SCALABILITY

OVERVIEW: BLOCKCHAIN LAYERS

TRILEMMA

BLOCKCHAIN TRILEMMA

- 블록체인 트릴레마
  - 확장성, 보안성, 탈중앙화의 세 속성을 다루는 용어

BLOCKCHAIN TRILEMMA

- 확장성(Scalability)
  - 블록체인이 많은 양의 트랜잭션을 처리할 수 있는 능력
  - 초당 트랜잭션 처리량(TPS)으로 수치화
  - 높은 TPS는 높은 확장성에 대응

BLOCKCHAIN TRILEMMA

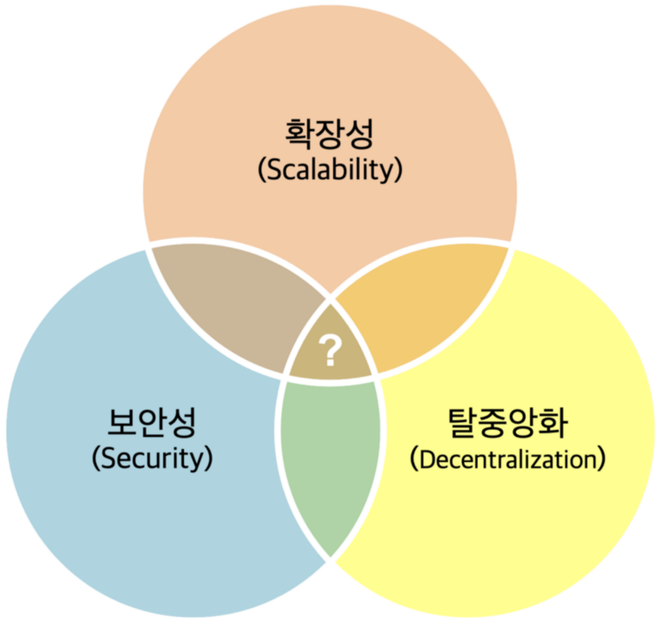
- 보안성(Security)
  - 트랜잭션의 안전한 처리를 보장할 수 있는 능력
  - 트랜잭션이 완결되기까지 요구되는 블록의 수 및 시간에 반비례
  - 블록 승인 시간이 낮을수록 보안성이 높음

BLOCKCHAIN TRILEMMA

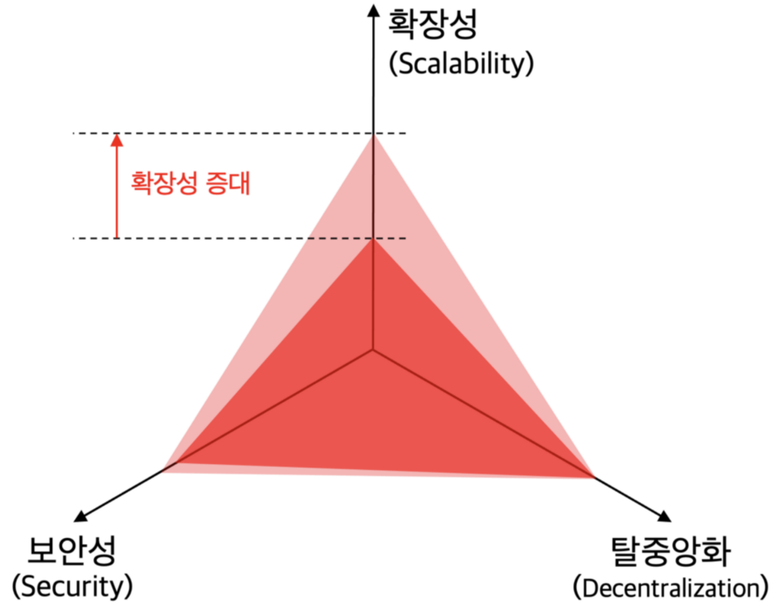
- 탈중앙화(Decentralization)
  - 제한된 자원을 가진 네트워크 참여자가 블록체인의 검증 프로세스에 현실적으로 참여할 수 있는 정도
  - 작업 증명 기반 블록체인의 해시 파워 분포
  - 블록체인의 활성화된(active) 사용자 수

BLOCKCHAIN TRILEMMA

- 블록체인의 한계를 언급할 때 주로 인용
- 비트코인과 이더리움
  - 보안성 및 탈중앙화를 확보한 대신 확장성 정도가 낮음
- 이오스
  - 확장성 및 보안성을 확보한 대신 탈중앙화 정도가 낮음
- Ref: Hinzen, Franz J., et al. “The public blockchain ecosystem: An empirical analysis.” NYU Stern School of Business (2019).



