



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

석사학위논문

블록체인을 이용한 학교생활기록부
신뢰성 확보 방안

The Method for Securing Reliability of
Students' Records Using Blockchain

제주대학교 대학원

융합정보보안학협동과정

김 희 경

2020년 8월

블록체인을 이용한 학교생활기록부 신뢰성 확보 방안

지도교수 박 남 제

김 희 경

이 논문을 융합정보보안학협동과정 석사학위
논문으로 제출함

2020년 6월

김희경의 융합정보보안학협동과정 석사학위
논문을 인준함

심사위원장 변 영 철 ①

위 원 조 정 원 ①

위 원 박 남 제 ①

제주대학교 대학원

2020년 6월

목 차

목 차	i
표 목 차	iii
그림목차	v
요 약	vii
I. 서 론	1
1. 연구의 배경 및 목적	1
2. 연구의 범위와 절차	3
II. 이론적 배경	5
1. 교육행정정보시스템	5
2. 학교생활기록부	15
3. 블록체인	22
III. 학교생활기록부 관련 최근 동향 연구	34
1. 학교생활기록부 보안관리체계 강화 방안	34
2. 학교생활기록부 대입전형자료 온라인 제공	38
3. 졸업생 학교생활기록부 이관	39
4. 4세대 나이스 블록체인구현 제안사항	41

IV. 학교생활기록부 보안관리 문제점 및 개선방안	43
1. 학교생활기록부 보안관리 문제점	44
2. 학교생활기록부 보안관리 개선방안 및 고려사항	48
V. 학교생활기록부 블록체인 구현 방안	56
1. 학교생활기록부 블록체인 제안	56
2. 학교생활기록부 블록체인 네트워크 구성	61
3. 학교생활기록부 블록체인 트랜잭션 합의 과정	68
4. 학교생활기록부 블록체인 PDC 적용	76
5. 4세대 나이스 블록체인 제안과의 비교	79
6. 현재 나이스 보안강화체계와의 비교	80
7. 기대효과	81
VI. 결 론	83
참고문헌	87

표 목 차

[표 I-1] 연구 절차	4
[표 II-1] 학교정보관리시스템과 교육행정정보시스템 비교	8
[표 II-2] 교무업무시스템 3가지 영역	9
[표 II-3] 기존 나이스와 차세대 나이스 개선사항 비교	11
[표 II-4] 교육행정정보시스템 운영업무	11
[표 II-5] 나이스 7단계 보안체계	14
[표 II-6] 학교생활기록부 영역 및 입력 가능 최대 글자 수	15
[표 II-7] 퍼블릭 블록체인과 프라이빗 블록체인 비교	30
[표 II-8] 블록체인 활용분야	30
[표 II-9] 국내와 국외에서의 블록체인 활용분야별 사례	31
[표 III-1] 졸업생 학교생활기록부 단계적 이관 계획	39
[표 III-2] 학년도별·학교급별 졸업생 현황	40
[표 IV-1] 1인 교사가 성적 기록 시 연간 접속횟수 및 시간 예측	44
[표 IV-2] 연간 교무업무 및 학교생활기록부 수정이력 DB 사용량 예시	45
[표 IV-3] 고등학교에서의 대입전형자료 관리 현황	46
[표 IV-4] 대입전형자료 온라인 제공 건수	47
[표 IV-5] 이더리움과 하이퍼레저 패블릭 비교	49
[표 IV-6] 블록체인 기술적용 결과 현행시스템과 비교 시 상대적 단점	54
[표 V-1] 참여차별 역할 및 체인코드	62
[표 V-2] 체인코드 기능	62
[표 V-3] 용어 정리	65
[표 V-4] 하이퍼레저 패블릭 블록체인 개발환경 및 도구	67

[표 V-5] 4세대 나이스와 본 연구 제안과의 비교 79
[표 V-6] 현재 보안강화방안과 본 연구 제안과의 비교 80

그림 목 차

[그림 II-1] 교육행정정보시스템 구성도	12
[그림 II-2] 4세대 교육행정정보시스템 구성안	13
[그림 II-3] 블록체인의 특징	23
[그림 II-4] 중앙시스템과 블록체인 분산원장	24
[그림 II-5] 블록체인 블록 구조	24
[그림 II-6] 블록체인 스마트 컨트랙트	25
[그림 II-7] 따복공동체 전자투표	32
[그림 II-8] 블록체인 기술 적용한 사용자간 전력거래 구상도	33
[그림 III-1] 학교생활기록부 권한관리 개선	34
[그림 III-2] 학교생활기록부 권한관리 모니터링 화면	35
[그림 III-3] 학교생활기록부 접근 시 2차 인증 절차 체계도	36
[그림 III-4] 수정이력 관리 화면 예시	37
[그림 III-5] 학교생활기록부 이력 보존 시스템 구성도	37
[그림 III-6] 대입전형자료 온라인 제공 구성도	38
[그림 III-7] 졸업생 학교생활기록의 보존·활용시스템 개념도	40
[그림 III-8] 3세대와 4세대 나이스 업무 비교	41
[그림 III-9] 4세대 나이스 블록체인 구현 예상도	42
[그림 III-10] 4세대 나이스 블록체인 구현 방안	42
[그림 IV-1] 교육행정정보시스템 학교생활기록부 블록체인 구성도	51
[그림 IV-2] 중앙집중형 시스템과 분산형 시스템 비교	52
[그림 V-1] 두 종류의 블록데이터	56
[그림 V-2] 학교생활기록부 블록체인 네트워크 메커니즘	57

[그림 V-3] 학교생활기록부 블록구조	58
[그림 V-4] 블록 헤더 구조도	59
[그림 V-5] 블록 트랜잭션 구조	59
[그림 V-6] 학교생활기록부 블록체인 네트워크 참여자 및 권한	61
[그림 V-7] 학교생활기록부 네트워크 구성 모델의 개념적 구조도	63
[그림 V-8] 하이퍼레저 패브릭 기반 트랜잭션 처리과정 노드	68
[그림 V-9] 읽기 체인코드 실행과정	70
[그림 V-10] 쓰기 체인코드 실행과정	71
[그림 V-11] 쓰기 트랜잭션 합의 전체 과정	73
[그림 V-12] 읽기 트랜잭션 합의 전체 과정	75
[그림 V-13] Authorized Peer와 일반 Peer 원장 구조 비교	76
[그림 V-14] PDC 기능 적용한 학교생활기록부 블록체인 네트워크	77
[그림 V-15] 체인코드 기반의 데이터의 효율적인 관리 방안	78

요 약

본 연구의 목적은 시·도교육청에서 공통적으로 사용하고 있는 교육행정정보시스템 내에 학교생활기록부가 학생이 초등학교에서 고등학교까지의 학교생활 전반에 대한 교육활동과 함께 개인의 성장과정이 매우 세밀하게 기록되어 있는 중요한 개인 정보이며 교육활동 결과물로서 안정적으로 보호되어야 하므로 현행시스템 기술방식보다 더 보안성이 강화된 기술 적용방식에 대한 연구의 필요성에 의해 블록체인 기술구현 방법을 제안하는 것이다.

교육행정정보시스템은 일반행정, 교무업무, 학교행정 등 전 교육행정업무를 교육청과 각급 학교에서 자체 운영 및 교육부와 대학 등에 전자적으로 연계 처리할 수 있도록 2002년 11월에 초기 구축을 시작으로 2006년과 2010년에 두 차례 개편하여 현재까지 운영되고 있으며, 교육부와 시·도교육청에서는 2022년에 4세대 시스템 개편을 목표로 준비하고 있다.

교육행정정보시스템은 교육행정의 효율성과 대국민 서비스를 향상시키는 등의 성과를 거두고 있으나, 일부 학교에서 관련 규정을 어기고 중요한 데이터인 학교생활기록부 내용을 부당하게 정정하는 사건이 간헐적으로 발생하고 있어 위·변조와 불법 유출의 위험성이 내포되어 있다.

이러한 교육행정정보시스템의 문제점을 개선하고 학교생활기록부 데이터의 신뢰성을 확보하기 위해 본 논문에서는 허가된 조직과 개인만이 참여할 수 있는 Private 블록체인을 적용하여 허가받지 않은 자에 의한 블록네트워크 참여를 방지하고, 내부자에 의한 위변조를 방지할 수 있는 방안을 연구하였다.

오픈소스인 하이퍼레저 패브릭 블록체인 기술을 기반으로 두 종류의 블록 데이터(학교생활기록부 학생정보 블록과 접근기록 블록)를 생성하여 허가된 권한을 받은 참여자에 의해서만 등록, 수정, 열람할 수 있는 블록 메커니즘을 제시하였다.

2018년 숙명여고 시험지 유출사건 및 학교생활기록부 조작 등의 일련의 사건으로 인해 교육기관에서는 학교생활기록부 권한체계 강화, 2차 인증 도입, 학교생활기록부 수정이력 저장 등으로 교육행정정보시스템 보안체계를 강화하고 있으나, 이는 근본적인 해결방안이라기엔 부족한 점이 있다.

하이퍼레저 패브릭 블록체인 기술기반 프라이빗 블록체인 네트워크를 구현함으로써 인증센터(Fabric-CA)를 통해 인증받은 참여자만 네트워크에 참여할 수 있다.

비트코인이나 이더리움은 블록네트워크에 모든 노드들이 데이터를 공유하나, 하이퍼레저 패브릭에서는 데이터 공유가 허용된 조직끼리만 채널을 구성할 수 있어 다수의 블록네트워크를 구현하여 채널별로 독립적인 블록체인을 유지할 수 있다. 또한 PDC(Private Data Collection) 기능을 적용함으로써 동일 채널내에서도 인가받은 조직만 암호화된 프라이빗데이터 원본을 공유할 수 있다.

이러한 하이퍼레저 패브릭 블록체인 기술을 적용한 블록체인 네트워크 구현시 블록네트워크 CA에 의한 권한인증 검증이 가능하므로 사람에 의한 2차인증을 하는 불편함을 해소할 수 있으며, 블록네트워크로 데이터를 관리함으로써 수정이력을 저장하는 관리상의 번거로움을 해결할 수 있다.

본 연구를 통해 제3자에 의한 생활기록부의 위·변조방지과 부인방지, 접근통제를 확보할 수 있는 방안을 마련하였으며, 실제 학교생활기록부 시스템에 적용하게 된다면 학교생활기록부 운영과 관리에 대한 사회적 신뢰형성이 향상될 것으로 기대한다.

주제어 : 교육행정정보시스템, 학교생활기록부, 블록체인, 하이퍼레저 패브릭, 프라이빗 블록체인, 학생기록블록, 접근데이터 블록, 데이터 암호화

I. 서 론

1. 연구의 배경 및 목적

2009년 비트코인으로 등장한 블록체인은 기술 발전이 가속화되면서 여러 가지 비즈니스 모델이 개발되고 있다. 블록체인은 절차 간소화, 비용절감은 물론 우리의 일하는 방식까지 혁신하여 사회편익을 높이는 성장잠재력이 높은 기술이다.

블록체인기술의 장점은 데이터 위변조 방지가 장점이며, 다양한 산업과 결합하여 효율성을 높이고 새로운 경제적 가치 창출이 가능하다[1].

이러한 데이터 위변조 방지가 큰 장점인 블록체인 기술은 준영구 보존해야하는 중요자료인 학생 학교생활기록부 데이터 관리시스템인 교육행정정보시스템(NEIS: National Education Information System, 나이스)에 적합한 지 연구가 필요하다.

전국 시·도교육청과 각급학교에서 사용하고 있는 교육행정정보시스템은 일반행정, 교무업무, 학교행정, 대국민서비스 등 전 교육행정업무를 자체 운영 및 교육부와 대학 등에 전자적으로 연계 처리할 수 있도록 함으로써 교육행정의 효율성과 대국민 서비스를 향상하기 위해 2002년 11월에 초기 구축으로 서비스를 시작하였다. 그 이후 교무/학사 등 3개 영역을 지원하기 위한 2세대 교육행정정보시스템으로 개편하였으며, 2010년에는 Green IT 개념을 도입하고 노후화된 장비를 교체, 부처간 정보시스템을 연계하는 차세대 교육행정정보시스템(3세대)를 구축하여 2020년 현재까지 운영하고 있다[24]. 이 시스템은 4개시스템, 44개 단위업무, 268개 세부업무로 구성되고, 대국민서비스는 학생 46종, 학부모 59종, 홈에듀 민원 18종을 제공하고 있으며, 사용기관은 초·중등학교(11,600여개), 교육행정기관(교육부, 17개 시·도교육청, 176개 교육지원청), 대학·전문대학(400여개) 등이다. 사용자는 교직원 약 55만 명, 학생 545만 명, 학부모 등이 사용하고 있다 [3].

교육행정정보시스템은 그동안 교육(행정)기관의 업무 효율성을 제고하고, 온라인 민원서비스를 통해 대국민 편의를 제공하는 등의 성과를 거두고 있으나, 최근 미래지향 교육정책과 전자정부 정책에 적극적으로 대응하기 위해 대폭 개편이 필요한 시점으로 교육부와 17개 시·도교육청에서는 2022년 3월 개통을 목표로 개편을 준비하고 있다.

이 광범위한 단일시스템에서 중요한 데이터는 무엇보다 교무업무 중에서 학교생활기록부라고 할 수 있다.

학교생활기록부는 학생이 학교에 입학한 순간부터 재적하는 순간까지 학생의 전반적인 학교생활과 성장, 발달을 교사가 관찰하여 기록한 문서이다. 학교생활기록부는 공식 법적 문서이며, 학생의 학적에 대한 증명 자료적 성격, 교수·학습 지도 자료로 활용되는 지도 자료적 성격, 진학이나 취업을 위한 전형 자료적 성격을 가지고 있다.

학교생활기록부는 여러 항목을 통해 학생의 학교생활 전반에 대한 내용을 담고 있어 학교생활기록부를 보면 학생의 학업능력과 성격, 발달 정도 등의 특성을 총체적으로 이해할 수 있다. 또한 학교생활기록부는 학생과 학부모, 교사, 교육행정기관, 상급학교에 제공되며 각각의 목적에 따라 활용된다.

이처럼 중요한 학교생활기록부가 성적조작, 유출, 위변조되거나, 훼손되는 등의 사고를 방지하기 위해서 현재 시스템에서 보안강화 방안으로 2차인증, 접근기록 관리강화, 생활기록부 수정이력 보관시스템 도입 등의 조치를 하고 있으나 이는 근본적인 해결이라 할 수 없다.

보다 획기적인 기술적 해결방안을 위해서 본 논문에서는 “신뢰의 인터넷”이라 불리며 4차 산업혁명의 핵심인 블록체인을 활용한 학교생활기록부 블록체인 시스템 도입방안을 제안하고자 한다.

2. 연구의 범위와 절차

본 연구는 전국 초·중·고·특수학교 학생의 학생생활과 성적 등의 정보가 수록된 학교생활기록부가 포함된 교육행정정보시스템에 대한 구축 경과와 최근 추진 사항에 대하여 고찰하고, 학교생활기록부의 내용과 중요도에 대하여 조사하며 현재 시스템에서의 학교생활기록부 보안관리방안에 대한 문제점과 개선방안을 도출한다.

또한, 최근 블록체인 기술동향과 특성을 분석하여 위·변조방지와 무결성확보를 위한 최적의 학교생활기록부 블록체인 시스템 구현에 대한 이론적 연구를 하고자 한다.

연구의 범위는 다음과 같다.

첫째, 학교생활기록부 블록체인 시스템 구현 방안 연구를 위해 교육행정정보시스템 구축 경과와 특성, 학교생활기록부 정의와 활용성, 블록체인 정의와 블록체인 종류, 공공기관에서의 적용사례와 같이 관련 이론적 배경을 조사한다.

둘째, 학교생활기록부 신뢰도 제고를 위한 최근 교육행정정보시스템에서의 보안관리 체계와 4세대 교육행정정보시스템에서 구현하고자 하는 블록체인 제안사항에 관하여 조사한다.

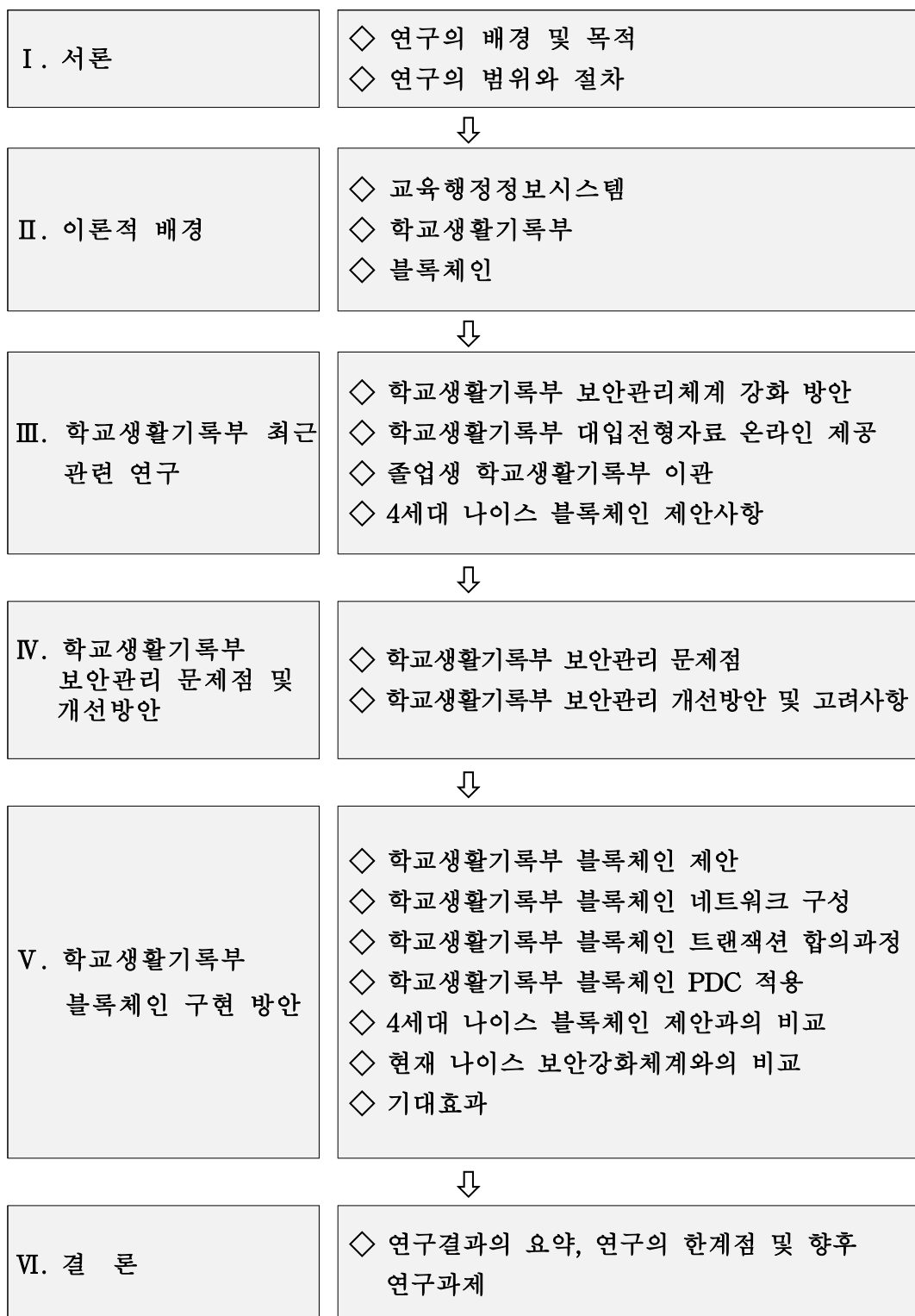
셋째, 학교생활기록부에서의 보안관리 문제점과 이를 해결하기 위한 최적의 개선방안으로서 하이퍼레저 패브릭 블록체인 기반 기술적용 방안을 연구한다.

넷째, 실제적인 하이퍼레저 패브릭 기반 학교생활기록부 블록체인 네트워크 구성형태와 트랜잭션 합의과정, 프라이빗 데이터(개인정보) 적용방안에 대한 연구를 통해 학교생활기록부 블록체인 구현 방안을 제안한다.

다섯째, 관련 연구와 제안하는 블록체인 메카니즘과 비교를 통해서 기대효과와 연구의 한계점, 향후 연구과제를 도출한다.

학교생활기록부 데이터 신뢰성 확보를 위한 하이퍼레저 패브릭 기반 학교생활기록부 블록체인 구현 연구를 위하여 수행된 절차는 [표 I-1]과 같다.

[표 I -1] 연구 절차



II. 이론적 배경

본 장에서는 학교생활기록부 블록체인 메커니즘 연구를 위한 이론적 배경을 고찰하고자 한다.

첫째, 먼저 학교생활기록부가 포함되어 있는 교육행정정보시스템에 대한 구축 배경과 구성 내용에 대하여 조사한다.

둘째, 본 주제의 핵심내용인 학교생활기록부 구성요소와 활용사항에 대하여 조사한다.

셋째, 마지막으로 구현하고자 하는 블록체인 기술에 대한 개념과 종류, 활용분야에 대하여 조사한다.

1. 교육행정정보시스템

1) 교육행정정보시스템 도입 배경 및 경과

먼저 1996년부터 본격적으로 추진되어 온 교육행정 정보화 지원서비스는 각급 학교 교원들이 순수 교육 활동 외에 반복적으로 처리해야 하는 교무/학사, 일반 행정업무 등을 경감하는 것을 목표로, 학교생활기록부를 전산화하는 것에서 출발하여 교무/학사 업무를 지원하기 위한 시스템이 우선적으로 개발되었으며, 그 후로 교육기관간 문서유통, 인사, 예산, 회계 등의 일반 행정 영역을 지원하는 시스템 개발이 뒤따랐다. 이러한 기능을 통합적으로 갖춘 최초의 프로그램이 1996년부터 개발·보급된 ‘학교정보관리시스템(SIMS: School Information Management System)’이다.

그러나 단위업무 중심의 개발로 인하여 업무처리 절차, 서식, 코드 등에 대한 표준이 제정되지 못하고, 시스템종류와 응용 소프트웨어가 통일되지 않아 정보의 공동 활용에 문제가 있다는 지적을 받아 왔다. 이에 전국 단위의 교육행정정보시

시스템을 구축하여 정보의 공동 활용을 지원해야 한다는 움직임이 생겨나기 시작했다.

이러한 이유로 교육인적자원부(현 교육부)에서는 전자정부 중점 추진과제이면서, 교육행정의 생산성 및 공유성을 극대화하고 국민에게 최적의 서비스를 제공하며 교육행정의 투명성을 높이기 위한 보다 종합적이고 체계적인 통합형 시스템이 필요함을 인지하여, 2001년 5월에 교육행정정보시스템 구축 사업을 추진하게 되었다[13].

교육행정정보시스템은 학교정보관리시스템의 보안, 상호 연계성 등의 문제점을 해결하고, 전 교육행정기관에서 이루어지는 업무를 유기적으로 처리할 수 있도록 전국 단위의 교육행정정보시스템인 나이스로 통합하여, 2002년 11월에 1세대 교육행정정보시스템이 탄생하였다.

그러나 나이스는 2003년 3월에 전면적 운영을 기획하였으나 개인정보의 수집·관리에 있어 인권문제가 대두되며 사회적 갈등이 발생하였다. 구체적으로 나이스 안에 포함된 교무/학사 등 3개 영역에 대해 사회단체가 인권침해 소지가 있음을 언급하였고, 국가인권위원회가 실제로 인권침해 요소가 있다고 판단함에 따라, 해당 영역에 대해서는 학교정보관리시스템이 사용되고, 일반 행정 지원을 위해서는 나이스가 활용되는 이원화 체제로 운영하게 된 것이다.

이에 교육정보화위원회는 교무/학사 등 3개 영역을 지원하기 위한 새로운 나이스에 대한 교육인적자원부(현 교육부)와 전교조 및 사회단체 간의 사회적 합의를 이끌기 위해 노력한 결과, 2005년 2월부터 이를 지원하기 위한 새로운 시스템이 개발되어, 2006년부터 교무/학사 등 3개 영역에 대한 독립된 교무업무시스템(신나이스 시스템)이 개발되어 2세대 교육행정정보시스템이 구축되었다. 교무업무시스템의 개통과 더불어, 2006년 학부모에게 학습자의 성적, 출결, 학교생활기록부 등의 학업 관련 정보를 알려주는 내 자녀 바로알기 서비스가 시작되었으며, 인터넷을 통해 자신의 컴퓨터에서 직접 제증명을 출력할 수 있고 정부 행정부처간 행정정보 공동이용으로 민원인이 제출해야 할 서류를 감축시켜주는 Home-Edu 민원서비스 운영도 시작되었다.

2010년에는 Green IT 개념을 도입하여 노후화된 장비를 교체, 부처 간 정보시스템을 연계하는 차세대 나이스를 구축하여 이 시기를 3세대 교육행정정보시스

템이라 할 수 있다. 이와 더불어 교원관련 무인민원발급서비스가 실시되어, 각종 증명서 발급이 한층 수월해졌으며, 나이스 연계를 통한 교육통계 조사가 시작되어, 교육 현황과 효과성 검증을 위해 활용되고 있다.

이와 같은 나이스 대국민서비스는 전환기에 들어서며 사용자 편의성을 최대화 하고 보안을 강화하기 위한 노력에 초점을 맞추었다. 또한, 2014년 2월에는 나이스가 교육부 소관 주요정보통신기반시설로 지정돼 국가 중요서비스와 동일한 보안 수준으로 운영되기 시작하였다. 이를 토대로 2015년 12월 나이스 중앙운영센터(한국교육학술정보원)는 정보보호관리체계(ISMS) 인증을 획득하게 된다[24].

이처럼 교육행정정보시스템은 2002년 1세대 개통이후 지속적으로 보완과 기능 개선 및 개편되면서 현재까지 운영되고 있다. 교육행정정보시스템의 1세대부터 3세대 개통까지의 세부현황과 2022년에 개통예정인 4세대 나이스 개통 계획에 대하여 살펴보고자 한다.

2) 1세대 교육행정정보시스템 (2002.11 ~ 2006. 2.)

1996년 말부터 개발·운영되어 오던 학교정보관리시스템은 데이터를 보관하는 서버가 일선 학교에 위치하고 있기 때문에 서버관리를 위한 교사의 업무 부담 발생과 보안에 대해 문제가 제기되어 왔다. 그리하여, 이의 대안으로 서버를 해당 시·도교육청으로 옮겨 관리의 편의를 꾀하고 전국의 학교와 교육청, 교육인적자원부(현 교육부)를 네트워크로 연결하여 전 교육행정업무를 전자적으로 연계처리할 수 있는 교육행정정보시스템의 개발이 추진되었다. 나이스는 학교정보관리시스템의 교무/학사 영역과 일반행정 영역이 통합된 체제로, 대국민 서비스를 가능하게 함으로써 행정정보서비스의 고도화를 실현하기 위한 목적에서 개발되었다.

교무/학사 지원 영역과 일반행정 지원 영역을 통합한 종합적인 교육행정정보 서비스를 제공하고, 교육행정정보시스템의 운영상 문제점을 해소하기 위해 중앙인터넷자문단을 운영하기 시작하고, 5단계 보안체제를 마련하였다.

[표 II-1]에서 교육행정정보시스템과 학교정보관리시스템과의 차이점을 보여준다.

