

# 블록체인 기반 학교생활기록부 작성 및 관리 방안

정승욱\*, 김두연°

## Blockchain-Based Student's School Record Book System Management

Seung Wook Jung\*, Dooyeon Kim°

### 요약

블록체인은 인터넷에 신뢰를 제공하는 기술로써 신뢰를 필요로 하는 다양한 분야에 적용되고 있다. 교육분야 중에서 학교생활기록부는 그 신뢰성이 무엇보다 중요한 분야로 블록체인을 적용하였을 때 학교생활기록부의 위변조를 원천적으로 차단하여 학교생활기록의 신뢰성을 제고할 수 있다. 본 논문에서는 퍼블릭 블록체인과 허가형 블록체인을 비교하여 허가형 블록체인이 학교생활기록부에 적합함을 밝혔다. 본 논문에서는 허가형 블록체인인 하이퍼레저 패브릭을 이용하여 블록체인 기반 학교생활기록부 프레임워크를 제안하였다. 또한 본 논문은 학교생활기록부 블록구조 및 트랜잭션 구조를 제안하였다. 마지막으로 블록체인 기반 학교생활기록부의 기록 및 관리의 기본적인 흐름을 중심으로 작업 프로세스를 설명하였다. 이 본문에서 제안한 블록체인 기반 학교생활기록부 프레임워크를 4세대 나이스 추진에 반영한다면 학교생활기록부의 신뢰성 문제를 획기적으로 개선할 것으로 기대된다.

**Key Words** : Blockchain application, Student's school record book, School life record, Education, NEIS

### ABSTRACT

Blockchain is a technology that provides trust to the Internet and is being applied to various fields that require trust. In the field of education, the school record book is the most important field, and when the blockchain is applied, the forgery and falsification of the school life record can be fundamentally blocked and the trust of the school life record can be improved. In this paper, we compares public blockchain and permissioned blockchain and revealed that permissioned blockchain is suitable for school record book. In this paper, we propose a blockchain-based school record book framework using Hyperledger Fabric, a permissioned blockchain. In addition, this paper propose the block structure and transaction structure of the school record book. Finally, the work process is explained focusing on the basic flow of recording and management of the blockchain-based school record book. If the blockchain-based school record book framework proposed in this paper is applied to the 4th generation NICE, it is expected to dramatically improve the trust problem of the school record book.

### I. 서론

블록체인은 신뢰가 필요한 다양한 분야에서 적용되

고 있다<sup>1)</sup>. 교육분야에서도 블록체인 활용이 다양한 방식으로 시도되고 있다<sup>4-6,9)</sup>.

교육분야 중에서 학교생활기록부는 대학입학에 매

\* First Author : Konyang University, Department of Cyber Security, swjung@konyang.ac.kr, 정희원

° Corresponding Author : Konyang University Department of Convergence Information Technology, kimdoo@konyang.ac.kr, 정희원  
논문번호 : 202108-184-0-SE, Received July 30, 2021; Revised August 24, 2021; Accepted August 24, 2021

우 중요한 자료이므로 철저히 관리함에도 불구하고 신뢰성과 공정성 문제가 지속적으로 제기 되고 있다. 따라서 학교생활기록부에 대한 접근, 기록, 관리에 대한 근본적인 신뢰성 확보가 필요하다<sup>6,9)</sup>.

본 논문은 블록체인 기반으로 학교생활기록부를 작성 및 관리함으로써 학교생활기록부의 위변조를 근본적으로 해결하여 공정성, 신뢰성을 확보하는 방안을 제시하고자 한다.

제2장에서는 학교생활기록부에 대해서 살펴본다. 제3장에서는 학교생활기록부에 대한 블록체인 적용 방안을 제시한다. 제4장은 기대효과 및 향후 발전 방안을 살펴본다. 제5장에는 결론을 맺는다.

## II. 학교생활기록부

### 2.1 학교생활기록부 관련 근거 및 운영 배경<sup>10,11)</sup>

학교생활기록부는 학생의 학교생활모습과 발달상황을 기록하여 보존하는 문서로서, 학생들로 하여금 개인의 적성과 소질을 발견하여 전인적 성장을 통해 자아를 실현하도록 돕기 위해 제안되었다. 「초·중등교육법」시행규칙 제25조에 근거하여 학교의 장을 통하여 관리·감독하도록 하며, 교사가 학생의 학업성취도와 인성 등을 종합적으로 관찰·평가하여 작성한다.

학교생활기록부는 학교에서의 학생 지도 및 상급학교에서의 학생 선발에 활용할 수 있는 학생의 인적사항, 학적사항, 출결상황, 자격증 및 인증 취득상황, 교과학습 발달상황, 행동특성 및 종합의견, 그밖에 교육목적으로 필요한 범위 안에서 교육부령이 정하는 사항에 대하여 교육부령으로 정하는 기준에 따라 작성·관리하고 있다.

