

하이퍼레저 패브릭 활용 효율적 데이터 검증방안 연구

채봉수⁰, 백승현*, 김태윤**, 이한진**

⁰한국정보통신기술협회(TTA),

*G마켓(주),

**한동대학교(창의융합교육원)

e-mail: duser@tta.or.kr⁰, seunghbaek@gmarket.com*, 22000194@handong.ac.kr**, cus@handong.edu**

Research on Efficient Data Verification Methods Using Hyperledger Fabric

Chai Bong-Soo⁰, Baek Seunghyun*, Kim Taeyoon**, Lee Hanjin**

⁰Telecommunications Technology Association,

*Gmarket Inc.,

**Handong Global University

● 요약 ●

하이퍼레저 패브릭(Hyperledger Fabric)은 참여자의 신원을 확인하고, 정보교환(트랜잭션)의 유효성을 검증하는 허가형 블록체인 모델이다. 기존의 대표적인 블록체인 모델인 비트코인, 이더리움과 대비하여 효율적인 데이터 검증 방안이 가능한데, 체인코드와 채널, 그리고 피어를 중심으로 구성되어 있기 때문이다. 먼저 본 블록체인 모델은 '체인코드'라는 스마트 계약(컨트랙트)를 실행하며 허가된 사용자만 네트워크에 참여할 수 있다. 또한, '채널' 기능이 있어 서로 다른 조직 간의 데이터 공유와 검증에 대한 새로운 접근방식을 보여 줄 수 있으며, 특정 네트워크 내에서 데이터를 분리할 수 있다. 이를 통해 특정 데이터에 대한 접근권한을 제어하는 기능을 제공하며 동시에 데이터의 신뢰성과 보안성을 높일 수 있다. 마지막으로 '피어'는 체인코드를 통해 들어온 트랜잭션을 검증하고, 유효한 데이터만 원장에 추가하는 기법으로 무결성을 유지하는 데 중요한 역할 담당하고 있다. 본 연구결과를 기반으로 하이퍼레저 패브릭을 효과적으로 활용하여 데이터 검증 프로세스가 산업계에 널리 적용될 수 있기를 기대한다.

키워드: 하이퍼레저 패브릭(Hyperledger Fabric), 블록체인(Blockchain), 데이터 검증(Data Verification), 신뢰성(Trustworthy), 스마트계약(Smart Contract)

I. Introduction

블록체인 기술은 디지털 데이터를 분산적으로 저장하고 관리를 가능하게 하는 기술이다[1]. 블록체인 기술을 통해 데이터의 무결성과 투명성을 보장할 수 있으며, 기존의 중앙 집중식 시스템이 가지고 있는 여러 한계점을 보완할 수 있다[2]. 이러한 특성은 정보시스템 구축 및 운영에 필요한 데이터들의 소프트웨어 품질 향상을 위한 뒷받침이 될 수 있다.

반면에, 1세대 블록체인 비트코인이나 2세대 블록체인 이더리움의 경우 공개형 블록체인이 가지고 있는 보안성, 익명성 관련 이슈 및 합의 프로세스가 고정된 네트워크 시스템을 보유하고 있는 등의 문제를 가지고 있다[3]. 이를 극복하기 위해 MS사에서 제공하는 블록체인 플랫폼인 하이퍼레저 패브릭(Hyperledger Fabric)을 활용하는 경우가 점점 늘어나는 추세이다[3].

본 논문에서는 블록체인에 기반한 데이터 검증 특징에 대해 논의하고, 하이퍼레저 패브릭이라는 특정 블록체인이 가지고 있는 기술의 특징 및 구성요소를 분석한다. 나아가, 기존 데이터의 검증방식을 어떻게 효율적으로 개선할 수 있을지 연구하여 체인코드(Chain Code), 채널(Channel), 피어(Peer)라는 하이퍼레저 패브릭의 핵심 구성 요소를 활용한 실질적인 데이터 검증방안을 제시한다[4].

II. Preliminaries

2.1 Related works

2.1.1 블록체인 데이터 검증 특징

블록체인은 네트워크 내에서 정보를 투명하게 공유할 수 있으며, 순차적으로 연결된 블록에 데이터를 저장한다[1]. 대중적으로 알려진 비트코인, 이더리움 등의 경우 다른 네트워크의 합의 없이 체인을 수정하거나 삭제할 수 없기에 데이터의 일관성과 투명성을 보장받는다. 결국 블록체인 기술을 활용하면 데이터 생성 및 전송 시 효율적인 데이터 검증을 진행할 수 있다[5]. 다음은 블록체인 기술을 통한 데이터 검증의 특징이다.

