WHAT IS BLOCKCHAIN

BLOCK AND CHAIN

BLOCKCHAIN

BLOCK

- 블록체인을 구성하는 기본 단위
- 블록 = 블록 헤더 + 블록 바디

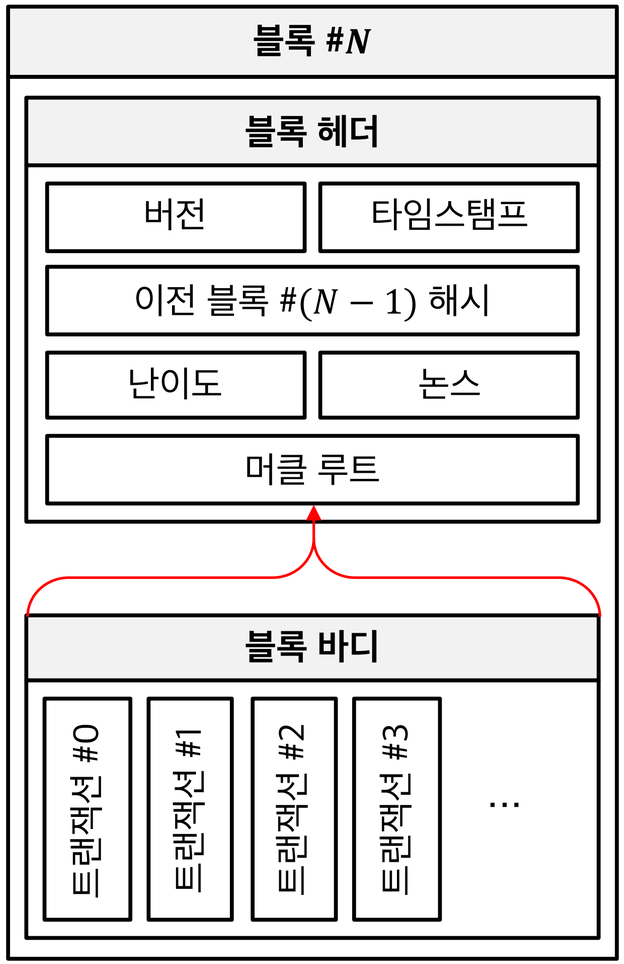
BLOCK

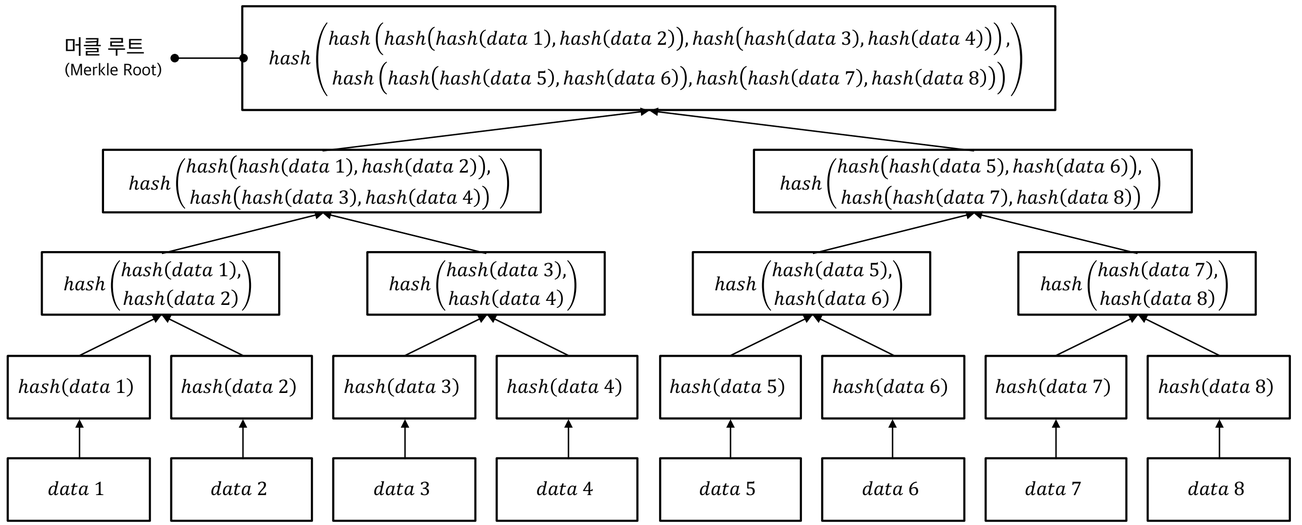
- 헤더(header)
  - 블록 자체의 메타데이터
  - 블록 바디를 대표하는 정보
  - 블록체인의 규칙을 만족하기 위한 정보

BLOCK

- 바디(body)
  - 해당 블록이 포함하는 트랜잭션들의 리스트(list)
  - 머클 트리의 형성 등 트랜잭션이 포함된 순서 정보도 중요
  - 집합(set)이 아닌 리스트로 간주

BLOCK


블록 #N
블록 헤더
버전
타임스탬프
이전 블록 #(N − 1) 해시
난이도
논스
머클 루트
블록 바디
트랜잭션 #0
트랜잭션 #1
트랜잭션 #2
트랜잭션 #3
...


머클 루트
(Merkle Root)
hash(hash(hash(data 1), hash(data 2)), hash(hash(data 3), hash(data 4)))
hash(hash(hash(data 5), hash(data 6)), hash(hash(data 7), hash(data 8)))
hash(hash(data 1), hash(data 2))
hash(hash(data 3), hash(data 4))
hash(hash(data 5), hash(data 6))
hash(hash(data 7), hash(data 8))
hash(data 1)
hash(data 2)
hash(data 3)
hash(data 4)
hash(data 5)
hash(data 6)
hash(data 7)
hash(data 8)
data 1
data 2
data 3
data 4
data 5
data 6
data 7
data 8

