Blockchain #5

Bitcoin - 1

Prof. Byung Il Kwak

Review

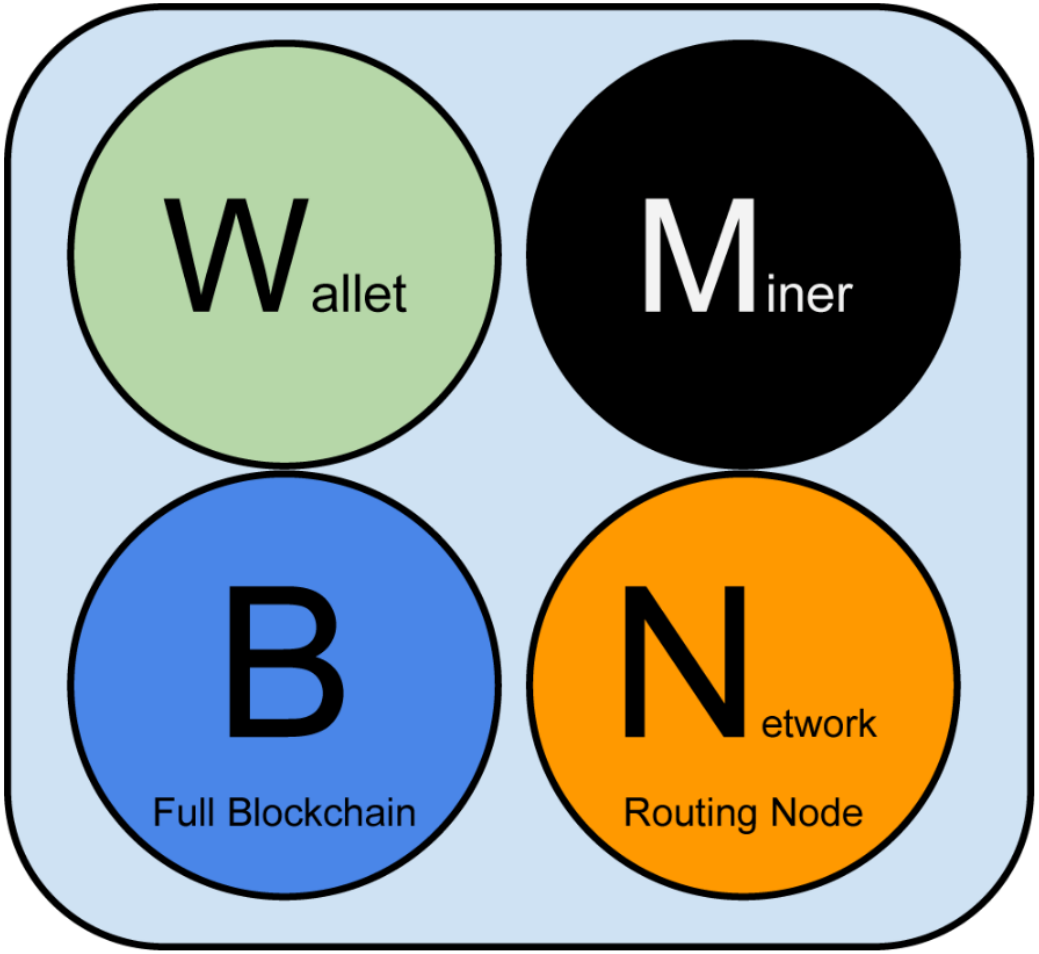
- The history of bitcoin
- Bank and blockchain
- Blockchain's present and future

CONTENTS

- Bitcoin’s nodes

Bitcoin's nodes

Bitcoin's address
Bitcoin transfer



PoW worker

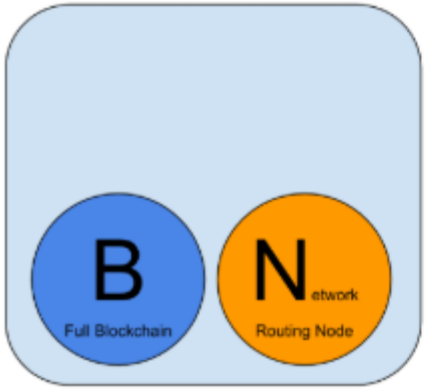
Blockchain's transactions

P2P networks

A bitcoin network node with all four functions

Bitcoin's nodes

- Full Blockchain Node
  - 블록체인 데이터 전체를 관리하는 노드
    - 2009년 1월 3일부터 현재까지 발생한 모든 거래 내역(트랜잭션)들이 보관되어 있음
  - 풀 블록체인 노드가 최근 트랜잭션이 담긴 새로운 블록을 받으면, 합의 알고리즘에 따라 유효성 검증 후 기존 블록체인에 연결하고, 다른 노드들에게 전파함

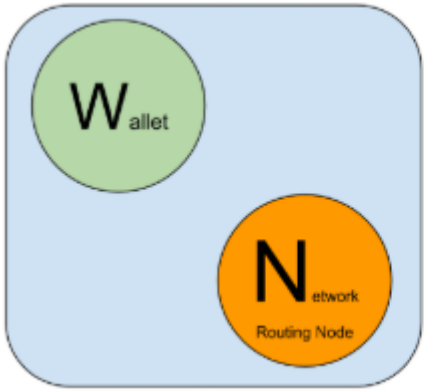


Full Block Chain Node

Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.

Bitcoin's nodes

- Lightweight (SPV) wallet
  - Simplified Payment Verification (SPV) 노드라고 불리며, 블록체인 전체가 아닌 블록의 헤더 정보만 가지고 있음
    - 새로운 블록이 생성되면, Full Blockchain Node로부터 블록 헤더를 받아 자신의 헤더 체인에 연결함 (공간 절약)
    - SPV는 주로 스마트 기기 등 소형 장비에 적합함 (송금과 같은 기능만 필요)
    - 지갑 애플리케이션으로 트랜잭션의 유효성을 검증함

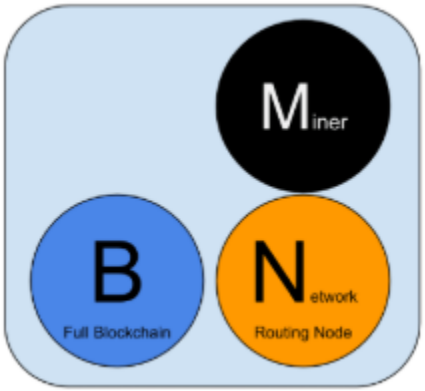


Lightweight (SPV) wallet

Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.

Bitcoin's nodes

- Solo Miner
  - 블록체인 네트워크를 유지하는데 필수적인 구성원으로, 채굴자들은 경쟁적으로 수학적 퍼즐을 풀고 블록 헤더에 그 해답을 제시함
    - 먼저 해답을 제시한 채굴자의 블록이 Full Blockchain Node로 전송되며, 이 해답에 대한 유효성 검증이 끝나면, 그 대가로 보상을 받음

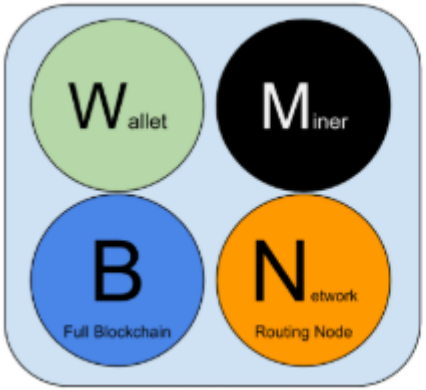


Solo Miner

Contains a mining function with a full copy of the blockchain and a bitcoin P2P network routing node.

Bitcoin's nodes

- Reference Client (Bitcoin Core)
  - 모든 기능을 다 활용하는 노드로써 Wallet, Miner, Full Blockchain, Network 4개가 모두 포함된 노드를 가리킴



Reference Client (Bitcoin Core)

Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.

Bitcoin's nodes

- Pool Protocol Server
  - Pool Protocol Server는 다른 프로토콜을 실행하는 노드를 연결시키는 역할을 수행함 (채굴, 블록체인, wallet 연결)

Pool Protocol Servers

Gateway routers connecting the bitcoin P2P network to nodes running other protocols such as pool mining nodes or Stratum nodes.

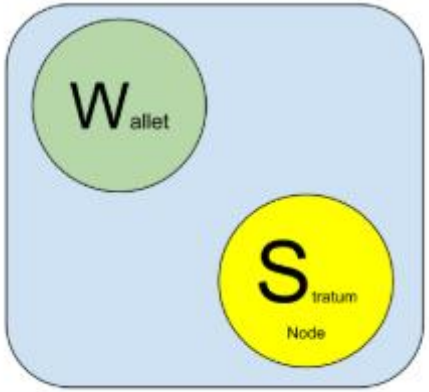
- Mining Nodes
  - 블록체인 없이 채굴만 담당
    - Pool과 연결하여 채굴할 경우, 채굴만 담당
    - Stratum Protocol 가지고 연결할 경우, Network 기능이 있는 노드와 먼저 연결 후 Pool에 접근하여 채굴 수행

Mining Nodes

Contain a mining function, without a blockchain, with the Stratum protocol node (S) or other pool (P) mining protocol node.

