산업융합연구 제21권 제7호 pp. 41-49, 2023
ISSN 2635-8875 / e-ISSN 2672-0124
DOI : https://doi.org/10.22678/JIC.2023.21.7.041

위변조에 안전한 블록체인 기반 학력 검증 시스템 설계 및 구현

박중오*
성결대학교 파이데이아학부 조교수

Design and Implement a Forgery-safe Blockchain-based Academic Credential Verification System

Jung-oh Park*
Assistant Professor, Division of Paideia, Sungkyul University

요 약 최근 다양한 교육기관에서 졸업 및 성적에 관련된 학력 검증에 온라인 증명서 서비스의 활용도가 높다. 그러나, 기존 시스템의 증명서는 사실 여부와 세부 학력에 대한 검증과 추적에 한계가 있다. 관련하여 온라인/오프라인 증명서의 위조/변조 사건이 지속하여 발생하고 있다. 본 연구는 대학 기관을 중심으로 위변조에 안전한 블록체인 기반 검증 시스템을 제안한다. 학과 별 세부 수업 카테고리와 출석 및 세부 성적 등 필요한 정보를 수집/분석하여 연계 관계를 블록체인으로 생성했다. 이외 블록체인 공유에 필요한 시스템/네트워크 환경을 고려하였고, 독립적인 웹 애플리케이션 형태의 확장 모듈로 구현했다. 블록체인 검증 결과, 학력 정보의 안전한 신뢰 검증과 세부 정보들의 관계를 추적할 수 있음을 증명하였다. 본 연구는 향후 국내 교육기관 학력 검증 서비스 및 정보 보안 개선에 이바지하고자 한다.

키워드 : 학력 정보, 웹-애플리케이션, 블록체인, 교육 기관, 웹 보안

Abstract In recent years, various educational institutions have used online certificate services to verify academic achievement related to graduation and grades. However, the certificate of the existing system has limitations in verifying and tracking whether it is true or not and detailed academic background. In this regard, cases of forgery/falsification of online/offline certificates continue to occur. This study proposes a blockchain-based verification method that is safe from forgery and alteration, focusing on university institutions. Necessary information such as detailed class categories for each department, attendance, and detailed grades was collected/analyzed to create a linkage relationship through blockchain. In addition, the system/network environment required for blockchain sharing was considered, and it was implemented as an extension module in the form of an independent web application. As a result of the block chain verification, it was proved that the safe trust verification of educational information and the relationship between detailed information can be traced. This study aims to contribute to the improvement of academic credential verification services and information security for Korean educational institutions in the future.

Key Words : Academic background, Sharing the information, Data standards, Educational institutions, Information verification

*Corresponding Author : Jung-oh Park(pjo21@naver.com)
Received May 17, 2023
Revised June 15, 2023
Accepted July 20, 2023
Published July 28, 2023

1. 서론

학력 검증은 관공서, 교육기관, 기업체 등 취업 및 승진과 직접 연결되기 때문에, 명확한 신뢰 검증기관을 통해 진위를 검증해야 한다. 그러나 단순 증명서 진위가 아닌 학위를 부풀려 표기하거나 조금씩 다르게 표기하는 등 정보를 일부 변경하면 자동화된 증명서 검증 시스템에서 조회가 어렵다. 최근 대검찰청에 의하면 학력 위조로 부정 취업과 대학원 진학한 피의자 등 95명을 검거한 사실이 있다[1]. 실제 대학 및 대학원(학위) 증명서, 주민등록등본, 가족관계증명서 등 온라인으로 출력된 PDF나 오프라인으로 출력된 문서를 위/변조했다. 대법원 판례에 따르면 전자파일 및 기록은 형법상 문서 죄 처벌에 사각지대의 가능성이 존재한다[2]. 핵심 문제는 증명서 검증 시스템의 한계와 세부 학력에 대한 법적 판단과 분석의 어려움이다. 단순 증명서 검증으로는 이력의 세부 정보를 검증할 수 없다.

본 논문은 대학 기관을 중심으로 새로운 학력 데이터 모델을 설계하고, 위/변조에 안전한 블록체인 기반의 학력 검증 기법을 제안한다. 본 논문의 구성은 다음과 같다. 2장 관련 연구에서 기존 학력 위/변조 검증의 문제점 분석과 기존 블록체인 위/변조 관련 연구를 비교 분석한다. 3장은 제안하는 블록체인 기반 검증 기법을 설명한다. 4장은 안전성 및 성능 분석, 5장은 결론으로 마친다.

2. 관련 연구

2.1 기존 학위 검증의 문제점 분석

학력 위조는 석/박사, 의료인, 변호사, 유명기관 인증 등 부당한 이익(사회적 지위와 명성, 수많은 금전적 혜택)을 목적으로 정보를 과장/사칭 또는 위/변조하는 모든 행위를 의미한다[3].