블록체인 트릴레마



블록체인 중요 속성

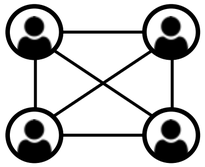
- 확장성, 보안성, 탈중앙화의 잘못된 해석(좌측)과 올바른 해석(우측)
- 세 속성을 모두 충족하는 것이 매우 어려울 뿐, 불가능하지 않음

LAYERS

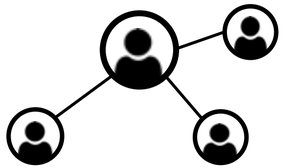
BLOCKCHAIN LAYERS

- 블록체인 시스템을 네 개의 계층으로 구분:
  - 하드웨어(hardware) 계층
  - 네트워크(network) 계층
  - 블록체인(blockchain) 계층
  - 오프체인(off-chain) 계층
- Ref: Gudgeon, Lewis, et al. "SoK: Off The Chain Transactions." IACR Cryptology ePrint Archive 2019 (2019): 360.

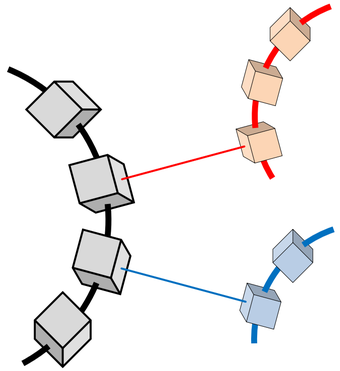
오프체인
(레이어-2)



채널

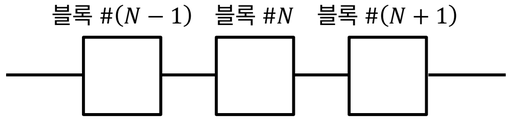


커밋 체인



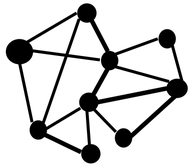
허브 앤 스포크

블록체인
(레이어-1)

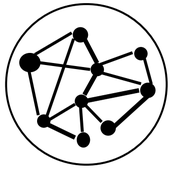


블록체인

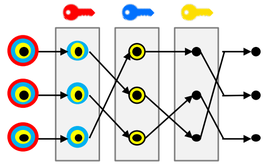
네트워크
(레이어-0)



