클레이튼 블록체인 어플리케이션 만들기

6기_이희제

기존 블록체인 플랫폼의 약점

- [x] Scalability
- [x] Finality
- [x] Fork

Scalability

TPS + Block Interval

TPS => Transaction Per Second : 초당 몇개의 거래를 처리하는지를 의미한다.

Block Interval : 블록 생성 간격

Scalability

TPS

visa: TPS 1700

비트코인: TPS 7

이더리움 : TPS 15~20

Scalability

비트 코인과 이더리움

- 많은 양의 트랙잭션 처리하기 부족
-네트워크 자체 속도 느림

Finality

변경 불가능한 최종적인 상태

Final block : 블록에 담긴 거래가 바뀔 수 없다는 것을 보증

비트코인과 이더리움
-최종성 부족
-확률론적 최종성만 제공

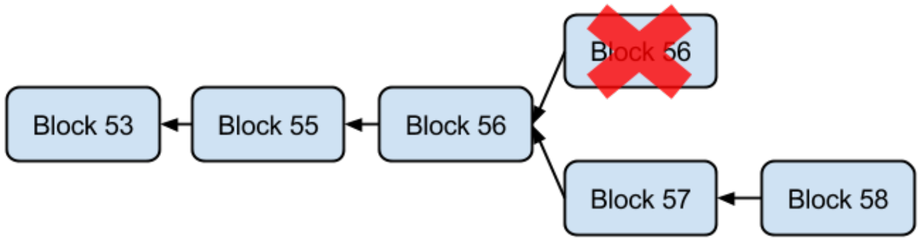
Finality => 거래가 변경 불가라는 합리적인 보장받기까지 기다려야하는 시간.

Fork

거래의 분기

작업증명(PoW) 방식

- 블록체인에 블록 추가하기 위해 문제를 품(Hash 값 찾기)



클레이튼 이해하기

- [x] 합의
- [x] 블록 생성 및 전파
- [x] 네트워크 구조
- [x] 코어 셀
- [x] 서비스 체인

합의(Consensus)

Public 블록 체인: PoW, PoS 등등
Private 블록 체인: pBFT, Raft 등등

BFT (비잔티움 결함 허용)
- 참여 노드수 제한/ 성능 높임

합의(Consensus)

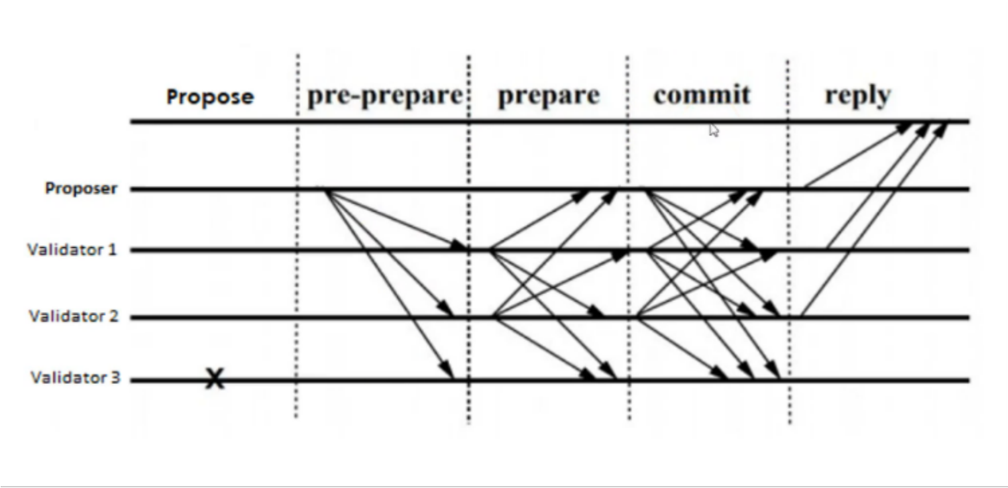
클레이튼의 합의 알고리즘 IBFT (이스탄불 비잔티움 결함 허용)

공개를 통한 개인적인 합의 신뢰 모델 채택

- 합의 달성 소수 private 노드
- 블록 생성 결과 접근 및 검증 노드

합의(Consensus)

라운드 로빈 방식



블록 생성 및 전파

블록 생성 사이클

- 블록 생성 주기 = 라운드 (round)
- 블록 생성 간격 = 약 1초

제안자와 위원회 선택

- 제안자를 무자위 그리고 결정적으로 Governance Council 노드들 중 뽑는다.
- 각각의 합의 노드가 가장 최근의 블록 헤더에서 파생된 난수 사용-> 라운드에서 선택됐는지 증명