[표 II-1] 학교정보관리시스템과 교육행정정보시스템 비교

구분	학교정보관리시스템	교육행정정보시스템
주요 업무	교무업무(학사, 교무행정)에 한정	교무, 학사, 인사, 회계, 물품, 시설 등 교육행정 전반
물리적 환경	학교 단위로 서버 설치, Client/ Server 환경에서 사용	시·도교육청에 서버 설치, 학교에서는 인터넷으로 이용
데이터 관리	학교별로 책임부여 및 관리	데이터는 시·도교육청 서버에 있으나, 데이터의 접근은 학교 사용자만 가능
데이터 공유, 활용 방법	학교 내에서만 운영되는 폐쇄형 시스템이므로, 데이터 취합하여 정보를 생성하는 것이 불가능	네트워크를 이용하는 시스템이므로, 온라인상에서 데이터 가공 및 생성 가능
대국민 서비스	실시간 서비스 불가능	실시간 서비스 가능

교육행정정보시스템이 제공하는 서비스는 크게 교무/학사 등의 학교행정 영역과 인사, 예산, 회계 등의 일반행정 영역으로 나뉜다. 각 서비스는 교육행정기관에 따라 운영 범위를 서로 달리 하였다. 학교행정영역에는 입(진)학, 교무/학사, 보건, 교구/기자재, 체육 5가지 단위업무가 있으며, 일반행정 영역에는 교원인사, 일반직인사, 급여, 예산, 회계, 학교회계, 장학, 시설, 재산, 평생교육, 민원, 검정고시, 감사, 재산등록, 법인, 기획, 홍보, 법인, 급식, 비상계획, 교육통계, 시스템관리 단위업무가 있다[24].

3) 2세대 교육행정정보시스템 (2006. 3. ~ 2009. 12.)

2006년 3월 교무업무 3개 영역을 대상으로 한 새로운 나이스 교무업무시스템이 개통되었다. 교무업무시스템은 교무·학사, 입학, 보건의 3개 영역으로 구성된 학교행정영역에 관한 시스템으로, 교육행정정보시스템의 영역에서 분리된 시스템이다.

새로운 나이스 교무업무시스템은 2003년 5월, 국가인권위원회의 권고사항을 받아들여 인권침해 소지가 있다고 판단한 항목들을 교육행정정보시스템에서 분리하여 새로운 시스템으로 구축한 것이다. 국가인권위원회의 권고를 반영하여 교육행정정보시스템에서 교무/학사, 입(진)학, 보건 세가지 영역이 분리되었다.

[표 II-2] 교무업무시스템 3가지 영역

구분	내용
교무/학사	학적 등 3개 하위영역 56개 항목
입(진)학	신입생 입학과 진학 관련 3개 항목
보건	학교보건관리 등 5개 하위영역 135개 항목

교무업무시스템 보호를 위해 침입차단 장치 등의 보안장비를 추가하고, 주민등록번호 등 신상정보를 암호화하여 학생정보 보안이 강화되었으며, 전자업무승인 기능을 도입함으로써 교사들의 실질적인 업무 부담을 줄어뜨리게 하여 교사들이 교수·학습 지도에 더 시간을 할애할 수 있도록 하였다.

교무업무시스템은 학교 급별 단독서버 또는 그룹서버로 분리하여, 학생 개인정보에 관련된 DB를 학교별로 구축하고 관리하며, 학교장이 DB에 대한 접근권한을 통제할 수 있도록 하였다. 시스템 설치와 물리적 관리는 각 시·도 교육청 정보시스템운영센터에 위임하여 일괄적으로 관리 및 운영할 수 있도록 하였다.

교무·학사 영역은 학교정보, 교육과정, 학적, 학생생활, 성적, 학교생활기록부, 학부모서비스, 업무결재 및 승인, 대학입학전형 자료 등이 있다.

입학 영역은 각 학교급에서 신입생 입학과 관련된 업무를 처리한다.

보건 영역의 단위업무는 모든 학교급에서 공통적으로 사용하며 기초 자료 관리, 재학생(졸업생) 건강기록부 관리, 전염병환자 관리, 학생현황 및 통계업무 등이 있다.

이 시기에 2006년 3월 2일부터 제공된 대국민서비스인 Home-Edu 민원서비스는 자신의 PC에서 직접 제 증명을 출력하는 온라인 발급 민원서비스를 제공하게 되었으며, 2009년 까지 확대되어 인터넷 민원발급 활성화(13종) , 행정정보공동이용이 확산(11개 부처, 29종)되었다. 2006년 9월 1일부터는 초·중·고등학교 및 특수학교의 학부모를 대상으로 내 자녀 바로알기 인터넷 학부모 서비스를 시작하여 학교를 직접 찾아가지 않아도 학교정보뿐만 아니라 자녀의 성적, 일일출결, 학교생활기록부 등 자녀의 학교생활을 인터넷으로 한 눈에 열람할 수 있는 서비스를 제공하였다[24].

4) 3세대 교육행정정보시스템 (2010. 1. ~ 2020년 현재)

교육부에서는 수혜자 중심의 사용자 친화적인 교육행정서비스를 재편하고, Green IT 개념을 도입한 정보자원의 효율성을 제고하여 사용자 만족도를 극대화하기 위해 2010년 차세대 나이스를 구축하였다. 차세대 나이스는 전국 시·도교육청과 초·중등학교에서 사용되어 오던 나이스를 한 단계 개선한 교육행정정보시스템으로 교과 교실제, 입학사정관제 등 새로운 교육정책을 반영하고, 방과후학교관리, 성적 및 통계처리 기능 등을 제공하여 교원업무를 경감하고 시스템 사용 편의성을 한층 더 강화시켰다.

또한 차세대 나이스는 대국민 서비스포털(<http://www.neis.go.kr>)을 통해 학교 정보, 학교생활기록부 등 54종의 학생관련 정보를 학생이 직접 열람할 수 있는 서비스를 구축하여 학생에게도 유용한 서비스를 제공하게 되었다.

차세대 나이스 구축과 관련된 특징은 물적기반(인프라) 교체·통합, 사용자 편의성과 운영 효율성을 고려한 업무 프로그램 개편, 부처간 정보시스템 연계 및 대국민서비스 확대, 개인정보보호 및 보안체계 강화이다[2][24].

[표 II-3] 기존 나이스와 차세대 나이스 개선사항 비교

구분	기존 나이스 현황	차세대 나이스 개선사항	비고
2009 개정교육과정 지원	-	- 2011년 2009 개정교육과정 시행에 맞춰 지원기능 개발	신규
방과후 학교관리 시스템 도입	-	- 방과후 학교 관리시스템을 개발하여 학교 운영관리의 편의를 도모하고 각종 보고통계의 자동생성기능 개발	신규
업무포털을 통한 통합로그인	- 나이스(일반행정, 교무업무), 에듀파인시스템 개별 로그인 화면 제공	- 업무포털을 통한 통합로그인으로 접근권한이 있는 모든 업무 시스템에 접근 가능, 교직원의 시스템 업무서비스 접근성 향상	신규
대국민서비스 단일접속 창구 마련	- 시·도교육청, 서비스별 별도 로그인 후 서비스 이용	- 서비스 기능별 인증방식을 다양화하고, 통합사용자 관리를 통해 사용자 편의 제공	신규
물리적 기반 교체통합 인프라 규모의 변화	- H/W 102종 5,293식	- H/W 16종 331식	개선

2010년 개편이후 지속적으로 기능개선하며 운영되고 있는 교육행정정보시스템은 2019년 12월 기준 운영 업무는 4개시스템, 44개 단위업무, 268개 세부업무로 구성되고, 대국민서비스는 학생 46종, 학부모 59종, 홈에듀민원 18종을 제공하고 있다.

[표 II-4] 교육행정정보시스템 운영업무

구분	일반행정	교무업무	학교행정	대국민서비스
주요 업무	인사, 급여, 민원, 평생교육 등	교무/학사, 입(진)학, 보건 등	장학, 방과후학교 체육, 급식 등	대국민서비스, 설문조사 등
업무 규모	21개 단위업무, 102개 세부업무	7개 단위업무, 92개 세부업무	12개 단위업무, 56개 세부업무	4개 단위업무, 18개 세부업무

나이스 운영기관은 교육부(KERIS 위탁) 및 17개 시·도교육청이며 사용기관은 초·중등학교(11,600여개), 교육행정기관(교육부, 17개 시·도교육청, 176개 교육지원청), 대학·전문대학(400여개)이며, 사용자는 교직원 약 55만 명, 학생 545만 명, 학부모 등이 있다.

나이스 운영인프라규모는 H/W 642종(1,986식), 시스템S/W 796종(11,366식)으로 구성되어 있다[3].



[그림 II-1] 교육행정정보시스템 구성도(출처:교육부)

5) 4세대 나이스 구축 (2022. 2. ~) 추진안

그간의 나이스는 교육(행정)기관의 교육행정 업무 전반을 전자적으로 처리할 수 있도록 구축한 시스템으로 교육(행정)기관의 업무 효율성을 제고하고, 온라인 민원서비스를 통해 대국민 편의를 제공하는 등의 성과를 거두고 있으나, 최근 미래지향 교육정책과 전자정부 정책에 적극적으로 대응하기 위해, 대폭 개편이 필요한 시점으로 교육부와 17개 시·도교육청에서는 2022년 3월 개통을 목표로 개편을 준비하고 있다. 그 개편방향은 미래를 열어가는 교육 실현을 위한 교육정책의 변화와 범정부 차원에서 추진 중인 「디지털 정부혁신 정책」에 부응하고, 사용자 요구에 따른 업무처리절차를 개선하고, 기능 고도화를 위하여 나이스 운영인프라의 노후화로 인한 교체와 IT기술의 발전에 부응하고자 하는 것이다.

개편 전략으로는 첫째, 고교학점제, 과정중심평가 등의 학생 성장 중심 교육정책 도입을 뒷받침 할 수 있도록 기존 나이스를 확대·개편하고자 한다. 학교급별, 학교유형별 특성을 고려한 다양한 교육과정 운영 지원, 교육과정 운영과 학교생활기록 중심에서 수강신청, 과제제출, 수업, 피드백 등의 교수학습 활동을 적극 지원하는 서비스로 확대하고자 하는 것이다.

둘째, 업무 효율성 강화와 사용자 친화적 서비스 기반을 구축하는 것이다.

학생·학부모, 민원인 등이 이용하는 대국민 서비스는 교육 공공클라우드를 통합하여 교육관련 정보서비스 창구를 일원화하고, 모바일기기(스마트폰, 태블릿 등) 보급 및 활용이 증가하는 사회적 변화를 고려한 모바일서비스 플랫폼 구축 전자정부 공통 플랫폼과 연계한 행정정보 공동이용 확대, 증명서의 전자적 발급·보관(전자지갑), 통합 로그인체계(디지털원패스) 도입을 목표로하고 있다[5].



[그림 II-2] 4세대 교육행정정보시스템 구성안(출처:교육부)

6) 교육행정정보시스템 7단계 보안 아키텍처

교육행정정보시스템은 정보보안체계의 효율적 관리와 새로운 보안위협에 효과적인 대응을 위해 통합보안관리체계(ESM)를 도입하여 상시적으로 감시하고, 보안취약점 진단 등을 통하여 보안관리 대응을 철저히 하고 있다.

차세대 나이스 도입부터 7단계의 보안체제로 DB접근을 통제하고 있으며, 개인 정보 취급에 대한 기록관리 및 주요 민감정보 암호화 저장을 통해 개인정보 유출을 차단하고 있다.

또한 2014년에 나이스가 주요정보통신기반시설로 지정됨으로서 보안수준이 더

격상되어 운영하게 됨에 따라 안정성이 더욱 향상되었다[2][24].

[표 II-5] 나이스 7단계 보안체계[24]

구분	내용	적용 대책
1단계	개인PC방화벽 및 키보드 입력암호와 + 웹DRM	송수신 자료의 암호화 기능, 사용자 인증기능 제공
2단계	PC와의 데이터 통신암호화 + 통합인증권한관리	
3단계	침입탐지시스템(IDS), 침입방지시스템(IPS), VPN(IPSEC,SSL)	전용망 구성으로 해킹차단, 해킹프로그램 통과 불가 (사전 탐지 후 차단)
4단계	서버 이중화	
5단계	전자인증시스템(EWS) + 교육부 표준보안API	송수신자료의 암호화기능
6단계	서버보안 + 서버보안관리시스템	외부통신망 주소는 접근불가, 실시간 DB접근 로그관리
7단계	DB암호화 + DB접근제어, 로그관리시스템	

2. 학교생활기록부

1) 학교생활기록부의 정의

학교생활기록부는 학생이 학교에 입학한 순간부터 재적하는 순간까지 학생의 전반적인 학교생활과 성장, 발달을 교사가 관찰하여 기록한 문서이다. 교육부에서 발간한 학교생활기록부 기재요령에 따르면 학교생활기록부는 학생들로 하여금 자신의 소질을 계발하여 자아를 실현하고 지성과 인성의 균형을 이룬 전인으로 성장하도록 도와주기 위해 제안된 것으로서, 초·중등 교육법 제25조에 따라 학교의 장이 학생의 학업성취도 및 인성 등을 종합적으로 관찰·평가하여 학생 지도 및 상급학교의 학생선발에 활용할 수 있는 학생의 인적사항, 학적사항, 출결상황, 자격증 및 인증 취득상황, 교과학습발달상황, 행동특성 및 종합의견, 그 밖에 교육목적에 필요한 범위에서 교육부령이 정하는 사항에 대하여 교육부령이 정하는 기준에 따라 작성·관리되는 문서로 정의된다[14][28].

2) 학교생활기록부 구성요소

초·중등 교육법 시행령 제 21조의 규정에 근거하여 학교생활기록부는 인적사항, 학적사항, 출결상황, 수상경력, 자격증 및 인증 취득상황, 교과학습발달상황, 행동특성 및 종합의견 등의 항목으로 구성되어 있으며, 이 중 고등학교 학교생활기록부의 영역과 각 항목별 입력내용 및 입력가능 최대 글자 수는 [표 II-6]과 같다.

[표 II-6] 학교생활기록부 영역 및 입력가능 최대 글자 수

영역	세부항목	최대글자수 (한글기준)	비고
1.인적사항	학생성명, 학부모성명, 주소, 특기사항	835자	
2.학적사항	특기사항	500자	
3.출결사항	특기사항	500자	
4.수상경력	수상명, 참가대상(인원)	125자	
5.자격증 및 인증 취득사항	명칭 또는 종류	100자	

영역	세부항목	최대글자수 (한글기준)	비고
6.진로희망사항	희망사유	200자	2020년 3학년만
7.창의적 체험활동상황	자율활동 특기사항	500자	2020년 3학년만
	동아리활동 특기사항	500자	
	봉사활동 특기사항	500자	
	진로활동 특기사항	750자	
	봉사활동실적 활동내용	250자	
8.자유학기활동	진로탐색활동 특기사항	1,000자	중학교만
	주제선택활동 특기사항	1,000자	
	예술,체육활동 특기사항	1,000자	
	동아리활동 특기사항	1,000자	
9.교과학습발달상황	일반과목 세부능력 및 특기사항	과목별 500자	2020년 3학년만
	체육·예술과목 세부능력 및 특기사항	과목별 500자	
	개인별 세부능력 및 특기사항	500자	
	개인별 특기사항	500자	
10.독서활동상황	공통(500), 과목별(250)	750자	
11.행동특성및종합의견	행동특성 및 종합의견	500자	
12.전공·과정	1학기	60자	
	2학기	60자	
	비고	250자	

인적사항란은 학생의 정보와 함께 부모의 성명과 주소를 기록한다.

학적사항은 중·고등학교에서는 입학 전 전적학교의 졸업연월일과 학교명을 입력하며, 검정고시의 경우에는 검정고시 합격 연월일을 입력한다. 학적 변동이 발생할 경우 전출교와 전입교에서 각각 학적변동내용을 입력한다

출결상황은 수업일수와 결석, 지각, 조퇴, 결과 등을 입력한다. 특별한 결석사유나 개근과 같은 특기사항이 있는 경우 해당 내용은 특기사항란에 담임교사가 입력할 수 있으며, 특기사항 중 학교폭력과 관련된 사항은 학교폭력 예방 및 대책에 관한 법률 제17조에 따른 가해학생에 대한 조치사항을 함께 입력한다.

수상경력은 재학 중 중·고등학교 학생이 교내에서 수상한 상의 정보만 입력할 수 있으며, 동일한 작품이나 내용으로 수준이 다른 상을 여러 번 수상할 경우 최

고 수준의 수상경력 하나만을 입력한다.

자격증 및 인증 취득상황은 고등학생이 재학중에 취득한 자격증의 명칭 또는 내용, 취득연월일, 발급기관을 입력하며 원본을 대조한 후에 취득한 순서대로 입력한다. 진로희망사항은 2020년 3학년에만 해당되며 폐지되었다.

자유학기활동은 중학교에서 자유학기에 학교별로 실시한 자유학기 활동영역별 이수시간 및 특기사항을 입력한다.

창의적 체험활동은 자율활동, 동아리활동, 봉사활동, 진로활동의 4가지 영역으로 구성되어 있으며 이중 동아리활동 기재사항도 2020년 3학년만 해당된다.

교과학습발달상황은 고등학교인 경우 교과, 과목, 단위수, 원점수/과목평균(표준편차), 성취도(수강자수), 석차등급을 산출하여 각 학기말에 입력한다. 중학교는 교과, 과목, 단위수, 원점수/과목평균, 성취도(수강자수)를 산출하여 각 학기말에 입력한다. 초등학교는 각 교과별 성취기준에 따른 성취수준의 특성 및 학습활동 참여도 등을 ‘세부능력 및 특기사항’란에 교과별로 문장으로 입력하되, 1,2학년 ‘바른생활’, ‘즐거로운 생활’, ‘즐거운 생활’ 교과는 통합하여 입력한다.

독서활동상황은 중·고등학교의 개인별·교과별 독서활동 상황은 독서활동에 특기할 만한 사항이 있는 학생을 대상으로 학기말에 입력한다.

행동특성 및 종합의견은 학급담임교사가 수시로 관찰하여 누가 기록된 행동특성을 바탕으로 총체적으로 학생을 이해할 수 있는 종합의견을 문장으로 입력한다.

이렇게 다양한 항목을 모두 포함하는 학교생활기록부는 그 작성의 엄격성과 효율성을 위하여 학교생활기록의 작성 및 관리지침(교육부훈령)에서 정하는 작성과 관리의 방법을 따르도록 법적으로 규정되어 있다[14][19][28].

3) 학교생활기록부 성격

학교생활기록부는 공식 법적 문서이며, 학생의 학적에 대한 증명 자료적 성격, 교수·학습 지도 자료로 활용되는 지도 자료적 성격, 진학을 위한 전형 자료적 성격을 모두 가지고 있다.

먼저, 학교생활기록부는 초·중등 교육법 제25조와의 교육부훈령에 의하여, 반드시 작성해야 하는 공식 문서인 동시에 작성하도록 되어 있는 사항은 반드시 작성해야 하는 강제성을 가지고 있다는 점에서 법적 장부로서의 성격을 가지고 있다. 다음으로 학교생활기록부는 학생에 대한 교수-학습 지도 자료로 활용되는 성격과 상급학교의 진학 등의 자료로 활용하는 진학전형자료 성격을 가진다. 또한 학교생활기록부는 학교에 재적하는 동안의 학생에 대해 기록하고 기록을 보관함으로써 학생의 학적에 대한 증명으로서의 측면을 가진다.

이러한 교육자료로서의 학교생활기록부의 중요성과 법적 문서로서의 공신력을 위하여 기록의 주체인 교사는 학생의 전반적인 학교생활에 대하여 사실에 입각하여 정확하게 기록해야 할 의무가 있다[14][19][28].

4) 학교생활기록부의 정정과 보존

학교생활기록 및 관리지침(교육부훈령 제331호)에서 학교의 학년도는 3월 1일에 시작하여 다음 해 2월 말일까지로 하며, 매 학년이 종료된 이후에는 당해 학년도 이전의 학교생활기록부 입력 자료에 대한 정정은 원칙적으로 금지한다. 그러나 기록에 누락이나 수정사항이 발생할 수 있기에 이때는 반드시 정정할 내용에 대한 객관적인 증빙자료를 첨부하여 정정의 사유, 정정내용 등에 대하여 학교학업성적관리위원회의 심의 절차를 거쳐 학교생활기록부 정정대장의 결재 절차에 따라 정정 처리해야 한다.

고등학교의 경우에는 9월부터 진행되는 수시입학전형에 대비하여, 3학년 1학기에 학교생활기록부를 점검하고 오류를 발견하는 작업을 수행하는데 이때 많은 정정 사항이 발생한다. 대부분 이전 학년도의 오류이기에 교사가 임의로 수정할 수 없고 공식적인 정정 절차를 거쳐야 하며, 객관적인 증빙자료를 포함해야 한다. 학교생활기록부 허위사실 기재와 부당정정(학생 본인 및 가족의 질병명정정은 예외)은 학교생활기록부의 엄정한 공적 성격에 의해 교육공무원 징계양정 등에 관한 규칙에 의해 시험문제를 유출하거나 성적을 조작하는 것과 같은 학생 성적 비위와 동일하게 취급되고 징계 시 감경대상에서 제외되는 중대한 비위로 처리된다.

학교생활기록부의 보존에 관하여는 학교생활기록 및 관리지침(교육부훈령 제 331호)의 훈령 제18조에서 다루고 있는데, 자료의 보존 기한과 학교폭력 가해학생의 기록 삭제에 대한 내용이 주요하다. 먼저 자료의 보존 기한의 경우, 공공기록물 관리에 관한 법률 및 동법 시행령에 의거하여 학교생활기록부의 공공기록물로서의 성격을 분명히 하고 있으며, 보존기간은 준영구 보존으로 기록물로서의 중요성을 강조하고 있다. 다만 학교생활기록부의 일부 항목만을 다루고 있는 학교생활기록부Ⅱ의 전산자료는 학생 졸업 후 5년 동안만 보존하면 되고, 그 이후에는 폐기 처분하여 자료를 남기지 않도록 한다[14][19][28].

학생이 졸업한 후 5년 동안은 학교에서 보관하고 그 이후에는 이관하여 보관하도록 하고 있다.

학생은 매년 존재하고 졸업생은 매년 늘어나므로 학교생활기록부를 준영구보존한다는 것은 사실 양적으로도 어려운 일이다. 그리하여 학교생활기록부 업무의 효율성을 증대하고 종이 출력물 보관 시의 행정력 낭비를 막기 위하여 학교생활기록부는 출력본이 아닌 전산자료로 보관하고 있으며, 교육부와 시·도교육청에서는 졸업 후 5년이 지난 학교생활기록부 이관을 2002년 졸업생 자료부터 2019년에 실시하였으며, 연차적으로 이관을 실시할 계획이다[6].

5) 학교생활기록부의 활용

학교생활기록부는 여러 항목을 통해 학생의 학교생활 전반에 대한 내용을 담고 있어 학교생활기록부를 보면 학생의 학업능력과 성격, 발달 정도 등의 특성을 총체적으로 이해할 수 있다. 따라서 학교생활기록부는 학생과 학부모, 교사, 교육행정기관, 상급학교에 제공되며 각각의 목적에 따라 활용된다고 할 수 있겠다 [14][19][28].

(1) 학생과 학부모에게 활용

학교생활기록부는 학생의 학업능력뿐만 아니라 행동발달상황에 대한 기본적인 정보를 제공함으로써 학생이 자기 자신에 대해 잘 파악할 수 있도록 도울 수 있어야 한다.

먼저 학업능력의 경우, 현재의 교과 성적을 포함하여 학업과 관련된 여러 활동

을 종합하여 기록함으로써 학생의 학습 성과와 학업 관심도, 관심 있는 학습 분야 등을 파악할 수 있도록 한다. 시험점수와 석차 등급 등 숫자로 표시되는 객관적 지표 이외에도, 교사의 서술형 평가는 학업능력과 관련한 학생의 잠재적 능력을 파악하는 데 큰 도움이 된다.

학교생활기록부에는 교사가 1년 동안 관찰한 학생의 성격과 교우관계, 행동적 특성이 기록되어 있다. 인성, 교우관계 등을 포함하는 행동발달상황 또한 학교생활기록부가 학생과 학부모에게 제공할 수 있는 중요한 정보이다.

이처럼 학생과 학부모에게 제공되는 학생의 학업능력과 행동발달상황에 대한 정보는 학생의 현재 상태뿐만 아니라 학생의 미래 직업과 성격 등에도 영향을 줄 수 있는 자료가 된다.

(2) 교사에게 활용

교사는 학교생활기록부를 통해 학생의 학업능력에 대한 기초적인 정보를 파악하여 학생의 학습 지도를 효과적으로 실행할 수 있는 학습계획을 세울 수 있다. 교사는 단순히 학생의 학업능력을 평가하는 평가자로서만 존재하는 것이 아니라 학업능력의 발달을 도와주는 도움자이자 지원자가 되어야 하므로, 과거의 학교생활기록부를 활용하여 학생의 학업적 능력을 끌어줄 수 있어야 한다. 또한 생활지도와 인성교육 측면에서도 학교생활기록부는 교사에게 매우 중요한 자료이다.

(3) 교육행정기관에 활용

학교를 포함한 교육행정기관에서도 학교생활기록부는 중요한 의미를 가지고 있다. 학생과 학부모, 교사가 학교생활기록부를 통해 학생의 전인격적인 발달사항을 파악하는 데 가장 큰 목적을 둔다면, 교육행정기관에서는 행정적인 측면에서 접근하여 학생의 학적과 관련된 부분이 학교생활기록부의 가장 중요한 목적이 된다.

학교에서는 학교생활기록부를 근거로 학생의 전적 학력을 파악하고 입학할 수 용하며, 진급과 졸업을 결정하게 된다. 학생이 현재 학교에 재적하고 있거나 휴학, 자퇴, 퇴학하였다는 등의 재적 사항을 확인하고 증명하는 자료로 활용한다. 학교생활기록부는 단위학교뿐만 아니라 교육청과 교육부에도 중요한 자료로서, 학생과 관련된 여러 정책의 기본적인 사항으로 활용되고 있다.

(4) 상급학교에서 활용

학교생활기록부는 학생이 상급학교 진학자료로 활용된다. 고등학교의 학교생활기록부가 대학입시에 활용되는 경우이다. 대학에서는 대학수학능력시험이나 논술고사, 면접 등을 통해서 확인할 수 없는 학생의 전인격적인 발달에 대해 정보를 얻기를 원하는데 고등학교 3년간의 학교생활기록부는 이러한 사항을 모두 담고 있기 때문이다. 대학은 학교생활기록부를 통하여 학생의 3년간 학업능력 변화 추이와 전공에 대한 관심, 적합도 등을 파악하고 출결과 인성, 사회성 등 전반적인 학교생활에 대해 알고자 한다. 전형에 따라 대학에서는 학교생활기록부의 항목을 입시에 반영하여, 해당 학생의 입학 여부를 결정한다. 학생부종합전형이 실시되면서 대학에서 학교생활기록부를 활용하는 정도는 매우 커졌으며 이는 고등학교에서 학교생활기록부를 작성하는 방법에도 많은 영향을 미쳤다.

이외에도 학교생활기록 및 관리지침(교육부훈령 제331호)에 따르면, 초등학교 및 중학교의 장은 지속적인 진로교육을 위하여 학교생활기록부의 진로관련 사항을 해당 학생의 동의를 받아 상급학교의 장에게 전산자료의 형태로 진학이 확정된 후에 제공할 수 있다. 입시뿐만이 아니라 진로교육과 같이 학생에 대한 지속적인 관심이 요구되는 부분에서도 상급학교는 하급학교의 학교생활기록부를 통해 정보를 얻고 연계교육을 할 수 있는 것이다.

3. 블록체인

1) 블록체인 기술

(1) 블록체인(Blockchain) 정의 및 특징

기존의 시스템들은 중앙에 원장을 관리하는 시스템으로 발전해 왔으며, 원장의 조작과 개인정보 유출, 시스템 오류, 처리속도의 저하를 예방할 수 있어야 하고, 해킹과 같은 외부의 악의적인 공격 시도를 방지하여 원장에 저장되어 있는 자산의 신뢰성을 보증한다. 보통 이런 역할을 하는 시스템이나 기관을 “신뢰 보증하는 제 3자, 즉 Trusted Third Party(TTP)”라고 한다. 그러나 이런 TTP를 설립하고 운영하는데 소요되는 비용은 이용자의 높은 수수료 부담으로 전가되고, 신뢰를 보증하기 위한 규제 및 감독은 거꾸로 진입 장벽이되어 혁신적인 신규 서비스 및 사업자의 진출을 제약하는 요인으로 작용할 수 있다[15].