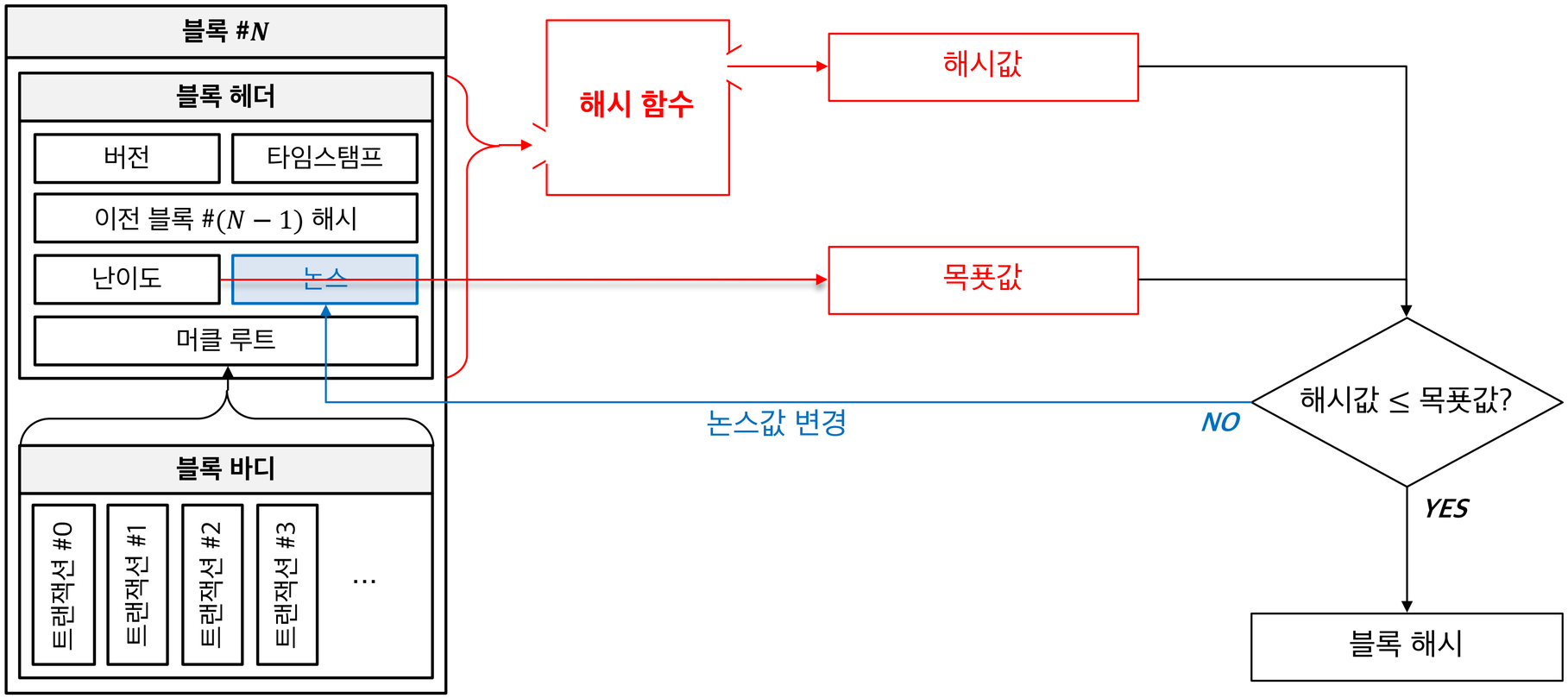
MINING

- 새로운 트랜잭션들의 묶음을 포함한 새 블록을 생성하는 과정
  - 블록 해시는 난이도로부터 구해지는 목푯값보다 작거나 같아야 함
  - 블록 헤더의 다른 항목들은 바꿀 수 없는 상수
  - 논스만이 변수

MINING

- 채굴자는 논스값을 변경해가며 규칙을 만족하는 블록 해시를 찾음
  - 논스를 찾는 과정은 많은 연산을 요구
  - 반면, 블록의 유효성을 검증하기는 쉬움

MINING


블록 #N
블록 헤더
버전
타임스탬프
이전 블록 #(N − 1) 해시
난이도
논스
머클 루트
블록 바디
트랜잭션 #0
트랜잭션 #1
트랜잭션 #2
트랜잭션 #3
...
해시 함수
해시값
목푯값
해시값 ≤ 목푯값?
NO
논스값 변경
YES
블록 해시