초·중등교육법 제30조의6에서 학교생활기록부는 해당 학생(학생이 미성년자인 경우에는 학생과 학생의 부모 등 보호자)의 동의 없이 제3자에게 제공하여서는 안 되도록 규정하고 있으며, 자료는 준영구로 보존하며 학생 졸업 후 5년 동안 학교에서 보관하고, 그 이후엔 「공공기록물 관리에 관한 법률 시행령」에 따라서 국가가 지정한 기관에서 보존·관리 한다.

학교생활기록부는 학교에서 학생의 교수·학습 및 진로·진학지도 자료로 활용되며, 학생이 학교생활을 통해 수행하고 경험한 대부분의 활동 내역과 결과를 입력하기 때문에 학생에 대한 총체적 이해를 돕는 자료로서 상급학교에 진학하거나, 취업 등의 자료로 활용된다<sup>8-10)</sup>.

### 2.2 학교생활기록부 구성<sup>10,11)</sup>

학교생활기록부는 고등학교를 기준으로 설명하면 인적사항, 학적사항, 출결상황, 수상경력, 자격증 및 인증 취득상황, 진로희망사항, 창의적 체험 활동 상황, 교과학습발달상황, 독서활동상황, 행동특성 및 종합의견으로 구성된다. 각각의 세부 내용을 살펴보면 다음과 같다<sup>8)</sup>.

- 인적사항 : 학생의 이름, 주민등록번호를 입력하고 현재 거주하는 주소지와 부모의 이름과 생년월일 등 학생의 개인적인 정보에 관하여 입력한다.
- 학적사항 : 학생이 입학하기 이전 학교의 이름과 졸업 일자를 입력한다. 검정고시 합격자는 합격한 연월일을 입력하고 ‘검정고시 합격’이라고 입력한다. 재학 중에 학적에 변동이 발생한 경우 전출학교와 전입학교에서 각각 학적변동에 관하여 기록하는데, 여기에는 학적변동이 발생한 일자, 학년과 학교, 학적의 변동 내용을 입력한다. 그리고 ‘특기사항’란에는 학적 변동이 발생한 사유를 입력한다.
- 출결상황 : 학생의 학년별 출석일과 결석일에 관한 정보를 입력한다. ‘특기사항’란에는 결석사유 또는 개근 등과 같은 특기사항이 있는 경우에 담임교사가 입력한다.
- 수상경력 : 교내에서 수상한 상의 이름, 등급(위), 수상 일자, 수여기관 이름, 참가대상 (참여인원)을 입력한다. 같은 작품 또는 한 가지의 내용으로 수준을 다르게 여러 번 수상하였을 경우, 가장 최고 수준의 수상 경력만을 입력하도록 한다.
- 자격증 및 인증 취득상황 : 반드시 고등학교 재학 중에 취득한 것만 기재가 가능하다. 학생이 취득한 자격증의 이름, 자격증 번호, 취득한 일자 및 자격을 발급한 기관명을 입력한다. 기재가 가능한 자격증은 국가 기술자격법에 의한 국가기술자격증, 개별 법령에 의한 국가자격증, 자격기본법에 의해 국가가 공인한 민간자격증 중에서도 기술과 관련이 있는 내용으로 한정한다.
- 진로희망사항 : 담임교사가 학기 중에 진로지도를 실시하여 학생과 학부모의 진로희망을 파악한 후, 이를 기록한다. 학생의 진로희망 사유를 구체적으로 기술하며 빈칸으로 둘 수 없게 되어 있다. 담임교사 외 진로교육 담당자의 자료가 있을 경우 이를 받아 담임교사가 입력한다.
- 창의적 체험활동상황 : 창의적 체험활동은 총 네 가지 영역으로 구성되는데, 자율활동, 동아리활동, 봉사활동, 진로활동이 이에 해당한다. 각 영역별로 활동내용, 평가의 방법과 기준은 교육과정을 근거

로 학교별로 정하도록 한다. 영역별 이수시간을 입력하고, 해당 영역에서 활동실적이 우수하거나 개별적 특성이 드러나는 사항을 특기사항으로 입력한다.

- 교과학습발달상황 : 평가에 따른 ‘교과’와, ‘과목’, 해당 교과와 ‘단위수’, 취득한 점수에 대한 ‘원점수/과목평균(표준편차)’, ‘성취도 (수강지수)’, 과목별 ‘석차등급’을 산출하여 학기가 종료될 때마다 입력한다.
- 세부능력 및 특기사항: 교과담당교사가 해당교과에서 특별히 두각을 드러내거나 특기할 만한 것이 있는 학생에 대하여 해당 과목별 성취기준에 따른 학생의 성취 수준의 특성, 학습활동에 참여한 정도 등을 문장으로 기재한다.
- 독서활동상황 : 학생이 개인적으로 읽은 책과 교과별 독서활동상황 중 특기할 만한 학생을 대상으로, 학생이 읽은 책의 제목과 저자, 학생이 이를 통해 느낀 짧은 감상 등을 입력한다.
- 행동특성 및 종합의견 : 담임교사가 학생을 수시로 관찰하여 학교교육 이수 중 학생의 행동특성을 바탕으로 학생의 학교교육 이수 상황, 학생을 총체적으로 이해할 수 있는 종합의견 등을 입력한다.

