https://doi.org/10.5392/JKCA.2020.20.05.011

학점은행제를 위한 블록체인 시스템

Blockchain System for Academic Credit Bank System

손기봉, 손민영, 김영학
금오공과대학교 컴퓨터공학과

**Ki-Bong Son(gukb@kumoh.ac.kr), Min-Young Son(son0804@kumoh.ac.kr),
Young-Hak Kim(kimyh@kumoh.ac.kr)**

요약

학점은행제는 평생학습사회를 구현하기 위한 교육 시스템이다. 이 시스템의 조건을 충족한 학습자는 전문대, 4년제 대학교의 학위와 동등한 학사 학위를 취득할 수 있다. 이 학습자의 학점과 학위 정보는 중앙 기관에 기록되어 관리되고 있다. 그러나 이러한 시스템은 중앙관리로 인해 해킹 등과 같은 보안 문제가 발생할 수 있다. 본 논문에서는 블록체인 기술을 기반으로 학점과 학위 정보를 관리할 수 있는 학점은행제 시스템을 제안한다. 제안된 시스템은 학점과 학위 정보는 블록에 저장되고 영구적인 방식으로 공개 원장에 기록된다. 블록들은 해킹과 조작 등의 보안 문제를 개선하기 위해 분산 네트워크 환경에서 블록체인 형식으로 연결되어진다. 또한 중앙 기관의 기능들이 네트워크 참여자들에게 분산되기 때문에 학점 은행 관리의 효율성이 증대될 수 있다. 제안된 시스템의 프로토타입은 Go-Ethereum 플랫폼에서 구현되었으며 스마트 컨트랙트를 사용하여 참여기관 간의 블록체인 정보를 실험적으로 검증하였다.

■ 중심어 : | 블록체인 | 이더리움 | 학점은행제 |

Abstract

The academic credit banking system is an educational system to implement a lifelong learning society. Students who meet the requirements of this system can achieve academic degrees equivalent to those of junior colleges or four-year universities. Credits and degree information of these students are recorded and managed by the central institution. However, this system can cause security problem such as hacking due to centralized management. In this paper, we propose an academic credit banking system which can manage credits and degree information based on blockchain technology. In the proposed system, credits and degree information are stored in block and managed in the public ledger in a permanent manner. Blocks are connected in the form of blockchain on a distributed network to improve security problems such as hacking and manipulation. Also, the efficiency of credit bank management can be increased because the functions of the central institution are distributed to the network participants. The prototype of the proposed system was implemented on the Go-Ethereum platform and experimentally verified the blockchain information among participating organizations using smart contracts.

■ keyword : | Blockchain | Ethereum | Academic Credit Bank System |

* 이 연구는 금오공과대학교 학술연구비로 지원되었음(2019-104-025)
접수일자 : 2020년 03월 04일
심사완료일 : 2020년 04월 29일
수정일자 : 2020년 04월 29일
교신저자 : 김영학, e-mail : kimyh@kumoh.ac.kr

I. 서 론

최근 취업난의 장기화로 인해 경쟁이 과열됨에 따라 국내외에서는 해킹 등을 통해 서버에 접근하여 학점을 조작하는 사례가 발생하였다. 그뿐만 아니라 학점 증명서 또한 위조하여 제출하는 등 공문서위조죄에 상응하는 위법도 일어나고 있다[1][2]. 학생들의 성적을 중앙 집중 형태인 서버에 보관하여 관리하기 때문에 해킹으로 인한 조작이나 증명서의 조작에 취약하다고 할 수 있다.

이수한 학점을 확인하거나 다른 기관에 학습 정보를 전달하기 위해서는 기존에 학습을 이수하였던 교육 기관에 접근하여 확인서를 출력하여야 한다. 이를 수행하기 위해서는 각 기관은 서버 해킹 등의 공격에 방어하며 학생의 인증을 확인하는 인증 시스템을 각자 구축하여야 한다. 학생은 기관별로 상이한 인증시스템에 비용과 시간을 들여 인증해야 하는 불편함이 따른다. 또한 기관별로 독자적인 시스템을 구축하는 데는 어려움이 있기 때문에 이를 위한 서비스를 제공하는 제3기관들이 있으나 이 또한 비통합적이며 비용이 발생하는 단점이 있다. 이 비용은 학습자와 학습기관에 전가될 수밖에 없다.

학점 은행제는 법률에 따라 학교 안팎에서 다양한 형태의 학습 및 자격을 인정하는 시스템이다. 이 시스템은 열린 평생학습 사회와 열린 교육을 실현하기 위한 제도라고 할 수 있다. 모든 학점은 중앙 기관인 국가평생교육진흥원의 통합 시스템에 의해 관리되고 있기 때문에 서비스가 통일적으로 제공되는 장점이 있다. 그러나 국가평생교육진흥원에서 관리하는 학점 정보도 중앙 집중형으로 관리되어 해킹 등에 취약하다는 문제가 존재한다.

블록체인 기술은 개인 간(P2P)의 모든 거래 내역이 네트워크에 참여한 참여자들에게 분산 저장되어 해킹으로부터 보호될 수 있다. 뿐만 아니라 블록체인을 사용하는 것은 중앙 시스템(제3의 시스템)의 개입이 없기 때문에 비용을 절감할 수 있고 네트워크 참여자들의 합의를 통해야 하기 때문에 투명한 거래가 가능하다.

본 연구에서 제안하는 시스템은 블록체인의 보안, 익명성, 무결성, 투명성의 장점을 활용하여 고등 교육 이수 정보를 관리하는 프라이빗 블록체인 시스템을 제안한다. 학생들이 이수한 학점을 블록체인에 활용함으로써 보안과 투명성을 보장할 수 있다. 다른 조직에서는 학생의 허가를 받은 후 학점 이수 정보를 확인할 수 있다. 그뿐만 아니라 자신의 지갑(Wallet)에 저장할 수 있기 때문에 확인서와 같은 사본이 필요할 때에도 자신의 지갑을 통해서 학점을 증명하여 비용과 시간을 절약할 수 있다. 따라서 학점은행 정보를 영구적인 방식으로 공개 원장에 기록함으로서 기존 문제점인 해킹과 조작 등의 보안 문제를 개선할 수 있다. 또한 학생 등록 및 정보 기록 등과 같은 권한을 네트워크 참여자인 기관들에게 공유함으로써 중앙 기관에 집중되던 기능을 분산하여 업무의 효율성을 향상 시킬 수 있다.