공용 네트워크

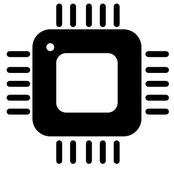


사설 네트워크



믹스넷

하드웨어



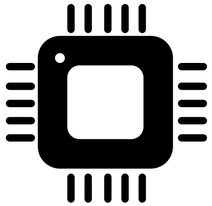
하드웨어

신뢰 실행 환경

HARDWARE

BLOCKCHAIN LAYERS

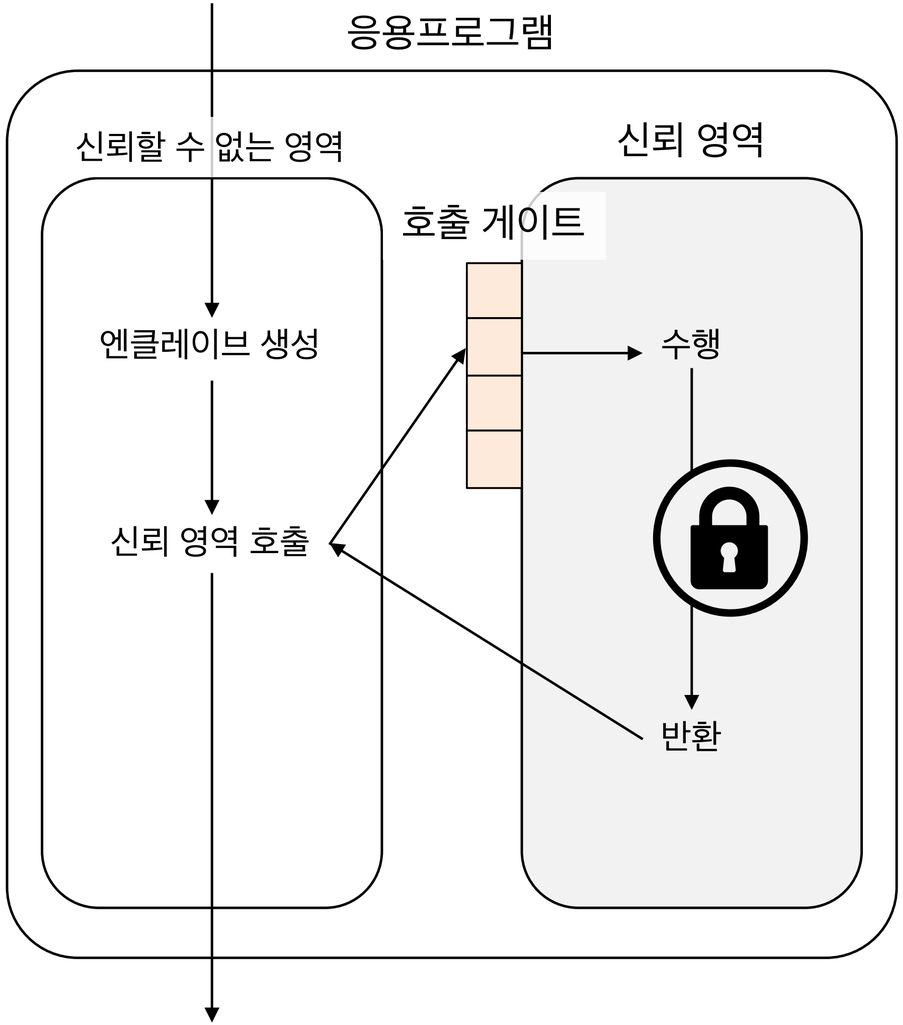
- 하드웨어 계층

하드웨어		
	하드웨어	신뢰 실행 환경

BLOCKCHAIN LAYERS

- 신뢰 실행 환경(Trusted Execution Environment, TEE)
  - 보안이 중요한 응용프로그램 코드를 enclave에서 구동
  - 운영체제나 권한이 높은 프로그램으로부터 쉽게 조작될 수 없음
  - 효율적인 오프체인 솔루션 및 프로토콜이 가능

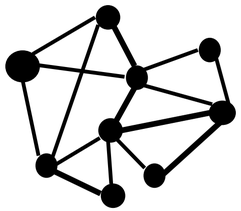
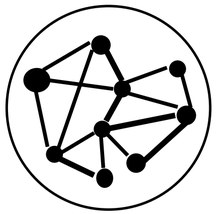
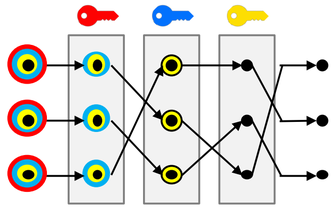
BLOCKCHAIN LAYERS



NETWORK

BLOCKCHAIN LAYERS

- 네트워크 계층

네트워크 (레이어-0)			
	공용 네트워크	사설 네트워크	믹스넷

BLOCKCHAIN LAYERS

- 네트워크
  - 노드 간 비동기적으로 정보를 교환하는 P2P
  - 효율적인 레이어-0은 높은 트랜잭션 처리량 및 악의적인 행위자에 대한 강한 회복력을 보장

BLOCKCHAIN LAYERS

- FIBRE
  - 블록체인에 트랜잭션을 쓰는(write) 채굴자들
  - 공개(public) 블록체인 P2P 네트워크에 더해, 더 빠르고 효율적인 채굴을 위해 전용의 마이너 네트워크를 사용