### 2.3 학교생활기록부의 활용<sup>10,11)</sup>

#### 2.3.1 학생과 학부모에게 정보 제공

학교생활기록부를 통해서 학생과 학부모에게 정보를 제공하는 가장 큰 이유는 학생의 학업 성취를 통해 나타난 적성과 소질을 발견하며 이를 지속적으로 개발하여 진로를 선택하고 자아를 실현하도록 함에 있다. 학교생활기록부에 나타난 교과 성적과 교과별 담당 교사가 작성한 세부능력 및 특기사항, 독서 활동상황, 창의적 체험활동상황 등 학교생활기록부의 여러 항목을 종합적으로 기록함으로써 학부모가 자녀의 학업성취를 폭넓게 파악할 수 있다.

#### 2.3.2 학생과 학부모에게 정보 제공

교사가 학생에 대하여 종합적이고 진단적인 충분한 정보를 생활기록부에 기록한다면, 그것은 학교에서의 교수-학습 지도와 생활지도 프로그램을 효율적으로 운영하는데 큰 도움이 된다.

교사는 ‘교과학습 발달상황’에 기록된 학생의 각 교과별 학업성취 정도를 통해 향후 교수-학습 프로그램을 개발하는데 활용할 수 있으며 각 학생별 세부교과 영역에서의 강·약점을 파악하여 학생의 개별 교과

지도에도 활용할 수 있다.

생활지도와 진로지도 측면에서도 학생의 성격, 진로희망 사항, 행동특성 등이 매년 기록되어 다음해에 전달되므로 학년 초 교사가 새로운 학생을 맡게 되었을 때에도 학생의 행동발달사항을 빠르게 파악하여 학생이 원하는 진로에 대해 원활히 지도 할 수 있다.

#### 2.3.3 상급학료로 진학 또는 취업에 활용

학교생활기록부는 상급학교로의 진학과 취업에도 활용된다. 고등학교 학교생활기록부는 대학입시에서 진학을 위한 기본 자료로 활용된다. 대학은 대학수학능력시험 성적과 대학별 논술, 면접 고사 외에도 해당 학교와 전공을 선택하고 진학할 학생들에 대한 전인격적 발달에 대한 정보를 학교생활기록부를 통해 얻고자 한다. 대학은 학교생활기록부를 통해 학생의 ‘교과학습발달상황, 수상경력, 창의적 체험활동상황’ 등을 통해 학생의 소질과 적성에 따른 경험 및 활동을 파악하고 평가할 수 있고, 해당 전공에 대한 관심도와 기초 소양능력을 판단 할 수 있다.

이로 인해 고등학교에서 상급학교 진학 자료로서의 학교생활기록부는 매우 중요한 문서이다<sup>8,10)</sup>.

## III. 블록체인 기술 적용 방안

### 3.1 학교생활기록부를 위한 블록체인 유형 제안

블록체인 기술은 비즈니스 목적에 따라 서로 다른 기술들로 구현되며 퍼블릭(Public) 블록체인과 허가형(Permissioned) 블록체인으로 나누어진다<sup>12)</sup>. 퍼블릭 블록체인은 비트코인이나 이더리움 같이 누구나 블록체인 네트워크에 참여할 수 있는 유형이며, 허가형 블록체인은 허가된 기관만이 블록체인 네트워크에 참여할 수 있다<sup>2)</sup>. 블록체인의 대표적인 플랫폼 세 가지를 비교하면 표 1과 같다<sup>2)</sup>.

나이스와 학교생활기록부는 개인정보 중에서도 가장 민감한 정보인 학생의 데이터를 다룬다는 점에서 공개형 블록체인보다는 인증 받은 사용자만 참여할 수 있는 허가형 블록체인의 사용이 보다 적합하다.