본 연구의 구성은 다음과 같다. 2장에서는 본 연구와 관련된 분야의 중요한 프로젝트와 연구에 대해 설명하고 3장에서는 연구에서 제안하고 있는 학생의 학점관리 블록체인에 대한 플랫폼을 설명한다. 4장에서는 연구의 실험과 결과를 수행하고 5장에서는 본 연구의 결론을 제시한다.

II. 관련 연구

1. 학점 은행제

학점 은행제가 도입된 배경을 살펴보면 1995년 5월 교육 개혁 위원회는 학점 은행제를 제안하며 평생 열린 학습 사회의 발전을 촉진하는 새로운 교육 시스템에 대한 비전과 학점 인정 법률을 포함한 관련 법률을 제정 시행하였다. 이것은 평생 학습에 대한 사람들의 권리와 다양한 학습 경험을 장려하고 대학 교육을 받지 못한 사람들에게 대학 교육 기회를 제공하기 위함이다. 학점 은행제는 고등학교 졸업과 같은 학력을 가졌다면 누구나 이용할 수 있고 학점 은행제에서 이수한 과정에 따라 전문대학 졸업자 또는 학사 졸업자에 해당하는 학력을 인정받을 수 있다.

[그림 1]은 학습자와 국가평생교육진흥원, 학습 기관의 관계를 나타낸 것이다. 학점 은행제 교육 기관으로는 특수 학교 및 고등기술학교, 학원, 직업훈련시설, 정부·지자체, 평생교육 시설 등 570여 개 기관이 포함된

다. 학습을 희망하는 학생은 학점 은행제 학습자로 등록을 해야 한다. 수강을 원하는 학습자는 등록 신청을 한 번만 하면 되는데 학습 전 또는 학습 중에 등록 신청을 할 수 있다. 학생이 학위를 받기 위한 모든 학점을 충족하였을 때 교육부 장관 명의 또는 대학장의 명의로 학위가 발급된다.

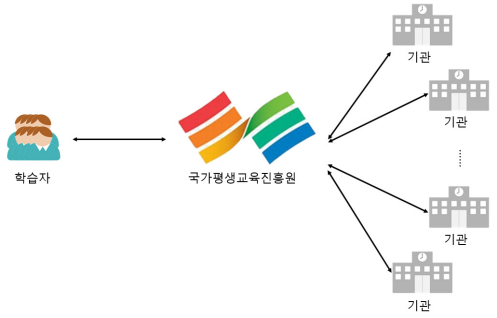

그림 1. 현 학점 은행제 운영 관계도

참여기관에서 학생이 특정 과목을 이수하면 학점을 부여받고 이수한 과목과 학점은 [그림 1]과 같은 중앙관리 시스템에 등록된다. 중앙관리 시스템의 경우 독자적인 시스템과 데이터베이스를 사용하여 학생들의 정보를 관리한다[1]. 이러한 중앙관리 방식은 해킹과 조작 등의 보안 문제에 쉽게 노출될 수 있다. 이런 문제를 해결하기 위해 라플라타 국립대학(UNLP)에서는 블록체인 기반의 학업 성취도 검증을 위한 프레임 워크를 설계하였고 학생들에게 블록체인 기술과 암호화를 사용하여 졸업장을 발급한다[3][4]. 그러나 이 사례의 경우 졸업장 발급과 같은 제한적인 범주에서 블록체인을 응용하고 학생의 이수 교과목의 학점과 같은 구체적인 관리 방법에 대해서는 다루지 않고 있다.

2. 블록체인

블록체인은 거래 및 데이터를 관리하는 중앙 집중 시스템에서 벗어나 개인 간의(P2P) 거래가 이뤄질 수 있게 해주는 분산 환경을 만드는 것을 목표로 한다[5]. 분산 데이터베이스인 블록체인은 각각의 블록을 체인 형태로 연결하여 안전하고 변하지 않는 형태를 유지하면서 시간의 순서대로 저장된다. 사용자에 의해 생성된 블록은 사전 정의된 구조에 따라 트랜잭션으로 구성되고 암호로 보호된다[6]. 새 블록이 블록체인 끝에 추가될 때 직전 블록에 대한 참조(해시 값)를 포함시켜 새로운 블록으로 연결된다[7]. 이 작업을 하기 위해서는 암호화 단방향 해시 함수(SHA-256)가 적용되어 블록의 익명성과 불변함을 보장한다[8]. 블록이 원장 끝에 추가되면 네트워크에 참여한 참여자들에게 복제 및 동기화되어 분산 저장되게 된다.

블록체인에는 크게 퍼블릭 블록체인(Public blockchain), 프라이빗 블록체인(Private blockchain), 컨소시엄 블록체인(Consortium blockchain) 으로 나눌 수 있다. 퍼블릭 블록체인은 데이터의 공개 부분을 강조하므로 누구나 자유롭게 블록체인 네트워크에 참여할 수 있다. 자유롭게 참여할 수 있는 퍼블릭 블록체인이지만 일부분은 참가자의 익명성을 유지하기 위해 암호화될 수 있다[9]. 이러한 블록체인의 형태로는 대표적으로 비트 코인과 이더리움 블록체인이 있다. 프라이빗 블록체인은 허가받은 사람만이 블록체인 네트워크에 참여할 수 있는 형태이다. 그러나 프라이빗 블록체인은 소수의 참여자만 네트워크에 참여할 수 있어서 탈 중앙화를 벗어나기 힘들다는 단점이 있다. 컨소시엄 블록체인은 퍼블릭 블록체인과 프라이빗 블록체인의 중간 형태이다. 프라이빗 블록체인처럼 네트워크 참여를 허가해주는 주체를 통해 네트워크에 참여할 수 있지만 프라이빗 블록체인과는 다르게 같은 목적을 가진 여러 기관이 하나의 컨소시엄 형태를 구성하여 네트워크를 운영한다.

