하이퍼레저 패브릭 개요

박승철교수

하이퍼레저 프로젝트

❖ 목표

- 기존 블록체인 시스템 : 낮은 성능, 신원 확인 결여, 무한 경쟁에 따른 과다한 자원 소모
- 기존 블록체인 시스템들에 비해 높은 성능, 신뢰성, 자원 효율성, 그리고 참여자 관리 등 비즈니스 응용의 요구사항을 충족시킬 수 있는 블록체인과 분산 원장 (distributed ledger)에 개발에 산업계의 협력 촉진

하이퍼레저 프로젝트

❖ 수행 기관

- 리눅스 재단(Linux Foundation)
- 프로젝트에는 IBM, 인텔을 포함한 많은 ICT 업체, J.P. Morgan 을 포함한 유수의 금융 서비스 관련 업체, SAP 을 포함한 많은 비즈니스 소프트웨어 업체 등이 참여

하이퍼레저 프로젝트

❖ 하이퍼레저 비즈니스 블록체인 프로젝트

프로젝트	목표
Fabric	모듈 구조를 가지는 분산 응용 플랫폼 개발. 합의 프로토콜, 멤버십 서비스 등의 모듈을 필요에 따라 교체 가능
Sawtooth	경과 시간 증명(Proof of Elapsed Time) 기반의 합의 알고리즘을 적용하여 적은 자원으로 많은 수의 참여자를 지원하는 모듈형 플랫폼 개발
Iroha	패브릭 프로젝트를 모바일 응용 적용에 초점
Burrow	허가형 스마트 계약 해석기를 가지는 모듈 구조의 블록 체인 클라이언트 제공. 허가형 이더리움에 초점
Indy	블록체인 상에서 독립적인 디지털 신원 제공
Explorer	블록체인에 저장된 정보 분석 도구 개발
Composer	블록체인 비지니즈 네트워크와 스마트 계약의 개발과 적용을 돕는 도구 개발
Chello	서비스에 맞는 블록체인을 온-디멘드(on-demand) 방식으로 제공하는 블록체인 생태계 제공
Quilt	서로 다른 블록체인간의 상호동작성(interoperability) 제공

하이퍼레저 패브릭

❖ 현황

- 하이퍼레저 프로젝트들 중에 가장 먼저 제안
- 2017년 상반기에 버전 0.6이 발표
- 2017년 하반기에 버전 1.0이 발표되어 활용

❖ 참여 기관

- IBM이 개발을 주도
- 엑센추어(Accenture), 인텔, 히다찌, 시스코, 금융 서비스 업체들의 블록체인 컨소시엄인 R3 등

하이퍼레저 패브릭

❖ 목표

① 알려진 참가자를 대상으로 하는 비즈니스 응용 환경에 맞는 블록체인 개발

② 서로 다른 요구사항을 가지는 다양한 분산 응용 개발을 효율적으로 지원할 수 있는 플랫폼 개발

③ 모듈 구조를 가지는 분산 응용 플랫폼 개발 → 합의 프로토콜, 멤버십 서비스 등의 모듈을 필요에 따라 교체 가능

하이퍼레저 패브릭의 특징

❖ 특징

① 허가형(permissioned) 블록체인
② 일반 프로그래밍 언어(general-purpose programming language) 사용
③ 내부 가상통화 부재(no internal cryptocurrency)
④ 높은 성능(high performance)
⑤ 교체 가능한 모듈 구조(pluggable modular architecture)
⑥ 멀티 블록체인(multi-blockchain) 지원

하이퍼레저 패브릭의 특징

1. 허가형(permissioned) 블록체인

- 멤버십 관리 서비스를 통해 허가된 참여자만 접근을 허용
- 참여자의 블록체인 접근 권한을 제어 가능
- 참여자 행위에 대한 책임성(accountability) 확인의 요구사항을 반영
- 작업 증명 기반의 합의 알고리즘을 사용하는 대신 보다 효율적인 합의 알고리즘을 사용 가능
- 높은 거래 완료성(transaction finality)

하이퍼레저 패브릭의 특징

❖ 비허가형 블록체인과 허가형 블록체인의 비교

구분	비허가형 블록체인	허가형 블록체인
참여자 관리	없음	있음
접근권한 제어	불가능	가능
책임성	없음	있음
합의 알고리즘	작업 증명	비작업 증명 유형
거래 완료성	낮음	높음

하이퍼레저 패브릭의 특징

2. 일반 프로그래밍 언어(general-purpose programming language) 사용

- 체인코드(chaincode) : 하이퍼레지 패브릭의 스마트 계약 프로그램
- 이더리움 : 모든 피어(peer)의 블록체인에서 실행된 스마트 계약의 결과가 항상 동일한 것을 보장하기 위해 결정적(deterministic) 프로그래밍 언어를 특별히 개발하여 사용(예, Solidity)
- 하이퍼레저 패브릭 : Go, Java 등 일반적인 프로그래밍 언어 사용

