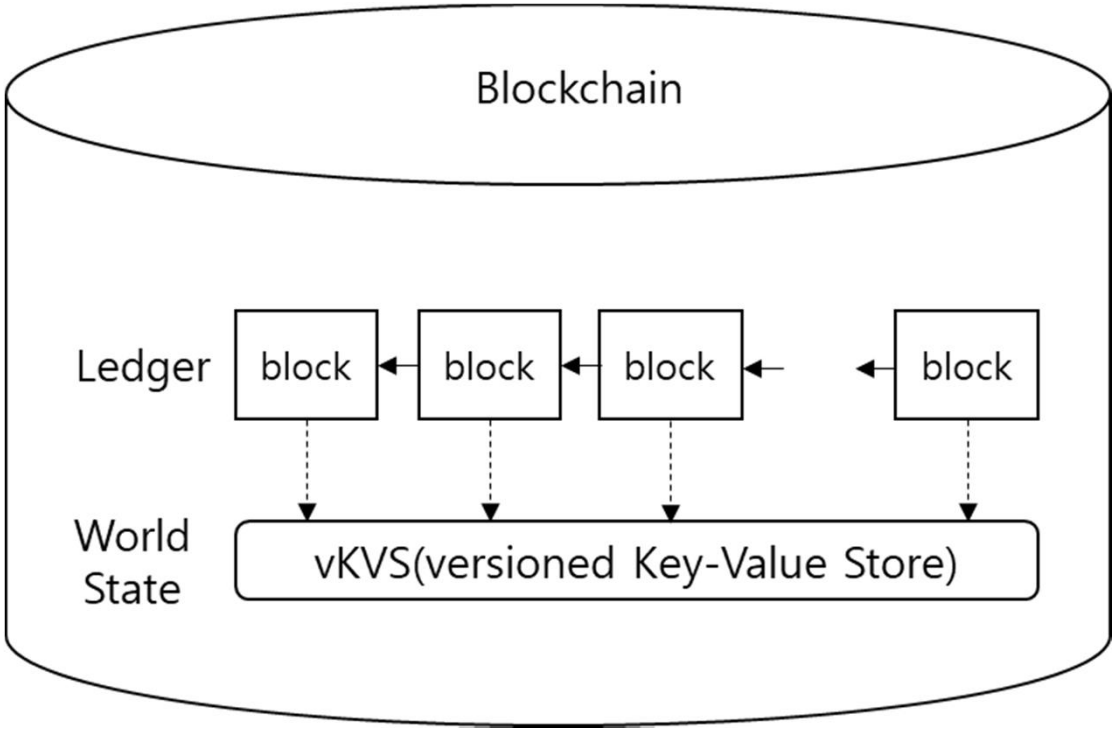
하이퍼레저 패브릭의 구조

박승철교수

블록체인 구조

❖ 구성

- 레저(ledger) + 전체 상태(world state)



블록체인 구조

❖ 전체 상태(world state)

- 거래 실행 결과에 따라 변경되는 블록체인의 상태 변화 정보를 저장
- 버전형 키-값 저장소(vKVS-versioned Key-Value Store) 형태로 모델링
- 키(key) : 체인코드(chaincode)가 사용하는 정보 이름
- 값(value) : 이름에 대응되는 정보
- 버전(version)은 특정 키와 값의 쌍의 상태를 번호(number)로 표시
- 값이 갱신될 때마다 새로운 버전 번호(version number)가 부여되어 기존의 키-값의 쌍의 상태 구분

블록체인 구조

❖ 전체 상태(world state)

- 상태 변화 예 : (car.no = 1234, car.owner = park, car.maker = Hyundai) → (car.no = 1234, car.owner = kim, car.maker = Hyundai)
- 키 버전 변화 :
  s(car.owner.value) = park), s(car.owner.version) = 5)
  →
  s(car.owner.value) = kim), s(car.owner.version) = 6)
- 전체 상태 = 블록체인의 모든 거래가 접근하는 키 집합에 대한 현재의 값과 버전 정보 집합

