

한 번에 끝내는 블록체인 개발 A to Z

Chapter 1

Blockchain 1.0 - Bitcoin

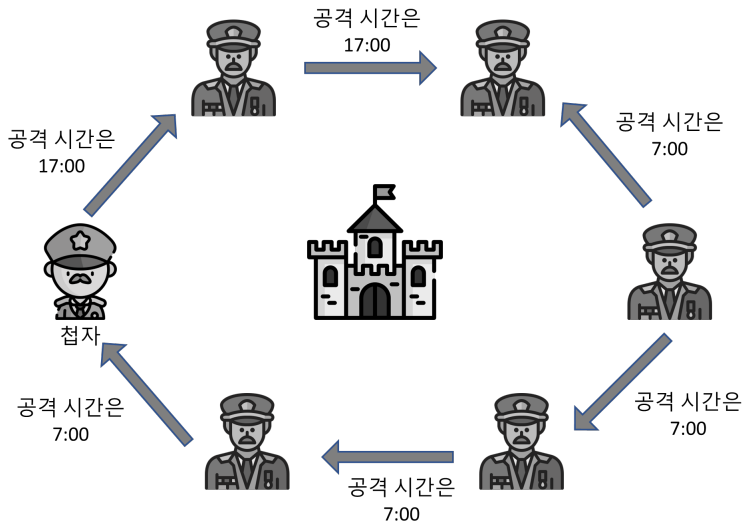
Chapter 1

Blockchain 1.0 - Bitcoin

Consensus

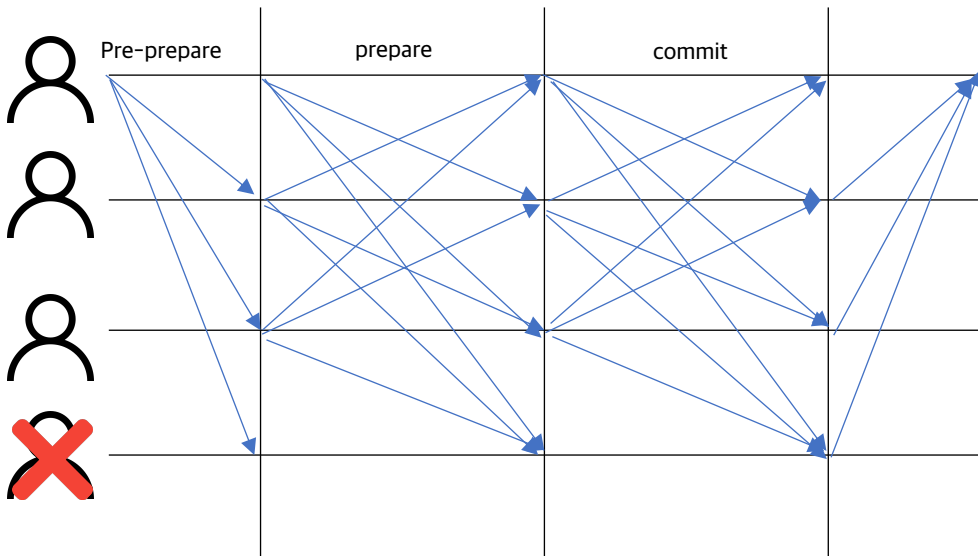
비잔틴 장군 문제

- 특정 수 이상의 장군이 동시에 공격을 해야 성을 공략할 수 있다.
- 서로 P2P로만 연락을 주고 받을 때, 첩자의 방해가 있더라도 이 공격을 성공시키는 방법은?



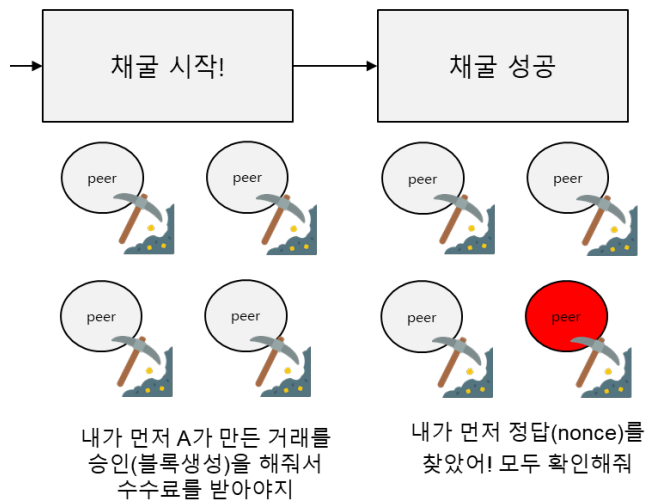
BFT

- Byzantine Fault Tolerance(BFT)란 분산화된 네트워크에서 일부 장애가 발생하더라도 네트워크가 정상적으로 동작할 수 있도록 하는 알고리즘이다.
- PBFT(Practical BFT)가 블록체인 생태계에서 많이 사용되고 있으며, Cosmos, Hyperledger 등에서 사용되고 있다.