학생의 생활기록사항은 학교생활, 진학, 진로 등 활용분야가 광범위하여 확장성이 중요하다. 확장성은 트랜잭션 수가 증가할 때 이를 무리 없이 처리할 수 있는지의 여부를 결정하는 속성이다. 확장성 측면에서 퍼블릭 블록체인 유형은 블록의 크기 제한(비트코인 1MB)이나 블록 당 수용할 수 있는 가스의 총량 제한(약 800만 가스) 때문에 많은 트랜잭션을 수용할 수 없다<sup>12-14)</sup>. 하이퍼레저 패브릭의 경우 이러한 제한이

표 1. 블록체인 비교  
Table 1. Comparison of blockchains

Division	public blockchain		permissioned blockchain (Hyperledger Fabric)
	Bitcoin	Ethereum	
Network	public blockchain	public, permissioned blockchain	permissioned blockchain
Coin	Bitcoin	Eth	Not existence (Coin can be implement as chain code)
Consensus Algorithm	PoW	PoW, PoS	SOLO, Kafka, PBFT, Raft
Finality	10 Minutes, 6 confirmations	15 Sec, 25 confirmation	Block creation time
Scalability	Not good (Block size limited to 1MB)	Not good (Gas limited to 8M)	good (parallel computation)
Smart Contract	Limited	EVM	Chain code
	Bitcoin script	Solidity, Serpent, LLL	Golang, Java, Node.js

적어 타 블록체인 네트워크에 비해 많은 트랜잭션을 포함할 수 있다<sup>2)</sup>.

또한 하이퍼레저 패브릭은 노드를 그 역할에 따라 구분(보증피어, 커밋피어)하고 일부 노드에서만 트랜잭션 검증 작업을 수행할 수 있으므로 병렬성을 증가시켜 처리 속도 향상에 유리하다<sup>2,3,5,7)</sup>.

학생의 기록은 담당교사에 의해서만 기록되어 기록자의 신원에 대한 확인만 필요하므로 복잡한 합의 알고리즘을 쓸 필요가 없어 하이퍼레저 패브릭의 Raft 합의 알고리즘을 채택하면 된다. 따라서 학교생활기록부는 하이퍼레저 패브릭을 기반을 선택하여 제안한다.

### 3.2 학교생활기록부 모델 설계

블록체인 기반의 학교생활기록부 작성 및 관리는 4세대 나이스의 ISP방형<sup>10,11)</sup>을 기본으로 설계하고자 한다. 나이스의 플랫폼을 중심으로 각 참여자 그룹은 교육부, 시도교육청, 한국교육학술정보원, 각 급 학교 그리고 사용자로 구분할 수 있고 나이스 클라우드 저장소를 중심으로 운영이 예상된다.

각 참여자 그룹별로 노드(피어)를 둘 수 있으며 체인코드와 분산원장을 관리한다. 클라우드 저장소는 학생기록 사항을 저장 및 공유하기 위한 데이터 저장소로 사용된다. 이를 하이퍼레저 패브릭 기반의 네트워크 형태로 나타내면 그림 1과 같다.

그림에서는 그룹별로 하나의 피어노드만 표시했으나 실제 그룹에는 다수의 노드가 존재하며, 역할에 따라 보증 또는 커밋 노드가 될 수 있다. 네트워크를 구성하고 있는 노드, 채널, 오더러의 역할은 다음과 같다.

#### 3.2.1 Peer(node)

각 참여자들은 해당 DApp(Distributed Application)을 통해 블록체인 네트워크의 노드들과 통신한다. 노드는 분산원장과 체인코드를 관리하는 개체로 역할에 따라 보증(Endorser) 또는 커밋(Committer) 노드로 동작한다. 체인코드를 실행하고 결과 값을 반환하는 역

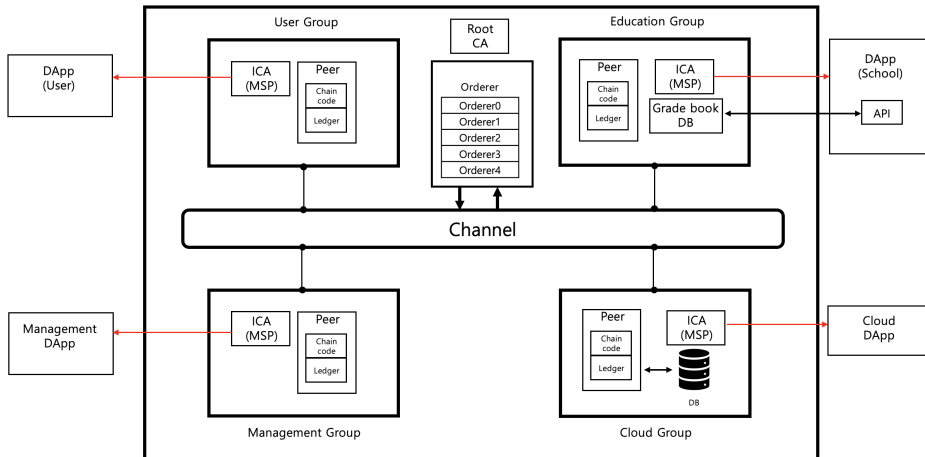


그림 1. 블록체인기반 학교생활기록부 프레임워크  
Fig. 1. Blockchain-based Student's School Record Book System Framework

할을 하는 노드를 보증 노드라 하며, 블록을 받아 결과 값과 인증서를 검증하는 역할을 하는 노드를 커밋 노드라 한다. 노드와 직·간접적으로 연관성을 갖는 참여자 그룹에 대한 설명은 다음과 같다.