블록체인은 중앙 집중 형태를 벗어나 원장을 네트워크 참여자들에게 복제하여 저장하는 구조이다. 새로운 블록이 생성되면 원장 끝에 추가하여 블록체인 형태를 유지하여야 하는데 이때 새롭게 생성된 블록을 원장에 추가하기 위해서는 네트워크 참여자들의 합의(Consensus)가 이루어져야 한다.

분산 합의 프로토콜을 통하여 원장에 연결될 블록을 결정하는데 이때 사용되는 합의 알고리즘으로는 PoW(Proof of Work, 작업 증명), PoS(Proof of Stake, 지분 증명), DPos(Delegated Proof of Stake, 위임지분 증명), DDPoS(Dual Delegated Proof of Stake, 이중위임지분 증명), PoB(Proof of Burn, 소각 증명), PoI(Proof of Importance, 중요도 증명) 등이

있다. 이중 가장 보편적으로 사용하는 합의 알고리즘으로는 PoW와 PoS 방식 등이 있다.

PoW 알고리즘은 비트코인, 비트코인 캐시 등의 방식에서 사용되는 알고리즘으로 원장에 연결할 해시를 찾는 과정(Mining)을 반복함으로써 해당 작업에 참여했음을 증명하는 알고리즘이다. 반복적으로 해시를 계산해야 하기 때문에 컴퓨팅 성능 중에 연산 능력이 중요시된다. 새로운 블록을 연결하기 위해서는 네트워크의 모든 참여자들에게 승인을 거쳐야 하기 때문에 PoW 방식은 거래 내역을 위조하기 힘들다는 장점이 있다. 반면 모든 참여자들에게 승인을 거쳐야 하는 만큼 원장의 길이가 길어지고 참여자가 많아질수록 처리 속도가 늦어지는 단점이 있다.

PoS 합의 알고리즘은 참여자가 가지고 있는 지분율에 비례하여 합의의 의사결정 권한이 부여되는 방식이다. PoW의 연산을 통한 방식이 아니기 때문에 채굴(Mining)이 불필요하다. PoS는 리워드를 많이 가지고 있는 참여자가 원장에 새로운 블록을 연결할 수 있는 기회를 많이 가진다. PoW와 같이 원장에 블록을 연결할수록 리워드가 주어지는데, 주어지는 리워드의 양 또한 지분율에 따라 비례한다.

블록체인은 스토리지의 분산과 추적 기능으로 여러 분야에 활용되고 있다. 의료 건강 분야 중 최근 일부 연구에서는 블록체인을 이용하여 EHR(Electronic Health Recordm, 전자 건강 기록)을 획기적으로 개선할 수 있다는 연구가 진행되고 있다[10][11]. 물류 및 운송 분야에서도 블록체인을 활용한 연구들이 활발하게 진행되고 있으며, 이는 원재료의 생산부터 소비까지의 모든 거래를 블록체인 시스템을 사용함으로써 투명성을 보장할 수 있다는 장점이 있다[12-14]. 또한 4차 산업시대 분야 중 하나인 IoT(Internet of Things, 사물 인터넷)에서도 블록체인 기술 활용에 대한 연구가 이루어지고 있다[15][16]. 블록체인을 이용하여 IoT 기기들 간의 통신 보안성을 강화하고 해킹으로부터 안전하게 사용될 수 있는 연구도 진행 중이다[17]. 그러나 학습 교육 분야에서 블록체인을 활용한 연구는 부족한 실정이다[2].

따라서 본 연구에서는 블록체인 기반 학점은행관리 시스템을 제안한다. 제안한 시스템은 프라이빗 블록체인에서 PoW방식을 사용하며, 참여한 계정의 권한을 차등으로 부여하여 기관과 학습자의 역할을 분리한다. PoW는 채굴이 필수적이기 때문에 일반적으로 보상을 통해 채굴을 장려하는데, 본 연구에서는 권한이 부여된 학습기관과 국가평생교육진흥원이 필수적으로 채굴하도록 하며 별도의 보상은 주어지지 않는다.

Ⅲ. 제안 시스템

본 연구에서 제안하는 블록체인 형태의 학점관리 시스템은 [그림 2]와 같다. 본 연구는 학생의 성적에 관련된 정보를 블록체인에 보관하는 방식으로 보안성과 무결성, 투명성을 보완한 방법을 제안한다. 이 방법은 기존 중앙 집중형 학점 관리 시스템의 단점을 다음과 같이 개선할 수 있다. 첫째, 학점 처리 과정에 학습자가 참여하여 검증할 수 있다. 둘째, 학습 결과를 투명하게 공유함으로써 조작에 대한 의심을 제거하고 신뢰성을 확보한다. 셋째, 학습 데이터를 분산 저장하여 단일 공격 지점을 제공하지 않아 네트워크 장애가 발생하여도 시스템이 동작가능하다.

학습자는 자신의 수료 이력을 저장할 수 있는 지갑을 가지고 있고, 학습기관은 학습자가 과목을 이수할 때마다 이수 학습 정보를 블록 형태로 만들어서 원장의 끝에 연결한다. 블록은 학습자가 이수한 학점, 과목과 같은 정보를 저장되는 형태로 구성도는 [그림 3]과 같다.

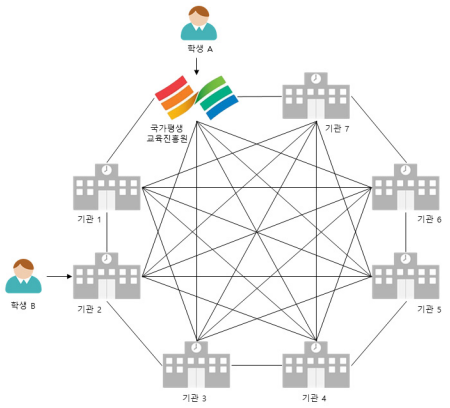

그림 2. 블록체인 기반 학점 은행제 관계도

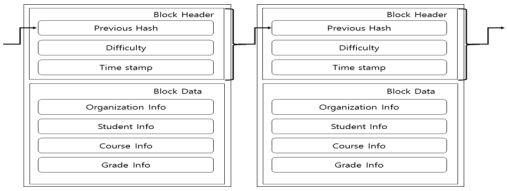

그림 3. 제안한 학점 은행제 블록체인 구성도

학습자가 학습자 등록 신청하게 되면 학습자 계정이 국가평생교육진흥원이나 학습 기관을 통해 시스템에 등록한다. 학습자가 수업을 수료할 경우 이수한 과목에 관해 블록이 체인 형태로 저장되며 저장된 블록체인은 네트워크 참여자인 기관에게 복제되고 분산 저장된다.

