하이퍼레저 패브릭 : 이론

https://youtu.be/cyDdqHxSsbo

하이퍼레저 패브릭이란?

하이퍼레저 패브릭의 특징

하이퍼레저 패브릭 구성요소

세부 동작 과정

하이퍼레저 패브릭이란?

- **하이퍼레저 패브릭**
  - 하이퍼레저 프로젝트 중 가장 많이 사용되는 프레임워크
  - 모듈 구조를 이용한 어플리케이션/솔루션 개발을 도와주는 블록체인 프레임워크

하이퍼레저 패브릭의 특징

- **하이퍼레저 패브릭의 특징**

1. 허가형 프라이빗 블록체인 → **악의적인 노드 참여 방지**
2. 교체 가능한 모듈 구조

   → 모듈 단위로 작동하기 때문에 네트워크 구성이 비교적 명확

   → 합의 알고리즘, 스마트계약 등과 같은 다양한 기능을 원하는 모델에 맞춰 선택 가능
3. 암호화폐 기반 플랫폼이 아님 → 자체 토큰 X
4. 일반적인 프로그래밍 언어 사용 가능 → go, node.js, java

구성요소

- **분산원장** : 공유하고자 하는 데이터의 변화를 모두 기록해둔 것으로 월드스테이트와 블록체인으로 구성
  → 월드스테이트 : 현재의 상태를 기록해둔 데이터베이스
  → 블록체인 : 상태변화에 대한 모든 로그 기록을 저장
- **체인코드** : 클라이언트가 어플리케이션을 통해 호출되는 코드
  → 이더리움의 스마트 컨트랙트와 같은 개념
- **Peer Node** : 블록체인 네트워크를 유지하며, 트랜잭션을 처리하고 원장과 체인코드를 관리하고 저장하는 노드
  → Endorsing peer : 체인코드 시뮬레이션을 통해 트랜잭션이 적절한지 판단하는 역할
  → Committing peer : 모든 peer가 수행하는 역할로, 최신 블록에 대한 검증
  → Anchor peer : 다른 조직의 peer와 통신하는 역할
  → Leader peer : orderer와 연결되어 최신 블록을 전달받아 조직 내 다른 peer들에게 전송하는 역할
- **Orderer Node** : Endorsing peer들이 적절하다고 판단된 트랜잭션을 모아서 정렬 후 블록을 생성하는 노드
  → Ordering Service Node (OSN)

구성요소

- **Membership Service Provider, MSP : 블록체인 네트워크에 인증 서비스를 제공하는 인증 관리 시스템**
  - 네트워크에 접속하려는 클라이언트의 신원을 확인, 접근 권한 제공
    → MSP를 통해 인증서를 발급 받아야 블록체인 네트워크에 접근 가능
  - 네트워크 내 노드의 역할과 권한 등이 정의되어 있음
- **Certification Authority, CA : 인증서를 관리하는 기관**
  - MSP에서 인증을 위해 필요한 인증 기관
  - 네트워크에 참여할 수 있는 인증서를 발급하고 배포
  - 공개키 기반 구조 → 공개키 및 개인키 발급

