https://doi.org/10.5392/JKCA.2021.21.06.001

교육행정정보시스템의 보안성 강화를 위한 하이브리드 블록체인 설계

Hybrid Blockchain Design to Improve the Security of Education Administration Information System

손기봉, 손민영, 김영학
금오공과대학교 컴퓨터공학과

Ki-Bong Son(gukb@kumoh.ac.kr), Min-Young Son(smy8484@naver.com), Young-Hak Kim(kimyh@kumoh.ac.kr)

요약

나이스 시스템은 우리나라의 초•중등학교에서 운영되던 행정 정보를 통합한 시스템이다. 현재 이 시스템은 중앙 서버 방식으로 운영되고 있고 학교 행정 정보와 학생의 중요 교육 정보를 포함하고 있다. 학생 정보 중 학생생활기록부는 학생이 상급 기관으로 진학하기 위한 중요한 정보를 포함하고 있지만, 악의적인 공격에 정보가 유출되거나 조작되는 등의 문제가 발생할 수 있다. 본 논문에서는 기존 나이스 시스템에서 관리하던 서버와 블록체인 기술을 접목한 하이브리드 블록체인 시스템을 제안한다. 제안된 시스템은 학생 정보의 접근 시 데이터베이스의 쿼리 정보를 블록에 기록한다. 학생의 정보 수정이나 증명서 발급 등의 요청이 오면 블록체인의 쿼리와 데이터베이스의 정보, 학생의 키값을 확인하여 정보의 유출이나 조작 여부 등을 판단하고 정상 데이터일 경우에만 기록 수정 등의 요청을 수행한다. 이러한 과정은 블록체인을 통해 데이터 조작 등을 검사하기 때문에 기존 중앙 서버보다 보안이 향상된다. 제안된 시스템은 이더리움 플랫폼에서 구현되었으며 스마트 컨트랙트를 사용하여 블록체인의 쿼리 정보를 실험적으로 확인하였다. 본 연구는 기존의 나이스 시스템에 블록체인을 결합하여 학생 자료의 위변조에 대한 보안을 강화하여 나이스 시스템의 신뢰도를 높이는 데 기여한다.

■ 중심어 : | 나이스 시스템 | 블록체인 | 이더리움 |

Abstract

The Neis System is a system integrating administrative information that was operated in elementary and secondary schools in Korea. Currently, this system is operated by a central server method and contains school administration information and important educational information of students. Among student information, the student life record contains important information for a student to advance to a higher level institution, but problems such as information leakage or manipulation may occur due to malicious attacks. In this paper, we propose a hybrid blockchain system that combines the server and blockchain technology managed by the existing Neis system. The proposed system records the query information of the database in a block when student information is accessed. When a request for correction of student information or issuance of a certificate is received, the query of the blockchain, the information in the database, and the student's key value are checked to determine whether the information has been leaked or manipulated, and only if the data is normal, the request for revision of the record is performed . This process is more secure than the existing central server because it checks the manipulation of data through the blockchain. The proposed system was implemented on the Ethereum platform, and the query information of the blockchain was experimentally verified using smart contracts. This study contributes to enhancing the reliability of the Nice system by strengthening the security against forgery and alteration of student data by combining the existing Nice system with a block chain.

■ keyword : | Neis System | Blockchain | Ethereum |

* 본 연구는 금오공과대학교 학술연구비로 수행되었습니다. (202001850001)

접수일자 : 2021년 03월 03일
심사완료일 : 2021년 04월 19일
수정일자 : 2021년 04월 19일
교신저자 : 김영학, e-mail : kimyh@kumoh.ac.kr

I. 서 론

나이스 시스템(교육행정 정보시스템)은 기존 학교에서 운영·관리하던 것을 통합한 것으로 교육청에서 별도로 관리하는 중앙 서버에서 서비스하고 있다. 나이스 시스템은 90년대 각 학교에서 관리하던 학생 정보 및 행정 시스템을 하나로 통합하여 행정업무의 효율성을 증진시켰다. 행정업무 중 학생생활기록부는 학생이 상위 기관에 진학하기 위한 중요한 자료로서 교원이 정확한 기준에 의해 작성되어야 하며 작성 마감 후에는 변경 사유와 함께 정해진 절차를 거쳐 수정이 이루어져야 한다[1].

학교의 행정업무를 관리하는 나이스 시스템은 서버-클라이언트 구조의 중앙 집중형 서버로 운영되고 있는데 이러한 시스템은 중앙 서버가 해킹 등의 악의적인 공격을 받으면 행정 정보가 유출되거나 조작되는 문제점을 가지고 있다. 나이스 시스템의 허점을 이용하여 교사가 시험 전 정답을 유출하는 등과 같은 악의적인 목적으로 성적 조작이나 유출 등의 사건이 발생하기도 했다[2-4]. 이러한 조작 및 유출 등의 문제점들은 나이스 시스템의 신뢰성과 안정성을 저하하는 결과를 초래한다. 이런 문제점들을 해결하기 위해서 분산 네트워크를 이용하여 보안을 향상하는 방안이 연구되고 있다.

블록체인은 P2P(Peer To Peer) 기반의 분산 시스템으로 사용자 간의 거래 명세가 블록체인 네트워크에 참여한 참여자들에게 저장됨으로써 외부의 공격에 보호될 수 있다[5]. 중앙 서버나 기관의 개입 없이 누구나 거래를 할 수 있다는 장점으로 개인 사이의 거래뿐만 아니라 운송, 의료 데이터 등 블록체인의 활용 분야는 확대되고 있다[6]. 나이스 시스템의 모든 행정 정보를 블록체인으로 관리하면 보안성과 안정성을 향상할 수 있지만, 블록이 많아질수록 검증에 필요한 자원과 처리 시간이 증가하는 단점이 있다.

