비트코인 개요

목차

비트코인의 정의

- 블록체인 기반의 최초의 암호화폐
- 블록체인의 기술적 기본 개념을 정의
- 중앙화된 기관 없이도 거래 성립이 가능하다는 것을 제시 및 증명
- 사토시 나카모토, 그외의 개발자들

비트코인의 역사

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort

비트코인 근황

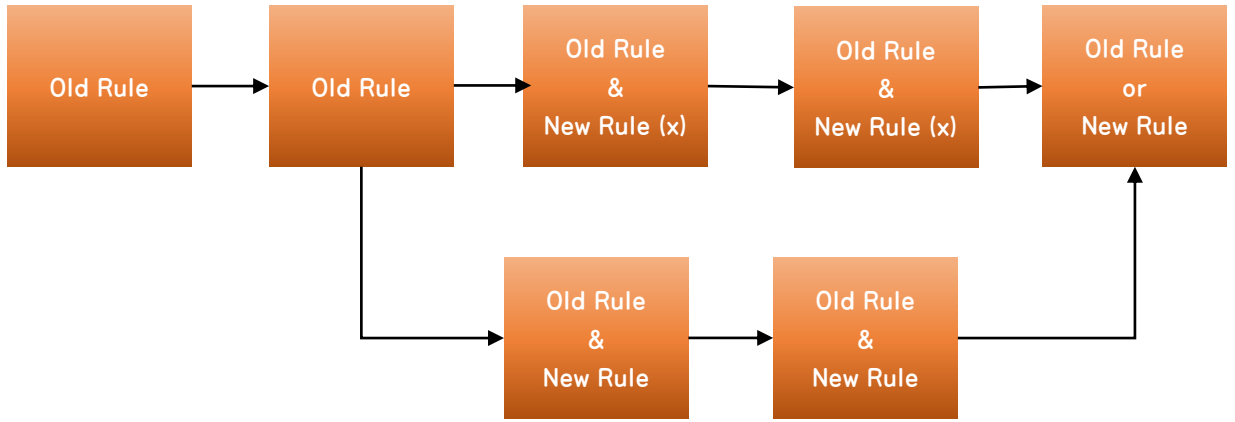

Bitcoin Cash
Bitcoin Gold
Bitcoin Diamond
Bitcoin Classic
bitcoin
Aug 2017
Oct 2017
Nov 2017
Feb 2016
Super Bitcoin
Bitcoin Hot
Dec 2017
Dec 2014
Bitcoin XT
Jan 2009
Jan 2018
Bitcoin Interest
Bitcoin Genesis Block
Mar 2018
Feb 2018
Bitcoin All
Bitcoin Private
Bitcoin Cash Plus
BITCOIN MARKET JOURNAL

목차

소프트포크, 하드포크

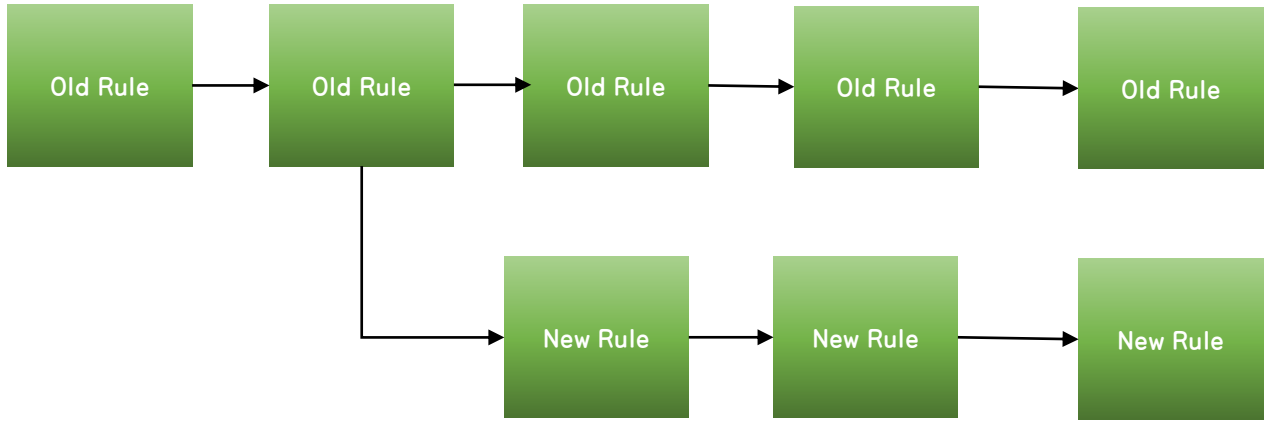
포크는 특정 커뮤니티, 개발자에 의해서 이루어 질 수 있음

소프트 포크



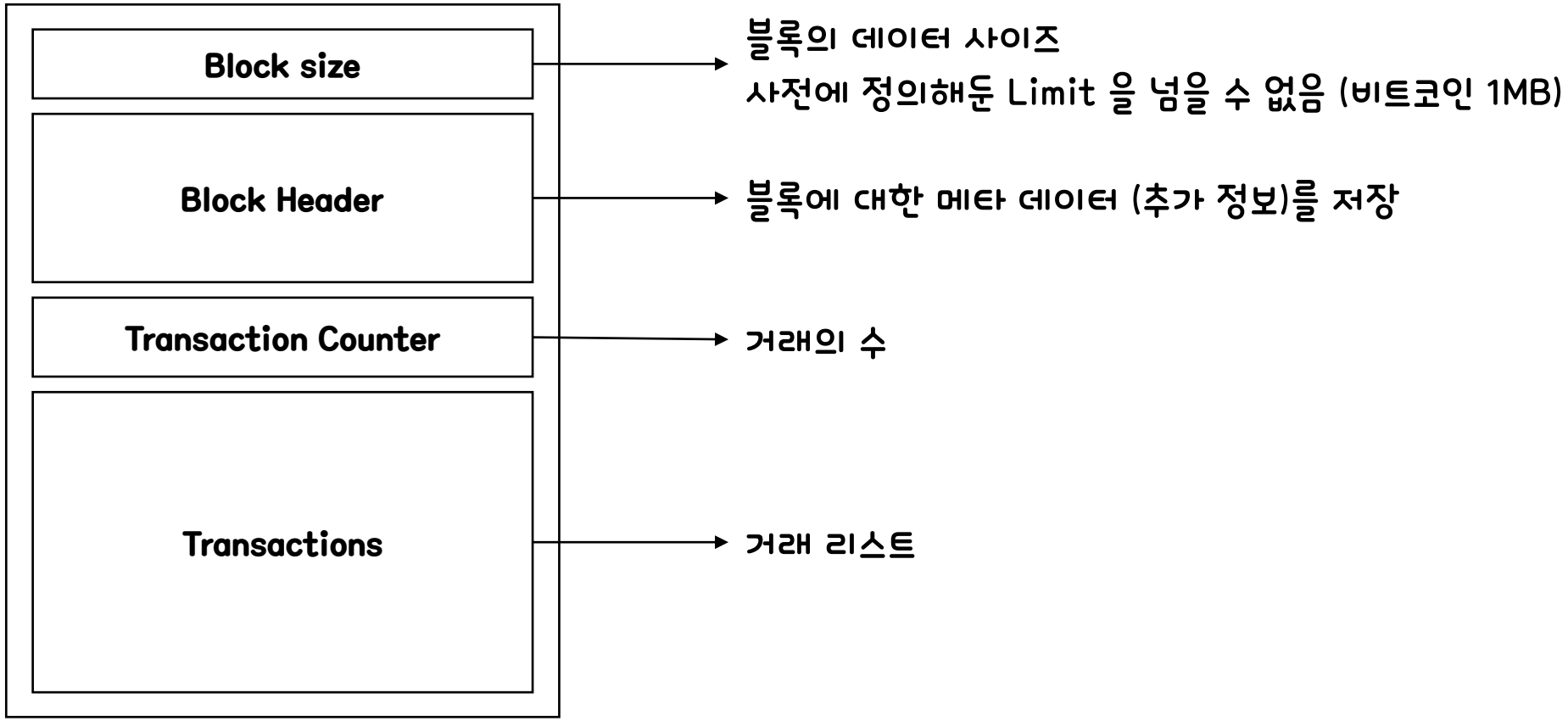
- 간단한 업데이트
- 기존 규칙에서 새로운 규칙을 추가 하는것
- 최종적으로 어떤 규칙이 선택될지는 네트워크 참여자 마음