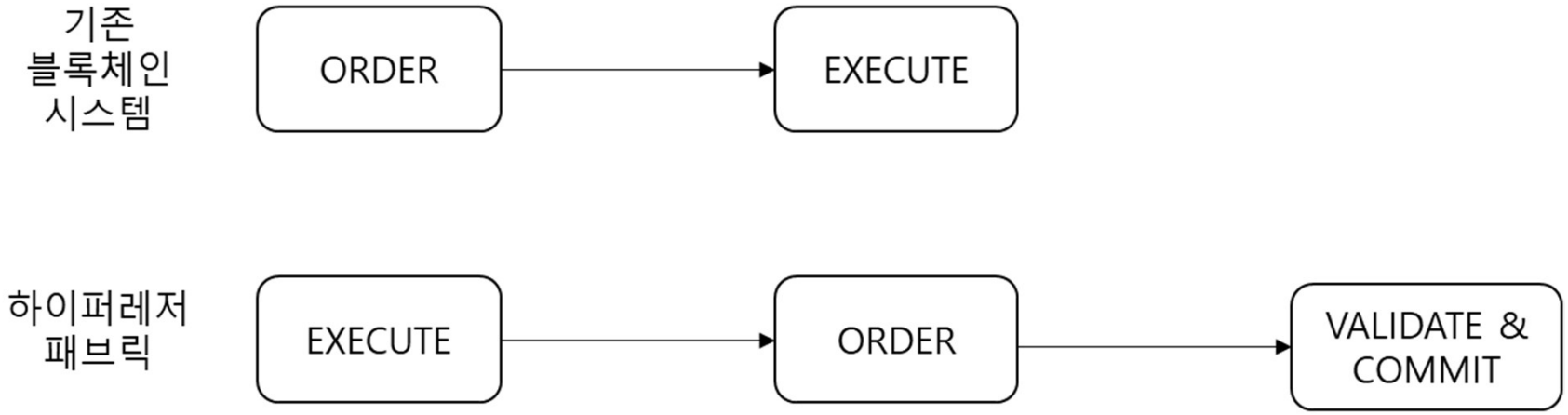
블록체인 구조

❖ 레저(ledger)

- 시스템 운영 과정에서 발생하는 모든 거래 정보를 해시 체인(hash chain) 형태로 저장
- 블록에 포함되는 거래의 수는 응용의 요구사항에 따라 달라질 수 있음
- 레저를 통해 전체 상태 변경의 이력 추적 가능

