Journal of KIIT. Vol. 18, No. 3, pp. 67-77, Mar. 31, 2020. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2020.18.3.67

자격증 위조 방지와 빠른 진위 확인을 위한 블록체인 기반 자격증 관리 시스템 설계 및 구현

배승훈*, 이석훈**[1], 정동원**[2]

Design and Implementation of a Blockchain-based Certificate Management System for Counterfeiting Prevention and Quick Authenticity Verification of Certificates

Seunghun Bae*, Sukhoon Lee**[1], and Dongwon Jeong**[2]

요 약

이 논문에서는 자격증 위조 방지와 빠른 진위 확인을 위해 블록체인 기술을 이용한 자격증 관리 시스템을 제안한다. 자격증 위조는 사회적으로 심각한 문제를 초래하기 때문에 자격증 위조 방지에 대한 다양한 연구가 진행되어 왔다. 그러나 지금까지 수행된 연구는 위조 문제 및 진위 확인에 많은 시간이 소요된다는 문제점을 지닌다. 따라서 이 논문에서는 기존 연구의 한계점을 분석하고 보안성이 강화된 자격증 위조 방지와 빠른 진위 확인이 가능한 블록체인 기반 자격증 관리 시스템을 제안한다. 제안 시스템은 탈중앙화 형태로 위·변조가 불가능한 블록체인을 이용하여 기존 문제를 해결한다. 실험 및 평가 결과, 위조 방지와 진위 확인 시간 부분에서 기존 시스템보다 나은 성능을 보였다.

Abstract

This paper proposes a certificates management system based on blockchain technology for counterfeiting prevention and quick authenticity verification of certificates. Certificates counterfeiting raises serious problem in society, and thus various research has been studied on the counterfeiting prevention of certificates. However, the exiting research consumes much time for verifying the authenticity verification including the counterfeiting issue. Therefore, this paper analyzes the existing research and proposes a blockchain-based certificates management system that enables the anti-counterfeiting with enhanced security and quick authenticity verification of certificates. The proposed system in this paper is devised in a decentralized way and resolves the existing problems by using a blockchain that cannot be counterfeited. The experiment and evaluation shows an improved performance comparing with the existing systems.

Keywords

blockchain, certificate, counterfeiting prevention, authenticity verification

* 군산대학교 소프트웨어융합공학과 학사과정
- ORCID: https://orcid.org/0000-0002-3202-6390
** 군산대학교 소프트웨어융합공학과(교신저자)
- ORCID[1]: http://orcid.org/0000-0002-3390-5602
- ORCID[2]: http://orcid.org/0000-0001-9881-5336

· Received: Nov. 04, 2019, Revised: Jan. 02, 2020, Accepted: Jan. 05, 2020
· Co-corresponding Author: Dongwon Jeong and Sukhoon Lee
Dept. of Software Convergence Engineering, Kunsan National University, Korea
Tel.: +82-63-469-8912, Email: djeong@kunsan.ac.kr, leha82@kunsan.ac.kr

Ⅰ. 서 론

위조 기술이 발전함에 따라 자격증이 수많은 사이트를 통해 손쉽게 위조되고 있다[1]. 특히 자격증 중에는 생명과 연관된 자격증이 있으며 이러한 자격증이 위조되어 사용될 경우 많은 인명 피해와 경제적 손실 등 사회적으로 심각한 문제를 발생시킬 수 있다[2]. 이러한 자격증 위조 방지를 위한 다양한 연구가 진행되어 왔다[3]-[7].

[3]에서는 QR코드 및 디지털 워터 마킹을 이용한 인증서 위조 방지 시스템을 제안한다. QR코드는 모바일 기술의 발전으로 2차원 바코드 중 다른 바코드에 비해 많은 어플리케이션들이 개발되고 있으며, 빠른 속도로 확장되고 있다[8]. 그러나 QR코드는 누구든지 제작, 배포를 할 수 있다는 문제점을 지닌다.

[4]에서는 랜덤코드와 검증코드를 이용해 운전면허증 위조를 방지한다. 하지만 랜덤코드를 생성하는 해쉬 알고리즘과 식별코드가 유출될 경우 위조가 쉽게 가능하다는 문제점이 있다.

[5]에서는 다중척도를 이용하여 위조 인쇄물을 손쉽게 감식할 수 있는 기법을 제안한다. 하지만 원본 영상을 스마트폰을 이용해 미리 저장해야하는 비효율적인 문제점을 가지고 있다.

[6]에서는 지폐에 워터마크 등을 삽입시킴으로써 위조를 방지하는 기술을 제안한다. 하지만 워터마크가 삽입된 영상을 공격할 시, 완전하게 보안이 이루어지지 못한다는 문제점이 있다.

최근에는 2008년에 Satoshi Nakamoto라는 가명을 사용한 누군가가 비트코인을 소개한 것을 시작으로 금융·비금융권, 정부기관 등 많은 도메인에 중앙 데이터 저장 시스템이 아닌 탈중앙화를 지향하는 보안성이 뛰어난 블록체인 기술이 도입되고 있다[9]. 이러한 블록체인 기술을 기반으로 [7]에서는 블록체인을 이용한 졸업장 관리 시스템을 제안한다. 그러나 [7]에서 제안한 시스템은 졸업장 관리에 한정되어 있어서 이 시스템을 자격증 관리에 적용할 경우 자격증의 유효 기간을 고려하지 않는다는 문제점이 있다.

앞서 기술한 연구들은 기술적인 연구를 통해 위조를 방지하기 위한 연구들이다. 반면 대한상공회의소에서는 사용자의 요청에 따라 진위 확인 결과를 제공하는 서비스를 운영하고 있다[10]. 그러나 이 서비스는 즉각적으로 진위 확인이 이루어지지 않고 업무일 기준 5일 내에 회신을 통해 진위를 확인할 수 있다. 따라서 보안 문제를 떠나 자격증 진위를 확인하는데 수 일이 소요된다는 단점을 지닌다.

