨트랙트에서 버그를 발견하거나 기능 추가나 변경으로 인하여 코드를 업데이트를 하고자 한다, 블록체인의 특성으로 인해 기존의 컨트랙트는 수정이 불가하기 때문에, 새로운 스마트 컨트랙트를 작성하고 배포하여 업데이트를 진행한다. 하지만 이 방법의 경우 다음과 같은 문제점이 생긴다.

첫 번째로 사용자가 컨트랙트를 호출할 때, 기존의 컨트랙트 주소를 새로운 컨트랙트 주소로 바꿔줘야 한다는 문제이다. 사용자는 매번 서비스 제공자한테 가장 최신의 컨트랙트 주소를 알아내야 하는 불편함이 생긴다. 또한 서비스 제공자는 가장 최신의 컨트랙트의 주소를 물어보는 응답에 답해주는 별도의 시스템을 제공해줘야 한다.

두 번째로 기존 컨트랙트(A)에 보관하고 있던 정보들이나 환경 설정들이 사라지게 된다. 새로 배포한 컨트랙트(B)는 기존 컨트랙트(A)가 저장하고 있는 정보를 가지고 있지 않다. 이 경우, 정보를 새로 배포한 컨트랙트(B)로 옮겨야 하는 상황이 발생한다. 하지만 정보를 옮기는 일은 매우 복잡하고 비용이 많이 들며, 데이터가 유실될 위험이 있다.

4. 학력인증 서비스 전체 시나리오

블록체인에 기반을 둔 학력인증 서비스의 시나리오는 다음과 같다. 학교는 각 학생의 여러 가지 정보들을 DB에 관리를 한다. 학생은 학교 시스템에 졸업신청을 요청한다. 학교 시스템은 요청한 학생의 정보를 모아 학력인증 블록체인에 있는 스마트 컨트랙트를 호출한다. 스마트 컨트랙트는 작성된 조건에 학생의 정보를 대입하여 졸업 요건이 충족했는지 자동적으로 검사를 시행한다. 만약 졸업 요건이 모두 충족했다면, 요청한 학생의 정보를 담아 학교 학력인증 블록체인에 트랙잭션을 만들어 이를 블록체인에 등록한다. 이렇게 등록된 디지털 학력인증 증명서는 블록체인의 특성으로 인해 위변조되지 않고, 투명성을 유지한다. 반대의 경우 졸업 요건이 충족되지 못 하였다면, 블록체인 등록이 거부된다. 이를 그림으로 표현하면 [그림1]과 같다. 블록체인에 등록된 디지털 증명서는 이를 필요로 하는 학생은 단 한번만 학교에 요청을 하면 되고, 제출하려는 기관마다 종이 증명서를 발급받지 않아도 된다. 또한 한 학생의 학력증명서를 받는 기관은 따로 위변조의 여부를 확인하는 환경 없이도, 학력인증 블록체인을 통해 인증된 학력을 확인 할 수 있다.

[그림1] 블록체인 기반 학력인증 서비스 시나리오

이 시스템에서 중요한 역할을 하는 것은 블록체인에 학력을 인증해주는 증명서를 자동적으로 넣어주는 '스마트 컨트랙트'이다. 여기서 스마트 컨트랙트는 증명서를 요청한 학생의 요건이 졸업 요건이 충족하는지 확인해주고, 요건이 충족되면 학력인증 트랙잭션을 만들어 블록체인에 등록한다. 여기서 만약 스마트 컨트랙트의 요건이 잘 못 작성되거나, 새로운 졸업 요건이 생기고 없어질 경우 블록체인에 등록되는 증명서는 졸업요건을 충족하지 못한 학생이 인증서가 발급되거나, 졸업요건을 채웠음에도 발급되지 않는 상태가 되어 제기능을 하지 못한다. 그러므로 스마트 컨트랙트의 업데이트는 필수로 필요하다. 다음 목차에서는 proxy contract를 이용하여 컨트랙트를 업데이트 시키는 방법에 대해 다룬다.

5. Proxy를 이용한 업데이트 가능한 컨트랙트

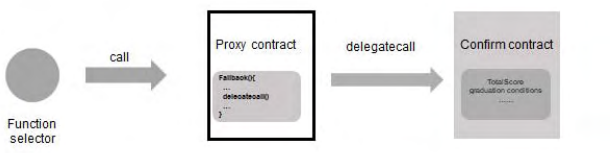
위에서 다뤘던 문제점인 사용자의 잦은 주소 변경과 기존의 데이터가 손실되는 문제를 해결하기 위해 이 모델에서는 proxy contract를 사용한다.