- 무결성: 블록체인 기술을 통해 데이터의 무결성을 보장할 수 있다. 한 번 블록체인에 기록된 데이터는 변경이 불가능하며, 이는 데이터의 원본이 보존되고 변조되지 않음을 의미한다. 결과적으로 데이터의 신뢰성이 향상되며, 특히 금융, 의료, 공공기록 등과 같은 분야에서 필요로 하는 기술이다.
- 투명성: 블록체인은 모든 트랜잭션을 공개적으로 기록하므로, 참여자들은 네트워크 내의 모든 트랜잭션을 검토할 수 있다. 이를 통해 높은 수준의 투명성이 제공되며, 부정행위를 방지하고 신뢰성을 높이는 데 도움이 된다.
- 분산 처리: 블록체인은 분산 네트워크에 기반하여 동작하므로 중앙 집중식 시스템의 취약점을 해결할 수 있다. 중앙 서버의 고장, 해킹 공격 등으로부터 데이터를 안전하게 보호할 수 있다.
- 자동 검증: 블록체인은 스마트 컨트랙트(Smart Contract)를 통해 자동화된 거래 검증을 제공할 수 있다. 스마트 컨트랙트를 통해 복잡한 업무 프로세스를 효율적으로 처리하고, 오류를 최소화 할 수 있다.

블록체인이 보유한 특징과 장점들로 인해 블록체인 기술은 데이터 검증 분야에서 많은 주목을 받고 있으며, 다양한 산업 분야에 활용되는 추세이다[6].

2.1.2 블록체인별 특징

블록체인 기술을 기반으로 한 플랫폼 중 대표적인 공개형 블록체인으로는 비트코인, 이더리움 등이 있으며, 허가형 블록체인 기술로는 본 논문에서 다루고 있는 하이퍼레저 패브릭이 있다. 세 블록체인 기술의 차이점을 정리하면 <Table 1>과 같다[3-7].

Table 1. System Environment

Item	Bitcoin	Ethereum	Hyperledger Fabric
Type	Public Blockchain	Public Blockchain	Permissioned Blockchain
Consensus Mechanism	Proof of Work (PoW)	PoW to Proof of Stake (PoS)	Pluggable
Smart contract	Not supported	All users execute and verify	Chaincode used, limited
Privacy	Disclosure of all transaction information	Disclosure of all transaction information	Guaranteed through privacy channels
Performance	Limited performance	Limited performance	High performance
Scalability	Limited scalability	Limited scalability	High scalability

하이퍼레저 패브릭이 가지고 있는 허가형 블록체인 유형은 비즈니스 네트워크 구축 시 보안성과 데이터 신뢰성을 높일 수 있다. 또한 다른 블록체인 기술보다 높은 성능과 확장성을 통해 효과적인 데이터 생성 및 전송을 가능하게 한다.

2.1.3 하이퍼레저 패브릭 구조

하이퍼레저 패브릭은 체인코드, 채널, 피어 등 여러 구성 요소로 이루어져 있으며[3], 각 구성 요소들은 데이터의 유효성을 검증하는 데 중요한 역할을 수행한다(Fig. 1).

체인코드(Chaincode)는 하이퍼레저 패브릭에서 스마트 컨트랙트의 역할을 수행한다. 트랜잭션을 처리하고, 트랜잭션의 유효성을 검증하며, 블록체인 원장을 업데이트한다. 데이터 검증 관점에서 보면, 체인코드는 트랜잭션이 사전 정의된 규칙과 일치하는지 확인하는 역할을 한다[7]. 블록체인 데이터 검증 시 체인코드를 통해 데이터의 신뢰성과 무결성을 효과적으로 보장받을 수 있다.

채널(Channel)은 하이퍼레저 패브릭이 가지고 있는 큰 특징으로, 데이터의 프라이버시와 보안성을 제공한다. 채널은 프라이빗 블록체인의 형태로 동작(Fig. 1)한다. 특정 참가자 그룹인 Org1, Org2 이외에는 접근이 안되기에, 특정 참가자 그룹만이 트랜잭션을 볼 수 있도록 하고, 이 트랜잭션들만이 해당 채널의 원장인 Org1 CA, Org2 CA에 기록된다. 이는 데이터의 프라이버시를 보장하며, 동시에 데이터의 유효성을 검증하는 데 중요한 역할을 수행한다[6].

피어(Peer)는 체인코드를 설치하고 실행하는 노드로서, 블록체인 원장을 유지하고, 트랜잭션을 검증하는 역할을 수행한다. 피어는 체인코드를 통해 들어온 트랜잭션을 검증하고, 유효한 트랜잭션만 원장에 추가 할 수 있기에 데이터의 검증 시 유효성과 무결성을 제공한다[5].

