ARGOS 동계 세미나_0129

201502086 이성복

contents

- 합의 알고리즘
- 하이퍼레저 패브릭

합의 알고리즘

합의 알고리즘

비잔틴 장군 문제

합의 알고리즘

FLP Impossibility

- Safety(finality)
  - 노드 간 합의가 발생했다면 어느 노드가 접근하든 그 값이 동일해야함
- Liveness
  - 블록(합의 대상)에 문제가 없다면 반드시 합의가 이루어짐
- FLP Impossibility
  - 비동기 네트워크에서는 합의 문제를 완벽히 해결할 수 있는 분산 알고리즘이 없음

합의 알고리즘

Safety VS Liveness

Safety VS Liveness

합의 알고리즘

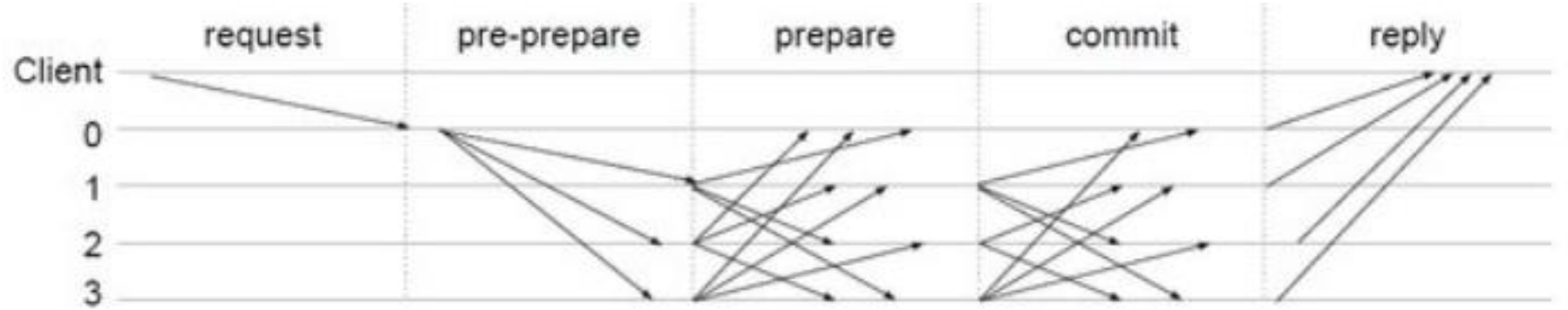
종류

- Proof of Work
- Proof of Stake
- PBFT

합의 알고리즘

BFT(Byzantine Fault Tolerance), P(Practical)BFT

- 네트워크에 배신자가 존재해도 합의의 신뢰를 보장하는 알고리즘
- 배신자가 f명일 때 총 3f + 1명 이상이면 해당 네트워크에서 이루어지는 합의는 신뢰할 수 있음



합의 알고리즘

BFT(Byzantine Fault Tolerance), P(Practical)BFT

- 네트워크에 배신자가 존재해도 합의의 신뢰를 보장하는 알고리즘
- 배신자가 f명일 때 총 3f + 1명 이상이면 해당 네트워크에서 이루어지는 합의는 신뢰할 수 있음

하이퍼레저 패브릭

블록체인

블록체인 종류

	Public	Private	Consortium
허가가 필요한가	X	O	O
누가 읽을 수 있나	누구나	허가된 사용자	경우에 따라 다름
누가 쓸 수 있나	누구나	허가된 사용자	허가된 사용자
소유자	X	단일 주체	복수 주체
참여자를 알 수 있나	X	O	O
트랜잭션 스피드	느림	빠름	빠름