블록 생성 및 전파

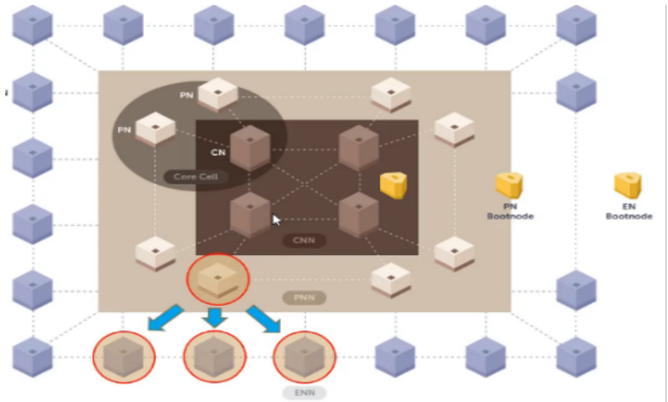
블록 제안과 검증

- 제안자의 공개키 통해 입증가능한 암호증명을 사용
- 누가 제안자이고 누가 위원회인지 파악 후 제안자가 블록을 만들고 합의

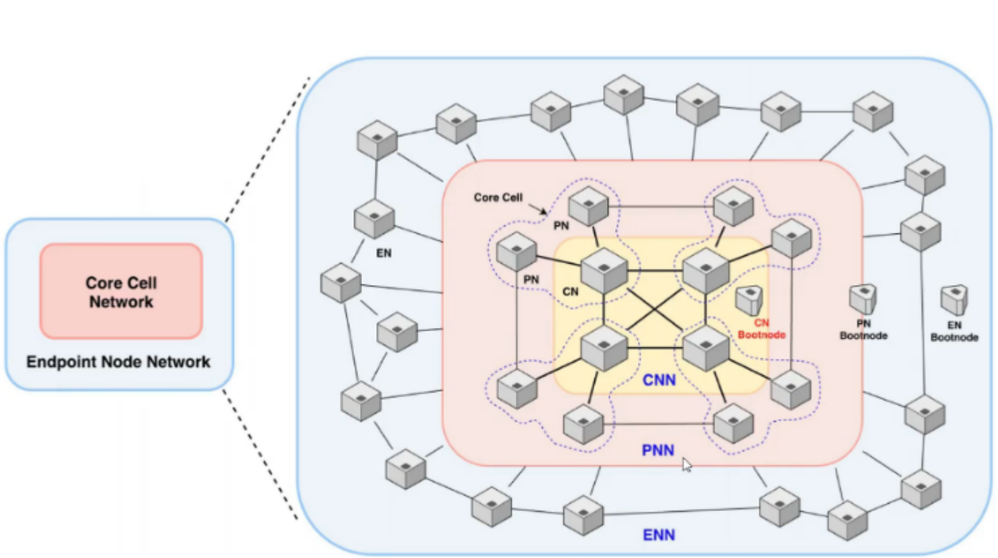
블록 생성 및 전파

블록 전파

- 프록시 노드 통해 엔드 포인트 노드들에게 전달.