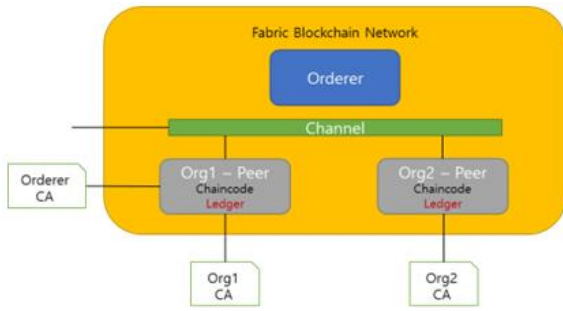


Fig. 1. Hyperledger Fabric Architecture

위에서 살펴본 바와 같이, 하이퍼레저 패브릭 모델은 데이터 검증 시 효율적으로 유효성과 신뢰성을 보장할 수 있다. 3장에서는 체인코드, 채널, 피어 각각의 데이터 검증 방식, 장단점 등에 대해 살펴본다.

III. The Proposed Scheme

3.1 Chaincode

요약하면 하이퍼레저 패브릭의 체인코드는 스마트 컨트랙트의 역할을 수행하며, 트랜잭션의 유효성을 검증한다. 이에 원장을 업데이트하는 중추적인 역할 수행하여 데이터의 무결성과 신뢰성을 보장할 수 있다[4, 5].

체인코드는 트랜잭션을 처리하기 전에 사전에 정의된 규칙에 따라 트랜잭션의 유효성을 검증한다. 규칙은 비즈니스 로직에 따라 다르게 설정할 수 있으며, 이는 조직별로 맞춤조정(커스터마이징) 할 수 있다. 이를 기반으로 특정 조건을 충족하지 않는 트랜잭션은 체인코드를 통해 필터링된다[8].

아울러 체인코드는 원장의 상태를 업데이트하는데 사용되며, 유효한 트랜잭션은 체인코드에 의해 원장에 기록되어 그 영속성을 보장한다. 이를 통해 데이터의 불가역성을 보장하며, 검증된 데이터의 신뢰성을 높일 수 있다.

하지만, 체인코드를 통한 데이터 검증은 체인코드의 정확성에 매우 의존적이다. 체인코드에 결함이 있거나 비정상적인 상황이 빠르게 처리되지 않으면 원장에 신뢰성이 저하될 수 있다. 따라서 체인코드 로직 분석 및 설계 시 정적테스트와 검증이 필요하다.

3.2 Channel

채널은 특정 참가자 그룹 간에 데이터를 공유하고, 데이터의 유효성을 검증하는 데 사용되는 하이퍼레저 패브릭의 중요 특징이다. 채널은 특정 참가자 그룹만 접근을 허가하여, 데이터의 보안성을 높일 수 있다[3, 5].

채널은 각 참가자가 공유해야 하는 데이터를 분리하여 해당 데이터에 대한 접근을 제어할 수 있게 해준다. 예를 들어, Org1과 2, 그리고 Org2와 3이 서로 다른 트랜잭션을 수행해야 하는 경우, 두 개의 별도 채널을 생성할 수 있다. 이렇게 하면 A와 B 간의 트랜잭션은 A와 C 간의 트랜잭션에 영향을 주지 않는 상태에서 데이터 공유 및 검증이 가능하다[6].

데이터의 유효성 검증 관점에서 채널은 특정 참가자 그룹만이 트랜잭션을 볼 수 있도록 하고, 이 트랜잭션들만이 해당 채널의 원장에 기록된다. 이를 통해 채널은 각 참가자가 원장의 상태와 트랜잭션의 유효성을 검증할 수 있게 해준다. 채널 참가자들은 해당 채널의 체인코드를 실행하여 들어온 트랜잭션을 검증하고, 유효한 트랜잭션만 원장에 추가할 수 있다[5].

3.3 Peer

피어는 네트워크 내에서 체인코드를 실행하고, 원장을 유지하며, 트랜잭션을 검증하는 역할을 수행한다[4, 7]. 이러한 피어의 기능을 활용하여 데이터 검증 프로세스를 개선하는 방법은 아래와 같다.

- 체인코드 실행을 통한 데이터 검증: 피어는 네트워크 내에서 체인코드를 설치하고 실행할 수 있도록 도와준다. 피어가 들어온 트랜잭션을 체인코드에 따라 검증하고, 유효한 트랜잭션만 원장에 추가할 수 있음을 의미하며, 이를 통해 데이터의 신뢰성과 무결성을 보장할 수 있다.
- 원장 유지를 통한 데이터 검증: 피어는 블록체인 원장을 유지하며, 원장의 모든 블록과 트랜잭션을 검증한다. 원장의 무결성을 유지하기 위해, 피어는 원장에 새로운 블록을 추가하기 전에 해당 블록의 해시(Hash)값을 계산하고, 이전 블록의 해시값과 비교한다. 이 과정을 통해 원장의 무결성을 보장하고, 데이터의 신뢰성을 높일 수 있다.
- 합의 알고리즘을 통한 데이터 검증: 하이퍼레저 패브릭은 여러 합의 알고리즘을 지원한다. Order 단계에서 개발자가 원하는 합의 알고리즘의 선택이 가능하다. 피어는 합의 알고리즘에 따라 트랜잭션의 순서를 결정하고, 트랜잭션의 유효성을 검증한다. 결국, 데이터 검증 시 데이터의 일관성을 보장하여 블록체인 네트워크의 내결함성을 높일 수 있다.

