JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 24, No. 11, pp. 2909-2917, Nov. 2023

Check for updates

# 고등교육에서 블록체인 기반의 학위 이수 검증 시스템의 설계

손 용 범[1] · 김 영 학[2*]
[1]한국지능정보사회진흥원 책임연구원
[2*]금오공과대학교 컴퓨터공학과 교수

# Degree Completion Verification System Based on Blockchain in Higher Education

**Yong-Bum Son[1] · Young-Hak Kim[2*]**

[1]Principal Manager, Information Security Team, National Information Society Agency, Daegu 41068, Korea
[2*]Professor, Department of Computer Engineering, Kumoh National Institute of Technology, Gumi 39177, Korea

**[요 약]**

국내 대학의 경우 상위 학위 과정에 입학한 학생을 대상으로 학위 이수 여부를 검증하며 검증 과정이 기관과 기관 간에 공문으로 이루어져 많은 시간과 행정부담을 가중한다. 본 연구에서는 이러한 문제를 해결하기 위해 블록체인 기반의 고등교육기관 학위 이수 검증 시스템을 설계하였다. 제안 시스템의 실현 가능성을 확인하기 위해 이더리움 플랫폼 환경에서 프로토타입을 구현하였으며 실제 환경과 연동을 위해 학사 데이터베이스와 인터페이스를 별도로 구현하였다. 제안 시스템의 평가를 위해 학사 정보 데이터와 키값과 블록체인 주소의 쌍을 갖는 실험용 데이터베이스를 구축하였으며, 실험 결과 매우 효율적이며 신뢰성 있게 학위 이수 여부를 검증할 수 있음을 확인하였다. 제안된 시스템에는 고등교육기관 누구나 풀 노드 또는 SPV 노드로 참여할 수 있다.

**[Abstract]**

In the case of domestic universities, degree completion is verified for students admitted to higher degree programs, and the verification process is conducted through official documents between institutions, adding considerable time and administrative burden. We designed a degree completion verification system for higher education institutions (HEIs) based on blockchain to solve this problem. To confirm the feasibility of the proposed system, a prototype was implemented in the Ethereum platform environment. Furthermore, the academic database and interface were separately implemented to link with the real environment. To evaluate the system, an experimental database was constructed with academic information data and pairs of key values and blockchain addresses. The experiment confirmed that degree completion can be verified very efficiently and reliably. Any HEI can participate in the proposed system as a full node or Simplified Payment Verification (SPV) node.

**색인어 :** 블록체인, 학위 이수 검증, 이더리움 플랫폼, 고등교육, 대학 학적

**Keyword :** Block Chain, Degree Completion Verification, Ethereum Platform, Higher Education, University Records

**http://dx.doi.org/10.9728/dcs.2023.24.11.2909**



**Received** 12 September 2023; **Revised** 25 September 2023
**Accepted** 26 September 2023

***Corresponding Author; Young-Hak Kim**

**Tel:** +82-54-478-7524
**E-mail:** kimyh@kumoh.ac.kr

## Ⅰ. 서 론

블록체인 기술은 2009년에 사토시 나카모토에 의해 비트코인 플랫폼이 소개된 이후부터 널리 활용되고 있다[1]. 블록체인은 블록들이 해시 체인에 의해서 선형 방식으로 연결된다. 각 블록에는 응용 영역에서 발생 된 트랜잭션(거래)들이 저장된다. 블록체인은 중앙 집중식 방식의 문제를 해결하기 위해 분산 시스템 방식을 사용한다. 일반적인 분산 시스템은 데이터를 서로 다른 장치에 분산 보관하여 분산 처리하는 방법을 사용하나, 블록체인은 분산 시스템에 참여하는 모든 참여자가 동등한 입장에서 모든 데이터를 복사하여 저장한다. 이러한 블록체인의 특성으로 누군가가 악의적으로 데이터를 조작할 경우 분산 시스템에 참여하는 모든 장치의 데이터를 변조해야 한다. 또한, 블록체인에서 각 블록은 해시 주소로 연결되어 특정 블록이 수정되면 이후의 모든 블록에 영향을 주기 때문에 데이터 변조가 쉽지 않다.

블록체인 기술은 초기에 비트코인, 이더리움 등과 같은 전자 화폐 분야에 응용되었으나 최근에는 산업 전반에 활용되고 있다[2]-[6]. 교육 분야에서 국내외 사례를 살펴보면 주로 대학을 중심으로 한 고등교육 기관에서 졸업증명서, 시험, 성적 등의 학사 관리에 부분적으로 응용되고 있다. 우리나라의 경우 초·중등학교의 경우 교육부 및 각 시도교육청에서 교육행정정보시스템(National Education Information System: NEIS)을 사용하여 학생들의 학적 정보를 종합 관리한다. 고등교육기관의 경우 개별적으로 자체 구축된 시스템을 사용하여 학적 정보를 관리한다. 최근에 일부 고등교육 기관 등에서 부분적으로 블록체인 기술을 접목하고 있으나, 이들 시스템은 대부분 중앙 집중식 방식을 사용하고 있다.

국·내외 고등교육기관에서 졸업한 많은 학생이 매 학기 상위 학위 과정의 학업을 수행하기 위해 타 기관으로 진학한다. 국내의 경우 해당 기관에서는 이 학생들에 대한 학위 이수 여부를 검증하기 위해 학생이 졸업한 기관에 공문으로 요청한다. 공문으로 요청받은 기관에서는 해당 학생에 대한 학위 이수 여부의 결과를 다시 공문으로 보낸다. 해외 학위의 경우 학생이 졸업한 기관에 직접 또는 한국연구재단 등과 같은 대행 기관을 이용하여 학위 이수 여부를 검증한다. 한국대학교육협의회에서 운영하는 대학알리미에 의하면 2022년 기준 우리나라의 고등교육기관 428개에서 562,995명의 졸업생이 배출되었다[7]. 이와 같은 대규모 인원에 대해서 기관과 기관 간의 공문 요청에 의한 학위 이수 여부의 검증 절차는 행정부담이 가중되고, 공식적인 문서의 요청 및 응답에 많은 시간이 소요된다.