- (1) 참여자 그룹 : 본 논문에서 참여자 그룹은 사용자 그룹, 교육행정기관 그룹, 총괄운영기관 그룹이 있다. 이외에도 연동하는 다양한 그룹이 존재하나 이 논문 범위에서는 학교생활기록부와 직접관련이 있는 그룹으로 한정하고자 한다.
  - a. 사용자 : 사용자 그룹은 학교생활기록부를 활용하는 교사, 학생, 학부모가 있고 이들은 인가된 범위에서 작성, 전송 또는 조회를 허가한다.
  - b. 교육기관 : 교육부, 17개 교육청, 학교 등 학교생활기록부를 생성, 저장 및 관리하는 역할을 담당한다.
  - c. 총괄운영기관 : 학교생활기록부 네트워크의 기술적 운영 전반을 담당하는 전문기관으로 한국교육학술정보원이 있다.
  - d. 클라우드 저장소 : 학교생활기록부의 전반적인 데이터를 저장·관리하는 저장소로 교육부의 저장소 또는 각 시도교육청의 저장소가 될 수 있다.

(2) DApp

각 참여자들은 해당 DApp, 즉 사용자 DApp, 교육기관 DApp, 총괄운영기관 DApp, 클라우드 DApp 등을 이용하여 블록체인 네트워크에 연결된다. DApp은 프라이빗 키를 가진 지갑역할을 수행하며, 참여자가

블록체인 네트워크에 액세스 할 수 있도록 인터페이스 역할을 수행한다. 교육행정기관 DApp은 각 행정기관과 상호 연계를 위한 API를 제공해야 하며 블록체인과 클라우드 저장소에 사용자의 데이터를 전송하는 역할을 수행한다. 사용자 DApp 기능으로는 사용자와의 인터페이스를 통해 동작하는 프론트엔드 기능, 다른 DApp과 상호작용하거나 내부적으로 지원되어야 하는 백그라운드 기능 등을 가질 수 있다. 프론트엔드의 주요 기능은 학생정보 조회, 학생정보 요청, 학생정보 기록 등 이다.

(3) 분산원장

하이퍼레저 페브릭의 분산원장은 현재 상태를 저장하는 World State와 원장의 생성 시점부터 현재까지 트랜잭션들의 이력을 저장하는 분산원장 등 두 가지로 구분할 수 있다. 그림 2는 본 논문의 블록 구조 및 트랜잭션 구조를 나타내며, 블록의 헤더를 구성하는 각 항목에 대한 설명은 표 2와 같다.

블록의 헤더와 메타데이터는 일반적으로 하이퍼레저 페브릭에서 제공하는 구조 사용하였고, 블록의 데이터 부분에 해당하는 트랜잭션은 그림 2와 같다.

트랜잭션은 헤더(Header)와 바디(Body) 두 부분으로 구성되는데 바디는 가변형으로 트랜잭션 항목에 따라 서로 다른 내용을 갖고 있다. 아래의 표 2는 트랜잭션의 헤더 항목과 서명에 대한 설명이다.

트랜잭션 유형에 따른 트랜잭션명과 그 내용은 아래 표 3의 예시와 같이 구성할 수 있다.

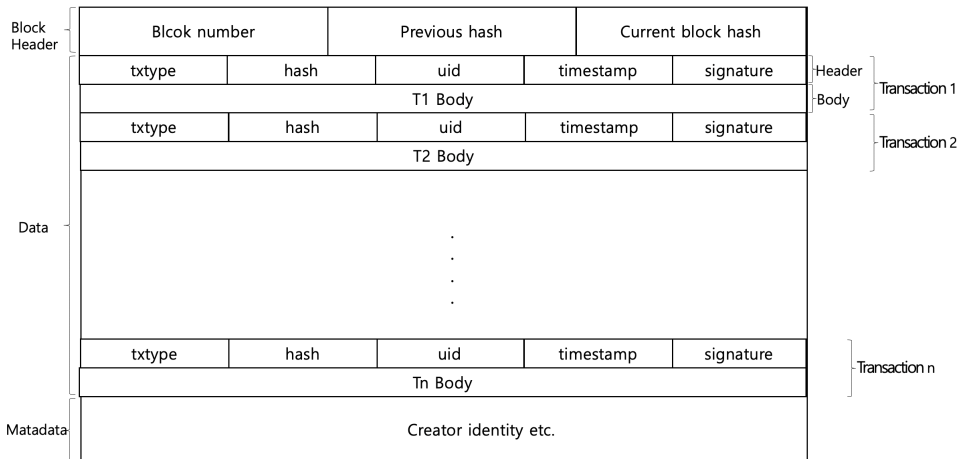


그림 2. 블록 구조 및 트랜잭션 구조  
Fig. 2. Block Structure and Transaction Structure

표 2. 트랜잭션 항목의 내용  
Table 2. Transaction Contents

Unit	Meaning
txtype	type of transaction Body content depends on txtype
uid	user ID
timestamp	transaction generating time
hash(=txid)	hash value of body
signature	signature of body except signature itself. Signature generated by transaction creator

표 3. 트랜잭션 타입에 따른 바디기록 사항  
Table 3. Body Contents by Transaction Type

txtype	transaction name	contents
0000	personal information	name, parent name, address etc.
0001	school register	change school register
0010	attendance	a record of student attendance
...	....	....