하드 포크

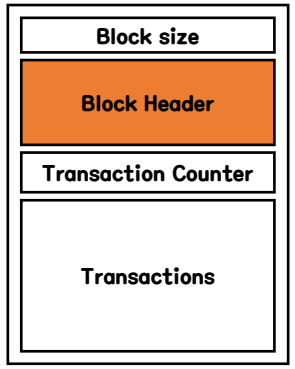


- 대규모 업데이트
- 기존 규칙을 지우고 완전히 새로운 규칙을 가진 블록을 생성
- 새로운 블록체인을 만드는 것
- 기존 블록과 연동될 수 없음

블록 구조

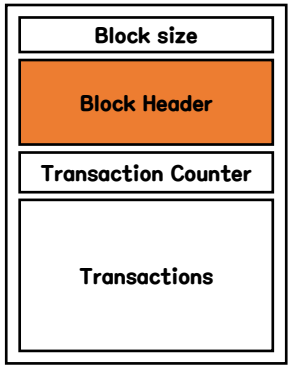

Block size
Block Header
Transaction Counter
Transactions
블록의 데이터 사이즈
사전에 정의해둔 Limit 을 넘을 수 없음 (비트코인 1MB)
블록에 대한 메타 데이터 (추가 정보)를 저장
거래의 수
거래 리스트

블록 구조



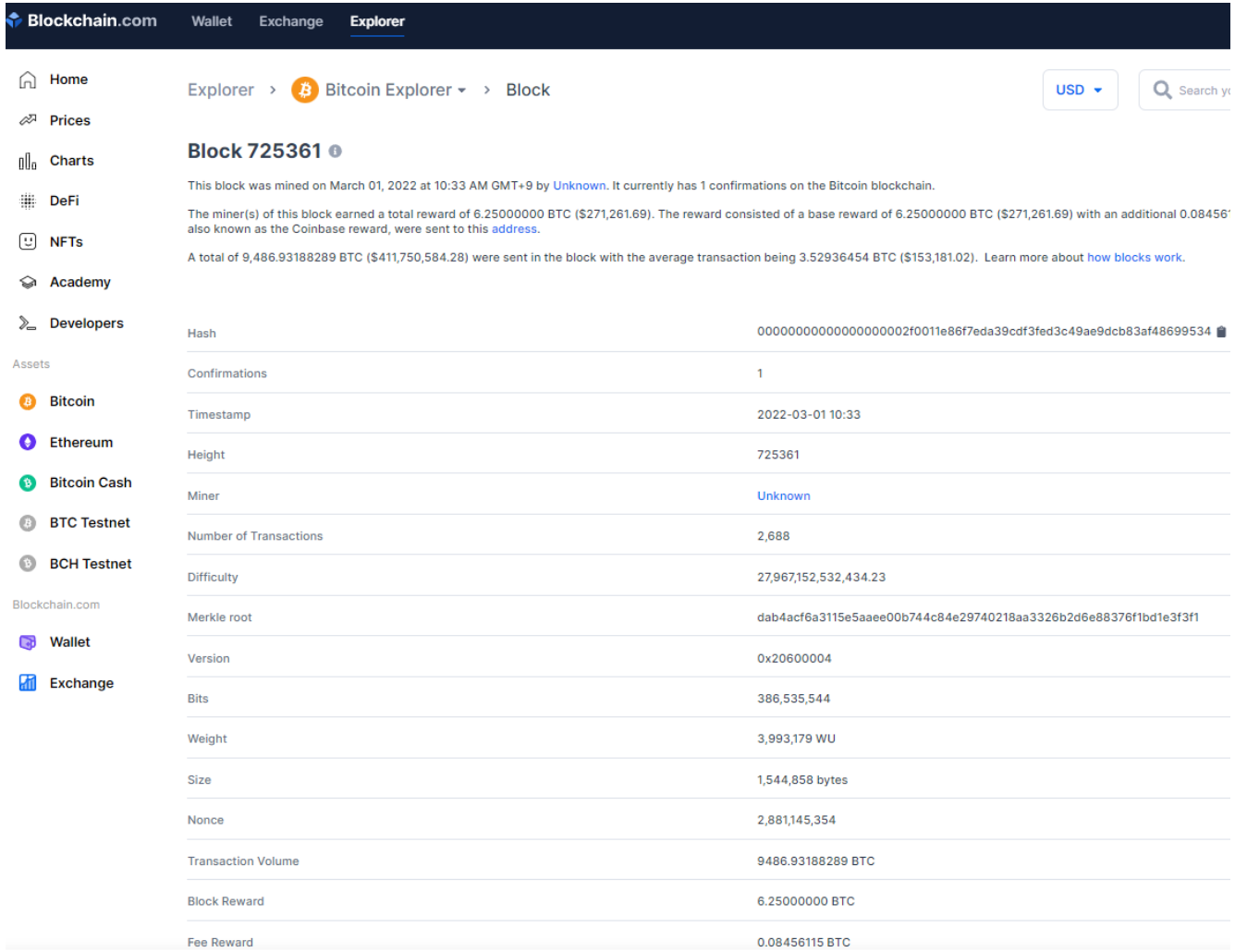
Block Header 정보	
버전	소프트웨어 / 프로토콜 업그레이트 추적을 위한 버전
이전 블록 해시	이전 블록의 해시 값
머클 루트	머클 트리로 만들어진 머클 루트 값
타임 스탬프	블록의 대략적인 생성 시간 (유닉스 타임)
난이도 목표	작업증명 알고리즘에 대한 난이도 목표
논스	작업증명에 사용되는 정답

블록 구조



Block Header 정보

버전	소프트웨어 / 프로토콜 업그레이드 추적을 위한 버전
이전 블록 해시	이전 블록의 해시 값
머클 루트	머클 트리로 만들어진 머클 루트 값
타임 스탬프	블록의 대략적인 생성 시간 (유닉스 타임)
난이도 목표	작업증명 알고리즘에 대한 난이도 목표
논스	작업증명에 사용되는 정답



거래 과정

잔액 보관함

30 BTC

10 BTC

잔액 보관함

10 BTC

거래 과정

잔액 보관함

20 BTC

잔액 보관함

20 BTC

거래 과정

10 BTC

UTXO

10 BTC
5 BTC
5 BTC
10 BTC

Script

Script

UTXO

1 BTC
5 BTC
4 BTC

거래 과정

UXTO (Unspent Transaction Output, 소비되지 않은 거래 출력)

- 사용자 마다 본인의 UTXO를 가지고 있음
- 사용자가 알고 있는 잔액 이라는 개념음 UTXO 값을 합친 값
- 사용자가 비트코인을 수령할때마다 모든 금액은 UTXO에 저장됨

Script Language

- 비트코인은 잠금, 해제 스크립트를 사용하여 거래를 완료함
- 스택(stack)이라 불리는 데이터 구조를 사용
- 향후 출력값을 소비하기 위해 충족되어야 하는 요건을 명시
- 잠금 스크립트는 공개키 혹은 비트코인 주소를 포함
- 해제 스크립트는 잠금 스크립트가 출력값에 놓아 둔 조건을 해결 하거나 충족시켜 출력값이 소비될 수 있도록 함
- 해제 스크립트는 사용자의 개인키로부터 생성한 디지털 서명을 가지고 있음