이 논문에서는 기존 연구들이 지니는 문제점을 해결하기 위해 블록체인 기반의 자격증 관리 시스템을 제안한다. 기존 접근 방법의 문제점을 정리하면, 첫 번째는 낮은 보안성 문제이며, 두 번째는 자격증 진위 확인에 많은 시간이 소요된다는 점이다. 이 논문에서는 이러한 기존 연구의 한계를 극복하기 위해 블록체인 기술을 이용하여 높은 보안성과 빠른 진위 확인이 가능한 시스템을 제안한다. 추가적으로 자격증은 각각 유효 기간이 존재하기 때문에 이 시스템에서는 자격증의 유효 기간도 고려한다. 또한 블록체인 기술을 이용하여 프로토타입을 구현하고 제안 시스템의 장점을 보이기 위해 실험 및 평가를 수행한다.

이 논문의 구성은 다음과 같다. 제 2장에서는 관련 연구를 소개하고 문제점을 분석하며 제 3장에서는 제안한 시스템의 블록체인 기술 분류, 전체적인 구조도, 주요 프로세스 등을 서술한다. 제 4장에서는 시스템의 구현 환경과 내용 및 결과를 기술하고, 제 5장에서는 제안 시스템의 실험 결과 및 평가를 기술한다. 마지막으로 제 6장에서는 결론 및 향후 연구를 서술한다.

Ⅱ. 관련연구

2.1 문서 위조 방지를 위한 연구

앞서 언급하였듯이, 자격증 위조 문제는 사회적으로 심각한 문제를 초래한다. 이러한 자격증 위조 문제를 해결하기 위해 다양한 연구가 진행되어 왔다[3]-[7]. [3]에서는 QR코드 및 디지털 워터 마킹을 이용한 인증서 위조 방지 시스템을 제안한다. QR코드 및 디지털 워터 마킹 정보를 2차원 바코드에 삽입함으로써, 인증서가 이중 위조 방지 기능을 가질 수 있어 위조 방지 성능이 크게 향상된다. 그러나 QR코드는 누구든지 제작, 배포를 할 수 있다는 문

제점을 가지고 있어서 보안에 위험성이 있다.

[4]에서는 랜덤코드와 검증코드를 이용해 운전면허증 위조를 방지한다. 사용자가 제출한 사진으로부터 개인을 식별할 수 없는 검증 이미지를 도출하고 해쉬 알고리즘을 통해 최종 식별코드를 생성한다. 마지막으로, 생성한 식별코드를 운전면허증 상에 표시한다. 위조여부를 판별하기 위해서는 식별코드를 입력해 도출한 검증 이미지를 운전면허증 상의 검증이미지와 비교하여 위조여부를 판별한다. 하지만 검증이미지를 시각적으로 확인하여 오인율이 있을 수 있고, 랜덤코드를 생성하는 해쉬 알고리즘과 식별코드가 유출될 경우 위조가 쉽게 가능하다는 문제점을 지닌다.

[5]에서는 단일척도를 이용한 1차 판별 이후 다중척도를 이용한 2차 판별을 사용하여 스마트폰으로 위조 인쇄물을 손쉽게 감식할 수 있는 기법을 제안한다. 그 결과 인식률을 크게 높였지만, 물리적인 자격증과 스마트폰이 있어야 감식이 가능하고, 시스템적으로는 확인이 불가능하다는 비효율적인 문제가 있다.

[6]에서는 원 지폐에 워터마크라는 사용자 아이디나 자신만의 정보를 삽입시킴으로써 불법적인 복제를 막고, 지적 재산권 및 저작권을 보호하는 기술을 제안한다. 그 결과 1%의 에러 픽셀을 가진 위조지폐에 대해서도 진위 여부를 검출할 수 있으며, 지폐보안 키의 크기가 작을수록 PSNR이 증가하는 것을 확인하였다. 그러나 워터마크가 삽입된 영상을 회전하거나 필터링하는 등의 공격을 완벽하게 차단하지 못한다.

[7]에서는 블록체인을 이용한 졸업장 관리 시스템을 제안한다. 이 시스템은 프라이빗 블록체인인 Hyperledger 기반으로 졸업장의 개인정보를 보호하는 디지털인증서 시스템이다. 그러나 [7]에서 제안한 시스템은 졸업장 관리에 한정되어 있어서 이 시스템을 자격증 관리에 적용할 경우 자격증의 유효기간을 고려하지 않는다는 문제점이 있다.

대한상공회의소에서는 자격증의 진위를 확인해주는 서비스를 제공한다[10]. 이 서비스는 사용자가 등록된 양식을 다운받아 양식에 맞게 명단을 기재하고 공문과 함께 진위 확인을 요청한다. 업로드를 통한 요청이 제출되면 진위를 확인하는 기관이 제출된 공문을 확인하여 그 결과를 업무일 기준 5일 내에 회신한다. 따라서 자격증 진위를 확인하는데 수 일이 소모된다는 문제점이 있다.

지금까지 자격증 위조 문제를 해결하기 위한 다양한 연구가 진행되어 왔고 각각이 의미 있는 연구이다. 그러나 앞서 기술하였듯이, 각 연구마다 한계를 지니고 있다. 이러한 기존 연구의 문제점을 요약하면 다음과 같이 크게 두 가지로 집약할 수 있다.

- 낮은 보안성 문제 : 위조 기술이 발전함에 따라 자격증이 수많은 사이트를 통해 손쉽게 위조 됨
- 진위 확인을 위한 많은 시간 소요 문제 : 기존 시스템에 진위 확인 결과를 요청 시 진위 확인 결과가 나오는데 수 일이 걸림

2.2 블록체인과 응용

기존의 시스템은 서버-클라이언트 구조로 모든 정보가 중앙에 있는 서버로 집중된다. 반면에 블록체인 기술은 탈중앙화 형태로 개별 노드들의 자발적이고 자율적인 연결에 의해 P2P 방식으로 작동한다. 따라서 이미 널리 알려진 블록체인 기술은 위·변조가 불가능하고 보안성이 뛰어나다는 장점을 지닌다[11].