Bitcoin's nodes

- Lightweight (SPV) Stratum wallet
  - Stratum 프로토콜을 이용하여 Network 기능이 있는 노드와 연결하고 이웃 노드에게 트랜잭션을 전달함



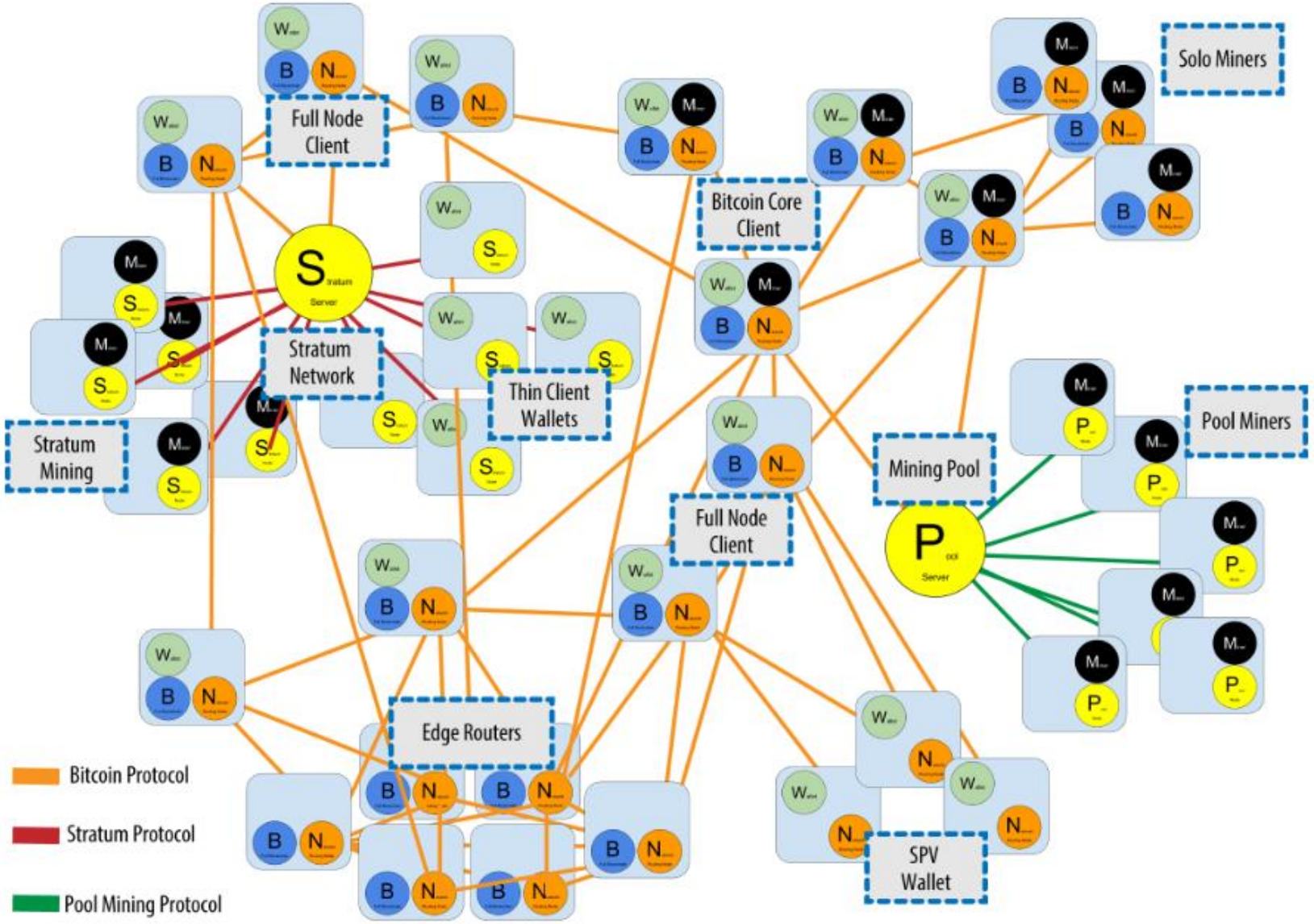
Lightweight (SPV) Stratum wallet

Contains a Wallet and a Network node on the Stratum protocol, without a blockchain.

** "Bitcoin network"라는 용어는 **Bitcoin P2P protocol**을 실행하는 노드들의 모음을 나타냄

** Bitcoin P2P protocol 외에도 **마이닝 및 경량 또는 모바일 지갑에 사용되는 Stratum** 과 같은 다양한 프로토콜들이 있음

Bitcoin's nodes



Bitcoin's nodes

- https://bitnodes.io/

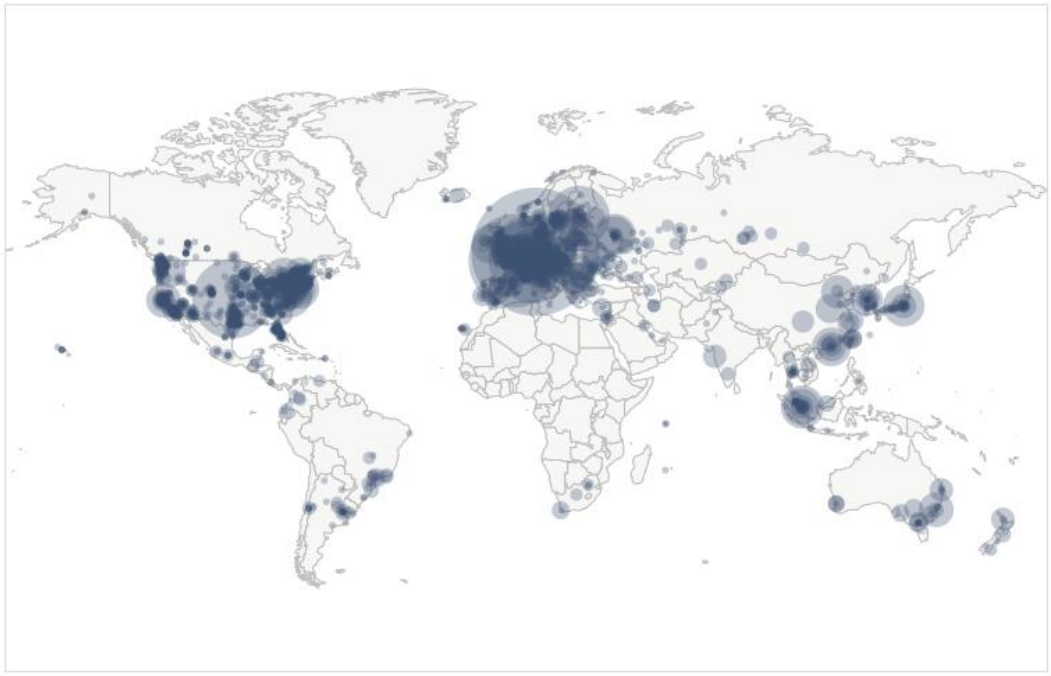
GLOBAL BITCOIN NODES DISTRIBUTION
Reachable nodes as of Mon Aug 30 18:19:34 2021 KST.