거래 과정

3BTC를 보내고 싶을때

지갑

UTXO (1) - 10 BTC
UTXO (2) - 5 BTC
UTXO (3) - 5 BTC
UTXO (4) - 10 BTC

지갑

UTXO (1) - 10 BTC
UTXO (2) - 5 BTC
~~UTXO (3) - 5 BTC~~
UTXO (4) - 10 BTC
UTXO (5) - 2 BTC

3 BTC

거래 시 마다 새로운 UTXO를 형성하므로 익명성과 보안성에 장점이 있다

인출이 일어날때마다 UTXO를 새롭게 생성하고 사라짐으로 프라이버시가 보장

단, UTXO 생성마다 수수료가 생성된다는 단점이 존재

거래 과정

잠금 스크립트: UTXO 잠금장치

해제 스크립트: 잠금 스크립트를 해제하기 위한 키

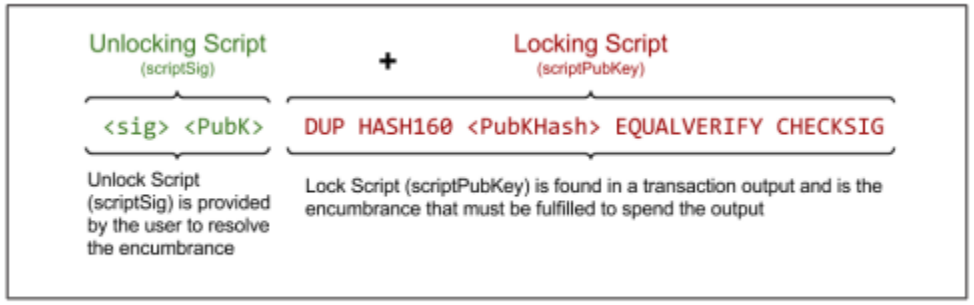
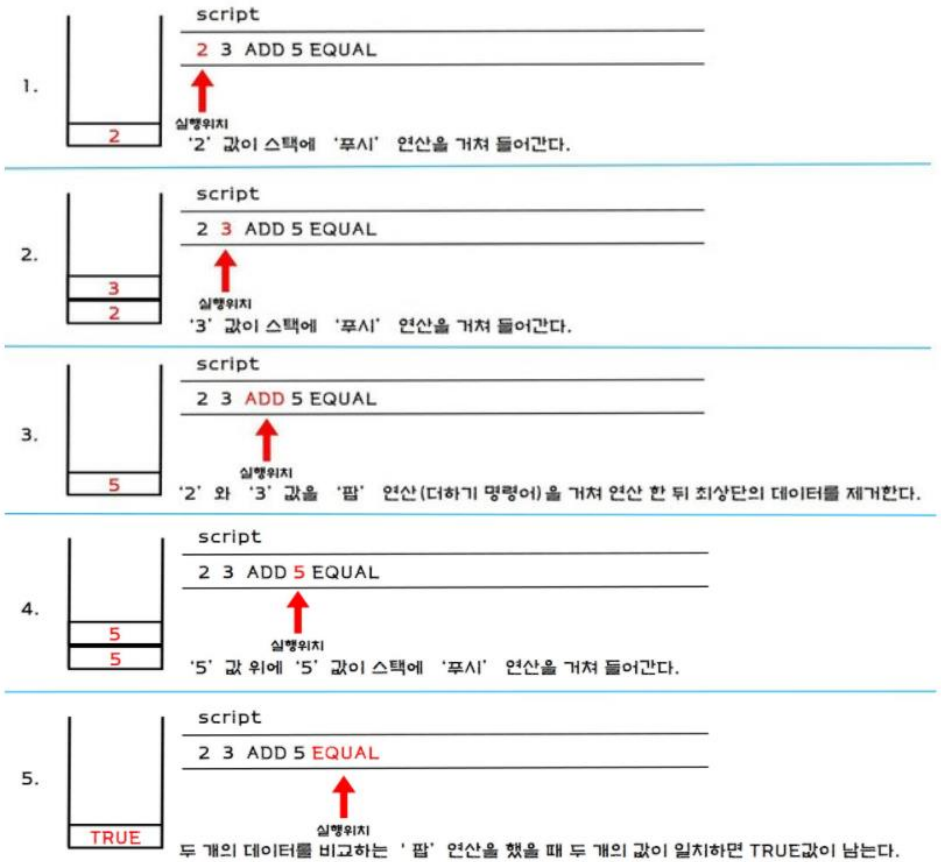


Figure 5-1. Combining scriptSig and scriptPubKey to evaluate a transaction script

Mastering Bitcoin

잠금 스크립트: +3 = 5

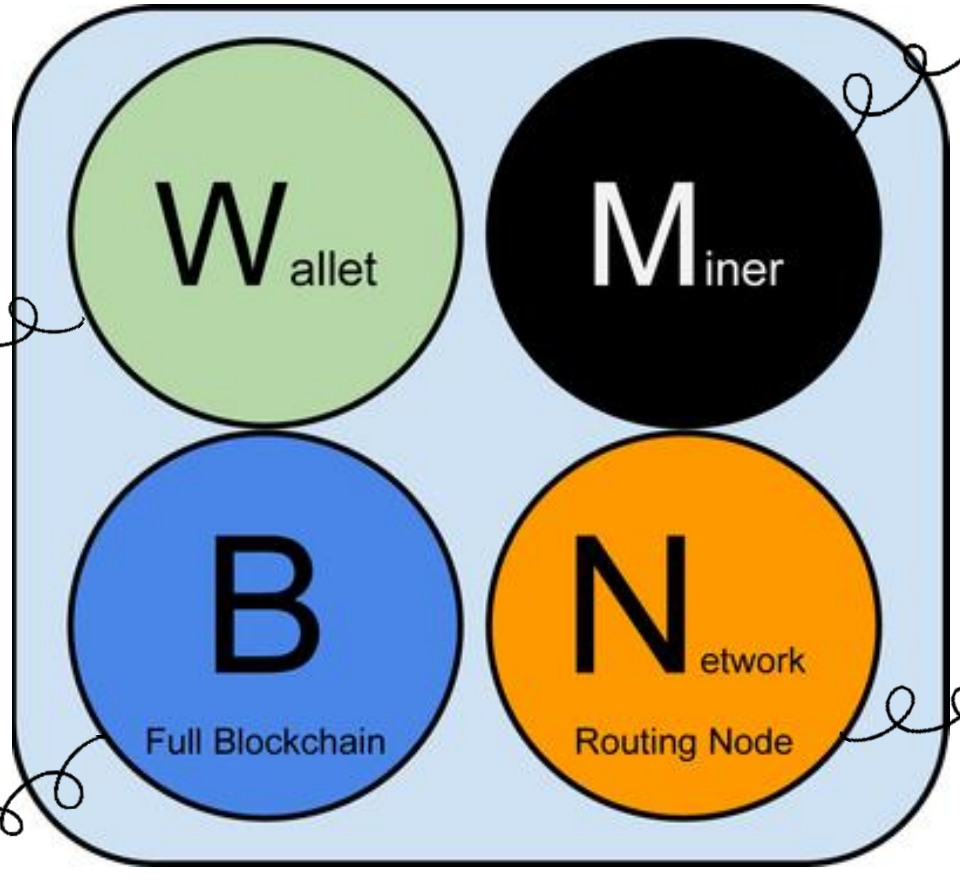
해제 스크립트: 2



https://steemit.com/kr/@easyblockchain/5y38ab

노드의 구성

✓ 작업증명 알고리즘을 풀어 새로운 블록을 생성하기 위해 경쟁
✓ 블록 생성시 비트코인을 보상으로 받음



✓ 소유한 비트코인 송수신 및 잔고 확인

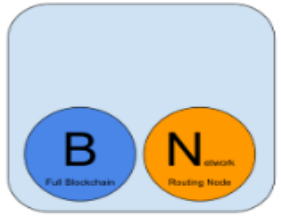
✓ 거래와 블록을 검증하고 전파하며, 이웃 노드들과의 연결을 유지

✓ 모든 노드 유형에 필수

✓ 온전한 최신 블록체인 복사본을 유지. 외부 참조 없이 독자적으로 거래 검증 가능
✓ 블록체인 부분집합(주로 헤더)만 유지하는 경우 SPV 노드 혹은 라이드웨이트 노드라 불림