이러한 블록체인의 종류는 접근성에 따라서 크게 세 가지인 퍼블릭 블록체인, 프라이빗 블록체인, 컨소시엄 블록체인으로 나뉜다[12]. 퍼블릭 블록체인은 말 그대로 대중 모두가 이용 가능한 공공의 블록체인이다. 모든 노드의 접근이 가능하지만 많은 수의 노드가 참여하고 모든 노드가 해당 트랜잭션을 검증하는 만큼 상대적으로 속도가 느리다. 프라이빗 블록체인은 한 집단의 독자적인 블록체인이다. 대중의 접근이 제한되어 있고 해당 블록체인을 접근하기 위한 권한이 필요하다. 컨소시엄 블록체인은 프라이빗 블록체인과 마찬가지로 승인이 필요하지만 특정한 집단이 참여하고 참여한 해당 집단만이 사용 가능한 네트워크이다.

지금까지 이러한 블록체인의 특성을 기반으로 한 다양한 연구가 진행되어 왔다[13]-[16]. [13]에서는 전통적인 신용장 방식의 문제점을 해결하기 위해 블록체인 기술을 신용장 방식에 적용할 경우에 대한 장·단점을 비교 분석하고, 블록체인 기술이 발

전시키기 위한 내용을 제안한다.

[14]에서는 블록체인 기술을 활용하여 사물인터넷 시스템을 설계 및 구현한다. 결과적으로, 블록체인 데이터의 사물인터넷 서비스를 신뢰할 수 있게 되고 데이터의 위·변조가 불가능하고 또한 데이터의 유출 방지도 가능하다.

[15]에서는 블록체인을 기반으로 개인 건강 기록 및 전자 건강 기록을 통합하고 성능을 평가한다. 이 결과 평균 응답 시간이 낮고 가용성이 높으며 데이터 보안이 뛰어나 데이터 복구가 쉽게 가능하다.

[16]에서는 비트코인의 문제점을 개선한 이더리움 블록체인[17]을 플라즈마 방식을 이용하여 온라인 투표 시스템을 구현하였다. 이 시스템은 투표한 사용자들도 중앙 관리 감독의 개입 없이 투표한 결과 및 투표 내역에 대해서 공유할 수 있다. 이로 인해, 위·변조가 불가능하고 신뢰성을 높일 수 있다. 또한 투표 결과가 블록체인에 바로 기록되기 때문에 불필요한 집계, 보안 비용을 지출하지 않아도 된다.

III. 제안 시스템

3.1 제안 시스템의 블록체인 기술 분류

이 논문에서는 자격증을 발급해주는 특정 집단만을 연결한 컨소시엄 블록체인 기술의 특성을 이용하여 자격증의 위조가 불가능하고 높은 보안성을 지원하는 자격증 관리 시스템을 개발한다. 또한 높은 보안성을 지원하는 블록체인 기술을 기반으로 개발한 시스템을 통해 안정적이고 빠른 진위 확인 서비스를 지원한다.

앞서 언급하였듯이, 이 논문의 목적은 탈중앙화 형태의 보안성이 뛰어난 블록체인 기반 자격증 관리 시스템 개발이다. 이러한 목적을 이루기 위해, 리눅스 재단에서 주관하는 블록체인 오픈소스 프로젝트인 Hyperledger[18]를 사용한다. Hyperledger 프로젝트는 크게 두 가지로 분류된다. 하나는 Hyperledger 프레임워크이고, 다른 하나는 Hyperledger 도구이다. 이 논문에서는 Hyperledger 프레임워크 중 하나인 Hyperledger Fabric[19]을 이용한다. Hyperledger Fabric 프로젝트는 현재 35개 이상의 조직들과 200명이 넘는 개발자가 참여하고 있다. 또한 합의 알고리즘의 선택적 사용, 네트워크 참여 권한 통제, 채널 및 멀티 장부 사용 등의 추가적인 여러 가지 기능을 제공한다. 이러한 기능을 이용하여 누구든지 특정 인원의 개인정보를 알고 있다면 그 인원의 자격증 취득 유·무를 판별할 수 있다. 또한 블록체인 네트워크에 연결된 특정 기관만이 자격증 취득 유무를 등록할 수 있도록 구현한다.

3.2 제안 시스템 구조

그림 1은 전체적인 시스템 구조를 보여준다.

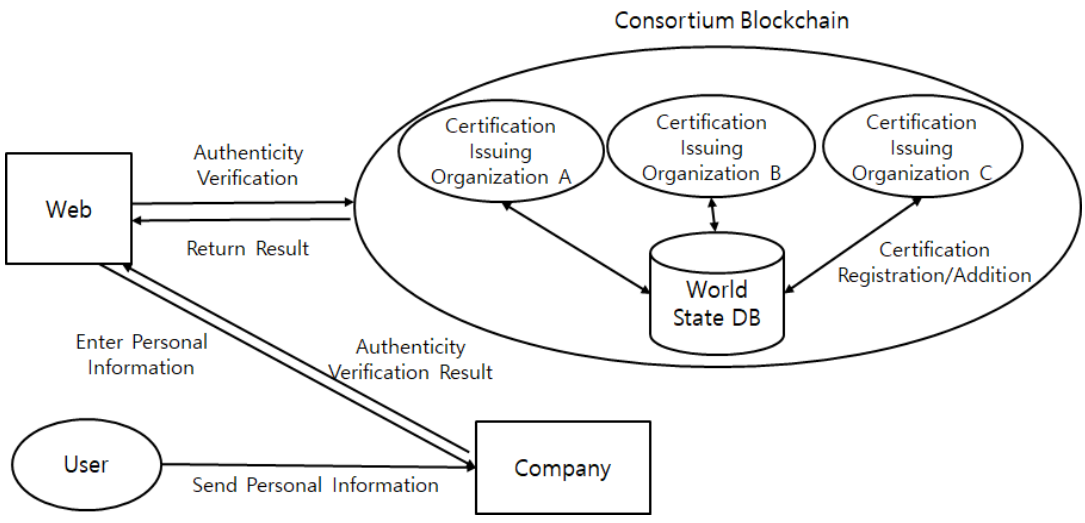

그림 1. 전체적인 시스템 구조
Fig. 1. Overall system architecture

사용자는 회사에 개인정보를 전송하고, 회사는 구현한 시스템을 통해 사용자 자격증의 진위를 확인하는 역할을 담당한다. 자격증 발급 기관은 자격증을 등록하는 역할을 수행한다. Key-value 데이터베이스인 World State DB는 체인코드가 호출될 때 블록체인 네트워크의 최신 데이터를 저장하는 역할을 담당한다.