본 연구에서는 PoW 방식의 블록체인 분산 합의 방식을 사용한다. 초기단계에서 참여기관이 한정된 프라이빗 네트워크를 사용하기 때문에 가장 이해관계가 깊은 국가평생교육진흥원과 해당 교육기관에서 채굴을 하도록 한다.

다음은 새로운 학습 기관과 학습자를 등록하는 경우와 학습자의 학점이수 정보를 등록하는 경우에 대한 시나리오의 설명이다.

1. 기관 등록

새로운 기관이 기존 네트워크에 참여하기 위한 방법은 [그림 4]와 같다. 새로운 기관이 네트워크에 참여하기 위해서는 계정을 생성한 후 계정 주소를 국가평생교육진흥원에 전달하고 가입 신청을 해야 한다. 국가평생교육진흥원에서 가입 신청이 확인되면 새로운 기관을 검증하고 권한을 부여한다. 등록이 완료되면 새로운 기관은 학습자의 이수한 학습정보 블록을 생성할 수 있는 권한이 부여된다.

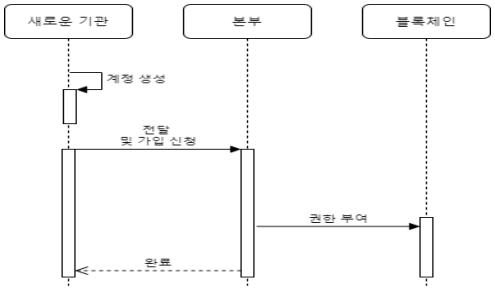

그림 4. 블록체인 네트워크에 새롭게 참여하는 기관

2. 학습자 등록 및 수강 신청

학습자가 학점 은행제를 이용하기 위하여 가입을 할 수 있는 방법은 2가지 형태가 있다. 먼저 수강 전 국가평생교육진흥원에 회원가입을 통하는 방법과 수업을 수강하는 도중 학습기관을 통해 회원가입을 하는 방법이 있다. 수강 전 회원 가입하는 방법은 [그림 5]와 같다. 학습자가 국가평생교육진흥원에 가입 신청을 하면 국가평생교육진흥원은 학습자의 계정과 학습자의 정보를 블록체인에 등록한다. 학습자는 전달받은 계정을 이용하여 블록체인 지갑의 설정을 완료하고 국가평생교육진흥원에 블록체인 지갑이 준비되었다고 알려주면 최종 가입 승인된다.

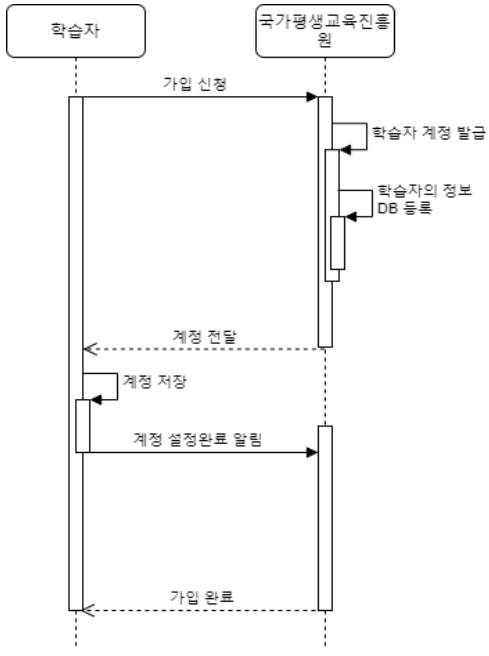

그림 5. 수강 전 학습자 등록

학습자가 수강 신청을 하기 위해서는 먼저 가입 여부를 확인하여야 한다. 가입 여부에 따라서 진행되는 방법은 [그림 6]과 같다. 첫 번째로 학습자가 가입이 되어 있지 않는 경우에는 원하는 수업을 기관을 통해 수강을 먼저 하고 나중에 가입을 한다. 학습자가 기관에 승인을 받고 수강을 하는 중 학점 은행제에 가입을 하기 위해서는 수강을 듣는 기관에 가입 신청을 하고 기관은

국가평생교육진흥원에 관련 데이터를 전송하여 학습자의 가입 신청을 알린다. 국가평생교육진흥원은 학습자의 계정을 생성하여 학습자에게 전달한다. 학습자는 전달받은 계정을 설정하고 국가평생교육진흥원은 학습자의 블록체인 지갑이 정상적으로 등록되었는지 확인되면 가입 완료한다. 두 번째로 학습자가 가입한 상태에서 수강 신청을 하게 되면 기관에서는 학습자와 과목의 정보를 받아서 국가평생교육진흥원에 등록 신청을 하고 완료가 되면 학습자는 수강 신청을 완료할 수 있다.

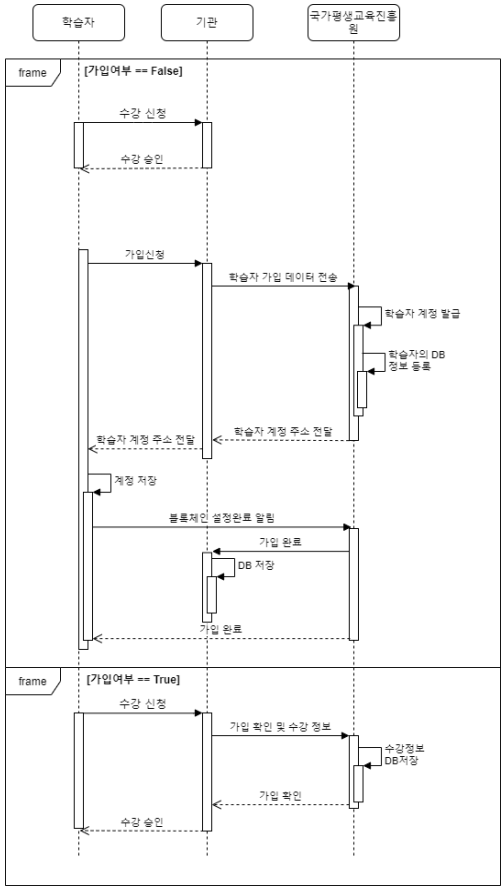

그림 6. 수강 신청

3. 학점 등록

학점 등록 방법은 [그림 7]과 같다. 학습자가 과목을 이수하면 기관은 학습자가 정상적으로 이수했는지 확인한다. 확인이 되면 학습자의 계정에 이수 기관 정보, 과목 정보, 이수 학점, 등급 정보를 블록으로 만들어 원장에 연결한다. 연결이 완료되면 학습자와 기관들은 새롭게 추가된 블록을 확인할 수 있다.