(4) 체인코드

체인코드는 분산원장에 학생의 기록사항과 변동기록 사항 등의 이력으로 남기는 기능을 갖는다. 보증노드는 트랜잭션의 txtype을 확인하고 해당 체인코드를 실행한다.

그림 3에서 인적사항 생성 체인코드는 학교에서 생성한 학생기본인적 트랜잭션, 학적기록 생성 체인코드는 학교에서 생성한 학적기록 트랜잭션에 대해 본인 또는 권한이 있는 관리자가 승인한 경우에만 원장에 저장하는 알고리즘이다. 자기정보결정권을 강화한다는 측면에서는 본인이나 보호자의 동의절차를 반영할 수 있다.

이와 같이 txtype에 따라서 해당하는 학교생활기록부의 각 항목별 데이터의 특성을 반영한 체인코드 알고리즘을 구현하여 트랜잭션을 처리하게 된다. 체인코드는 확인, 서명, 검증, 입출력 등 트랜잭션의 안전

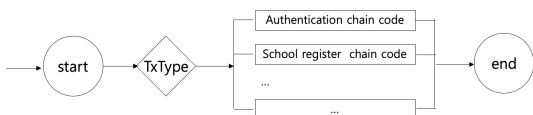


그림 3. 보증노드에서 트랜잭션 처리 흐름  
Fig. 3. Transaction Processing at Endorse Node

성, 정확성, 정합성 등을 보장할 수 있도록 구현할 수 있다.

3.2.2 채널(Channel)과 오더러(Orderer)

제안하는 학교생활기록부 프레임워크는 하나의 채널을 통해 분산원장을 공유한다. 채널에는 각 참여자 그룹 내의 노드들이 연결되어 있으며 채널을 통해 트랜잭션 및 블록들이 상호 간 전달된다. 특별한 기능을 하는 그룹이 필요하다면 그에 적합한 채널을 추가할 수 있다.

오더러는 트랜잭션을 시간 순으로 정렬하고 블록을 만들어 네트워크 내의 모든 노드들에게 전달하는 기능을 수행한다.

채널과 오더러의 역할을 트랜잭션의 처리절차를 통해 살펴보면 그림 4와 같다. 사용자가 DApp을 이용하여 블록체인 네트워크에 학생부 트랜잭션을 전송하고자 한다. DApp은 보증노드와 연결을 설정하고 노드는 학생부 체인코드를 실행한다. 보증노드는 학생부 트랜잭션을 전송하고자 하는 기기가 등록된 디바이스인지, 사용자는 정당한 권한을 가진 사용자인지 확인한 후, 결과 값과 자신의 서명 값 그리고 자신의 디지털 인증서를 사용자 DApp에 반환한다.

사용자 DApp은 보증노드로부터 받은 트랜잭션 결과 값, 보증노드의 서명 값, 보증노드의 디지털 인증서를 채널을 통해 오더러로 전송하고 오더러는 자신이 속한 네트워크에서 발생한 모든 트랜잭션을 수신하여 순서에 맞게 정렬하고 블록을 생성한다. 생성된 블록은 채널에 속한 모든 노드(커밋 노드)에게 전달된다. 커밋 노드들은 해당 블록의 모든 트랜잭션에 대한 결과 값, 보증노드 서명 값, 인증서를 검증하는 작업을 수행하고 문제가 없는 경우 자신의 로컬저장소에 저장된 분산원장을 업데이트하며 업데이트 결과를 사용자 DApp에 알려 준다.

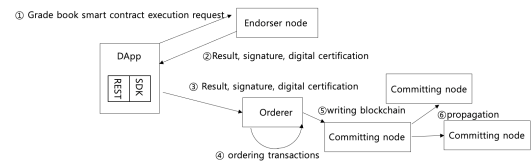


그림 4. 오더러 중심의 트랜잭션 처리 과정  
Fig. 4. Transaction Processing with Orderer

IV. 학교생활기록부 모델의 동작

블록체인 기반의 학교생활기록부 프레임워크는 사

용자 등록, 학생부의 생성, 전학 또는 상급학교 진학을 지원하는 변동사항의 기록, 학생부의 조회 등 그에 따르는 처리절차가 정의되어 있다. 다만 다음 몇 가지 전제 조건을 가지고 출발한다면 키는 안전하게 보관 및 사용되고, 데이터의 전송은 표준을 따르며 사용자와 교육행정기관은 표준화된 암호화 알고리즘을 채택하여 사용해야 한다. 일반적으로 하이퍼레저 패브릭의 데이터처리 과정은 Execute, Order, Validation 등 3 단계를 거쳐 처리된다.