본 연구에서는 위에서 기술한 문제를 효율적으로 개선하기 위해 블록체인 기술을 사용하여 학위 이수 여부 검증 시스템을 설계한다. 제안 시스템은 고등교육기관에서 개별적으로 운영하는 학적 정보시스템과 연계하여 학위 이수 여부의 검증에 필요한 정보를 추출하여 블록체인으로 구성한다. 제안된 블록체인 네트워크에는 고등교육기관 누구나 참여할 수 있으며 각 기관이 관리하는 학생의 학위 정보를 트랜잭션으로 블록체인 풀에 보낸다. 블록체인 풀에 저장된 트랜잭션들은 참여 기관의 합의 절차에 따라 블록으로 생성된다. 제안 시스템에서 빠른 검색을 위해 학위 등록번호와 해시 주소의 쌍을 갖는 별도의 데이터베이스를 운영한다. 이 데이터베이스는 블록체인 참여 기관이 학위 등록번호를 사용하여 빠르게 학위 이수 여부를 검증하기 위해 사용된다. 본 연구에서 제안된 시스템은 이더리움 플랫폼 환경에서 프로토타입으로 구현하여 실험적 평가를 통하여 효율성을 확인하였다.

2장에서 관련 연구를 기술하고 3장에서 본 연구에서 제안한 학위 이수 여부 검증 블록체인 시스템을 설계한다. 4장에서는 제안된 시스템의 프로토타입을 구현하여 평가한다. 마지막으로 5장에서 결론을 맺는다.

## Ⅱ. 관련 연구

고등교육 기관 측면에서 살펴보면 한 교육기관에서 다른 교육기관으로 진학을 위해 해당 학생은 자신이 졸업한 기관에서 온라인 또는 오프라인으로 학위증을 발급하여 제출한다. 학위증을 제출받는 기관은 학위 이수 여부 검증을 위해 학생이 졸업한 기관에 공문 요청을 통하여 학위 이수의 진위를 확인한다. 고혁수[8]는 블록체인을 기반으로 대학 학위 증명서 인증 모델을 제안하였다. 그러나, 이 연구에서는 공용 개념보다는 개별 대학에서 블록체인을 구성하여 학위 이수를 확인하였으며, 또한 구체적인 설계 및 프로토타입을 구현하지 않고 개념적인 측면만 제시하였다. Deenmahomed 등[9]은 대학 교육의 미래란 주제로 블록체인을 사용하여 학생들의 시험, 성적, 인증서 관리에 관한 방안을 전반적으로 고찰하였다. 이 연구에서는 학생이 하나의 코스를 등록하여 시험을 평가하고 이수한 코스를 인증하는 과정을 블록체인 모델로 설계하였다.

Raimundo 등[10]은 고등교육에서 블록체인 응용에 관한 연구 사례를 전반적으로 조사하였다. 이 연구에서는 블록체인, 블록체인과 교육, 고등교육 등을 키 워드로 사용하여 이미 발표된 연구 결과를 종합적으로 검색하여 키 워드를 기반으로 연구의 연계 관계를 정리하여 최근 연구 추세를 분석하였다. Palanivel[11]은 고등교육에서 학습 모델에 블록체인 기술을 적용하였으며 이러닝(E-learning) 학습을 위한 블록체인 구조를 제안하였다. 제안된 블록체인 구조에서 학생이 온라인 또는 오프라인 코스에 등록하여 해당 코스를 이수하는 과정 전반이 블록체인에 기록되어 관리된다. Timothy 등[12]은 모바일 환경에서 블록체인을 사용하여 고등교육의 성적 관리 방법을 연구하였다. 이 연구에서는 모바일 환경에서 학생들의 편의를 위해 블록체인 기반의 성적 관리 방법을 실험적으로 구현하였다.

Turkanovic 등[13]은 유럽의 고등교육 기관에서 공통적 활용을 위한 블록체인 기반의 고등교육 학점 관리 플랫폼인 EduCTX을 제안하였다. EduCTX 시스템은 블록체인 기반의 P2P 네트워크를 사용하며 유럽에서 기관 간에 통용할 수 있는 학점 관리 및 성적 부여 과정을 포함한다. 또한, 이 시스템은 오픈 소스인 Ark 블록체인 플랫폼을 기반으로 프로토타입이 구현되었다. 기술한 내용과 같이 블록체인 기술이 고등교육 분야뿐만 아니라 다양한 영역으로 확대되어 응용되고 있다[12]-[15]. 그러나 현재 고등교육의 학위 이수 여부의 검증을 위한 전문화된 연구 결과와 시스템 제안은 미비한 실정이다. 따라서 본 연구에서 고등교육기관에서 개별적으로 운영되는 시스템과 연계하여 학위 이수 여부의 검증을 위한 블록체인 시스템을 설계한다.

## Ⅲ. 제안 시스템의 설계

이 장에서는 본 연구에서 제안한 블록체인 기반의 고등교육기관의 학위 이수 검증 시스템을 설명한다.

### 3-1 제안 시스템 개요

그림 1은 고등교육기관에서 블록체인 기반의 학위 이수 검증 시스템의 총괄 개요를 보여준다. 제안된 시스템은 크게 3개의 영역으로 구분되며 각각의 기능은 다음과 같다.

● Higher Education Institution(고등교육기관) : 고등교육기관은 학위를 수여하는 대학 또는 대학원 등의 기관을 의미한다. 국내의 경우 고등교육기관은 교육부에서 인증한 전문대 이상의 기관을 포함한다. 현재 대부분의 고등교육기관은 자체적으로 중앙 집중식 방식의 서버를 운영하여 졸업생의 학적 정보를 관리하고 있다. 그림 1에서 HEI는 본 연구에서 제안한 학위 이수 검증 블록체인 시스템에 참여하는 고등교육 기관을 의미한다.

● Blockchain Management(블록체인 관리) : 학위 이수 검증 블록체인 시스템에 참여하는 고등교육기관은 자체 학적 서버에서 학위 이수 검증에 필요한 최소 정보를 추출한다. 다음에 이 정보를 블록체인 네트워크에 보내 참여 기관의 합의 과정을 거쳐 블록체인을 구성한다. 각 모듈에 대한 개략적인 개요는 다음과 같다.