2.1.1 가짜 증명서

국내 대학 기관의 경우 대부분 인터넷 증명발급이 가능하고, PDF 파일 또는 온라인 출력으로 목적에 따라 기관에 제출할 수 있다. 문제는 학교 출신의 학생이나 지인 등 다양한 경로로 임시 증명서를 구할 수 있어, 이를 손쉽게 위/변조할 가능성이 있다. 서명된 PDF 파일 등 문서는 바이너리 수준에서 취약점(Exploit) 등 변조가 가능하다[4]. 경찰은 SNS를 통해서 위조 증명서를 제작·판매한다는 수십 개 업체 광고에 대해 주의를 통보하기도 했다[5].

2.1.2 이력서 허위 기재

이력서에 존재하지 않는 이력을 일부 추가하거나, 확인이 어려운 내용을 다르게 표기하는 등 모든 경우를 의미한다. 이는 기존 검증 시스템의 증명서로 확인이 어렵기 때문에, 직접 기관에 문의 등 사람이 오프라인에서 사실관계를 분석해야 한다. 증명서와 달리 관계 증명이 필요하므로, 검증 시간이 길고 복잡해질 수 있는 점을 악용할 수 있다. 대법원 판례에 따르면 A의 경력이 허위이고 기간을 과장했기 때문에 해고하는 것이 정당하지만, 일한 동안의 임금은 지급해야 했다[6]. 즉, 허위 기재로 인한 피의자의 손해가 크지 않음을 나타낸다.

2.1.3 학위 수료 사칭

석사/박사 과정에서 학위를 수료한 상태(학점만 이수, 졸업 논문 없음)를 학위를 정상 수여 받았다고 표기하는 경우이다. 정상 학과 소속으로 등록되어 있으므로, 사람이 직접 수료라는 사실 여부를 직접 판단해야 한다. 제출한 증명서는 분명 정상으로 판별되나, 졸업과 수료는 확실히 큰 차이가 있다. 검증 과정에서 취직 및 승진이 취소되는 경우 지원자는 큰 문제가 되지 않는다. 대법원 판례에 의하면 일반적으로 상향 사칭에 대해서 징계 사유로 인정했지만, 하향 사칭의 경우 징계 사유로 인정하지 않았다[7]. 수료 사칭에 대한 처벌이 비교적 가볍다는 점을 악용할 수 있다.

2.1.4 기타(저서, 논문, 상장)문서 위조

개인 저서, 학위 논문, 상장 수여 등의 사문서를 위조하는 경우이다. 실제 온라인으로 올린 문서 파일이 존재하는 경우 조회가 가능하지만, 검증 시스템 수준에서 이를 일일이 검사할 수 없는 점을 악용할 수 있다. 이력 관련 증명 자료를 보통 오프라인 출력으로 첨부하여 서류를 제출하는 형태가 일반적이기 때문이다. 사문서위조는 형법 231조 위/변조에 대해 5년 이하 징역 또는 1천만 원 이하 벌금으로 형법 225조 공문서위조(10년 이하 징역)에 비해 처벌이 미약한 편이다[8,9].

2.1.5 전공 지식, 인물 관계

학력과 관련 없는 전공 지식, 같은 학과에 교수 또는 유명 인물 등 활동 내용 등을 허위로 기재할 수 있다. 증

명할 수 없는 정보들은 확인할 방법이 없다. 타인 사칭의 경우 특별한 피해나 명예 손해가 없는 경우 이를 처벌할 입법이 없는 실정이다[10]. Table 1은 기존 검증 시스템의 다양한 문제점을 분석한 결과이다.

Table 1. Verification system(existing) problem analysis

Malfeasance	Verification method	Problem
Fake Certificate	Certificate Authenticity	Forgery, Falsification
False Entry	Reak Check	Very Time consuming
Impersonating a Degree	Certificate Authenticity, Reak Check	Ambiguity of Judgment
Forgery of Other Documents	Unverifiable, Reak Check	Forgery, Falsification
Major Knowledge and Personal Relationships	Unverifiable	Unverifiable

대체로 기존 증명서 검증 시스템의 한계는 명확하다. 단순 증명서 진위를 확인 이외에는 위/변조에 대한 신뢰가 어렵다. 즉, 복잡한 허위 이력과 다양한 관계 사실의 검증 방법으로서 적합하지 못하다. 자동화된 시스템으로 검증을 운영하지 않으면, 미숙한 기존 검증 정책과 함께 법적 제도를 악용한 범죄가 지속 반복되어 발생할 것이다. 학력은 대부분 개인 이력의 한 부분으로 포함된다. 이는 오랜 시간 동안 위/변조에 안전한 검증 방법에 관한 연구가 필요하다는 것을 의미한다.