본 논문에서 사용하는 학생정보는 학교에서 생성되는 학교생활기록부에 기록되는 정보에 한정한다. 이 정보들은 소속 시도교육청과 총괄센터 클라우드에 대칭키를 이용하여 암호화 되며, 클라우드로 전송할 정보의 암호화를 위해 학교는 대칭키를 이용하여 복호화키와 암호화키를 생성한다.

학생부 생성의 예 중 학적변동 사항을 살펴보자.

- 단계 1 그림 5와 같이 교사는 학생의 학적변동 사항을 기록하여 학생부에 저장한다. 학교 DApp은 나이스(NEIS) 시스템을 모니터링 하며, 저장 이벤트 발생 시 해당 내용을 복사하여 표준 형식으로 변환하고 변환된 데이터를 클라우드 전송용 암호화키로 암호화한다.
- 단계 2. 학교 DApp은 학생 등 사용자 DApp에 txid를 포함한 알람을 전송하여 자신의 기록내역을 확인하게 할 수 있다.
- 단계 3. 사용자 DApp은 사용자의 고유식별자를 MSP로부터 받은 다중벡터 값과 해시하여 새로운 식별자를 생성하고 이를 학교와의 공개

키와 비밀키를 이용해 암호화한 후 학교에 전송한다.

- 단계 4. 학교 DApp은 새로운 식별자를 포함하는 학적사항 트랜잭션을 생성하여 블록체인에 전송한다.
- 단계 5. 사용자 DApp은 자신의 학적내역을 확인 후 학적사항 확인 트랜잭션을 블록체인에 전송한다.
- 단계 6. 블록체인의 보증노드는 학적기록 트랜잭션과 학적기록 확인 트랜잭션을 비교하여 두 값이 일치 하는 경우, 결과 값과 자신의 서명을 추가하여 학교 DApp에 응답한다.
- 단계 7. 이후 학적사항 트랜잭션은 분산원장에 기록된다.
- 단계 8. 학교 DApp은 암호화된 표준형식의 학적변동 데이터를 클라우드 저장소에 저장한다.

클라우드 저장소로 전송되는 학적 데이터는 헤더와 바디로 구성되며 헤더는 클라우드 관리자의 공개키로, 바디는 사용자와 학교 간 대칭키를 통해 생성된 암호키로 암호화되어 전송된다. 학적 데이터의 경우 헤더는 사용자 식별자(학번 등 User\_ID), 주민번호, 날짜(Date) 등 학적기록에 대한 메타데이터가 포함되고 바디에는 실제 학적데이터가 기록된다.

클라우드는 학적데이터를 받으면 헤더를 자신의 개인키로 복호화하고 바디에는 파일번호(Encrypted FileNo.)를 할당하여 별도로 관리한다.

본 논문에서는 하이퍼레저 패브릭을 중심으로 블록체인을 활용한 학교생활기록부의 기록 및 관리의 기본 흐름을 중심으로 설계했다. 블록체인은 사회적으로 매우 민감한 정보를 생성, 관리하는 데 신뢰성을 확보할 수 있는 가장 최신의 방법이다. 향후 추가 연구 등을 통하여 학교생활기록부 전반의 기록관리를 블록체인 기반 체계로 상세하기 설계하고 구현해 볼 수있다.

또한 각종 증명서, 봉사활동 등 학생활동기록 등도 블록체인 기반으로 설계한다면 교육정보 전반에 대한 신뢰성이 높아질 것이다.

이번 제안 모델이 구현된다면 학교생활기록부의 기술적 위변조를 원천 차단하여 대학입학 등 상급학교 진학을 둘러싼 학교생활기록부의 신뢰성 논란은 획기적으로 개선될 것으로 기대된다.

## V. 결 론

최근 4차 산업혁명 기술을 활용한 정보서비스로 이

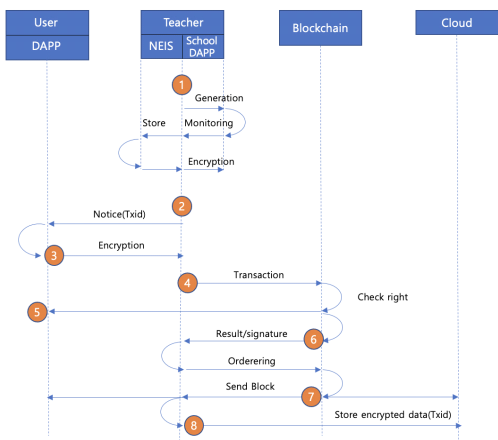


그림 5. 학생부 학적 변동사항 처리 절차  
Fig. 5. School register processing

용자의 편리성을 확대하고 미래의 상황을 예측하는 등 새로운 가치 창출 시스템이 등장하고 있다. 빅데이터, 인공지능, 블록체인 기술은 우리산업의 패러다임을 바꾸고 있으며 교육 분야도 예외가 될 수 없다.