10490 NODES [24h] [90d] [1y]

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	2978 (28.39%)
2	United States	1863 (17.76%)
3	Germany	1797 (17.13%)
4	France	548 (5.22%)
5	Netherlands	399 (3.80%)
6	Canada	303 (2.89%)
7	United Kingdom	257 (2.45%)
8	Russian Federation	193 (1.84%)
9	Finland	182 (1.73%)
10	Switzerland	143 (1.36%)

More (87) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

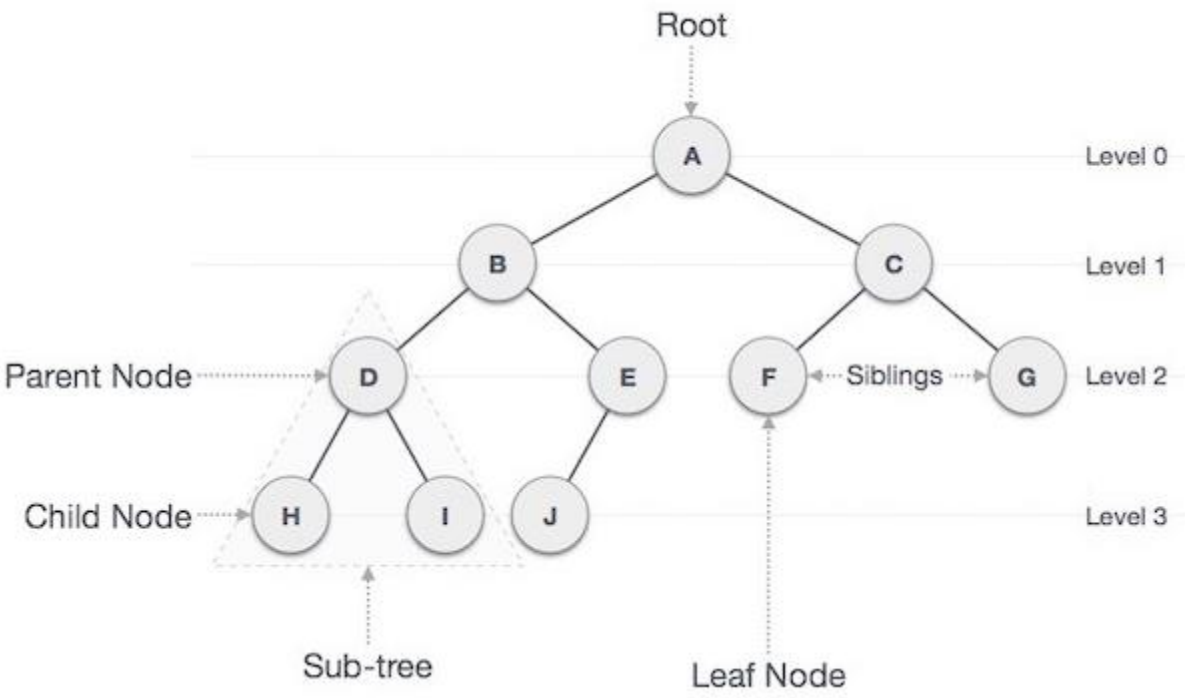
LIVE MAP

What is the important node in Bitcoin?

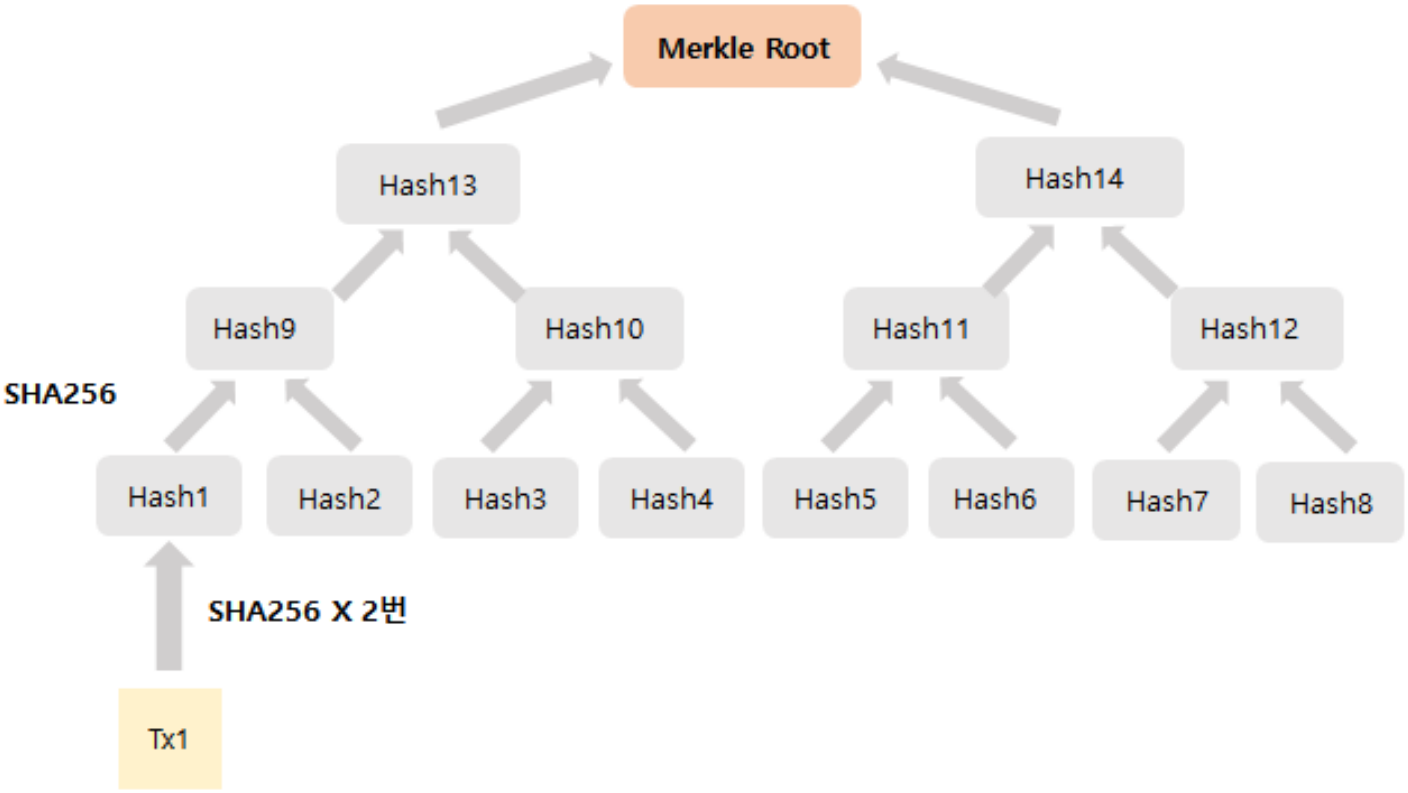
CONTENTS

- Merkel tree

Tree structure



Merkle tree



[Source: https://brunch.co.kr/@skkrypto/1]

Merkle tree

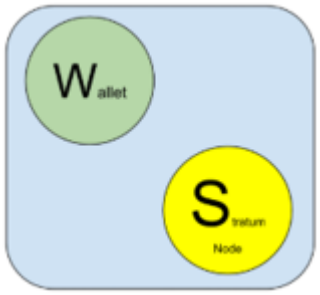
- 블록 내에서 다수의 트랜잭션들을 암호화하고 합치는 과정을 반복하여 한 개의 유닛으로 암호화하는 방식
  - 즉, 여러 거래들을 이진 트리의 형태로 반복 해시 과정을 통해 암호화하여, 한 개의 머클 루트 (Merkle Root)를 만드는 방식

Merkle tree

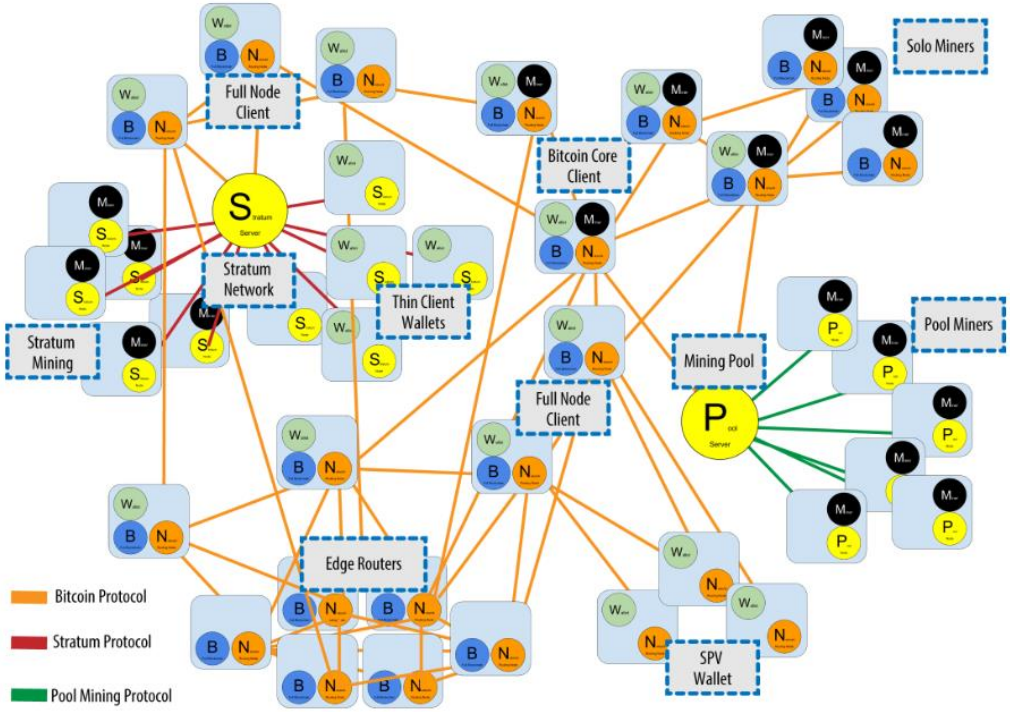
- Why Merkle tree?