블록체인은 이와 같은 제3의 신뢰기관이 없이 원장의 신뢰성을 보증하기 위하여 참가자 간에 발생한 거래정보를 기록한 원장을 특정 기관 중앙 시스템이 아닌 분산 네트워크에서 참가자가 공동으로 기록하고 관리하는 분산 장부 기술(distributed ledger technology)이다. 블록체인에서 데이터는 ‘블록’이라는 단위로 연결고리형태의 분산 저장환경에 저장되어 이미 블록으로 연결 되었다면 누구도 수정할 수 없고 거래의 흐름은 모두에게 공개 된다[15].

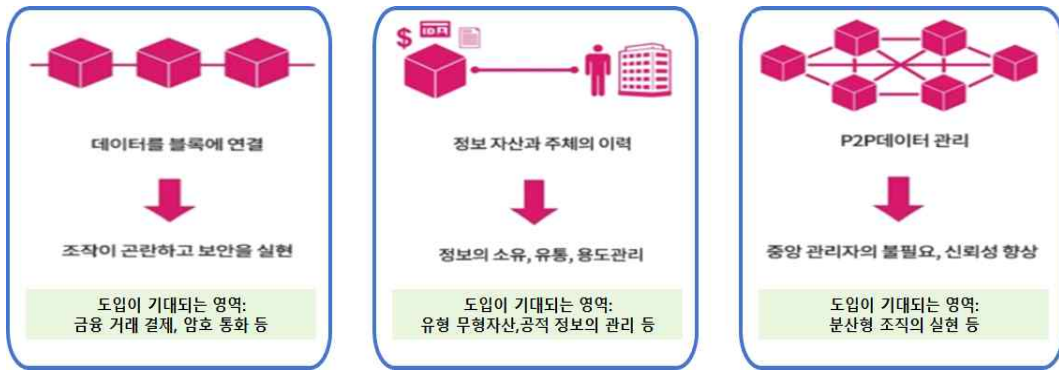
탈중앙식·분산식은 거래내역이 기록된 원장 전체를 모든 참여자가 각각 보관하고, 새로운 거래를 반영·갱신하는 작업을 공동 수행한다.

데이터 관리기관(은행, 공공기관 등) 운영비용을 절감하고, 해킹에 보다 안전하며, 일부 오류가 발생해도 전체 기능은 동작하는 장애내성이 장점인 반면, 참여자들이 함께 합의를 이루고 각자 기록을 관리하는 것이 부담될 수 있다.

블록체인의 특징을 아래의 3가지로 요약할 수 있다.

첫째, 거래 데이터를 일정 시간마다 집약된 블록에 정리하고, 블록을 작성할 때 과거의 블록요소를 다음 블록에 넣어 연결 하므로 데이터의 위조를 방지 할 수 있다. 둘째, 자산과 그것들을 소유하는 존재를 연결함으로써 이중 이용을 방지하

고 누구에게 양도 되었는지를 정확하게 관리할 수 있다. 셋째, 중앙의 서버가 아닌 다수의 컴퓨터에서 같은 데이터를 분산 관리하여 어느 1개의 데이터가 상실되더라도 다른 참가자의 컴퓨터가 가동되고 있으면 시스템을 유지하는 것이 가능하다[15].

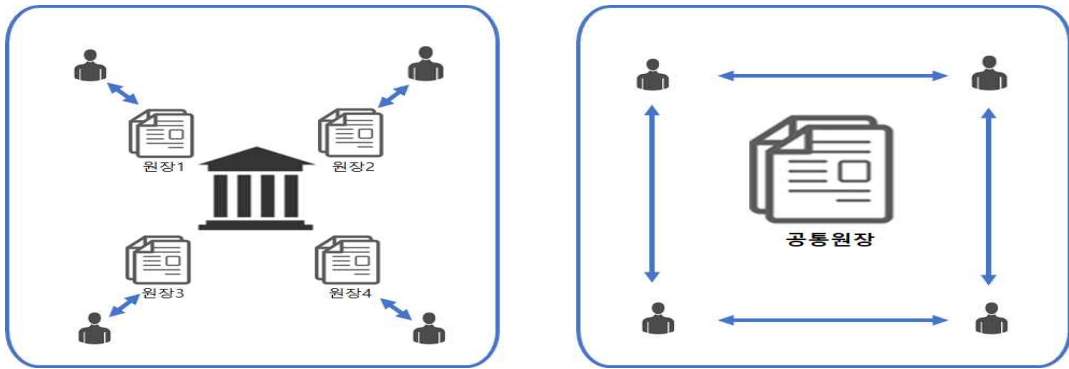


[그림 II-3] 블록체인의 특징(출처:한국 블록체인 협회)

(2) 분산원장(Distributed Ledger)

분산원장은 블록체인을 구성하는 가장 중요한 요소 중 하나이다. 블록체인을 탈중앙화된 시스템으로 만들어 주는 핵심기술이다. 거래 기록 등의 데이터를 저장하는 데이터베이스(원장)를 중앙화된 서버가 소유하는 것이 아니라, 블록체인에 참여하는 모든 사람이 동일한 원장을 소유하고 관리하는 기술이다[16].

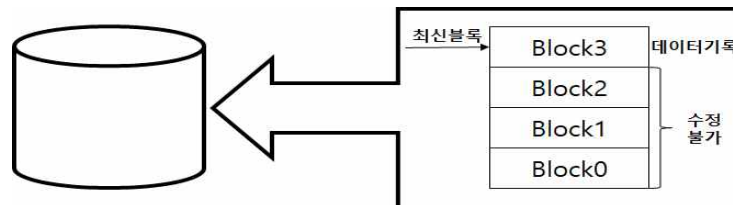
기존의 시스템에서는 동일한 비즈니스 네트워크에서도 사용자마다 서로 다른 원장에 비즈니스 정보를 기록하는 것과는 달리 블록체인에서는 블록체인 사용자 모두 동일한 원장에 비즈니스 정보를 기록하고 관리한다. 예를 들어, A은행을 이용하는 고객들은 각각의 서로 다른 고유한 계좌(원장)를 가지고 금융 정보를 기록하는 반면, 비트코인, 이더리움 등과 같은 블록체인 플랫폼의 경우 모든 사용자에 대한 거래 기록이 하나의 비트코인 원장에 모두 기록된다. 하지만 이러한 구조에서는 프라이버시 문제가 발생할 수 있는데, 하이퍼레저 패브릭에서는 채널(Channel) 개념을 도입하여 프라이버시 문제를 해결하였다[16].



[그림 II-4] 중앙시스템과 블록체인 분산원장

기술적 관점에서 보면, 원장은 통상 거래에 필요한 정보(거래번호, 거래일시, 송신자, 자산, 수신자 등)로 항목을 구성하게 되며, 원장은 순차적이고 시간이 표시된 거래의 목록이라 할 수 있다.

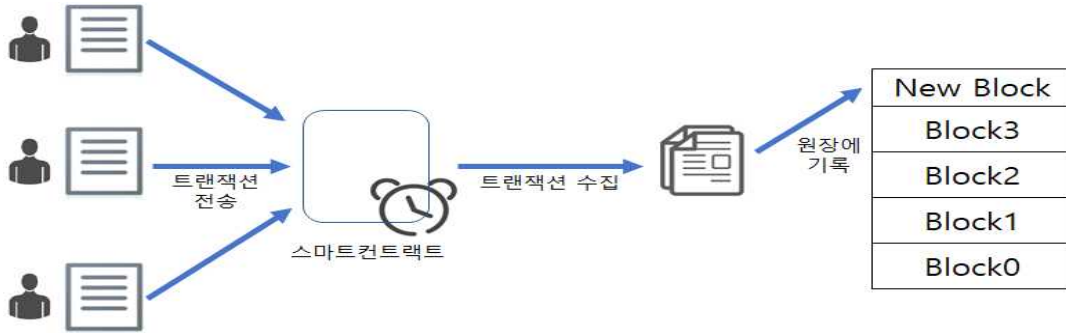
블록체인 분산원장의 또 다른 특징은 모든 정보가 해시화되어 Append-only 방식으로만 원장에 저장되기 때문에 한번 원장에 기록된 정보들은 절대 수정할 수 없다. 이와 같은 불가변성의 특성은 블록체인 데이터에 대한 악의적인 변조를 불가능하게 만들어 데이터에 대한 신뢰도를 향상시켜 주는 역할을 한다[16].



[그림 II-5] 블록체인 블록 구조

블록은 블록체인의 단위개념으로 블록의 상태 정보와 다수의 트랜잭션(거래) 정보가 포함되어 있다. 블록체인(데이터베이스)에 데이터를 저장하기 위한 데이터 묶음 단위이다

(3) 스마트 컨트랙트



[그림 II-6] 블록체인 스마트 컨트랙트

블록체인 참여자는 스마트 컨트랙트를 통해서 분산원장에 정보를 기록하거나 불러올 수 있다. 또한, 스마트 컨트랙트를 이용하여 단순히 거래 정보를 읽고 쓰는 것뿐만 아니라 프로그래밍을 통해 거래 자동화 등의 다양한 응용프로그램을 만들 수도 있다. 예를 들어, 그룹 공동 명의의 계좌를 만들어서 특정 인원 수 이상의 서명이 있어야 잔액을 출금할 수 있는 기능이나, 특정 날짜에 월급이 입력되는 기능 등을 스마트 컨트랙트를 통해 구현할 수 있다.

또한, 스마트 컨트랙트를 좀 더 편리하게 사용하기 위해 개발되는 프로그램을 분산 애플리케이션(Decentralized Application, DApp)이라고 한다[16].

(4) 합의

블록체인에 참여하는 모든 사람이 동일한 원장을 소유해야 한다. 이러한 조건을 만족시키기 위해 비트코인과 이더리움에서는 블록체인에 참여한 모든 노드 중 암호화된 퍼즐의 답을 가장 먼저 찾아내는 노드의 블록을 최신블록으로 업데이트하는 PoW(Proof of Work)방식이 있다. EOS는 블록체인 참여자가 21명의 블록 생성자를 선출하여 선출된 블록 생성자가 최신 블록을 생성하는 DPoS(Delegated Proof of Stake) 방식을 사용한다. 이 밖에도 대부분의 블록체인 플랫폼에서 PoW와 PoS 알고리즘을 기반으로 PBFT(Practical Byzantine Fault Tolerance) 등으로 변형하여 합의 과정에 사용하고 있다.

하이퍼레저 패브릭에서는 조금 다른 관점으로 합의 알고리즘을 정의한다.

PoW, PoS 혹은 BFT와 같이 특정 알고리즘에 국한시키지 않고 세 가지 일련의 과정을 통틀어 합의 과정이라고 말한다. 세 가지 과정이란 첫째, 보증 정책 확인, 둘째, 트랜잭션을 정해진 순서에 맞춰 정렬, 셋째, 정렬된 트랜잭션의 유효성 검증 후 최신 블록 업데이트이다[16].

2) 블록체인 기술 구분

(1) 비트코인(Bitcoin)

비트코인은 블록체인기술을 기반으로 만들어진 최초의 암호화폐이다. 중앙은행 없이 전 세계적 범위에서 개인 간에 금융 거래를 할 수 있도록 설계된 암호화폐이다. 2008년 10월 사토시 나가모토는 비트코인 논문(Bitcoin : A Peer-to-Peer Electronic Cash System)을 공개하였고, 2009년 1월에는 프로그램 소스를 배포하였다.

비트코인의 화폐 단위는 BTC이다. 비트코인의 총발행량은 총 2,100만개로 고정되어있다. 계속 발행할 수 있는 전통적인 화폐와 달리 제한된 액수의 화폐를 발행하여 더 큰 기대치를 얻을 수 있었다.

비트코인은 합의 알고리즘인 작업 증명(Proof-of-Work)알고리즘을 통해 탈중앙화 시스템의 기술적 문제인 이중지급과 비잔티움 장군 문제를 해결하였으며, 네트워크에 기여를 한 구성원에게 보상을 제공하였다. 이러한 방식으로 선의의 경쟁을 통해 더 많은 노드가 네트워크에 참여하고 기여할수 있는 환경을 제공하였다[17].

비트코인 블록체인은 블록체인을 성공적으로 구현한 첫 번째 응용으로 큰 의미가 있지만, 아래의 몇 가지 한계점을 갖고 있고 이러한 한계점으로 인해 암호화폐 이외의 분야에 활용하기가 어렵다.

첫째, 지나친 자원 낭비이다. 비트코인은 발행 수의 제한이 있고, 투기 심리로 인한 과도한 경쟁으로 인해 작업 증명의 난이도가 높아지면서 작업증명 과정에서 지나치게 많은 컴퓨팅 자원을 소모하게 된다.

둘째, 긴 거래 소요시간이다. 비트코인에서는 새로운 블록이 약 10분에 한번씩 생성되는데, 새롭게 생성된 블록 이후 대략 6블록이 지났을 경우 체인으로 유효

이지 못한 ‘스테일 블록’이 될 가능성이 매우 낮아지기 때문에 블록에 포함된 거래가 정상이라고 판단한다. 그리고 블록의 크기가 1MB로 제한되어 있어 하나의 블록에 포함되는 거래의 숫자가 제한적이라는 문제점도 거래를 지연시키는 원인이 된다.

셋째, 확장성의 부족이다. 비트코인은 거래를 처리하기 위해 충족되어야 하는 조건을 지정하기 위하여 트랜잭션 스크립트를 사용한다. 하지만, 이 스크립트에는 화폐의 전달에 해당하는 조건만 기술할 수 있기 때문에 암호화폐 이외의 분야에 적용하는데 한계가 있다[15].

(2) 이더리움(Ethereum)

이더리움은 블록체인기술을 기반으로 스마트 계약(smart contract) 기능을 구현하기 위한 분산 컴퓨팅 플랫폼이다. 이더리움에서 이더(Ether)는 비트코인과 마찬가지로 암호화폐의 일종이며, 이더리움의 화폐 단위는 ETH이다.

이더리움은 2015년 7월 30일 Vitalik Buterin에 의해 개발되었다. Vitalik Buterin은 암호화폐 비트코인에 사용되는 핵심 기술인 블록체인에 기존 화폐 거래 기록뿐 아니라 스마트 계약 등의 추가 정보를 기록할 수 있게 하였다. 스마트 계약이란 금융 거래, 부동산 계약 및 공증인과 같은 다양한 유형의 계약을 블록체인 기반으로 체결하고 이행하는 것을 말한다.

이더리움은 기존 비트코인에서 볼 수 없었던 다양한 새로운 기술을 개발·도입했다[17].

첫째, 블록 크기가 1MB인 비트코인에 비해 이더리움은 블록 크기 제한이 없다. 또한 10분에 한 번 블록이 생성되어 거래 확정 시간이 길었던 비트코인에 비해 블록 생성 주기가 15초 내외로 빠른 검증이 가능하다.

둘째, 스마트컨트랙트(Smart Contract)를 도입했다는 점이다. 스마트 컨트랙트는 디지털 명령어로 계약을 작성하면 조건에 따라 계약 내용을 자동으로 실행할 수 있다는 개념이다.

암호화폐의 거래 조건만 기입할 수 있었던 비트코인의 트랜잭션 스크립트와 달리 스마트컨트랙트는 블록에 거래 데이터 외에도 조건문 이나 반복 문과 같은 프로그램이 가능한 실행코드를 포함시켜 블록체인의 활용범위가 비약적으로 넓

어지는 계기가 되었다[15].

(3) 하이퍼레저 패브릭(Hyperledger Fabric)

IBM과 Digital Asset에서 시작하여 2015년 리눅스재단으로 이관된 하이퍼레저 프로젝트는 새로운 디지털 자산의 거래 수행 방식을 제공할 수 있는 공유원장의 표준 기능을 블록체인으로 발전시키기 위한 오픈소스 협력 프로젝트로 여러 회원사가 가입되어 있다. 하이퍼레저 프레임워크 중에서 가장 활발하게 활동 중인 하이퍼레저 패브릭은 어플리케이션이나 기업용 솔루션을 개발할 수 있는 블록체인 기반 프레임워크로서 합의나 멤버십 서비스 등 핵심 기술 요소들이 plug-and-play 방식으로 구현될 수 있도록 구성되어 있다. 하이퍼레저 패브릭의 특징은 체인코드(chaincode)로 구현된 분산 원장 및 스마트컨트랙트를 지원하며 회원 서비스를 통해 개인정보 보호 및 접근을 제어하는 허가형(permissioned) 프라이빗 블록체인이다.

프라이빗 블록체인은 동일한 목적을 가진 참여자 혹은 기업이 블록체인 네트워크를 구성하게 되므로 퍼블릭 블록체인과 달리 성실한 참여를 이끌어 내기 위한 방식의 합의 알고리즘과 보상이 불필요하다. 즉, 블록 생성에 소요되는 시간이 퍼블릭 블록체인에 비해 비약적으로 빠르기 때문에 실시간 트랜잭션 처리가 중요한 분야에 블록체인을 활용할 수 있다는 장점이 있다[15].

하이퍼레저 패브릭은 대표적으로 프라이버시와 기밀성, 작업구간별 병렬처리, 체인코드, 모듈화된 디자인 네 가지 특징이 있다.

첫째, 블록체인 참여 조직 간에 채널 개념을 도입하여 프라이버시와 기밀성을 제공한다. 예를 들어, 블록체인 참여 기업 중 특정 정보를 특정 회사에만 공유하고 싶은 경우를 가정해보면, 해당 기업들은 정보를 공유하고 싶은 회사와 협정을 맺은 후 채널을 생성하여 정보를 공유한다. 같은 블록체인 네트워크에 있다고 하더라도 채널에 소속되지 않은 조직은 채널의 거래 내용을 확인할 수 없다.

둘째, 트랜잭션의 생성부터 합의하는 과정까지 단계별로 분리하여 처리할 수 있다. 첫 번째 실행(Execute)단계에서는 트랜잭션을 실행하고 결과값을 검증하는 작업을 수행한다. 두 번째 단계인 정렬(Order)단계에서는 실행 단계에서 검증이 끝난 트랜잭션을 취합하여 순서에 맞게 정렬한 후 블록을 생성하는 작업을 수행

한다. 마지막으로, 검증(Validate) 과정에서는 블록에 포함된 모든 트랜잭션에 대한 결과값 검증을 수행하고, 각종 인증서 등을 확인한 후 이상이 없을 시 최신 블록을 업데이트한다. 이처럼 단계를 분리하여 처리하여 트랜잭션을 실행하고 검증하는 노드와 트랜잭션을 정렬하는 노드의 부하를 줄일 수 있고, 동시에 두 가지 이상의 작업을 수행하는 병렬처리가 가능하기 때문에 시스템 성능이 향상된다.

셋째, 체인코드는 기존 블록체인의 스마트 컨트랙트와 동일한 기능을 가지고 있으며, Go와 Node.js를 이용해서 다양한 형태의 응용프로그램으로 개발될 수 있다. 또한 시스템 체인코드는 트랜잭션의 보증, 블록 검증, 채널 설정 등 시스템 레벨에서의 설정이 필요할 때 사용된다.

넷째, 시스템 구축 시 인증, 합의 알고리즘, 암호화 등의 기능을 참여자들이 원하는 형태로 선택해서 블록체인을 운영할 수 있도록 모듈화된 디자인을 지원한다. 이와 같이 모듈화된 디자인은 하이퍼제저 패브릭 블록체인을 다양한 비즈니스 모델에 맞추어 개발할 수 있는 유연성을 제공한다[16].

3) 블록체인 구분 및 활용분야

블록체인은 사용 특성에 따라 퍼블릭(public)과 프라이빗(private) 블록체인으로 구분할 수 있다.

퍼블릭 블록체인이란 무허가(Permissionless) 블록체인이라고도 불리우며 거래소에서 그 토큰(암호화폐)이 거래되는 대다수의 블록체인으로 대표적으로 비트코인, 이더리움 등을 들 수 있으며, 네트워크 참여자가 모두 동일한 권한으로 블록체인에 참여할 수 있고 거래 기록을 확인 할 수 있으며 트랜잭션 내역을 검증할 수 있다.

프라이빗 블록체인은 허가(Permissioned) 블록체인, 혹은 동일한 목적을 지닌 주체가 모여 구성할 경우 컨소시엄(Consortium) 블록체인 이라고 불리는데 별도의 망을 구축하거나 인증을 하여 제한된 참여를 허용하는 블록체인을 의미한다. 보통 기업에서는 모든 정보를 공개할 수 없기 때문에 권한 기반 접근 통제를 하는 경우가 있으므로 대부분 프라이빗 블록체인을 선호한다[17].

[표 II-7] 퍼블릭 블록체인과 프라이빗 블록체인 비교

구분	퍼블릭 블록체인	프라이빗(컨소시엄) 블록체인
입기권한	누구나 열람 가능	허가된 기관만 열람 가능
거래 검증 및 승인	누구나 네트워크에 참여하면 거래 검증 및 승인을 수행	승인된 기관과 감독기관
트랜잭션 생성자	누구나 트랜잭션을 생성	법적 책임을 지는 기관만 참여
합의알고리즘	부분 분기를 허용하는 작업증명이나 지분증명 알고리즘	부분 분기를 허용하지 않는 BFT 계열의 합의알고리즘
속도	7~20TPS	1000TPS 이상의 고성능
권한관리	누구나 모두가 모든 일을 할 수 있음	Private Channel, Tierd System 등을 통해 읽기 쓰기 권한 관리가 가능
예시	비트코인, 이더리움	IBM Fabric, R3 Corda 등

블록체인은 암호화폐, 장외시장에서의 주식거래, 스마트 계약, 사물 인터넷, 인증, 결제 및 송금, 유통 등 다양한 영역에서 활용되고 있다[17].

[표 II-8] 블록체인 활용분야

구분	퍼블릭 블록체인
암호화폐	블록체인의 특징을 기반으로 암호화폐의 거래내역을 기록하는 데 활용, 비트코인, 이더리움 등 다양한 암호화 화폐 존재
주식거래	블록체인을 활용하여 주식 거래 시 증권등록, 거래처리, 결제대금 청산 등 후처리 과정의 효율성 높임
스마트 컨트랙트	블록체인에 계약문서를 등록하여 위변조 방지, 조건 만족에 따른 자동문서 이행 보장
사물인터넷	블록체인 기반으로 한 스마트컨트랙트 기술 연계, 제품 스스로가 소모성 품목을 재주문하거나 자동 결제 등으로 활용 가능

4) 블록체인 공공부문 적용 사례

(1) 국내의 공공·민간의 블록체인 추진사례

국외에서는 국내보다 폭넓은 블록체인 적용대상(토지·범죄증거·행정문서부터 건강데이터까지)과 정부업무 전반(등록부터 거래·처리·공유까지)에 걸친 전환을

추진 및 확대중이다.

[표 II-9]에서 국내와 국외에서의 활용분야별 사례를 비교하여 보여준다[26].

[표 II-9] 국내와 국외에서의 블록체인 활용분야별 사례

구분	세부 분야	국내	국외
금융	송금 거래	-	-포스트코인 거래플랫폼(미국)
생활 경제	요금 결제	-지역기반 가상화폐(노원구) -전기에너지 거래플랫폼(한진) -실손의료보험금 자동청구(교보)	-복지수당 결제시스템(영국)
	인증	-본인인증 금융서비스(국민카드)	-
비즈니스	사물 인터넷	-전기화재 발화지점 분석 (전기공사)	-식품안전망솔루션(IBM) -물류운송추적시스템(머스크)
	소셜 트레이드		-뉴스기사 플랫폼(시빌)
공공 행정	전자 투표	-따복공동체 전자투표(경기도) -온라인 전자투표시스템 (한국예결원)	-블록체인 전자투표 앱(러시아)
	기록 관리	-차세대 전자문서시스템(KT) -의료정보플랫폼(메디블록)	-건강데이터 공유,활용(미국) -디지털 증거보존,활용체계 (영국) -전자문서 기록,관리시스템 (두바이)
	디지털 계약	-	-토지 등록,거래 플랫폼(조지아)
	전자 시민증	-	-전자시민증(에스토니아) -디지털ID플랫폼(MS)

(2) 국내 공공분야 블록체인 주요사례

블록체인은 기존의 기술주도적 서비스 생성·제공방식의 한계를 벗어나, 다자간 네트워크중심의 협력을 통해 사회현안을 해결하고 가치를 창출하는 혁신을 선도할 것으로 여겨 국내 정부에서도 각 분야에 블록체인을 적용할 수 있도록 권고하고 있으며 실제 구현된 주요 사례 두 가지를 소개한다[26].

① 경기도 : 따복공동체 주민결정을 위한 전자투표


○(추진목적) 주민투표 참여율을 높이고 다수 국민의 의견을 반영한 정책결정을 위해 지자체 중에서 블록체인 기반의 전자투표를 선제적으로 도입

- 2016년, 1만 2,000여명의 주민참여로 따복공동체


○(추진내용) 공동체별 사업내용을 듣고 블록체인 기반의 따복공동체 앱으로 투표진행 후 즉각적인 결과확인이 가능한 점 등의 장점을 극대화

- 경기도는 2017년 2월 23일, 815개 주민공동체를 대상으로 '따복공동체 주민제안 공모사업'을 블록체인 기반 전자투표로 심사
- 투표할 공동체 번호를 확인한 후, 따복공동체 앱에 미리 배부된 투표권 QR코드를 인식하고 공동체 발표영상을 보며 앱으로 투표
- 기술적 한계, 이용활성화 등 보완사항을 반영하여 지속 추진여부 결정 예정


〈 따복공동체 앱 〉



〈 따복공동체 번호확인 〉



〈 영상을 보며 심사진행 〉



출처 : 경기도청 공식 블로그
 [그림 II-7] 따복공동체 전자투표(출처:경기도청)

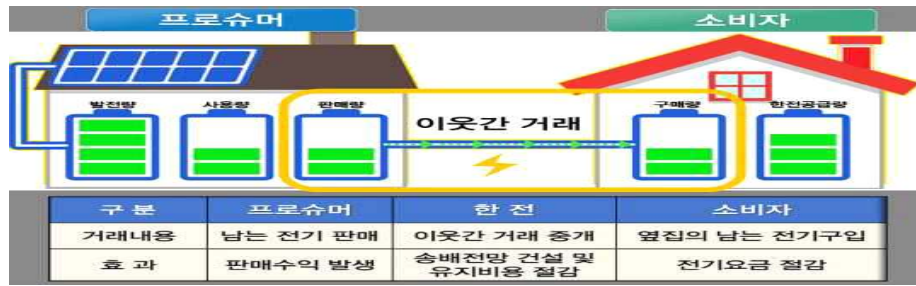
② 한국전력공사 : 이웃 간 전기에너지 거래플랫폼

○(추진목적) 프로슈머*가 스스로 생산하고 남는 전기를 한국전력공사의 중개로 전기요금 부담이 큰 이웃에게 전력을 판매할 수 있는 전력거래 활성화

* 프로슈머는 주택이나 상가 지붕에 설치한 태양광 패널 등을 통해 전기를 생산하는 사람

○(추진내용) 전력거래 플랫폼을 통해 실시간으로 최적의 프로슈머와 소비자를 매칭하여 거래가 가능하도록 서비스 제공

- 전력거래는 '에너지포인트'로 이루어지고 보유한 포인트는 전기요금 납부 외에도 현금 환급, 전기차 충전소에서 사용 가능
- 한국전력공사 인재개발원 내의 건물(9개)과 서울에 있는 아파트(2개) 단지를 대상으로 시범서비스를 실시하고 향후 실증사업 확대 예정



[그림 II-8] 블록체인 기술을 적용한 사용자(프로슈머-소비자)간 전력거래
구상도(출처:한국전력공사)

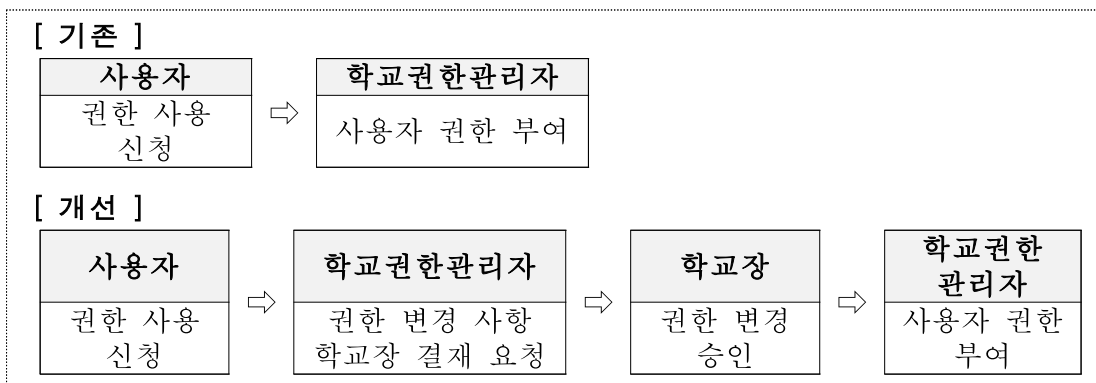
Ⅲ. 학교생활기록부 관련 최근 동향 연구

본 장에서는 학교생활기록부 데이터의 신뢰성 확보를 위한 최근 교육행정정보 시스템에서의 보안관리 강화방안과 학교생활기록부 관련 중점업무인 대입전형자료 온라인제공과 졸업생 학교생활기록부 이관에 대하여 고찰하고, 2022년 개통예정인 4세대 나이스에서 구현하고자 하는 블록체인 제안사항에 관하여 조사해 보고자 한다.