<Transaction Pool Interface> 이 모듈은 고등교육기관이 제안된 학위 이수 검증 시스템에 연동하기 위한 인터페이스이다. 블록체인에 참여하는 각 고등교육기관은 이 인터페이스를 통하여 자체 서버에 보관된 졸업생 학위 정보를 트랜잭션 풀로 전송한다.

<Degree Transaction pool> 제안된 블록체인에 참여하는 각 고등교육기관에서 보내진 졸업생 학위 정보의 트랜잭션들이 이 풀에 저장된다. 이 풀에 저장된 학위 정보 트랜잭션은 새로운 블록이 생성되어 블록체인으로 구성될 때까지 풀에서 대기한다.

<Transaction Collection/Block Consensus> 이 모듈에서는 제안된 블록체인 네트워크에 참여한 고등교육기관들이 새로운 블록을 생성하고 합의 과정을 수행한다. 합의 과정은

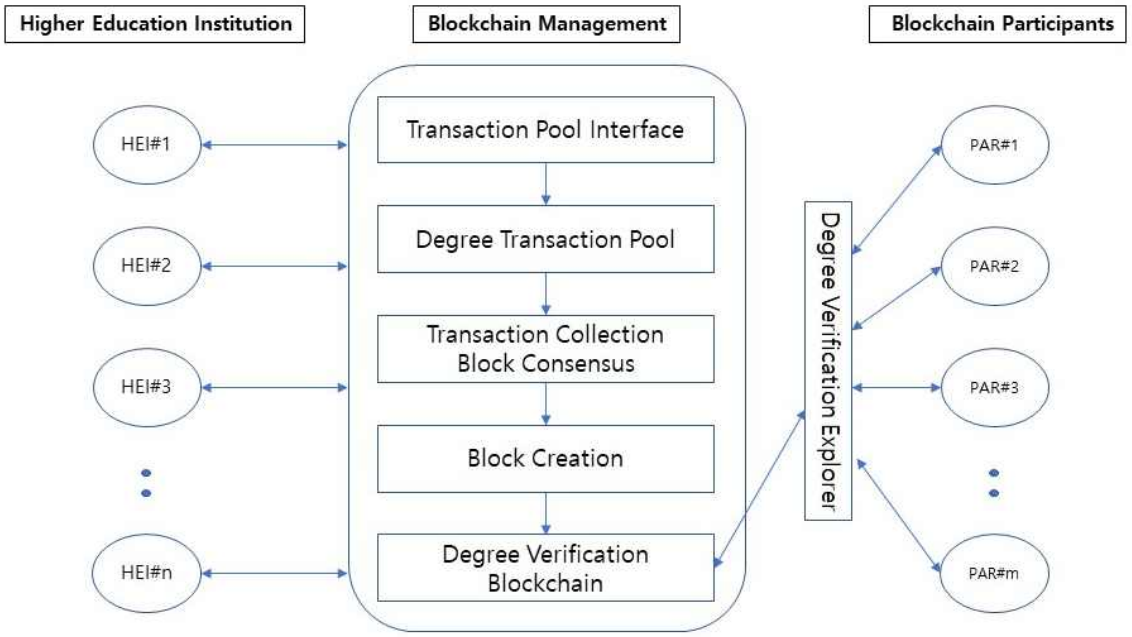



**그림 1.** 블록체인 기반의 학위 이수 검증 시스템
**Fig. 1.** Degree completion verification system based on blockchain

다양한 방법이 있지만 고등교육기관의 특성을 고려하여 본 연구에서는 대표 교육기관에 위임하여 새로운 블록의 합의를 수행하는 POA(Proof of Authority) 방식을 사용한다.

<Block Creation> 블록의 합의 과정을 거쳐 새로운 블록이 생성되고 이 블록이 학위 이수 검증 블록체인에 추가된다. 새로운 블록이 생성 시 블록에 포함된 트랜잭션들은 효율적인 검색을 위해 별도의 데이터베이스로 구성된다. 이 부분은 모듈의 상세 설계 과정에서 구체적으로 설명한다.

<Degree Verification Blockchain> 이 모듈은 제안된 블록체인 시스템에 참여한 고등교육기관들이 합의를 거쳐 만들어진 졸업생의 학위 이수 검증 블록체인을 의미한다. 새로운 블록이 생성될 때마다 이 블록체인에 추가된다.

● Blockchain Participants(블록체인 참여자) : 제안된 학위 이수 검증 블록체인은 고등교육기관이 참여하는 블록체인이지만 필요할 경우 누구나 참여할 수 있다. 본 시스템의 참여자(PAR)는 학위 이수 검증 탐색기(Degree Verification Explorer)를 통하여 블록체인에서 해당 학생에 대한 학위 이수 검증을 할 수 있다. 학위 이수 여부의 검색을 효율적으로 수행하기 위해 별도의 저장소를 두며 세부적인 내용은 주요 모듈의 상세 설계 과정에서 설명한다.

### 3-2 주요 모듈의 상세화

그림 1에서 보인 것과 같이 본 연구에서 제안한 블록체인 기반의 학위 이수 검증 시스템은 다음과 같은 절차에 따라 블록체인이 구성되고 운영된다.

1) 제안된 학위 이수 검증 블록체인에 참여하는 각 고등교육기관은 자체 서버의 학적 데이터베이스에서 졸업생의 학적 정보를 추출한다. 제안된 시스템의 블록체인에 포함될 학적 정보는 학위 이수 검증을 위해 필요한 최소한 항목을 포함하며 그 내용은 다음과 같다.

```
Transaction_Information_for_Degree_Verification {
  String Student_ID //학번
  String Name //이름
  String Birthday //생년월일
  String Institution_Name //학위수여 기관명
  String Degree_Type //학위 구분(학사/석사/박사)
  String Department_Name //학(부)과명
  Date Entrance_Date //입학일
  Date Graduation_Day //학위수여일
  String Degree_Registration_Number //학위등록번호
}
```

각 고등교육기관에서 추출된 졸업생의 학위 이수 검증 정보는 자체 서버와 블록체인을 연동하는 Transaction Pool Interface를 통하여 Degree Transaction Pool로 보내진다. 참여 기관에서는 졸업생이 배출될 때마다 매번 이 과정을 반복하며 이러한 트랜잭션들은 블록으로 생성되어 최종적으로 학위 이수 검증 블록체인에 포함될 때까지 풀에서 대기한다.

