블록체인 확장성

https://youtu.be/j9YZwCe8hAA

Blockchain Layer

Scaling Solution

Lightning Network

Raiden Network

Blockchain Layer

- 블록체인은 탈중앙화, 보안, 확장성(트랜잭션 처리량)을 고려해야 함.

-> 블록체인의 트릴레마에 의해 세가지를 동시에 최적화하는 것은 불가능

- 확장성 vs 탈중앙화

  트랜잭션을 정산하기 위해서는 네트워크 구성원의 동의가 필요함

  이때, 구성원이 많은 경우 계약에 더 오랜 시간이 걸림

  즉, 확장성과 탈중앙화는 반비례 관계

  ex) VISA: 24,000 TPS

  비트코인: 7 TPS

- 확장성 vs 보안

  작업 증명에서, 해시레이트에 따라 보안이 비례

  즉, 확장성과 보안은 비례 관계

Blockchain Layer

- 확장성
  - 수평적 확장성
    - 암호 자산의 상호 운용성
    - 블록체인 간의 암호자산을 교환하는 것
  - 수직적 확장성
    - 트랜잭션 처리량 (TPS)
    - Layer 2를 통해 해결하고자 하는 문제

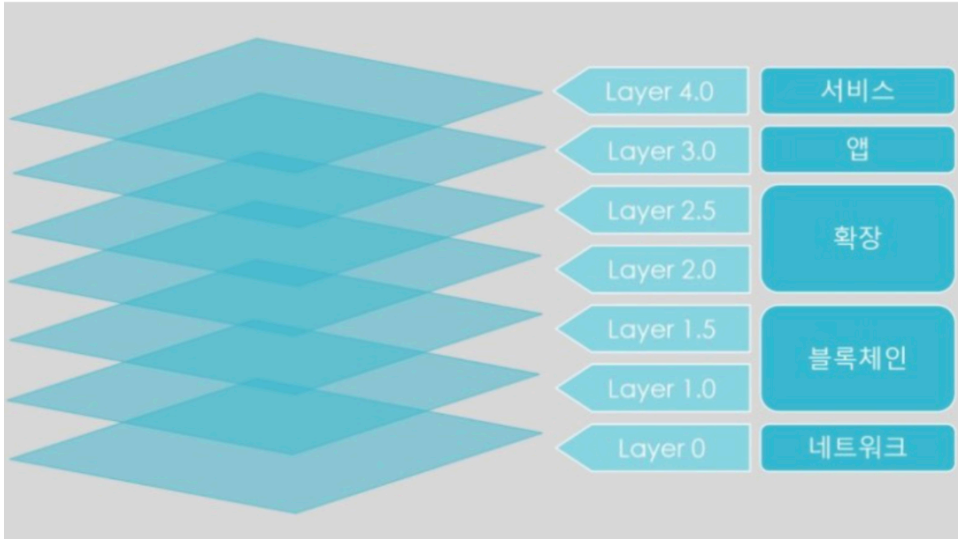
Blockchain Layer

- Layer 2

  - 기존 블록체인의 확장성을 향상시키기 위한 레이어

  - 기존 레이어(Layer 1) 위에 추가적인 레이어(Layer 2)를 쌓아,

  기존 레이어의 일부 기능을 추가적인 레이어에서 수행하게 된다.



Layer 2 Solution (Scaling Solution)