1. 학교생활기록부 보안관리체계 강화 방안

1) 학교생활기록부 권한관리 강화

교육부에서는 학교생활기록부 종합전형 확대와 학교생활기록부 부당 정정 등의 일련의 상황이 발생함에 따라 신뢰도 제고를 위해 학교생활기록부 접근 시 권한관리를 강화하는 방안을 고안하여, 2018년부터 학교생활기록부의 사용자 권한 부여와 변경 시 반드시 학교장의 결재를 받도록 기능개선 하였다.



[그림 Ⅲ-1] 학교생활기록부 권한관리 개선(출처:교육부)

또한 권한부여 현황에 대하여 상시 모니터링 할 수 있도록 권한부여 및 변경 총괄 현황과 항목별 세부현황, 개인별 권한 보유현황 등을 제공하여 권한 관리를 고도화 하였다[7][9].

권한 보유 현황(사용자별/학교별/교육지원청별/교육청별) - 보유 건수

사용자명 사용자ID

사용자명	사용자아이디	시스템	사용자그룹	조직	학년반	교과목	동아리활동	자유학기
테스트	Test0000	3	10	3	1	1	2	0

권한 보유 상세 현황

서브시스템	등록조직	사용자그룹ID	사용자그룹명	부여가능	사용가능	사용여부	적용일자
교무/학사	공통	0000001	사용자그룹1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2017.09.01
교무/학사	○ 고등학교	0000002	사용자그룹2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2017.09.01

클릭시 해당 항목 상세 권한 보유현황 Pop-Up

[그림 III-2] 학교생활기록부 권한관리 모니터링 화면(출처:교육부)

2) 학교생활기록부 접근 인증체계 강화

학교생활기록부 종합전형 확대 등에 따른 학교생활기록부의 신뢰도 및 공정성 제고가 지속적으로 요구되고 있어, 학교생활기록부 입력 권한자에 대한 본인 인증 절차 강화를 위해 금융거래 인증 수준의 2차 인증체계를 2019년부터 도입하여 운영하고 있다.

1차 인증은 교육행정정보시스템 업무포털에 접근하기 위하여 개인별 신원인증서로 접속하고, 2차 인증은 mOTP 또는 ARS 두 가지 방법이 있다.

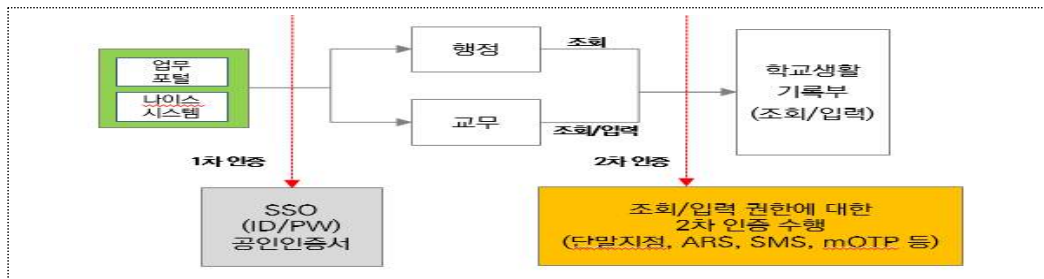
mOTP는 모바일 One Time Password이며 스마트폰 등의 모바일 디바이스에서 일회용 비밀번호를 생성해주는 보안솔루션이다.

ARS는 Automatic Response System(자동응답)으로 사용자에게 필요한 정보를 검색할 수 있도록 음성으로 사용방법을 안내해 준다.

2차 인증 운영 적용 메뉴는 초등학교 성적메뉴에 ‘학기말 종합의견’과 ‘교과 학습발달상황’ 2개 분야이다. 중학교는 성적메뉴에 ‘과목별세부능력 및 특기사항’과 ‘개인별세부능력 및 특기사항’ 2개 분야이다. 고등학교는 성적메뉴에 ‘과목별세부능력 및 특기사항’, ‘개인별세부능력 및 특기사항’, ‘편입/복학생 세부능력

및 특기사항 관리’ 3개 분야이다. 특수학교는 성적메뉴에 ‘과목별세부능력 및 특기사항’, ‘개인별세부능력 및 특기사항’ 2개 분야이다.

해당 메뉴 사용 시 2차 인증 후 허용시간 내 재인증은 불필요하다. 허용시간은 1시간이나, 허용시간이 초과되어도 계속 이용 여부 메시지에 수락을 하면 연장하여 사용이 가능하다[7][8][9].



[그림 III-3] 학교생활기록부 접근 시 2차 인증 절차 체계도(출처:교육부)

3) 학교생활기록부 수정이력 보관 시스템 도입

학교생활기록부 신뢰도 제고를 위하여 수정이 자주 발생하는 정성적 기재영역에 대한 수정이력 보관을 위하여 2019년부터 ‘나이스 학생부 수정이력 보관시스템’을 별도로 구축하여 운영하고 있으며, 수정이력 보관 대상은 ‘교과학습발달상황(‘세부능력 및 특기사항’, ‘특기사항’), 창의적 체험활동 상황, 진로희망사항(희망사유), 자유학기활동상황, 행동특성 및 종합의견, 고등학교/특수학교(고) 진로선택 과목 세부능력 및 특기사항에 대한 수정사항에 대하여 이력관리를 한다.

‘나이스 학생부 수정이력 보관시스템’ 적용 학교급은 초·중·고·특수학교 전체이며, 졸업 후 5년까지 보관하도록 하고 있다.

학생부 수정 이력 현황(학생별/사용자별/학교별/교육지원청별/교육청별) - 수정 건수

학년도: 2017 과정: 주간 계열/학년/학과: 일반계/1/7차일반 반: 1

성명	번호	창의적체험활동				교과학습발달상황				자유학기				행동특성 및 종합의견
		자율	동아리	봉사	진로	일반과목 특기사항	개인별 세부능력	예체능 특기사항	개인별 특기사항	진로 선택	주제 선택	예술 체육	동아리	
김ㅇㅇ	10	2	1	3	4	5	0	3	4	5	1	2	3	4

클릭시 해당 항목 상세 수정 이력현황 Pop-Up

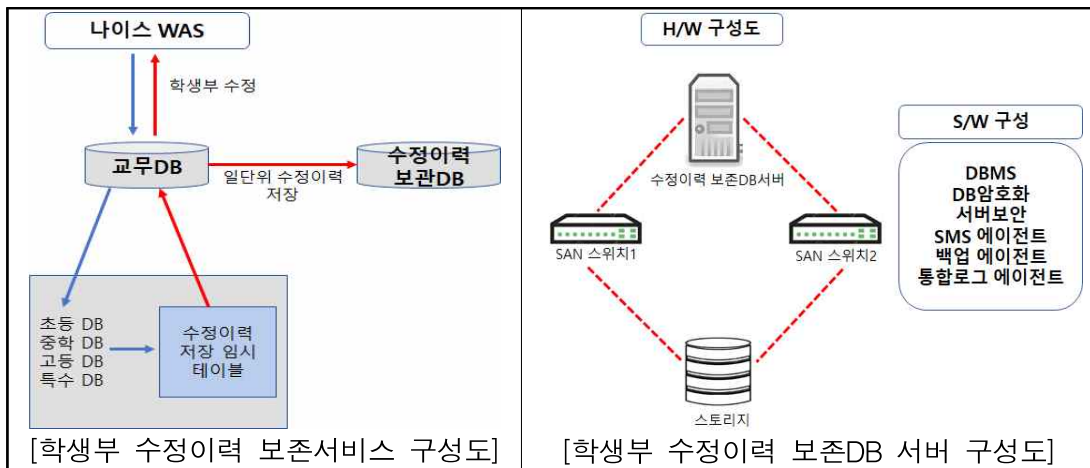
세부항목별 수정이력 상세 현황

자율 동아리 봉사 진로 일반과목 특기사항 개인별 세부능력 예체능 특기사항 개인별 특기사항 진로탐색 주제선택 예술체육 동아리 종합의견

순번	수정구분	수정일시	수정자	이수시간	특기사항	글자수
1	수정	2017.07.11 10:11	Test11	10	자율활동 특기사항 수정사항..	150
2	신규	2017.07.01 14:06	Test11	5	자율활동 특기사항 신규 등록..	200

[그림 III-4] 수정이력 관리 화면 예시(출처:교육부)

‘나이스 학생부 수정이력 보관시스템’은 기존 나이스 시스템과 분리된 시스템을 구축하여 연동하였다. H/W는 서버와 스토리지, S/W는 DBMS, DB암호화, 서버보안, SMS 에이전트, 백업 에이전트, 통합로그 에이전트 등으로 구성하였다.

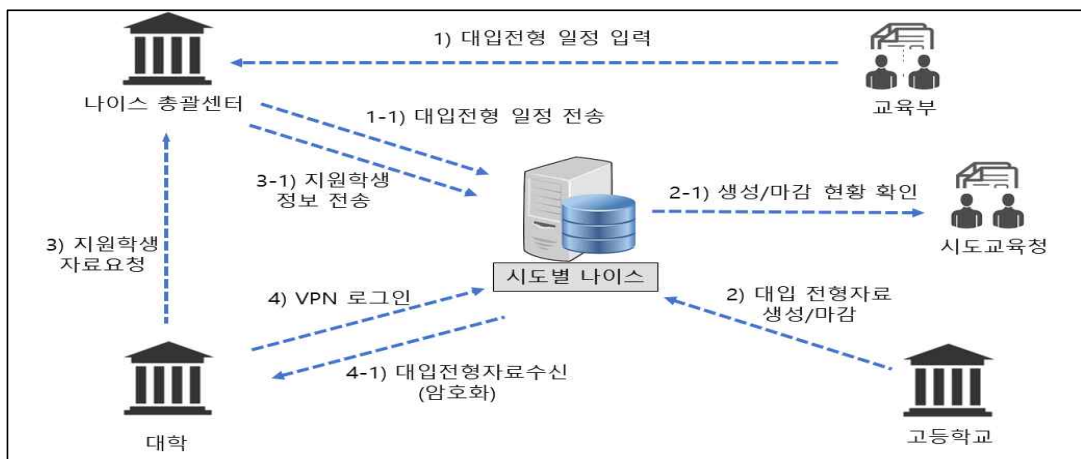


[그림 III-5] 학교생활기록부 이력 보존 시스템 구성도(출처:교육부)

‘나이스 학생부 수정이력 보관시스템’ 데이터 관리는 학생부 수정 후 저장 시 이력을 등록하되, 수정 전/후 학생부 데이터를 저장하며, 수정이력 저장에 따른 업무 프로그램 속도 저하 최소화를 고려하여, 임시 저장 테이블에 보관했다가 일정 시간 간격으로 DB로 이관하여 저장한다[7][9][23].

2. 학교생활기록부 대입전형자료 온라인 제공

고등학교와 대학의 대입전형 업무 부담 감소 및 지원 서류 제출에 대한 학생·학부모의 불편을 해소하고, 학교생활기록부 민원서류 및 성적표 위·변조 방지와 학생 사진 제공을 통한 대리 응시 등 부정행위를 방지하기 위하여 대입전형자료를 온라인으로 대학에 제공하고 있다.



[그림 III-6] 대입전형자료 온라인 제공 구성도(출처:교육부)

2020년 기준 대입전형자료 온라인 제공 대상 범위는 졸업 후 5년으로, 고등학교 3학년 재학생을 포함하여 총 6개 학년도를 제공한다.

제공 내용 및 범위는 학생부 전산자료 중 대입전형에 필요한 내용만으로 제공 범위를 설정하며, 인적사항(학생 본인의 성명·주민등록번호·사진 등 3개 세부 항목만 제공), 학적사항, 출결상황, 수상경력, 자격증 및 체험활동상황, 진로희망사항, 창의적 체험활동상황, 교과학습발달상황, 독서활동상황, 행동특성 및 종합의견 10개 항목이다.

생성 및 제공시기는 매해 6월에 사전운영을 하며, 수시모집시기에는 9월에 생성하여 제공하며, 정시모집시기에는 12월에 생성하여 제공한다.

대학에서는 VPN으로 로그인하여 해당 지원자에 대한 암호화된 대입전형자료를 제공받는다.

대입전형자료 온라인 제공서비스는 학교생활기록부는 2005학년도부터, 검정고시는 2015년부터 시행하고 있으며, 온라인 제공으로 절감되는 사회적 비용은 연평균 1,914억원이라고 한다. 학생/학부모가 자료제출에 따른 대학 방문시간 및 교통비 등 사회적 비용이 연평균 1,630억원 절감되며, 대학에서 전형자료 입력 비용 및 원본대조작업 비용은 연평균 284억원이 절감되는 것으로 예측하고 있다 [4][11].

3. 졸업생 학교생활기록부 이관

교육부 ‘학교생활기록 작성 및 관리지침’ 제18조(자료의 보존)에 따르면 학교생활기록은 학생이 졸업한 후 5년 동안은 학교에서 보관하고 그 이후에는 이관하여 보존·관리하도록 규정하고 있어, 2019년도부터 시·도교육청에서는 졸업 후 5년이 경과한 학교생활기록을 보존·활용시스템으로 이관을 원칙으로 하고 있다.

이 학교생활기록 보존·활용시스템은 2016년도부터 시작하여 2018년도에 구축이 완료되었다.

졸업생 학교생활기록부 보유 현황은 약 2,270만 건이며, 매년 평균 약 190만건을 누적 관리하고 있다.

이관할 학교생활기록은 2019년 기준 2002학년도부터 2013학년도까지 12년간의 자료로서, 정확한 이관과 업무 부담경감을 고려하여 2023년까지 단계적으로 이관할 계획이다[6].

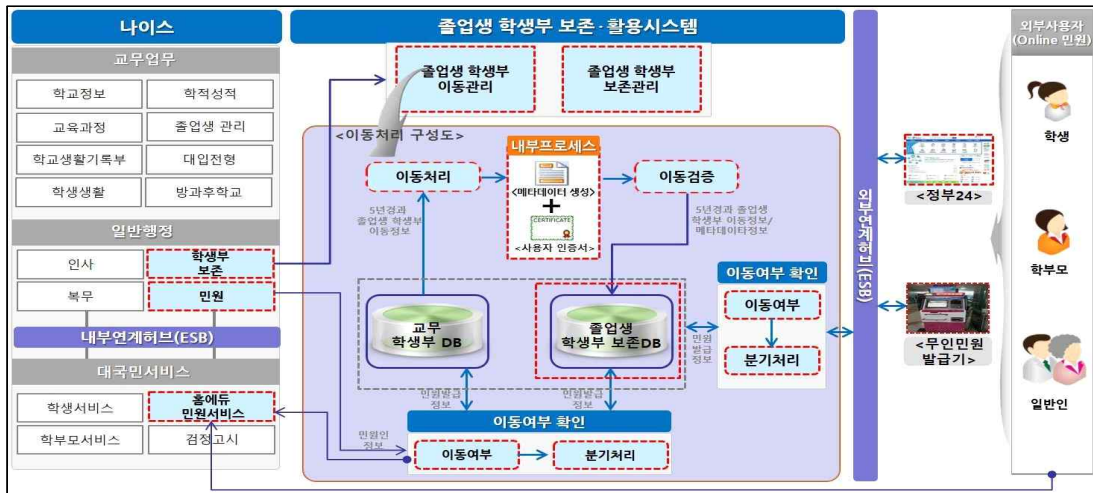
[표 III-1] 졸업생 학교생활기록부 단계적 이관 계획(출처:교육부)

구 분	2019년	2020년	2021년~2023년
이관대상 학교생활기록부	‘02년 졸업생	‘03년 졸업생	‘04~‘16학년도 졸업생
	약 182만 건	약 188만 건	약 2,531만 건
이관 주체	각급 학교	각급 학교	4세대 나이스 구축 자료이관과 연계하여 진행

[표 III-2] 학년도별 · 학교급별 졸업생 현황(출처:교육부)

졸업학년도 (차년도 2월 졸업)	졸업생 수(연도별 교육통계 기준, 명)			합 계
	초등학교	중학교	고등학교	
2002학년도	627,964	597,576	590,413	1,815,953
2003학년도	693,076	600,378	588,550	1,882,004
2004학년도	707,126	616,499	569,272	1,892,897
2005학년도	691,774	612,936	568,055	1,872,765
2006학년도	682,911	677,547	571,357	1,931,815
2007학년도	680,804	690,438	581,921	1,953,163
2008학년도	657,402	674,864	576,298	1,908,564
2009학년도	647,572	668,575	633,539	1,949,686
2010학년도	617,533	668,224	648,914	1,934,671
2011학년도	597,426	645,975	636,724	1,880,125
2012학년도	602,343	635,827	631,197	1,869,367
2013학년도	530,819	606,494	632,983	1,770,296
합 계	7,736,750	7,695,333	7,229,223	22,661,306

졸업생 학교생활기록부 이관은 「교무업무 학교생활기록 DB」에서 자료(학생부 데이터셋, 메타데이터)를 생성하여 보존·활용DB에 저장(학생부 데이터셋, 전자서명된 PDF/A 파일)하는 절차로 처리하며, 이관된 졸업생 학교생활기록에 대한 학생부 정정과 민원발급은 「학생부 보존·활용DB」에서 처리한다[6].



[그림 III-7] 졸업생 학교생활기록의 보존·활용시스템 개념도(출처:교육부)

4. 4세대 나이스 블록체인구현 제안사항

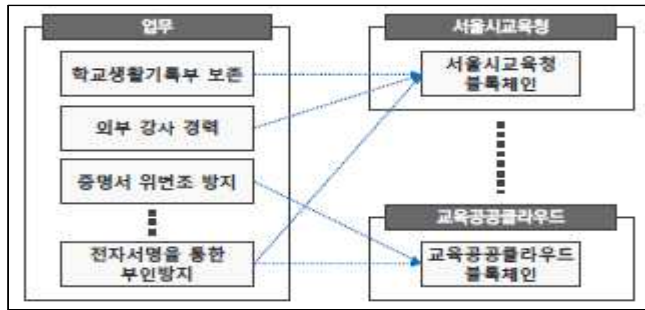
2022년에 개통될 예정인 4세대 나이스는 6개영역 53개 단위업무, 236개 세부업무로 구성될 예정이다. 3세대 나이스는 4개영역 44개 단위업무, 268개 세부업무보다 2개영역이 확대되고 세부업무는 32개가 축소되지만, 학교수업지원플랫폼(6개 대메뉴, 36개 중메뉴)을 확대 제공할 예정이다[5].

3세대			4세대		
영역	단위업무	비고	영역	단위업무	비고
교무업무	교무학사, 입/진학, 보건, 학생부보존 등	7개 단위, 92개 세부업무	교무업무	교무학사(초/중/고), 입/진학, 보건 등	7개 단위, 49개 세부업무
학교행정	장학, 체육, 급식, 정보공시, 교육복지 등	12개 단위, 56개 세부업무	학교행정	교과용도서, 학업중단, 기숙사관리 등	13개 단위, 55개 세부업무
일반행정	인사, 급여, 복무, 민원, 시스템관리 등	21개 단위, 102개 세부업무	일반행정	인사, 급여, 복무, 비공무원급여, 연말정산등	14개 단위, 78개 세부업무
대국민	홈에듀민원, 온라인채용, 학생/학부모서비스 등	4개 단위, 18개 세부업무	대외업무	교육민원, 교직원채용, 교육복지, 교육설문 등	7개 단위, 18개 세부업무
4개 영역 44개 단위, 268개 세부업무			공통업무	코드관리, 사용자관리, 권한관리, 설문관리 등	6개 단위, 20개 세부업무
			연계업무	기관연계, 디지털원패스, 정보개발, 정보공시 등	6개 단위, 16개 세부업무
			6개 영역 53개 단위, 236개 세부업무		
			학교수업지원플랫폼		
영역	대메뉴	비고	영역	대메뉴	비고
수업지원 플랫폼	교사, 학생, 학부모, 교육기관, 자료관리 등	6개 대메뉴, 36개 중메뉴			

[그림 III-8] 3세대와 4세대 나이스 업무 비교(출처:교육부)

4세대 나이스에서는 4차 산업혁명 시대의 핵심 IT기술인 클라우드, 빅데이터, 인공지능(AI), 블록체인 등을 활용한 지능형 정보시스템 구축 필요성이 대두되고 있어, 위변조방지와 부인방지를 위하여 블록체인 기술적용 모델을 검토하고 있다.

블록체인 적용을 검토하고 있는 분야는 각 시·도교육청 및 교육공공클라우드 업무서비스와 문서 위변조방지 및 부인방지를 목적으로 데이터를 효율적으로 관리하기 위하여 블록체인 플랫폼 구축을 제안하고 있다[5][10].



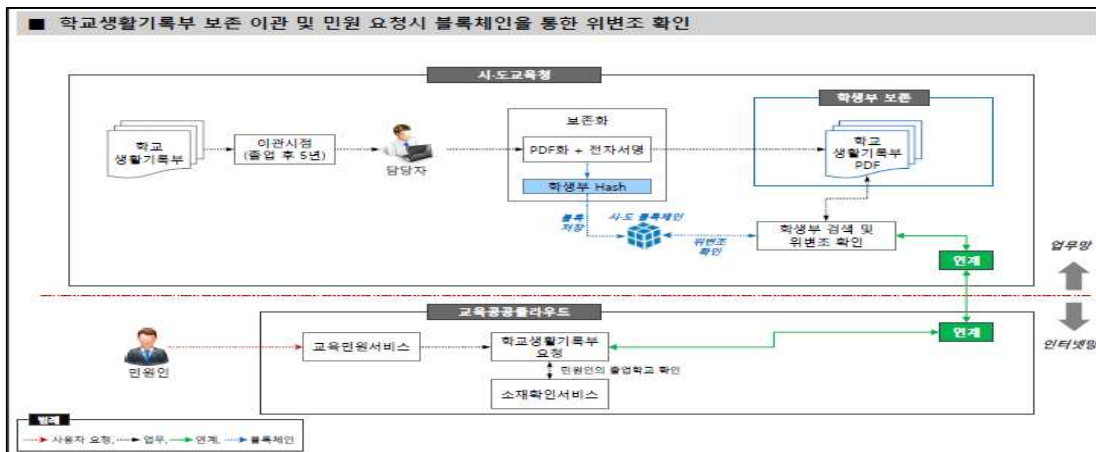
[그림 III-9] 4세대 나이스 블록체인 구현 예상도(출처:교육부)

각 교육청 블록체인은 각 교육청내 블록체인을 활용하는 업무에 대한 플랫폼이며, 교육공공클라우드 블록체인은 전체 시·도교육청이 효율적으로 상호 확인하기 위한 업무에 대한 블록체인 플랫폼이다.

블록체인 구현 시 기대효과는 신기술 적용에 따라 위변조방지 및 부인방지를 보장하며, 블록체인의 분산처리기능으로 안전하고 효율적으로 데이터를 저장하고 관리할 수 있다.

블록체인 구현 시 고려사항으로는 첫째, 필요하다고 판단되는 업무선정 후 블록체인 플랫폼에 적용하고, 둘째, 블록에는 개인정보가 포함된 원본데이터는 저장하지 않으며, 향후 새로운 업무서비스에 추가 적용할 수 있는 확장성이 고려된 블록체인 구조로 설계하여야 한다.

이에, 4세대 나이스 계획에서 학교생활기록부 관련 블록체인 구현모델은 ‘학교생활기록부 보존 이관 및 민원 요청 시 블록체인을 통한 위변조 확인 모델’ 두 가지를 제시하고 있다[5][10].



[그림 III-10] 4세대 나이스 블록체인 구현 방안(출처:교육부)

IV. 학교생활기록부 보안관리 문제점 및 개선방안

학교생활기록부 종합전형 확대 등 상급학교 입학 전형자료로써 학교생활기록부의 신뢰도 및 공정성 제고 요구가 증가함에 따라, 교육부에서 2016년 하반기부터 학교생활기록부 부당 정정 방지를 위한 나이스 시스템 개선방안을 발표하여 시·도교육청에서는 2019년도부터 적용하여 운영하고 있다.

첫째, 권한관리 강화 방안으로 학교생활기록부의 사용자 권한 부여·변경 시, 학교장의 결재를 받도록 하고, 권한부여 현황에 대한 상시 모니터링을 할 수 있도록 개선하였다.

둘째, 학교생활기록부 나이스 시스템 인증체계 강화 방안으로 학교생활기록부 입력 권한자에 대한 본인 인증 절차를 강화하기 위하여 금융거래 인증 수준의 2차 인증체계를 도입, ARS 또는 mOTP 두가지 방법으로 접근하도록 개선하였다.

셋째, 학교생활기록부 수정이력 보관방안으로 입력·수정 이력 보관 시스템을 구축하여 수정이 자주 발생하는 정성적 기재영역에 대한 수정이력을 별도 보관하는 저장공간을 확보하였다.

학교생활기록부에 대한 신뢰도와 공정성 향상을 목적으로 운영체계를 개선하여 이전보다 더 강화된 보안체제로 신뢰도는 향상되었으나 세 가지 측면의 한계점이 존재한다.

첫째, 기존 RDB시스템 구조에 추가된 기능개선으로 권한부여시 학교장 필수 결재를 받아야하고, 2단계 인증을 거쳐야하는 학교사용자의 불편함이 있다. 둘째, 기존 교무업무시스템에 수정이력시스템 장비가 추가되어 시스템 관리대상이 증가하였다.

셋째, 학교생활기록부 위변조방지와 부인방지, 접근통제를 위한 근본적인 기술적 해결방안으로 신뢰성 확보가 필요하다.

따라서 본 장에서는 현재 학교생활기록부시스템 운영·관리상의 문제점을 살펴보고 근본적인 기술적 해결방안으로서 블록체인 도입방안을 제안하고자 한다.

1. 학교생활기록부 보안관리 문제점

1) 학교생활기록부 접근 시 2차 인증

교육행정정보시스템에 신원인증서로 1차 인증한 후에 학교생활기록부 성적메뉴에 접근할 때는 mOTP 또는 ARS 인증, 두 가지 방법 중 하나로 2차 인증을 해야 접속할 수 있다.