세부 동작 과정

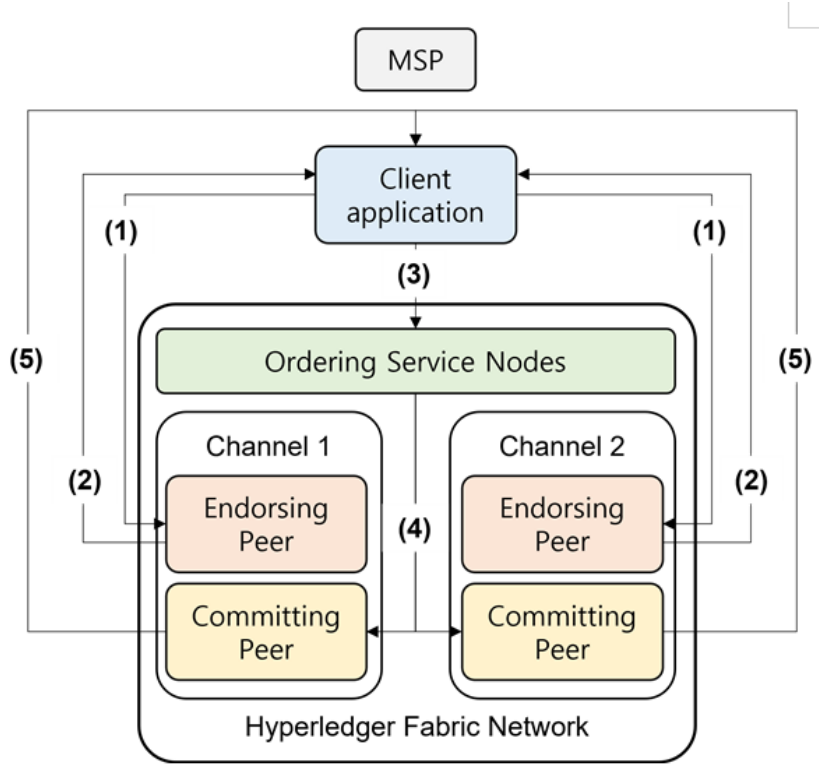
(1) Transaction Proposal

(2) Proposal Response

(3) Submit Transaction

(4) Order Transaction

(5) Ledger Commit



세부 동작 과정

(1) Transaction Proposal

→ Application은 먼저 트랜잭션 제안서를 Endorsing peer들에게 전송

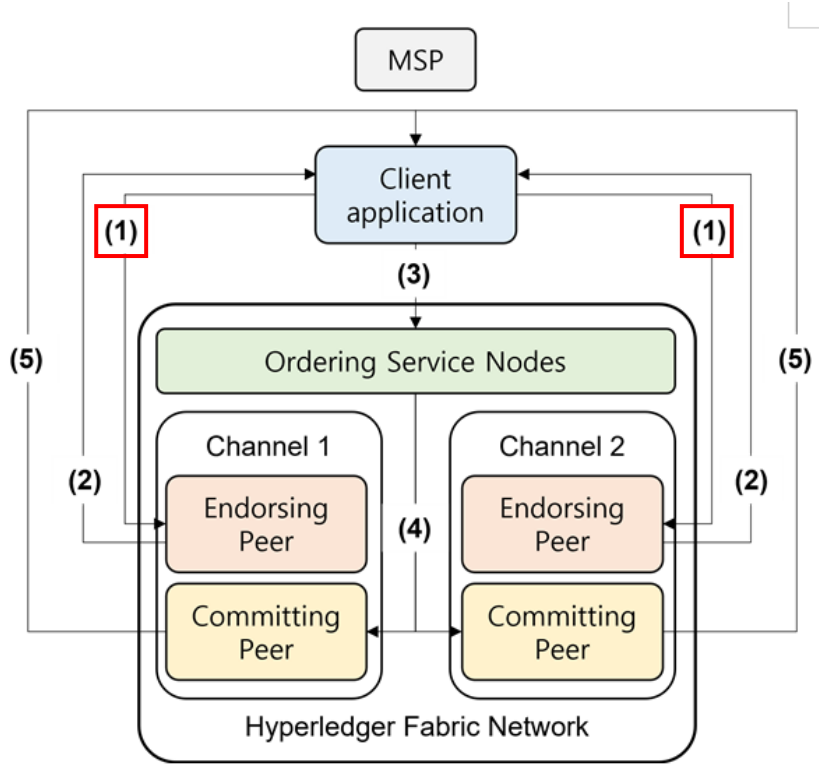
→ 트랜잭션 제안서 : 클라이언트의 ID, 클라이언트 서명 등이 포함됨

(2) Proposal Response

(3) Submit Transaction

(4) Proposal Response

(5) Proposal Response



세부 동작 과정

(1) Transaction Proposal

(2) Proposal Response