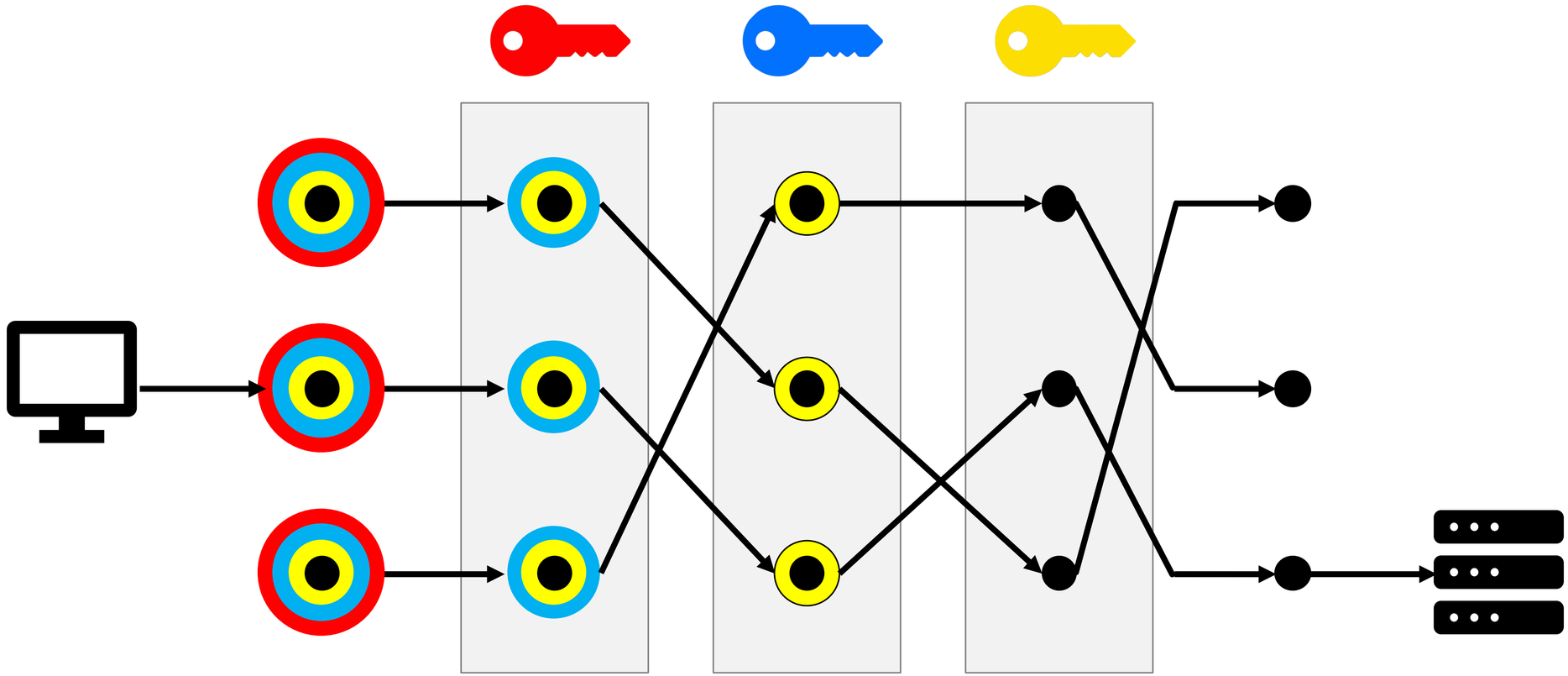
BLOCKCHAIN LAYERS

- 믹스넷(Mix network)
  - 여러 송신자의 메시지를 섞어 무작위 순서로 전송
  - 프록시 서버(proxy server)들의 체인(chain)을 사용
  - 통신의 추적이 어려움

BLOCKCHAIN LAYERS

- 믹스넷
  - 클라이언트와 서버 사이의 연결(link)을 깸
  - 도청자가 엔드-투-엔드(end-to-end) 통신을 추적하기 어려움
  - 대표적 구현체: 토르(Tor)
  - 상위 레이어의 보안성을 근본적으로 향상

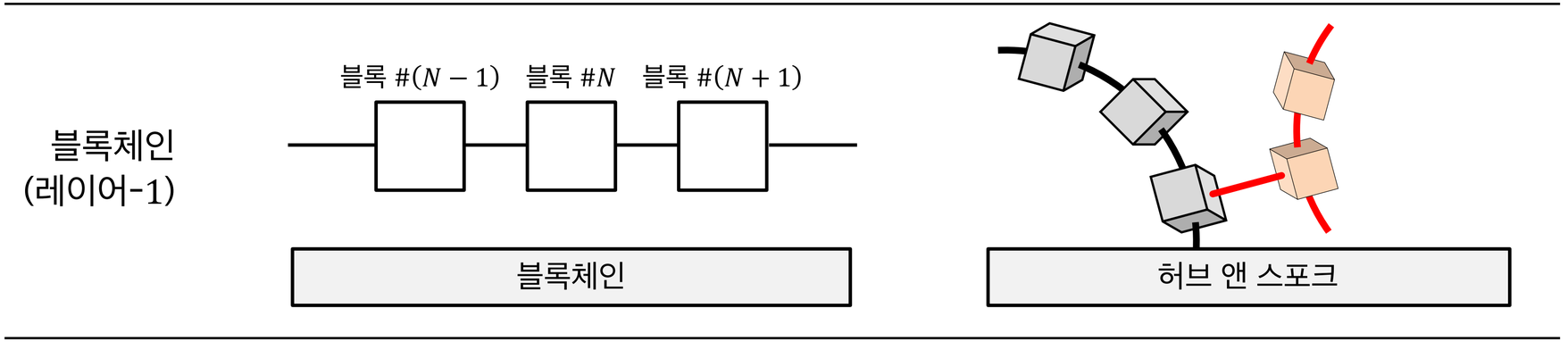
BLOCKCHAIN LAYERS



BLOCKCHAIN

BLOCKCHAIN LAYERS

- 블록체인 계층



BLOCKCHAIN LAYERS

- 불변의 확장만 가능한(append-only) 블록의 체인
- 블록체인의 무결성은 참여자들 간 합의 알고리즘으로부터 보장
- 트랜잭션은 디지털 자산을 교환하거나 응용프로그램을 발발