Full nodes

Verification of transactions

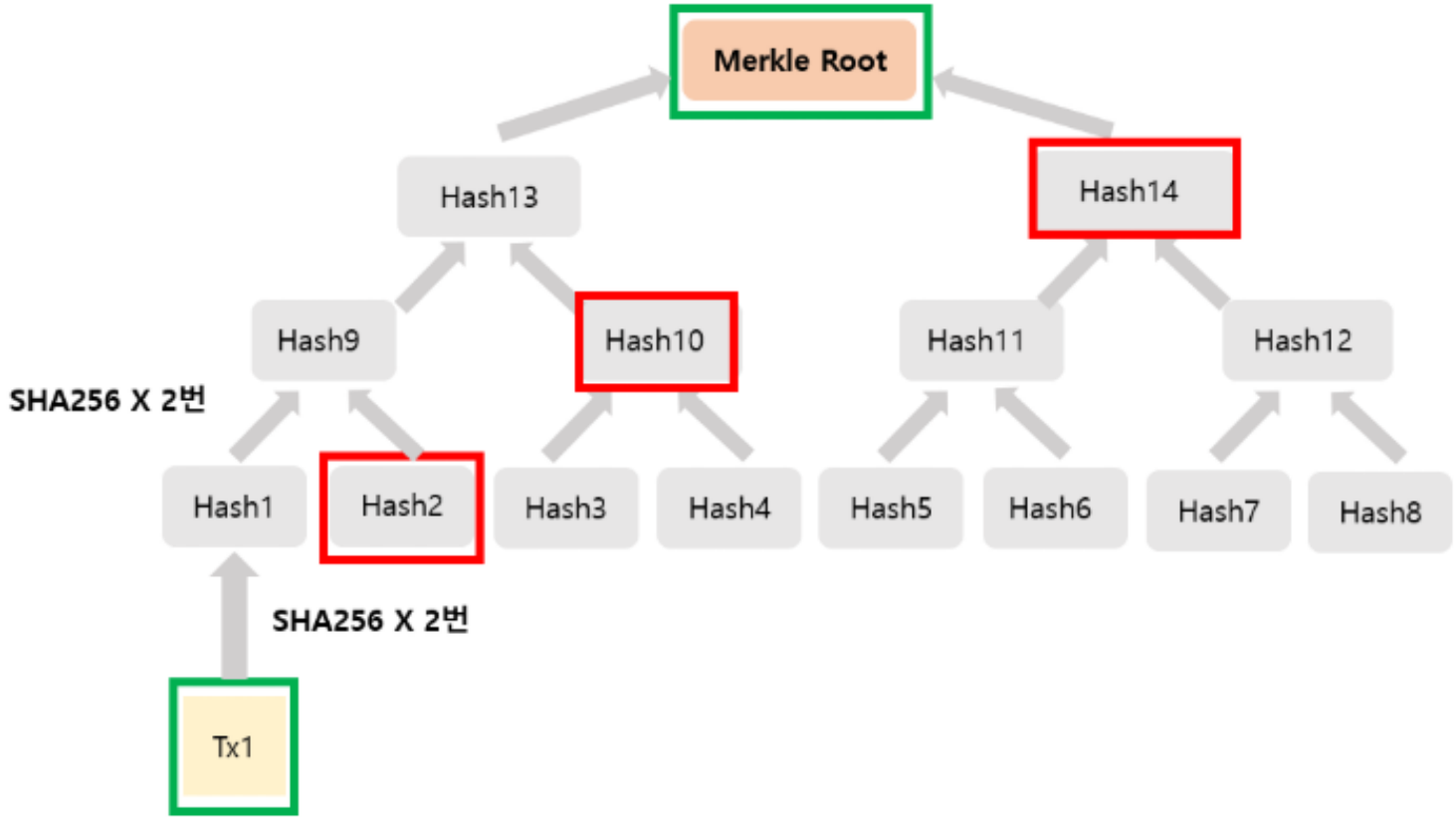


Lightweight nodes



Merkle tree

- 머클 트리에서 거래를 찾는 방식



[Source: https://brunch.co.kr/@skkrypto/1]

Merkle tree

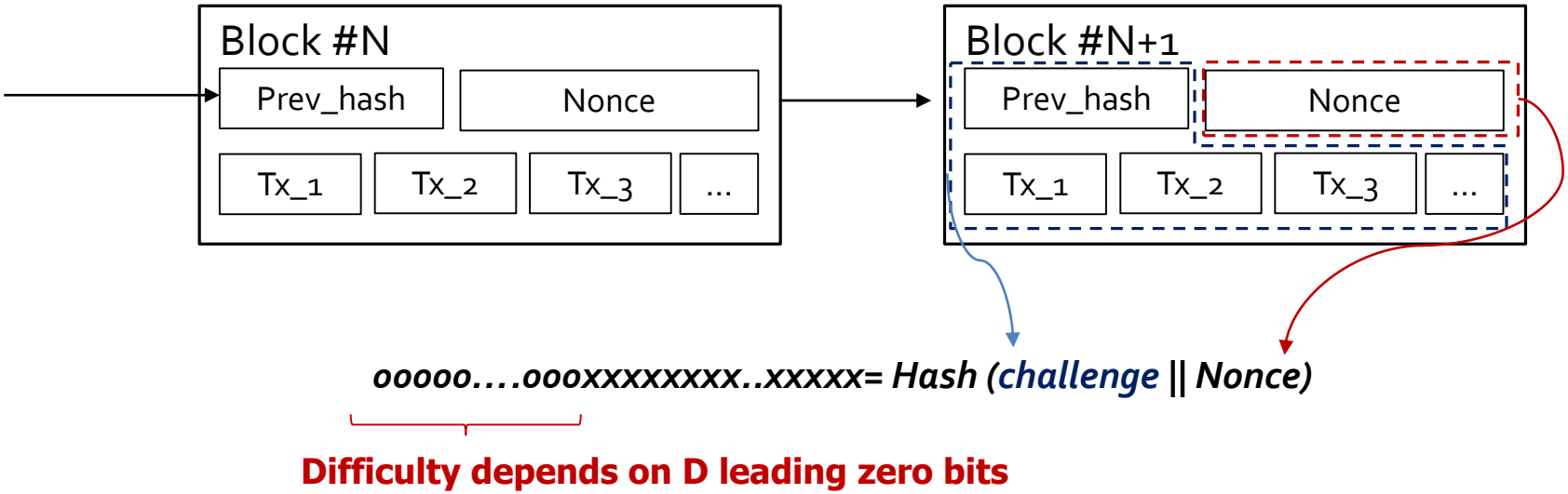
- 특정 거래가 해당 블록에 존재하는지 검색할 경우
  - 검색의 수가 N 개 증가 할 때마다, 선형적으로 증가하는 것이 아닌 $log_2(N)$ 만큼만 검색하면 확인이 가능
  - 특정 거래에 대한 위변조 가능성과, 빠른 탐색을 용이하게 해줌 (어떠한 거래가 들어있는지를 확인)

CONTENTS

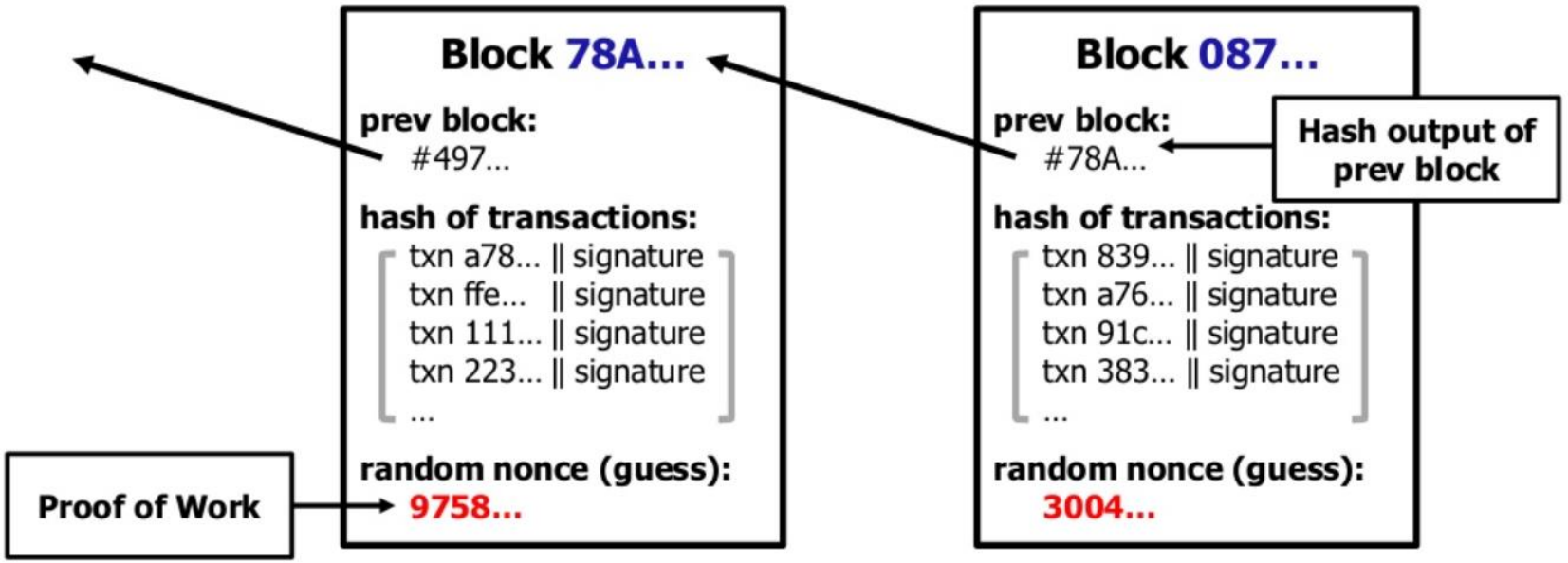
- PoW (Proof-of-Work)