요컨대 피어는 하이퍼레저 패브릭에서 데이터의 유효성을 검증하고 무결성을 유지하는 중요한 역할을 수행한다. 이는 블록체인 기술 중 하이퍼레저 패브릭이 데이터 검증 및 관리 시 강력한 플랫폼으로 제안할 수 있는 이유 중 하나라 볼 수 있다.

IV. Conclusions

블록체인 기술은 그 자체로 데이터의 무결성과 신뢰성을 보장할 수 있다. 그 중 하이퍼레저 패브릭은 허가형 블록체인 모델로 체인코드, 채널, 피어 등의 구성 요소를 통해 데이터의 유효성을 검증하며, 데이터의 신뢰성을 높일 수 있다. 이는 정보시스템 구축 및 운영에 필요한 데이터들의 소프트웨어 품질 향상을 위한 뒷받침이 될 수 있다[8]

체인코드는 스마트 컨트랙트의 역할을 수행하여 트랜잭션의 유효성을 검증하고, 원장을 업데이트한다. 채널은 특정 참가자 그룹 간에 데이터를 공유하고, 이 데이터의 유효성을 검증하는 데 사용된다. 피어는 체인코드를 실행하고, 원장을 유지하며, 합의 알고리즘을 통한 트랜잭션 및 데이터 검증을 통해 데이터의 신뢰성과 무결성을 보장한다.

본 논문에서는 이러한 하이퍼레저 패브릭의 구성 요소를 활용하여 데이터 검증 프로세스를 개선하는 방안을 제시하였다. 본 논문을 통해 하이퍼레저 패브릭을 이용한 데이터 검증 방안에 대한 이해를 높일 수 있다.

하지만, 하이퍼레저 패브릭 플랫폼 도입 시 체인코드 개발의 복잡성, 네트워크 참가자가 많은 경우의 채널 복잡성, 피어 관리 및 유지보수의 어려움 등의 한계점도 가지고 있다[9]. 향후 이러한 한계점을 보완한 하이퍼레저 데이터 검증 방안에 대한 후속연구를 제안한다.

REFERENCES

- [1] ISO, ISO 22739: Blockchain and Distributed Ledger Technologies - Vocabulary, 2020.
- [2] Ghassan Al-Sumaidae, Rami Alkhudary, Zeljko Zilic, Andraws Swidan, "Performance analysis of a private blockchain network built on Hyperledger Fabric for healthcare," *Information Processing & Management*, Vol. 60, Iss. 2, pp. 1-13, 2023.
- [3] Hanool Choi, "A Study on Application of Blockchain Platform to Trade Process based on Hyperledger Fabric," *International Commerce and Information Review*, Vol. 23, No. 2, pp. 3-20, 2021.
- [4] Khatri, Sabita, Khalil al-Sulbi, Abdulaziz Attaallah, Md Tarique Jamal Ansari, Alka Agrawal, and Rajeev Kumar. "Enhancing Healthcare Management during COVID-19: A Patient-Centric Architectural Framework Enabled by Hyperledger Fabric Blockchain," *Information*, Vol. 14, No. 8, pp.1-23, 2023.
- [5] Myung Jae Lee and Young Taek Jin, "Software Development Based on Blockchain Using Hyperledger Fabric," *Journal of Knowledge Information Technology and Systems(JKITS)*, Vol. 17, No. 2, pp. 211-220, April 2022.
- [6] Hyperledger Fabric, www.hyperledger.org
- [7] Valenta, M.; Sandner, P. Comparison of Ethereum, Hyperledger Fabric and Corda. *Frankf. Sch. Blockchain Cent*, Vol. 8, pp. 1-8, 2017.
- [8] Bong-soo Chai, Dae-whan Min, and Hanjin Lee, "Research to Improve the Quality of Non-Contact Education Systems," *The Society of Convergence Knowledge Transactions*, Vol. 11, No. 1, pp. 89-100, 2023.
- [9] Pancari S, Rashid A, Zheng J, Patel S, Wang Y, Fu J. A Systematic Comparison between the Ethereum and Hyperledger Fabric Blockchain Platforms for Attribute-Based Access Control in Smart Home IoT Environments. *Sensors*, Vol. 23, No.16, pp. 1-28, 2023.