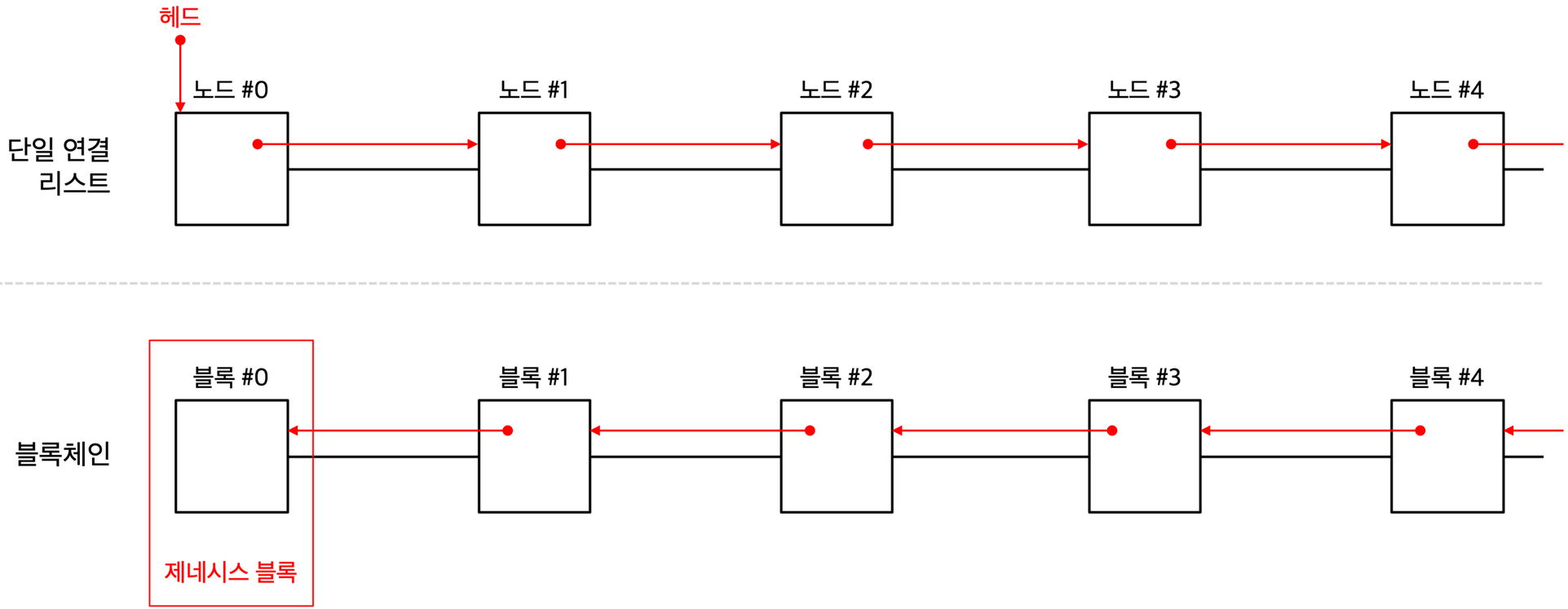
GENESIS BLOCK

- 제네시스 블록(genesis block)
  - 블록체인의 0번째 블록
  - 유일하게 참조하는 이전 블록이 없는 블록
  - 블록체인 클라이언트에 하드코딩돼 있음

BLOCKCHAIN

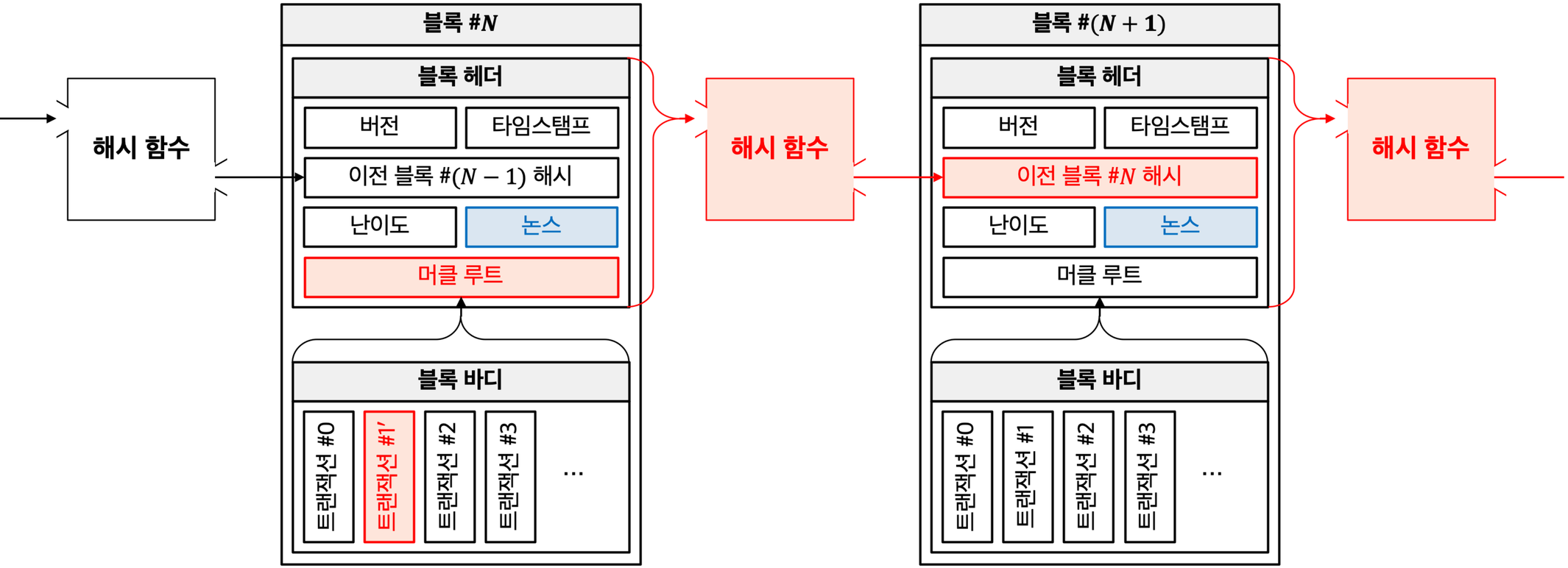
BLOCKCHAIN

- 블록체인은 여러 블록이 체인을 형성하는 구조



SECURITY

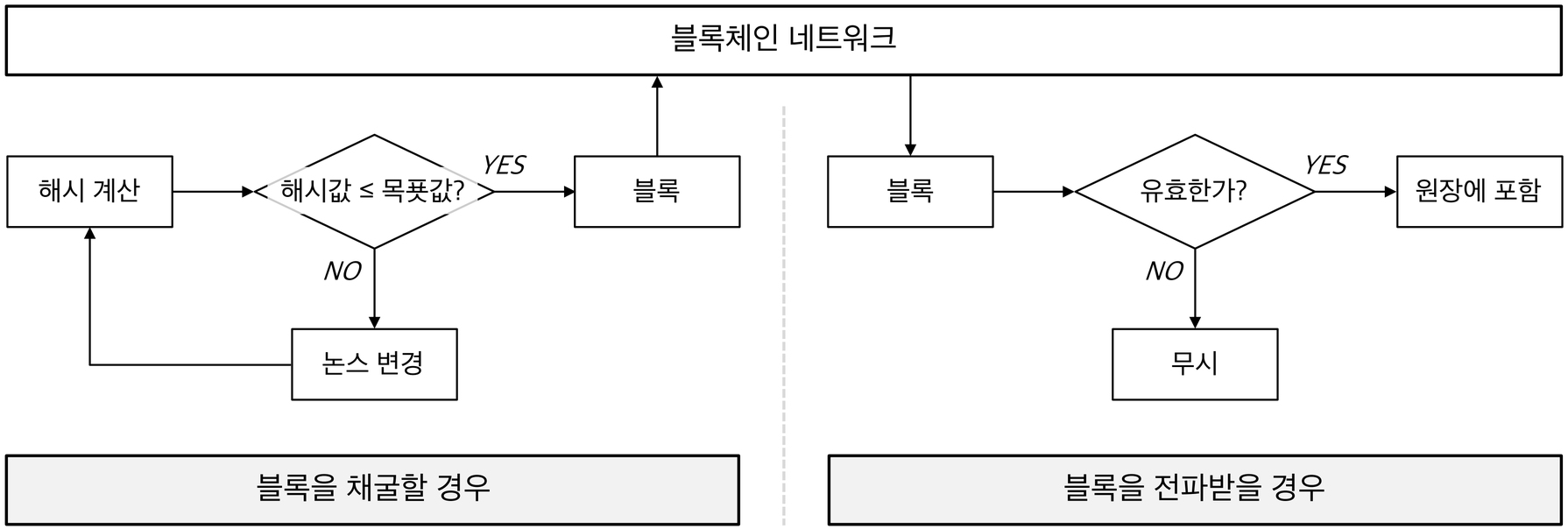
- 최신 블록은 지금까지의 모든 블록을 직/간접 참조
  - 과거 블록의 데이터를 임의로 수정하기는 사실상 불가능