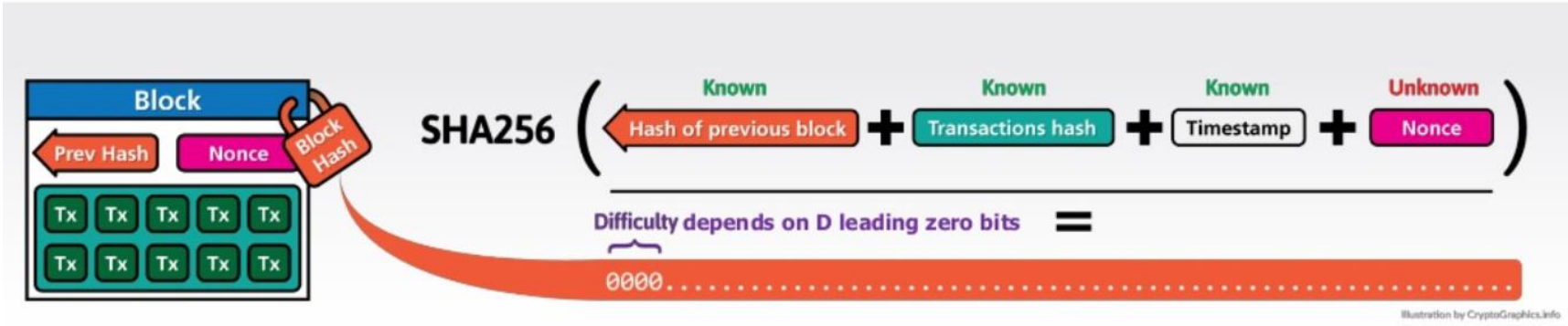
Proof-of-Work

- Hash 기반의 Proof-of-Work (PoW)
  - 채굴자 노드가 수행하는 문제
    - 랜덤한 값을 변화시키면서 D개의 0으로 시작하는 해시값을 찾는 행위
    - D의 수가 1씩 증가할 수록, 문제의 난이도는 2배가 됨



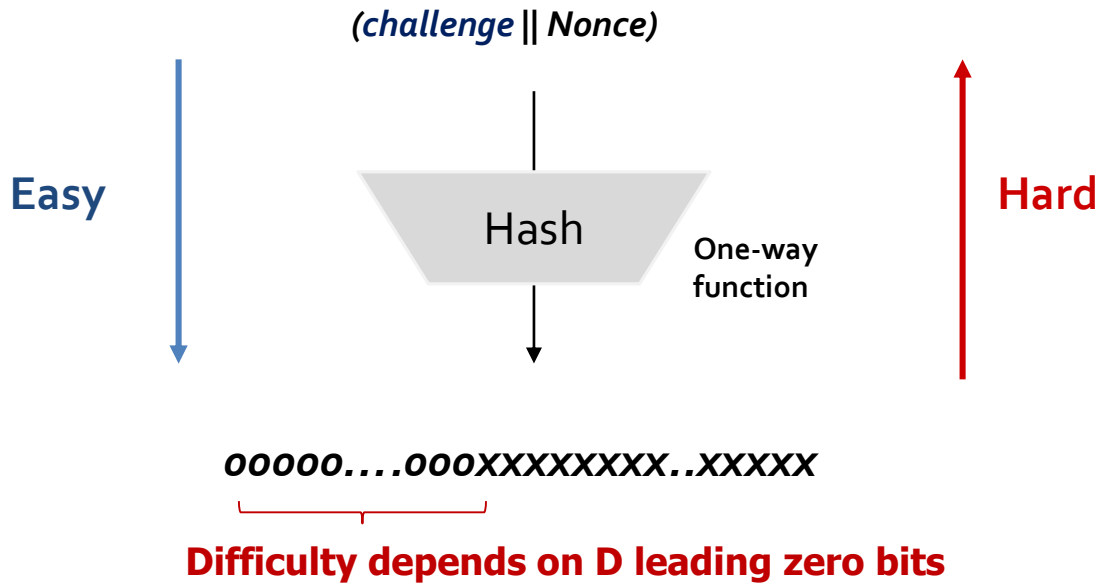
Proof-of-Work





Proof-of-Work

- 암호화 해시 (Cryptographic hash)
  - 암호화 해시 함수에서 출력 값 'Y'가 주어지면 Y=H(X)가 되는 해당 입력 값 'X'를 찾기가 어려움