하이퍼레저 패브릭의 특징

3. 내부 가상통화 부재(no internal cryptocurrency)

- 내부 가상 통화가 필요한 이유 :
  - ① 거래 수수료 지불
  - ② DoS 공격 방지

하이퍼레저 패브릭의 특징

3. 내부 가상통화 부재(no internal cryptocurrency)

- 비작업 증명 방식의 합의 : 수수료 불필요
- 지정된 보증 피어(endorsing peer)만 체인 코드 실행
- DoS 공격은 해당 보증 피어들에만 영향
- 보증 피어가 내부 정책을 통해 체인코드 실행 포기 시점 결정 가능 → 무한한 체인코드 실행 방지 가능

하이퍼레저 패브릭의 특징

4. 높은 성능(high performance)

- 서로 다른 보증 피어들을 통해 체인코드를 실행하는 다수의 거래들을 동시 처리 가능 → 높은 성능
- 정보 이름에 해당하는 키의 버전 관리를 통해 동시 처리에 따른 비결정적 실행(non-deterministic execution) 문제 해결

하이퍼레저 패브릭의 특징

5. 교체 가능한 모듈 구조(pluggable modular architecture)

- 하이퍼레저 패브릭은 전체 시스템을 모듈 구조로 설계하고, 합의 알고리즘 등 응용에 따라 요구사항에 차이가 큰 모듈을 필요에 따라 교체 가능
- 합의 프로토콜 : SOLO, Kafaka, PBFT(Practical Byzantine Fault Tolerant) 등