PROOF-OF-WORK

- 블록체인 네트워크의 노드는 각기 블록체인의 복사본을 저장
- 합의 알고리즘(consensus algorithm)
  - 모두가 다음 블록에 합의하고 같은 버전의 원장을 바라보기 위해서 필요
- 작업 증명(Proof-of-Work, PoW)
  - 채굴 과정을 이용해 합의를 이루는 시스템

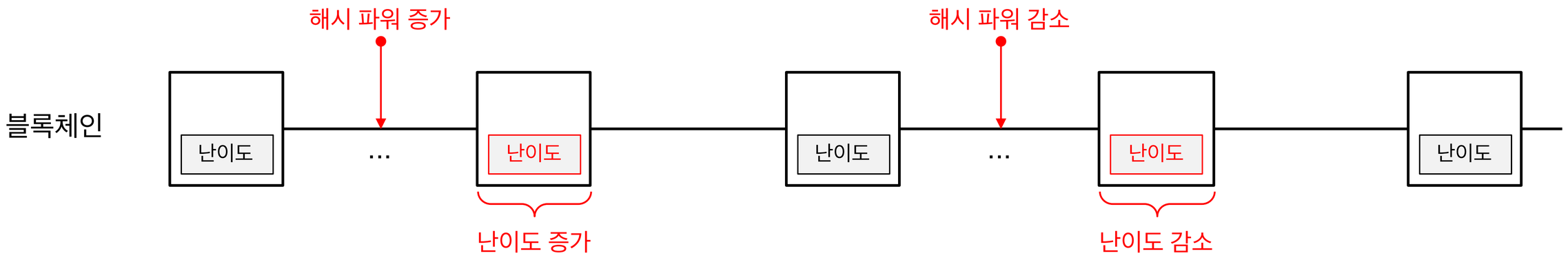
PROOF-OF-WORK



PROOF-OF-WORK

- 작업 증명은 분산 시스템의 무결성을 위한 합의 알고리즘
- 무결성(integrity):
  - 완전성(completeness), 정확성(accuracy), 유효성(validity)
  - **완전성**은 기대한 데이터와 실제의 차이를 나타내는 지표
  - **정확성**은 내포하는 정보가 얼마나 정확한지를 나타냄
  - **유효성**은 데이터가 실제로 활용될 수 있는지 여부를 나타냄
- Boritz, J. "IS Practitioners' Views on Core Concepts of Information Integrity". International Journal of Accounting Information Systems. Elsevier. Archived from the original on 5 October 2011. Retrieved 12 August 2011.

SELF REGULATING SYSTEM



- 블록체인은 블록 생성 간격(interval)을 스스로 조절하는 자가 제한 시스템
- 전체 해시 파워가 변하면 난이도를 조절
  - 평균 블록 생성 간격을 일정하게 유지
- 무분별한 새 블록의 제안을 방지, 과거 블록의 위/변조를 어렵게 함

INCENTIVIZED

REWARD

- 작업 증명 시스템에서 채굴자는 블록을 찾기 위해 경쟁
  - 코인(coin)으로 주어지는 보상(reward)을 받기 위함
  - 보상 = 블록 보상 + 포함된 트랜잭션들의 수수료 보상