2) Degree Transaction Pool에는 각 고등교육기관에서 보내진 졸업생의 학위 이수 검증 트랜잭션들이 모여 대기한다. 학위 이수 검증 블록체인에 참여하는 기관은 트랜잭션 풀에서 대기하는 트랜잭션들을 모아 새로운 블록을 생성할 수 있다. 새로운 블록을 생성하기 위해 트랜잭션 풀에서 대기 중인 트랜잭션들의 우선순위는 없으며 큐 방식으로 오래 대기 중인 트랜잭션부터 순서대로 선택하여 처리한다. 학위 이수 검증을 위한 트랜잭션 데이터는 암호와 화폐를 다루는 비트코인 블록체인과 같이 빈번하게 트랜잭션이 생성되지 않고 주로 학기 또는 코스 이수가 끝나는 시점에서 트랜잭션이 생성된다.

3) 학위 이수 검증 블록체인에 참여하는 고등교육기관은 트랜잭션 풀에서 대기 중인 트랜잭션들을 모아 새로운 블록 생성을 할 수 있다. 새로 생성된 블록은 학위 이수 검증에 참여하는 모든 참여 기관에 보내지고 블록 합의 절차를 거친다. 본 연구에서는 블록 합의를 위해 고등교육기관의 특성을 감안하여 참여 기관의 대표를 선정하여 위임하는 대표자 작업증명(Proof of Authority) 방법을 사용한다. 블록 생성 및 합의 절차는 다음과 같이 수행된다.

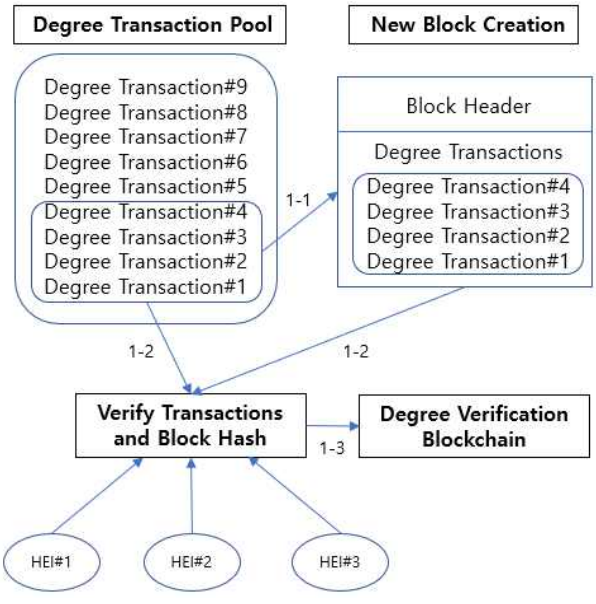



**그림 2.** 새로운 블록의 생성 및 합의 과정
**Fig. 2.** The process of creation and consensus of a new block

(1-1) 참여 기관 중에 대표로 위임된 기관은 트랜잭션 풀에 대기 중인 트랜잭션을 모아 새로운 블록과 블록의 해시값을 생성한다. 트랜잭션 처리를 위해 트랜잭션 풀에서 오래 대

기 중인 것을 먼저 처리하는 큐 방식을 사용한다. 블록은 일반적 블록체인과 같이 블록 헤더와 트랜잭션으로 구성된다. 블록 헤더는 머클 해시, 타임스탬프, 이전 블록의 해시, 현재 블록의 해시값을 갖는다. 새로운 블록의 생성에 참여한 기관은 모든 참여 기관에 새로 생성된 블록과 블록의 해시값을 전송한다.

(1-2) 참여 기관 중에서 대표로 위임받은 기관은 전송된 블록의 검증을 위해 트랜잭션 풀에서 해당 트랜잭션을 모아 해시값을 계산하여 전송된 블록의 해시값과 일치 여부를 확인한다. 만일 검증한 해시값이 일치할 경우는 올바른 블록으로 합의하고 그렇지 않을 경우는 합의에 동의하지 않는다.

(1-3) 새로운 블록을 생성한 참여 기관은 대표로 위임받은 참여 기관들의 합의가 완료되면 이 블록을 학위 이수 검증 블록체인(Degree Verification Blockchain)에 추가하고, 이를 학위 이수 검증 블록체인에 참여하는 모든 기관에 알려준다.

그림 2는 이러한 과정을 거쳐 트랜잭션 풀에서 새로운 블록을 생성하고 대표 참여 기관이 블록을 합의하는 과정을 보여준다. 새로운 블록의 생성을 위해 학위 트랜잭션 풀에서 먼저 도착한 트랜잭션들을 선택한다. 그림2의 예에서 한 블록에 4개 트랜잭션이 저장된다고 가정하고 트랜잭션 #1~#4가 선택되었다. 다음에 이들 트랜잭션을 기반으로 블록 헤더에 포함될 해시값을 계산하고, 합의를 위해 생성된 블록을 참여 기관에 전송한다.

그림 2에서 보인 것과 같이 대표로 위임받은 3개의 참여 기관(HEI#1~HEI#3)이 전송받은 블록의 합의 절차를 수행한다. 합의에 참여하는 대표 기관은 전송받은 새로운 블록에 포함된 트랜잭션들을 트랜잭션 풀에서 확인하고 이를 기반으로 블록 해시값을 계산한다. 계산된 해시값이 전송받은 해시값과 일치하면 합의를 완료한다. 그림 3은 그림 2의 결과로 트랜잭션 풀에서 대기 중인 학위 트랜잭션들을 모아 블록을 생성하고 합의 과정을 완료한 후에 생성된 학위 이수 검증 블록체인의 예를 보여준다.