https://steemit.com/kr/@niipoong/block-chain-nodes-and-roles

노드의 구성

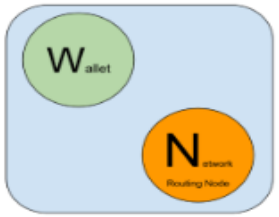


Full Block Chain Node

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

Solo Miner

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



Lightweight (SPV) wallet

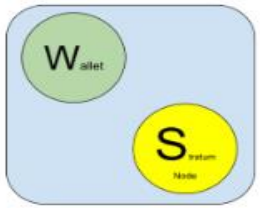
Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.

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

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



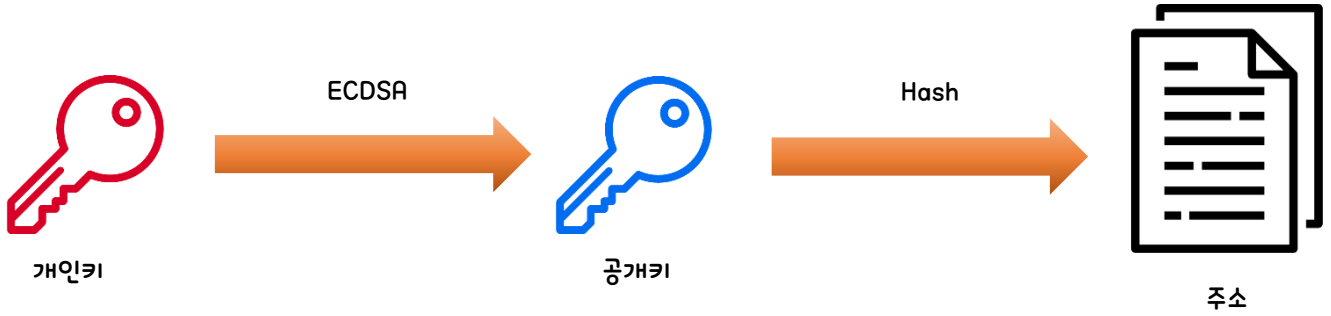
Lightweight (SPV) Stratum wallet

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

https://steemit.com/kr/@niipoong/block-chain-nodes-and-roles

목차

키, 주소, 지갑

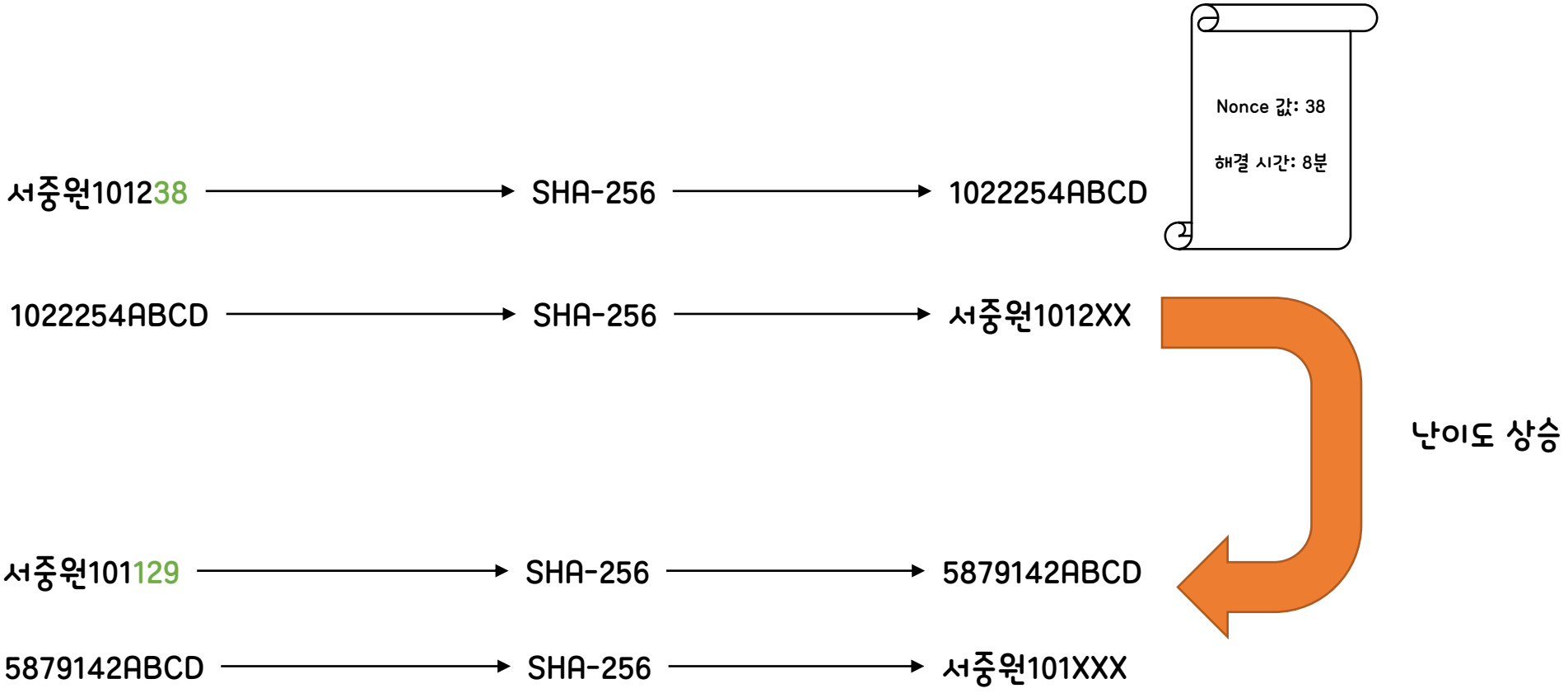


합의 알고리즘

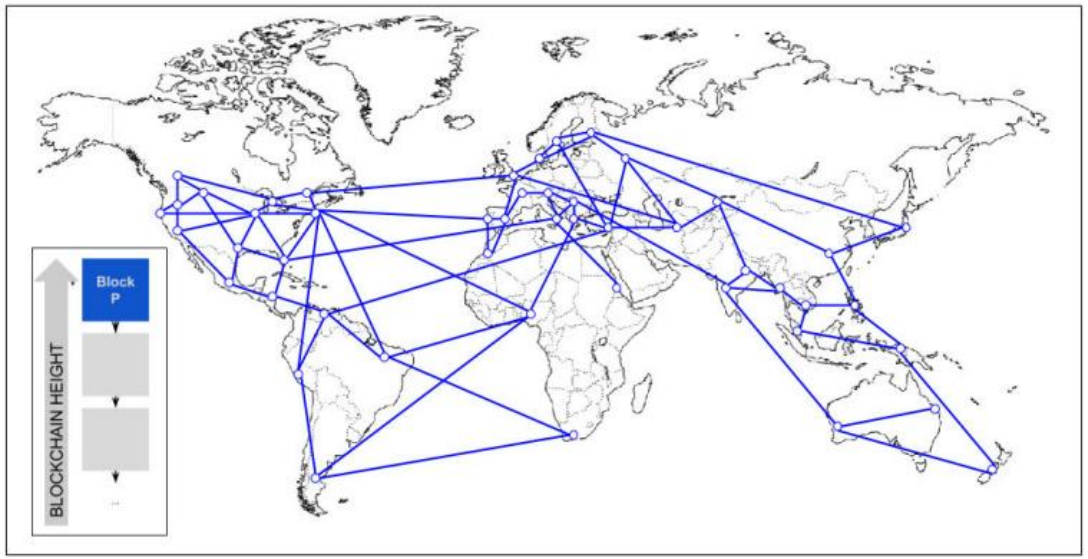
작업증명 (PoW: Proof of Work)