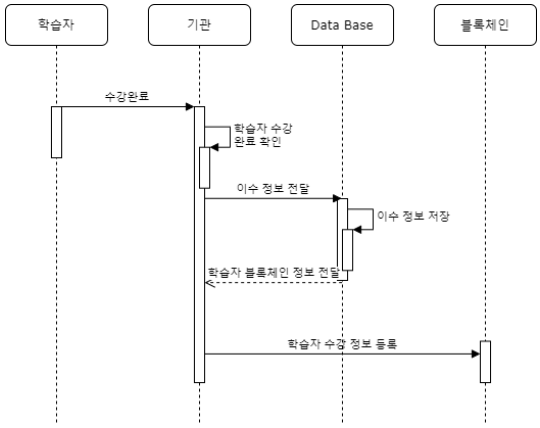

그림 7. 학습자의 학점 등록

Ⅳ. 제안 시스템의 구현

1. 구현 환경 및 내용

본 연구에서 제안한 시스템의 프로토타입 구현을 위해 Go-Ethereum 플랫폼을 사용하여 블록체인에 스마트 컨트랙트를 활용하여 학습 데이터를 기록 조회할 수 있는 DApp을 개발한다. 이더리움은 블록 크기에 제한이 없으며 키값을 중복 저장하지 않기 때문에 공간을 절약한다.

상태 트리(Merkle Patricia Tree)는 블록에 저장된 거래를 기반으로 생성되고 각 블록은 상태 루트(stateRoot) 노드 값을 저장한다. 각 계정 상태는 상태 트리의 각 노드에 배치되며 상태 트리의 루트 노드는 각 노드의 계정 주소를 사용하여 해시 값을 계산하여 구한다. 상태가 변경되면 루트 노드 값이 변경되어 데이터 조작을 즉시 확인할 수 있다[18]. 악의적인 사용자가 노드 데이터를 조작할 때 부모 노드의 해시 값 또한 모두 변경되기 때문에 위조 및 변조를 감지할 수 있다. 각 블록의 해시 값은 다음 블록의 parentHash (이전 해시) 값과 연결되어 블록체인을 형성하므로 데이터를 신뢰할 수 있다.

이더리움의 데이터 모델은 비트코인과 비교했을 때 스마트 계약을 가진다는 점이 가장 큰 차이점이라고 할 수 있다. 스마트 계약은 블록체인에서 실행되는 응용 프로그램 단위이다. 스마트 컨트랙트를 통해 이 연구에서 제안한 시스템 코드를 작성하고 이더리움 가상 머신(EVM) 컴파일러에 의해 EVM 바이트 코드가 블록체인에 작성 및 배포된다. EVM은 가상 시스템에서 실행되므로 플랫폼 독립적 기능이다. 블록체인 네트워크에 참여하는 모든 노드는 동일한 블록을 가지므로 모든 노드는 EVM 바이트 코드를 보유하고 실행한다[19].

본 연구에서는 스마트 계약 개발 및 컴파일을 용이하게 하기 위하여 Remix로 시스템을 프로토타입을 구현하고 결과를 확인한다. 이 연구에서 제안한 학습 데이터를 블록체인에 기록하기 위해 Solidity 언어를 사용한다.

스마트 컨트렉트는 [코드 1]과 같으며 [코드 1]의 학생과 기관, 학점에 대한 구조체의 정보는 [표 1], 함수에 대한 정보는 [표 2]와 같다. Solidity는 현재 소수점 데이터 타입에 대해 완벽하게 지원하지 않기 때문에 향후 소수점 연산을 포함하는 코드를 구현하거나 기존 소수점 학점 표기를 정수 타입으로 변환하는 함수를 추가해 사용할 수 있다.

표 1. 구조체 정보

구조체명	설명
StudentDetail	학생 정보 구조체
OrganizationDetail	교육 기관 정보 구조체
SubjectDetail	수강 정보 구조체

표 2. 함수 기능 정보

함수명	설명
proposedSystem	생성자·관리자 설정
onlyAdmin	관리자 검사
onlyOrgs	교육기관 또는 관리자 검사
insertOrganization	교육기관 추가
insertStudent	학생 추가
insertGradeInfo	수강 정보 추가
setViewAuthority	보기 권한 부여
getStudentInfo	학생 성적 조회

본 연구에서 제안하는 시스템을 구축하기 위하여 블록체인의 스마트 컨트랙트를 ProposedSystem으로 나타내었으며, ProposedSystem은 국가평생교육진흥원(admin), 학습자들(students), 학습 기관들(orgs)에 대한 정보를 가지고 있다. 학습자(StudentDetail)는 이름(name), 생일(birth), 평균 학점(averageGrade), 총 시수(totalCredit), 학습 내역 배열(history), 조회 허용 기관 배열(allowList)로 구성되어있다. 학습 내역(SubjectDetail)은 학습 기관(org), 과목명(subjectName), 시수(credit), 학점(grade)으로 이루어져 있으며, 학습 기관(OrganizationDetail)은 기관명(name)으로만 구성되어 있으나 필요에 따라 향후 추가할 수 있다.