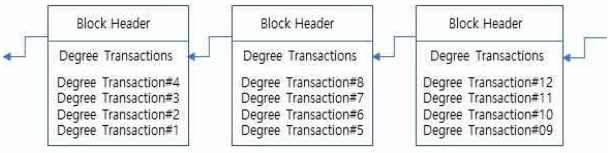



**그림 3.** 학위 이수 검증 블록체인의 예
**Fig. 3.** Example of degree completion verification blockchain

4) 그림 2에서 보인 것과 같이 학위 이수 검증을 위한 참여자는 고등교육기관뿐만 아니라 졸업생의 학위 이수 검증이 필요한 기타 기관도 참여할 수 있다. 제안된 블록체인에 참여하는 각 고등교육기관의 졸업생 학위 정보가 학위 이수 검증 블록체인으로 만들어져 있어, 블록체인 참여자는 이 블록체인을 통하여 해당 졸업생에 대한 학위의 진위를 검증할 수 있다.

그림 4는 학위 이수 검증 블록체인과 연계하여 특정 졸업생의 학위 이수 검증을 빠르게 검색하기 위한 과정을 보여준다. 일반적으로 학위 등록번호는(대학명-학위-년도-순번)으로 구성되어 중복되지 않아 키값(Key Value)으로 사용할 수 있다. 이 키값을 기반으로 하여 새로운 블록이 생성될 때 학위 이수 검증 데이터베이스를 구성하는 과정은 다음과 같다.

(1-1) 새로운 블록이 생성될 때마다 합의 과정을 완료한 후에 해당 블록에 포함된 모든 트랜잭션의 학위 등록번호(Verification Key) 키값과 블록 해시값을 학위 이수 검증 데이터베이스에 전송한다.

(1-2) 전송된 학위 등록번호와 블록의 해시값 쌍을 학위 이수 검증 데이터베이스에 저장한다. 한 블록에 포함되는 서로 다른 키값을 갖는 트랜잭션들은 같은 해시값을 갖는다.

(1-1)과 (1-2)의 절차는 새로운 블록을 생성하는 참여 기관이 합의가 완료되어 블록이 학위 이수 검증 블록체인에 추가되는 과정에서 작업을 수행한다. 다음은 제안된 학위 이수 검증 블록체인 네트워크의 참여자가 해당 졸업생의 학위를 검증하는 과정을 살펴본다.

(2-1) 학위 이수 검증은 Degree Verification Explorer를 통하여 수행된다. 학위 이수 검증을 위한 특정 졸업생의 학위 등록번호를 키값으로 사용하여 학위 이수 검증 데이터베이스에서 이 키값을 갖는 블록의 해시값을 찾는다.

(2-2) 검색된 블록의 해시값을 사용하여 학위 이수 검증 블록체인(Degree Verification Blockchain)에서 해시값과 일치된 블록을 찾는다. 다음에 해당 블록에서 트랜잭션들을 순차적으로 비교하여 학위 등록번호와 일치하는 트랜잭션이 있는지를 검색한다. 만일 학위 등록번호와 일치하는 트랜잭션이 있다면 학위 이수 검증 절차가 완료된다.

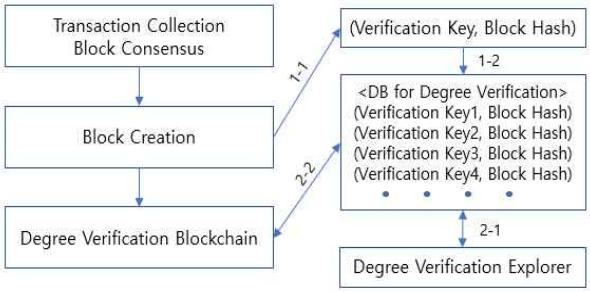



**그림 4**. 학위 이수 검증 블록체인과 연계하여 빠른 검색을 위한 데이터베이스 구성
**Fig. 4**. Database construction for quick search in conjunction with degree completion verification blockchain

본 연구에서는 그림 4와 같이 학위 이수 검증 블록체인과 연계하여 별도의 데이터베이스를 구성하여 순차적 특성을 갖는 블록체인의 검색 속도를 향상하였다. 실제로 찾고자 하는 학위 등록번호를 갖는 트랜잭션을 갖는 해시값을 알고 있다면 해당 블록은 상수시간에 찾을 수 있다. 반면에 블록에서 원하는 학위 등록번호를 갖는 트랜잭션을 찾는 수행시간은

블록 내의 트랜잭션의 수에 비례한다. 학위 이수 검증 블록체인에는 참여자의 상황을 고려하여 풀 노드 또는 SVP 방식으로 참여할 수 있다. 여기서 풀 노드로 참여하면 학위 이수 검증 블록체인의 완전한 복사본을 가질 수 있으며, SVP 방식의 참여는 블록체인의 헤더 정보만을 가실 수 있다.

## Ⅳ. 제안 시스템의 구현 및 평가

본 연구에서 제안한 학위 이수 검증 블록체인 시스템의 프로토타입을 구현하기 위해 이더리움 기반의 Geth v1.8.22를 사용하였다. 이더리움 블록체인 플랫폼은 리믹스(Remix) 개발 환경을 지원하며, 스마트 컨트랙트(Smart Contract) 기능을 제공한다. 먼저, 학위 이수 검증 블록체인을 위해 제네시스 블록을 생성하고 시스템의 동작을 실험하기 위해 표1과 같이 4개의 계정을 생성하였다. 블록체인에 참여하는 고등교육기관의 학적 정보시스템에서 개인의 학위 정보를 제안된 시스템의 트랜잭션 풀에 전송하기 위해 Ethereum JavaScript API를 사용하여 인터페이스를 구현하였다. 이 인터페이스를 통하여 블록체인에 참여하는 기관의 학적 정보시스템에 저장되어있는 졸업생의 학위 정보가 그림2에서 보인 학위 트랜잭션 풀에 전송된다. 제안된 학위 이수 검증 블록체인에서는 트랜잭션 풀에 있는 트랜잭션들을 모아 기관들의 합의를 통해 새로운 블록을 생성한다.