- 비트코인의 총량이 약 2100만 비트코인으로 고정되어있음
- 2100만 비트코인이 2140년이 될동안 작업증명 (채굴)을 통해 생성됨
- 해시알고리즘의 특징을 활용하여 사용된 알고리즘
- 10분안에 풀수 있도록 되어있음

합의 알고리즘


서중원101238
SHA-256
1022254ABCD
Nonce 값: 38
해결 시간: 8분
1022254ABCD
SHA-256
서중원1012XX
난이도 상승
서중원101129
SHA-256
5879142ABCD
5879142ABCD
SHA-256
서중원101XXX

블록 분기



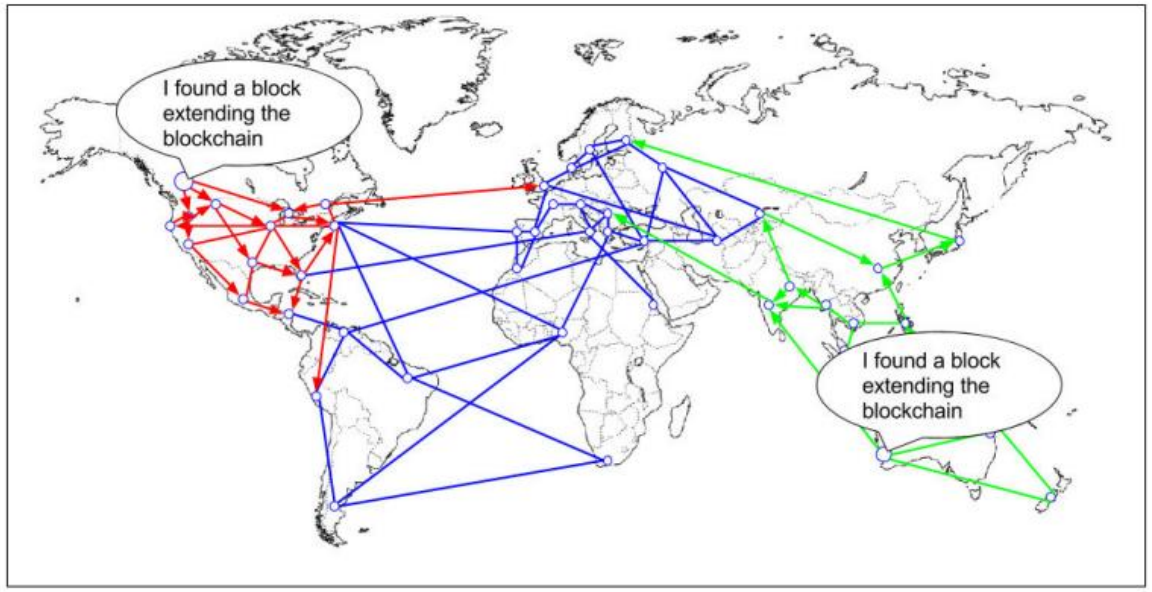


그림 출처: Mastering Bitcoin

블록 분기

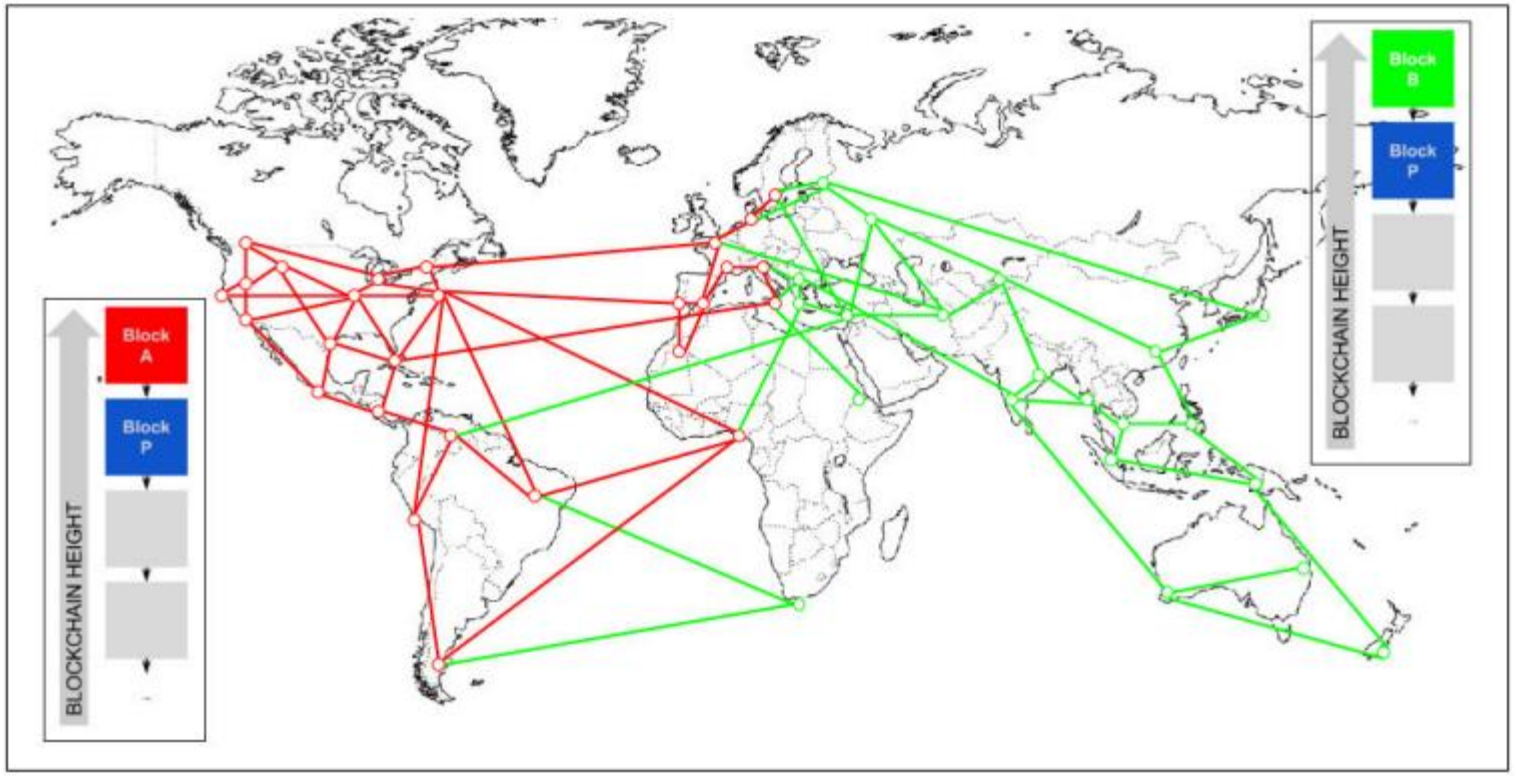
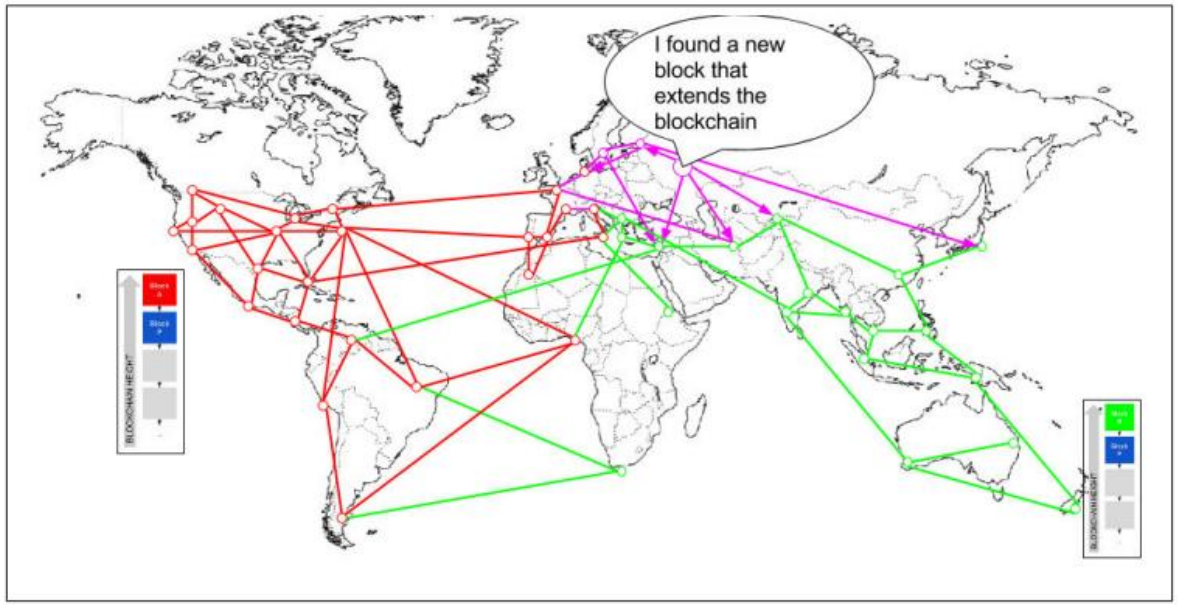