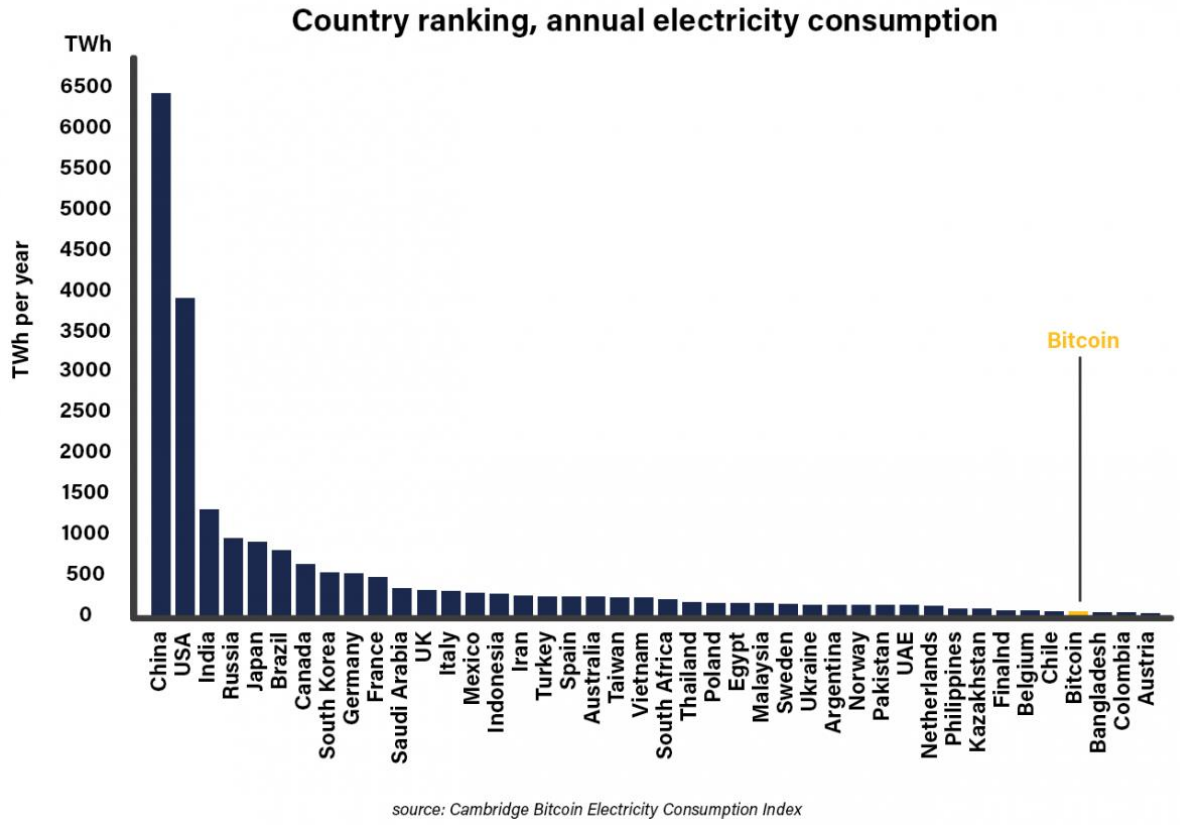


Proof-of-Work

- PoW의 문제
  - 전력 소비
    - 채굴 기계들은 해시 함수 기반의 PoW 알고리즘을 수행하기 위해서 과도한 전력을 소모함

Proof-of-Work

- PoW의 문제
  - 전력 소비
    - 채굴 기계들은 해시 함수 기반의 PoW 알고리즘을 수행하기 위해서 과도한 전력을 소모함



Proof-of-Work

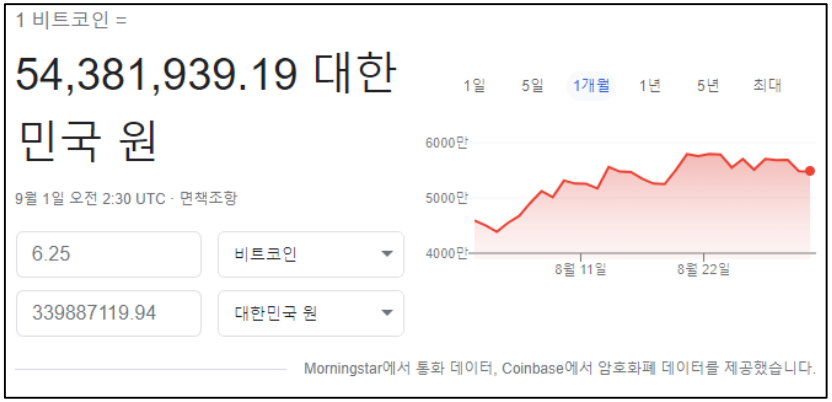
- PoW의 문제

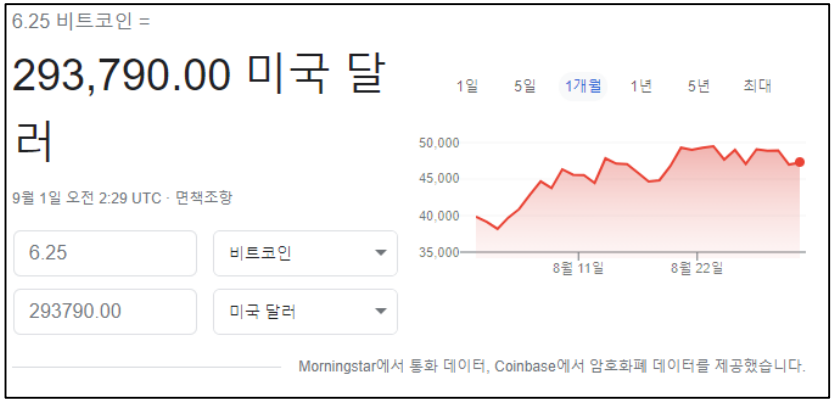
출처 : 코인데스크 & 디지코노미스트

Proof-of-Work

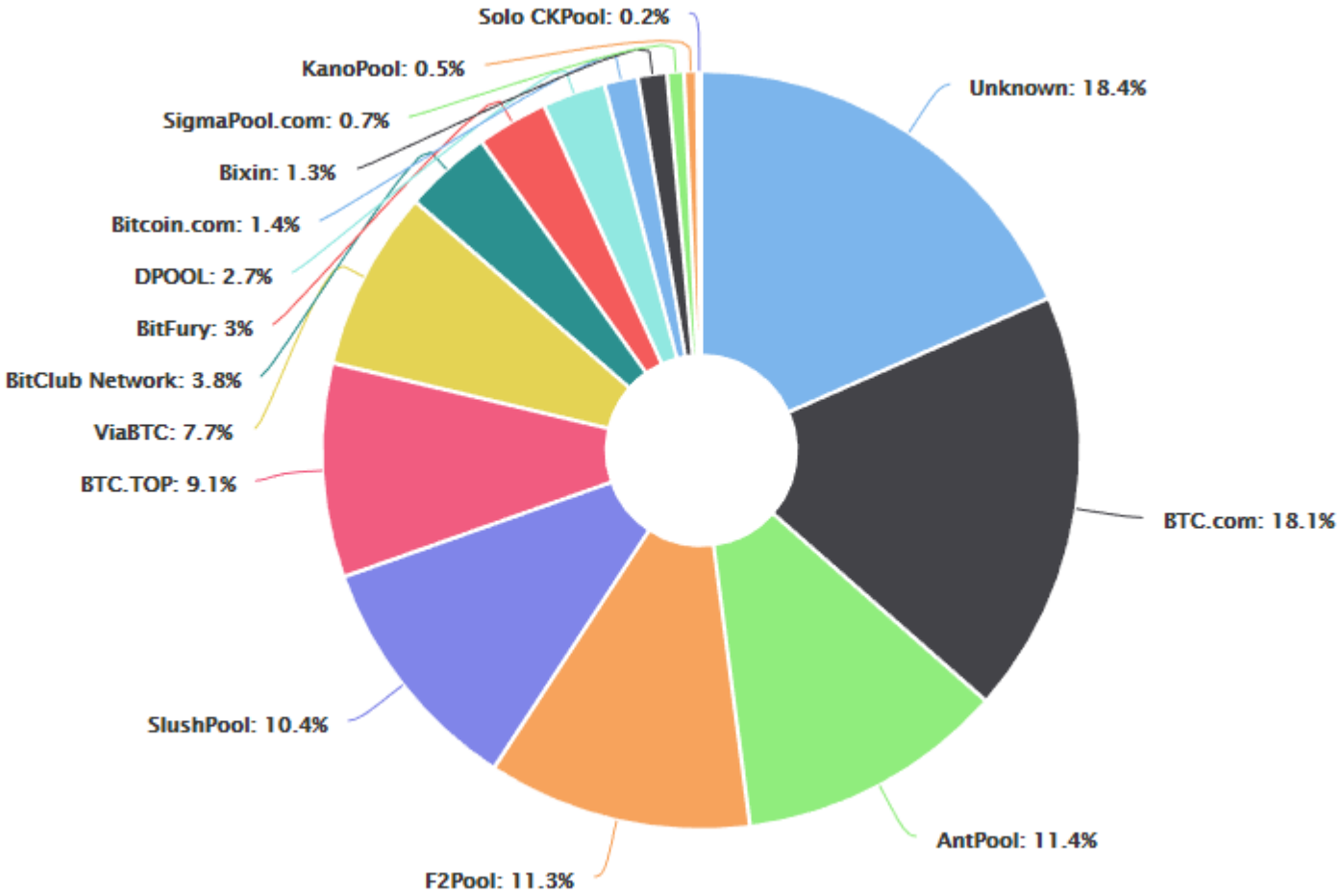
- 블록 생성 시간: 10 분

- 채굴 보상: 6.25 BTC ≈ $29,3790 (2021.09.01)