**표 1.** 제안 시스템의 실험을 위한 계정
**Table 1.** Accounts for experiment of proposed system

| Authority | Address |
|---|---|
| HEI#1 | 0x37dce8e0dc7a18aba4c418ccbdc151c844f5e483 |
| HEI#2 | 0x479833a0a9ab16e126b820494e0a9dd60d2b4284 |
| HEI#3 | 0x6515e903d558cf73fe48bfbde9dcf6c5a69281eb |
| Participant | 0x5c765e4aaa4a785522f08ece7ea1a37573d5510c |

제안된 학위 이수 검증 블록체인에 참여하는 각 기관은 졸업생의 학위 정보를 보관하는 학적 정보시스템을 갖는다. 본 연구에서는 실제 환경을 사용할 수 없는 점을 고려하여 실험을 위해 최소한 정보를 갖는 학적 정보시스템을 별도로 구현하였다. 실험을 위한 학적 정보시스템의 구현을 위해 웹서버(Apache Tomcat8.0)와 데이터베이스(Cubrid 9.3), 스프링 프레임워크, Ajax, Html, CSS, Java Script 등의 개발 환경 및 도구를 사용하였다. 학적 정보 데이터베이스의 스키마는 실험을 위한 최소 정보인 학번, 이름, 생년월일, 수여 기관, 학위 구분, 학과명, 입학일, 졸업일, 학위번호로 구성하였다.

그림 5는 제안된 블록체인에 참여하는 기관의 실험용 학적 데이터베이스를 구축하기 위한 입력화면을 보여준다. 그림 5의 입력화면에서 각 필드의 항목을 입력하고 저장 버튼을 클릭하면 실험용 학적 데이터베이스에 저장된다. 입력 항목 중에서 학위번호는 중복되지 않는 유일한 값으로 향후 학위 이수 검증을 위한 기본 키값으로 사용된다.

그림 6은 그림 5에서 입력받은 개별 학위 정보가 학적 데이터베이스에 구축된 예를 보여준다. 그림6에서 리스트 형태로 출력될 때 블록 생성 여부 필드의 초기값은 N이며, 실험용 트랜잭션의 생성을 위해 실행 버튼을 추가로 만들어 두었다. 제안된 시스템의 실험을 위해 트랜잭션 실행 버튼을 클릭하면 해당 학위 정보가 블록체인 네트워크로 전송된다.

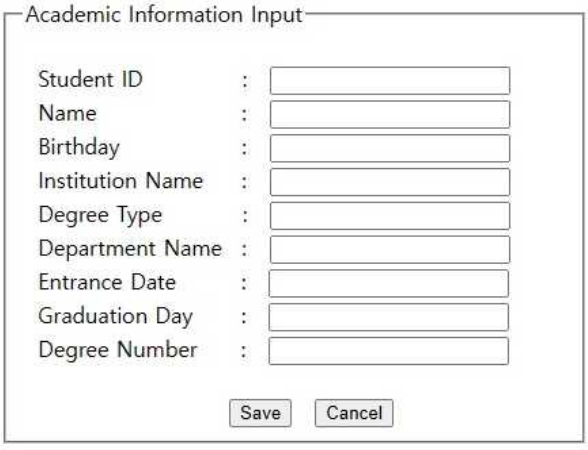
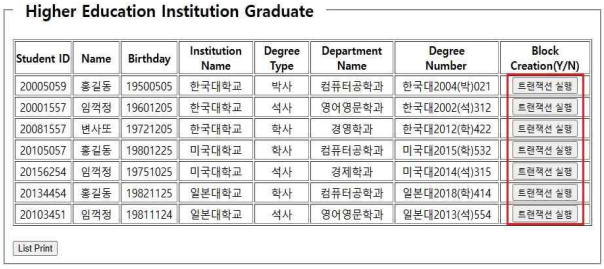



**그림 5.** 학적 정보시스템의 데이터베이스를 위한 입력화면
**Fig. 5.** Input screen for database of academic information system


Higher Education Institution Graduate

| Student ID | Name | Birthday | Institution Name | Degree Type | Department Name | Degree Number | Block Creation(Y/N) |
|---|---|---|---|---|---|---|---|
| 20005059 | 홍길동 | 19500505 | 한국대학교 | 박사 | 컴퓨터공학과 | 한국대2004(박)021 | 트랜잭션 실행 |
| 20001557 | 임꺽정 | 19601205 | 한국대학교 | 석사 | 영어영문학과 | 한국대2002(석)312 | 트랜잭션 실행 |
| 20081557 | 변사또 | 19721205 | 한국대학교 | 학사 | 경영학과 | 한국대2012(학)422 | 트랜잭션 실행 |
| 20105057 | 홍길동 | 19801225 | 미국대학교 | 학사 | 컴퓨터공학과 | 미국대2015(학)532 | 트랜잭션 실행 |
| 20156254 | 임꺽정 | 19751025 | 미국대학교 | 석사 | 경제학과 | 미국대2014(석)315 | 트랜잭션 실행 |
| 20134454 | 홍길동 | 19821125 | 일본대학교 | 학사 | 컴퓨터공학과 | 일본대2018(학)414 | 트랜잭션 실행 |
| 20103451 | 임꺽정 | 19811124 | 일본대학교 | 석사 | 영어영문학과 | 일본대2013(석)554 | 트랜잭션 실행 |

List Print

*Korean language was used to construct experimental data
**그림 6.** 실험을 위한 학적 데이터베이스 예
**Fig. 6.** Example of academic database for experiment

그림 7은 학적 정보시스템과 제안된 학위 이수 검증 블록체인을 연동하기 위한 트랜잭션 풀 인터페이스의 예를 보여준다. 이 인터페이스를 통하여 블록체인에 참여하는 기관에서 학위 정보를 트랜잭션 풀로 전송할 수 있다. 실험을 위해 그림 6에서 트랜잭션 실행 버튼을 클릭하면 Transaction_Start 함수가 실행되며, 학위번호와 해당 졸업자의 학위 정보가 함수의 인자 값으로 전달된다. 전달된 인자는 Ethereum JavaScript API인 sendTransaction 함수를 이용하여 학위 이수 검증 블록체인의 대표 기관의 주소를 통해 트랜잭션을 실행하도록 하였다.

```
var Web3 = require('web3');
var web3 = new Web3(new Web3.providers.
                    HttpProvider('http://localhost:8545'));

function Transaction_Start(degree_registration, degree_data){

    const txHash = web3.eth.sendTransaction({
        from: '0x37dce8e0dc7a18aba4c418ccbdc151c844f5e483',
        to: '0x479833a0a9ab16e126b820494e0a9dd60d2b4284',
        gas: '100000',
        value: '20000',
        data: web3.eth.abi.encodeParameter('bytes', degree_data)
    });
    console.log('txHash # ' + txHash);
}

var filter = web3.eth.filter('latest');

filter.watch(function(error, result){
    var block = web3.eth.getBlock(result, true);
    console.log('block number      # ' + block.number);
    console.log('block hash        # ' + block.hash);
    console.log('block block hash # ' + block.transactions[0].hash);
});
```