본 논문은 현재 나이스 시스템의 문제점을 해결하기 위하여 블록체인을 결합한 하이브리드 시스템을 제안한다. 제안한 시스템은 기존 나이스 시스템의 서비스를 그대로 운용하면서 발생하는 문제점만을 방지하는 모델로서 현실성과 안정성을 달성하는 시스템이다. 기존 나이스 시스템은 학생의 학적부를 수정하더라도 마지막 수정자 정보 기록만 남아 있고 기존의 수정 내용이 저장되지 않아 악의적인 조작을 감시하거나 조작되었다 하더라도 조작 전 데이터의 소실 등의 문제점이 있다. 반면에 본 논문에서 제안하는 시스템은 데이터베이스 쿼리를 블록체인에 저장함으로서 데이터 위·변조가 있더라도 원본 데이터와의 비교 분석을 통해 쉽게 복구할 수 있다는 차별성을 가진다. 따라서 학생들의 학생생활기록부를 투명하게 관리하고 유지할 수 있다.

본 연구는 다음과 같이 구성되어 있다. 2장에서는 우리나라의 전산 교육 시스템인 나이스와 블록체인의 관련 연구에 대해 알아보고 3장에서는 제안 시스템에 관하여 서술한다. 4장에서는 제안 시스템의 블록체인 부분을 구현하여 분석하고 5장에서 결론 및 향후 연구에 관해 이야기하며 마무리한다.

II. 관련 연구

1. 나이스 시스템

교육행정 정보시스템(National Education Information System : NEIS(나이스))은 교육부, 각 시도교육청 그리고 약 1만여 개 학교의 행정 시스템을 인터넷으로 연결한 시스템이다. 나이스 시스템은 각 학교에서 이루어지는 모든 행정업무를 온라인으로 처리할 수 있도록 서비스하며 2000년대 1세대 구축을 시작으로 현재 3세대 서비스를 제공하고 있다. 나이스 시스템에서는 각 교육청 담당의 모든 학교 정보를 [그림 1]과 같이 교육청 담당 서버와 백업 센터의 DR(Disaster Recovery) Storage에 저장하여 보관한다.

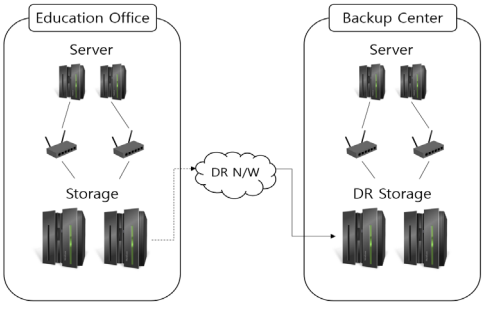

그림 1. 교육행정정보시스템의 백업

학교생활 기록부는 학생의 대내외 활동을 기록한 문서이며 나이스 시스템에서 관리된다. 이 문서는 학생의 인적 사항, 학적, 출결, 수상, 자격 등의 학교생활을 종합적으로 기록한다. 학교생활 기록부는 학생이 상급 교육기관에 진학하기 위해 중요한 자료로 사용된다. 2020년 기준 고등학교 진학률은 99.7%이고 고등교육기관 진학률은 72.5%를 기록할 만큼 많은 학생이 상급기관에 진학하고 있다[7]. 상급 기관 진학은 취업으로 연계되기 때문에 학생들은 좋은 기관으로 진학하기를 원하고 있고 그만큼 학교생활 기록부의 중요성은 대두되고 있다.

나이스 시스템에서 학교생활 기록부를 관리하기 시작하면서 편의성과 보안이 향상되었지만 생활 기록부의 조작 사건이 완벽하게 없어지지는 않았다. [그림 1]과 같이 정보를 중앙 집중 형태로 관리하는 것은 보안에 취약할 수 있고 서버 관리자와 같은 관계자가 악의적으로 정보를 조작할 수 있다.

2016년 한 고등학교에서는 교사가 담당하는 동아리 학생의 학교생활 기록부를 임의로 삭제하거나 추가하는 조작 사건이 있었고, 2017년도에도 한 고등학교에서 학교장과 교사가 가담하여 특정 학생의 학교생활 기록부를 조작하는 사건이 있었다. 조작 사건뿐만 아니라 나이스 시스템에서는 수정 작업이 많이 이루어진다. 이는 대학 입시 기간에 많이 증가하고 있고 교육부에서 제출한 자료에 따르면 2012년 ~ 2016년도까지 371개교에서 419건의 학생부 조작 및 오류가 발생하였고 정정 횟수도 2014년 278,985건에서 2015년 296,170건으로 증가하였다.

이러한 수정 기록 중에서 조작된 자료를 찾기는 쉽지 않다. 조작된 자료를 찾았다 할지라도 조작 이전의 원본 데이터가 없는 경우 복구가 불가능하다. 어떠한 부분이 수정되었는지 로그를 통해 남기기도 하지만 전산원이 악의적인 마음을 가진다면 이 또한 삭제할 수 있으므로 누가 관리해도 문제가 없는 시스템이 제시되어야 한다.

학생의 성적 관련된 부분을 수정하기 위해서는 증빙자료와 학업성적 관리 위원회와 같은 정식 절차를 거쳐 정정해야 하고 반드시 누가·언제·무엇을 수정하였는지 기록하여야 한다. 이때 기록은 보안 사고가 발생할 경우 대처할 수 있는 자료로 사용될 수 있기 때문에 철저히 기록되어야 한다. 데이터를 악의적으로 조작하는 사람이 행위를 감추기 위해 기록을 변경하면 추적하기가 힘들다. 그러므로 기록은 변경할 수 없는 형태로 관리되어야 한다.

2. 블록체인

블록체인은 중앙 집중 형태로 이루어져 있는 시스템을 벗어나 개인 간의(Peer to Peer) 거래를 기록하는 분산 데이터베이스로 정보를 블록의 형태로 구성하고 시간의 순서대로 저장한다. 각 블록은 Hash, Time stamp 및 사전 정의된 트랜잭션으로 구성되어 있고 암호화 기술을 사용하여 체인 형태로 구성된다.