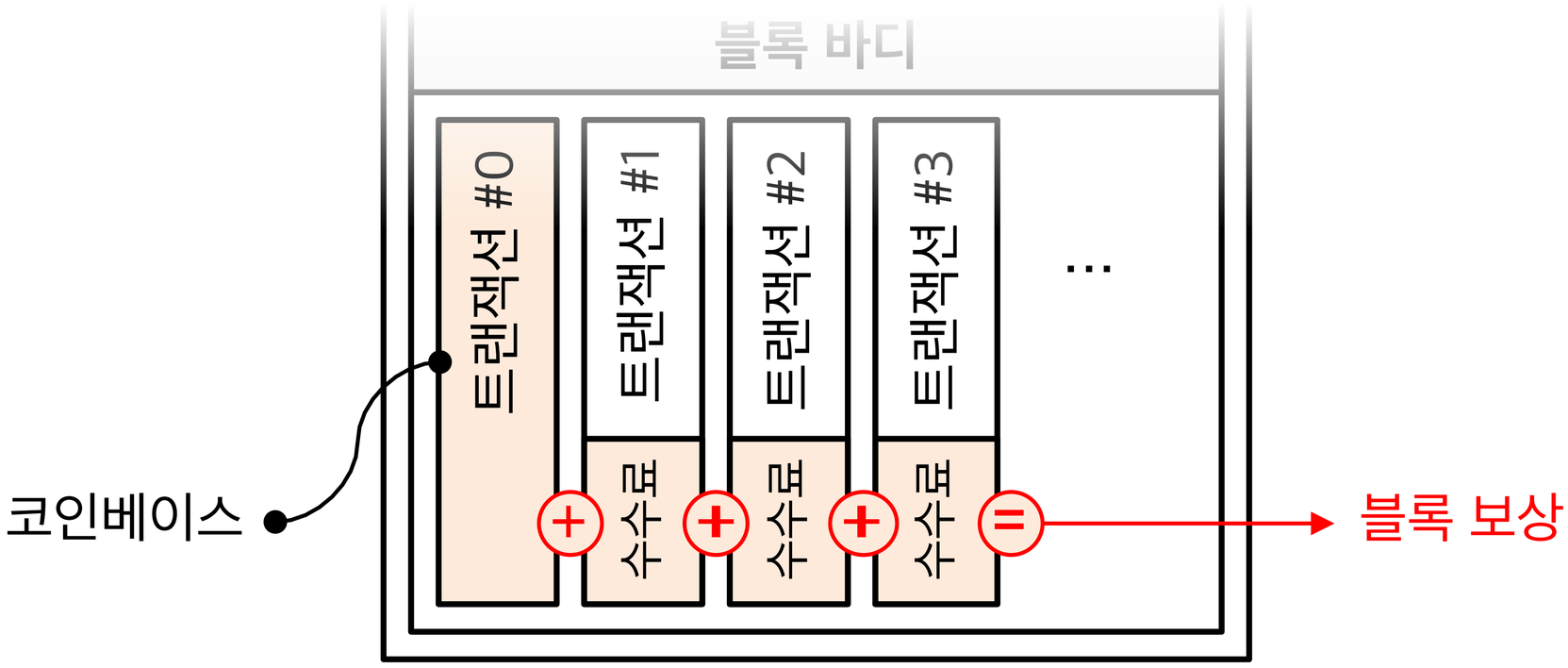
REWARD

- 블록 보상(block reward)
  - 트랜잭션의 형태로 주어짐
  - 블록의 첫 번째 트랜잭션: 코인베이스(coinbase)
  - 채굴자는 블록을 생성하며
    블록 바디의 첫 번째에 코인베이스 트랜잭션을 추가

REWARD

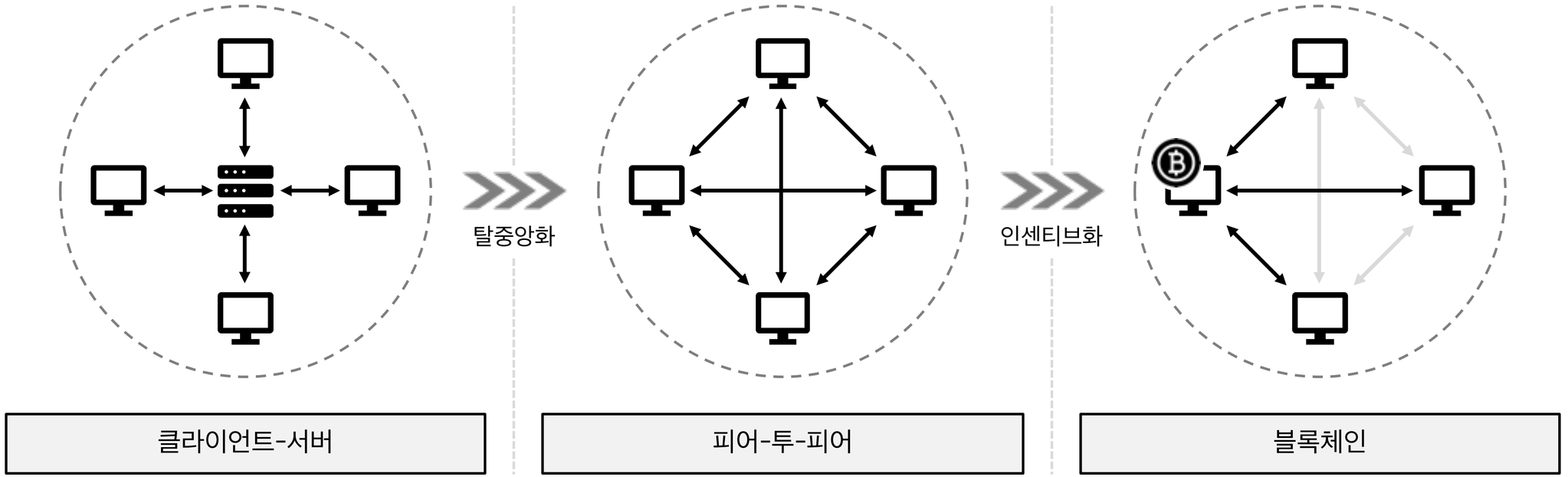
- 수수료 보상(fee reward)
  - 블록 바디에 포함된 트랜잭션들의 수수료의 총합
- 채굴자는 한정된 블록 용량 안에서 최대의 이윤을 창출하고자 함
  - 수수료가 높은 트랜잭션을 우선적으로 블록에 포함
  - 트랜잭션에 높은 수수료를 부여하면 블록에 빨리 채택