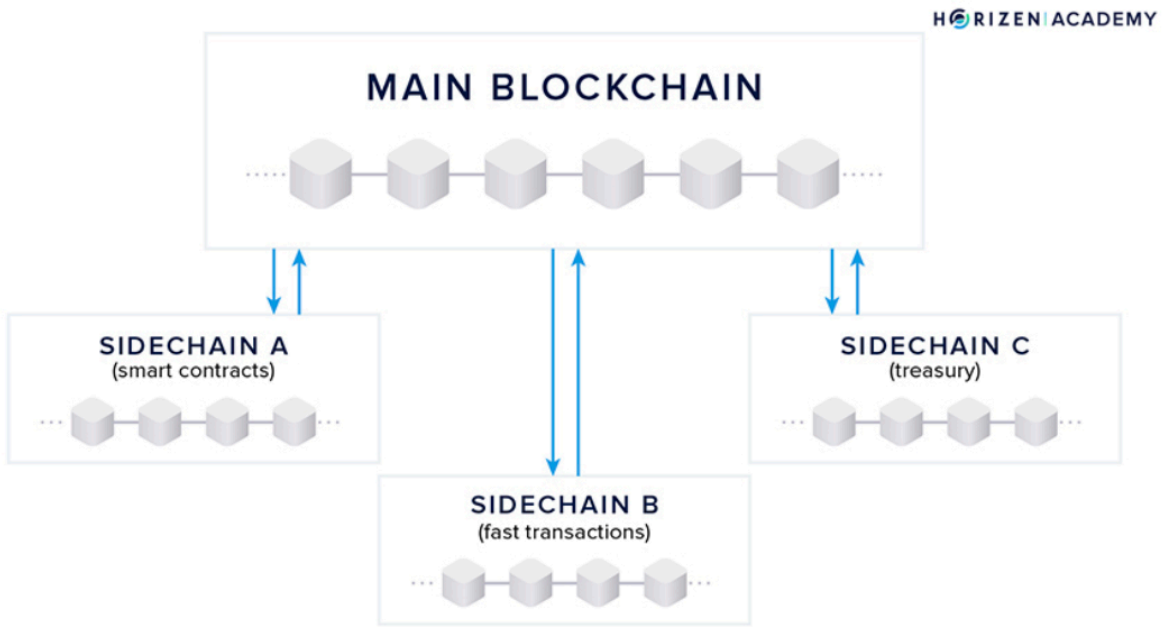
- Layer 2에서의 수많은 트랜잭션을 묶어서 처리한 후

Layer 1(블록체인)에 가끔씩만 쿼리하는 방식

- ex) 중첩 블록체인, 상태 채널, 사이드체인, 롤업, etc...

Scaling Solution (1)

- Side-chain
  - 메인넷에 대해 독립적으로 작동하는 분산 원장
  - IBC 프로토콜을 기반으로 한 양방향 연결을 통해 Layer 1 블록체인의 확장성 문제를 해결
  - 트랜잭션 확인 및 처리, 트랜잭션 작성, 합의 유지, 보안



Scaling Solution (1)

- Side-chain 단계
  - 블록 생성, 블록 헤더 전송, 블록 헤더 검증 및 기록

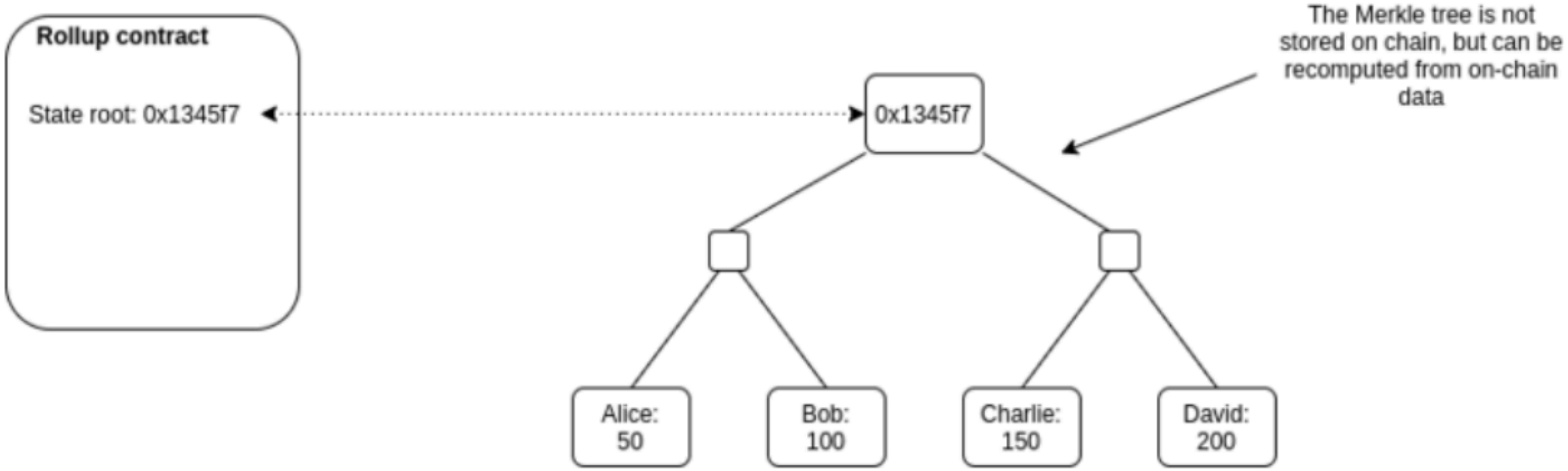
1) 블록 생성: 사이드체인 노드 자체 합의 알고리즘에 따라 블록을 생성한다. 그 후, 사이드체인 내에서 거래를 진행한 후 해당 거래를 블록에 기록한다.