2.2 블록체인 기반 위/변조 방지 연구분석

최근 블록체인 기반 기술은 탈중앙화 보호 기술로써 금융/물류/제조 등 산업 분야에서 분산원장 또는 공공 거래 장부 등 다양한 데이터의 보호 목적으로 활용되고 있다. Table 2는 본 연구에서 조사/분석한 블록체인 기반 연구 논문을 비교 분석한 것이다. 최근 3년 이내 전 분야에 걸쳐 확장 모듈로써 개발하기 쉬운 웹 환경, 비교적 소규모 네트워크, 구현을 통한 안전성 및 성능 분석 등 대학 기관의 데이터 관리(추적성)에 적합한 연구 논문[11-18]을 분석했다.

Hong은 블록체인 기반 DID(Decentralized Identity) 신원 증명이 높은 신뢰성을 제공하고, Wang은 다중 사용자 및 익명 인증 등 다양한 블록체인의 높은 활용성을 설명했다[11,12]. Bae는 기존 블록체인의 위변조 검증에 트랜잭션의 보안성과 성능 개선의 필요성에 관해 설명했고, Adnan은 정보의 전파력이 높은 뉴스를 검증하여 가짜(위변조된)정보 확산을 방지했다[13,14].

Table 2. Blockchain-based research analysis

Paper	Function	Distributed sharing	Block-chain
User Management	Authentication	Certificate	Ethereum
	Anonymous Authentication	Authentication Information	Ethereum, PBFT, etc.
Certification Management	Forgery verification	Certificate	Hyperledger Fabric
News Management	Forgery verification	News Content	Ethereum
Exam Cheating Detection	Cheat Detection	Facial Recognition	Self-Development
Grade Management	Grade Management	Study Information	Ethereum
File Management	Sharing of Files	Drawing (BIM)	Self-Development
Car Management	Decentralization	Maintenance History	Ethereum, EOS, etc.

Nam은 온라인 시험에서 안면 인식 등 시험 진행 중에 모든 정보를 블록체인으로 생성하여 부정행위를 탐지했다[15]. Son은 학습자의 학점과 학위 정보를 공개 원장에 기록하여 공유하는 방식으로 학습자의 세부 정보에 대한 추적의 용이 등 관리 효율성 증대를 설명했다[16]. Seo는 분산된 BIM 파일의 저장에 분산 파일 시스템과 함께 블록체인을 적용함으로써 지속적인 파일 저장에 대한 효율성, Jo는 P2P 네트워크 구축과 자동차 관련 정보를 연계하는데 다른 분야(외부) 주체에 대한 권한 분산 기법을 설명했다[17,18].

3. 블록체인 기반 학력 검증 기법

3.1 학력 검증 시스템 요구사항 분석

Table 3은 앞서 연구 논문의 분석 결과 블록체인 기반 검증 시스템 개발 요구사항을 도출한 결과이다.

Table 3. Functional requirements

Functions	Development	Method
User authentication	Public Key	Protocol
Forgery checks	Encryption/Decryption	Lightweight
Fraud detection	Detection	Protocol
Traceability	Data modeling	SQL Compatibility
file systems	Distributed	-
External lookup	Server Redirect	Protocol

3.1.1 사용자 인증

아이디, 패스워드 이외 내부 프로토콜 수준에서 추가 인증을 수행한다. 회원가입에서 교환한 공개키를 기반으로 사용자의 서명을 개인키로 검증하는 방식을 의미한다. 보안성 강화를 위해 인증용 키는 (RSA-2048)을 사용한다.

3.1.2 위변조 검사

사용자(관리자 포함)로부터 입력 데이터는 실시간으로 암호화하고, 기존 체인의 데이터와 일치하는지 서명을 검사한다. 기본 암/복호키는 안전하다고 알려진 AES-256 표준 암호 알고리즘을 사용한다.

3.1.3 부정행위 탐지

전체 수행과정에서 정상적이지 않은 요청 및 다수 요청 처리를 탐지하고 기록하는 기능을 프로토콜 상에서 구현한다. 비정상 IP 주소 탐지, 로그인 시간/횟수에 대한 임계치 검사가 일반적이다.

3.1.4 추적성(학력 관계 분석)

일반 대학 기관에서 관리하는 학력의 공통요소로 추출하고, 이외 정보들을 조합(쿼리문 조인)하여 검증 시스템 전용 데이터베이스를 구축한다. 조합이란 기존 데이터베이스로부터 새로운 데이터베이스를 생성하는 과정을 의미한다. 초기 데이터베이스 생성 후 최상위부터 최하위 테이블 사이 새롭게 입력되는 학력은 1개 이상의 고유 키를 포함하여 관계를 생성한다.