거래 처리 구조

❖ 거래 처리 방식 비교



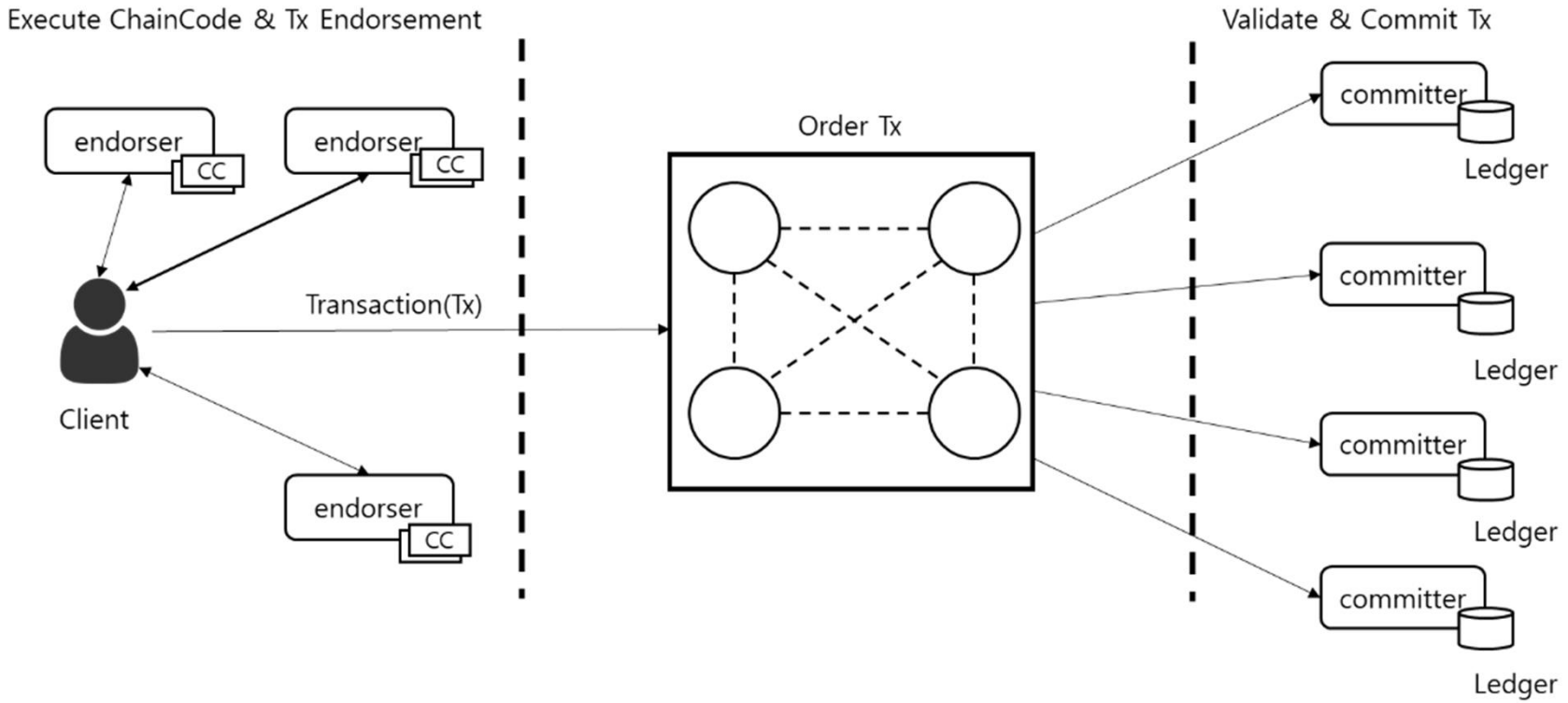
거래 처리 구조

❖ 기존의 블록체인 시스템

- 대부분 발생한 거래들을 합의 알고리즘을 통해 순서화 시킨 다음 피어(풀 노드)들에게 전달
- 블록체인을 유지하는 피어에 의해 독립적으로 처리
- 거래들은 순서가 매겨진 대로 순차적으로 실행
- 결과가 동일하게 유지되도록 하기 위해 스마트 계약 프로그램은 반드시 결정적으로(deterministically) 작성

거래 처리 구조

❖ 하이퍼레저 패브릭의 거래 처리 순서



거래 처리 구조

❖ 하이퍼레저 패브릭의 거래 처리 순서

- 비결정적 프로그램(non-deterministic program) 지원, 거래의 병렬 처리 등을 위해 거래 처리 구조를 변경
- 실행 → 순서화 → 검증 및 확정의 단계로 처리
- 클라이언트는 해당 체인코드의 보증 정책에 맞는 보증 노드에게 거래를 송신하고, 거래의 실행은 보증 노드에 의해 수행
- 보증 노드는 거래 실행 결과를 별도의 자료구조 (readset, writeset)에 담아 클라이언트에게 회신
- 보증 노드는 거래 실행 결과를 블록체인에 미적용

거래 처리 구조

❖ 하이퍼레저 패브릭의 거래 처리 순서

- 실행 결과를 수신한 클라이언트는 순서화 서비스 채널을 통해 거래 결과를 전송
- 순서화 서비스를 수행하는 노드들은 적용하는 합의 알고리즘에 따라 그 동안 발생한 거래들을 순서화
- 순서화된 거래들은 블록에 담겨 채널에 연결된 모든 피어들에게 안전하게 전달
- 거래 결과를 수신한 피어들은 거래 결과가 보증 정책에 맞게 만들어졌는지 검증하고, 적합하게 실행된 거래의 결과를 블록체인에 저장함으로써 해당 거래를 확정