진행 과정은 다음과 같다. 먼저, 사용자가 회사에 개인정보를 전송한다. 회사는 블록체인과 연결된 웹에 접속하여 전송받은 개인정보를 입력하면 웹에서는 입력받은 개인정보로 체인코드를 실행한다. 체인코드에서는 해당 개인정보에 저장되어 있는 자격증을 검색한다. 하지만 해당 자격증이 존재하더라도 유효 기간이 초과한 자격증은 유효하지 않으므로 진위를 확인할 수 없다. 따라서 해당 자격증이 존재할 경우 자격증의 유효 기간 초과 여부를 확인하여 유효 기간이 초과하지 않은 유효한 자격증만을 반환하고 유효 기간이 초과된 자격증은 갱신 전까지 진위 확인이 불가능하다. 회사는 블록체인과 연결된 웹을 통해 자격증 진위 확인 서비스를 이용한다.

3.3 블록의 구조

그림 2는 이 논문에서 제안한 시스템의 블록 구조를 보여준다. 블록과 블록은 체인으로 연결되며, 체인은 이전 블록의 Hash 값을 가리킨다.

Proof of work는 블록 헤더 정보를 입력 값으로 SHA256 해쉬 함수를 2회 적용해서 계산되는 값이다. Previous Block은 해당 블록의 바로 앞에 연결되어 있는 블록의 Hash 값이다. Transaction에는 자격증을 등록할 때 입력한 사용자의 정보와 해당 사용자의 자격증 정보가 등록된다. Transaction의 구성요소는 표 1과 같다. 등록 기관의 개인키, 자격증 취득 인원의 이름, 자격증 취득 인원의 주민등록번호, 취득한 자격증의 이름, 취득한 자격증의 유효기간 총 5가지 요소로 구성되어 있다. 블록체인 네트워크에 존재하는 모든 사용자는 같은 블록을 가지고 있으므로 기존 블록의 위·변조는 불가능하다.

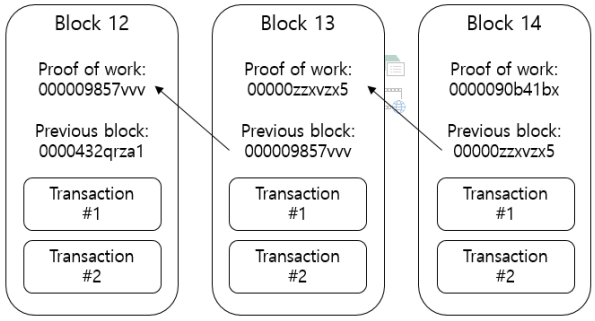

그림 2. 블록 구조
Fig. 2. Block structure

표 1. 트랜잭션의 구성요소
Table 1. Components of a transaction

Variable name	Variable value	Type
TransID	Private key of the registrar	Hash
Name	Name of the person who acquired certificate	String
Resident registration number	Resident registration number of the person who acquired certificate	int
Certificate name	Name of the certificate	String[]
Expiration date	Validity period of the acquired certificate	int[]

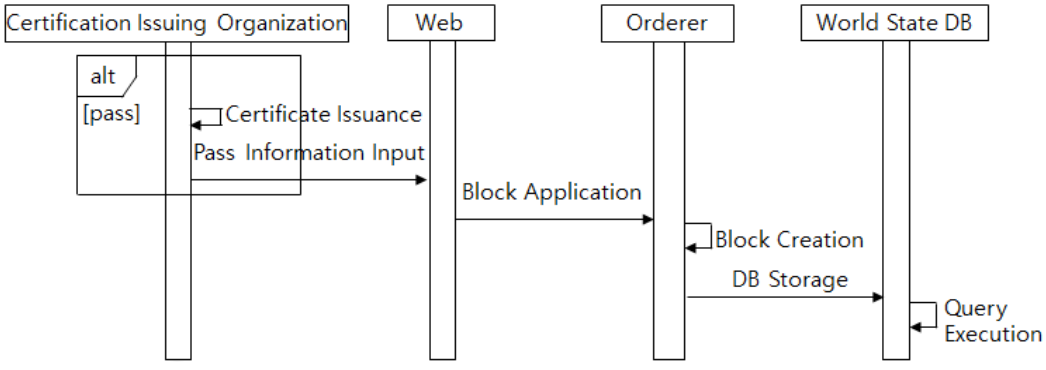

그림 3. 사용자 취득 자격증 등록 프로세스
Fig. 3. Registration process of user acquisition certificates

3.4 주요 프로세스

그림 3은 이 논문에서의 사용자 취득 자격증 등록 프로세스를 보여준다. 사용자가 자격증 시험을 통해 자격증을 취득할 경우 자격증 발급기관에서 블록체인과 연결된 웹을 이용해 합격정보를 입력한다.

합격정보를 입력받은 웹은 오더러에게 블록을 신청한다. 오더러는 Transaction의 순서를 정렬하고 블록을 생성하는 역할을 수행한다. 블록신청을 요청받은 오더러는 Hyperledger Fabric에서 제공하는 kafka 방식을 통해 블록을 생성한다. 생성된 블록은 블록체인 네트워크에 연결된 모든 기관들의 World State DB에 합격정보를 저장한다. 예를 들어, 여러 기관에서 여러 개의 자격증을 동시에 등록했을 경우 오더러는 해당 Transaction의 순서를 정렬하고 블록을 생성한다.

그림 4는 자격증 진위 확인 프로세스를 보여준다. 그림 4에서, 먼저 사용자가 회사에 개인정보를 제출한다. 회사는 사용자 자격증의 진위 여부를 확인하기 위해 블록체인과 연결된 웹에 제출받은 개인정보를 입력한다. 웹에서는 입력받은 개인정보를 World State DB에 진위 확인을 요청한다. World State DB에서는 질의문을 이용해 입력받은 개인정보와 일치하는 자격증이 존재하는지 확인한다. 자격증이 확인될 경우 질의문을 이용해 해당 자격증의 유효 기간을 확인한다. 유효 기간이 초과하지 않은 자격증의 경우 진위를 확인할 수 있고, 유효 기간이 초과되었을 경우에는 진위를 확인할 수 없다. 마지막으로, 웹은 World State DB에서 전송된 최종 진위 확인 결과를 회사에 전달한다.