전국 440,000여명의 교직원이 2차 인증으로 생활기록부 성적메뉴에 접근하여야 하며, ARS서비스 임대운영비가 전국 2천6백여만원이 소요될 예정이라고 한다.

교사가 학교생활기록부 접근을 위하여 2차 인증을 거치는 것은 보안측면에서 불편함을 감수하여야 하나, 사용자 용이성 측면에서는 접근성이 용이하지 않으므로 불편함이 있다. 또한, 학교생활기록부 전체가 아닌 일부 메뉴에만 적용하고 있어, 학교생활기록부 위변조 방지와 부인방지를 위한 최소한의 제어기능이라고 할 수 있다.

[표 IV-1] 1인 교사가 성적 기록 시 연간 접속횟수 및 시간 예측(초등)

구분		내용	비고
조 건	관리 학생수	평균 30여명	
	성적 등록 횟수	연 2회 이상	학기말
	1인당 성적입력 시간	20분	예상소요시간
	2차 인증 유지시간	60분(1시간)	연장 가능
30명 성적입력 시간		30명×20분=600분(10시간) → 1시간단위로 2차인증 → 결론은 10회 2차인증	한 학급에 30명 인원 예상
연2회 성적 등록		→ 연 20회 이상 2차인증 시도	최소 횟수

[표 IV-1] 기준으로 1인 교사가 학교생활기록부 성적 기록을 위하여 연간 접속횟수를 예측해보면 연2회(학기말) 성적 기록을 하고 반기당 최소10회, 연 20회 이상 2차 인증을 하여야 한다.

반기 1회당 10시간을 기록하여야 하는데 2차인증 유지시간이 1시간이므로 이론적으로는 10회이지만 성적기록을 10시간동안 지속적으로 하기는 불가능므로, 10회이상 2차인증 또는 연장메세지 클릭을 해야 하는 불편함을 예측할 수 있다.

2) 학교생활기록부 수정이력 보관

학교생활기록부 내용의 신뢰성 제고를 위하여 수정이 자주 발생하는 정성적 기재영역에 대하여 수정이력을 보관하기 위하여 시·도교육청에서는 별도 수정이력보관 시스템을 구축하여 운영하고 있다.

수정이력 내용을 저장할 별도 스토리지와 DB서버, 스위치, DB암호화, DB접근 제어, 서버보안 등의 보안SW가 필요하다. 이는 기존 학교생활기록부를 기록 저장하는 교무업무 DB서버와 기타 장비이외에 학교생활기록부 수정이력 저장을 위한 장비가 추가되어, 시·도교육청에서는 물적기반 관리사항이 증가하게 된 것이다.

별도로 구축한 학교생활기록부 수정이력 DB구성은 수정이력을 해당DB에 임시테이블을 생성하여 저장 후 일정시간 간격으로 이력보존DB로 복사하여 저장하는 구성이다.

[표 IV-2] 연간 교무업무 및 학교생활기록부 수정이력 DB 사용량 예시

구분	교무업무DB 사용량	학교생활기록부 수정이력 DB 사용량
제주교육청 연간DB 사용량	78GB(565-487)	20GB

[표 IV-2]에서는 제주교육청 사례로 학교생활기록부가 포함된 교무업무 연간 DB사용량은 78GB이고, 학교생활기록부 수정이력이 저장된 DB사용량은 20GB이다 교무업무DB의 1/4정도의 용량이 필요하다. 따라서 교무업무 DB이외에 수정이력 DB가 매해 증가하게 되므로 자원증설 시기는 더 빨라질 것이고, 별도 백업관리 등의 자원관리 사항이 증가할 것이다.

3) 대입전형자료 온라인 제공

학교생활기록부는 대입전형의 기준이 되므로 매해마다 정시와 수시전형에 전국 400여개 대학에 대입전형자료를 온라인으로 제공하고 있다.

제공 절차는 교육부에서 대입전형 일정을 진송하면, 고등학교에서는 학교생활기록부 대입전형자료를 생성하여 검증한 후 마감하고, 교육청에서는 관할 고등학교 대입전형자료 총괄 마감현황을 확인하며, 전국 대학교에서는 17개 시·도교육청 나이스시스템에 VPN으로 접속하여 지원학생에 대한 대입전형자료를 암호화 통신으로 제공받는다[4][11].

대입전형자료 온라인 제공은 종이 학교생활기록부로 접수하던 과거와는 달리 연평균 1,914억원이라는 사회적 비용이 절감되고 업무처리방식의 획기적인 변화를 가져왔으나, 전국 대학교에서는 17개 시·도교육청 개별 나이스시스템에 접속하여 해당 자료를 가져와야 하는 불편함이 있으며, 전용회선이 아닌 VPN통신으로 전송함에 따른 불안정성을 내포하고 있다.

전국 대학에서 시·도교육청 시스템에 연간 2회 이상 접속한다면, VPN통신 구간에 대한 해킹 등의 보안사고를 방지하기 위하여 보안관리가 철저히 이루어져야 한다.

전국 2,500여 고등학교에서도 매해마다 정시와 수시에 학교생활기록부 대입전형자료를 생성하여 점검과 마감처리 작업을 하고, 대학에 제공한 이후에는 초기화하기 전까지 데이터관리를 철저히 해야 하는 등의 관리단계가 복잡하여 교원 업무가 부담되는 측면이 있다.

[표 IV-3] 고등학교에서의 대입전형자료 관리 현황

구분	대입전형자료 관리 기간	데이터관리
수시 전형	매해 9월(생성) ~ 12월(초기화)/ 4개월	생성,보관,초기화
정시 전형	매해 12월(생성) ~ 익년도 3월(초기화)/4개월	생성,보관,초기화

대학에서 접근을 허용하는 대입전형자료 제공을 위한 블록체인 네트워크를 구현한다면, 대학에서 개별 시·도교육청을 접속할 필요없이 블록네트워크에서 제공받을 수 있으며, 시·도교육청 시스템도 안정적 보안구성으로 관리업무가 경감될

것으로 예측할 수 있다.

[표 IV-4] 대입전형자료 온라인 제공 건수(출처:교육부)

(단위: 건)

학 년 도	학생부					검정고시			총계
	대상고교 수		수시	정시	소계	수시	정시	소계	
	수시	정시							
'05	-	2,037	-	1,419,094	1,419,094	-	-	-	1,419,094
'06	2,066	2,067	1,681,690	1,322,324	3,004,014	-	-	-	3,004,014
'07	2,135	2,131	1,769,799	1,353,277	3,123,076	-	-	-	3,123,076
'08	2,188	2,182	2,157,941	1,909,636	4,067,577	-	-	-	4,067,577
'09	2,263	2,255	2,501,590	1,426,948	3,928,538	-	-	-	3,928,538
'10	2,268	2,254	3,085,430	1,703,690	4,789,120	-	-	-	4,789,120
'11	2,307	2,297	3,764,737	1,899,012	5,663,749	-	-	-	5,663,749
'12	2,344	2,323	4,546,068	1,408,781	5,954,849	-	-	-	5,954,849
'13	2,373	2,344	3,546,180	1,182,102	4,728,282	-	-	-	4,728,282
'14	2,393	2,368	3,472,280	987,444	4,459,724	-	-	-	4,459,724
'15	2,432	2,440	3,851,648	980,603	4,832,251	122	4,191	4,313	4,836,564
'16	2,449	2,421	3,512,601	895,595	4,408,196	13,611	7,033	20,644	4,428,840
'17	2,460	2,443	3,791,477	739,514	4,530,991	5,762	2,981	8,743	4,539,734
'18	2,471	2,451	3,833,475	655,959	4,489,434	17,071	5,873	22,944	4,512,378
'19	2,459	2,439	4,119,987	586,735	4,706,722	22,978	7,429	30,407	4,737,129
'20	2,451	2,437	3,745,937	-	3,745,937	26,947	-	26,947	3,772,884
계			45,634,903	18,470,714	64,105,617	59,544	27,507	87,051	64,192,668

4) 학교생활기록부 신뢰성 부족

17개 시·도교육청이 2015~2018년 사이에 진행한 학교 감사결과, 고등학교에서 시험지 유출이 숙명여고를 포함해 모두 13건으로 적발되어 징계를 받은 교사와 학생이 13명이다. 또한 학교생활기록부 기재 시 관련 규정을 어기거나 부당하게 정정하여 적발된 사례도 15건이 있다고 한다. 2015년에는 경기 분당 대진고에서 교무부장이 딸의 학생부를 조작했다가 파면된 사례도 있었다.

2019년에는 모 법무부장관 후보 딸의 학교생활기록부가 본인의 동의없이 유출되어 정치권의 이슈로 사용되는 등으로 학교생활기록부 위변조와 유출사건이 간헐적으로 생기고 있어 학교생활기록부 데이터 관리에 대한 사회적 신뢰도는 떨어지고 있다.

학생생활기록부는 학생의 학교생활 전반의 교육활동과 함께 개인의 성장과정이 매우 세밀하게 기록되어 있는 중요한 개인정보이며 교육활동 결과물이므로

이에 대한 관리사항의 중요성은 더 부각되고 관심의 대상이 될 수 밖에 없으며 신뢰도 제고 요구가 증가하고 있다.

이에 교육부와 시·도교육청에서는 이를 보완하고자 나이스 보안관리체계 강화를 위하여, ‘학교생활기록부 권한관리 강화’, ‘학교생활기록부 성적메뉴 접근 시 2차 인증체계 도입’, ‘학교생활기록부 수정이력보관’을 도입하였다.

그러나 이 보안관리체계 강화 방안은 현재 RDB시스템 구조에서 부분 확대한 방안일 뿐이며, 중앙집중형 데이터 관리 구조를 유지하고 있으므로 슈퍼관리자에 의한 접근과 수정시도라는 위험성이 항상 존재하며, 중앙시스템에만 의존하므로 치명적 시스템 오류 시 전체 데이터가 훼손될 수 있는 구조이다.

따라서 중요한 데이터인 학교생활기록부의 위변조방지와 훼손방지를 위한 보다 더 발전된 형태의 기술적 개선방안을 적용하여 신뢰성 확보가 필요하다.

2. 학교생활기록부 보안관리 개선방안 및 고려사항

본 절에서는 학교생활기록부 보안관리 방안의 한계점 개선을 위하여 블록체인 기반 학교생활기록부 시스템 운영 모델을 개선방안으로 제안하고자 한다.

1) 블록체인 기술적 적용방안

학교생활기록부에 대한 접근은 허가된 조직에서만 접근하여야 하므로 프라이빗 블록체인으로 구성하여야 하며, 위변조방지를 위한 참여자의 접근 권한이 제어가능 하여야 하며 신뢰성과 무결성이 보장되어야 한다.

따라서 허가형 블록체인 중에서 업무프로세스를 구현하기에 적합한 하이퍼레저 패브릭 기술적용을 제안하고자 한다.

하이퍼레저 패브릭은 오픈소스이며 프라이빗 블록체인으로 현재 엔터프라이즈 환경에서 가장 범용적인 블록체인기술로 채택되어 사용되고 있다. 특정 기업이나 정부 기관이 지정한 참여자만 블록체인 네트워크에 참여할 수 있고, 일반언어인

Java 개발 환경 지원과 기존 Legacy 시스템 연결을 쉽게 할 수 있으며, 기업(조직)이 요구하는 높은 성능과 필요한 기술요소들을 많이 제공하고 있기 때문이다.

하이퍼레저 패브릭은 정부의 가상화폐 규제정책을 준수하며 특정 가상화폐 생태계로부터의 독립성을 가진다. 즉, 코인이나 토큰에 기반한 블록체인이 아니므로, 트랜잭션을 발생할 때 암호화폐를 이체할 필요가 없다.

[표 IV-5]는 비허가형 블록체인인 이더리움과 허가형 블록체인인 하이퍼레저 패브릭과의 차이를 나타내는 것이며 하이퍼레저 패브릭의 특징을 중심으로 살펴보고자 한다[27][29][30].

[표 IV-5] 이더리움과 하이퍼레저 패브릭 비교

구분	이더리움	하이퍼레저 패브릭
유형	비허가형	허가형
프로그램 이름	스마트 계약(Smart Contract)	체인코드(Chaincode)
프로그램 형태	결정적(deterministic)	비결정적(non-deterministic)
내부 통화	있음(ETH)	없음
거래 수수료	있음(gas)	없음
프로그램 언어	자체 언어(Solidity)	일반 언어(Go, Java, Node.js)
거래 처리방식	순차적	병렬적
합의 알고리즘	작업 증명(PoW)	비작업 증명(SOLO, Kafka, 등)
결제 완료시간	1분 이상	즉시
멀티 블록체인	미지원	지원
업그레이드	불가능	가능
의존성	오픈소스	오픈소스(IBM)
멤버십	address	x.509

첫째, 하이퍼레저 패브릭은 일반 프로그래밍 언어를 사용할 수 있다. 이더리움은 모든 피어(peer)의 블록체인에서 실행된 스마트 계약의 결과가 항상 동일한 것을 보장하기 위해 결정적(deterministic) 프로그래밍 언어인 Solidity를 특별히 개발하여 사용하고 있으나, 하이퍼레저 패브릭은 스마트계약 프로그램을 체인코드(chaincode)라고 하며, Go, Java 등 일반적인 프로그래밍 언어를 사용할 수 있다.

둘째, 하이퍼레저 패브릭은 내부 가상통화가 없다.

이더리움에서는 많은 참여자의 참여를 유도하기 위해 수수료(인센티브)가 필요

하여 거래 수수료를 지불한다. 프라이빗 블록체인은 원하는 참여자만 참여하기 때문에 수수료(인센티브)가 필요 없으므로 비작업 증명 방식으로 합의한다.

셋째, 하이퍼레저 패브릭은 높은 성능을 보인다. 서로 다른 보증 피어들을 통해 체인코드를 실행하는 다수의 거래들을 동시에 처리가 가능하므로 상대적으로 높은 성능을 구현한다.

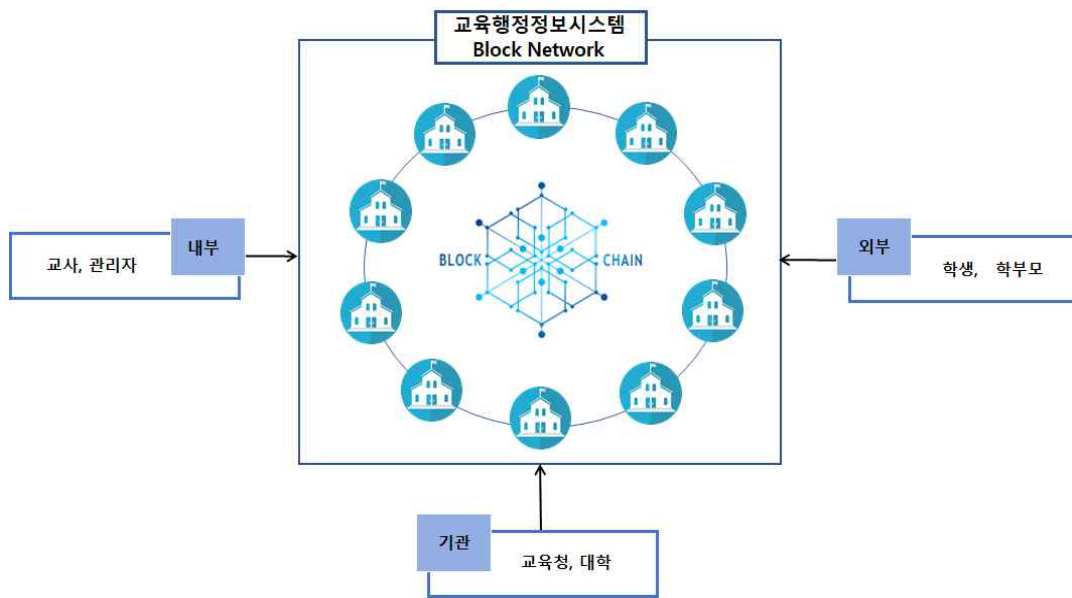
넷째, 교체 가능한 모듈 구조이다. 하이퍼레저 패브릭은 전체 시스템을 모듈 구조로 설계하고, 합의 알고리즘 등 응용에 따라 요구사항에 차이가 큰 모듈을 필요에 따라 교체 가능하며, 합의 프로토콜에는 SOLO, Kafka, PBFT(Practical Byzantine Fault Tolerant) 등이 있다.

다섯째, 멀티 블록체인을 지원한다. 전체 시스템을 다수의 채널(channel)로 구분하여 채널별로 별도의 독립적인 블록체인을 유지하며, 참여자는 특정 채널에 가입함으로써 공유할 블록체인을 선택할 수 있고, 다수의 채널에 가입이 가능하다.

여섯째, 멤버십 관리 서비스를 통해 허가된 참여자만 접근을 허용한다. 허가된 참여자에 대해 블록체인 접근 권한 제어가 가능하다. 참여자 행위에 대한 책임성(accountability) 확인의 요구사항을 반영할 수 있다. PKI기반의 멤버십 서비스를 제공하여 참여자에게 책임 부여와 감사가 가능하며 부인방지가 가능하다.

일곱째, 작업 증명 기반의 합의 알고리즘을 사용하는 대신 보다 효율적인 합의 알고리즘을 사용한다. 하이퍼레저 패브릭은 거래는 승인이 완료되는 즉시 거래가 완료되어 비허가형 블록체인보다 높은 거래 완료성(transaction finality)을 보인다.

이러한 특징을 가진 하이퍼레저 패브릭 블록체인으로 제안하고자하는 학교생활기록부 관리시스템은 분산원장으로 데이터를 관리하며, 허가된 참여자만 접근 가능하도록 한다. 학교생활기록부를 작성 및 수정하거나 열람하는 권한은 멤버십 서비스에서 인증받은 클라이언트(Client)를 통해서만 가능하도록 설계한다.



[그림 IV-1] 교육행정정보시스템 학교생활기록부 블록체인 구성도

학교생활기록부시스템을 이용하는 사용자는 내부적으로 학교생활기록부를 기록하는 교사와 접근 승인을 관리하는 학교 관리자로 나눌 수 있다. 외부적으로는 학생의 학교생활기록부 열람 조회가 가능한 학생과 학부모가 있다. 그리고 전입학 및 대학진학자료 이용을 위한 교육청, 대학 등 기관으로 나눌 수 있다.

이들 사용자는 하이퍼레저 패브릭의 멤버십서비스에서 인증과 권한을 받아야 생활기록부 블록체인에 접근할 수 있으므로 현재 시스템에서의 ‘권한강화방식’과 ‘2차인증’에 대한 불편함을 해결할 수 있다.

또한, 블록원장에 블록생성시간과 블록 수정이력 등이 포함되어 있으므로 ‘생활기록부 수정이력 보관’ 문제점을 해결할 수 있다.

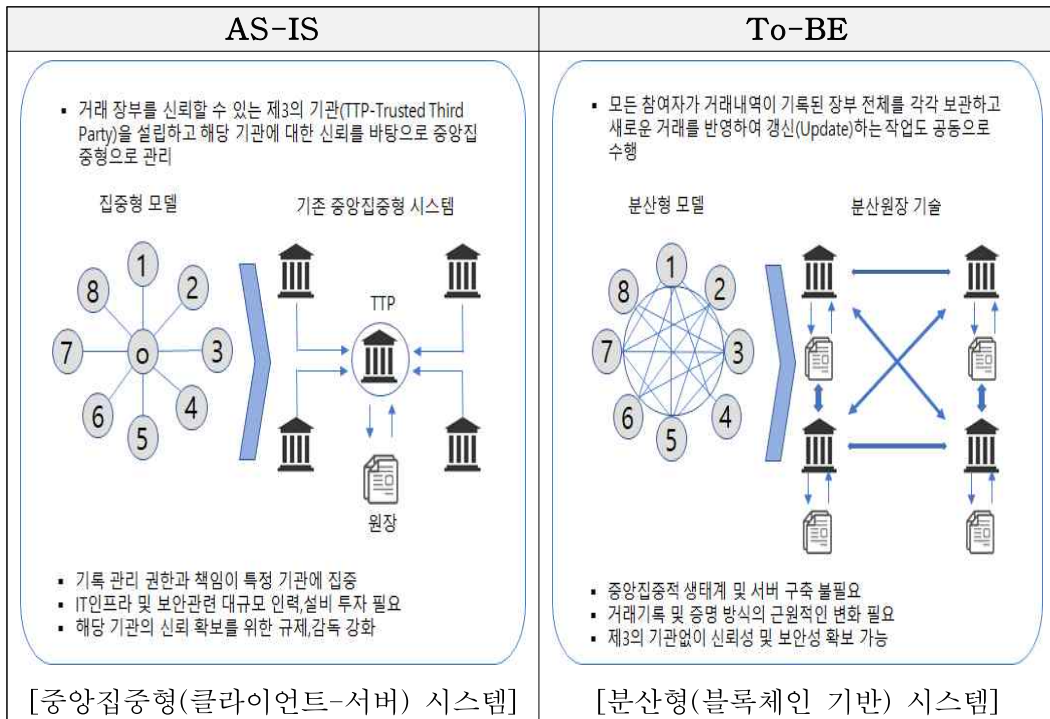
무엇보다 학교생활기록부 데이터에 대한 신뢰가 높아질 수 있다.

기존 중앙집중형 시스템에서는 신뢰 확보를 위하여 기관의 규제 및 감독 강화와 대규모 인력과 설비 투자가 필요로 하였다면, 블록체인기반 시스템에서는 기술적으로 모든 참여자가 거래기록을 각각 보관하고 거래증명을 공동으로 수행함으로써 제3의 기관없이 보안성 확보가 가능하여 학교생활기록부 부당정정 및 유출방지에 더 효과적이라 할 수 있어 학교생활기록부 데이터에 대한 신뢰도가 보다 더 향상될 것으로 기대한다.

2) 블록체인 기술 적용 시 장점

본 연구에서는 학교생활기록부 데이터관리를 블록체인네트워크 모델로 제안하여 학교생활기록부시스템 신뢰성 확보를 위해 현행 시스템에서의 한계점을 개선하려고 한다.

현재 교육행정정보시스템은 중앙집중형시스템이며, 제안하는 블록체인 기반 학교생활기록부시스템은 분산형시스템으로서 [그림 IV-2]은 현재 시스템 대비 본 연구에서 제안하는 블록체인 시스템 차이를 나타낸 것이다[25].



[그림 IV-2] 중앙집중형 시스템과 분산형 시스템 비교

AS-IS 시스템은 중앙에서 정보를 관리했다면 TO-BE시스템은 탈 중앙화 형태로 정보를 분산원장으로 관리하게 한다.

TO-BE시스템에서는 허가된 참여기관만 참여가 가능하도록 하여, 각각의 역할과 프로세스에 대해 정의한다.

제안하는 블록체인기반 학교생활기록부 데이터는 분산되어 동일하게 저장된 공개 데이터베이스(블록체인)에 문서 서명(해시)과 함께 보관할 수 있으므로 다음과 같은 중요한 장점을 가질 수 있다.

첫째, 위변조할 수 없다. 학교생활기록부를 기록 및 수정한 작업에 대한 이력이 블록에 저장되기에 원본임을 확인할 수 있다.

둘째, 블록체인에 기록된 생활기록부는 소프트웨어를 호스팅하는 모든 컴퓨터에 있는 모든 사본이 파괴된 경우에만 폐기될 수 있다.

셋째, 해시는 사용자가 보유하고 있는 원본 문서에 대한 ‘링크’를 만드는 방법일 뿐이다. 즉 위의 메카니즘을 사용하면 문서자체를 게시할 필요 없이 문서의 서명을 게시할 수 있으므로 문서의 개인정보가 보호된다.

넷째, 다수의 검증으로 객관성이 확보된다. 학교생활기록부는 교육기관 및 검증 기관등과 같은 제3자가 검증할 수 있다.

다섯째, 영속성이 보장된다. 학교생활기록부는 블록체인 기반 영구적인 기록이 가능하다.

3) 블록체인 기술 적용 시 고려사항

본 연구에서 학교생활기록부 신뢰성 확보를 위한 하이퍼레저 패브릭 블록체인 기술구현을 제안하고자 하여, 2항에서는 블록체인 기술 적용 시 장점과 기대효과를 살펴보았으나, 본 항에서는 반대 측면으로 하이퍼레저 패브릭 기술을 적용할 경우의 고려사항에 대하여 검토해 보고자 한다.

한국예탁결제원에서는 2018년 9월에 ‘채권장외결제시스템 블록체인기술 적용 타당성검토를 위한 컨설팅’ 실시 결과 발표 자료에 의하면, 하이퍼레저 패브릭 블록체인 기술을 적용하여 모의테스트한 결과 [표 IV-6] 에서와 같이 검증항목에 따라 현행시스템보다 블록체인 시스템에서의 부족한 점을 도출하였다[25].

[표 IV-6] 블록체인 기술적용 결과 현행시스템과 비교 시 상대적 단점[25]

구분	항목	현행 시스템	블록체인 시스템
성능	거래처리 성능	이중화 및 부하분산 등 시스템 최적화	트랜잭션에 대한 Consensus(합의) 및 Peer간 원장동기화로 인하여 성능이 떨어짐 (평균50배 처리시간 소요)
확장성	Peer 확장성	참여기관 추가에 따른 하드웨어, 소프트웨어 설치 불필요	참여기관 추가 시 하드웨어/소프트웨어 설치 필요, 블록크기에 따라서 상당한 동기화 시간 소요
유지 보수	개발/배포 용이성	지원 솔루션 고도화	지원 솔루션 부족 (개발기간 상당소요, 개발 진행 가이드라인 부족)
	모니터링 용이성	다양한 모니터링 도구 지원	모니터링 도구 부족, 추가 개발 필요
투자 비용	도입/유지비용	초기투자비용: 중앙운영기관 높음 운영유지비용: 중앙운영기관 높음	초기투자비용: 참여기관별 노드구성 위한 비용발생 운영유지비용: 참여기관별 일정 수준의 유지비용발생

첫째, 거래처리 성능은 트랜잭션에 대한 Consensus(합의) 및 Peer간 원장동기화로 인하여 현행시스템보다 평균50배 처리시간이 소요되어 성능이 떨어진다는 테스트 결과가 나왔다.

둘째, 확장성 측면에서 현행시스템은 참여기관이 추가되어도 H/W 및 S/W추가 설치가 불필요하나, 블록체인 시스템은 추가 설치가 필요하고 참여기관 추가로 블록크기에 따라서 상당한 동기화 시간이 소요된다.

셋째, 아직까지는 개발 진행 가이드라인 등, 지원 솔루션이 부족하여 개발기간이 상당히 소요되어 개발과 배포가 용이하지 않다.

넷째, 운영을 위한 관리 모니터링 도구가 부족하여 추가 개발이 필요하며 모니터링이 용이하지 않다.

다섯째, 투자비용측면에서 현행시스템은 중앙운영기관이 높은 비용이 필요하며, 블록체인시스템은 참여기관별로 비용이 발생한다는 차이점이 있으나 과도한 추가 운영

/유지보수 비용이 발생할 가능성이 있다고 검토되었다.

하이퍼레저 패브릭 블록체인은 기존 블록체인보다 병렬적 처리로 처리시간이 단축되어 성능이 높다고 할 수 있으나, 현행 시스템과 비교하여서는 성능이 떨어진다는 테스트 사례가 있고 일반적인 평가이다. 하지만 워털루 대학 연구진이 하이퍼레저 패브릭 TPS(Transaction Per Second)를 7배 늘린 연구결과가 발표되는 등 지속적인 성능개선을 기대할 수 있다[32].

어플리케이션 개발지원 솔루션이 부족하여 개발이 용이하지 않으며, 운영을 위한 모니터링 도구가 부족하고, 참여기관 추가 시 상당한 동기화 시간이 소요되는 단점은, 오픈소스이며 신생 기술이므로 안정화되어 있지 않기 때문이라 할 수 있다.

또한 블록체인도 변조가 가능할 수 있다는 연구와 주장이 있기에, 하이퍼레저 패브릭 기술도 변조의 가능성은 없는 지에 대한 실증연구 결과가 필요하며 향후 커뮤니티가 더 다양하게 발달하여 지속적인 연구와 발달이 필요하다는 한계점이 있다.