'proxy contract'는 fallback함수와 fallback함수 속에 있는 delegatecall()이 핵심이 되어 컨트랙트가 작성된다. fallback 함수란 정의되지 않은 상황 또는 정의되지 않은 경우에 대하여, default로서 작동하는 Function 이다. 즉, 사용자가 어떤 컨트랙트의 함수를 호출 할 때, 해당 컨트랙트에 그 함수가 존재하지 않을 경우에 실행되는 함수이다. delegatecall()은 어떤 스마트 컨트랙트(A)가 다른 스마트 컨트랙트(B)를 호출하는 상황에서 A의 프로그램이

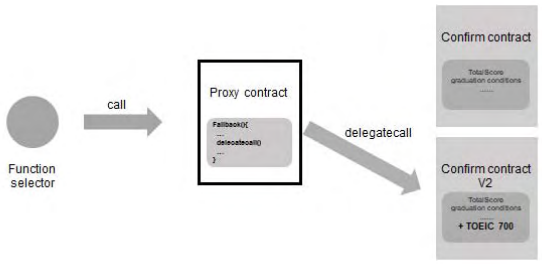
실행될 때 프로그램이 참고할 만한 모든 변수 등의 환경을 유지하며 B 컨트랙트를 호출하는 것이다. 여기서 A를 프록시 컨트랙트, B를 로직 컨트랙트라고 생각하면 된다. 즉, 사용자는 프록시 컨트랙트를 통해 필요한 함수가 있는 로직 컨트랙트를 호출하고, 그에 대한 변경 내용은 프록시 컨트랙트에 저장하는 것이다. 이를 통해 기존 데이터를 보존하는 문제를 해결 할 수 있다. 또한 새로운 로직 컨트랙트를 업데이트 할 시, 새로운 컨트랙트를 배포하고 프록시 컨트랙트의 delegatecall()에 사용되는 컨트랙트 트랜잭션 주소 값만 변경해주면 된다. 그 결과 사용자는 업데이트 된 새로운 스마트 컨트랙트 주소를 바꿀 필요 없이 프록시 컨트랙트 주소를 계속 사용하면 되기 때문에, 사용자 쪽에서 주소를 변경해야 한다는 문제점을 해결 할 수 있다. [2][3]

이번 단락에서는 Proxy contract를 통해 학력인증서비스의 업데이트의 과정을 간단한 예시를 통해 설명하려고 한다. ‘confirm contract’는 기존의 졸업요건들의 조건들로 이루어져 조건들이 충족할 시 블록체인에 등록해주는 컨트랙트이다. 사용자가 등록하기 위해 등록해주는 함수(이 함수는 ‘confirm contract’에 존재함)를 호출 할 것이다. 이 때 함수를 호출하는 과정은 [그림 2]과 같이 도식화 할 수 있다. 처음에 프록시 컨트랙트로 실행하고자 하는 함수를 Function Selector를 통해 호출을 한다. 해당 함수는 프록시 컨트랙트에 존재하지 않기 때문에 fallback함수가 실행되고 delegatecall()을 통해 confirm 컨트랙트를 호출하여 그 안에 있는 함수를 실행한다.

여기서 졸업요건에 “영어공인점수 700점 이상”이 추가요건으로 들어갔다고 가정한다. 이 상황에서는 졸업충족요건을 확인해주는 컨트랙트에 조건을 업데이트시켜야한다. 업데이트를 위해서, 개발자는 업데이트 된 새로운 스마트 컨트랙트를 배포를 해준다. 후에 delegatecall()에서 사용되는 컨트랙트 주소를 새로운 컨트랙트 주소로 변경해준다. 업데이트 이후에 사용하는 사용자는 업데이트 이전과 동일한 과정으로 함수를 호출할 것이다. 하지만 프록시 컨트랙트 속 delegateall()을 통해 호출하는 컨트랙트가 새로 배포된 업데이트된 컨트랙트이다. 이 결과 사용자는 업데이트 된 컨트랙트를 통해 서비스를 이용할 수 있게 된다. [그림3]은 이를 도식화하여 표현한 것이다.[4]



[그림 2] 컨트랙트를 호출하는 과정



[그림 3] 업데이트 후 컨트랙트를 호출하는 과정

6. 결론

본 논문에서는 복잡하고 비용이 많이 드는 기존의 학력인증 서비스 시스템을 대체할 블록체인 기반의 학력인증 서비스를 통해 간단한 절차와 낮은 비용으로 확실하게 학력을 인증하는 서비스를 설계하였다. 본 서비스에서 가장 중요하고 문제가 될 수 있는 “스마트 컨트랙트”에 대해서 단순히 새로운 컨트랙트를 배포 할 시 생기는 문제를 해결하여, 업데이트가 필수불가결한 증명서 등록 요건에 대한 문제도 고려하여 살펴보았다. 이 플랫폼은 블록체인이라는 기술의 장점인 장부 공유의 성격을 이용하여 학력인증 이외에도 여러 인증 서비스에 적용 될 수 있다. 이는 인증 서비스의 비용절감과 과정 간소화에 많은 도움이 될 것이다.

참고문헌

[1] 아카하네 요시하루, 아이케이 마나부, “블록체인 구조와 이론”, 위키북스, 31, 2017.

[2] 가사키 나가토, 시노하라 와타루, “처음 배우는 블록체인”, 한빛미디어, 14-18, ,155-196, 2018

[3] 리테시 모디, “솔리디티 프로그래밍 에센셜”, 위키북스, 2018

[4] Solidity Documentation https://solidity.readthedocs.io