Ⅳ. 구 현

4.1 구현 환경

이 논문에서 구현한 시스템의 구조는 그림 5와 같다. 자격증 발급기관 A, B, C를 데스크 탑 3대로 사용하여 프로토타입을 구현한다. 그리고 오더러를 이용하여 블록 안의 Transaction의 순서를 정하고 블록을 생성하여 연결된 노드에 전달하는 합의 시스템을 설정한다. 이 논문에서는 합의 시스템을 Pub/Sub구조의 메시지큐 미들웨어인 kafka기반의 오더링 서비스를 사용한다. kafka기반의 오더링 서비스는 최소 4개의 오더러를 가지고 있어서 일부 시스템 구성 요소들이 작동하지 않더라도 올바른 합의에 도달할 수 있는 기능을 제공해준다. 모든 오더러에 시스템이 분산 저장되어 있기 때문에 하나의 오더러에 장애가 발생할 경우 다른 오더러들로 인해 올바른 합의가 가능하다.

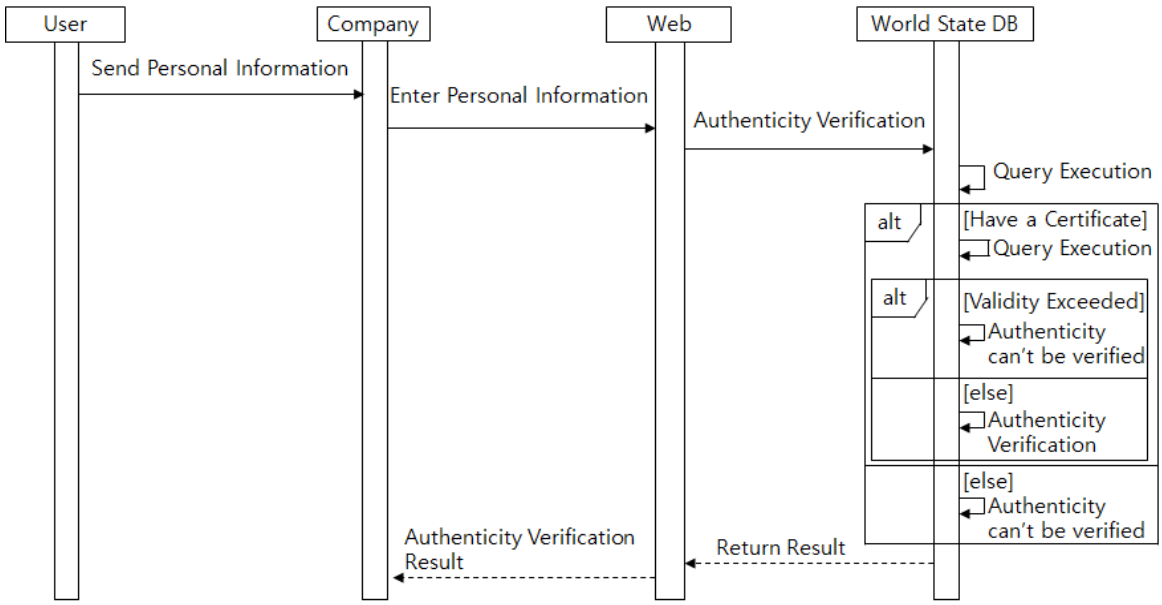

그림 4. 자격증 진위 확인 프로세스
Fig. 4. Process for authenticity verification of certificates

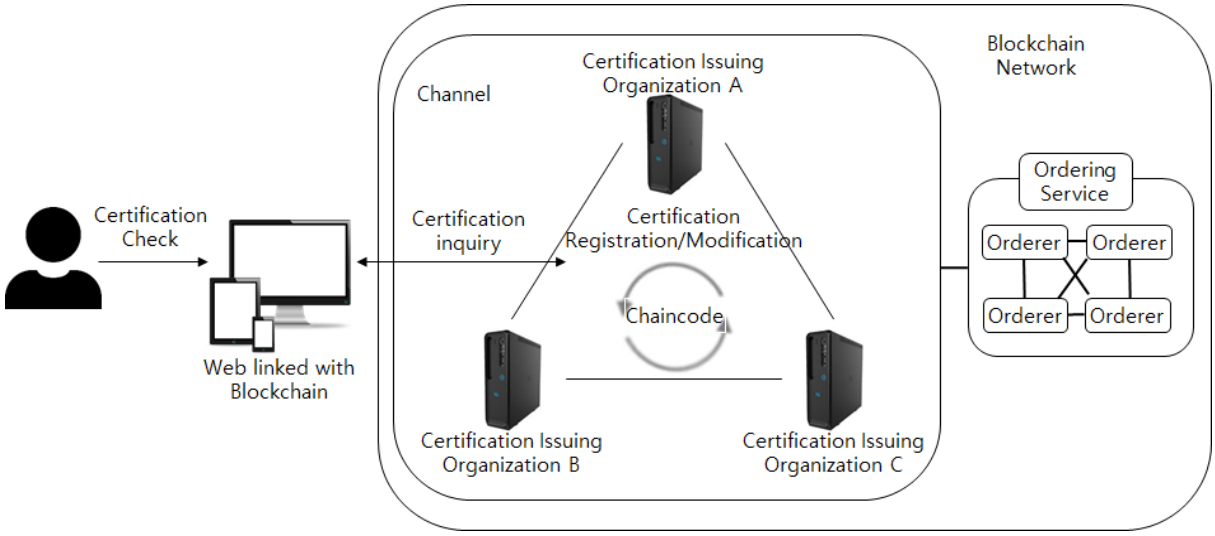

그림 5. 구현된 시스템 구조
Fig. 5. Implemented system architecture

그 후, 데이터 분리와 기밀화를 위해 컨소시엄이 이용하는 채널을 생성한다. 자격증 발급기관 A, B, C는 생성된 채널에 가입한다. 연결된 자격증 발급기관들은 구현된 체인코드로 인해 자격증 취득 유·무를 등록하고 수정할 수 있다. 사용자는 블록체인과 연동된 웹을 통해 자격증 진위를 조회할 수 있다.