블록이 암호화되어 체인으로 연결될수록 블록의 불변함을 보장한다[8-10]. 블록은 해시 함수와 머클 트리 방법으로 암호화된다. 해시 함수는 단방향 해시 함수(SHA-256)로 입력 데이터가 조금이라도 틀리면 전혀 다른 값이 출력되기 때문에 입력 데이터로 출력 데이터를 찾는 것은 가능하나 반대로 출력 데이터로 입력 데이터를 찾는 것은 불가능하다. 이러한 특징으로 인해 블록체인의 악의적인 조작을 불가능하게 만든다. 머클 트리는 이진 트리의 형태로 제일 아래층의 데이터를 두 개씩 묶어 SHA-256을 통해 해시값을 추출하고 추출된 해시값을 또다시 두 개씩 묶어 또 다른 해시값을 추출하는 방식이다. 이진 트리의 루트인 머클루트(Merkle Root)가 생성되면 머클 트리가 완성되고 이것은 특정 거래를 쉽고 빠르게 찾아주는 특징을 가진다. 또한, 블록체인의 경우 시간에 따라 블록이 연결되면 총용량이 커지기 때문에 라이트 웨이트 노드(Light Weight Node) 형태로 블록체인을 사용할 수 있다.

블록체인은 퍼블릭 블록체인(Public Blockchain), 프라이빗 블록체인(Private Blockchain)으로 나누며 퍼블릭 블록체인은 데이터의 공개를 강조하여 누구나 블록체인 네트워크에 참여할 수 있고 거래 내역을 확인할 수 있다. 퍼블릭 블록체인의 경우 개인의 금융 정보와 같은 민감한 정보들 또한 공개될 수 있다는 문제점 때문에 허가된 사람들만 네트워크에 참여할 수 있는 프라이빗 블록체인이 등장하였다. 프라이빗 블록체인의 경우에는 주체의 허가가 있어야 네트워크에 참여할 수

있으므로 참여자의 익명성이 없고 중앙 관리 주체가 있을 수 있다.

블록체인은 시간이 지나갈수록 발전하고 있다. 1세대는 사토시 나카 모토가 제안한 최초의 블록체인이며 기존 중앙 집중형 시스템에 따른 결제 및 송금 방식을 탈중앙화하는 것에 목적을 둔 블록체인이다. 하지만 특정 분야에서만 사용할 수 있다는 제한성과 실시간으로 블록체인이 형성되지 않는다는 문제점 그리고 합의의 어려움이 있다. 2세대 블록체인은 자동 계약 기능인 스마트 컨트랙트를 포함해 개발된 블록체인이다. 사전 설정된 계약 조건이 만족하면 네트워크에서 시스템이 자동으로 계약을 체결해 주는 방식이다. 3세대 블록체인은 이전 블록들의 문제점 중 합의, 속도, 의사결정 등의 기능을 추가한 블록체인이다. 의사결정 방식으로는 PoW(Proof of Work, 작업 증명), PoS(Proof of Stake, 지분 증명), DPos(Delegated Proof of Stake, 위임지분 증명), DDPoS(Dual Delegated Proof of Stake, 이중위임지분 증명), PoB(Proof of Burn, 소각 증명), PoI(Proof of Importance, 중요도 증명) 등이 있다[11-13].

3. 교육기관에서의 블록체인

블록체인의 특성 중 하나인 데이터 무결성을 이용하여 학생 정보를 관리할 경우 학생 정보의 잘못된 정보 입력 및 고의적인 수정, 삭제 등을 방지할 수 있고 데이터가 허가받지 않고 수정될 경우 수정된 내용을 추적하여 잘못된 부분들을 분석할 수 있다. 새로운 블록이 체인에 연결되기 위해서는 이전 Hash 정보를 포함하고 있어야 한다. 블록의 Hash를 저장함으로써 이전 블록에 대해 의존성을 가지게 되고 체인으로 연결되면서 모든 트랜잭션의 무결성이 보장된다. 블록체인의 연결된 블록이 많아질수록 변조할 수 없고 트랜잭션에서 데이터가 변경될 경우 탐지가 쉽다. Muhammad Zaid는 데이터의 조작과 무결성을 위해 스냅 샷을 블록체인에 저장하는 방법을 제안했다[14]. 전진형은 DDoS 등의 외부 공격을 차단하기 위해 IoT 서버 플랫폼을 이용해 데이터 정보를 블록체인으로 구성한 방법을 제안했다[15]. 3세대 블록체인이 개발되면서 다양한 분야에 블록체인이 접목되고 있다[16-17]. MIT에서는 학교나 관련 기관이 문을 닫을 때도 언제든지 자신의 기록을 조회할 수 있도록 2017년에 블록체인 기술을 접목한 블록서트(Blockcerts)를 통해 디지털 학위증을 발급하고 있다[18-19]. 그뿐만 아니라 바레인의 공립대학에서도 2019년도부터 블록체인 기반의 졸업 증명서를 발급하고 있고 브라질에서는 대학 졸업장의 위·변조를 방지하기 위해 졸업장을 관리할 수 있는 블록체인을 개발 중이고 국내 포항공과대학교에서도 블록체인을 이용해 학위 증명서를 발급하고 있다.

교육기관에서는 교육 인증 및 보안, 수업료 결제 등과 같은 블록체인 기술을 접목하고 있지만, 아직 초기 단계의 연구 성과를 보인다.