그림 출처: Mastering Bitcoin

블록 분기



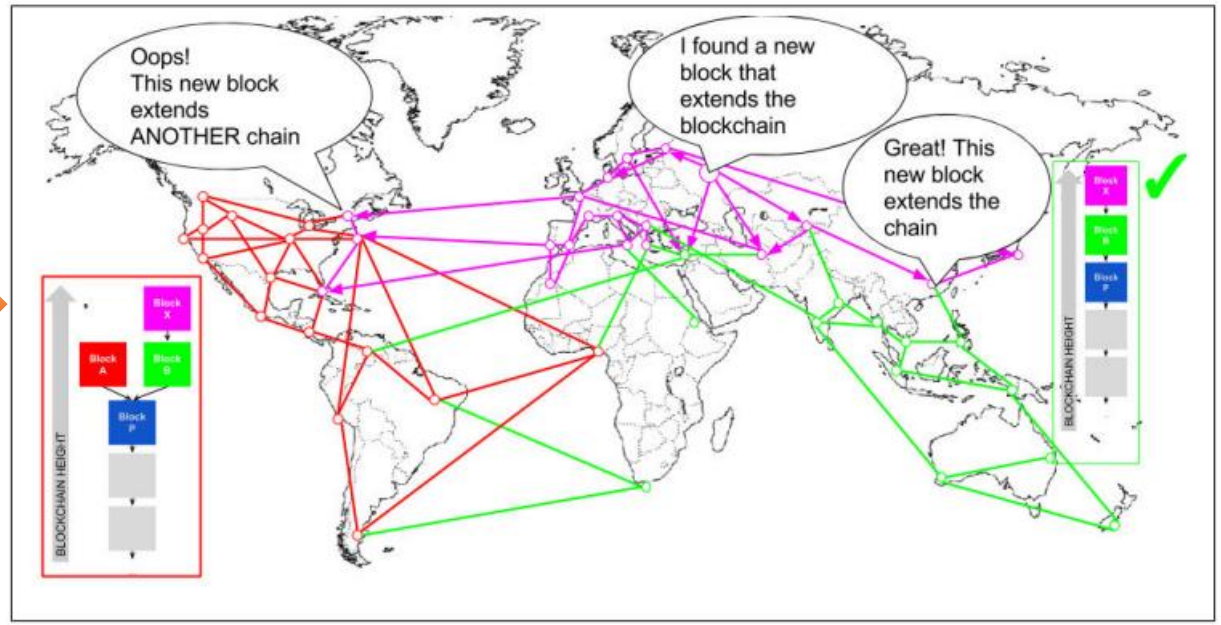
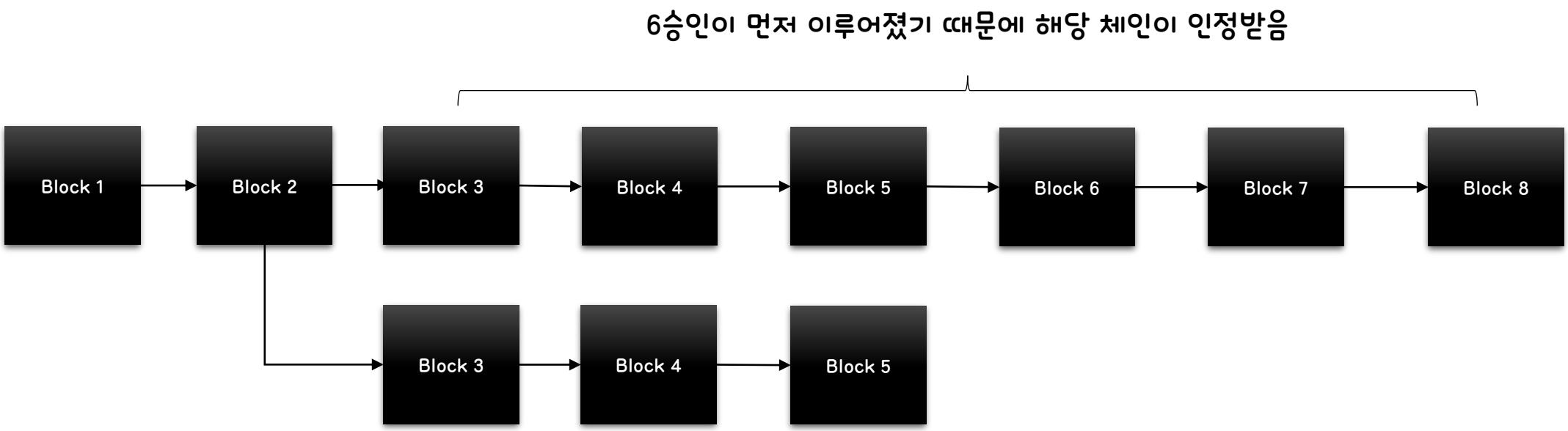


그림 출처: Mastering Bitcoin

블록 분기


6승인이 먼저 이루어졌기 때문에 해당 체인이 인정받음
Block 1
Block 2
Block 3
Block 4
Block 5
Block 6
Block 7
Block 8
Block 3
Block 4
Block 5

블룸필터

- 특정 원소가 집합에 속하는지 검사하기 위한 자료 구조
- 비트코인에서는 거래 식별을 위해서 사용
- 많은 양의 데이터를 줄여서 공간 효율적으로 빠르게 검색 가능
- 처리능력 대비 적은 메모리 공간만이 필요