이 논문에서 제안한 시스템의 구현 환경은 표 2와 같다. 자격증 발급기관 모두 동일한 환경으로 구현한다. 운영체제는 ubuntu-18.04.02 LTS이며, 네트워크 구축을 위한 개발 언어로는 YAML, Shell Script 등을 사용한다. 웹 서버는 Express를 사용하고, 자격증 취득 유·무를 확인하기 위해서는 World State DB를 이용한다. 웹 개발 언어는 Node.js, 체인코드 개발 언어는 Go를 사용하여 구현한다.

표 2 구현 환경
Table 2. Implementation environment

Classification	Contents
Operating system	ubuntu-18.04.02 LTS
System specification	Intel Xeon(R) CPU E3-1270 v5 @3.60GHz
RAM	3.9GB
Web Server	Express
Development language	HTML, YAML, Shell Script, Node.js, Go
Database	World State DB

4.2 구현 결과

그림 6은 구현한 프로토타입의 진위 확인을 위한 정보 입력 화면이다. 회사에서 사용자 자격증의 진위 확인을 할 경우, 확인할 사용자의 정보를 입력하고 제출 버튼을 누른다. 그 결과, 해당 사용자의 유효 기간이 지나지 않은 유효한 자격증을 그림 7과 같이 확인할 수 있다.

오른쪽 상단의 관리자로그인 버튼을 클릭하면 그림 8인 관리자 인증 화면을 볼 수 있다.

관리자의 아이디와 비밀번호를 입력하고 로그인 버튼을 클릭하면 그림 9인 관리자 메인 화면으로 이동한다. 메인 화면으로 이동한 관리자는 사용자 등록 기능과 자격증 등록 기능을 사용할 수 있다.

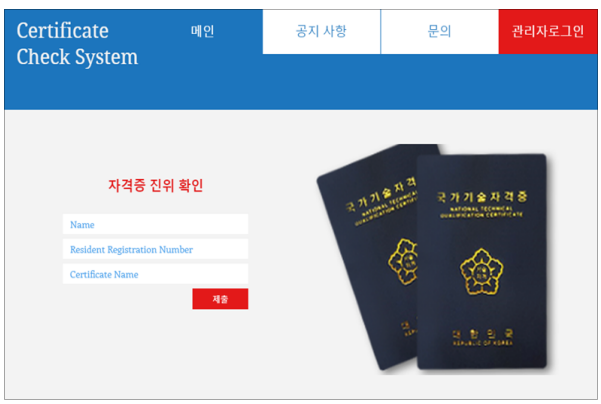

그림 6. 진위 확인을 위한 정보 입력 화면
Fig. 6. Input information for authenticity verification

그림 7. 자격증 진위 확인 결과
Fig. 7. Certificate authenticity verification result

그림 8. 관리자 인증 화면
Fig. 8. Manager authentication

그림 9. 관리자 메인 화면
Fig. 9. Main page for manager

그림 10은 관리자가 새로운 사용자를 등록하는 화면을 보여준다. 자격증이 없는 사용자가 자격증을 취득했을 경우 관리자가 자격증을 취득한 사용자의 이름, 정보, 자격증, 해당 자격증의 유효 기간을 입력한다. 입력한 내용은 World State DB에 등록되어 관리된다.

그림 11은 관리자가 사용자의 새로운 자격증을 등록하는 화면이다. 이미 자격증을 소지하고 있는 사용자가 새로운 자격증을 취득할 경우, 관리자가 자격증 취득 정보를 확인한다.

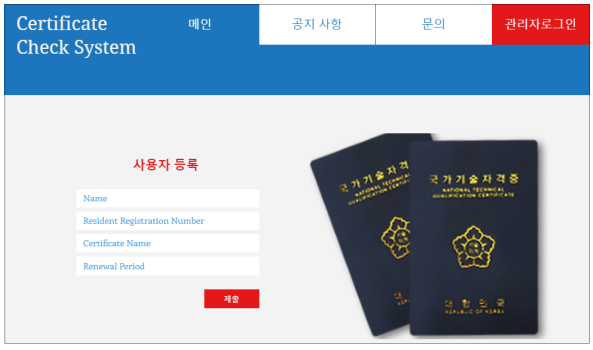

그림 10. 새로운 사용자 등록 화면
Fig. 10. Registration of new users

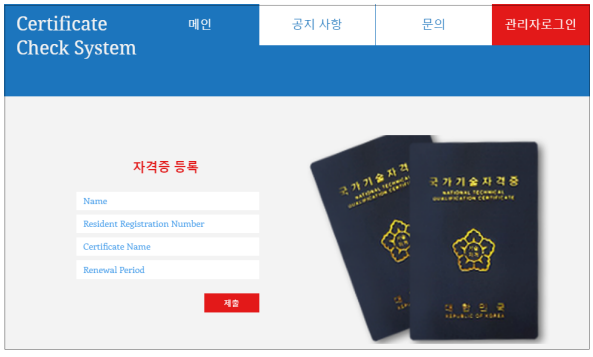

그림 11. 새로운 자격증 등록 화면
Fig. 11. Registration of new certificates

관리자는 자격증을 취득한 사용자의 이름, 정보, 자격증, 해당 자격증의 유효 기간을 그림 11에 입력한다. 입력한 내용은 World State DB에 등록되어 관리된다.

V. 실험 및 평가

5.1 진위 확인 시간 결과

그림 12는 자격증 진위 확인을 위해 소요되는 시간을 측정한 결과를 보여준다. 그림 12에서 볼 수 있듯이, 블록체인과 연결된 웹 페이지에 진위 여부 확인을 위한 해당 자격증 소지자의 개인정보를 입력한 결과 진위 확인에 소요되는 시간은 104ms이다.

존 시스템인 대한상공회의소에서는 사용자 한 명의 자격증 진위 확인을 하는데 수 일이 소요된다. 기존 시스템의 진위 확인 시간은 제출 양식 작성 시간, 관리자가 정보를 확인하는 시간 등 시간이 소요되는 과정이 여러 가지 존재한다.