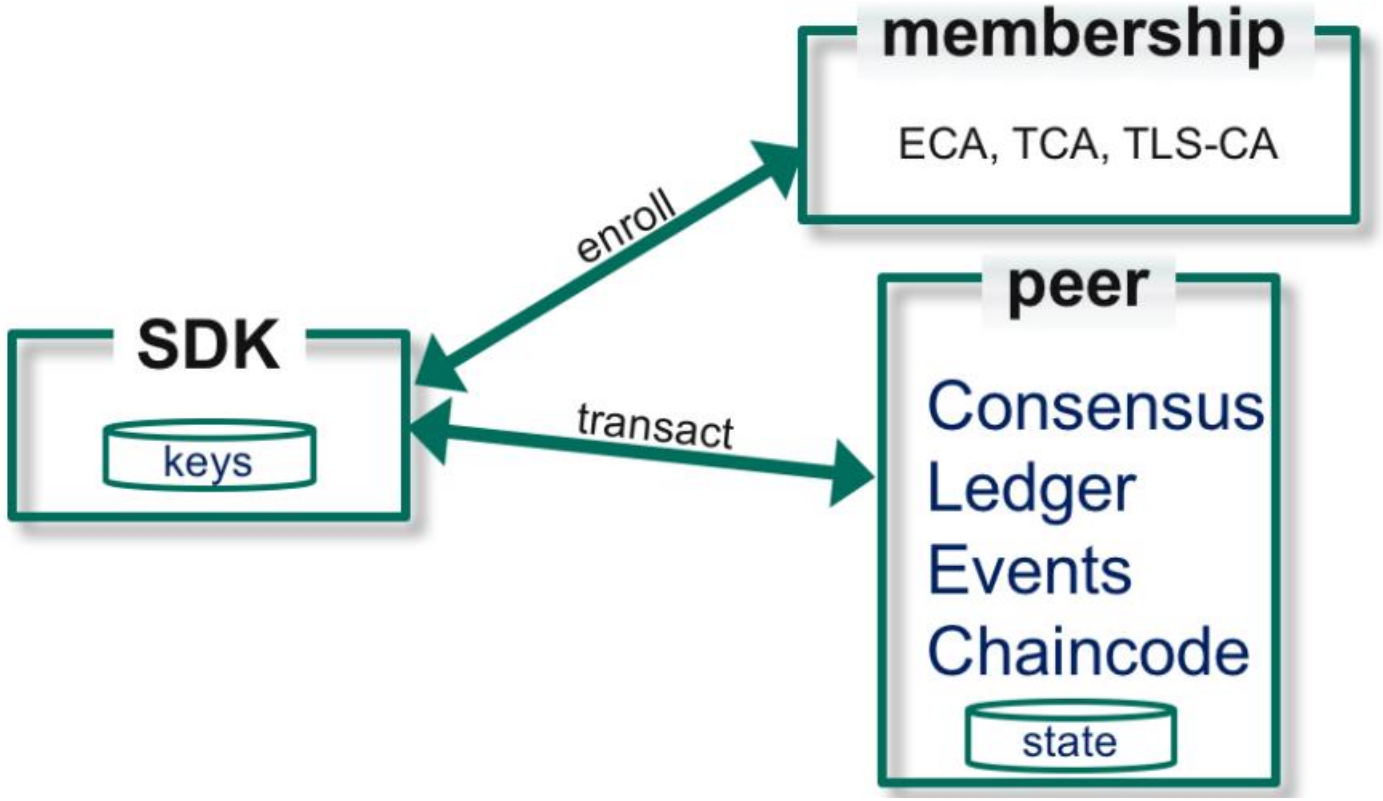
하이퍼레저 패브릭

주요 구성요소

- Orderer
- Peer
- Client
- Chaincode
- Channel
- CA
- MSP
- Ledger

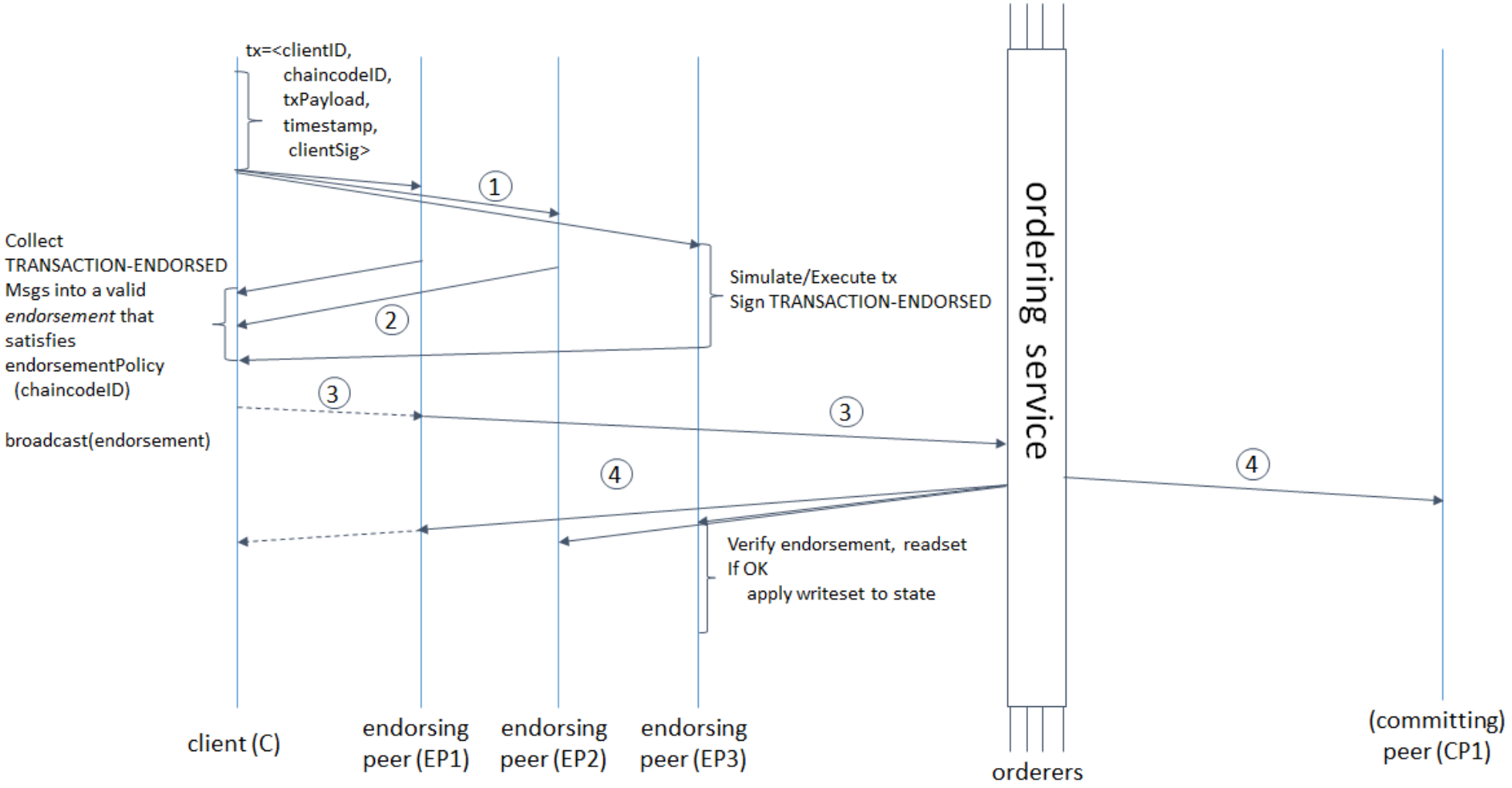
하이퍼레저 패브릭

v0.6



하이퍼레저 패브릭

v1.4



Question