3.1.5 분산 파일 시스템

본 연구에서 블록체인으로 생성하는 학력 정보 모델은 데이터베이스에 분산된 정보를 일부 활용하기 때문에, 실제 수 킬로바이트 이하로 용량이 작다. 작은 파일의 빈번한 접근 및 검증의 성능 최적화가 우선이기 때문에 대용량 파일 처리를 위한 분산 파일 시스템으로 확장하지 않는다.

3.1.6 외부 조회

외부 기관이나 기업의 학력 검증 조회를 위해 읽기전용의 일회성 공개 URL 링크를 임시로 생성한다. 이력서 제출이나 메일 전송 단계에서 조회에 동의하에 제공한다는 부분을 명시해야 한다.

3.2 제안 검증 모델 계층과 동작 과정

Fig. 1, 2는 전체 학력 검증 기법의 계층과 세부 동작 과정을 나타낸다.

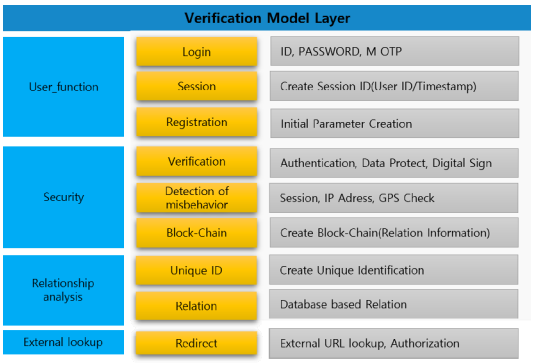

Fig. 1. Verification model layer

분석 결과 학력 검증에 필요한 대표 계층으로 첫 번째 사용자 기능(로그인, 세션, 등록), 둘 때 보안(인증, 데이터보호, 서명 등), 셋째 관계 분석(고유 정보 식별), 넷째 외부 조회(임시 URL 생성, 외부 요청 인가) 계층으로 정의했다. 웹 브라우저를 통한 접근을 고려하여, 웹 서버 내부 애플리케이션 수준으로 구현한다. 사용자 인증에 앞서

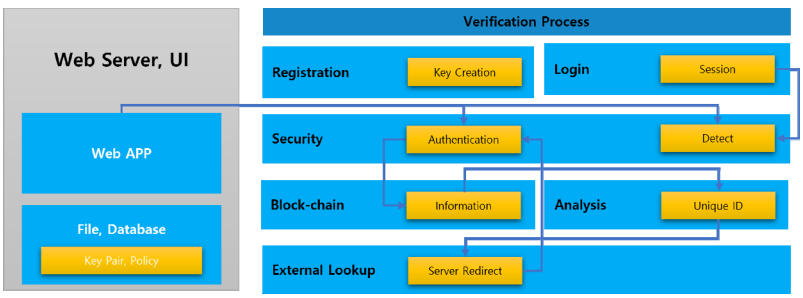

Fig. 2. Verification process

반드시 사용자 등록과정이 선행되어야 한다.

3.2.1 사용자 등록과정

암호화/복호화에 필요한 공개키/개인키를 생성하고 교환하는 과정을 포함한다. RSA 알고리즘 기반으로 n(n = p * q, n)을 구하고, $\phi(n) = (p-1) * (q-1)$를 구한다. $1 < e < \phi(n)$에 서로소를 만족하는 e를 구한 후 $(e * d) \bmod \phi(n) = 1$을 만족하는 개인키(n, d)를 생성한다. 개인키와 공개키는 로그인 과정에서 활용한다.

3.2.2 사용자 로그인(세션)

사용자의 로그인 요청 이후 고유 세션 ID를 생성한다. AES-256 알고리즘 기반 세션 키(세션 ID, 공개키(n, e)))인 S를 생성한다. 세션 키의 역할은 내부 데이터의 암/복호화를 수행한다. 표준 웹 스토리지(Web Storage)를 활용하여 저장한다.

3.2.3 보안(인증 및 암호화)

블록체인에 추가된 정보를 암호화/복호화를 수행한다. 사용자 인증에 공개키(n, e)로 암호화(C = (M ^ e) mod n)하고, 개인키(n, d)로 복호화(검증)할 수 있다. 블록체인 데이터의 추가/수정/삭제 등에 동일한 암/복호화를 수행하며, 이외 세션 키(S)를 공개키(n, e)로 암호화하여 서명을 생성한다. 이후 사용자는 개인키(n, d)로 세션 키(S)를 얻을 수 있다. 서명 값 생성은 SHA 해시 알고리즘을 사용한다.