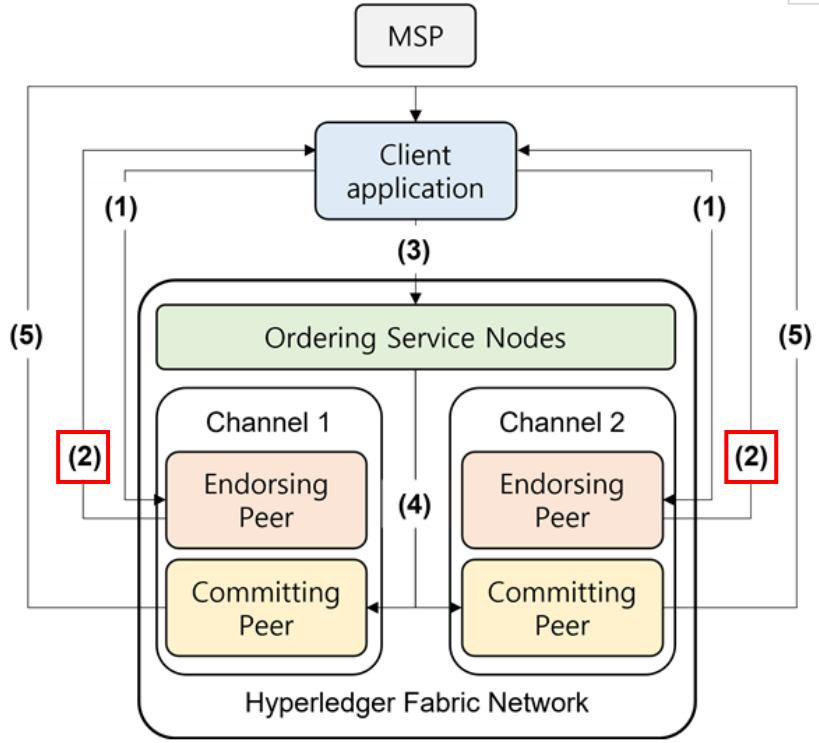
→ 제안을 받은 Endorsing Peer는 서명과 트랜잭션을 확인

→ 체인코드 실행 후, Application에게 Proposal Response 전송

(3) Submit Transaction

(4) Order Transaction

(5) Ledger Commit



세부 동작 과정

(1) Transaction Proposal

(2) Proposal Response

(3) Submit Transaction

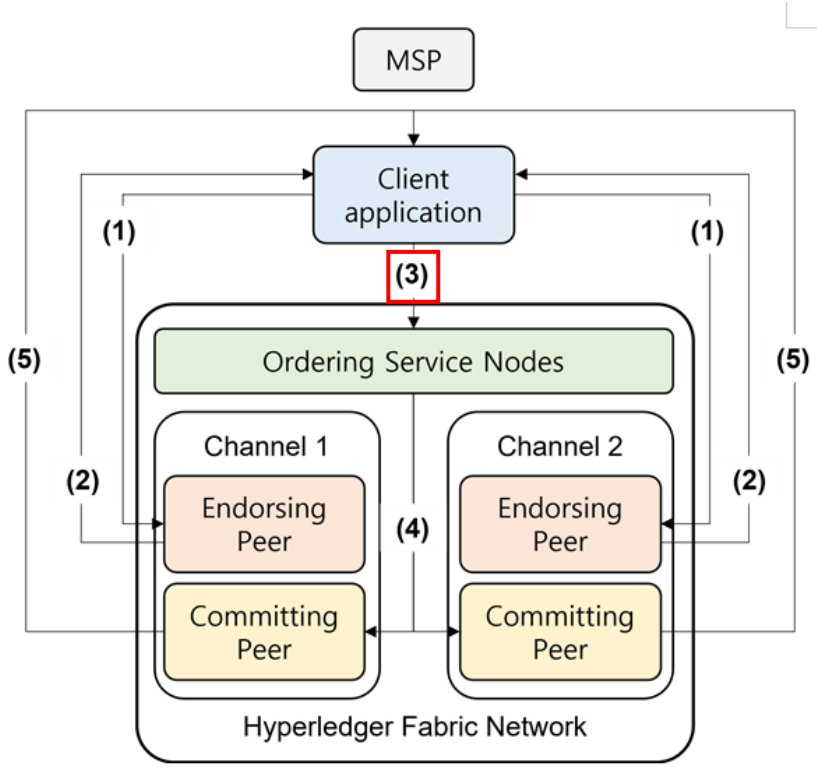
→ 클라이언트가 Endorsing Peer들의 서명 확인

→ 각 peer들로부터 수신한 proposal response를 비교 및 검증

→ Proposal과 proposal message가 담긴 트랜잭션을 OSN에게 전송

(4) Order Transaction