2) 블록 헤더 전송: 생성된 블록체인의 블록 헤더를 주기적으로 Layer 1 블록체인에 전송 및 검증을 요청한다.

3) 블록 헤더 검증 및 기록: Layer 1 블록체인 내 노드는 사이드체인으로부터 전송받은 블록 헤더를 검증하고, Layer 1 블록체인에 이를 기록하여 트랜잭션의 검증을 완료한다.

Scaling Solution (2)

- Rollup
  - 메인 체인 외부에서 트랜잭션을 실행하고 그 결과값만 메인 체인에 기록하는 솔루션.
  - 트랜잭션 처리량, 공개 참여, 가스 비용 측면에서 이점을 얻을 수 있다.



Scaling Solution (2)

- Rollup 장점
  - 사이드체인은 반정기적으로 해시값을 전송하기 때문에 확장성은 뛰어나나 메인 네트워크와의 접점이 적기 때문에 보안은 감소한다.
  - Rollup은 사이드체인에 비해 트랜잭션 처리량은 적으나, 보안성이 우수하다.
  - 이론상, Rollup만으로도 4,807 TPS를 제공할 수 있으며, 데이터 샤딩을 통하여 최대 ~100,000 TPS까지 제공 가능하다.

Scaling Solution (2)

- Rollup 문제점
  - 데이터 가용성 문제 (Data Avaliability Problem)
    - ZK-Rollup: 오프체인에서 계산을 수행하고 체인에 유효성 증명을 전송한다.
    - Optimistic Rollup: 기본적으로 트랜잭션이 유효하다고 가정하고, 문제가 발생한 경우 위조 증명을 통해 계산만 실행한다.

Lightning Network

- 비트코인의 확장성문제를 해결하기 위한 오프체인 기반 Layer 2 지불 프로토콜
- 거래 당사자들간의 양방향 지불 채널을 생성하여 즉각적인 트랜잭션 가능
- 직접적으로 지불채널을 생성하지 않아도 충분한 자금을 보유한 네트워크 경로가 존재한다면 트랜잭션 가능
- 지불 채널을 열고 닫는 것은 온체인 기반

- 거래 과정

1) 당사자들간의 다중 서명 지갑 설정

2) 두 당사자 모두의 개인키를 통하여 접근

3) 트랜잭션 이후, 각자가 보유하고 있는 자금을 기록하고 있는 잔고 증명서 사본에 서명 후 업데이트

4) 트랜잭션을 모두 마친 후 지불 채널을 닫고 잔고 증명서를 비트코인 블록체인에 전송

Lightning Network

- 다중서명(멀티시그) 주소를 통하여 수천 개의 트랜잭션을 한 번에 전송 가능하도록 한다.

  => 채널을 열고 닫을 때에만 수수료를 내면 된다.

- 다중서명이란
  - - 하나의 주소에 n개의 개인키가 설정되어 있어, 해당 주소에서 인출을 하기 위해서는 일정 개수 이상의 개인키가 요구되는 기법
  - - 2-of-2 다중서명 주소