3.2.4 보안(탐지)

블록체인 업데이트마다 임시 생성한 세션 값 검사 이외 IP 주소와 GPS 위치 정보를 추가 확인한다. 이는 중간자 공격(제3자)의 이상 접근을 탐지하기 위한 기본적인 보안 기능이다.

3.2.5 블록체인

사용자가 웹상에서 입력하는 정보를 기존 블록체인에 추가하고 업데이트하는 과정을 의미한다. Table 4는 학력 정보의 테이블 관계를 연결하여 표현했다.

Table 4. Relation information – table

TABLE NAME	COLUMN NAME	RELATION
EDU	UNI, GRAD	–
MEMBER	USER_ID, NAME, NUM	EDU
LECTURE	NUM, NAME, ROOM, TIME	MEMBER
ATTENDANCE	NUM, CHECK,. ROOM, TIME	LECTURE
SESSION	USER_ID, S_ID, S_KEY, TIME	MEMBER
DATA	ID, MEMBER, LECTURE, ATANDENCE	DATA 1~N

블록체인에 포함되는 기본 정보는 최상위에 대학교, 사용자, 강의, 출석, 세션(시간) 등 공통정보들을 표기하고, 데이터 내부에 연계된 세부 정보들을 포함하는 형태이다. 각 데이터는 블록체인의 변화에 따라 데이터를 업데이트 및 추가한다. Fig. 3은 제안 환경에서 블록체인 생성 및 처리 과정을 나타낸다.

사용자의 입력에 대해 해시값을 생성하고, 비밀키로 암호화 서명을 생성한다. 추가된 학력은 블록체인 분산원장에 기록되며, 내부 트랜잭션 정보를 교환하게 된다. 이후 분산된 네트워크에 해시값이 전송되고, 웹 서버 측 데이터베이스에 암호화하여 저장한다.

3.2.6 관계 분석

블록체인 내 추가되는 학력은 고유 식별자를 통해 연결된 해시값을 통해 관계를 형성하게 된다. 학력을 나타내는 기본 항목의 예는 앞서 표와 같이 대학교, 학과, 출석, 학생, 강의를 연계했다. 각 항목의 고유 식별자를 조

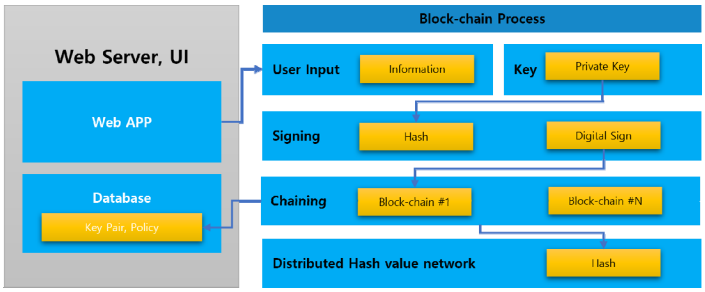

Fig. 3. Block-chain process

회한다. 학생을 기준으로 조회하는 경우 학과(학번, 이름), 강의(교수, 출석(시간)) 결과를 출력한다. 이외 세부 학력은 기존 기관에서 보유한 학력에 따라 속성 필드를 추가/변경하는 형태로 구현한다. 간단하게 조회 쿼리를 수정하면 된다. Fig. 4는 블록체인과 학력을 검증하는 방법을 나타낸다.

본 연구는 소규모 네트워크에 적합한 블록체인 알고리즘으로 PBFT(Practical Byzantine Fault Tolerant) 합의 알고리즘을 적용했다.

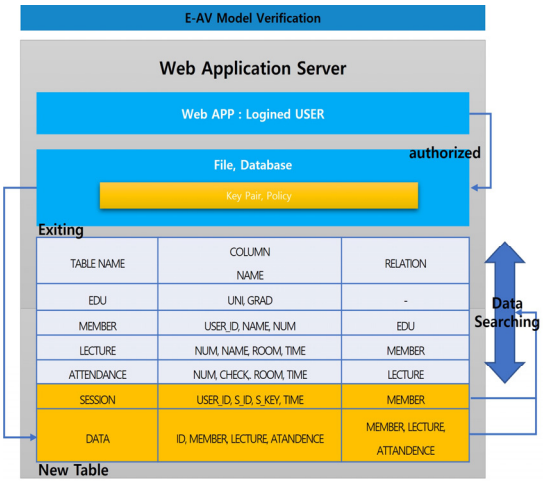

Fig. 4. Block-chain - verification

블록체인이 추가되는 경우 사전에 요청 유효성을 검사하고, 트랜잭션을 확인한 후 입력된 노드를 전체 네트워크에 전파한다. 노드의 2/3 다수가 유효한 경우 블록체인에 트랜잭션을 추가한다. 블록체인 네트워크 내 추가된 학력이 위변조에 안전하다고 선행 검증 후, 데이터베이스 내 조회 내용을 추가 비교 검증한다.