Ⅲ. 제안 시스템 설계

최근 블록체인의 대중화에도 불구하고 중앙 데이터베이스 대신하여 블록체인 기술을 사용하는 것은 어려운 과제이다. 모든 데이터베이스가 블록체인으로 옮겨졌다고 가정하더라도 기존 데이터베이스를 활용하던 모든 서비스의 기술이 블록체인을 사용하도록 구현하는 것이 현실적으로 불가능하거나 높은 비용이 발생할 수도 있고 낮은 효율성을 보일 수도 있다. 따라서 기존 시스템 인프라가 블록체인의 장점을 채택하기 위해 업그레이드하더라도 기존 개발 시스템을 점진적으로 바꾸어 나가야 할 필요가 있다. 그뿐만 아니라 블록체인은 기존 데이터베이스와 달리 쿼리 기능을 지원하지 않으며, 노드가 증가할 경우 네트워크 트래픽이 크게 증가한다. 이러한 단점으로 인해 기존 데이터베이스에 블록체인 기능을 추가하는 하이브리드 시스템을 구성하는 것이 현실적인 대안이 될 수 있다. 따라서 본 연구에서 제안하는 시스템에서는 기존의 데이터베이스를 활용하고 동시에 데이터베이스의 접근 쿼리(select, update, insert, delete)를 블록체인으로 저장하여 향후 발생할 문제에 대비하고자 한다.

데이터베이스 접근 쿼리를 블록체인으로 저장·관리할 경우 핵심적인 기능은 크게 두 가지로 블록체인의 블록을 생성하는 것과 기존 블록의 내용을 검증하는 프로세스이다. 제안한 시스템에서 누가 블록을 생성하고 관리

하는 책임을 질 것인지는 제안 시스템의 신뢰성과 효율성을 결정하는 핵심적인 부분이다. 따라서 이번 장에서는 시스템에 관련된 이해관계자(user)와 그들의 역할을 정의하고, 블록체인의 블록을 생성하는 프로세스와 블록체인에 기록된 내용을 기반으로 데이터의 무결성을 검증하는 프로세스 두 가지를 기술한다.

1. 제안 시스템의 구조

본 연구에서 제안한 하이브리드 시스템은 프라이빗 블록체인을 사용한다. 퍼블릭 블록체인에서 모든 노드는 같은 역할을 수행하며 공개되어 있고 분산된 네트워크를 사용하는 것에 반하여 프라이빗 블록체인은 한정적인 네트워크를 활용한다. 네트워크에 참여하는 노드는 서로 알려져 있으며 신뢰할 수 있음이 입증되어야 한다. 프라이빗 블록체인이 가지는 큰 특징 중 하나는 참가자의 권한이 다르게 주어질 수 있다는 점이다. 교육 시스템의 특수성을 고려한다면 네트워크의 사용자 노드를 교육자(기관)와 학습자라는 두 가지 이상의 역할로 분리해야 할 것이다. 즉, 단일 노드의 역할과 단일 유형 블록체인의 네트워크 모델링은 부족함을 의미한다. 본 연구에서 제안한 시스템의 참가자는 권한이 사전에 정의되며, 이에 따라 거래에 참여할 수 있다.

프라이빗 블록체인의 가장 큰 단점은 중앙화와 익명성을 보장하지 않는다는 점이다. 그러나 본 연구에서 대상으로 하는 사용자는 학생이나 교사, 학교 관련자 등으로 익명성이 필요하지 않으며, 학적을 처리하고 증명하기 위하여 중앙 기관의 역할이 필수적이므로 단점에 해당하지 않는다. 프라이빗 블록체인에서 참여자의 권한 부여를 효율적으로 정의하여 합의 범위를 제한함으로써 더 나은 확장성과 처리 속도를 달성할 수 있다.

[그림 2]는 제안한 시스템의 구조를 나타낸 것으로 참여하는 사용자의 구분과 역할은 다음과 같다.

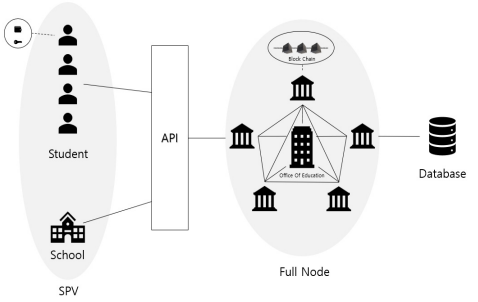

그림 2. 제안 하이브리드 시스템 구조

① 학습자 : 초·중·고등학교를 다니는 학생들은 누구나 학습자 노드로서 네트워크에 참여한다. 학습자의 계정에는 인증서 지갑과 하나 이상의 학적부에 대한 지갑이 있다. 학적부에 대한 지갑은 학교 과정별로 별도 생성될 수 있다. 블록체인에 학습자 관련 쿼리 블록이 추가될 경우 학습자의 학적부 지갑에도 해당 내용이 추가된다. 학교생활기록부에 대한 인증서가 필요할 경우 클라이언트 API의 스마트 계약을 실행함으로써 인증서 요청을 수행할 수 있다.

② 교육자(학교) : 다양한 종류의 학교나 교육자는 교육자 노드로서 네트워크에 참여한다. 교육자 노드는 학습자 노드와는 달리 insert, update, delete 쿼리를 클라이언트 API에 전송할 수 있다. 교육자(학교) 노드는 블록체인에서 일부 학습자들의 머클 트리 데이터 일부만 저장하는 SPV로서 네트워크에 참여한다. 교육자 노드는 블록체인의 일부 머클 트리를 통해 블록이나 학습자 데이터에 대한 간단한 검증이 가능하다.

③ 교육지원청과 교육청 : 교육지원청은 교육청의 업무를 지원하는 관청으로 지리적으로 분산 위치하며, 하나의 단위 교육청은 수십 개의 교육지원청을 담당한다. 교육지원청은 클라이언트 API의 요청을 검증하고 교육청의 데이터베이스에 쿼리를 실행하게 하며 블록체인의 블록을 생성한다. 교육지원청과 교육청 모두 모든 블록의 머클 트리를 저장하는 풀 노드(Full Node)로서 네트워크에 참여한다. 학습자 노드로부터 학교생활기록부에 대한 인증서를 요청받는 경우 블록체인과 데이터베이스를 검증한 후 서명한 인증서를 발급한다.