**그림 7.** 학적 정보시스템과 제안된 시스템의 인터페이스
**Fig. 7.** Interface between academic information system and proposed system

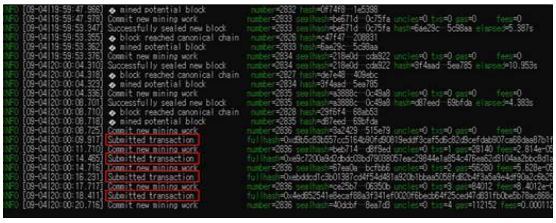


**그림 8.** 제안된 학위 이수 검증 블록체인 시스템의 실행 과정
**Fig. 8.** Execution process of proposed degree completion verification blockchain system

그림 8은 학위 이수 검증 블록체인이 실행(miner.start(1))된 결과를 보여주며, 이 결과를 통하여 학적 정보시스템에서 트랜잭션을 전송했을 때 블록체인에 올바르게 전달되었는가를 확인할 수 있다. 전송된 학위 정보들은 트랜잭션 풀에 저장되며 풀에서 트랜잭션들을 이용하여 학위 이수 검증 블록체인에 참여한 고등교육 기관들이 합의를 수행한다. 블록의 합의 과정을 거쳐 새로운 블록이 생성되고 이 블록이 학위 이수 검증 블록체인에 추가된다. 그림9에서 보인 것과 같이 특정 학위번호를 갖는 트랜잭션을 빠르게 검색하기 위해 별도의 데이터베이스에(학위번호, 블록해시)의 쌍이 저장되도록 하였다. 이 데이터베이스를 사용하면 특정 학위번호를 키값으로 갖는 블록해시의 주소값을 바로 찾을 수 있고, 해당 블록에서 학위번호와 일치하는 트랜잭션을 찾을 수 있다. 새로운 블록 생성 시 해당 블록의 정보를 가져오기 위해 Ethereum JavaScript API인 filter.watch 함수를 이용하여 구현하였다.

블록체인 고유의 특성으로 해시 주소에 의해 블록들이 순차적인 체인 형태로 연결된다. 이러한 블록체인 특성으로 인해 트랜잭션들이 증가할수록 블록의 수도 증가하게 된다. 더불어 특정 트랜잭션을 찾기 위한 검색 성능이 저하된다. 이러한 문제를 해결하기 위해 본 연구에서는 그림 9와 같이 키값

| NO | degree_number | block_hash | block_number |
|---|---|---|---|
| 1 | 한국대2004(박)021 | 0x0f9b7fe0e0cd1c44929e20a887d7d131b9631e7... | 3064 |
| 2 | 한국대2012(학)422 | 0x36ac8a961a6eab417d548ce7d0c4b555ae16ba6... | 3066 |
| 3 | 일본대2018(학)414 | 0x3beaf3c5173d449e4f184da82f03f75fa22eb0f9c... | 3067 |
| 4 | 미국대2015(학)532 | 0x17764b9c60441fb27be701c75dc3c74c251997c... | 3072 |
| 5 | 미국대2014(석)315 | 0x540056d1f2abd52ac3943c188eb7bafbc6ad5a3... | 3075 |
| 6 | 일본대2013(석)554 | 0x2e8cd962c83a28cfdb96401d979abb96c790e90... | 3137 |

* The Korean degree format was used as degree number.

**그림 9.** 학위 이수 검증 블록체인에서 검색을 위한 키값
**Fig. 9.** Key value for retrieval in degree completion verification blockchain system

**그림 10.** (키값, 블록해시)를 사용하여 검색한 결과
**Fig. 10.** Retrieval result using (key, block hash)

으로 사용되는 학위번호가 저장되는 블록해시 값을 별도로 관리하는 데이터베이스를 구성하였다. 그림 10은 블록체인 참여자 계정으로 데이터베이스에 저장된 블록해시를 이용하여 학위 이수 검증 블록체인에서 검색한 결과이며, 트랜잭션 주소의 값과 학위번호가 일치하는지 비교하여 검증 결과를 확인할 수 있다.

본 연구는 학위 이수 검증에 대한 시스템을 설계하여 실험적으로 그 결과를 평가하였다. 본 연구와 직접적 비교를 위한 적합한 연구 결과가 없어 정량적 측면의 비교가 어려운 면이 있다. 따라서 제안 시스템을 현재 국내 고등교육기관에서 학위 이수 검증을 위해 사용하는 방식과 비교하여 아래와 같이 평가한다.

(학위 이수 검증 방법) 국내의 사례를 보면 학위 이수 검증은 상호 기관 간의 공문을 통해 수작업으로 이루어지나 제안된 방법은 블록체인 시스템을 사용하여 검증할 수 있다.

(학위 검증 시간) 학위 이수 검증을 위해 공문 작성 및 발송, 결재 등으로 많은 시간이 소요되나 제안된 방법은 실시간으로 검증할 수 있다.

(행정 비용) 매년 각 대학은 상위 학위 과정에 입학한 학생들을 대상으로 학생이 졸업한 대학에 요청하여 학위 이수 여부를 검증한다. 이러한 과정은 학생의 수가 많을수록 행정부담이 증가한다. 그러나 제안된 시스템에 참여하면 해당 학생의 학위번호만 알면 즉시 조회가 가능하여 행정부담을 대폭 줄일 수 있다.

(신뢰도) 상호 기관 간의 공문에 의한 학위 이수 검증은 인위적으로 조작이 가능할 수 있지만, 제안된 시스템은 블록체인 기술을 사용하기 때문에 학위 정보의 위변조를 원천적으로 차단할 수 있다.