REWARD



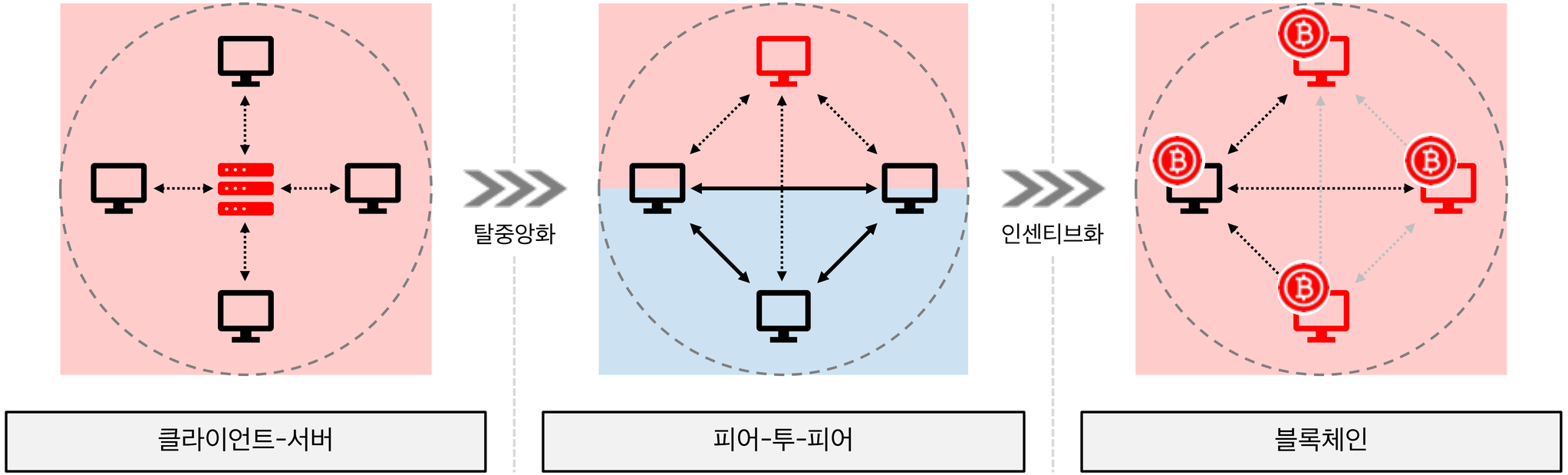
DECENTRALIZED AND INCENTIVIZED

- 블록체인 네트워크: 탈중앙화와 인센티브화



DECENTRALIZED AND INCENTIVIZED

- But, 블록체인이 P2P의 상위호환격 기술은 아님

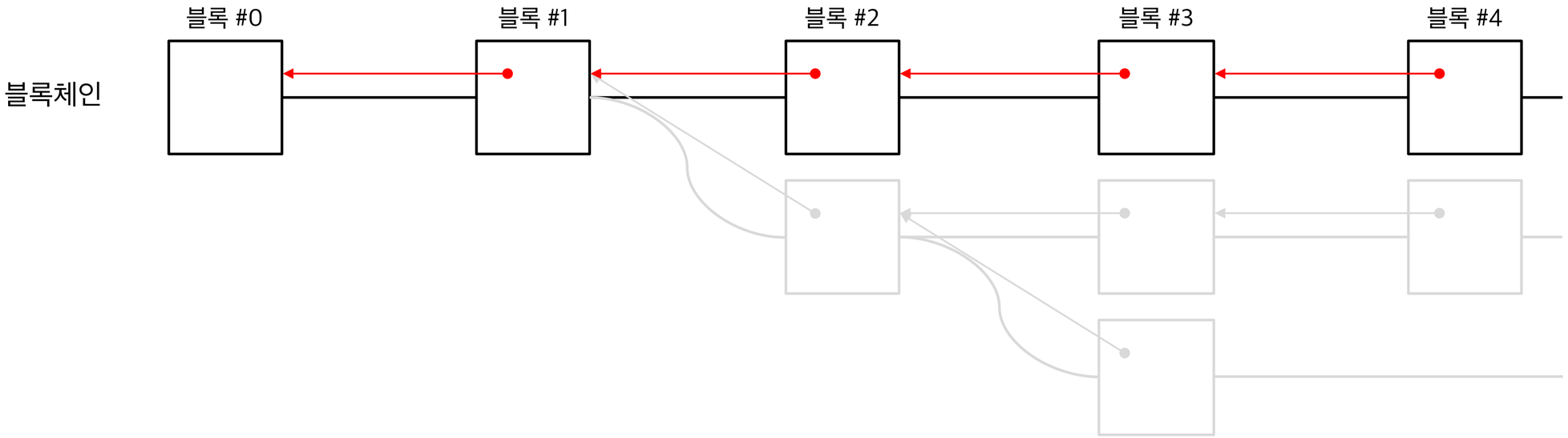


- Mirkin, Michael, et al. "BDoS: Blockchain Denial of Service." arXiv preprint arXiv:1912.07497 (2019).

FORK & FORK

FORK CHOICE RULE

- 분기(fork, 포크)
  - 같은 블록 높이를 가지는 서로 다른 블록이 동시에 존재하는 상황
  - 본질적으로 트리 (사실, Directed Acyclic Graph)

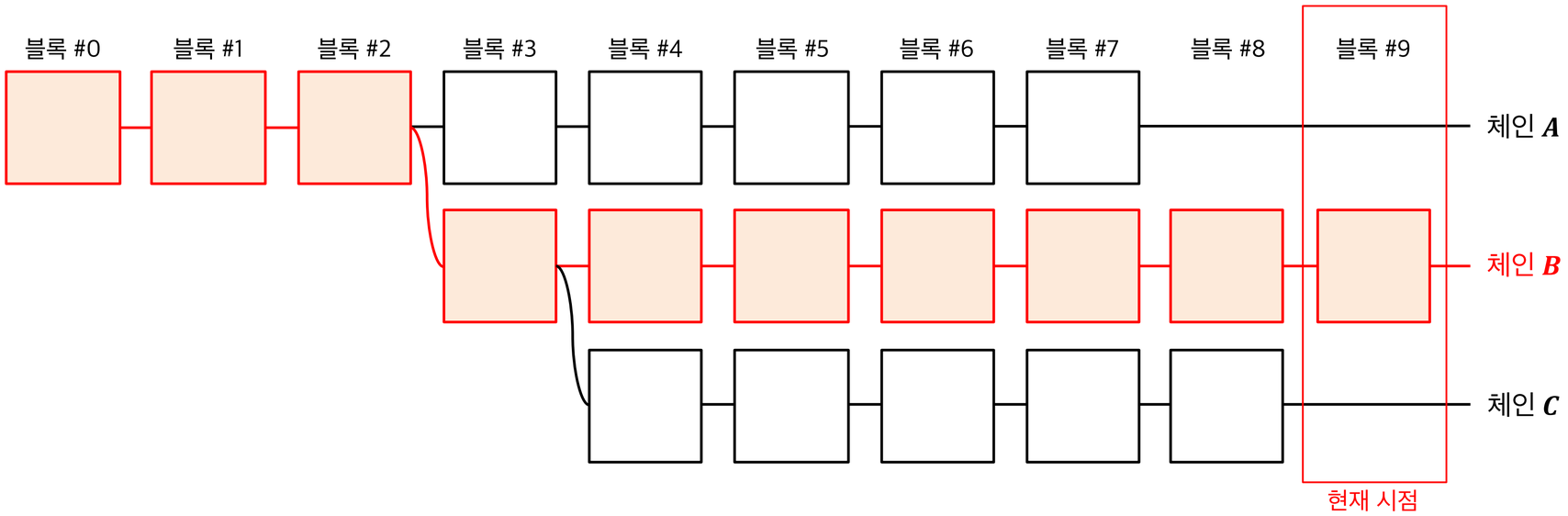


FORK CHOICE RULE

- 분기 선택 규칙(fork choice rule)
  - 여러 원장 중 하나를 선택하는 합의
  - 선택된 체인을 표준 체인(canonical chain)이라 함
  - https://medium.com/@VitalikButerin/minimal-slashing-conditions-20f0b500fc6c