BLOCKCHAIN LAYERS

- 참여 제한 여부에 따라 구분
  - 무허가형(permissionless)
  - 허가형(permissioned)
- 허가형 블록체인
  - 레이어-1에서는 고려 안 함
  - 레이어-2에서는 고려: 커밋 체인

BLOCKCHAIN LAYERS

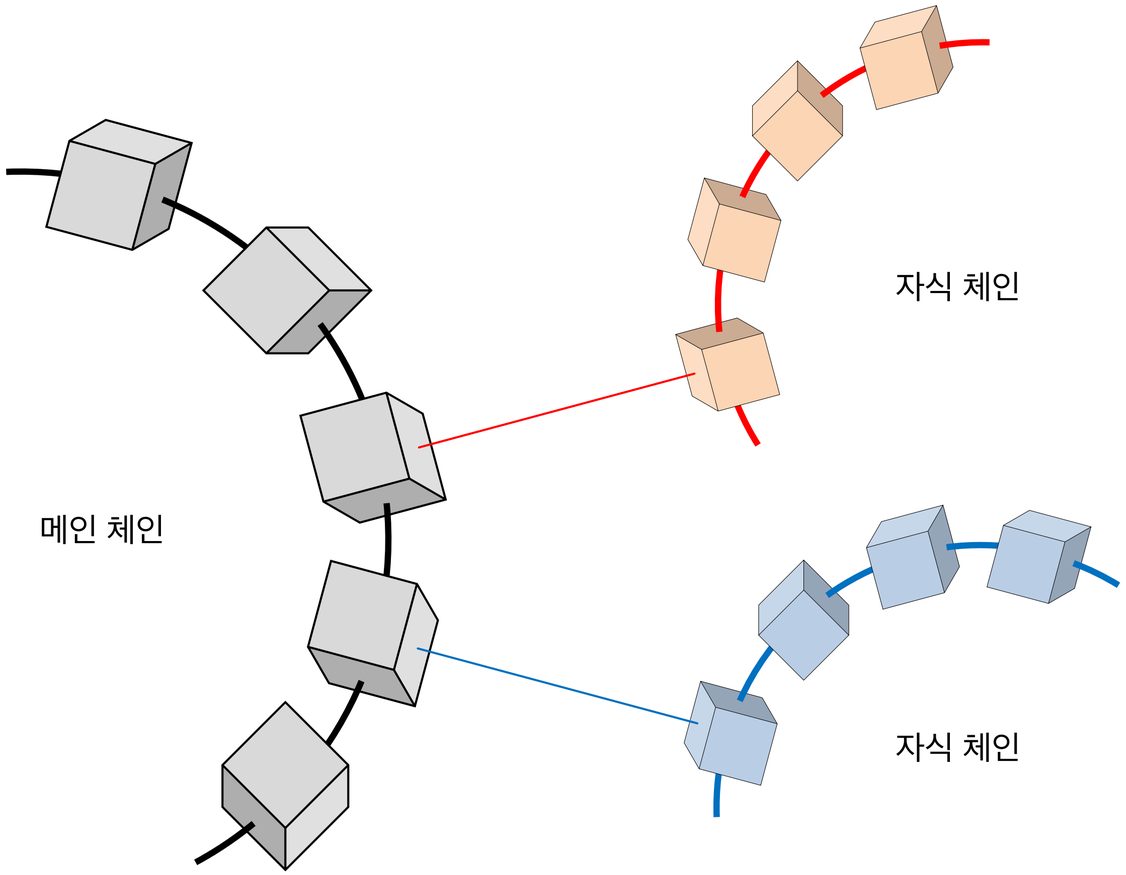
- 프로그래밍 언어
  - 레이어-2 프로토콜 설계에 있어 중요한 요소
  - 스크립팅 언어(scripting language)
  - 튜링 완전 언어
- 기능성 탈출 속도