블룸필터

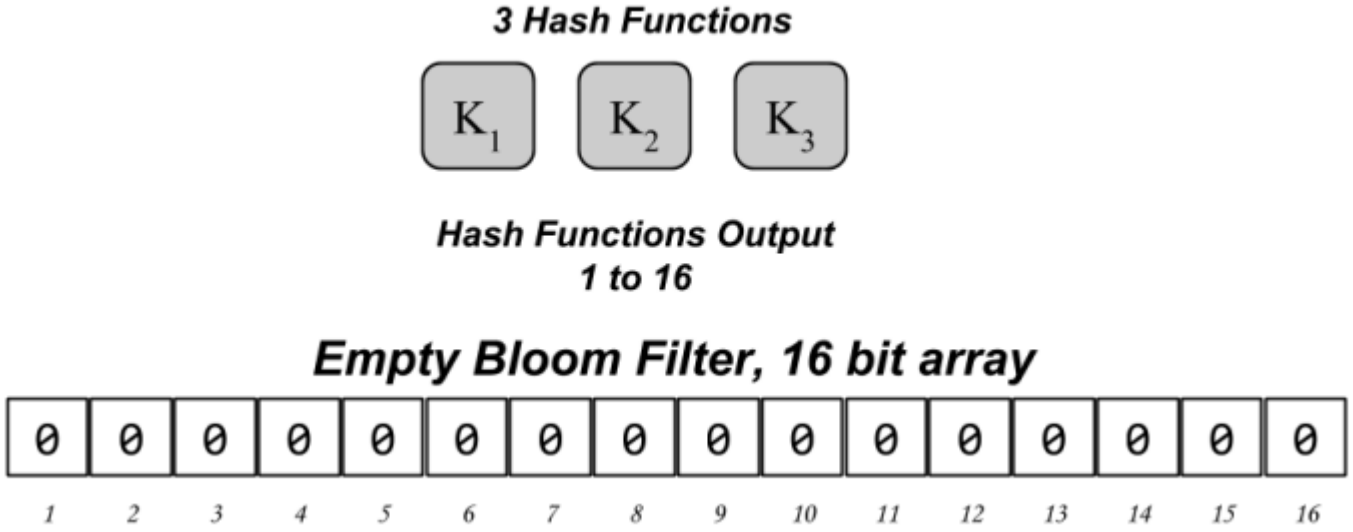
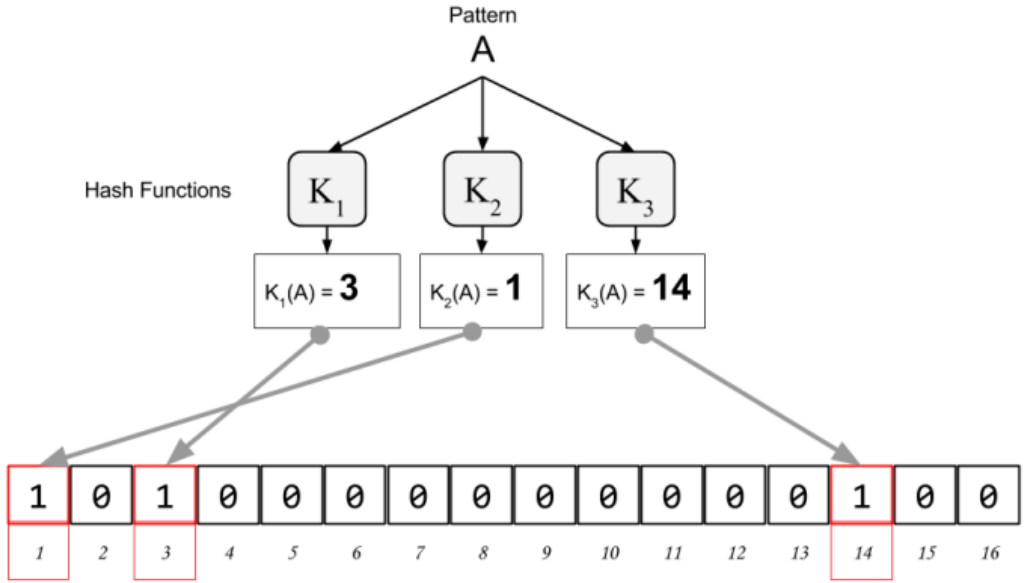


그림 출처: Mastering Bitcoin

블룸필터



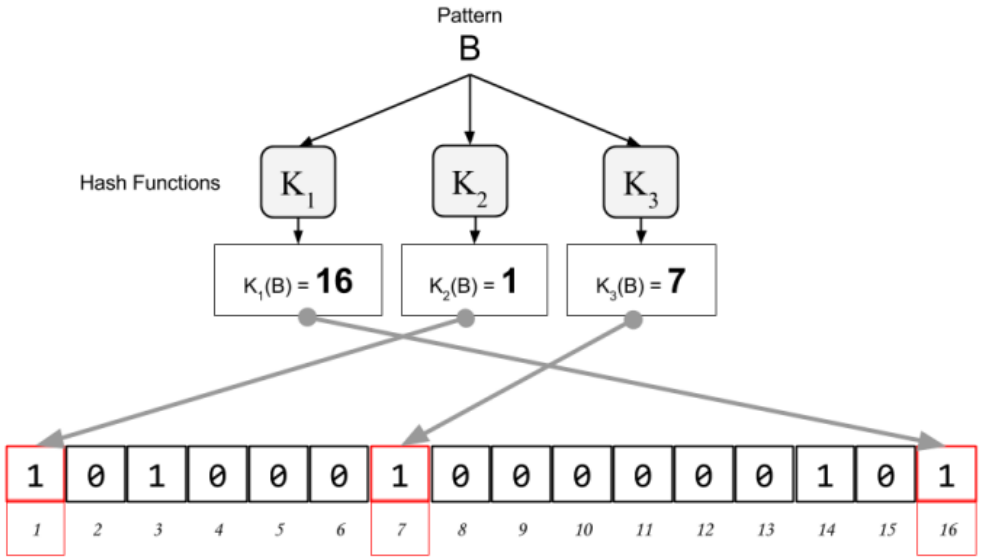
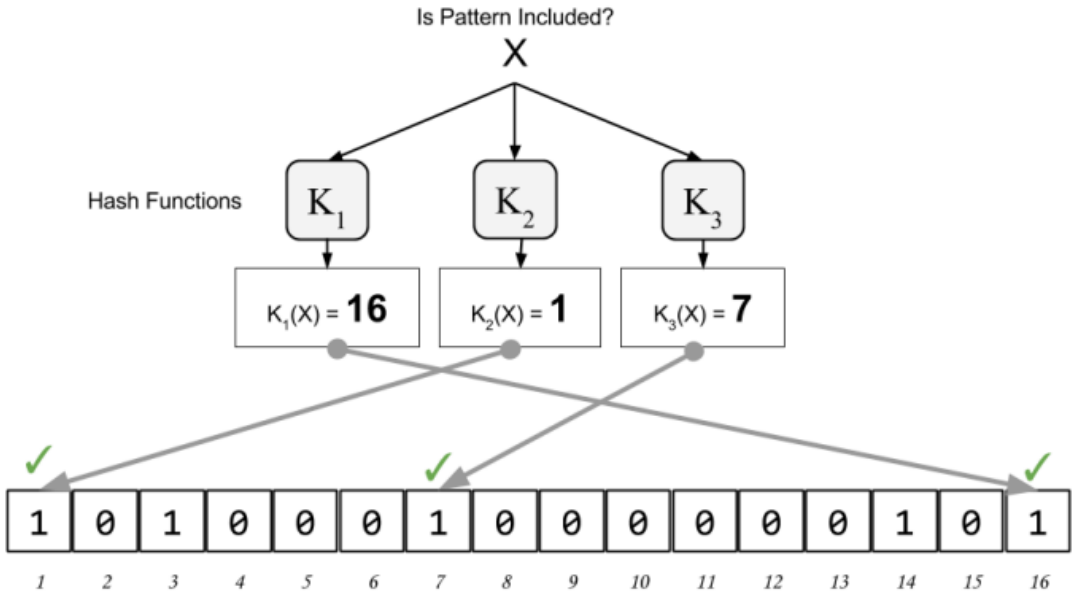


