

프라이빗 블록체인을 활용한 무결성이 보장되는 의료데이터 저장 시스템 구현

김범휘, 권기구, 최은창, 김규형

한국전자통신연구원

{bumhwi.kim, kwonkk, ecchoi, jaykim}@etri.re.kr

An Implementation of a medical record storage system that guarantees integrity using private blockchain technology

Kim Bumhwi, Kwon Kee-Koo, Choi Enchang, Kim Kyu Hyung

Electronics and Telecommunications Research Institute(ETRI)

요약

본 논문에서는 기존의 중앙 집중형 서버에 저장되는 데이터의 취약점에 대응하여 데이터의 무결성을 확보하고 외부 공격으로부터 강건하게 보호하기 위하여 프라이빗 블록체인을 통하여 의료데이터를 저장하고 검색할 수 있는 의료데이터 저장 시스템을 구현하는 것에 대해 설명하였다.

I. 서론

블록체인 기술은 최근 헬스케어 분야의 핵심 기술로 대두되었으며 여러 연구 결과를 통해 블록체인과 헬스케어의 접목성을 확인할 수가 있었 [1-3]다. 블록체인은 기존의 서면식, 중앙집중식의 데이터 보존방법을 떠나서 탈 중앙화, 디지털화를 위한 핵심 기술로서 환자 및 의료 서비스를 제공하는 기관에게 현대적인 의료경험을 제공할 수가 있다.

또한 블록체인을 통해 환자 기록 접근 및 제어, 비용 청구 및 지불 관리, 의료 기기 IoT 보안 관리와 같은 의료 데이터 관리와 의료 데이터 검증 및 투명한 재무 감사와 같은 응용을 수행할 수가 있게 된다. 이를 통해 수십 년간 지속된 전통적인 의료 시스템을 변화시킬 준비가 되었다고 볼 수 있다. 그리고 프라이빗 블록체인만의 특징으로 퍼블릭 블록체인과는 달리 허가형 블록체인으로써 이를 통해 의료기관이 허가받지 않은 사람의 민감한 정보에 액세스하는 것을 제한하도록 한다.

블록체인 관련 연구는 다양하게 진행되고 있는데, 그중 리눅스 재단(Linux Foundation)에서는 하이퍼레저(Hyperledger)라는 이름의 블록체인 기술 개발을 위한 Hyperledger Greenhouse라는 이름으로 다양한 오픈소스 프로젝트를 주도하고 있다[4].

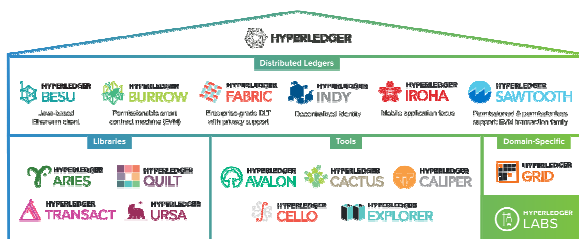


그림 1. Hyperledger Greenhouse

이 중에서 하이퍼레저 패브릭(Hyperledger Fabric)이 프라이빗 블록체인 분야의 메인 프로젝트로서 활발하게 개발이 진행 중이다[5].

본 논문에서는 위에서 언급한 블록체인의 장점을 취하여 하이퍼레저 패브릭 기반의 의료데이터 저장 시스템을 구현하였다.

II. 하이퍼레저 패브릭(Hyperledger Fabric) 구성요소

하이퍼레저 패브릭의 구성요소는 크게 원장(Ledger), 체인코드(Chaincode), 피어(Peer), 오더러(Orderer), 채널(Channel), 인증서버(Certificate Authority)가 있다. 각 구성요소에 대한 설명은 아래와 같다.

원장: 블록체인에서 공유하기 위해 저장되는 데이터의 변경 이력을 다 기록하고 있으며, 저장된 데이터들의 현재 상태를 저장하고 있는 월드 스테이트(World State)와 상태 변화에 대한 기록을 블록체인(Blockchain)형태로 기록하고 있는 원장(Ledger)로 나누어 져 있다.

체인코드: 스마트 컨트랙트(Smart Contract)로도 불리며, 블록체인 네트워크에 새 데이터를 추가하거나 읽어오기 위해 필요한 프로그램이다.

피어: 기관에 소속되어 블록체인 네트워크 상에서 원장과 체인코드를 관리하며 사용자를 대신해서 체인코드를 호출한다.

오더러: 블록체인 내에서 체인코드를 통해 발생하는 거래(Transaction)를 정렬해서 순차적으로 블록을 생성해준다.

채널: 블록체인 내에서 참여자들이 데이터를 공유하는 기준을 말한다. 다른 채널에 포함된 피어는 데이터를 열람할 수가 없다.

인증서버: 사용자의 권한 및 인증을 위한 MSP(Membership Service Provider)를 발급하고 관리하는 역할을 수행하며, 보통 신뢰있는 기관이 이를 운영한다. 본 논문에서는 하이퍼레저에서 제공하는 Fabric-CA를 의미한다.

III. 의료데이터 저장 시스템

기존의 웹 서비스에서 DB로 저장되는 중앙 집중화 구조를 블록체인으로 대체하여 모든 참여자의 데이터가 공유하고 기존처럼 데이터가 생성되고 검색되게 할 수 있다. 본 논문에서는 임의의 의료데이터 서버를 가정하고 의료데이터를 블록체인에 저장하고 검색하는 시스템을 제안한다.

제안하는 전체 시스템의 구조는 그림1과 같다. 전체 시스템 구성은 웹 클라이언트/서버, REST API서버, 블록체인 네트워크, 인증 서버로 구성되어 있다. 시나리오는 크게 사용자 인증과 의료데이터 생성/검색 2가지로 나눌 수 있다.