하이퍼레저 패브릭의 특징

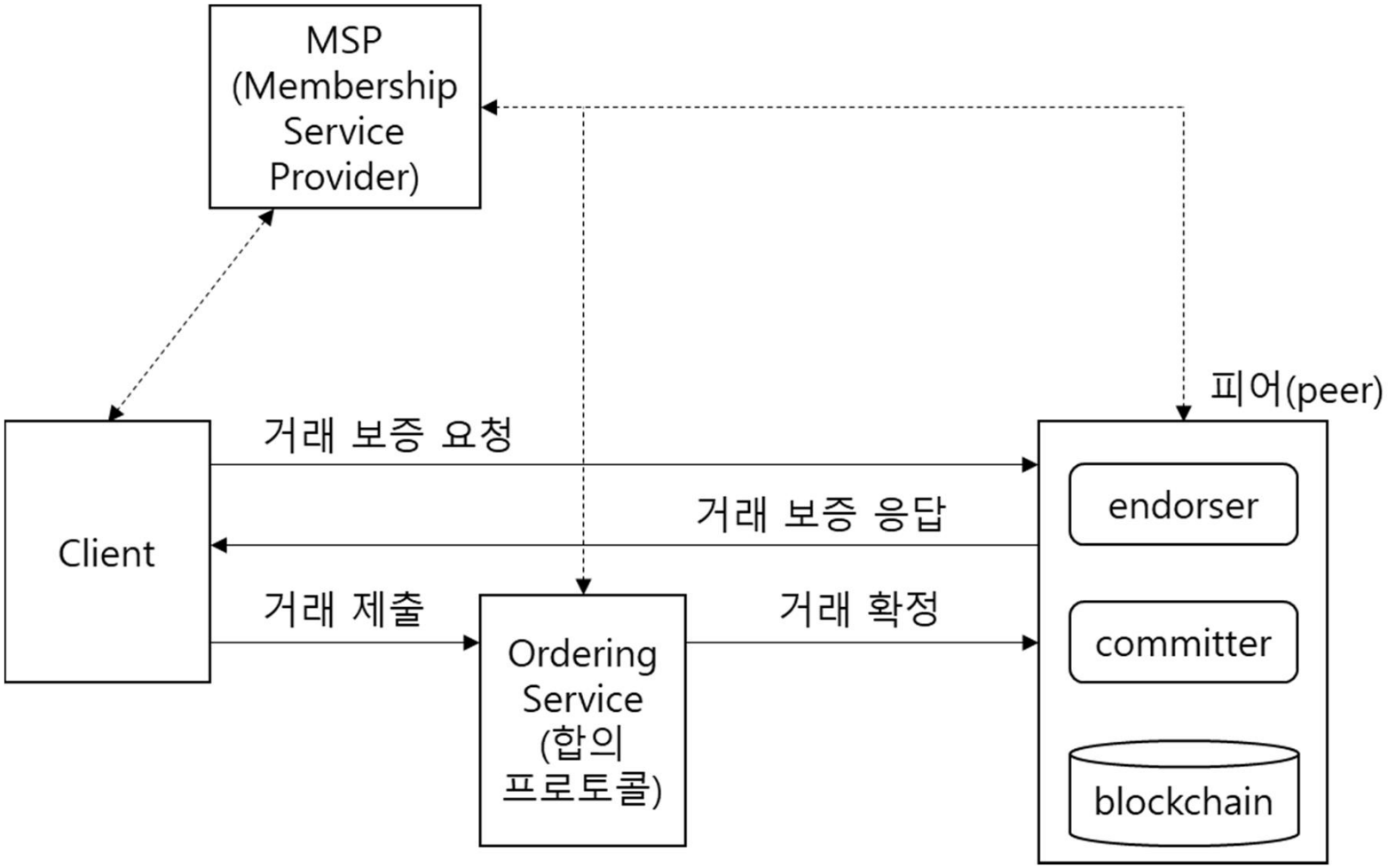
6. 멀티 블록체인(multi-blockchain) 지원

- 전체 시스템을 다수의 채널(channel)로 구분
- 채널별로 별도의 독립적인 블록체인 유지 가능
- 참여자는 특정 채널에 가입함으로써 공유할 블록체인을 선택할 수 있고, 다수의 채널에 가입 가능

이더리움과 하이퍼레저 패브릭 비교

구분	이더리움	하이퍼레저 패브릭
유형	비허가형	허가형
프로그램 이름	스마트 계약	체인코드
프로그램 형태	결정적(deterministic)	비결정적(non-deterministic)
내부 통화	있음(ETH)	없음
거래 수수료	있음(gas)	없음
프로그램 언어	자체 언어(Solidity)	일반 언어(Go, Java)
거래 처리방식	순차적	병렬적
합의 알고리즘	작업 증명(PoW)	비작업 증명형(SOLO, Kafaka, BFT 등)
결제 완료시간	1분 이상	즉시
멀티블록체인	미지원	지원

하이퍼레저 패브릭 시스템 구조



하이퍼레저 패브릭 시스템 구조

❖ 클라이언트 노드(client node)

- 사용자를 대신하여 거래(transaction)를 생성하여 체인코드 실행을 호출하는 노드
- 클라이언트 노드는 거래를 생성하여 보증 피어 노드(endorsing peer node)에게 제출(submit)함으로써 거래 보증을 요청하고 거래 보증 응답을 수집
- 거래 보증 응답을 수집한 클라이언트는 거래 제안(transaction-proposal)을 생성하여 순서화 서비스 노드에게 전달

하이퍼레저 패브릭 시스템 구조

❖ 피어 노드(peer node)

- 피어 노드는 거래를 확정(commit)
- 거래 정보를 저장하는 레저(ledger)와 거래 실행 결과에 따른 상태 정보를 저장하는 상태 저장소(state store)로 구성되는 블록체인 유지
- 순서화 서비스 노드(ordering service node)로부터 블록 형태로 거래와 상태 갱신 정보 수신
- 일부 피어 노드는 추가적으로 보증 노드(endorsing peer) 역할을 수행

하이퍼레저 패브릭 시스템 구조

❖ 피어 노드(peer node)

- 보증 노드는 클라이언트의 보증 요청에 따라 해당 체인코드를 실행하고 결과를 보증하는 역할을 수행
- 보증 노드와 보증 방법은 해당 체인코드와 연계된 보증 정책에 의해 결정
- 보증 정책은 체인코드와 함께 작성되어 체인코드가 블록체인에 배치될 때 함께 배치

하이퍼레저 패브릭 시스템 구조

- 순서화 서비스 노드**(ordering service node)**
  - 합의 알고리즘에 따라 클라이언트들로부터 제안되는 거래들을 순서화시켜 피어 노드들에게 안전하게 전달
  - 클라이언트는 채널을 통해 거래를 포함하는 메시지를 순서화 서비스 노드들에게 전달하고, 순서화 서비스 노드들은 거래 메시지들을 순서화시켜 채널에 연결된 모든 피어들에게 전달
  - 각 피어에게 전달되는 거래 메시지들이 동일한 순서를 가지고 안전하게 전달되는 것을 보장하는, 원자적 브로드캐스트(atomic broadcast) 서비스 제공

하이퍼레저 패브릭 시스템 구조

- 멤버십 서비스 제공자**(MSP-Membership Service Provider)**
  - 하이퍼레저 패브릭에 접속하는 노드의 신원 확인 후 네트워크에 접속할 수 있는 권한을 표시하는 자격증명(credentials)을 발급
  - PKI(Public Key Infrastructure) 기반의 인증 기관(Certification Authority)을 통해 서비스에 맞는 공개키 인증서(public key certificate)와 대응되는 개인키(private key)를 자격증명으로 발급