4. 안전성 및 성능 분석

4.1 실험 환경 설정

Table 5는 제안 기법의 개발을 위한 실험 환경을 나타낸다.

실험 환경은 리눅스 16.04 커널에서 80 포트에서 동작하는 임시 웹 서버(Apache) 환경을 구축했다. 내부 확장 모듈에는 인증 수행에 RSA 암호화/복호화를 위한 openssl, JSEncrypt 라이브러리, 블록체인 구현에 자바 프로그래밍 언어 Cipher 클래스를 활용했다.

Table 5. Development environment

-	Software and Language
OS	Linux 16.04 Kernel
Web Server	Apache 2
Programing Language	HTML5, JS, JAVA
Database	Mysql 5.7
External Library	OPENSSL, JSEncrypt Cipher Class(javax.)

4.2 위/변조에 대한 안전성 분석

Table 6은 취약점별 대응책으로 표준 프레임워크의 개발환경인 자바 언어와 내부 WAS(웹 서버 + 탐켓)의 보안 설정을 의미한다.

Table 6. Security requirements and safety analysis

requirements	Legacy Environment	Improvements
Consensus Algorithm	PBFT Algorithm	Add database validation
Session Key Exposure	HTTPS, requires implementation	Add unique session key
Third-party attacks		Mutual authentication on independent channels
Attack detection	requires implementation	IP Address, GPS checks

4.2.1 합의 알고리즘

PBFT의 합의 알고리즘은 기본적으로 악의적인 노드가 n개 있을 때, 전체 노드 개수가 3n+1개 이상 검증되면 합의는 신뢰할 수 있다. 합의 알고리즘은 무결성을 보장하면서 위변조된 악의적인 노드의 최대 1/3이 존재할 수 있다. 본 연구는 이를 보완하기 위해 추가 암호화된 데이터베이스의 블록체인 고유 식별자 정보를 양방향 검증했다.

4.2.2 세션 키 노출

세션 키는 기존 웹 사이트 수준에서 HTTPS 프로토콜을 사용으로 안전하게 전송할 수 있지만, 본 연구는 로그인에서 사용되는 임시 파라미터를 활용하여 공유 세션 키를 추가 적용했다. 공유 세션 키는 직접 공유되지 않고, 앞서 HTTPS 내에서 인증된 사용자만 접근할 수 있다. 서버의 헤더 보안, 세션 제한, 세션 키 재사용 제한 등 기존 알려진 세션 보호 기법은 모두 추가 구현이 필수가 아닌 선택사항이기 때문에 추가 설명하지 않는다.

4.2.3 제 3자 공격

블록체인 생성에서 교환한 키 쌍을 활용하여 서명을 검증하고, 상호인증을 수행하여 보안 및 기밀성을 보완한다. 이는 HTTPS 프로토콜과는 다른 독립적인 보안 채널에서 수행한다. 본 연구는 제 3자 공격의 능동적으로 방어하기 위한 공격 탐지 기법을 추가 구현했다. 외부 해킹의 경우 실시간 취약점 모니터링 및 이상 행위 탐지가 필수이기 때문이다.

4.2.4 공격 탐지

일반적으로 기관 내에서 접근하는 사용자에 대해서 할당된 고유 IP 주소 범위가 아니면, 보안 강화를 위한 추가 인증을 수행할 수 있다. 예로 수강 신청의 경우 외부 네트워크에서 수행할 수 있지만 모바일 OTP 등 인증을 추가 수행해야 한다. 출석 체크의 경우 물리적인 실제 위치를 나타내는 GPS 정보를 확인하여, 사용자의 기관 내 정상 접근 여부를 판단한다.

4.3 성능 비교 분석

Table 7은 PBFT 합의 알고리즘의 성능분석 - 기본 설정 정보를 나타낸다.

Table 7. Block-chain algorithm setting

	Description
Block-chain	Private, PBFT
Transactions	10~20
Node	10, 50, 100, 500, 1000
Access	Local, External
Size	100byte(Variable)

실제 사용자의 장치는 GPS를 포함하는 모바일 장치이다. 본 성능분석은 모바일 네트워크가 잘 연결됨을 가정(거리 및 전송률 제한 없음)하고, 제안 블록체인 자체의 성능을 비교 분석했다. 사용자 노드의 수를 10명, 50명, 100명으로 구분하여 10~20 트랜잭션의 처리 성능 오버헤드를 비교 분석했다. 접근 방식의 경우 내부는 정상 사용자의 경우 처리 속도(공격 탐지 포함), 외부는 IP, GPS가 검증이 아닌 추가 인증을 수행하는 경우이다. 기본 블록체인의 크기가 약 100byte(가변) 트랜잭션 크기를 사용한다.