네트워크 구조



CNN: Consensus Node Network

PNN: Proxy Node Network

ENN: Endpoint Node Network

코어 셀

코어 셀: 합의를 담당

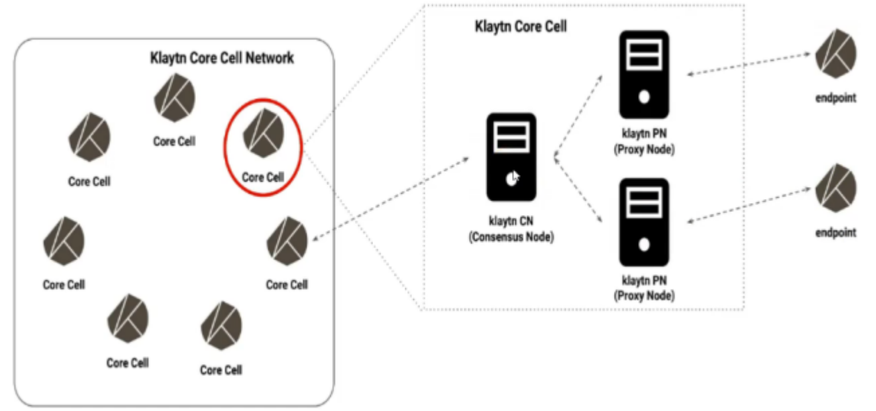
사용자가 많이져서 확장이 필요할 때

-일반적 : 서버 증대, request 증대

-클레이튼 : 노드 자체의 성능을 늘림

코어 셀

CN(합의 노드) 참여 조건
- physical core가 40개 이상
- 256GB RAM
- 1년치의 데이터 약 14TB
- 10G 네트워크



서비스 체인

메인넷과 연결된 독립적으로 운용되는 블록체인

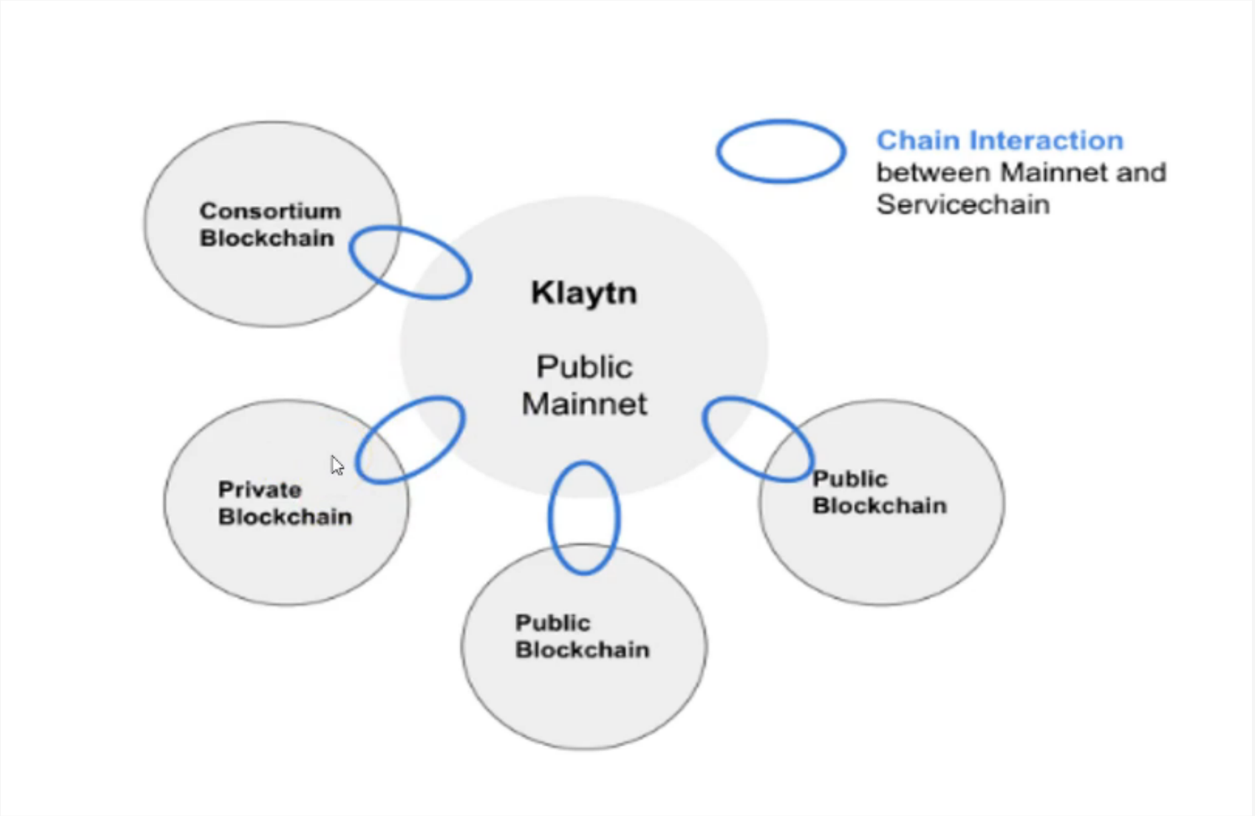
사용 상황

-특별한 노드환경에서 설정

-보안 수준 맞춤형으로 설정

-많은 처리량 요구/메인넷 배포시 경제성 낮음.

서비스 체인


Chain Interaction
between Mainnet and
Servicechain
Consortium
Blockchain
Klaytn
Public
Mainnet
Private
Blockchain
Public
Blockchain
Public
Blockchain