본 연구에서는 하이퍼레저 패브릭 기반 블록체인 학교생활기록부 시스템을 제안하지만, 신생 기술로서의 한계점을 극복하기 위해서 실제 적용하기 전에 성능 등의 타당성검토를 위한 ISP(Information Strategy Planning, 정보화전략계획)을 선제적으로 실시하는 것이 필요하다.

V. 학교생활기록부 블록체인 구현 방안

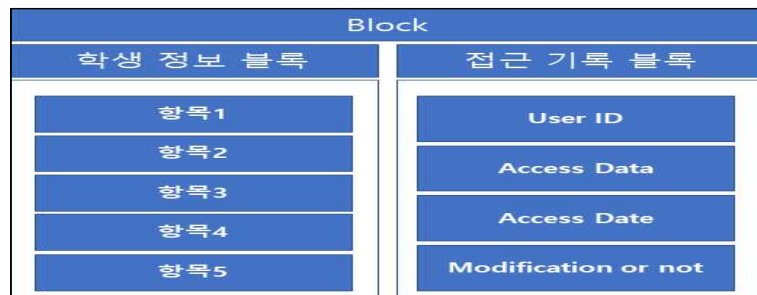
본 장에서는 블록체인기술을 적용한 학교생활기록부 구현방안에 대하여 제안한다. 제안하는 기법의 네트워크는 프라이빗 블록체인으로 구성하였다.

블록체인 참여자는 신뢰할 수 있는 인증기관(CA)을 통해 인증서를 발급받아야 네트워크에 참여할 수 있다. 생성된 블록은 네트워크 참여자가 공통으로 소유하고 있는 분산원장에 기록된다. 이러한 기술을 기반으로 하는 블록체인을 활용하여 학교생활기록부를 관리하는 기법을 제안한다.

1. 학교생활기록부 블록체인 제안

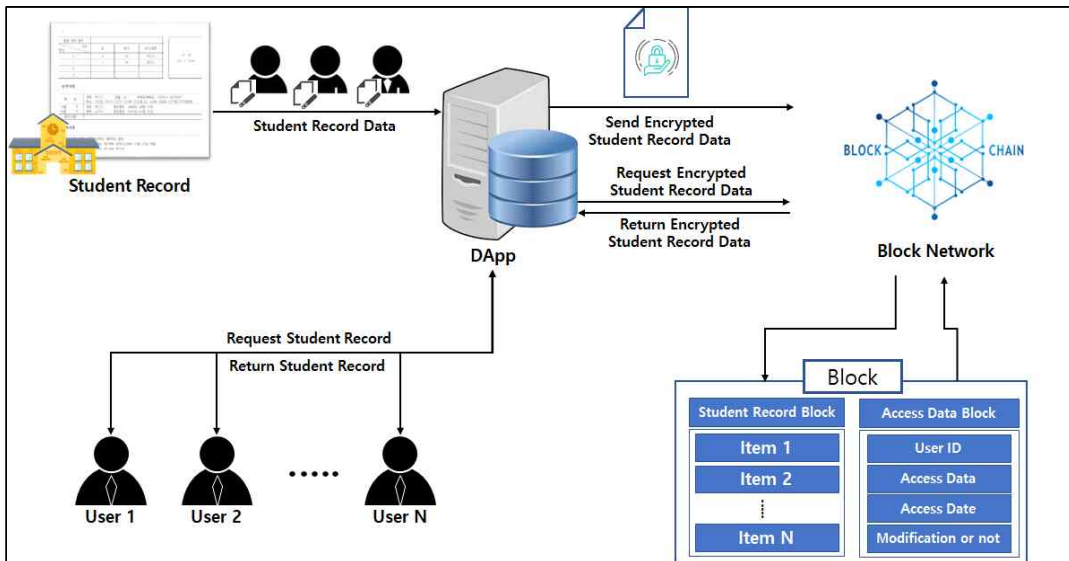
1) 학교생활기록부 블록체인 메커니즘

제안하는 블록체인 기반의 학교생활기록부 데이터 보호기법은 기존의 일반적인 RDB(Relation Database)에 학생의 생활기록부 기록을 암호화 저장하여 관리하는 기법에 대해 블록체인을 적용함으로써 생활기록 데이터에 대한 무결성을 보장하고, 데이터의 위·변조를 방지함을 목적으로 한다. 제안된 메커니즘은 프라이빗 블록체인을 적용하며, 생성되는 블록은 학생의 생활기록부에 대한 정보를 가지는 학생 정보 블록과 학생정보에 접근하는 사용자의 정보를 기록하는 접근 기록 블록의 두 종류의 블록 데이터를 생성한다. [그림 V-1]는 생성되는 블록을 가시적으로 보이는 것이다[12].



[그림 V-1] 두 종류의 블록데이터

본 논문에서 제안하는 메커니즘은 학교에서 작성된 생활기록부의 기록을 교육 행정정보시스템 블록체인 네트워크 분산애플리케이션(DApp)을 통하여 입력된 기록은 암호화된 데이터로서 블록네트워크에 기록된다. 블록 네트워크에 암호화되어 기록되어 있는 생활기록부 정보는 정당한 사용자에게 의해 요청될 수 있으며, 사용자의 요청이 들어오면 암호화된 생활기록부를 사용자에게 전송하고, 사용자가 제공된 생활기록부에 대한 이용이 종료되면, 접근기록 블록을 생성하고 수정된 생활기록부에 대한 블록을 생성한다. [그림 V-2]는 메커니즘의 전반적인 구성도를 보이는 것이다[12].



[그림 V-2] 학교생활기록부 블록체인 네트워크 메커니즘

교육행정정보시스템 블록체인 네트워크 시스템에서 요구하는 보안사항은 첫째, 신원관리(Identity)로서 업무사용을 위해서는 참가자의 신원 확인이 필요하여 참가자의 정체성과 특성 확인이 가능한 신원인증이 되어야 한다. 둘째, 트랜잭션의 기밀성(Confidentiality)이 보장되어야 하므로 트랜잭션이 암호화되어 일반 사용자에게 보이지 않도록 하여야 한다. 셋째, 재생(Replay)공격 대책으로 과거의 트랜잭션을 복사하여 재전송하는 공격을 방지할 수 있어야 한다. 넷째, 개인정보보호로 트랜잭션의 발행자의 익명화, 동일한 사용자가 발행한 여러 트랜잭션들은 연

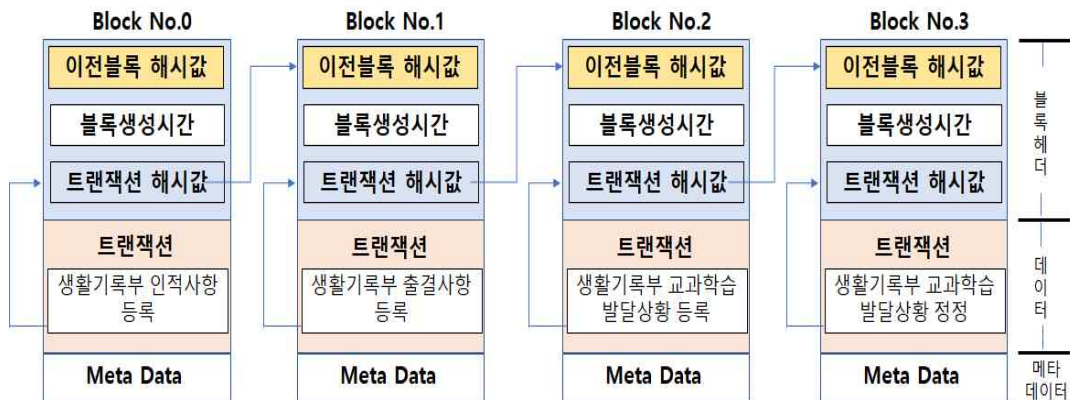
관성이 없도록 해야한다. 다섯째, 액세스 제어로 스마트계약(초기화, 함수 실행, 데이터 참조 등)을 실행할 수 있는 사람을 제한하여야 한다, 여섯째, PKI인증서와 전자서명을 적용하여 사용자의 신원을 확인하여야 하며, 개별 트랜잭션은 익명의 인증서를 통해 신원을 숨긴 채 인증할 수 있어야 한다[21][22].

이러한 교육행정정보시스템 보안요구사항을 충족하기 위해서는 허가형블록체인이 유일한 방법이다.

트랜잭션 발생시에 암호화폐를 이체할 필요가 없으며, 각 노드에 따라 권한을 차별화시키고, 권한이 없는 사용자는 접근할 수 없도록 하는 등의 기능을 도입하기 위하여 현재 발표된 허가형블록체인 중 하이퍼레저 패브릭 블록체인 오픈 소스 플랫폼을 적용한 모델을 제안하고자 한다.

2) 학교생활기록부 블록구조

제안하는 하이퍼레저 패브릭 블록체인 기반 생활기록부 블록체인 네트워크 내에 모든 트랜잭션이 기록되고 공유되는 분산공유원장을 이루는 블록구조는 [그림 V-3]과 같다[16].



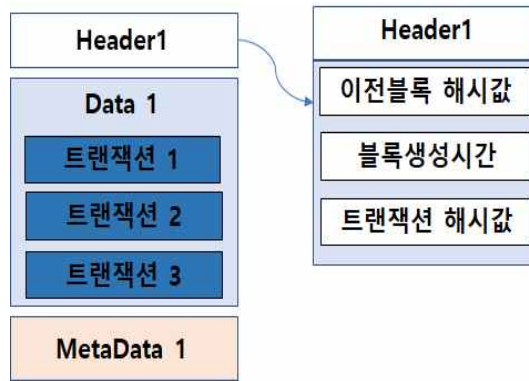
[그림 V-3] 학교생활기록부 블록구조

정해진 용량만큼 혹은 일정시간 동안 발생한 트랜잭션은 하나의 블록이 된다. 블록체인은 이렇게 생성된 블록들이 합의과정을 무사히 마친 후 암호학적 기법을 통해 생성된 순서대로 연결되어 저장되는 데이터이다.

블록헤더에는 현재 발생하고 있는 트랜잭션에 대한 해시값과 이전단계에서 생

성된 블록의 해시값이 포함되어 있다. 이처럼 블록의 해시값이 연결된 데이터 구조에서는 블록에 저장된 데이터를 안전하게 보관할 수 있다. 왜냐하면 첫 번째 블록부터 현재까지의 블록 안에 모든 트랜잭션에 대한 기록이 저장되어 있기 때문에 악의적인 노드가 이전 블록의 값을 변경하려고 시도해도 올바른 블록을 소유한 PEER들의 합의과정에 의해 저지당하게 된다.

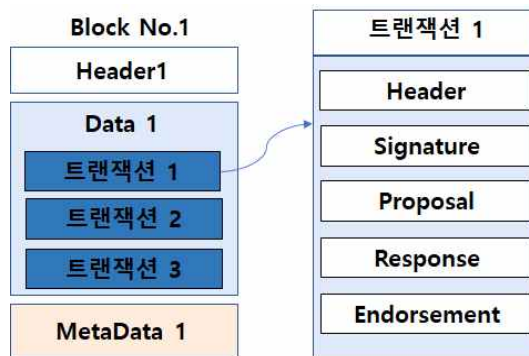
[그림 V-3]은 4개의 블록이 암호학적 해시 기법으로 연결되어 있으며, 각 블록마다 Header, Data, Metadata 필드가 존재한다.



[그림 V-4] 블록 헤더 구조도[16]

먼저 블록 헤더는 네가지 항목으로 구성되어 있다.

Block number는 0부터 시작하여 합의과정에 의해 블록이 생성될 때마다 숫자가 1씩 증가하게 된다. 트랜잭션 해시값(Current block hash)은 현재 블록에 포함되어 있는 트랜잭션의 해시값이며, 이전 블록에 대한 해시값(Previous block Hash)과 블록 생성시간(Timestamp)으로 구성된다.



[그림 V-5] 블록 트랜잭션 구조[16]

Block data에는 해당 블록에 포함된 트랜잭션이 순서대로 저장되어 있다.

Transactions Data에는 블록에 저장되는 실제 정보인데 Students record와 Access Record를 포함하게 된다. 또한 identity정보가 포함되어 인증서 정보를 알 수 있다.

[그림 V-5]에서 Block Data 필드에 3개의 트랜잭션이 저장되어 있고, 트랜잭션1을 구성하고 있는 각각의 항목들은 다음과 같다.

Header에는 트랜잭션의 version 정보와 트랜잭션이 실행되는 체인코드의 이름 등이 명시되어 있다. Signature는 트랜잭션 생성자의 Identity 관련 디지털인증서 정보가 있다. Proposal은 체인코드에 들어가는 트랜잭션의 입력값이 저장되어 있고, 해당 입력값을 이용해서 체인코드를 실행한다.

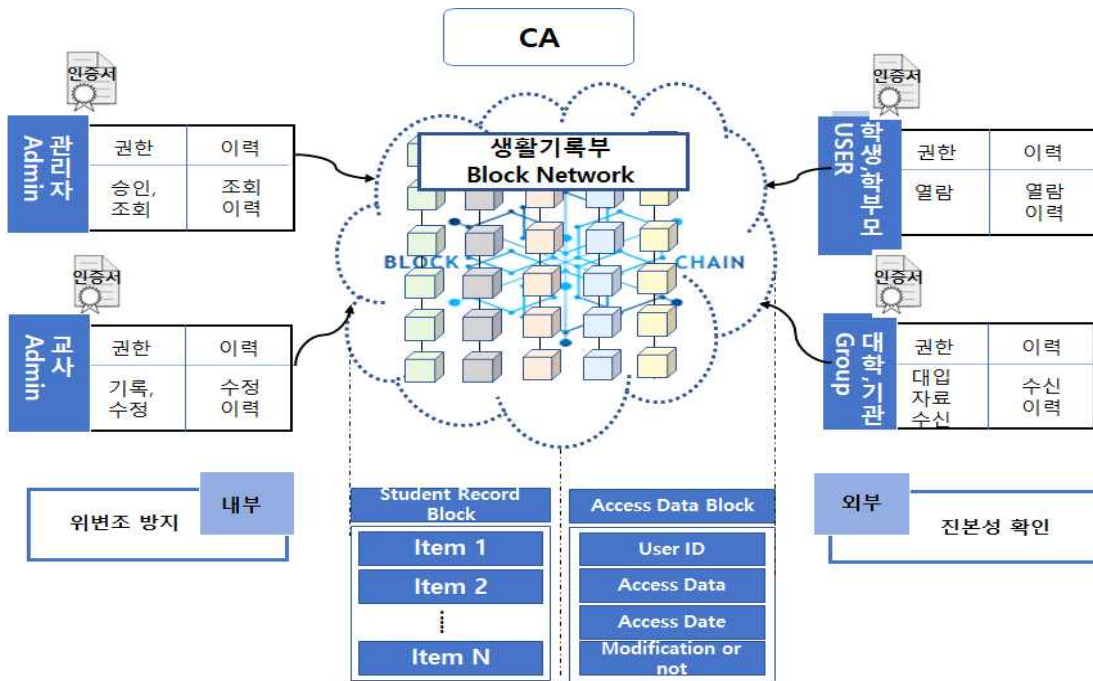
Response는 트랜잭션 처리 결과값을 Read/Write set 형태로 반환하는 필드를 포함한다. Read는 트랜잭션의 proposal이 반영되기 전 값이고, Write는 proposal 값이 반영된 후의 값을 의미하며, 추후 최신 블록 검증과정에 사용된다.

Endorsement는 트랜잭션을 보증해 준 peer의 Identity 정보가 포함되어 있으며, 보증정책에 따라서 Endorsement는 한 개 혹은 여러 개가 될 수 있다.

마지막으로, Metadata에는 블록생성자의 Identity정보와 블록에 포함되어 있는 Transaction 보증여부 등이 포함되어 있다[16].

2. 학교생활기록부 블록체인 네트워크 구성

1) 학교생활기록부 블록체인 참여자 및 권한



[그림 V-6] 학교생활기록부 블록체인 네트워크 참여자 및 권한

제안하는 생활기록부 블록체인 네트워크에 참여가 가능한 참여자는 Admin(학교교사, 관리자), User(학생, 학부모), Group(대학, 교육청기관) 세 가지로 구분하며, 권한별 인증을 부여하는 인증센터(CA)를 통하여 인증을 받아야만 네트워크에 참여할 수 있다. 프라이빗 블록체인으로 인증센터에서 각 참여자별 인증서를 발급한다. 참여자별 블록체인 네트워크접근 권한은 다음과 같다.

내부사용자로서 Admin(관리자)는 교사가 생활기록부에 접근할 수 있는 권한을 부여하고, 생활기록부를 작성하는 내용에 대한 승인과 학생생활기록부에 대한 열람 권한을 가지며, 열람에 따른 접근이력이 접근데이터 블록에 기록된다.

내부사용자로서 Admin(교사)는 관리대상 학생에 대한 학교생활기록부를 등록, 열람, 수정할 수 있으며, 등록, 열람, 수정 작업에 따른 접근이력이 접근데이터

블록에 저장되고, 학교생활기록부 등록과 수정한 내용은 학생레코드블록에 기록된다.

외부사용자 User로서 학생·학부모는 본인 학생 정보만 열람할 수 있으며, 열람 접근이력이 접근데이터 블록에 기록된다.

외부사용자 Group으로서 대학은 대학수학능력 정시 또는 수시에 지원한 학생에 대한 대입수능자료 수신을 할 수 있으며, 이에 대한 접근기록이 접근데이터 블록에 기록된다.

학교생활기록부 참여자를 제한하는 허가형 블록체인인 하이퍼레저 패브릭으로 구현함으로써 내부사용자에 의한 학교생활기록부 위변조 방지와 기밀성을 보장하고, 외부사용자에게는 진본성 확인과 무결성을 보장할 수 있을 것으로 기대할 수 있다. 각 참여자별 역할과 체인코드(스마트컨트랙트)는 [표 V-1]과 같다.

[표 V-1] 참여차별 역할 및 체인코드

구분	참여자	역할	체인코드
Admin	학교교사, 관리자	학교생활기록부 등록, 열람, 수정 수행	query, write, update
User	학생, 학부모	학교생활기록부 열람	query
Group	교육청, 대학	학교생활기록부 열람, 요청	query, request

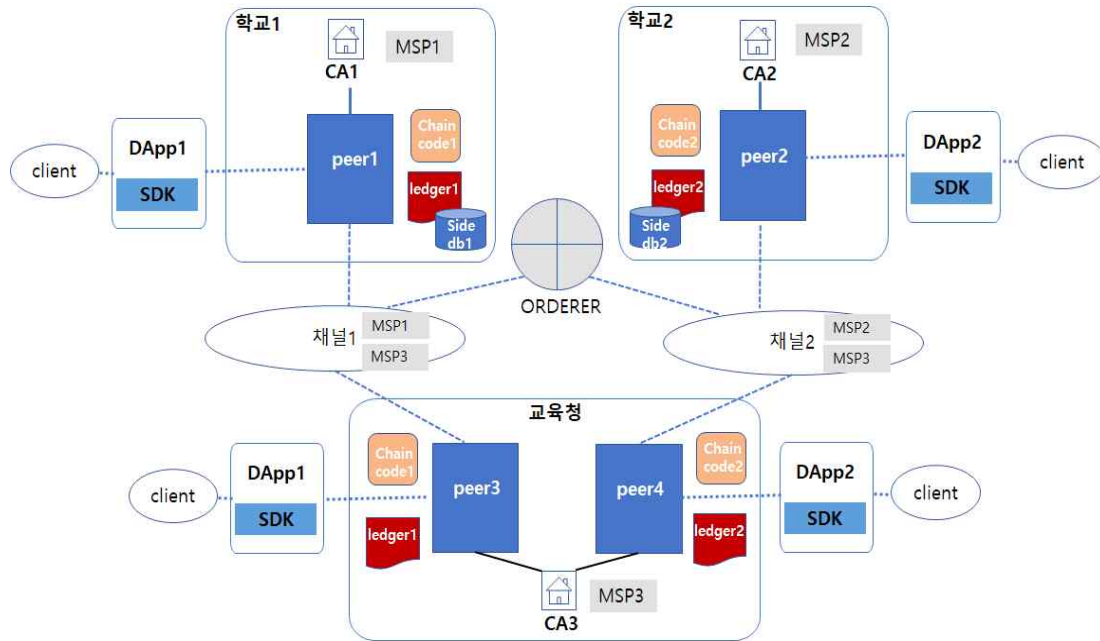
블록체인 네트워크에서 수행되는 체인코드종류에 따른 기능과 Input, Output은 [표 V-2]와 같다[20].

[표 V-2] 체인코드 기능

구분	기능	Input	Output
write	생활기록부를 등록함	ID, 등록할 생활기록부 정보, 타임스탬프	등록한 생활기록부 정보와 타임스탬프의 해시값
update	생활기록부를 수정함	ID, 수정할 생활기록부 정보, 타임스탬프	수정한 생활기록부 정보와 타임스탬프의 해시값
query	생활기록부를 열람함	ID, 타임스탬프	열람한 ID정보와 타임스탬프의 해시값
request	생활기록부를 요청함	ID, 타임스탬프	요청한 생활기록부 Key값과 타임스탬프의 해시값

2) 학교생활기록부 블록체인 네트워크 구성 개념도

[그림 V-7]는 제안하는 하이퍼레저 패브릭 블록체인 기술 기반의 학교생활기록부 네트워크 구성 모델의 개념적 구조도이다.



[그림 V-7] 학교생활기록부 네트워크 구성 모델의 개념적 구조도

하이퍼레저 패브릭은 비즈니스의 이해관계가 맞는 다수의 기업이나 기관 등의 조직이 함께 구축 가능한 프라이빗 블록체인이다.

그림에서 3개의 조직이 하이퍼레저 패브릭 기술을 적용하여 생활기록부 네트워크를 구축하였다고 가정하며, 실제로는 기관과 학교수만큼 네트워크에 연결된다. 조직1은 학교1, 조직2는 학교2, 조직3은 교육청이라 정의한다. 각 조직은 자신의 데이터센터에 하나 이상의 peer노드를 설치한다. 트랜잭션 보증과 블록에 대한 검증은 하는 peer노드를 각 조직마다 소유하고 있기 때문에 어느 한 조직에서 분산원장에 대한 기록을 독단적으로 변경하거나 조작하는 것이 불가능하다.

분산원장은 각 채널당 하나씩 존재한다. 분산원장은 채널에 소속된 peer간 데이터 공유를 위해서 사용된다. 위 그림에서 peer1과 peer3는 채널1의 분산원장 Ledger1을 가지고 있고, peer2와 peer4는 채널2의 분산원장 Ledger2를 가지고 있다.

학교1과 학교2 사이에는 채널이 없기 때문에 분산원장을 공유할 수 없다.

교육청과 학교1은 채널1을 통해서 데이터를 공유하고, 교육청과 학교2는 채널2를 통해서 데이터를 공유한다. 교육청은 두 개의 채널을 통해서 두 개의 분산원장을 분리해서 소유하고 있다. 참여자를 포함한 블록체인 네트워크의 모든 노드는 CA기술을 통해 소속된 조직의 MSP로부터 인증과 권한을 사전에 받아야만 블록체인 네트워크에서 역할을 수행할 수 있다.

[그림 V-7] 네트워크는 1개 교육청 블록체인 네트워크를 표현한 것이며, 1개 교육청에 소속된 각 학교들 중 2개의 학교 조직을 의미한다. 개별 조직(학교1, 학교2, 교육청) 안에는 여러개 peer들이 존재하는데 peer들은 조직에 소속된 교직원들 peer노드라고 할 수 있다.

개별 학교와 교육청은 서로 다른 채널로 데이터를 공유하나, 생활기록부 암호화된 원본 데이터는 동일 학교 조직안에서 PDC(Private Data Collection, 같은 채널에 속한 구성원들 간에 프라이버시를 보장하기 위한 기능) 기능으로 Side db 저장되며, 교육청에서는 채널을 공유하고 있지만 PDC 정보에는 접근할 수 없고 Side db 정보의 해시값만 공유하고 있으므로 학교생활기록부 원본데이터를 소유하고 있지 않아 학교정보의 프라이버시를 보장한다.

학교들 사이에는 채널을 생성하고 있지 않으므로 데이터를 공유할 수 없다. 즉 개별학교에서 같은 조직에 있는 peer들 끼리만 생활기록부 암호화된 원본데이터를 공유한다.

블록체인 참여자는 체인코드를 통해서 분산원장에 데이터를 기록하거나 읽을 수 있다. 이러한 체인코드는 체인코드 그 자체로도 사용될 수 있지만, 대부분의 경우 업무 모델에 맞는 분산애플리케이션(DApp)과 함께 개발되어 사용된다. 분산애플리케이션은 사용자가 분산환경에서 비즈니스 거래등을 편리하게 해 주기 위해 사용되는 애플리케이션을 통칭하는 단어이다. 하이퍼레저 패브릭에서는 분산 애플리케이션 개발을 위해 다양한 종류의 SDK를 제공하고 있다. 개발자는 SDK를 통해서 트랜잭션을 생성하고 체인코드 함수를 불러오는 등의 여러 기능을 좀 더 쉽게 개발할 수 있다[16].

하이퍼레저 패브릭으로 구축한 블록체인 네트워크와 여기에 설치된 스마트 컨트랙트(체인코드) 등이 일반적인 사용자들에게 서비스로 제공하기 위해서는

UI/UX를 포함한 클라이언트 애플리케이션과 연동되어야만 한다.

따라서 하이퍼레저 패브릭 네트워크 외부에서 블록체인 서비스를 쉽게 사용하고 접속할 수 있도록, 다양한 SDK로 개발된 분산애플리케이션(DApp)를 통해 네트워크에 접속하고 스마트 컨트랙트를 호출할 수 있다.