멤버십 서비스 제공자 구조

요구 사항

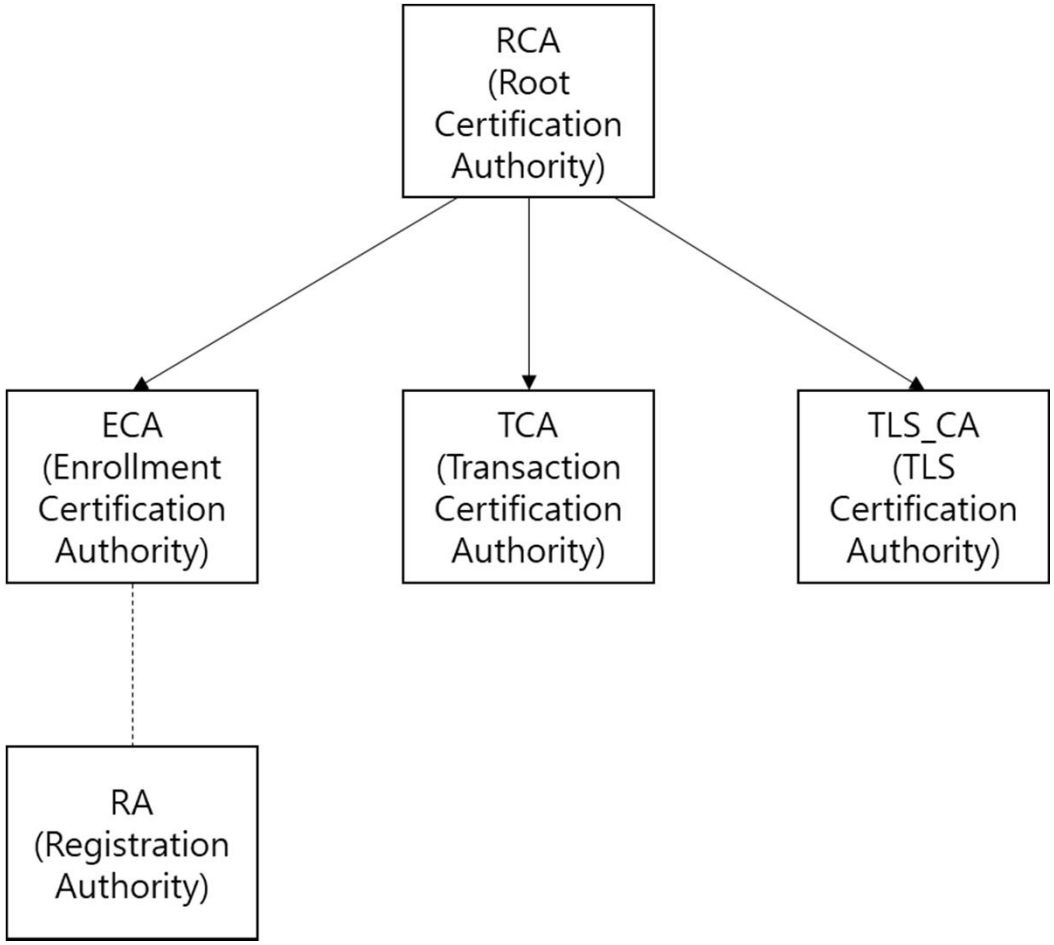
- 책임성(accountability) 보장
- 프라이버시(privacy) 보장

멤버십 서비스 제공자 구조

- 책임성(accountability) 보장
  - 모든 참가자의 행위에 대해 정당한 책임 부여
  - 참가자의 행위 추적
  - 참가자가 자신의 행위 부인 방지
  - 다른 참가자의 행위에 대해 부당하게 책임지지 않는 것을 보장
  - 제3자를 통한 참가자의 행위 감사(audit) 보장
- 프라이버시(privacy) 보장
  - 거래 익명성(transaction anonymity) 보장
  - 거래 비연결성(transaction unlinkability) 보장

멤버십 서비스 제공자 구조

❖ 하이퍼레저 패브릭의 **PKI** 구조



멤버십 서비스 제공자 구조

ECA(Enrollment CA)

- 블록체인에 접근하고자 하는 참가자의 신원을 검증한 후에 등록 인증서(ECert - Enrollment Certificate)를 발급하는 역할을 수행
- 등록된 참가자를 확인하는 데 필요한 공개키와 개인키 쌍의 생성을 포함
- 참가자 등록을 위한 신원 확인은 등록 기관(RA – Registration Authority)에 위임 가능
- 신원 확인 방법과 확인 결과의 전달 방법은 응용의 요구사항에 따라 달라질 수 있음

멤버십 서비스 제공자 구조

TCA(Transaction CA)

- ECA에 의해 발급된 등록 인증서에 근거하여 신원이 확인된 참가자에게 거래 인증서(TCert – Transaction Certificate)를 발급하는 역할
- 등록 인증서(ECert)를 기반으로 충분한 수의 거래 인증서(TCert)를 발급
- 등록 인증서를 유추할 수 있는 어떤 정보도 포함하지 않음으로써 참가자의 신원이 노출되지 않도록 보장
- 각 거래 인증서는 동일 등록 인증서를 통해 발급된 다른 거래 인증서와의 연관성 정보를 포함하지 않음으로써 거래 비연결성 보장

멤버십 서비스 제공자 구조

TLS_CA(Transport Layer Security CA)

- 신원이 확인된 참가자를 대상으로 보안 통신 프로토콜인 TLS 프로토콜이 사용할 수 있는 인증서를 발급
- 네트워크 연결을 설정하는 등록된 참가자를 확인하는데 필요한 공개키와 개인키 쌍의 생성 포함

멤버십 서비스 제공 절차

- 사용자와 클라이언트에 대한 멤버십 서비스 제공 과정