[그림 8]은 [코드 1]의 Solidity 소스 코드를 컴파일 후 배포한 모습이다. 생성된 학습 기관 계정을 통해 교육 정보가 입력되고 트랜잭션 버튼을 클릭하여 데이터가 블록에 기록된다. 학습 데이터를 블록에 기록하기 위해 생성된 계정은 한 명의 학습자나 교육 기관을 특정하게 되며 권한이 있는 계정은 메시지를 수신하고 코드를 실행하며 계정으로 메시지를 보낼 수 있다. 사용자는 브라우저 등을 통해 블록체인에 액세스하거나 학습자를 등록하거나 학점을 관리할 수 있다.

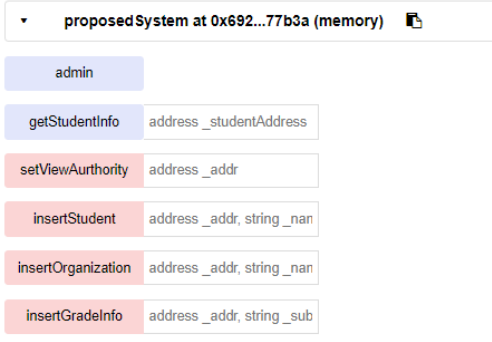

그림 8. 동작 화면

블록체인에 기반한 제안 시스템의 주요 프로세스는 (1) 학습기관 등록, (2) 학습자 등록, (3) 성적등록, (4) 제3자 조회 권한설정, (5) 제3자 학습자 성적 조회로 나눌 수 있다. 주요 5가지 프로세스를 테스트하기 위하여 아래와 같이 진행하였으며, 테스트를 위해 사용한 계정 정보는 [표 3]과 같다.

코드 1

```
pragma solidity ^0.4.8;

contract proposedSystem  {

    address public admin;
    mapping(address => StudentDetail) private students;
    mapping(address => OrganizationDetail) private orgs;

    struct StudentDetail {
        string name;
        string birth;
        int256 averageGrade;
        int256 totalCredit;
        SubjectDetail[] history;
        address[] allowList;
    }

    struct OrganizationDetail{
        string name;
    }

    struct SubjectDetail{
        OrganizationDetail org;
        string subjectName;
        uint8 credit;
        uint8 grade;
    }

    function proposedSystem() {    admin = msg.sender; }
    modifier onlyAdmin() { if (msg.sender != admin) throw; _; }
    modifier onlyOrgs() {
        bytes memory tempEmptyStringTest = bytes(orgs[msg.sender].name);
        if(tempEmptyStringTest.length == 0 && msg.sender != admin) throw; _;
   }

    function insertOrganization(address _addr, string _name) onlyAdmin {
        orgs[_addr].name=_name;
    }

    function insertStudent(address _addr, string _name, string _birth) onlyOrgs {
        students[_addr].name=_name;
        students[_addr].birth=_birth;
    }

    function insertGradeInfo(address _addr, string _subjectName, uint8 _credeit, uint8 _grade) onlyOrgs{
        students[_addr].history.push(SubjectDetail({ org:orgs[msg.sender], subjectName:_subjectName, credit:_credeit, grade:_grade}));
          students[_addr].averageGrade                                                                                                    =
students[_addr].averageGrade*students[_addr].totalCredit+_grade*_credeit)/(students[_addr].totalCredit+_credeit);
        students[_addr].totalCredit+=_credeit;
    }

    function setViewAurthority(address _addr) {
        bytes memory tempEmptyStringTest = bytes(students[msg.sender].name);
        if(tempEmptyStringTest.length != 0) students[msg.sender].allowList.push(_addr);
    }

    function getStudentInfo(address _studentAddress) public constant returns(bool _allowResult, string _name,
      string _birth, int256 _averageGrade,int256 _totalCredit) {
        _allowResult=false;
        for(uint i = 0; i < students[_studentAddress].allowList.length; i++) {
            if (students[_studentAddress].allowList[i]==msg.sender) {
                _allowResult=true;
                delete students[_studentAddress].allowList[i];
            }
        }
        if(_allowResult==true){
            _name = students[_studentAddress].name;
            _birth = students[_studentAddress].birth;
            _averageGrade=students[_studentAddress].averageGrade;
            _totalCredit=students[_studentAddress].totalCredit;
        }
    }
}
```

표 3. 테스트 계정 정보

권한	주소
국가평생교육진흥원	"0xca35b7d915458ef540ade6068dfe2f44e8fa733c"
교육기관1	"0x14723a09acff6d2a60dcdf7aa4aff308fddc160c"
교육기관2	"0x4b0897b0513fdc7c541b6d9d7e929c4e5364d2db"
수강생	"0x583031d1113ad414f02576bd6afabfb302140225"
열람자	"0xdd870fa1b7c4700f2bd7f44238821c26f7392148"

(1) 학습기관 등록

본 연구의 시스템에서 국가평생교육진흥원이 관리자 역할을 한다. 교육 기관을 추가하기 위해서는 관리자 계정이 필요하다. 관리자 계정으로 로그인 후 [그림 8]의 기능 중 InsertOrganization에 추가하고자 하는 기관의 주소와 기관명을 작성하면 기관이 추가된다.

(2) 학습자 등록

학생이 추가되기 위해서는 관리자 또는 교육 기관의 권한이 필요하다. 관리자 또는 기관의 계정으로 로그인 후 InsertStudent에 학생의 주소와 이름, 생년월일을 입력하면 학생 정보가 추가된다.

(3) 성적등록

관리자와 교육 기관은 학생이 수강을 완료했을 때 학점과 수강 정보를 입력할 수 있다. 수강생이 이수한 과목의 정보를 입력하기 위해서는 관리자 또는 기관으로 로그인 후 InsertGradeInfo에 과목 이수 정보를 입력할 수강생의 주소와 과목명, 학점, 등급을 입력하여 추가할 수 있다. 수강생이 과목을 이수할 때마다 이수 정보는 블록체인에 연결되어 기록된다.

(4) 제3자 조회 권한설정

학생은 자신이 이수한 교육들의 평점과 수강 정보를 제3의 기관이 조회할 수 있도록 권한을 부여할 수 있다. 이를 위해서 수강생으로 로그인 후 setViewAuthority에 열람자의 주소를 입력하면 열람자는 수강생의 이수과목에 대한 정보를 조회할 수 있다.