[표 V-3] 용어 정리[16][29][31]

구분	내용
Client	블록체인에 접근하기 위해 필요한 노드, Peer에게 보내는 거래(transaction)를 만든다
DApp	분산애플리케이션(Decentralized Application)으로 사용자가 분산환경에서 비즈니스 거래등을 편리하게 해주기 위해 사용되는 애플리케이션을 통칭
SDK	소프트웨어 개발 도구 모음(Software Development Kit)으로 Node.js, Java, Go 등 제공
Fabric CA (Certificate Authority)	프라이빗 블록체인에서 참여자의 ID와 권한을 관리할 주체가 필요하므로, CA(Certificate Authority)에서 디지털 증명서(Digital certificate)를 발급하는 기관 역할을 한다. 패브릭 네트워크에 참여하는 그룹들은 모두 개별 CA를 이용한다.
MSP (Membership Service Provider)	네트워크 내 노드의 역할과 권한 등을 정의, 각 조직 및 사용자에 대한 신원검증을 처리하고, 시스템에 참여하는 멤버들의 신원을 확인하고 접근 권한을 관리
Peer	패브릭에서 가장 기본이 되는 노드로서 장부(Ledger)를 물리적으로 호스팅하고 Chaincode를 저장하고 있는 독립체(entity), 수행하는 역할에 따라 4가지로 구분 1) Endorsing peer: 체인코드 시뮬레이션을 통해 트랜잭션이 적절한지 판단하는 역할, execution 역할 2) Commit Peer : 최신 블록에 대한 검증, validation 역할 3) Anchor Peer : 다른 조직과의 통신을 위해 다른 조직의 peer와 통신하는 역할 4) Leader peer : orderer와 연결되어 최신 블록을 전달받아 조직 내 다른 peer들에게 전송하는 역할
Orderer	검증된 트랜잭션들을 이용해 최종적으로 블록을 생성하는 노드, 보증된 트랜잭션(Read/Write Set) 을 받아서 정렬 한 후 블록으로 만들어 Commit Peer에 전달하는 역할

구분	내용
Chaincode	하이퍼레저 패브릭에서 스마트 컨트랙트를 체인코드라고 하며 블록 체인 네트워크 외부의 클라이언트 응용 프로그램에 의해 호출되는 코드로, 전체 상태(World State) 의 일련의 키-값(key-value) 쌍에 대한 접근 및 장부에 저장된 상태(state)를 업데이트 하는 코드(code). 패브릭은 체인코드 언어로 현재 Go 와 node.js 등 지원
Ledger	시스템 운영 과정에서 발생하는 모든 거래 정보를 해시체인(hash chain) 형태로 저장되어 있는 장부이며 Ledger를 통해 전체 상태 변경의 이력 추적 가능, 한 채널이 한 장부를 가진다. 이 장부를 물리적으로 호스팅 하는 노드들은 피어(Peer)이며, 한 채널 안의 여러 피어들이 한 장부의 복사본을 가진다. 장부의 업데이트는 여러 피어들의 합의(Consensus)를 통해 이루어지기 때문에 일관성을 유지할 수 있다.
채널(Channel)	하이퍼레저 패브릭에서 그룹간 커뮤니케이션 메커니즘으로 Peer간 통신은 채널을 통해서만 이루어진다. 모든 조직이 채널을 통해 정보를 공유할 수도 있고 또는 이해관계가 맞는 일부 조직간에만 추가로 채널을 생성하여 정보를 공유할 수도 있다. 각 채널마다 하나씩 분산원장이 존재하게 되는데, 채널에 참여한 조직의 구성원만이 분산원장에 접근할 수 있으므로 데이터 기밀성을 채널을 통해 제공이 가능하다.
Side DB	허가된 peer만 프라이빗 데이터를 저장할 수 있는 DB. PDC(Private Data Collection, 같은 채널에 속한 구성원들 간에 프라이버시를 보장하기 위한 기능)로 허가된 peer만 프라이빗 데이터를 Side db에 저장

[표 V-4]는 생활기록부 블록체인 네트워크를 구현하기 위한 테스트 개발환경 및 도구의 예시이며, 실제 기능구현 시에는 그 시점에 하이퍼레저 패브릭 최신 버전에서 제공되는 적절한 기능과 도구를 적용하면 될 것이다[25].

[표 V-4] 하이퍼레저 패브릭 블록체인 개발환경 및 도구

구분	오픈소스	사용용도	개발영역
블록체인네트워크	Hyperledger Fabric	블록체인 플랫폼	시스템구축
	Kafka	오더링서비스(분산 메시징)	
	Zookeeper	오더링서비스(분산 코디네이터)	
	CouchDB	state DB	
Application Server	Tomcat	테스트업무화면 및 블록체인모니터링을 위한 어플리케이션 서버	테스트업무 APP
	MariaDB	어플리케이션용 DBMS	
	OpenJDK	Java 어플리케이션 개발도구	체인코드
	Go	체인코드 개발도구	

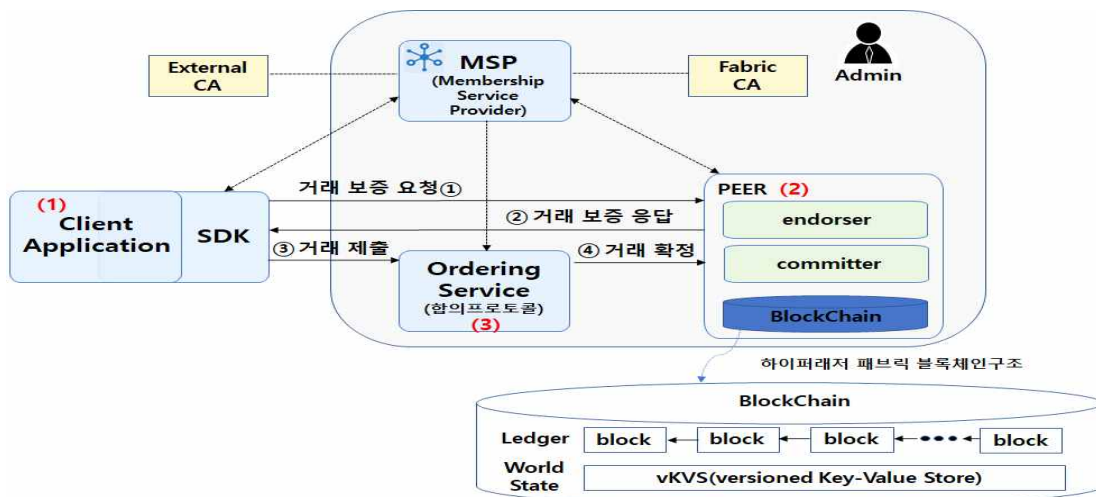
3. 학교생활기록부 블록체인 트랜잭션 합의 과정

비트코인, 이더리움 등이 POW(Proof of Work), POS(Proof of stake), BFT(Byzantine Fault Tolerance)와 같은 특정 알고리즘 하나를 합의라고 칭하는 것과 달리, 하이퍼레저 패브릭에서는 트랜잭션 생성부터 최신 블록이 peer에 저장되기까지의 모든 과정을 합의하고 한다. 크게 3단계 과정으로 1단계는 보증 정책을 확인(Endorsement), 2단계는 트랜잭션을 정해진 순서에 맞춰 정렬(Ordering), 3단계는 정렬된 트랜잭션의 유효성을 검증한 후 최신 블록을 업데이트(Validation) 하는 것이다[16][29].

이 절에서는 하이퍼레저 패브릭 블록체인 기술 기반의 학교생활기록부 네트워크 아키텍처 노드들의 역할과 블록체인 합의과정에 대하여 설명하고자 한다.

1) 트랜잭션 처리과정에 노드역할

External-CA에 의해서 기존 일반 신원인증서에 의해서 학교생활기록부 시스템에 접속로그인 한다. Fabric-CA는 하이퍼레저 패브릭 네트워크안에서 참여자와 노드들에 대한 인증을 한다.



[그림 V-8] 하이퍼레저 패브릭 기반 트랜잭션 처리과정 노드

[그림 V-8]에서 클라이언트, Fabric-CA, MSP, Peer(Endorse/Commit Peer), Orderer 등이 간단히 구현되어 어떻게 서로 유기적으로 작동하는지 살펴볼 수 있는데, 각 노드들의 역할은 다음과 같다[22][25][29].

(1) 클라이언트 노드(Client node)

사용자를 대신하여 거래(transaction)를 생성하여 체인코드 실행을 호출하는 노드로, 클라이언트 노드는 거래를 생성하여 보증 피어 노드(endorsing peer node)에게 제출(submit)함으로써 거래 보증을 요청하고 거래 보증 응답을 수집한다. 거래 보증 응답을 수집한 클라이언트는 거래 제안(transaction-proposal)을 생성하여 순서화 서비스 노드(ordering service node)에게 전달한다.

(2) 피어 노드(Peer node)

피어 노드는 거래를 확정(commit)한다. 거래 정보를 저장하는 레저(ledger)와 거래 실행 결과에 따른 상태 정보를 저장하는 상태 저장소(state store)로 구성되는 블록체인을 유지한다.

순서화 서비스 노드(ordering service node)로부터 블록 형태로 거래와 상태 갱신 정보를 수신한다. 보증 노드는 클라이언트의 보증 요청에 따라 해당 체인코드를 실행하고 결과를 보증하는 역할을 수행한다. 보증 노드와 보증 방법은 해당 체인코드와 연계된 보증 정책에 의해 결정되며, 보증 정책은 체인코드와 함께 작성되어 체인코드가 블록체인에 배치될 때 함께 배치된다.

(3) 순서화 서비스 노드(Ordering service node)

합의 알고리즘에 따라 클라이언트들로부터 제안되는 거래들을 순서화시켜 피어 노드들에게 안전하게 전달한다.

클라이언트는 채널을 통해 거래를 포함하는 메시지를 순서화 서비스 노드들에게 전달하고, 순서화 서비스 노드들은 거래 메시지들을 순서화시켜 채널에 연결된 모든 피어들에게 전달하는 것이다. 각 피어에게 전달되는 거래 메시지들이 동일한 순서를 가지고, 원자적 브로드캐스트(atomic broadcast) 서비스에 의해 안전하게 전달되는 것을 보장한다.

2) 체인코드 실행과정

블록체인 참여자는 체인코드를 통해서 분산원장에 데이터를 기록하거나 읽을 수 있다. 이러한 체인코드는 대부분의 경우 비즈니스 모델에 맞는 분산애플리케이션(DApp)과 함께 개발되어 사용된다.

따라서 하이퍼레저 패브릭 기반 학교생활기록부 블록체인에서 분산애플리케이션이 Peer와 함께 어떻게 동작할 지 연구해 본다.

사용자는 분산 애플리케이션을 통해서 Peer 네트워크에 설치된 체인코드를 실행한다. 체인코드는의 크게 읽기(Query)와 쓰기(Write/Update) 두 종류의 함수로 구분할 수 있는데, 읽기 함수는 5단계 과정을 거쳐서 실행되고 쓰기 함수는 9단계 과정을 거쳐서 실행된다[16].

읽기 작업은 작업을 수행함과 동시에 바로 결과값을 수신받을 수 있지만, 쓰기 작업은 좀 더 복잡한 과정을 거쳐 일정 시간이 경과된 후에야 결과값이 반영된다.

(1) 읽기 체인코드 실행과정



[그림 V-9] 읽기 체인코드 실행과정

사용자는 peer 네트워크의 peer1과 연결되어 있다고 가정한다면, 먼저 분산 애플리케이션은 분산원장에 접근하기 위해서 사용자A의 인증서를 이용해서 인증과정을 통과한 후 peer1과 연결한다.

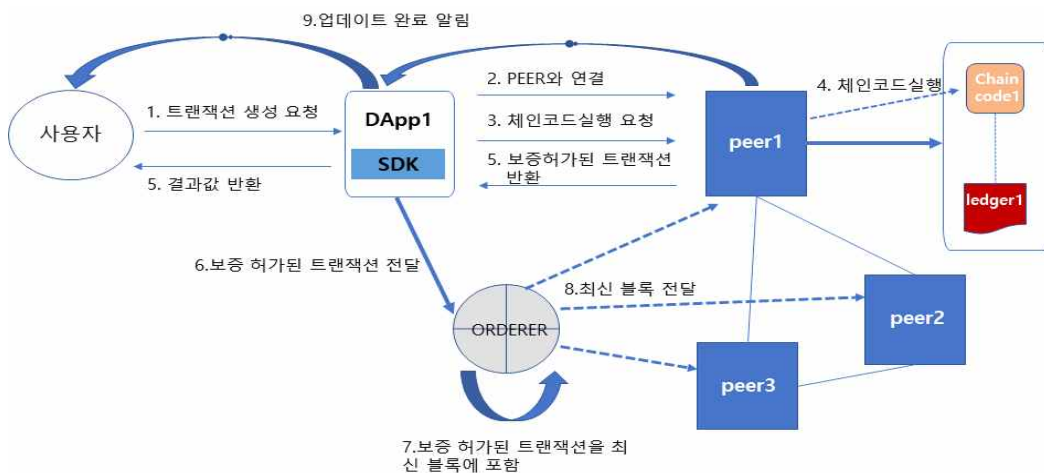
정상적으로 연결되고 난 후 분산애플리케이션은 peer1에 설치된 체인코드의 query함수를 호출한다.

마지막으로, peer1은 요청받은 체인코드의 query함수를 실행하여 자신의 로컬 저장소에 저장되어 있는 분산원장의 데이터를 분산애플리케이션에 전달한다.

데이터 읽기 과정에서는 분산애플리케이션으로부터 Query함수 실행을 요청받은 peer1외 다른 peer는 Query 함수 실행을 위한 어떠한 동작도 하지 않는다[16].

하이퍼레저 패브릭 블록체인 기반으로 학교생활기록부 시스템을 구현한다면 조회(열람) 권한을 부여받은 참여자(학생, 학부모 등)가 학교생활기록부 조회를 하고자 할 경우 읽기 체인코드가 실행되어 트랜잭션이 동작하여 요청한 참여자에게 그 결과값을 보여줄 것을 예상할 수 있다.

(2) 쓰기 체인코드 실행과정



[그림 V-10] 쓰기 체인코드 실행과정

분산원장에 데이터를 기록하는 작업은 데이터를 읽어오는 작업과는 달리 peer 간 합의과정이 필요하기 때문에 읽기 함수를 호출받은 peer1뿐만 아니라 모든 peer가 쓰기 과정에 참여해야 한다. 9단계 중 앞의 4단계는 query함수 대신 update함수를 호출하는 것 외에는 데이터를 읽어오는 과정과 동일하기 때문에 앞단계는 생략하고 5단계부터 설명한다.

분산원장에 데이터를 기록하기 위해서는 보증정책을 충족시켜야한다.

5단계에서는 peer1이 트랜잭션 입력값에 대한 결과값과 보증정책을 확인하는 작업을 수행한다. 트랜잭션 실행 결과값이 정상적이고 peer1의 보증조건을 충족시키면 peer1은 결과값과 함께 peer1의 디지털 인증서를 분산 애플리케이션에 전달한다.

6단계에서 분산 애플리케이션은 트랜잭션 결과값과 peer1의 디지털인증서와 함께 트랜잭션을 orderer노드로 전송한다.

7단계에서 orderer는 수신한 트랜잭션을 순서에 맞게 정렬하여 블록체인의 최신 블록을 생성하고, 8단계에서 생성한 블록을 자신이 속한 네트워크의 모든 peer에게 전달한다.

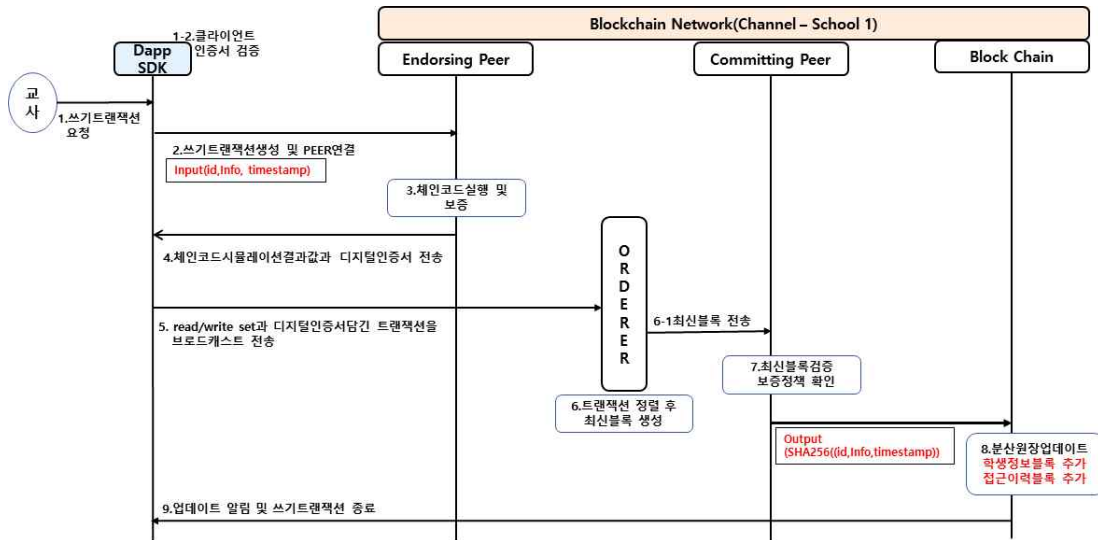
9단계에서 최신 블록을 전달받은 모든 peer는 해당 블록에 포함된 모든 트랜잭션에 대한 결과값과 인증서를 검증하는 작업을 수행한다. 검증과정에서 문제가 없을 시 자신의 로컬저장소에 저장된 분산원장을 업데이트한다. 마지막으로 peer는 블록 업데이트 결과를 분산 애플리케이션에 알려주는 것을 끝으로 분산원장 업데이트 과정을 완료한다[16].

하이퍼레저 패브릭 블록체인 기반에서 학교생활기록부 시스템에서 등록 및 수정 권한을 부여받은 참여자(교사)가 학교생활기록부를 기록하고자 할 경우, 쓰기 체인코드가 실행되어 트랜잭션이 동작하여 동일 채널에 있는 참여자 Peer들에게 최신블록을 전달하고 학생생활기록 블록과 접근이력블록이 동시에 업데이트가 완료될 것을 예상할 수 있다.

3) 트랜잭션 합의 전체 과정

하이퍼레저 패브릭 기반 학교생활기록부 네트워크를 구축하고, 관련 체인코드와 분산애플리케이션을 개발, 그리고 참여자의 디지털 인증서 생성이 모두 완료되었다는 가정하에 쓰기와 읽기 트랜잭션 처리과정에 대해서 살펴보고자 한다.

(1) 쓰기 트랜잭션 합의 전체 과정



[그림 V-11] 쓰기 트랜잭션 합의 전체 과정

생활기록부내용을 등록과 정정하는 역할은 교사의 권한이다. 쓰기 권한이 부여된 교사가 학생의 학교생활기록부를 등록 또는 수정 작업을 할 때 ‘update’ 체인코드가 실행되는 트랜잭션 처리과정을 설명한다.

① 교사는 개인공인인증서로 교육행정정보시스템에 접속한 후, 생활기록부 쓰기 트랜잭션을 생활기록부 블록체인 네트워크에 요청한다.

② 분산 애플리케이션(DApp)은 분산원장에 접근하기 위해서 교사의 인증서를 이용해서 인증과정을 통과한 후 블록네트워크(Peer)와 연결하고, 쓰기 트랜잭션을 생성하여 Endorsing Peer에 전송한다.

③ Endorsing Peer는 쓰기(update) 체인코드를 실행하고 보증하며, 인증과 권한을 확인한다. 트랜잭션의 Proposal과 체인코드name필드, World state 데이터베이스를 참조하여 시뮬레이션하여 그 결과값으로 생성된 Read/Write set을 확인

하여 트랜잭션의 보증여부를 판단한다. 또한 교사의 MSP가 유효한지, 교사가 분산원장 쓰기 권한을 가지고 있는 지 등을 검사한다.

④ Endorsing Peer는 검사하고 이상이 없으면 Read/Write set과 자신의 디지털인증서를 분산 애플리케이션에 전송한다.

⑤ 분산애플리케이션은 자신이 예상한 값과 Read/Write set이 동일한지를 확인하는 작업을 한다. 분산애플리케이션은 결과값 확인 후 Read/Write set과 Endorsing Peer의 디지털인증서가 담긴 트랜잭션을 Orderer로 브로드캐스트하여 전송한다.

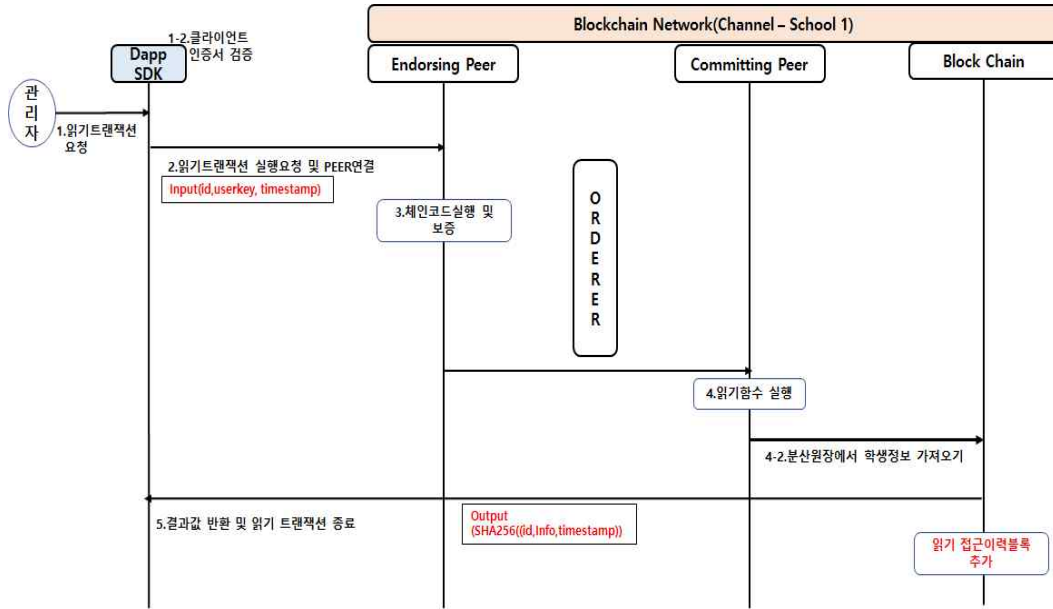
⑥ Orderer는 트랜잭션 정렬에 필요한 Timestamp 필드 등을 확인한 후, 블록에 포함될 트랜잭션을 정해진 순서대로 정렬하여 최신 블록을 생성하여 Committing Peer로 전달한다.

⑦ Committing Peer는 해당 블록을 검증한다. 블록에 포함된 각각의 트랜잭션마다 보증정책에 부합하는 Endorsing peer의 디지털 인증서가 존재하는 지 확인하며, 각 트랜잭션마다 Read/Write set 결과값을 확인한다.

⑧ 최신 블록 검증단계까지 모두 통과하면 Peer는 자신의 로컬 저장소에 저장되어 있는 블록체인에 최신블록을 추가하여 저장하고, 유효 태그를 가진 트랜잭션의 내용만을 world state에 업데이트한다. 학생정보 쓰기내용 블록이 생성되고 접근이력 블록이 동시에 추가된다. 생성된 학생정보는 블록에 해시로 암호화되어 저장된다.

⑨ 마지막으로 world state 데이터베이스까지 트랜잭션 업데이트가 완료되면 분산 애플리케이션에 업데이트를 알리며 쓰기 트랜잭션은 종료된다.

(2) 읽기 트랜잭션 합의 전체 과정



[그림 V-12] 읽기 트랜잭션 합의 전체 과정

읽기 권한이 부여된 사용자(학생, 학부모 등)가 학교생활기록부를 조회할 때 ‘query’ 체인코드가 실행되는 트랜잭션 처리과정을 설명한다.

① 사용자는 개인공인인증서 또는 신원확인을 한 후 대국민서비스에 접속한 후, 생활기록부 읽기 트랜잭션을 블록체인 네트워크에 요청한다.

② 분산 애플리케이션(DApp)은 분산원장에 접근하기 위해서 사용자의 인증서를 이용해서 인증과정을 통과한 후 블록네트워크(Peer)와 연결하고, Peer에 설치된 체인코드의 query 함수를 호출한다.

③ Endorsing Peer는 사용자의 인증과 권한을 검사한다. 즉 사용자의 MSP가 유효한지, 분산원장 읽기 권한을 가지고 있는 지 등을 검사한다.

④ Committing Peer는 요청받은 체인코드의 query 함수를 실행한다.

⑤ 실행된 query 함수에 의해 Peer 자신의 로컬저장소에 있는 분산원장의 데이터 결과값을 분산 애플리케이션에 전달해 주면 읽기 트랜잭션은 종료된다.

⑥ 읽기 트랜잭션 종료에 이어 사용자가 조회 접근한 접근이력블록이 추가로 블록체인에 생성된다.

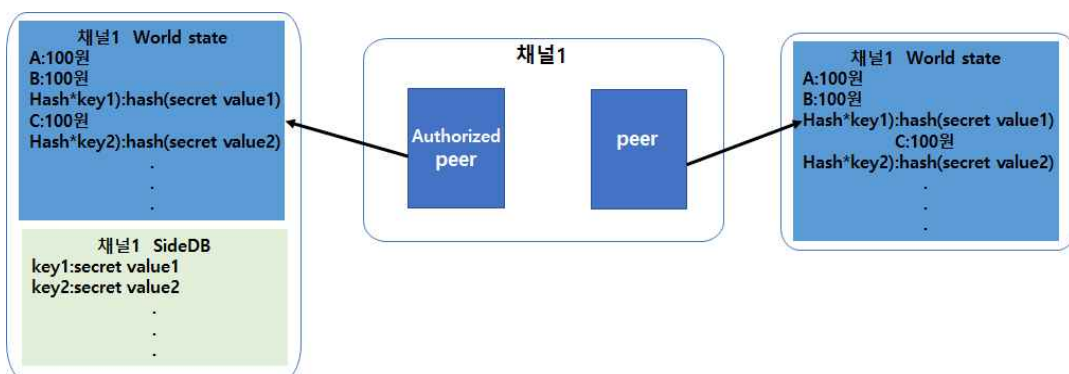
4. 학교생활기록부 블록체인 PDC 적용

하이퍼레저 패브릭에서 채널은 구성원 중 같은 채널에 있는 구성원 간에만 정보를 교환할 수 있으며, 서로 다른 채널에 있는 분산원장은 접근할 수 없도록 하여 프라이버시를 보장해 준다. 그러나 같은 채널에 있는 구성원 중 특정 구성원 간에만 정보를 교환하여 프라이버시를 보장하고자 할 경우, 또 다른 채널을 만든다면 시스템 운영에 부담과 성능에 영향을 미치기 때문에 하이퍼레저 패브릭 v1.2부터 프라이빗 데이터(PDC, Private Data Collection)라는 기능이 추가되었다.

프라이빗 데이터 콜렉션은 크게 두 가지 구성요소로 나누어 진다[16][18].

첫 번째는 프라이빗 데이터 열람이 허락된 Peer(Authorized Peer)만 내용에 접근할 수 있다. 일반 트랜잭션은 블록을 통해서 모든 Peer에게 전달되지만 프라이빗 데이터는 'Peer To Peer Protocol'를 통해 Authorized Peer에게만 전달된다. 프라이빗 데이터를 전달받은 Authorized Peer는 Transient data store(임시 데이터 저장소)에 잠시 저장하고 블록 검증 과정을 통해 자신의 Side DB에 최종 저장한다.

두 번째는 프라이빗 데이터 대신에 프라이빗 데이터 해시값으로 원장에 기록되며, Authorized peer뿐만 아니라 동일한 채널의 모든 peer들이 프라이빗 데이터 해시값을 확인할 수 있다. 보증/검증 과정에서 프라이빗 데이터 대신에 해시값을 사용한다.



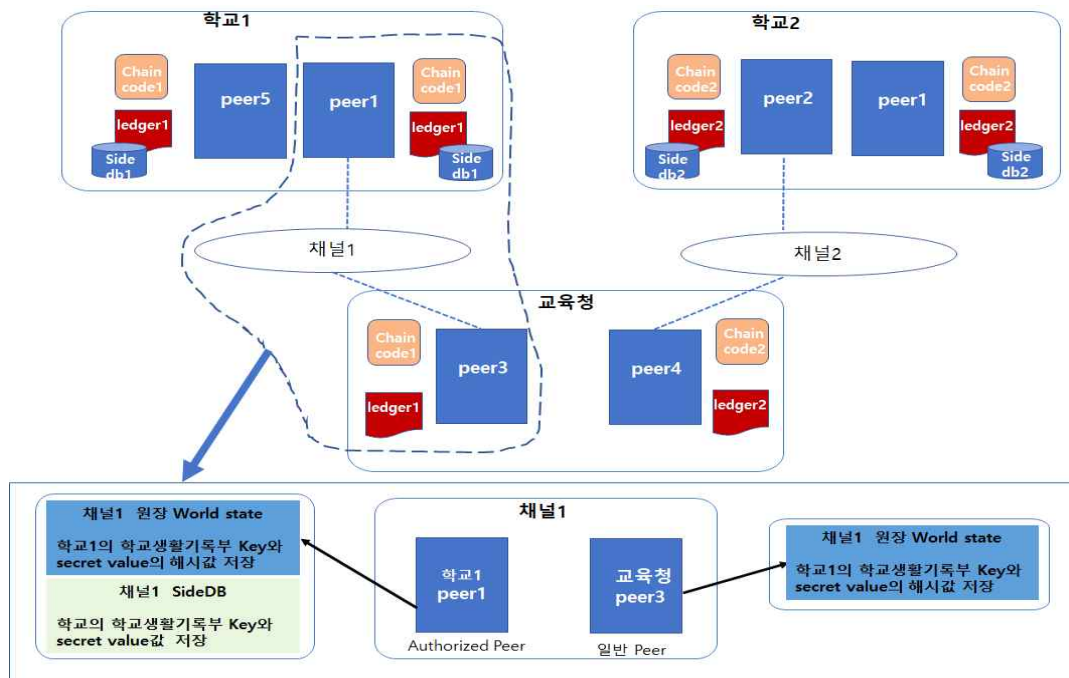
[그림 V-13] Authorized Peer와 일반 Peer 원장 구조 비교

[그림 V-13]와 같이 채널 원장에는 프라이빗 데이터의 해시값만 저장되며, Side DB에 프라이빗 데이터를 복호화할 수 있는 키(Key)가 저장된다. Side DB에 접근 가능한 Authorized peer는 프라이빗 데이터 해시값의 키를 이용해 채널 원장에 저장된 프라이빗 데이터를 열람할 수 있는 반면, 해시를 복호화할 수 있는 키가 없는 일반 Peer는 프라이빗 데이터를 열람할 수 없다[16].