(5) Ledger Commit



세부 동작 과정

(1) Transaction Proposal

(2) Proposal Response

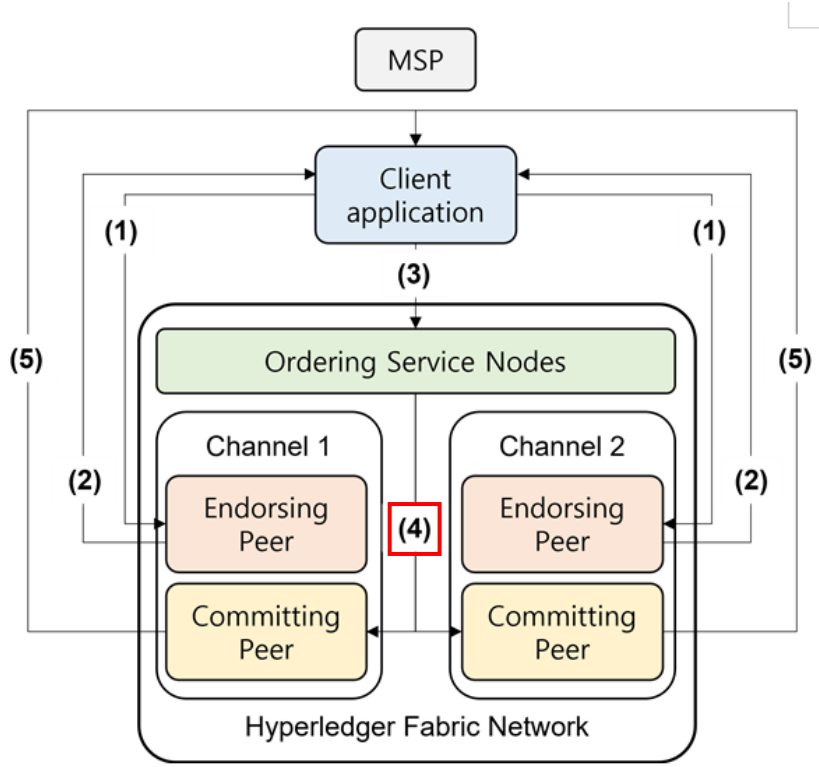
(3) Submit Transaction

(4) Order Transaction

→ 트랜잭션 정렬 후, 블록 생성

→ 각 채널의 committing peer들에게 블록 전송

(5) Ledger Commit



세부 동작 과정

(1) Transaction Proposal

(2) Proposal Response

(3) Submit Transaction

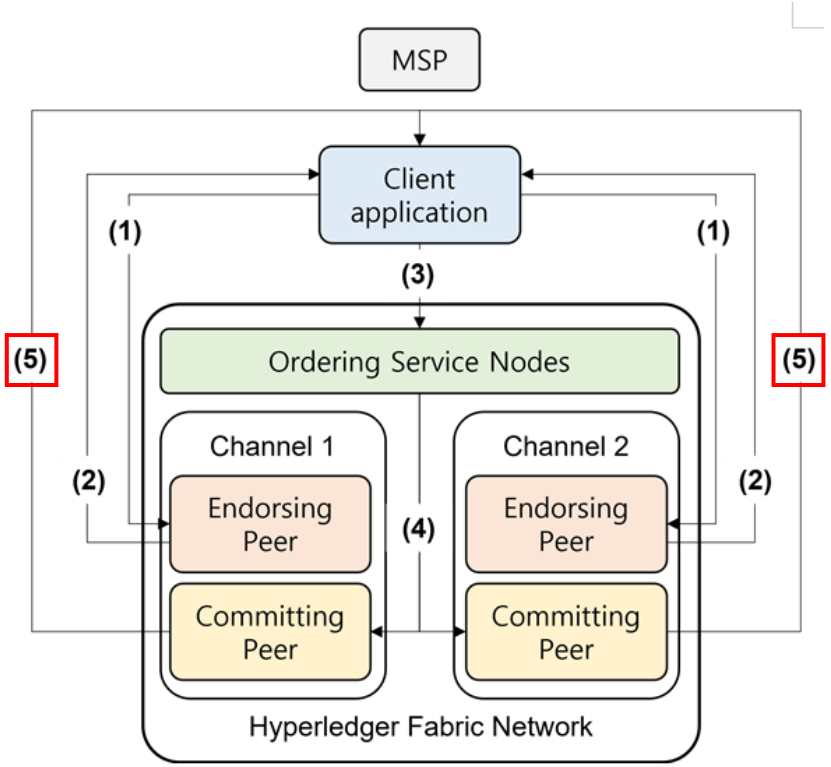
(4) Order Transaction

(5) Ledger Commit

→ 트랜잭션 유효성을 검사

→ 검증된 트랜잭션은 원장에 추가 후, 클라이언트에게 결과 전송

→ 검증 실패 시 트랜잭션 무효 처리



Q & A