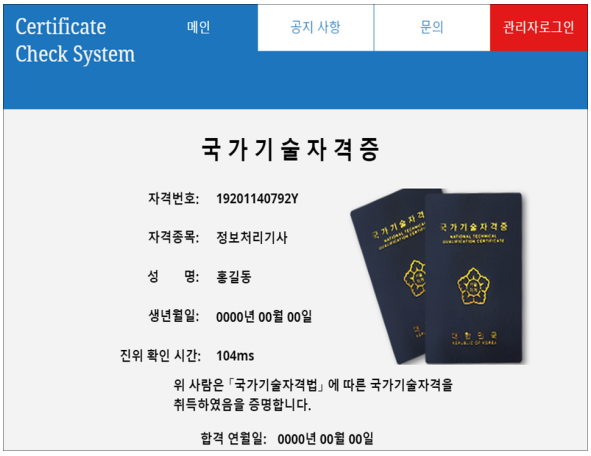

그림 12. 진위 확인 소요 시간
Fig. 12. Processing time for authenticity verification

하지만 이 논문에서는 진위 확인을 위한 사용자의 정보를 입력하는 시간, 시스템에서 진위를 확인하는 시간만 소요된다.

표 3은 기존 시스템과 제안 시스템의 진위 확인 시간을 보여준다. 이 논문에서는 제안 시스템의 자격증 진위 확인 시간 측정을 위해 30회의 실험을 수행하였고 표 3의 소요 시간은 평균 값을 나타낸다. 기존 시스템의 진위 확인 시간은 제출 양식 작성 시간, 관리자가 정보를 확인하는 시간 등 총 5일 이내의 시간이 소요된다. 반면 제안된 시스템은 진위 확인을 위한 사용자 정보 입력 시간이 11.75초가 소요되고 시스템에서의 진위 확인 시간이 0.11초의 시간이 소요된 것을 확인할 수 있다. 따라서 제안한 시스템에서의 진위 확인 시간이 더욱 빠른 것을 확인할 수 있다.

표 3. 진위 확인 시간 비교
Table 3. Comparison of authenticity verification time

Classification \ System	Existing system	Suggestion system
Time to fill out the submission Form	Within 5 days	none
Time to check information		none
Time to enter information to verify authenticity		11.75s
Authenticity check time		0.11s
Time to send authenticity verification results		none

5.2 정성 평가

표 4는 제안 시스템과 기존 시스템과의 정성적 비교 평가 결과를 보여준다.

먼저, 진위 확인 속도 측면에서, 제안 시스템은 보다 빠른 자격증 진위 확인 기능을 제공한다. 이는 앞서 기술한 진위 확인 비교 결과를 통해 확인할 수 있다. 이러한 빠른 진위 확인으로 인해 사용자가 자격증 진위를 확인하기 위해 소용해야 하는 시간을 절감시키고 효과를 제공한다.

표 4. 정성적 평가
Table 4. Qualitative evaluation

Evaluation Items \ System	Comparison result	
	Existing system	Suggestion system
Authenticity verification rate	Slow	Fast
Convenience	Low	High
Security	Normal	High
Forgery	Normal	Impossible
Responsibility	High	High

사용자 편의성 측면에서, 기존 시스템은 자격증 진위 확인 요청 후 진위 결과를 해당 기관에서 통보해 줄 때까지 대기해야 하는 불편함이 있다. 만일 진위 확인을 요청한 시점에 해당 업무 담당자의 공백이 있을 경우, 사용자는 더욱 많은 시간을 기다리게 된다. 또한 업무 담당자의 공백을 인지하지 못할 경우, 더욱 오랜 시간을 대기할 수 있으며, 무엇보다 사용자가 직접 해당 기관에 연락을 취하는 등의 추가적인 행위를 취해야만 하는 불편함이 있다. 반면, 제안 시스템은 진위 확인 프로세스가 시스템적으로 동작하기 때문에 즉시적으로 진위를 확인할 수 있으며, 앞서 언급한 업무 담당자의 공백과 무관하게 자격증 진위를 확인할 수 있다. 따라서 이러한 여러 가지 측면에서 제안 시스템이 높은 사용자 편의성을 제공한다.

지금까지 기존 시스템은 이미 자격증이 위조되어 많은 인명 피해와 경제적 손실을 안겨주었다[2]. 이러한 문제를 해결하기 위해 보안성을 강화할 수 있는 기술 적용이 중요하다. 이 논문에서 제안한 시스템은 블록체인 기술을 적용하였다. 블록체인은 탈중앙화, 집단 의사 결정 구조 등의 특성을 지니며, 무

엇보다 보안성 측면에서 그 안정성이 입증된 기술이다. 이러한 블록체인 기술을 적용한 제안 시스템은 적용 기술의 보안 수준이 높기 때문에 기존 시스템에 비해 높은 보안성을 제공한다. 또한 이러한 높은 보안성은 자격증 위·변조가 불가능하다는 장점으로 이어진다.

마지막으로, 진위 확인의 신뢰성 측면에서, 기존 시스템은 진위 확인 시간이 오래 걸린다는 문제점을 가지고 있지만 진위 확인의 신뢰성이 낮다고 볼 수는 없다. 그러나 보안의 안정성이 보장된 제안 시스템의 특성에 기인하여 제안 시스템이 보다 높은 신뢰성을 제공한다. 또한 사용자의 편의성, 서비스의 처리 속도 등도 사용자가 느끼는 신뢰성에 영향을 준다. 이러한 특성들로 인해, 기존 시스템에 비해 제안 시스템이 보다 높은 신뢰성을 제공한다고 판단할 수 있다.

결과적으로, 이 논문에서 제안한 시스템은 기존 시스템에 비해 진위 확인 속도, 편의성, 보안성 등의 측면에서 나은 성능을 제공한다. 또한 자격증 위·변조가 불가능하여 전체적인 신뢰성을 향상시킨다.

Ⅵ. 결 론

이 논문에서는 블록체인을 이용한 자격증 관리 시스템을 제안하고 구현하였다. 보안성을 높이기 위해 탈중앙화 형태의 보안성이 뛰어난 블록체인을 기반으로 오픈소스 프로젝트인 Hyperledger Fabric을 이용하였다.