100개의 트랜잭션 기준 임시 생성하는 세션(동일 크기)의 크기는 약 2n이다. 기관 내 사용자가 최대 10,000명을 가정했을 때, 필요한 저장소 공간은 2~3Mb의 블록체인을 생성한다. 예로 국내 대학생 수(대학 재학생 수 통계)가 가장 많은 대학교가 학생 수 약 2만 8천 명이다[19]. 3만 명을 예로 블록체인의 필요 공간은 10Mb 이내이다. 학력 추가로 인한 블록체인 증가에도 큰 문제가 없는 용량 수준이다. 즉, 서버에 통신 및 데이터베이스 공간에 큰 영향을 끼치지 않는다. 실제, 시스템의 성능에 영향을 주는 항목은 파악하기 위해 전체 블록체인 검증 성능을 추가 분석했다. Table 8과 Fig. 5는 블록체인의 생성/검증 과정의 평균 시간(ms) 나타낸다.

Table 8. Block-chain performance(ms)

Node	PBFT	Propose
10	35.11	41.20
50	79.53	92.17
100	587.82	731.32
500	2782.11	4151.07
1000	8101.26	10231.22

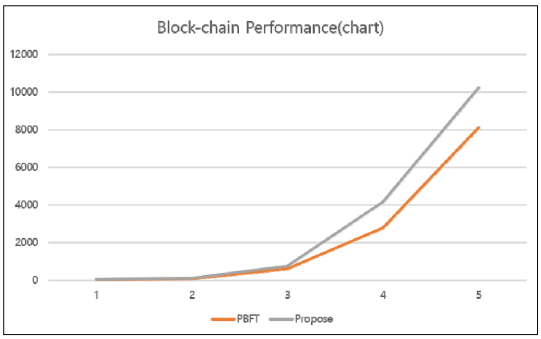

Fig. 5. Block-chain performance(chart)

노드 1개는 1명의 사용자를 의미한다. 10~50명의 동시 접속자는 평균 처리 시간 10 노드 기준 약 17%, 노드 50개 기준 약 15%의 오버헤드가 증가했다. 10~50 노드의 사용자 학력 검증에 0.06~0.13초의 지연(Delay)이 발생했다. 작은 크기의 데이터를 활용하기 때문에 통신량(Throughput)이 적고 지연이 매우 낮음을 알 수 있다.

100 노드부터 PBFT의 처리 지연이 급격하게 증가하여, 약 30% 가까운 성능의 오버헤드가 증가했다. 500 노드 이후부터 3~4초 처리 지연이 존재했고, 1000 노드 기준 최대 10초의 지연이 발생했다. 프로토콜 추가로 인한 성능의 오버헤드는 존재하는데, 가장 큰 요인은 노드 증가이다. 이는 블록체인 합의 알고리즘의 근본적인 문제이다. 자체 학력 검증을 확인하는 경우를 제외하고, 데이터베이스 내 전체 사용자의 학력을 동시에 전수 조사하는

경우는 드물다. 즉, 개인 사용자의 경우 성능적인 문제로 인해 큰 영향을 받지 않음을 알 수 있다. 전체 사용자가 세부 모든 항목에 대해 학력 검증을 동시에 수행할 확률은 낮기 때문이다.

5. 결론

문서 위변조를 전문적으로 수행하는 업체가 성행하고 있어, 기관에서 운영하는 시스템의 온라인/오프라인 증명서 위변조에 안전하지 않다. 본 연구의 학력 검증 시스템은 블록체인 기반의 연계된 학력 데이터베이스를 설계 및 구현했다. 웹 모듈 형태로 간단하게 구현되었기 때문에, 내부 데이터베이스 테이블에 적절하게 쿼리를 변환하는 수준으로 적용할 수 있다. 각 기관은 초기 도입 시기에서 데이터베이스 변환 작업, 그리고 보안 정책 및 내부 전산 행정절차가 추가 구현되어야 할 것이다.

성능분석 결과 PBFT와 같은 소규모 네트워크에서 사용하는 합의 알고리즘으로 충분히 블록체인 네트워크를 구축할 수 있다. 작은 크기의 블록체인 길이를 공유하기 때문에, 전수 조사 이외에 특정 사용자 조회에 최적화했다. 기관 내 추가적인 정보 및 대용량 데이터베이스를 활용하는 경우, 보안 강화를 위해 블록체인의 종류 및 암호학적 복잡도의 강도를 더 높이는 방안도 고려할 수 있다. 향후 연구로는 IP 주소 및 GPS 검증 등 모바일 장치에서 발생하는 고유 정보를 추가 활용하여 인증을 강화하는 연구로 개선할 계획이다.