- 해시타임락을 통하여 신뢰성 제공

Lightning Network

- 지불 정산

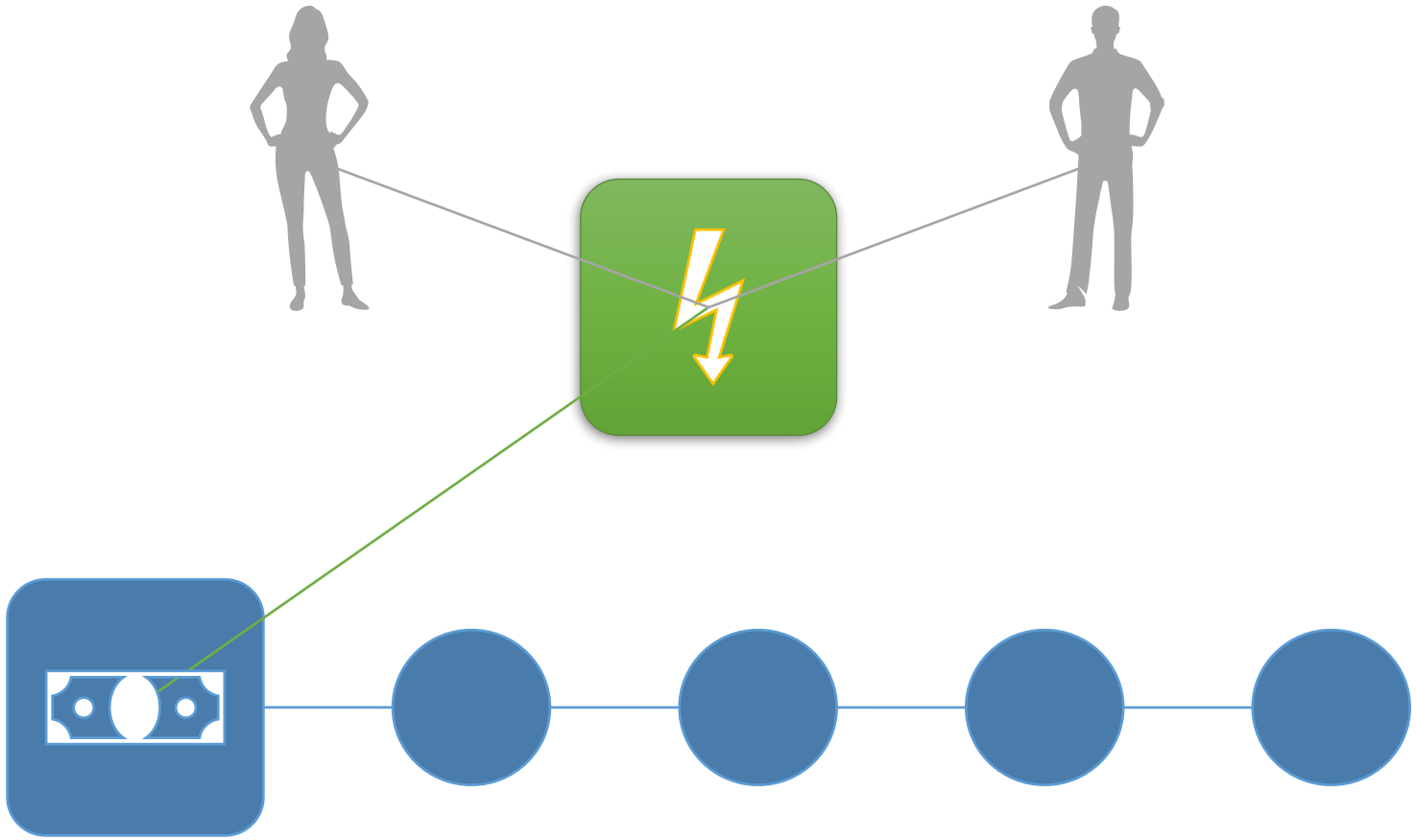
  1) 협조적 폐쇄

  2) 비협조적 폐쇄: 한 노드가 네트워크의 일부가 아니거나 오래된 배포를 브로드캐스팅하는 경우 수행

     - 자금이 즉시 결제되지 않으며, 노드가 브로드캐스팅 배포에 이의를 제기할 수 있는 기간이 존재

Lightning Network

- Lightning Network



Raiden Network

- 이더리움 블록체인에서 빠른 속도로 거래를 처리하기 위한 오프체인 방식의 네트워크 솔루션
- Lightning Network와 굉장히 유사

- 상태 채널 기반 1:1 양방향 거래

- Lightning Network와의 차이점
  - 글로벌 합의 없이 이용자들 간의 안전한 토큰 거래를 위하여 잔액 증명(balance proofs) 사용
  - ERC-20 토큰 거래를 위한 이더리움 특화 기술
  -> 비트코인의 Lightning Network와 비슷한 PLASMA

Q & A