BLOCKCHAIN LAYERS

- 암호학적 서비스로서의 블록체인
- 레이어-2 프로토콜의 레이어-1에 대한 가정
  - 무결성: 오직 유효한 트랜잭션만 장부에 추가됨
  - 가용성: 유효한 트랜잭션은 임계 시간을 초과하기 전,
    언젠가는 장부에 추가됨

BLOCKCHAIN LAYERS

- 허브 앤 스포크(hub-and-spoke) 구조

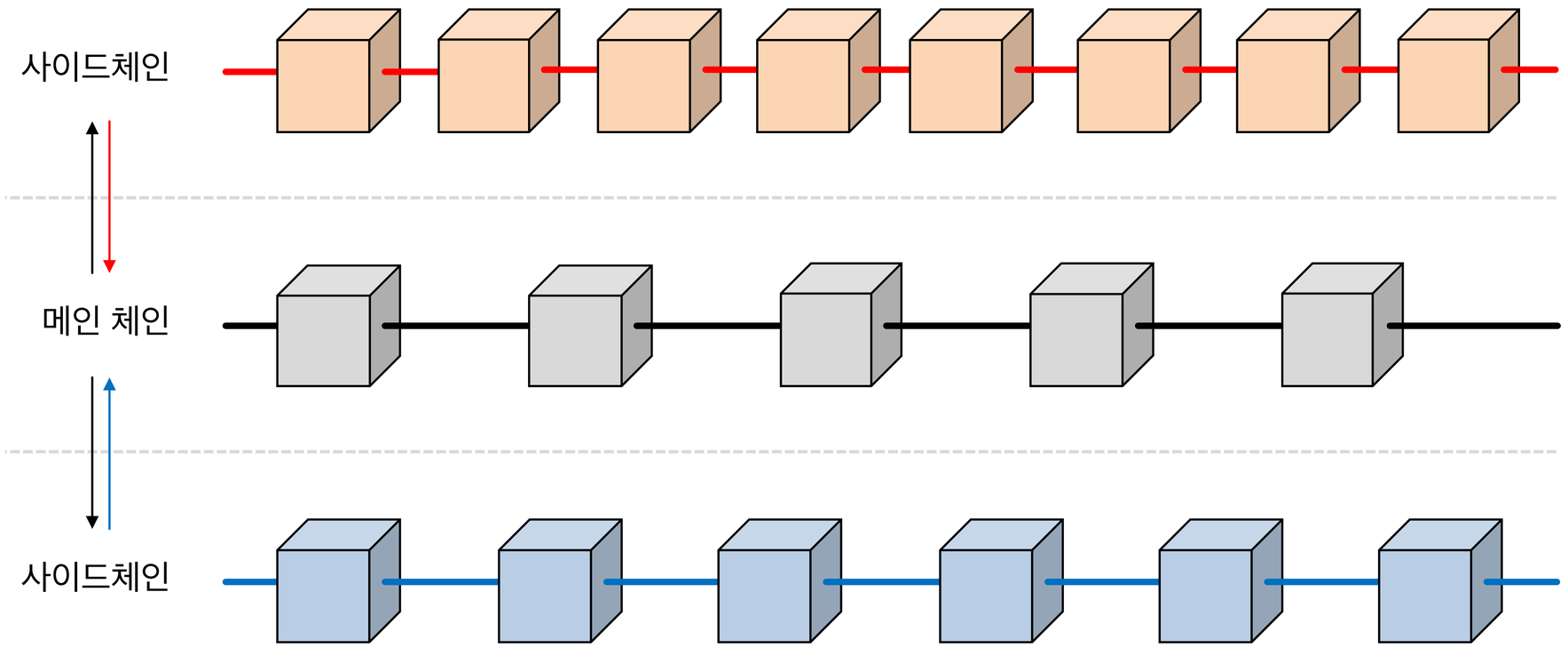


BLOCKCHAIN LAYERS

- 사이드 체인(side-chain)