REFERENCES

[1] Choi. S. W. (2022). 95 people arrested, including a suspect who fraudulently obtained employment by falsifying his doctoral degree, Retrieved from https://www.newsdaily.kr/

[2] Kim. H. C. (2020). Commentary on the Supreme Court case denying the documentary nature of electronic documents, Retrieved from https://m.lawtimes.co.kr/

[3] Lee. Y. J. (2013). A modern-day 'shepherd boy' The never-ending story of academic fraud, Retrieved from https://www.ohmynews.com/

[4] Mun. G. Y. (2019). PDF Docs Can't Be Manipulated? Vulnerability Study Shatters Preconceptions, Retrieved from https://www.boannews.com/

[5] Shin. J. H. (2022). '1.9 million won for a prestigious university'... Fake ads for education and career posted on SNS, Retrieved from https://www.joongang.co.kr/

[6] Supreme Court, (2018). 2017(242928) - Compensation for damages, Retrieved from https://www.scourt.go.kr/

[7] Supreme Court, (2009). Unfair Dismissal and Unfair Labor Practice Remedy Appeals Decision Reversed, Retrieved from https://www.law.go.kr/

[8] Supreme Court, (2020). Article 231 (Forgery and alteration of documents), Retrieved from https://www.law.go.kr/

[9] Supreme Court, (2020). Article 225 (Forgery and alteration of official documents), Retrieved from https://www.law.go.kr/

[10] Kim. J. H., (2020). Part 4. Riding the Blockchain, Future Logistics Will Be 'Fast and Secure, Retrieved from http://www.klnews.co.kr/

[11] Hong, S. and Kim, H. (2022) “A User-manageable Credential System based on Blockchain,” The transactions of The Korean Institute of Electrical Engineers. The Korean Institute of Electrical Engineers.
DOI : 10.5370/kiee.2022.71.1.210.

[12] Wang, J., Wu, L., Choo, K. K. R., & He, D. (2019). Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure. IEEE Transactions on Industrial Informatics, 16(3), 1984-1992.
DOI : 10.1109/TII.2019.2936278

[13] Bae. S. H, Lee. S. H & Jeong. D. W. (2020). Design and Implementation of a Blockchain-based Certificate Management System for Counterfeiting Prevention and Quick Authenticity Verification of Certificates. Journal of Korean Institute of Information Technology, 18(3), 67-77. DOI : 10.14801/jkiit.2020.18.3.67

[14] Qayyum, A., Qadir, J., Janjua, M. U., & Sher, F. (2019). Using blockchain to rein in the new post-truth world and check the spread of fake news. IT Professional, 21(4), 16-24.
DOI : 10.1109/MITP.2019.2910503

[15] Nam. G. M, Park. J. S. and Shon. J. G. (2022). A Blockchain-Based Cheating Detection System for Online Examination. KIPS Transactions on Software and Data Engineering, 11(6), 267-272. DOI : 10.3745/KTSDE.2022.11.6.267

[16] Son. K. B, Son. M. Y, & Kim. Y. H. (2020). Blockchain System for Academic Credit Bank System. The Journal of the Korea Contents Association, 20(5), 11-22. DOI : 10.5392/JKCA.2020.20.05.011

[17] Seo, J., Ko, D., Park, S., Kim, S., Kim, B.-S., & Kim, D. Y. (2021). Design and Implementation of a Blockchain System for Storing BIM Files in a Distributed Network Environment. Journal of the Korea Society of Computer and Information, 26(12), 159-168. DOI : 10.9708/jksci.2021.26.12.159

[18] Jo. B. J, & Kim. J. (2019). Design of Blockchain Application Model to Automobile Industry. Industrial Engineering & Management Systems, 45(6), 529-538. DOI : 10.7232/JKIIE.2019.45.6.529

[19] Ministry of Interior And Safety - Data Portal. (2022). Ministry of Education, Major Status by Department by University nationwide, Retrieved from https://www.data.go.kr/

박 중 오(Park, Jung Oh) [정회원]

• 2000년 7월 : 성결대학교 컴퓨터공학과 졸업
• 2003년 3월 : 명지대학교 전자계산교육 석사
• 2011년 8월 : 숭실대학교 컴퓨터공학 박사
• 2016년 3월~현재 : 성결대학교 조교수
• 관심분야 : Network security, Cryptography, PKI
• E-Mail : pjo21@naver.com