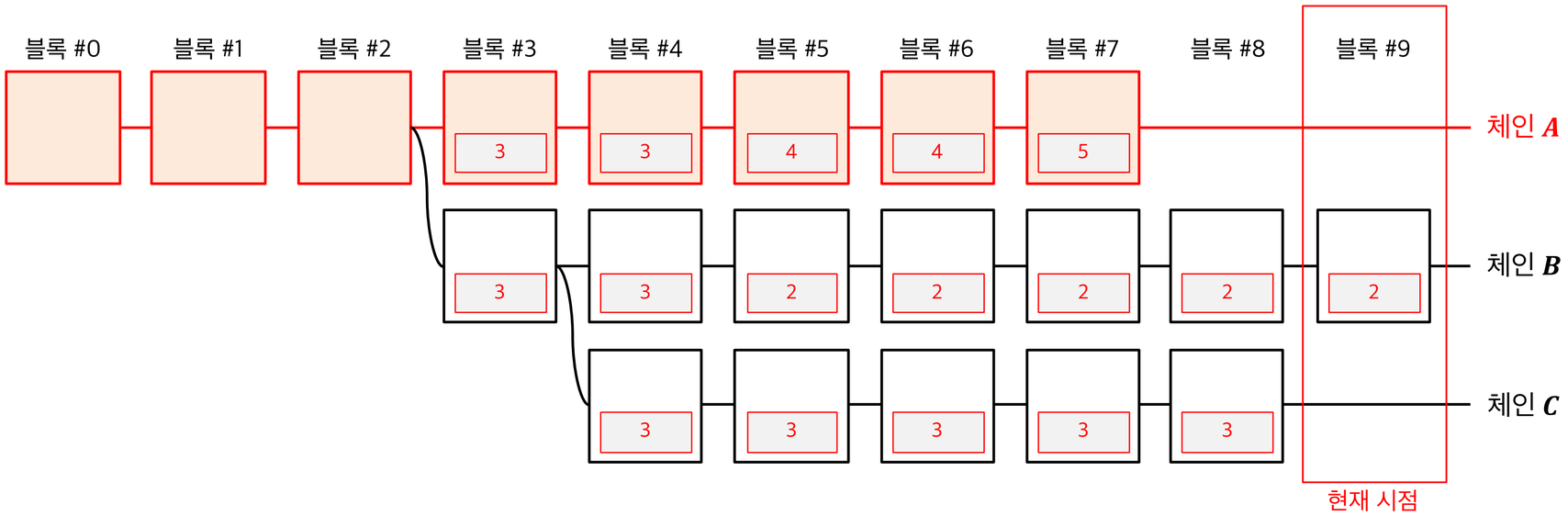
FORK CHOICE RULE

- 가장 긴 체인 규칙(the longest chain rule)



FORK CHOICE RULE

- 가장 무거운 체인 규칙(the heaviest chain rule)



BITCOIN

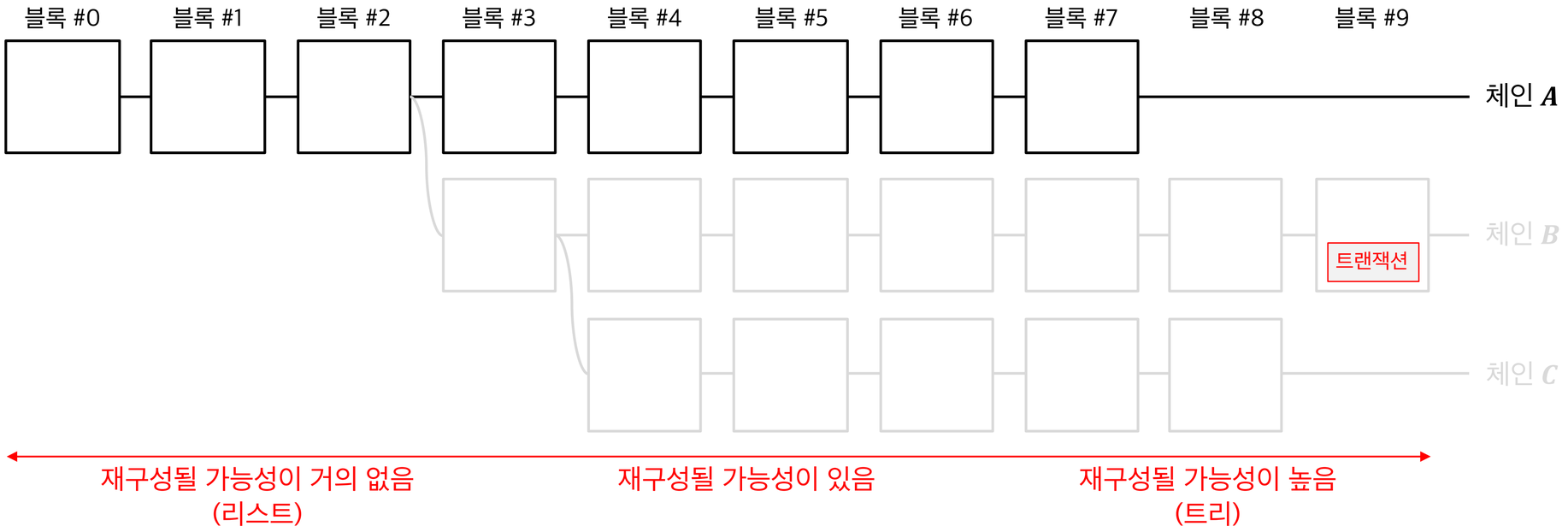
- 2010년 7월 27일자 비트코인 클라이언트 커밋

1216	1235		// New best
1217		–	if (pindexNew->nHeight > nBestHeight)
	1236	+	if (pindexNew->bnChainWork > bnBestChainWork)