블록체인은 분산 데이터베이스의 한 형태로 처리 정보를 여러 컴퓨터에 저장 및 보관하는 기술로 고도의 신뢰를 요구하는 다양한 분야에 적용이 가능하다. 특히 나이스는 학교생활기록부를 관리하는 시스템으로 신뢰에 대한 이슈가 끊임없이 제기되고 있다.

따라서 블록체인은 학교생활기록부 변조를 원천적으로 방지할 수 있다, 따라서 학교생활기록부에 대한 블록체인 적용 모델 설계 및 구현이 필요하다. 이번 연구에서는 교육분야인 학교생활기록부에 블록체인을 적용하는 기본 모델 설계를 제안하였다

이 모델 설계는 응용시스템에서 많이 사용하는 하이퍼레저 페브릭을 사용하였고, 학교생활기록부에 대한 블록의 구조, 블록의 생성과 트랜잭션을 저장하는 과정을 제시하고 인증과 권한 관리에 대하여 기술하였다.

블록체인기반의 학교생활부 작성 및 관리방안을 제안함으로써 대학입시 등에서 사용하는 학생부의 신뢰성 제고를 기대할 수 있다.

이번 연구의 제안을 4세대 나이스 추진에 반영한다면 학교생활기록부의 기술적 위변조를 원천 차단함으로써 교육의 신뢰를 높이는 데 크게 기여할 것이다.

## References

- [1] A. Tapscott and D. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*, Eulyoo Publishing, 2018.
- [2] J. Bong, "A personal health information sharing platform based on hyperledger fabric blockchain," Ph.D. Dissertation, Soongsil University Graduate School, 2019.
- [3] E. Androulaki, et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *EuroSys '18*, pp. 1-15, Porto, Portugal, Apr. 2018.
- [4] S. W. Jung, "HyperCerts : Privacy-Enhanced OTP-Based educational certificate blockchian system," *J. KIISC*, vol. 28, no. 4, pp. 987-997, Aug. 2018.
- [5] Y. Jang, J. Kim, and Y. Cho, "Proposal of military career certificate issuing system based on hyperledger fabric platform," in *Proc. KIISE*, pp. 48-50, Dec. 2019.
- [6] H. Kim and N. Park, "Design and implementation of blockchain for securing data of national education information system school life records," *J. Korea Convergence Soc.*, vol. 11, no. 3, pp. 27-35, 2020.
- [7] J. Y. Chung and C. S. Lee, "Theoretical approach to blockchain-based real estate transaction system. - focus on hyperledger fabric method," *Korea Real Estate Academy Rev.*, vol. 81, pp. 21-35, 2020.
- [8] H. Lee, "Data visualization of the student's cumulative record using text mining approach," M.S. Thesis, Ewha Womens University The Graduate School of Education, 2019.
- [9] J. Lee, "A study on the certificate issuing system of education based on blockchain," M.S. Thesis, Dongguk University Graduate School of International Affairs and Information Security, 2020.
- [10] *Current status of NEIS's school record book*, MOE, 2019.
- [11] <http://www.neis.go.kr>. Retrieved Jul. 25, 2021
- [12] <https://www.ibm.com/kr-ko/blockchain/hyperledger>. Retrieved Jul. 25, 2021
- [13] <http://www.hyperledger.org>. Retrieved Jul. 25, 2021
- [14] <http://github.com/hyperledger/fabric>. Retrieved Jul. 25, 2021.



정 승 욱 (Seung Wook Jung)



2000년 2월 : 숭실대학교 전자공학 석사

2005년 12월 : University of Siegen 정보보호 공학박사

2006년~2011년 : 한국인터넷진흥원 책임연구원

2011년~2017년 : 숭실대학교 정

보통신전자공학부 조교수

2017년~현재 : 건양대학교 사이버보안학과 조교수

<관심분야> 정보보호, 블록체인, 개인정보보호

[ORCID:0000-0002-1635-6218]

김 두 연 (Dooyeon Kim)



2007년 2월 : 숭실대학교 대학원 소프트웨어공학 공학박사

1988년2월 : 숭실대학교 공학석사

2003년~2012년 : 교육부 교육정보화과장

2012년 4월~현재 : 건양대학교 융합IT학과 교수

<관심분야> 소프트웨어공학, 빅데이터, 스마트교육

[ORCID:10363110]