## V. 결 론

본 논문에서는 국내 고등교육기관에서 현재 운영 중인 학위 이수 검증 과정의 문제점을 제시하고, 이를 개선하기 위해 블록체인 기반의 학위 이수 검증 시스템을 설계하였다. 제안된 시스템을 평가하기 위해 이더리움 플랫폼 환경에서 프로토타입을 구현하였으며, 실험 결과 검색과 신뢰도 측면에서 매우 효율적임을 확인하였다. 본 논문에서 제안된 시스템은 대학뿐만 아니라 학위 이수 검증이 필요한 다양한 기관으로 확대되어 사용될 수 있다. 제안 시스템은 참여 기관에서 보내진 학위 정보를 기반으로 블록체인이 구성되며, 블록체인의 고유한 특성으로 한번 생성된 블록은 위조 및 변조가 불가하다. 만일 블록이 구성된 이후에 특정인에 대한 학위가 취소되는 경우 그 정보가 추가 블록으로 구성되며, 별도로 구성한 키값과 블록해시 주소의 쌍을 갖는 테이블을 사용하여 학위 이수 검증이 가능하다.

제안된 시스템에서 참여 기관이 충분한 컴퓨터 시스템 환경을 갖는 경우 풀 노드로 그렇지 않을 경우는 SPV 노드로 참여할 수 있다. 이러한 참여 방법에도 불구하고 본 시스템을 운영하는 대표 참여 기관은 풀 노드 환경을 갖추어야 한다. 본 연구에서 이더리움 플랫폼 환경에서 프로토타입을 구현하여 실험적으로 제안된 시스템을 평가하였다. 향후 본 연구 결과가 실제 환경에 사용되기 위해서는 참여 기관의 학사 데이터베이스와 연동하는 인터페이스 보완이 필요하다.

## 감사의 글

이 연구는 금오공과대학교 대학 연구과제비로 지원되었음(2022~2023).

## 참고문헌

[1] Bitcoin. A Peer-to-Peer Electronic Cash System [Internet]. Available: https://bitcoin.org/bitcoin.pdf.

[2] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, “Untangling Blockchain: A Data Processing View of Blockchain Systems,” *IEEE Transactions on Knowledge and Data Engineering*, Vol. 30, No. 7, pp. 1366-1385, July 2018. https://doi.org/10.1109/TKDE.2017.2781227

[3] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” in *Proceedings of IEEE International Congress on Big Data (BigData Congress)*, Honolulu: HI, pp. 557-564, June 2017. https://doi.org/10.1109/BigDataCongress.2017.85

[4] Y. Yuan and F.-Y. Wang, “Towards Blockchain-Based Intelligent Transportation Systems,” in *Proceedings of the 19th International Conference on Intelligent Transportation Systems (ITSC)*, Rio de Janeiro, Brazil, pp. 2663-2668, November 2016. https://doi.org/10.1109/ITSC.2016.7795984

[5] H. Feng, J. Wang, and Y. Li, “An Efficient Blockchain Transaction Retrieval System,” *Future Internet*, Vol. 14, No. 9, September 2022. https://doi.org/10.3390/fi14090267

[6] G. W. Hong and H. B. Chang, “Study on Blockchain Based University Public Records Management Service,” *The Journal of Society for e-Business Studies*, Vol. 26, No. 1, pp. 79-91, February 2021. https://doi.org/10.7838/jsebs.2021.26.1.079

[7] Korean Council for University Education. Higher Education in KOREA [Internet]. Available: https://www.academyinfo.go.kr/index.do.

[8] H. Ko, The Blockchain Technology Based University Degree Certificate Authentication Model Design, Master’s Thesis, Hoseo University, Asan, August 2019.

[9] H. A. M. Deenmahomed, M. M. Didier, and R. K. Sungkur, “The Future of University Education: Examination, Transcript, and Certificate System Using Blockchain,” *Computer Applications in Engineering Education*, Vol. 29, No. 5, pp. 1234-1256, September 2021. https://doi.org/10.1002/cae.22381

[10] R. Raimundo and A. Rosário, “Blockchain System in the Higher Education,” *European Journal of Investigation in Health, Psychology and Education*, Vol. 11, No. 1, pp. 276-293, March 2021. https://doi.org/10.3390/ejihpe11010021

[11] K. Palanivel, “Blockchain Architecture to Higher Education Systems,” *International Journal of Latest Technology in Engineering, Management & Applied Science*, Vol. 8, No. 2, pp. 124-138, February 2019.

[12] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, “EduCTX: A Blockchain-Based Higher Education Credit Platform,” *IEEE Access,* Vol. 6, pp. 5112-5127, January 2018. https://doi.org/10.1109/ACCESS.2018.2789929

[13] A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, “Blockchain-Based Applications in Education: A Systematic Review,” *Applied Sciences*, Vol. 9, No. 12, 2400, June 2019. https://doi.org/10.3390/app9122400

[14] T. Arndt and A. Guercio, “Blockchain-Based Transcripts for Mobile Higher-Education,” *International Journal of Information and Education Technology*, Vol. 10, No. 2, pp. 84-89, February 2020. https://doi.org/10.18178/ijiet.2020.10.2.1344

[15] Y. Li, K. Zheng, Y. Yan, Q. Liu, and X. Zhou, “EtherQL: A Query Layer for Blockchain System,” in *Proceedings of the 22nd International Conference on Database Systems for Advanced Applications (DASFAA 2017)*, Suzhou, China, pp. 556-567, March 2017. https://doi.org//10.1007/978-3-319-55699-4_34

**손용범(Yong-Bum Son)**

2012년 : 금오공과대학교 컴퓨터공학과(공학석사)
2020년 : 금오공과대학교 컴퓨터공학과(공학박사)
2019년 2월~현 재: 한국지능정보사회진흥원 정보보안팀 책임연구원
※관심분야 : 블록체인, 분산처리, 웹서버 등

**김영학(Young-Hak Kim)**

1989년 : 서강대학교 전자계산학과(공학석사)
1997년 : 서강대학교 전자계산학과(공학박사)
1999년 3월~현 재: 금오공과대학교 컴퓨터공학과 교수
※관심분야 : 블록체인, 병렬알고리즘, 분산처리, 임베디드시스템 등