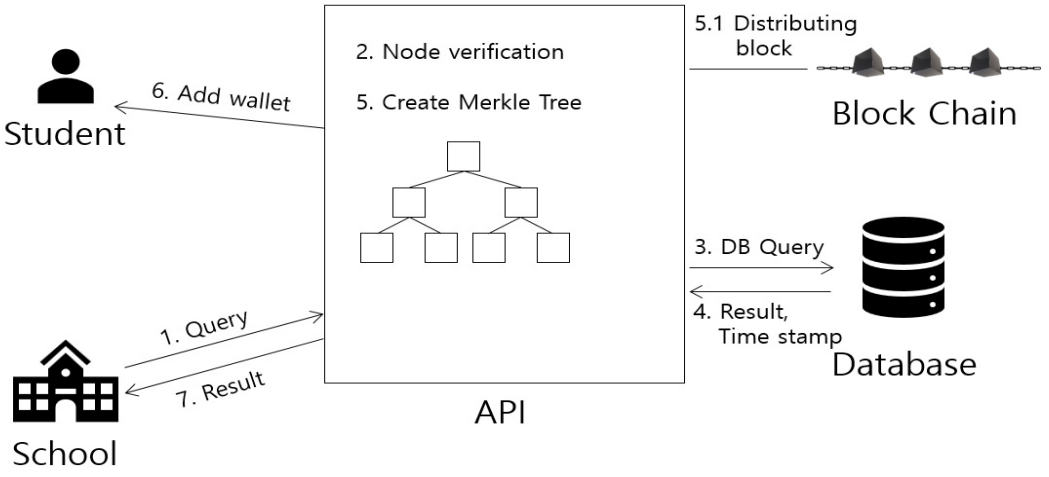

그림 3. 블록체인을 적용한 데이터 생성 및 변경에 대한 프로세스

모든 학교나 교육자가 풀 노드로서 참여하는 분산 시스템은 네트워크 사용량을 증가시키고 개인 정보의 유출 가능성이 있으므로 적절하지 않다. 교육지원청과 교육청이 풀 노드와 마이너(Miner)로서의 역할을 수행한다면 블록체인의 장점을 유지하면서 마이너의 동기 부여 문제와 네트워크 부하 문제, 개인 정보 유출 문제 등을 해소할 수 있을 것이다.

2. 데이터 생성 및 변경에 대한 프로세스

제안한 하이브리드 시스템에서 교육자(학교) 노드만 데이터를 생성하거나 갱신 및 삭제하는 요청을 할 수 있다. 교육지원청과 교육청은 클라이언트 API를 통해 교육자(학교)가 쿼리로 해당 서비스를 사용할 수 있도록 해야 한다. 이때, 쿼리는 데이터베이스에 요청받은 대로 수행되고 수행된 기록이 블록체인에 저장된다. [그림 3]은 데이터가 데이터베이스에 생성 및 갱신/삭제되고 블록체인 블록에 포함되는 프로세스를 나타낸다.

① 교육자(학교)로부터 쿼리가 요청된다.
② 클라이언트 API는 쿼리를 요청한 노드가 학습자에 대한 쿼리를 수행할 권한이 있는지 확인한다.
③ API가 데이터베이스에 쿼리를 전송한다.
④ 클라이언트 API는 해당 정보를 데이터베이스에 저장하고 그 결과와 저장된 타임스탬프를 전달받는다.
⑤ 교육자(학교), 학습자, 쿼리, 전달받은 데이터베이스 실행 결과, 타임스탬프의 정보를 머클 트리에 추가한다.
⑥ 쿼리에 해당하는 학습자의 지갑에 쿼리를 전달하여 추가한다.
⑦ 데이터베이스 실행 결과를 교육자(학교)에 반환한다.

블록체인의 블록을 구성하는 책임은 교육지원청이나 교육청이 가지고 있다. 블록은 머클 트리를 통해 여러 트랜잭션을 묶어 저장할 수 있다. 제안한 시스템에서 머클 트리를 구성하는 기본 트랜잭션은 데이터베이스에 전송되는 쿼리가 되는데 이 쿼리의 생성은 데이터베이스의 양에 비해 방대하므로 압축하여 저장할 필요가 있다. 따라서 본 연구에서 제안하는 하이브리드 시스템은 교육자(학교) 별로 여러 개의 쿼리를 묶어서 하나의 트랜잭션으로 처리한다. 예를 들어 40개의 쿼리를 하나의 트랜잭션으로 처리한다고 가정했을 때, A 학교에서 120개의 쿼리를 실행했을 경우 각각 40개씩 3개의 트랜잭션이 머클 트리에 포함된다. 하지만 학교에서 학기 말이나 학년 말과 같이 성적을 처리하는 특정 기간에 수행되는 쿼리의 양과 방학 기간이나 휴일 동안 수행되는 쿼리의 양이 현저하게 차이가 날 수 있다. 비트코인의 경우 10분마다 블록이 생성되도록 난이도를 조정하여 악의적인 공격을 방어하고 있다. 제안한 시스템에서 40개의 쿼리를 쌓는 시간이 길어진다면 악의적인 사용자의 공격에 취약할 수 있다.