(5) 제3자 학습자 성적 조회

제3의 기관은 조회 권한이 있는 학생들의 성적 조회가 가능하다. 열람자가 학생의 정보를 조회하기 위해서는 getStudentInfo에 수강생의 주소를 입력하면 해당 수강생의 과목 이수 정보를 확인할 수 있다. 본 연구에서 제안한 시스템의 수강생 학점 정보를 열람자가 조회한 결과는 [표 4]와 같다.

본 연구에서 구현한 프로토타입 시스템은 이더리움의 스마트 컨트랙트를 사용하여 국가평생교육진흥원, 학습 기관 뿐만 아니라 모든 사용자가 기학습정보를 임의로 수정할 수 없으며, 학습기관에 저장되어있는 학습정보가 위·변조되어도 실제 블록체인에는 반영되지 않는다. 본 구현에서 테스트를 통하여 학습자가 조회를 허용하는 경우에만 학습자의 성적이 조회되는 것을 확인하였고, 기존의 중앙화 서버를 데이터 분산 저장에 의하여 동작하도록 함으로써 데이터 위·변조로부터 안

표 4. 수강생 성적 조회 실행 결과

from	0xdd870fa1b7c4700f2bd7f44238821c26f7392148
to	proposedSystem.getStudentInfo(address) 0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
transaction cost	18329 gas (Cost only applies when called by a contract)
execution cost	10649 gas (Cost only applies when called by a contract)
input	4b82caec000000000000000000000000583031d1113ad414f02576bd6afabfb302140225

decoded input	{
	"address _studentAddress": "0x583031d1113ad414f02576bd6afabfb302140225"
	}

decoded output	{
	"0": "bool: _allowResult true",
	"1": "string: _name 홍길동",
	"2": "string: _birth 20010301",
	"3": "int256: _averageGrade 3",
	"4": "int256: _totalCredit 5"
	}

logs	[]

정성을 확보하였다.

2. 성능 평가

본 장에서는 현재 운영 중인 평생교육원 시스템과 제안된 블록체인 기반 시스템을 비교 분석을 한다. 현재 운영 중인 평생교육원 시스템은 국가평생교육진흥원의 중앙 집중형 통합 시스템으로 운영되는 방식이다. 기존 중앙 집중형 시스템은 원장을 신뢰할 수 있게 관리하기 위하여 제3의 기관을 선정하여 신뢰를 확보하는 방식으로 발전해왔다. 하지만 제3의 신뢰기관을 선택하고 신뢰를 유지하는 비용은 상대적으로 높다는 단점이 있다. 또한, 학습 기관 별로 정보의 교류가 어렵고, 학습 내용은 서버에 보관돼 해킹 등의 악의적인 접근 및 조작에 취약할 수 있다.

본 연구에서 제안한 방법을 사용하면 학습에 관련된 모든 이력이 블록체인으로 구성된다. 따라서 학습 정보가 필요한 이해 관계자는 블록체인의 정보를 사용하여 학습 이력을 조회할 수 있다. 또한, 해시 함수를 이용하여 데이터의 무결성을 확보할 수 있으므로 학습 내역의 조작 등이 어려워 이해관계자에게 신뢰성 있는 정보를 제공할 수 있다. 중앙 집중식 관리 시스템의 경우 해킹 등 악의적인 공격으로 인해 학습 정보가 변경될 수 있지만 본 연구에서 제안한 블록체인 시스템의 학습 정보는 조작이 불가능하다. 또 한 데이터 암호화를 위해 ECIES 및 AES-256 암호화 알고리즘을 사용하여 기밀성을 제공할 수 있고, Secp256k1 ECDSA 디지털 서명을 사용하여 인증 및 데이터 위조를 방지할 수 있다 [20].

표 5. 기존 방법과 제안기술 방식 비교

구분	기존방법	제안된 방법 (블록체인 기반)
서버유지비용	높음	낮음
외부공격으로 인한 데이터 변경	약함	강함
사고의 추적	어려움	쉬움
데이터의 저장	밀집	분산
확장성	어려움	쉬움
신뢰도	△	O
안정성	중앙서버 오류 시 심각한 문제 발생	일부 시스템 오류가 발생하여도 전체 네트워크에 영향 없음

이 연구에서는 제안한 시스템을 기존의 중앙 집중식 관리 시스템의 성능과 비교하며 그 결과는 [표 5]와 같다. 중앙 집중식 관리 시스템은 유지 관리 비용이 많이 들 뿐만 아니라 중앙 서버의 데이터 조작과 같은 보안에 취약하므로 데이터 변형과 왜곡 같은 사고를 추적하기 어렵다. 블록체인을 이용한 제안 시스템은 분산 관리를 통해 유지 보수 비용이 낮으며 분산 학습 히스토리 저장을 통해 학습자의 학습 히스토리를 검색할 때 안정성을 보장한다. 또한, 해당 학습자의 학업 내용이 공개되어 있기 때문에 역 추적 등을 통한 과정을 통해 다양한 시스템에 활용될 수 있다.

본 연구에서 제안하는 시스템에서는 학습 정보가 블록체인에 기록되고 관리되기 때문에 학습 정보의 왜곡이 어렵고, 학습자의 학습내용은 암호화되어 학습자가 동의하는 제3자에게만 공개 가능하도록 설정된다. 블록체인에 참여하는 모든 노드가 관리자 역할을 하기 때문에 운영 및 관리 측면에서 우수하다.

V. 결론 및 향후 과제

기존 시스템은 중앙 집중형 관리 시스템으로 모든 정보가 통합 관리되어 운영되는 방식이다. 중앙 집중형은 데이터를 관리하기는 용이하나 외부로부터 공격에 취약할 수 있고 중앙 시스템에 문제가 생길 경우 전체 시스템의 오류를 일으킬 수 있는 단점이 있다.

이를 해결하기 위해 본 연구에서는 블록체인 기술을 이용하여 학점은행제의 블록체인 기반 시스템을 제안하고 제시한 시스템 설계를 바탕으로 프로토타입을 구현하였다. 학습기관, 학습자 정보 들을 포함하여 학습 정보를 블록체인에 저장함으로서 관리를 하는 방법이다. 학습자의 등록부터 학점 확인 및 증명까지 학습 정보는 기관과 학습자 본인을 포함하여 학습자가 공개를 원하는 제3 자도 언제든 조회할 수 있다. 또한, 등록된 학습 정보는 역추적이 가능하며, 신뢰할 수 있는 학습 정보 히스토리를 제공한다. 이는 학습자의 학습 정보를 토대로 제공할 수 있는 추가 서비스의 개발이 가능하도록 기반을 마련할 수 있다.