  - 고유의 합의 알고리즘을 가짐
  - 레이어-2로 분류하지 않음

BLOCKCHAIN LAYERS

- 사이드 체인

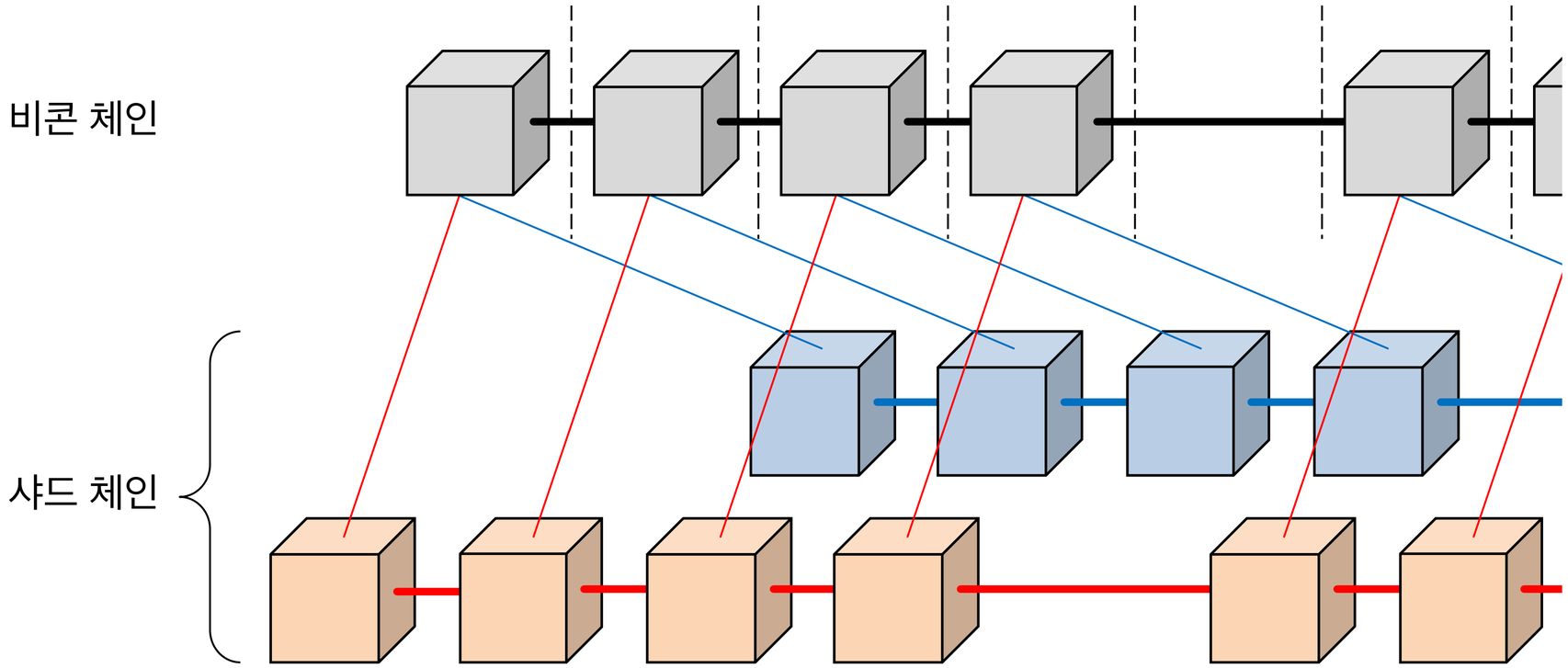


BLOCKCHAIN LAYERS

- 샤딩(sharding)
  - 긴밀한 결합(tight-coupling)
  - 메인 체인의 타당성이 자식 체인의 타당성과 분리될 수 없음
  - 유효하지 않은 메인 체인에 종속적인 자식 체인은 유효하지 않음
  - 유효하지 않은 자식 체인을 포함하는 메인 체인은 유효하지 않음