[그림 V-14]는 프라이빗 데이터(PDC) 기능을 학교생활기록부 블록체인 네트워크에 적용한 개념도이다.

본 연구에서 구현한 학교생활기록부 블록체인 네트워크에서는 교육청과 개별 학교간 별도의 채널을 구성한다. 동일 채널내의 교육청과 학교간에는 채널을 통하여 데이터를 공유할 수 있다. 그러나 교육청에서 학교생활기록부의 데이터 원장내용을 열람하게 하여서는 안되며, 통계 등 공유가능한 내용만 열람하게 하여야 하므로 여기에 프라이빗 데이터(PDC)를 적용한다.

동일 채널1을 통해서 학교1과 교육청이 분산원장을 공유하고 있으나, 학교생활기록부 프라이빗 데이터는 학교1 조직에서만 저장되고, 교육청은 프라이빗데이터의 해시값만 저장하여 본 내용을 열람할 수 없게 구성한다.



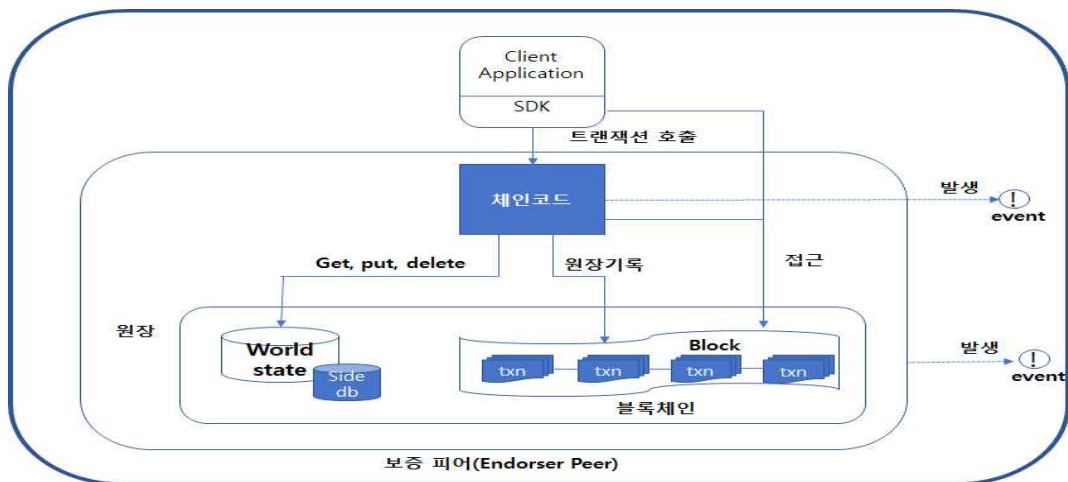
[그림 V-14] PDC 기능 적용한 학교생활기록부 블록체인 네트워크

학교1과 교육청간의 채널1의 구성만 별도로 확인하면 다음과 같다.

학교1 peer1에는 학교1의 학교생활기록부 내용의 KEY와 Secret value의 해시값이 state DB에 저장되며, 실제 학교생활기록부 KEY와 Secret value값은 SideDB에 저장되어 학교1에서만 저장한다.

교육청 peer3에는 학교1의 학교생활기록부 내용의 KEY와 Secret value의 해시값이 state DB에 저장되고 SideDB는 없으므로 학교생활기록부 실제 내용은 볼 수 없다.

하이퍼레저 패브릭에서 구현한 PDC를 이용한 트랜잭션 처리과정에 대한 전체적인 도식화는 [그림 V-15]과 같으며 개인정보 처리에 대한 기능 구현이 가능함을 알 수 있다.



[그림 V-15] 체인코드 기반의 데이터의 효율적인 관리 방안(출처:한국IBM)

World state db는 블록체인에 포함되기 전 트랜잭션의 실행 결과를 저장할 수 있는 Key-Value방식의 데이터베이스이다. World State에 저장된 데이터는 삭제/변경이 가능하기 때문에 유효하지 않은 데이터가 있다면 체인코드를 통해서 파악할 수 있다. Side db에서는 개인정보 등의 민감한 데이터를 프라이빗 트랜잭션을 통해 전송하여 World state대신에 Side DB에 저장하여 관리 및 삭제가 가능하다.

v1.3이후에는 영지식증명(zero-knowledge proof) 기능이 추가되어 트랜잭션에 대한 익명성이 더욱 강화되고 world state영역뿐만 아니라 블록체인에 있는 데이터에 대한 관리 기능이 추가되었으며, 유효한 거래 및 기간을 설정하여 데이터를

관리할 수 있도록 할 예정이라고 하니 더 다양하고 고도화 된 블록체인 기술로 학교생활기록부 네트워크를 실제 적용한다면 보다 안정적인 시스템 구현이 실현 될 수 있으리라 기대한다[16].

5. 4세대 나이스 블록체인 제안과의 비교

2022년에 개통될 예정인 4세대 나이스에서 학교생활기록부관련 블록체인구현 모델은 두가지를 제시하고 있다.

학교생활기록부 졸업생 보존이관 및 민원 요청 시 블록체인을 통한 위변조 확인 모델과 블록체인 기반의 졸업생 학교생활기록부 보존방안이다.

본 연구에서는 학교에서 학생에 대한 학교생활기록부 데이터를 등록, 수정, 조회하는 데이터 생명주기 전체를 블록체인으로 구현하는 것을 제안하였다.

[표 V-5] 4세대 나이스와 본 연구 제안과의 비교

구분	4세대 나이스	본 연구 제안
내용	졸업생 학교생활기록부 보존 블록체인기반 구현	재학생 학교생활기록부 등록, 수정, 조회 시스템 운영기반 블록체인 구현

4세대 나이스에서는 이미 등록된 재학생 학교생활기록부를 졸업 5년후 이관해야 함에 따른 진본성 확인을 위한 블록체인을 제안하였다면, 본 연구에서는 학교생활기록부의 무결성과 위변조방지를 위하여 원 자료를 기록하는 시점부터 허가 와 권한이 부여된 사용자만 접근할 수 있고, 데이터 등록, 수정, 조회 전체 과정을 블록체인화함으로써 학교생활기록부 데이터에 대한 신뢰성을 확보할 수 있는 방안을 제안하였다.

허가된 참여자만 접근할 수 있는 프라이빗블록체인 기술중에서 가장 왕성히 연구 중인 하이퍼레저 패브릭 오픈소스를 적용한 학교생활기록부 블록체인 네트워크를 제안하였으며, 하이퍼레저 패브릭은 교체가능한 모듈구조이므로 구현하는 시점에 새롭게 발표되는 버전의 새로운 기능을 적용할 수 있을 것이다.

6. 현재 나이스 보안강화체계와의 비교

현재 교육행정정보시스템에서 학교생활기록부의 신뢰도 제고를 위한 보안강화 방안으로 세 가지를 제시하여 운영하고 있다.

첫 번째는 학교생활기록부 권한관리 강화 방안으로 학교생활기록부의 사용자 권한 부여·변경 시, 학교장의 결재를 받도록 나이스 시스템을 개선하고, 권한부여 현황에 대한 상시 모니터링할 수 있도록 개선하였다.

두 번째는 학교생활기록부 나이스 시스템 인증체계 강화 방안으로 금융거래 인증 수준의 2차 인증체계를 도입하여 ARS와 mOTP 두가지 방안을 사용하고 있다. 학교생활기록부 중에서 성적메뉴 접근할 경우에만 2차 인증을 한다.

세 번째는 학교생활기록부 수정이력 보관방안으로 수정이 자주 발생하는 정성적 기재영역에 대한 수정이력을 별도 저장공간을 확보하여 저장하고 있다.

[표 V-6]는 본 연구에서의 현재 시스템 보안강화 방안과에 블록체인제안모델과 비교한 것이다.

[표 V-6] 현재 보안강화방안과 본 연구 제안과의 비교

구분	현 시스템 보안강화 방안	본 연구 제안
권한 관리 강화	학교생활기록부의 사용자 권한 부여·변경 시, 학교장의 결재	허가형(permissioned) 블록체인은 멤버십 관리 서비스를 통해 허가된 참여자만 접근을 허용하며, 참여자의 블록체인 접근 권한 제어가 가능
인증 체계 강화	2차 인증체계를 도입하여 ARS와 mOTP 두가지 방안을 사용	블록체인에 접속하기 위해서는 Fabric-CA에서 인증서를 발급받고, MSP에 의해 참여자 및 노드의 역할과 권한이 제어되므로 2차 접근 제한 구현이 시스템적으로 가능
수정 이력 보관	수정이력을 보관하는 별도 저장공간을 확보하여 저장	블록원장에 블록생성시간과 블록 수정이력 등을 포함하여 저장하므로, 원 데이터와 수정이력 데이터를 별도 보관할 필요가 없음

첫째, 허가형 블록체인으로 권한이 허가된 참여자만 접근할 수 있으므로 권한부여시 학교장 결재를 반드시 받아야 하는 번거로움을 줄일 수 있다.

둘째, 기본 신원인증과 Fabric-CA에서 블록접근 권한과 인증을 받을 수 있는

므로 ARS 또는 mOTP를 통한 2차인증으로 접속하는 불편함을 해소할 수 있다.

셋째, 학교생활기록부 등록, 정정에 대한 기록이 모두 블록체인에 시간단위로 기록되며, 접근이력기록도 블록체인으로 구현할 수 있으므로 수정이력을 보관하는 별도 시스템이 불필요하여 시스템 관리 부담을 줄일 수 있다.

위 세 가지 사항 이외에 본 연구에서는 하이퍼레저 패브릭 기능 중 프라이빗 데이터(PDC)을 적용하여 학교별 학교생활기록부의 데이터를 학교에만 저장되고, 동일 채널에 있는 기관에서는 열람할 수 없게 구현하는 방법을 제안하였다.

블록체인 구현 시 고려사항으로 첫째, 필요하다고 판단되는 업무선정 후 블록체인 플랫폼에 적용하고, 둘째, 블록에는 개인정보가 포함된 원본데이터는 저장하지 않아야 하며, 향후 새로운 업무서비스에 추가 적용할 수 있는 확장성이 고려된 구조로 블록체인을 설계하여야 한다는 기준에 의하면, 본 연구에서 제안하는 블록체인 모델은 세 가지 고려사항을 모두 충족하는 제안 모델이라고 할 수 있다.

7. 기대효과

블록체인 기술은 학교생활기록부의 위·변조 방지와 무결성 확보를 위한 새로운 인프라로서 이상적이며, 관리적 기대효과는 다음과 같다.

하이퍼레저 패브릭 블록체인 기반 기술을 적용함으로써 기존 권한부여 시 학교장까지 결재와 2차 인증 접속의 불편함이 해소되므로 학교 관리자 및 교사의 사용자 편의성이 향상되어 업무 만족도를 향상시킬 수 있다.

학교생활기록부 최초 등록부터 정정될 때마다의 기록이 타임스탬프와 함께 블록이 추가되어, 수정할 수 없는 블록으로 분산원장에 저장되므로, 현재 시스템처럼 수정이력 보관 시스템을 별도 관리할 필요가 없어 시스템 저장 공간이 절약되어 관리비용 감소와 업무부담 감소를 예상할 수 있다.

무엇보다 하이퍼레저 패브릭 기반 학교생활기록부 블록체인 구현에 따른 위변조방지와 부인방지를 보장할 수 있으며, 블록체인의 분산처리기능으로 안전하고

효율적으로 데이터를 관리할 수 있으므로 신뢰도는 보다 더 향상될 것으로 기대할 수 있다.

블록체인 구현 시 예상되는 기술적 측면에서의 보안우수성은 네 가지로 예측할 수 있다.

첫째, 현행 시스템보다 기밀성이 더 보장될 수 있다.

현행 시스템은 학생 번호, 이름, 고유식별정보만 암호화 저장되지만, 블록체인은 분산원장 자체가 해시 암호화 후 DB에 저장된다. 현행시스템은 WEB-WAS 구간엔 SSL 통신으로 구간 암호화를 적용하지만 블록체인시스템에서는 블록체인을 기본구성으로 통신채널 암호화하므로 기밀성이 더 강화된다.

둘째, 현행시스템보다 무결성을 더 보장될 수 있다.

현행시스템은 참여기관과 전송구간이 암호화 되지 않으면 위변조가 가능하나, 블록체인은 기본구성이 블록체인 네트워크와 트랜잭션이 암호화되어 있어서 위변조가 어렵다. 중요파일 위변조 방지를 위해 현행 시스템은 백업과 접근관리 모니터링으로 대응하고 있으나, 블록체인은 사용자인증은 물론 트랜잭션 및 통신채널 인증으로 네트워크를 유지하므로 비인가 접근 자체가 불가능하다.

셋째, 현행시스템보다 가용성이 더 향상될 수 있다.

현행시스템은 중요시스템 이중화 및 재해복구시스템으로 대비하고 있지만 장애 발생 후 복구메커니즘이 복잡하다. 블록체인은 노드 복구 시 오더러를 통해 원장을 동기화하므로 부분 오류가 발생하여도 전체 기능이 작동되므로 장애 내성이 강하다.

넷째, 현행시스템보다 부인방지가 보장된다.

현행시스템은 거래부인방지를 위해 시스템 로그 또는 학교생활기록부 정정이력 저장을 하고 있으나, 블록체인의 특징이 거래 부인방지가 성립되지 않으므로 더 효과적일 것이다.

VI. 결 론

17개 시·도교육청이 2015~2018년 사이에 진행한 학교 감사결과, 고등학교에서 시험지 유출이 숙명여고를 포함해 모두 13건으로 적발되어 징계를 받은 교사와 학생이 13명이다. 또한 학교생활기록부 기재 시 관련 규정을 어기거나 부당하게 정정하여 적발된 사례도 15건이 있으며, 2015년에는 경기 분당 대진고에서 교무부장이 딸의 학생부를 조작했다가 파면된 사례도 있었다.

2019년에는 모 법무부장관 후보 딸의 학교생활기록부가 본인의 동의없이 유출되어 정치권의 이슈로 사용되는 등의 중요정보를 침해하는 사건이 간간히 발생하고 있다.

교육행정정보시스템 내에 학교생활기록부는 학생의 학교생활 전반의 교육활동과 함께 개인의 성장과정이 매우 세밀하게 기록되어 있는 중요한 개인정보이며 교육활동 결과물이므로 불법유출과 위·변조를 방지하여 무결성을 확보할 수 있어야 한다.

학교생활기록부 데이터의 보안성 개선과 신뢰성 확보를 위하여 본 논문에서는 프라이빗 블록체인을 적용하여 외부자에 의한 블록네트워크 참여를 방지하고, 교육행정정보시스템의 정당한 관리자가 아닌 제 3자에 의한 생활기록부의 위·변조 방지와 무결성 확보를 위한 하나의 대안을 연구하고 제안하였다.

학교생활기록부 블록체인 네트워크 구현을 위한 연구를 하기 위하여 먼저, 관련 사항에 대한 이론적 배경을 고찰하였다. 교육행정정보시스템 초기 구축에서 2세대, 3세대 개편에 대한 내용과 향후 2022년에 개편될 예정인 4세대 나이스 준비 사항에 대해서도 조사하였다. 또한, 본 연구의 주제인 학교생활기록부에 대한 정의와 학생정보를 다루는 학교에서의 역할과 중요성에 대한 조사와 블록체인 개념과 기술종류 및 활용현황에 대해서도 연구하였다.

다음으로 학교생활기록부 데이터의 신뢰성 제고를 위한 현행 교육행정정보시스템에서의 보안관리체계 강화방안에 대한 연구 결과, 세가지 방안을 도입하여 시행되고 있음을 알 수 있었다. 그 방안은 첫째, 학교생활기록부 권한관리를 강

화하여 이 권한만큼은 반드시 학교장의 결재를 받도록 하고, 둘째는, 학교생활기록부 성적메뉴 접근 시 금융거래 수준의 2차 인증체계를 도입하였으며, 셋째, 학교생활기록부는 수정이력을 별도 DB로 관리하도록 하고 있다. 이전 보다 더 강화된 보안체계로 신뢰도는 향상되었으나, 기존 RDB시스템 구조에 종속되는 추가 기능개선 방안으로 학교 사용자의 불편함과 시스템관리 비용과 관리대상이 증가할 것으로 분석되었다. 이에 근본적인 학교생활기록부 데이터의 신뢰성 확보를 위한 새로운 기술적 해결방안으로 블록체인기반 시스템 메커니즘을 제안하였다.

학교생활기록부에 대한 접근은 허가된 조직에서만 접근하여야 하므로 프라이빗 블록체인으로 구성하여야 하며, 위변조방지를 위한 참여자의 접근 권한이 제어가능 하여야 하며 신뢰성과 무결성이 보장되어야 한다. 따라서 허가형블록체인 중에서 업무서비스를 구현하기에 적합한 하이퍼레저 패브릭 기술적용을 제안하였다.

제안하는 생활기록부 블록체인 네트워크는 교육행정정보시스템 서버에 등록된 학교생활기록부 데이터는 암호화된 블록네트워크에 기록되며, 정당한 사용자에 의해 요청될 수 있도록 접근기록 블록을 생성하여 수정된 생활기록부에 대한 블록을 생성하여 보호하는 메커니즘이다.

생활기록부 블록체인 네트워크 참여자는 Admin(학교교사, 관리자), User(학생, 학부모), Group(교육청, 대학) 세 종류로 분류할 수 있다. 학교교사는 학교생활기록부를 등록, 열람, 수정할 수 있고, 학생·학부모는 학생 본인정보만 열람할 수 있으며, 교육청과 대학은 대입전형자료와 통계자료 등에 대한 열람을 할 수 있다.

참여자에 대한 접근제한을 위하여 하이퍼레저 패브릭 블록체인에서는 인증센터(Fabric-CA)를 통해 참여자별 권한인증을 부여받아 블록체인 네트워크에 참여할 수 있도록 한다.

블록체인네트워크 구성은 하이퍼레저 패브릭의 채널기능을 도입하여 동일 채널에 속한 기관(학교)끼리만 데이터를 공유하고 활용할 수 있도록 한다. 이 채널을 통하여 동일 학교조직 내 블록네트워크를 통해 분산원장을 학교구성원간에 공유하며, 다른 학교와는 채널을 공유하고 있지 않으므로 학교간 데이터는 공유할 수 없다. 학교와 기관(교육청)간에 연결된 채널을 통해서도 기관에서 학교의

데이터를 모두 공유하는 것이 아니라, 기관에 제공 가능한 사항만 공유하도록 설정한다.

이처럼 하이퍼레저 패브릭 블록체인을 도입함으로써 참여자의 접근통제와 권한구분이 가능하며, 채널구성에 따라 조직간 데이터 공유를 편리하게 구분하고 통제할 수 있다.

하이퍼레저 패브릭 블록체인에서의 합의과정은 비트코인과 이더리움처럼 특정 알고리즘 하나로 하는 것과는 달리, 트랜잭션 생성부터 블록저장 되기까지의 모든 과정이 합의 과정이므로 학교생활기록부 쓰기와 읽기 트랜잭션 처리과정에 대하여 연구하였다.

무엇보다 동일 채널에 속한 조직끼리 분산원장을 공유하기 때문에 하이퍼레저 패브릭의 PDC(Private Data Collection) 기능을 활용하여, 동일 조직 내에서만 암호화된 학교생활기록부 분산원장을 Side DB에 공유하며, 다른 조직에서는 학교생활기록부 데이터의 key와 secret value의 해시값만 공유하므로 원 데이터에 대한 열람 접근이 불가능하게 구현할 수 있는 방법을 연구하였다.

블록체인 기반 학교생활기록부시스템을 구현한다면 시스템에서 요구하는 보안사항인 신원인증(Identity), 트랜잭션의 기밀성(Confidentiality), 재생(Replay)공격방지, 개인정보보호로 트랜잭션의 발행자의 익명화, 액세스 제어로 프로그램 실행할 수 있는 참여자 제한, PKI인증서와 전자서명을 적용하여 사용자의 신원확인 등을 충족할 수 있으므로, 현행 시스템운영 방식보다 보안성이 강화되고 효율적으로 운영될 수 있을 것으로 기대할 수 있다.

하지만 하이퍼레저 패브릭 블록체인은 기존 블록체인보다 성능이 높다고 할 수 있으나, 현행 시스템과 비교하여서는 성능이 떨어진다는 평가와 오픈소스이면서 신생 기술이므로 안정화되어 있지 않기 때문에 개발과 검증이 어렵다는 평가도 있으므로 실제 적용하기 전에 타당성검토를 위한 ISP(Information Strategy Planning, 정보화전략계획)을 선제적으로 실시하는 것이 필요할 것이다.

본 연구는 4개 시스템, 44개 단위업무, 268개 세부업무로 운영되는 방대한 교육행정정보시스템이라는 단일시스템에서 그 중 학교생활기록부라는 하나의 세부업무에 대하여 블록체인기술을 적용하는 이론적 연구로서 실제로 구현해 보지 않았다는 제한점이 있다. 향후 실제 하이퍼레저 패브릭 제작툴로 구현하여 성능

을 측정하고 실효성에 대한 연구가 필요하다.

기업형 블록체인을 지향하는 하이퍼레저 프로젝트가 2020년 1월 29일에 하이퍼레저 패브릭 2.0버전을 공개했다. 2.0버전에서는 체인코드의 변수값을 분산화해 관리하는 기능이 탑재되고, 프라이빗 데이터의 보안성을 향상시키는 기능 등이 탑재되었다고 한다. 그러나 최신 버전에 대한 이해가 부족하여 본 연구에서는 최신 기능을 접목시킨 연구를 도출하지 못했다는 한계점이 있다.

본 연구결과를 토대로 후속연구를 할 수 있는 세 가지 제언을 다음과 같이 제시한다.

첫째, 학교와 교육청, 400여개 대학간의 학교생활기록부 대입전형자료 제공 및 수신을 블록체인으로 구성하는 방법에 대한 연구와 실증연구가 필요하다. 대입전형자료 온라인 제공이 블록체인화 된다면 VPN통신에 따른 불안정성이 해결되고, 효율적인 데이터 송수신을 기대할 수 있다.

둘째, 학교생활기록부는 졸업후 5년이 지나면 공공기록물관리에 관한 법률 시행령에 의해 기록물로 보존하도록 하고 있으므로, 기록물보존관점에서 진본성유지를 위한 블록체인 기술구현 실증연구도 필요하겠다.

참 고 문 헌

- [1] 과학기술정보통신부, “신뢰할 수 있는 4차 산업혁명을 구현하는 블록체인 기술 발전전략”, 2018. 6
- [2] 교육과학기술부(현 교육부), “차세대 나이스 구축 기본계획(안)”, 2010. 1
- [3] 교육부, “2020년 나이스(나이스) 운영 기본 계획”, 2020. 1
- [4] 교육부, “2020학년도 수시 대입전형자료(학교생활기록부) 온라인 제공 안내”, 2019. 8
- [5] 교육부, “4세대 나이스 구축 기본 계획”, 2019. 12
- [6] 교육부, “졸업생 학교생활기록 이관 계획”, 2019. 9
- [7] 교육부, “학교생활기록부 관련 나이스 기능 개선 추진 안내”, 2017. 11
- [8] 교육부, “학교생활기록부 접근권한 인증체제 개선(2차인증 도입)관련 변경사항 안내”, 2019. 8
- [9] 교육부, “학생부 관리체계 강화를 위한 나이스 기능개선 사항 안내”, 2019. 3
- [10] 교육부, 17개 시·도교육청, 한국교육학술정보원, “4세대 나이스 구축방안 마련을 위한 정보화전략계획(ISP) 수립 사업 완료보고”, 2019. 10
- [11] 교육부, 한국교육학술정보원, “2020학년도 대입전형자료 온라인 제공 시스템 사용자 설명서”, 2019. 5
- [12] 김희경, 박남제, “교육행정정보시스템 학교생활기록부 데이터의 안정성 확보를 위한 블록체인 설계 및 구현”, 한국융합학회논문지, 2020. 27-35, 한국융합학회
- [13] 박용성, “차세대나이스의 문제점 및 개선방향”, 2012, 경인교육대학교 교육대학원
- [14] 안희진, “고등학교 학교생활기록부의 운영 실태 및 개선 방안 연구”, 2018, 고려대학교 교육대학원
- [15] 염세경, “오픈소스 블록체인을 활용한 전자문서 신뢰시스템 구현”, 2019, 동국대학교 대학원
- [16] 윤대근, “하이퍼레저 패브릭으로 배우는 블록체인”, 경기도:주식회사제이펍, 2019. 11

- [17] 이진수, “블록체인 기반 교육 분야 인증서 발급시스템에 관한 연구”, 2020, 동국대학교 대학원
- [18] 정예나, “블록체인 기반 영상 정보 관리 시스템”, 2018, 아주대학교 대학원
- [19] 제주특별자치도교육청, “2020 학교생활기록부 기재요령”, 2020. 2
- [20] 지용선, “블록체인을 활용한 개인정보관리기법”, 2018, 숭실대학교 대학원
- [21] 한국IBM, “블록체인으로 변화될 미래의 모습”, 2017
- [22] 한국IBM, “하이퍼레저 패브릭 구조 및 주요 구축사례”, 2018. 2
- [23] 한국교육학술정보원, “나이스 학생부 수정이력 보관시스템 인프라 구성 계획 (안)”, 2018. 11
- [24] 한국교육학술정보원, “한국의 교육정보서비스 모델”, 2016. 12
- [25] 한국예탁결제원, “채권장의결제시스템 블록체인기술 적용 타당성검토를 위한 컨설팅”, 2018
- [26] 한국정보화진흥원, “지능형 정부 추진을 위한 블록체인 동향분석 및 시사점”, 2018
- [27] IBM, “하이퍼레저란 무엇인가”,
<https://www.ibm.com/kr-ko/blockchain/hyperledger>
- [28] 국가법령정보센터, “학교생활기록 작성 및 관리지침”, <https://www.law.go.kr>
- [29] 박승철, “블록체인과 하이퍼레저패브릭 유튜브 강의”, 2018. 6,
<https://www.youtube.com/watch?v=rrQp-ncNFm4>
- [30] 블록센스, “퍼블릭(Public) 블록체인과 프라이빗(Private) 블록체인을 알아보자”, 2018. 7, <https://cryptochain.tistory.com/42>
- [31] 정성동, “하이퍼레저 패브릭 네트워크 구조”, 2019. 6,
<https://medium.com/decipher-media/%ED%95%98%EC%9D%B4%ED%8D%BC%EB%A0%88%EC%A0%80-%ED%8C%A8%EB%B8%8C%EB%A6%AD-%EB%84%A4%ED%8A%B8%EC%9B%8C%ED%81%AC-%EA%B5%AC%EC%A1%B0-hyperledger-fabric-network-structure-d7fd9c759983>
- [32] 토큰포스트(TokenPost), “워털루 대학 연구진, 하이퍼레저 패브릭 TPS 7배 늘려”, 2019. 5, <https://www.tokenpost.kr/article-9037>