본 연구에서 제안된 시스템의 프로토타입은 이더리

움 플랫폼 상에서 구현되었으며, 스마트 컨트랙트를 사용하여 참여기관 사이의 블록체인 정보 공유를 실험적으로 검증하였다. 본 논문에서 제안된 시스템은 프로타입으로 구현되어 실제 환경에 적용하는데 한계가 있다. 본 시스템을 실제 환경으로 확장 운영하기 위해서는 일반 사용자들이 쉽게 접속하기 위한 사용자 인터페이스를 위한 API가 추가적으로 개발되어야 한다. 또한 참여기관 간의 블록체인 채굴에 대한 합의 방법이 개선되어야 한다. 본 연구에서는 블록체인 합의를 위해 PoW 분산 합의 방식을 사용하여 채굴을 시스템 이해 관계자에게 할당하였다. 그러나 학생이 수강하지 않은 참여기관도 합의의 주체가 되는 문제가 있을 수도 있기 때문에 향후 합의와 관련된 부분을 발전시키거나 채굴이 필요없는 PoS 분산 합의 방식으로의 연구가 필요하다.

참 고 문 헌

[1] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A Blockchain-Based Higher Education Credit Platform," in IEEE Access, Vol.6, pp.5112-5127, 2018.

[2] A. Third, J. Domingue, M. Bachler, and K. Quick, "Blockchains and the Web position paper," Proc. W3C Workshop Distrib. Ledgers Web, 2016.

[3] F. Bond, F. Amati, and G, Blousson, *Blockchain academic verification use case*, 2015.

[4] A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-Based Applications in Education: A Systematic Review," Applied Sciences, Vol.9, No.12, p.2400, 2019.

[5] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—A systematic review," PLoS ONE, Vol.11, p.e0163477, 2016.

[6] T. Aste, P. Tasca, and T. Di Matteo, "Blockchain technologies: The foreseeable impact on society and industry," Computer, Vol.50, No.9, pp.18-28, 2017.

[7] M. D. Sleiman, A. P. Lauf, and R. Yampolskiy, "Bitcoin message: Data insertion on a proof-of-work cryptocurrency system," Proc. Int. Conf. Cyberworlds (CW), pp.332-336, 2015.

[8] Secure Hash Standard (Shs) Federal Information Processing Standards Publication, 2012.

[9] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture consensus and future trends," Proc. IEEE Int. Congr. Big Data (BigData Congr.), pp.557-564, 2017(6).

[10] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," Proc. IEEE 18th Int. Conf. e-Health Netw. Appl. Services (Healthcom), pp.1-3, 2016(9).

[11] C. He, X. Fan, and Y. Li, "Toward ubiquitous healthcare services with a novel efficient cloud platform," IEEE Trans. Biomed. Eng., Vol.60, No.1, pp.230-234, 2013(1).

[12] Y. Yuan and F. Y. Wang, "Towards blockchain-based intelligent transportation systems," Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC), pp.2663-2668, 2016(11).

[13] 선화, 김현덕, "블록체인 기술이 물류산업에 미치는 영향에 관한 연구," e-비즈니스연구, 제20권, 제3호, pp.137-148, 2019.

[14] 이예지, 원종운, 김용태, "블록체인을 이용한 위험물질 운송관리시스템 구현," 한국지능시스템학회 논문지, 제28권, 제6호, pp.545-551, 2018.

[15] 홍은기, 이수진, 서승현, "사물 인터넷을 위한 블록체인 기술 동향," 정보보호학회지, 제28권, 제3호, pp.38-46, 2018.

[16] 김미희, 김영민, "블록체인 DPoS 합의 알고리즘을 활용한 IoT 장치 관리 시스템 개발," 전기전자학회논문지, 제23권, 제2호, pp.508-516, 2018.

[17] D. Fakhri and K. Mutijarsa, "Secure IoT Communication using Blockchain Technology," 2018 International Symposium on Electronics and Smart Devices (ISESD), Bandung, pp.1-6, 2018.

[18] 박경호, *누구나 쉽게 배우는 블록체인 DApp 개발*,

비제이퍼블릭, 2019.
[19] 와타나베 아츠시, 마츠모토 유타, 니시무라 요시카즈, 시미즈 토시야, *블록체인 애플리케이션 개발 실전 입문*, 위키북스, 2018.
[20] 이동영, 박지우, 이준하, 이상록, 박수용, "블록체인 핵심 기술과 국내외 동향," 정보과학회지, 제35권, 제6호, pp.22-28, 2017.

저 자 소 개

손 기 봉(Ki-Bong Son) 정회원

- 2012년 2월 : 가톡릭대학교 컴퓨터정보공학부(공학사)
- 2015년 2월 : 조선대학교 전기·전자·통신교육(교육학석사)
- 2015년 3월 ~ 현재 : 금오공과대학교 컴퓨터공학과 박사과정

〈관심분야〉 : 블록체인, Front-end Design & Verification Methodology

손 민 영(Min-Young Son) 정회원

- 2008년 2월 : 고려대학교 컴퓨터정보학과(공학사)
- 2010년 2월 : 고려대학교 정보경영공학과(공학석사)
- 2017년 2월 : 금오공과대학교 컴퓨터공학과 박사(공학박사)
- 2017년 3월 ~ 현재 : 금오공과대학교 컴퓨터공학과 연구원

〈관심분야〉 : 블록체인, 네트워크, 분산처리, 그래프, 데이터마이닝

김 영 학(Young-Hak Kim) 종신회원

- 1984년 2월 : 금오공과대학교 전자공학과(공학사)
- 1989년 2월 : 서강대학교 전자계산학과(공학석사)
- 1997년 8월 : 서강대학교 전자계산학과(공학박사)
- 1999년 3월 ~ 현재 : 금오공과대학교 컴퓨터공학과 교수

〈관심분야〉 : 블록체인, 병렬알고리즘, 분산처리, 임베디드 시스템 등