BLOCKCHAIN LAYERS

- 샤딩

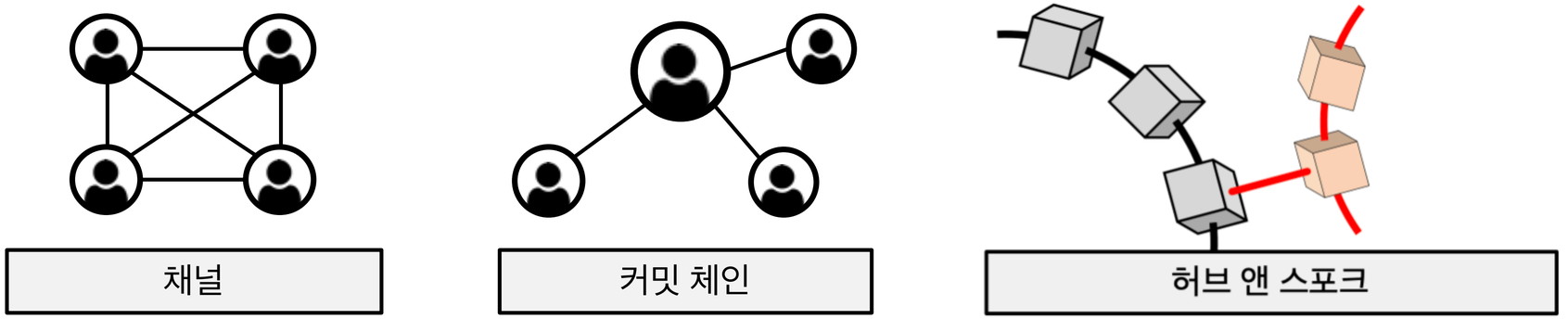


OFF-CHAIN

BLOCKCHAIN LAYERS

- 오프체인 계층

오프체인
(레이어-2)



BLOCKCHAIN LAYERS

- 오프체인 또는 레이어-2 프로토콜
  - 온체인 트랜잭션과는 달리, 모든 트랜잭션을 즉각적으로 블록체인에 공시(publish)하지 않음
  - 부모 체인의 합의 알고리즘에 전적으로 의존

BLOCKCHAIN LAYERS

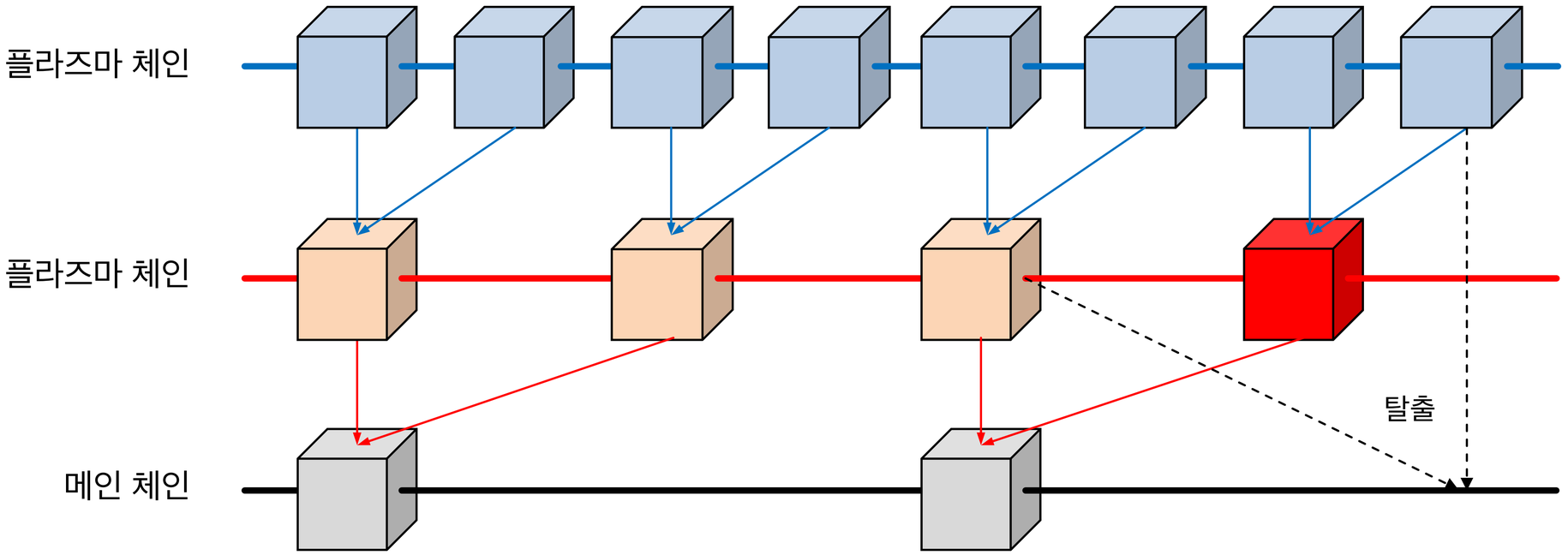
- 오프체인 프로토콜을 크게 두 부류로 구분
  - 채널(channel)은 N명의 동등한 당사자들로 구성
  - 커밋-체인(commit-chain)은 하나의 중앙화된,
    그러나 신뢰할 수 없는 중간자에게 의존

BLOCKCHAIN LAYERS

- 플라즈마(Plasma)
  - 커밋-체인
  - 비구금형(non-custodial) 특성을 가짐
    - 플라즈마 체인에서의 탈출이 가능

BLOCKCHAIN LAYERS

- 플라즈마



SCALABILITY

OVERVIEW: BLOCKCHAIN LAYERS