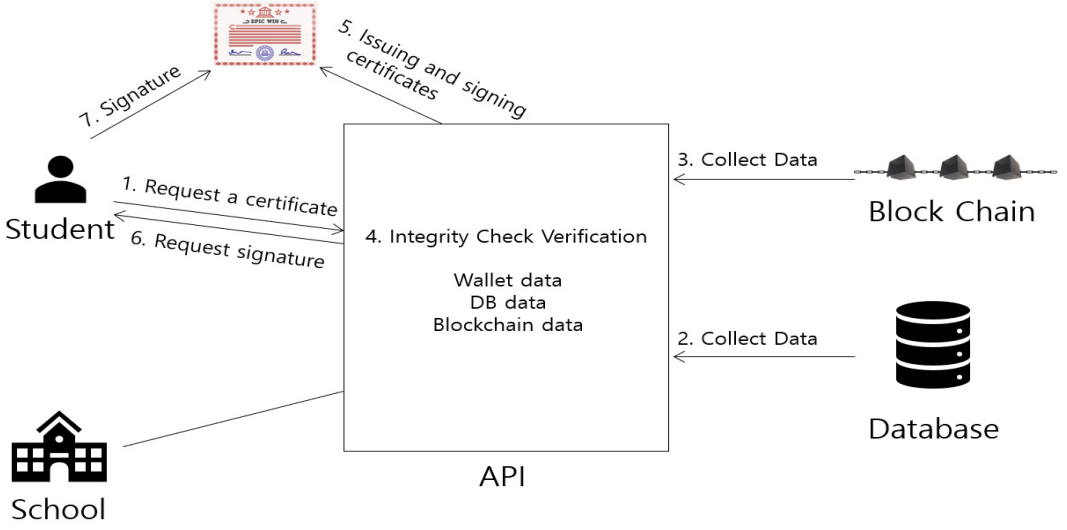

그림 4. 데이터 무결성 검증을 위한 프로세스

따라서 하나의 트랜잭션을 구성하는 시간은 아래 식과 같이 유동적으로 선택될 필요가 있다. 사전에 정의된 트랜잭션을 구성하는 쿼리의 개수가 도달하는 시간($t_{full-query}$)과 최대 트랜잭션 지연 생성 시간($t_{threshold}$) 중 이른 시간으로 트랜잭션을 생성한다.

$$t = \min\left(t_{full-query}, t_{threshold}\right) \quad (1)$$

트랜잭션이 생성되고 머클 트리가 완성되면 블록체인 네트워크에 참여하는 교육지원청과 교육청에 해당 블록을 배포해야 한다. 이때 SPV로 참여하고 있는 교육자(학교)에게도 블록을 배포한다. 교육자(학교)는 SPV 노드로서 전달받은 블록의 머클 트리 내용의 일부를 통해 새로운 블록을 검증하거나 관련 학습자의 지갑에 기록된 내용의 사실 확인 등의 비교적 간단한 역할을 수행할 수 있다. 또한, 블록체인 기반의 별도의 애플리케이션을 구축하여 이를 관리하거나 서비스를 제공할 수도 있다.

3. 데이터 무결성 검증을 위한 프로세스

학습자는 본인의 데이터에 대해 무결성을 증명하고자 인증서를 요청할 수 있다. 교육지원청이나 교육청은 학습자로부터 무결성 인증을 요청받았을 경우 해당 데이터 무결성을 인증하는 책임을 진 자로서의 역할을 수행해야 한다. [그림 4]는 데이터의 무결성을 검증하기 위한 프로세스를 나타낸다.

① 학습자는 학적부 지갑을 클라이언트 API에 올리고 인증서 발급을 요청한다.
② 중앙에 저장된 데이터베이스에서 해당 학습자에 관련한 자료를 수집한다.
③ 블록체인에서 해당 학습자에 관련한 자료를 수집한다.
④ 교육지원청이나 교육청은 API로부터 전달된 지갑 속 자료의 진위를 데이터베이스와 블록체인 내 자료와 비교 검증한다.
⑤ 검증된 자료를 기반으로 인증서를 발급하고 서명한다.
⑥ 학습자에게 서명을 요청한다.
⑦ 학습자는 인증서를 확인하고 서명한다.

위와 같은 데이터 무결성 프로세스를 통해 인증서를 발급할 수 있다. 만약 데이터베이스의 데이터가 악의적으로 변경될 경우 블록체인에 기술되지 않았기 때문에 인증받을 수 없다. 이 외의 클라이언트 API를 통해 데이터베이스의 자료를 변경하는 쿼리는 모두 학습자에게 전달되어 이에 대한 학습자의 즉각적인 이의 제기나

문제의 빠른 감지가 가능하다. 학습자와 교육자(기관)가 단합하여 악의적인 의도로 기존 데이터를 변경 및 훼손하더라도 블록체인의 시간적 특성으로 인해 데이터를 변경하는 시점에 대한 기록은 변경할 수 없다. 다른 시점에 적절하지 못한 데이터의 변경은 인증서를 확인하는 제삼자에게 합리적인 의심을 불러오기 충분할 것이다.

제안한 하이브리드 시스템을 통해 학습자가 인지하지 못한 데이터의 발생이나 수정도 방지할 수 있으며, 악의적인 사용자로부터 데이터가 생성되거나 갱신되었다고 하더라도 블록체인에 기록된 기록을 통해서 해당 데이터베이스의 무결성을 검증할 수 있다.

Ⅳ. 제안 시스템의 블록체인 프로토타입 구현

본 연구에서는 제안 시스템의 주요 분야인 블록체인의 프로토타입을 구현하고 그 성능을 분석하고자 한다. 본 연구의 프로토타입은 이더리움의 스마트 컨트랙트(Smart Contract)를 실행하여 구현하였다. 비트코인과 같은 블록체인은 제한된 스크립트 언어를 사용하여 화폐 이상의 기능을 수행하도록 구현하기에 어렵다. 이에 반해 이더리움은 프로그래밍할 수 있어 다양한 애플리케이션을 운영할 수 있는 블록체인 플랫폼이다. 이더리움 플랫폼은 추상화된 세부사항과 프로그래밍 환경을 제공함으로써 프로토타입 블록체인의 P2P 네트워크, 합의 알고리즘 등의 기본적인 구조를 구현하지 않고도 본 연구에서 제안한 프로토타입의 기능을 구현할 수 있다는 장점이 있다.