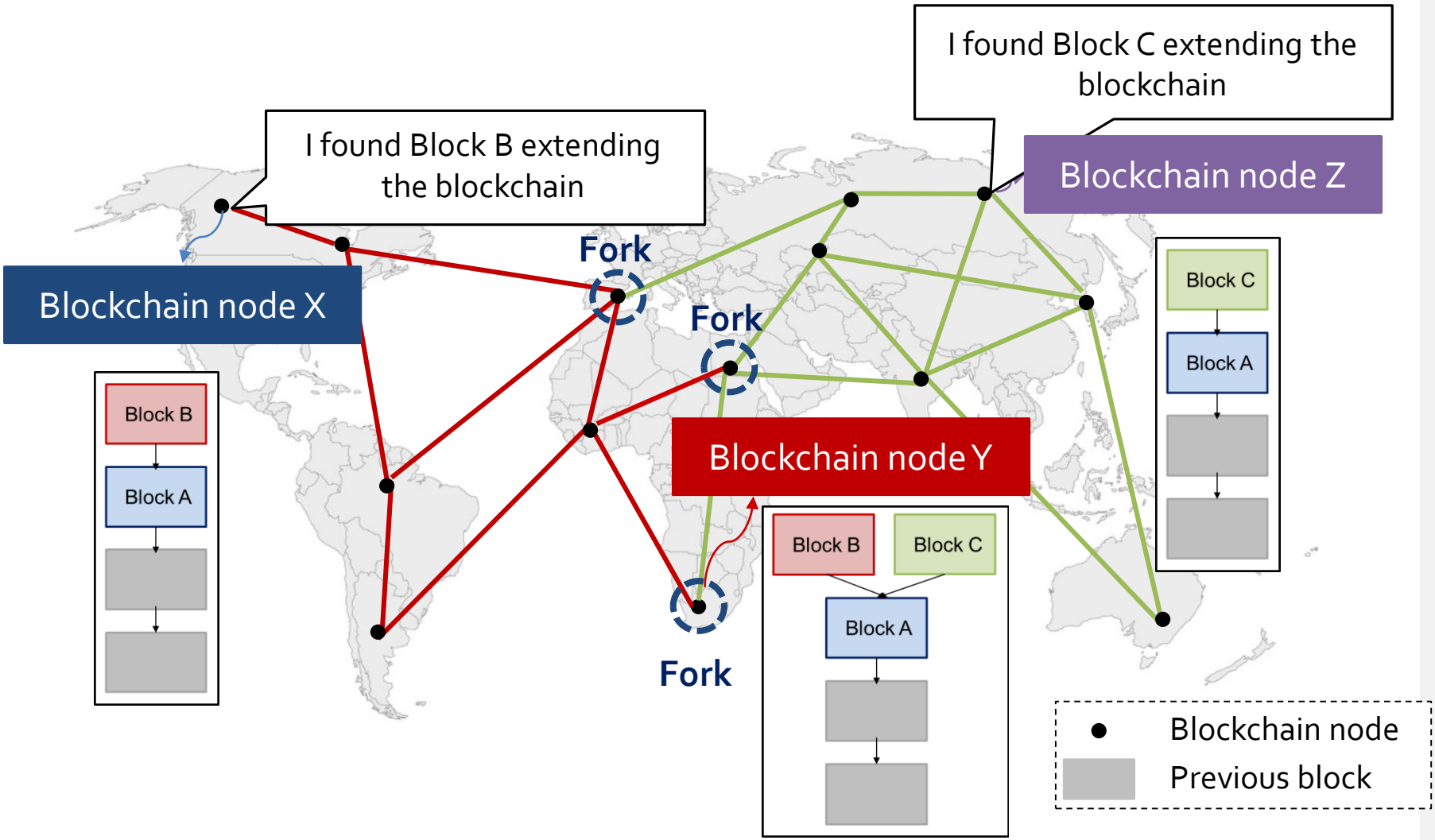


Proof-of-Work

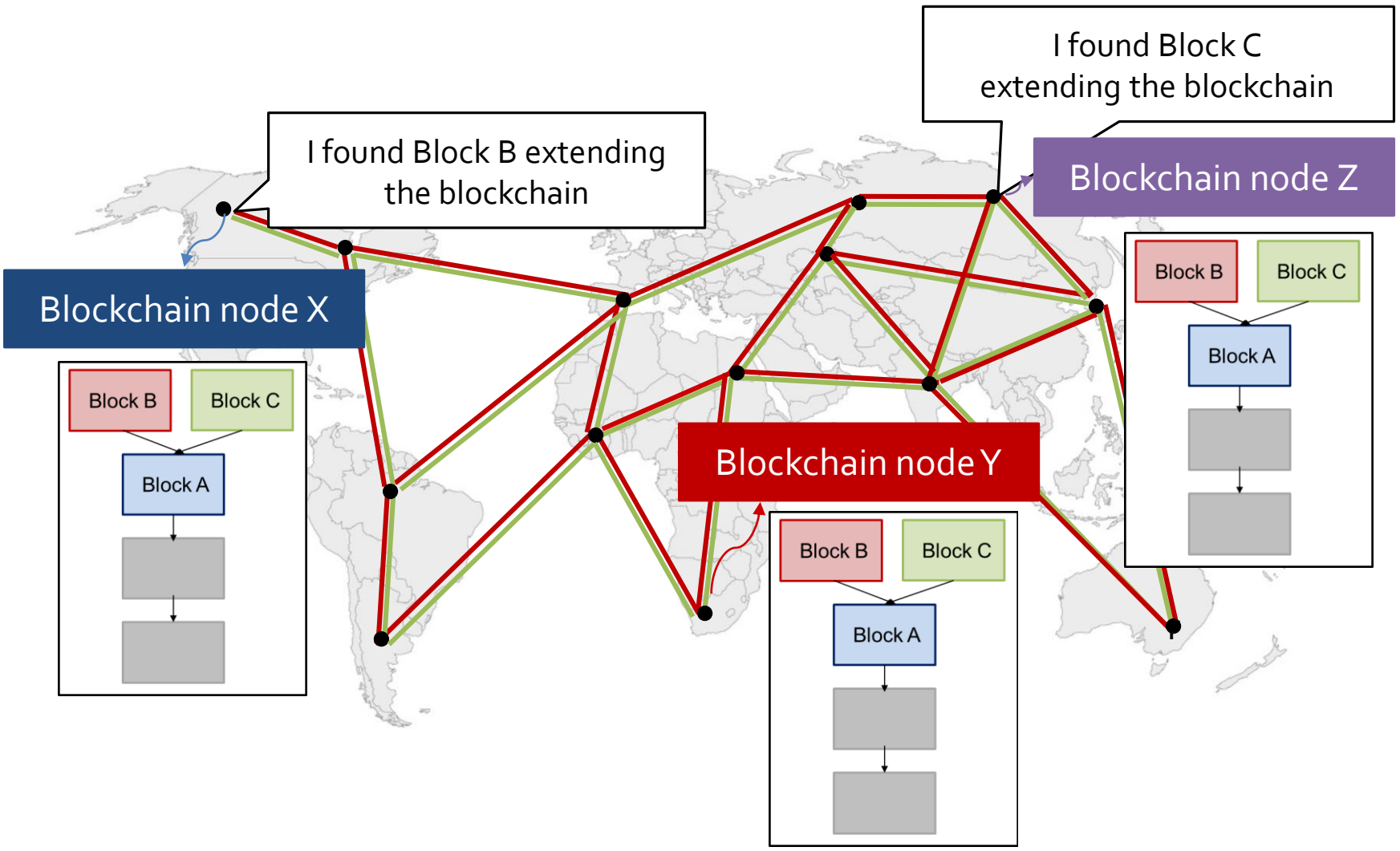


[Source: https://www.blockchain.com/ko/pools]