그림 출처: Mastering Bitcoin

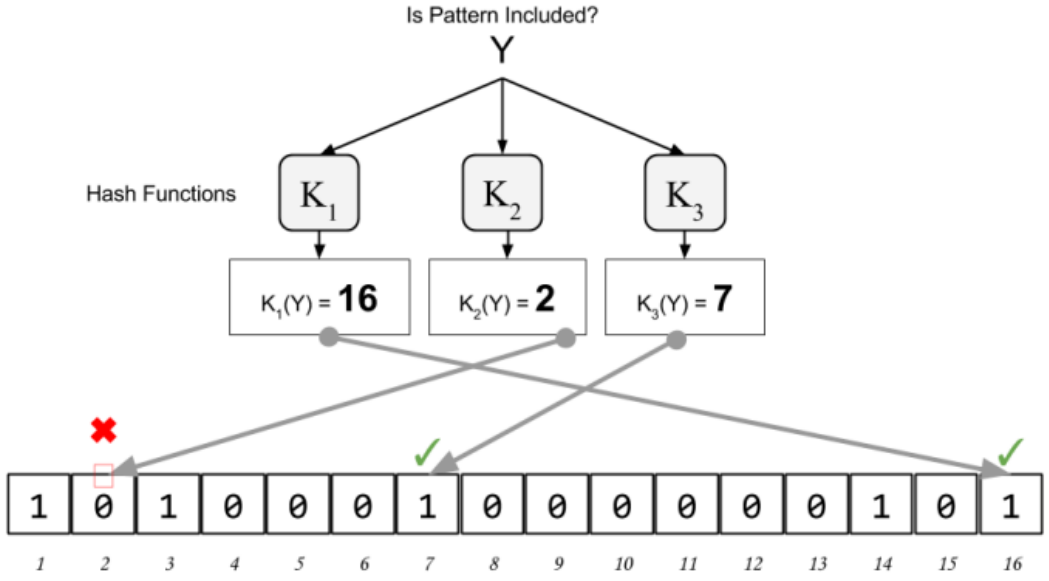
블룸필터

긍정 오류가 발생할 확률이 있으나,

틀린건 확실하게 파악 가능



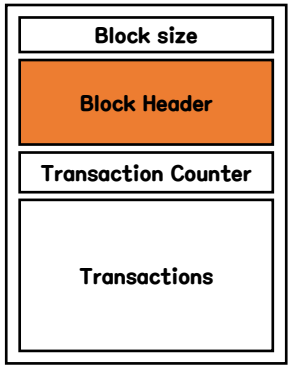
Maybe, Yes



Definitely Not!

그림 출처: Mastering Bitcoin

머클트리



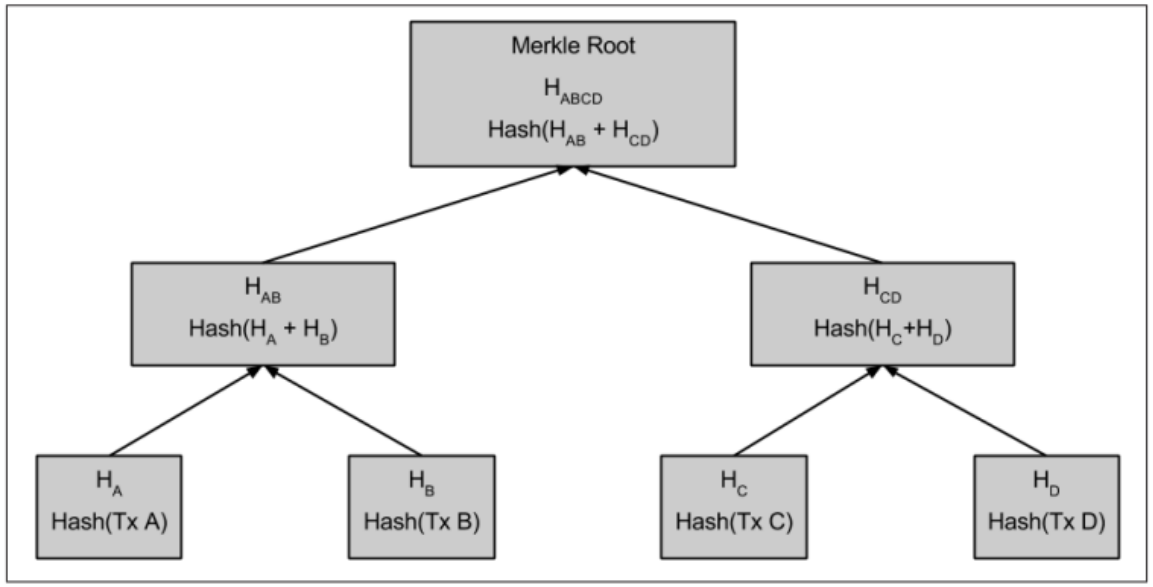
Block Header 정보

버전	소프트웨어 / 프로토콜 업그레이드 추적을 위한 버전
이전 블록 해시	이전 블록의 해시 값
머클 루트	머클 트리로 만들어진 머클 루트 값
타임 스탬프	블록의 대략적인 생성 시간 (유닉스 타임)
난이도 목표	작업증명 알고리즘에 대한 난이도 목표
논스	작업증명에 사용되는 정답

머클트리

- 해당 블록에 들어있는 모든 거래의 요약본
- 이진 해시 트리
- 특정 거래가 블록 내부에 포함되는지 여부를 검증하는데 효율적임

머클트리



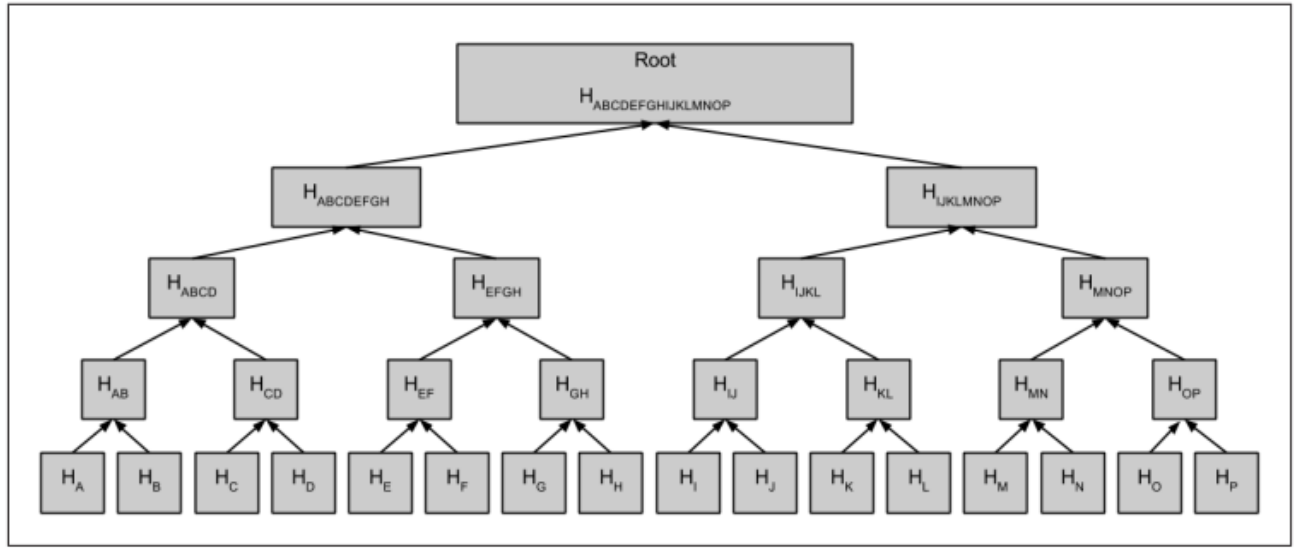


그림 출처: Mastering Bitcoin

Q & A