본 연구는 현재 서비스 중인 테스트 네트워크에서 프로토타입을 구현하고 테스트하였다. 향후 이더리움 네트워크를 별도로 구축한다면 교육청과 교육지원청이 풀 노드로서의 역할을 수행하여 블록체인의 건전성, 복원력 등의 특성을 달성할 수 있을 것이다. 각 학교는 라이트 클라이언트의 역할을 수행하여 블록 헤더 유효성 검사 등의 역할을 수행할 수 있도록 할 수 있다. 풀 노드의 수가 많으면 많을수록 블록체인의 신뢰성이 높아지므로 일부 지리적으로 분산된 학교에 그 역할을 부담시킬 수도 있다. 학생과 교육자(교사)들은 개인별 하드웨어와 네트워크 자원 운용의 한계가 발생하기 쉽다. 이를 고려할 때 학생과 교육자(교사) 노드는 이더리움의 원격 클라이언트로서 네트워크에 참여하는 것이 적절하다. 원격 클라이언트는 블록체인의 사본을 저장하지 않고 블록의 유효성을 확인하지 않지만, 지갑을 소유하고 트랜잭션을 생성하고 전파할 수 있다.

본 연구의 프로토타입은 솔리디티 언어를 사용하여 스마트 컨트랙트를 구현하였다. [알고리즘 1]의 코드는 [그림 3]의 5단계인 머클 트리를 생성하는 과정에서 수행되는 스마트 컨트랙트의 예를 보여준다. 머클 트리에 필수적으로 포함되어야 하는 SQL 코드와 그 대상이 되는 학생, 교사, 학교의 주소, SQL 실행 결과와 SQL 실행 타임스탬프가 머클 트리에 기록된다.

알고리즘 1. Solidity를 사용한 스마트 컨트랙트의 예

```
pragma solidity ^0.4.18;
contract test {
    address student;
    address teacher;
    address school;
    string sql;
    string result;
    uint timestamp;

    function SetTest(string _sql, uint _timestamp, string _result,
                     address _student, address _school) public {
        student = _student;
        teacher = msg.sender;
        school = _school;
        sql=_sql;
        result=_result;
        timestamp=_timestamp;
    }
    function GetTest() public view returns(string, uint, string,
                                           address, address, address)
{
        return(sql, timestamp, result, student, school, teacher);
    }
}
```

[표 1]과 [표 2]는 배포된 스마트 컨트랙트의 동작을 테스트하기 위하여 임의로 부여된 데이터이다. 테스트에서 [표 1]과 같이 4가지 유형(교육청, 학생, 학교, 교사)의 테스트 계정 주소를 사용하였다. 우선, 교육청 주소를 가진 노드가 [알고리즘 1]의 스마트 컨트랙트에 대해 생성 트랜잭션을 수행하여 배포하였다. 그다음 학적부 데이터베이스에 대한 작업을 교사 노드에서 수행하였으며, [표 2]와 같이 그 결과가 성공적으로 저장되었음을 확인하였다.

[표 2]의 내용을 자세히 살펴보면 status에 성공적으로 트랜잭션이 실행되었으며 이를 실행시킨 노드의 주소는 from을 통해 교사임을 알 수 있다. 이더리움에서는 트랜잭션을 생성하고 배포하기 위해 가스라는 화폐

를 사용하는데 이는 교육청에서 급여처럼 교사와 학교에 지급하는 방법을 고려해 볼 수 있다. 스마트 컨트랙트의 주요 변숫값으로 저장된 내용은 decoded input을 통해 확인할 수 있다.

표 1. 테스트를 위한 사용자의 주소와 구분

구분	주소
교육청	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
학생	0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2
학교	0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db
교사	0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB
...	

표 2. 스마트 컨트랙트 실행 결과

분류	내용
status	true Transaction mined and execution succeed
transaction hash	0x85f19b4eaf02a9cbb7f7147f43c0cae8ddd618e1a6d884c053fe95ca0a225c77
from	0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB
to	test.SetTest(string,uint256,string,address,address) 0xd9145CCE52D386f254917e481eB44e9943F39138
gas	3000000 gas
transaction cost	152242 gas
execution cost	125530 gas
hash	0x85f19b4eaf02a9cbb7f7147f43c0cae8ddd618e1a6d884c053fe95ca0a225c77
input	0x6f4...00000
decoded input	{ "string _sql": "insert query", "uint256 _timestamp": { "type": "BigNumber", "hex": "0x602f6251" }, "string _result": "success", "address _student": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2", "address _school": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2" }

표 3. 기존 시스템과 제안 시스템과 성능 비교

비교 요인	기존 시스템	제안 시스템 (하이브리드 시스템)
데이터 가용성 및 복구	약함 (중앙 서버)	강함 (분산 저장)
외부 공격에 대한 보안 (재해, 물리적 침입)	보통 (중앙 서버)	강함 (분산 저장)
내부 공격에 대한 보안 (관리자에 의한 데이터 훼손)	약함	강함
무결성 인증	X	O
데이터 변경 추적	X	O

현재 운영 중인 나이스 시스템과 본 연구에서 제안한 하이브리드 시스템을 비교 분석한 결과는 [표 3]과 같다. 나이스 시스템은 중앙 집중형 시스템으로 신뢰할 수 있는 원장을 관리하기 위하여 백업 서버를 다수 운영하고 방화벽을 구축하는 등 높은 비용과 노력을 소모한다. 그러나 이미 훼손이나 변형이 된 데이터에 대한 인증과 변형이 어려우며, 악의적인 내부자에 의한 공격에는 취약하다는 단점이 있다.

본 연구에서 제안한 하이브리드 시스템은 기존 중앙 서버는 그대로 운영하면서 데이터의 접근 기록이 모두 블록체인으로 기록된다. 따라서 중앙 서버에 기록된 데이터의 무결성 인증이나 변경 추적이 가능하다. 블록체인은 분산 저장되기 때문에 일부 블록체인을 저장하고 있는 풀 노드나 데이터베이스를 보관하는 서버가 공격을 당한다고 하더라도 블록체인의 특성상 복구가 가능하다.

V. 결론

각 학교에서 운영했던 행정 정보를 통합한 나이스 시스템은 분산되었던 정보를 통합하여 관리를 쉽게 만들었다. 학부모가 자녀의 학교생활을 더욱 쉽게 확인할 수 있는 편의를 제공하고 있고 비대칭 암호화를 이용하여 권한이 부여된 사람만 열람 및 수정할 수 있도록 보안에 힘쓰고 있다.