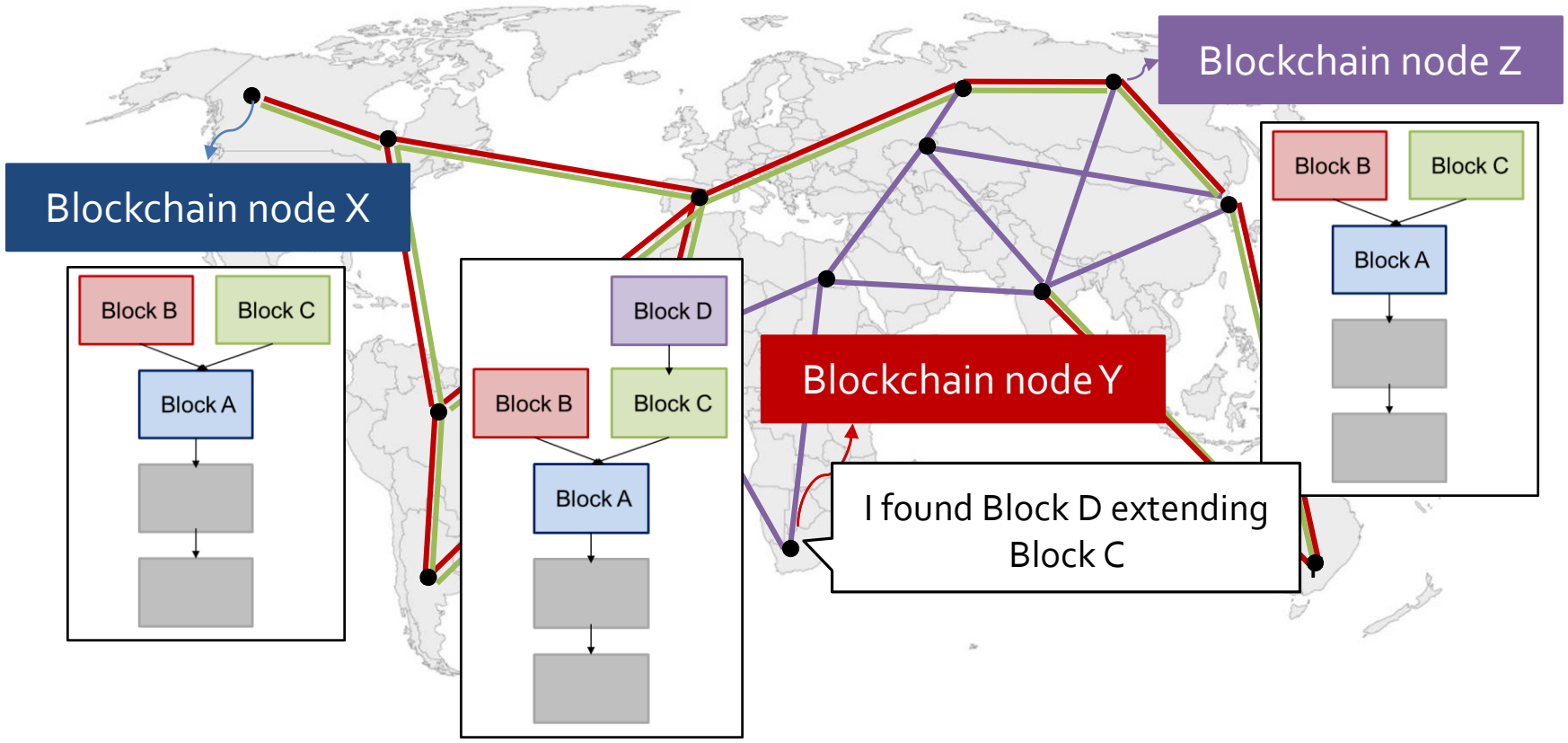
(Temporary) Fork - Data synchronization



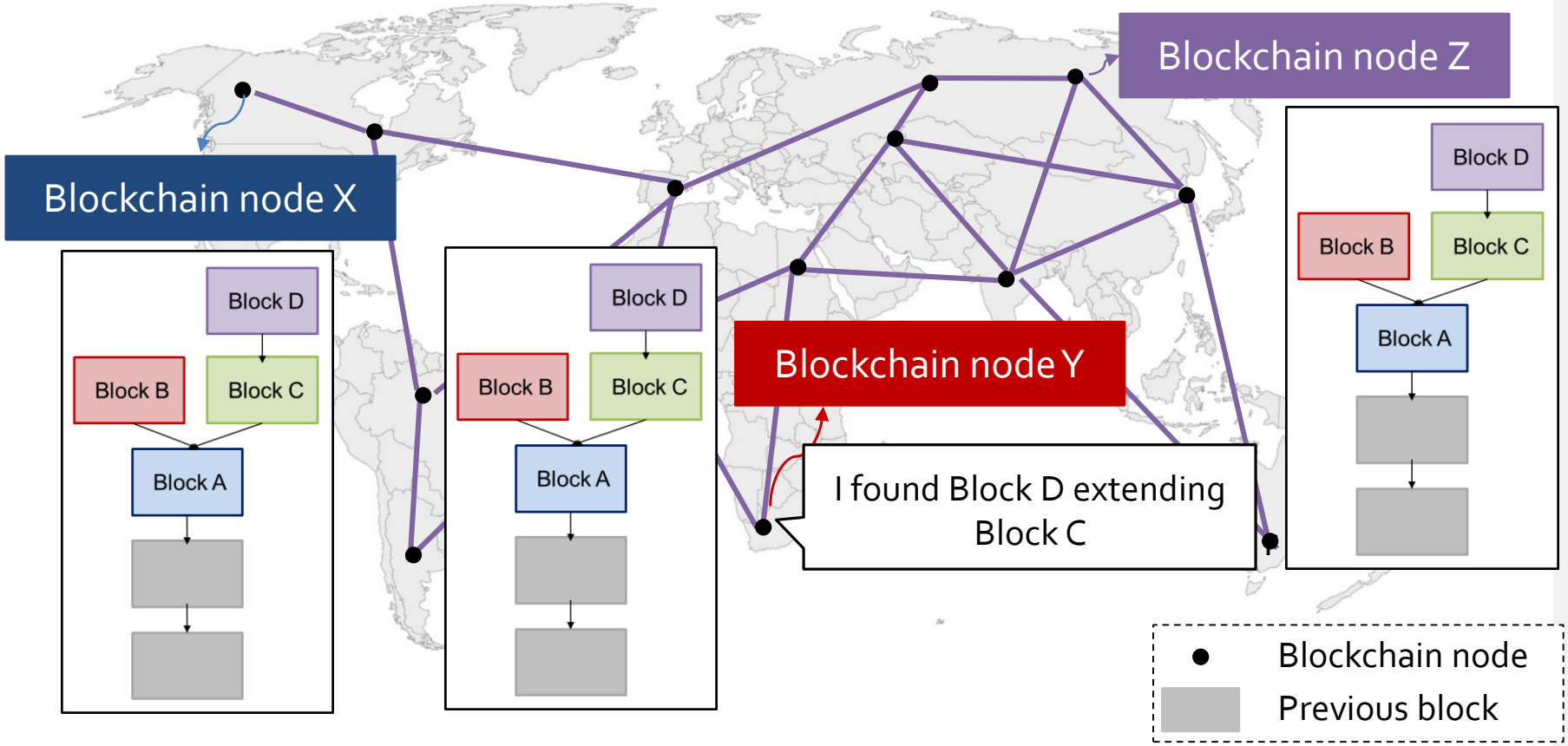
(Temporary) Fork - Data synchronization



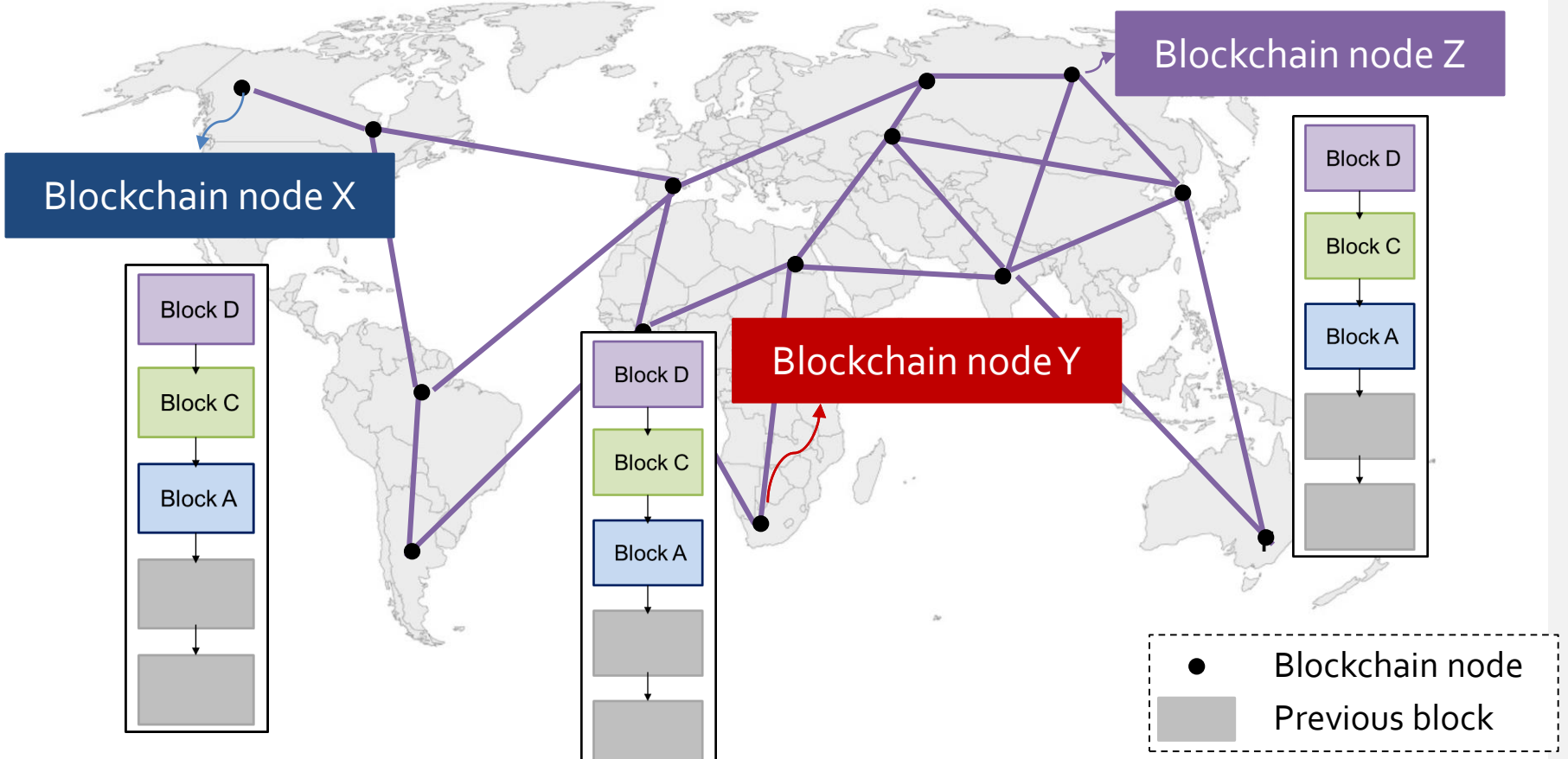
(Temporary) Fork - Data synchronization



(Temporary) Fork - Data synchronization



(Temporary) Fork - Data synchronization



Summary

- Bitcoin's nodes
  - Full nodes
  - Lightweight nodes
- Merkle tree
- PoW (Proof-of-Work)
  - Hash-based PoW
  - Mining pool

Reference

- Mastering Bitcoin, 2nd Edition

- Lecture slides from BLOCKCHAIN @ BERKELEY

Q & A