실험 및 평가 결과, 이 논문에서 제안한 시스템은 기존의 시스템과는 달리 위조가 불가능한 블록체인을 이용하여 보안성이 높은 자격증 위조 방지 기능을 제공한다. 또한 기존 시스템보다 진위 확인을 빠르게 수행함으로써 사용자에게 높은 편의성과 신뢰성을 제공한다.

이 논문에서는 진위 확인 속도 측면을 제외한 다른 평가 항목에 대해서 정성적인 평가 결과를 기술하였다. 따라서 향후에는 주요 평가 항목에 대한 정량평가 연구가 수행되어야 하며, 이를 위해 설문조사를 통한 통계분석 및 추가적인 정량평가에 대한 연구가 요구된다. 또한 다른 Hyperledger 프레임워크인 Iroha, Sawtooth 등을 이용하여 진위 확인 소요시간, 보안성 등에 대한 성능 비교 평가 연구도 수반되어야 한다.

References

[1] Korea Occupational Safety and Health Agency, "Global Newsletter on Safety and Health at Work", Korea Occupational Safety & Health Agency International Cooperation Team, Apr. 2015.

[2] Ministry of Land, Infrastructure and Transport, "Final Report on Pilot Management of Domestic Low-cost Airlines and Domestic Airlines", Dec. 2014.

[3] M. Chen, "Certificate Anti-counterfeiting System Based on QR Code and Digital Watermarking", International Journal of Hybrid Information Technology, Vol. 9, No. 10, pp. 109-116, Oct. 2016.

[4] J. S. Nam, "Improvement of driver's license verification system using photo information", Master thesis, Sogang University Graduate School of Information & Technology, Seoul, Korea, Jun. 2013.

[5] D. Y. Choi and J. S. Kim, "A Code Authentication System of Counterfeit Printed Image Using Multiple Comparison Measures", Journal of the Korea Industrial Information Systems Research, Vol. 23, No. 4, pp. 1-12, Aug. 2018.

[6] S. H. Lee, "Forgery Prevention with Digital Watermarking Scheme Based on Integer Wavelet Transform", Master thesis, Graduate School of Kongju National University, Kongju, Korea, Dec. 2010.

[7] S. W. Jung, "HyperCerts: Privacy-Enhanced OTP-Based Educational Certificate Blockchian System", Korea Institute Of Information Security And Cryptology, Vol. 28, No. 4, pp. 987-997, Aug. 2018.

[8] I. H. Maeng, "Design Algorithm of Extended

Sector for Improving Security of QR Code", Doctoral dissertation, Graduate School of Hansei University, Gunpo, Korea, Dec. 2012.

[9] S. Y. Hong, S. R. Cho, and S. H. Kim, "Blockchain Beyond Bitcoin", Electronics and Telecommunications Research Institute, Vol. 32, No. 1, pp. 72-81, Feb. 2017.

[10] The Korea Chamber of Commerce & Industry, Authenticity Verification of Certificates, license. korcham.net/kor/pass/organpass.jsp. [accessed: Sep. 20, 2019]

[11] H. J. Kim, G. C. Lee, M. G. In, J. C. Lee, Y. H. Choe, B. N. Lee, and S. E. Hyeon, "[Standardization Trend] Blockchain", Electronics and Telecommunications Research Institute, Oct. 2017.

[12] Sungshin Women's University, "A Study on the Introduction of Blockchain Technology in the Financial Sector", Financial Services Commission, Jun. 2016.

[13] Q. Chen, "An Application of Blockchain Technology in Letter of Credit Transaction", Master thesis, Graduate School of Changwon National University, Changwon, Korea, Aug. 2019.

[14] C. H. Lee, "Design and Implementation of IoT System using Blockchain Technology", Master thesis, Graduate School of Sejong University, Seoul, Korea, Feb. 2019.

[15] A. Roehrs, C. A. Costa, R. R. Righi, V. D. Silva, J. R. Goldim, and D. C. Schmidt, "Analyzing the performance of a blockchain-based personal health record implementation", Journal of Biomedical Informatics, Vol. 92, Apr. 2019. https://doi.org/10.1016/j.jbi.2019.103140.

[16] T. J. Park, "Design and Implementation of Online Voting System using BlockChain", Master thesis, Graduate School of Engineering Hanyang University, Seoul, Korea, Feb. 2019.

[17] P. Fairley, "Ethereum will cut back its absurd energy use", IEEE spectrum, Vol. 56, No. 1, pp. 29-32, Jan. 2019.

[18] hyperledger, https://www.hyperledger.org/. [accessed: Sep. 20, 2019]

[19] hyperledger fabric, https://www.hyperledger.org/projects/ fabric/. [accessed: Sep. 20, 2019]

저자소개

배 승 훈 (Seunghun Bae)

2014년 3월 ~ 현재 : 군산대학교 소프트웨어융합공학과 학부생
관심분야 : 웹 프로그래밍, 데이터베이스, 블록체인

이 석 훈 (Sukhoon Lee)

2009년 2월 : 고려대학교 전자및정보공학부(학사)
2011년 2월 : 고려대학교 컴퓨터·전파통신공학과(공학석사)
2016년 2월 : 고려대학교 컴퓨터·전파통신공학과(공학박사)
2016년 3월 ~ 2017년 3월 : 아주대학교 의료정보학과 연구강사
2017년 4월 ~ 현재 : 군산대학교 소프트웨어융합공학과 조교수
관심분야 : 사물인터넷, 메타데이터, 센서 레지스트리, 시맨틱 웹, 경로 예측

정 동 원 (Dongwon Jeong)

1997년 2월 : 군산대학교 컴퓨터과학과(이학사)
1999년 2월 : 충북대학교 전자계산학과(이학석사)
2004년 2월 : 고려대학교 컴퓨터학과(이학박사)
2005년 4월 ~ 현재 : 군산대학교 통계컴퓨터과학과, 소프트웨어융합공학과 교수
관심분야 : 데이터베이스, 시맨틱 서비스, 빅데이터, 사물인터넷, 지능형 융합 서비스