하지만 학교장 또는 권한을 위임받은 교사가 학생의 성적을 임의로 조작하거나 학생의 동의 없이 정보를 유출하는 문제가 발생하고 있다. 학생의 개인 정보를 포함하는 학생생활기록부는 상급 교육기관으로 진학하기 위해 중요한 자료로 사용되기 때문에 불법 유출이나 조작 등의 악의적인 행위가 이루어져서는 안 된다. 나이스 시스템의 모든 정보를 블록체인에 저장하면 보안성을 더욱 향상시킬 수 있으나 기존 중앙 서버의 방대한 데이터를 블록체인에 옮길 경우 블록의 양이 많아져 검증에 필요한 자원과 처리 시간이 증가되는 문제점이 있다.

이를 개선하기 위해 본 논문에서는 기존 중앙 집중형 방식과 블록체인의 특징을 결합한 하이브리드 시스템을 제안하였다. 이더리움을 사용하여 제안한 시스템의 프로토타입을 제시하여 구현 가능성을 검증하였다. 제안한 시스템은 블록체인의 장점을 채택하여 기존의 문제점을 개선하면서도 현재 사용 중인 시스템을 유지하

여 현실성과 안정성 두 가지 목적을 모두 달성하였다. 이를 통해 악의적인 사용자가 중앙 관리되는 데이터베이스를 조작한다고 하더라도 분산 저장된 블록체인을 통해 데이터의 훼손을 검증하여 무결성을 지킬 수 있을 것이다. 블록체인에 저장되어 있는 쿼리와 데이터베이스의 정보, 학생의 킷값을 확인하여 수정 및 증명서 발급이 되기 때문에 현 나이스 시스템에서 발생할 수 있는 위·변조를 방지할 수 있을 것이다. 그뿐만 아니라 기존 나이스 시스템에서 발생할 수 있는 위·변조 시 원본 데이터 유실에 관련된 문제를 본 논문의 시스템에서 제안한 쿼리를 블록에 저장함으로서 조작된 데이터가 있을 경우 쿼리가 저장된 블록체인을 통해 원본 데이터를 찾아 원상복구할 수 있다.

그러나 본 논문은 나이스 시스템에서 관리하는 모든 지역의 서버가 아닌 각 서버에서만 적용되는 모델이다. 학생이 교육청에서 관리하는 지역을 벗어나 다른 지역으로 전출 갈 때 해당 학생의 정보 또 한 전출가는 지역의 서버로 이전된다. 때문에 본 논문에서 제안한 하이브리드 시스템이 적용되지 않는다는 제한점을 가진다.

이러한 제한점을 해결하기 위해 향후 학생이 다른 도 교육청 담당으로 전출 갈 경우에도 본 논문에서 제안한 하이브리드 시스템을 적용하기 위해 학생의 데이터베이스 정보뿐만 아니라 블록체인도 함께 옮겨 갈 수 있는 크로스 체인 형태의 연구가 필요하다.

참 고 문 헌

[1] 전북교육연구정보원, *2020학년도고등학교나이스사용자설명서(성적)*, 2020.

[2] https://news.kbs.co.kr/news/view.do?ncd=3627443

[3] https://news.joins.com/article/20685150

[4] 교육부, https://www.moe.go.kr

[5] Nakamoto and Satoshi, *Bitcoin: A peer-to-peer electronic cash system,* Manubot, 2019.

[6] T. Alladi, V. Chamola, R. M. Parizi, and K. R. Choo, "Blockchain Applications for Industry 4.0 and Industrial IoT: A Review," in IEEE Access, Vol.7, pp.176935-176951, 2019.

[7] 한국교육개발원, *교육통계분석자료집*, 2020.

[8] M. 안드레아스, 안토노폴로스, *비트코인, 블록체인과 금융의 혁신*, 고려대학교 출판부, 2015.

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

[10] M. D. Sleiman, A. P. Lauf, and R. Yampolskiy, "Bitcoin message: Data insertion on a proof-of-work cryptocurrency system," 2015 International Conference on Cyberworlds, pp.332-336, 2015.

[11] 손기봉, 손민영, 김영학, "학점은행제를 위한 블록체인 시스템," 한국콘텐츠학회논문지, 제20권, 제5호, pp.11-22, 2020.

[12] 정현준, 이흥노, "블록체인개발 현황과 보안이슈 변화 동향," 정보보호학회지, 제28권, 제3호, pp.47-52, 2018.

[13] 이제영, "블록체인 3.0 시대와 암호화폐의 미래," FUTURE HORIZON, 제37호, pp.32-35, 2018.

[14] M. Zaid, M. Waheed Akram, N. Ahmed, and S. Saleem, "Web Server Integrity Protection Using Blockchain," 2019 International Conference on Frontiers of Information Technology (FIT), Islamabad, pp.239-2395, 2019.

[15] C. H. Lee and K. Kim, "Implementation of IoT system using block chain with authentication and data protection," 2018 International Conference on Information Networking (ICOIN), Chiang Mai, pp.936-940, 2018.

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

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

[18] A. Grech and A. F. *Camilleri, Blockchain in Education, Inamorato dos Santos A(ed),* EUR 28778 EN, 2017.

[19] Shallu Sharma, Ranbir Singh Batth, "Blockchain Technology for Higher Education Sytem: A Mirror Review," Intelligent Engineering and Management (ICIEM) 2020 International Conference on, pp.348-353, 2020.

저 자 소 개

손 기 봉(Ki-Bong Son) 정회원

- 2012년 2월 : 가톨릭대학교 컴퓨터정보공학부(공학사)
- 2015년 8월 : 조선대학교 전기·전자·통신교육(교육학석사)
- 2015년 9월 ~ 현재 : 금오공과대학교 컴퓨터공학과 박사과정

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

손 민 영(Min-Young Son) 정회원

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

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

김 영 학(Young-Hak Kim) 종신회원

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

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