- https://github.com/bitcoin/bitcoin/commit/40cd0369419323f8d7385950e20342e998c994e1#diff-118fcbaaba162ba17933c7893247df3aL1216

REORGANIZATION

- 블록체인 재구성(reorganization, reorg)
- 선택되지 않은 다른 브랜치들의 합의됐던 트랜잭션이 다시 미합의 상태가 됨



SOFT FORK & HARD FORK

- 소스코드를 복사해 새로운 소프트웨어를 개발하는 것을 의미
  - 개선된 혹은 새로운 프로토콜을 적용하기 위한 업데이트

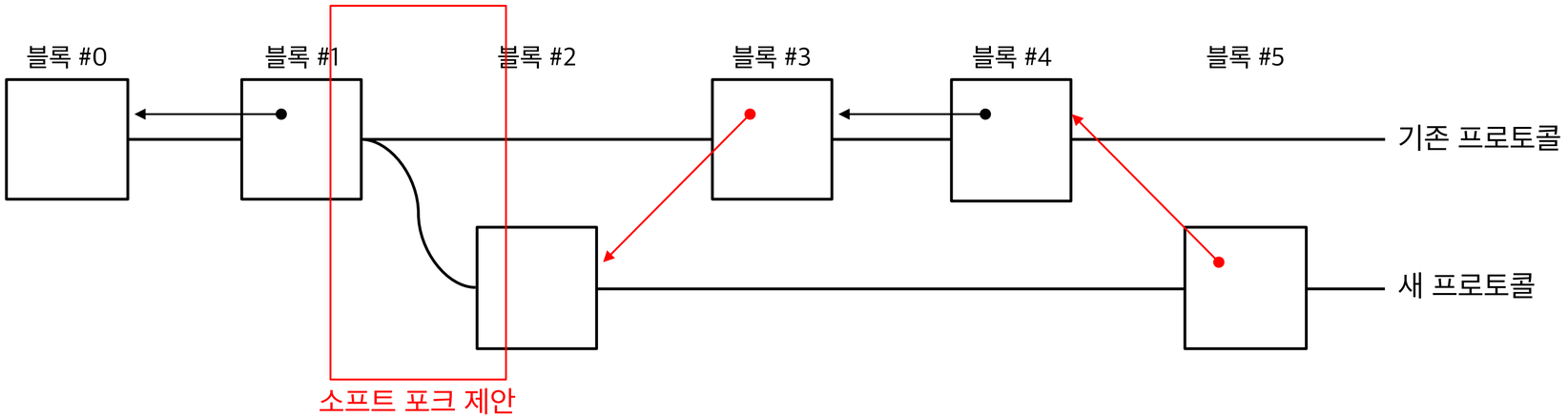
SOFT FORK & HARD FORK

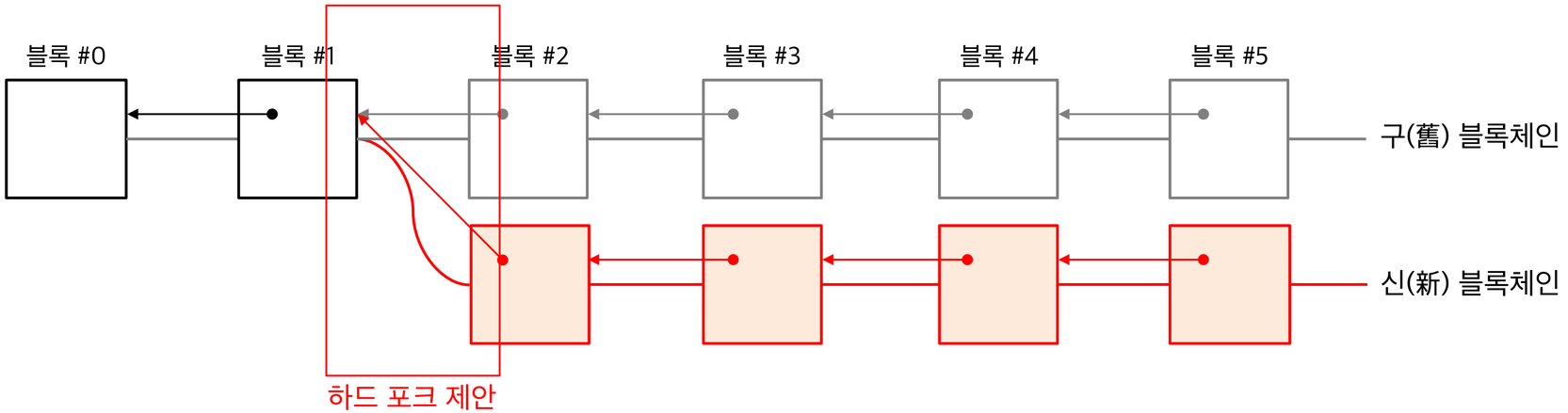
- 소프트 포크(soft fork)
  - 하위 호환성을 제공하는 프로토콜 업데이트
  - 참여자들의 소프트 포크 적용 여부는 선택사항
  - 개선을 온전히 누리고자 한다면 업데이트를 수용

SOFT FORK & HARD FORK

- 하드 포크(hard fork)
  - 하위 호환성을 제공하지 않는 프로토콜 업데이트
  - 업데이트를 수용하지 않은 참여자는 트랜잭션 혹은 블록을 처리할 수 없음
  - 통상 프로토콜의 대대적인 변화 또는 롤백 상황에서 제시
  - 성공적인 하드 포크는 모든 참여 노드의 업데이트를 요구

SOFT FORK & HARD FORK





WHAT IS BLOCKCHAIN

BLOCK AND CHAIN