Proof Of Work

- Computing Power로 Double Spending과 같은 거래 위변조 공격을 막는 방법
- 새로운 블록을 생성하는 것이고 그 방법은 그 블록 내에 Field로 포함되는 Nonce값을 찾는 것
- 전체 Network Hash에 따라 Difficulty 가 변화하고, 10분마다 Block이 생성되게 조정



채굴 과정

- 1) 새로운 블록(a)이 생성됨을 알림받는다.
- 2) 다음 블록 생성을 위해서 임시 Pending 중인 Transaction을 포함한다.
- 3) Coinbase 거래를 임시 블록에 포함한다.
- 4) 이전 블록(a)와 Transaction들을 포함한 임시 Block구조(b)를 만든다.
- 5) 새로운 Block(b)의 Header Hash가 결과값이 나올 때 까지 brute force 방식으로 nonce를 찾는다.

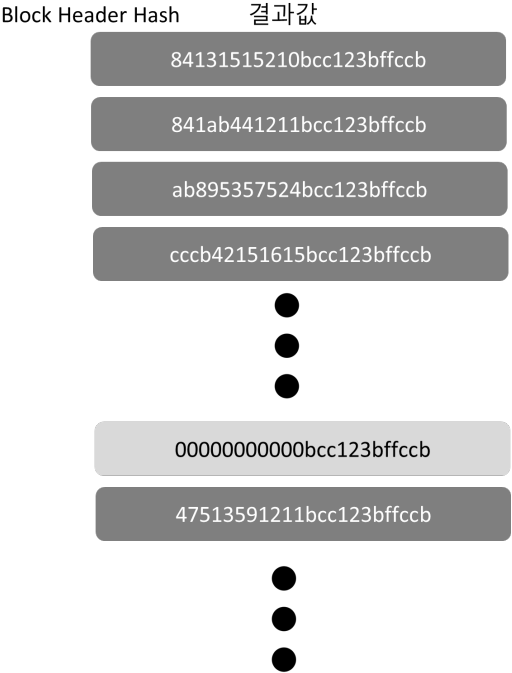
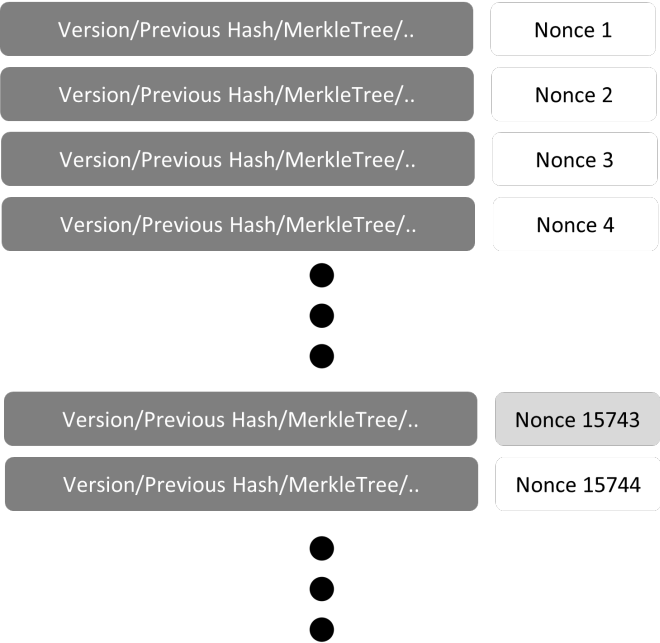
size	Field	설명
4 bytes	Version	버전 정보
32 bytes	Previous Block Hash	이전 Block의 Header Hash
32 bytes	Merkle Root	Transaction들의 Hash Root
4 bytes	Timestamp	블록 생성 시간(UNIX Epoch)
4 bytes	Difficulty Target	PoW의 어려움 정도
4 bytes	Nonce	PoW의 결과(채굴 정답)

Hash 진행

Block Header Hash


00000000000bcc123bffccb

채굴 과정



Network Hash Rate와 Difficulty

- Miner 참여자 수가 증가하고, 성능이 좋은 채굴 장비를 이용하게 되면 채굴의 속도가 점점 빨라진다.
- Difficulty에 따라 Bit(Target)가 조절 되고 정답이 되는 Header Hash의 0의 개수가 늘어난다.

Hash	0000000066f9e170c5e8c33be66566562e044aba689af05a853c8784d28768... 
Confirmations	734,951
Timestamp	2009-03-26 13:14
Height	8727

Hash	000000000000000000000006e5a41436767b3c119d8a0d05f0394b24b26258c62... 
Confirmations	1
Timestamp	2022-07-05 13:17
Height	743677

Find Nonce

Bits = 388618029

Bits(Hex) = 0x1729D72D

Target = 0x29D72D * 2 ** (8 * (0x17 -3))

```
= 0x00000000000000000029D72D0000000000000000000000000000000000000000
```

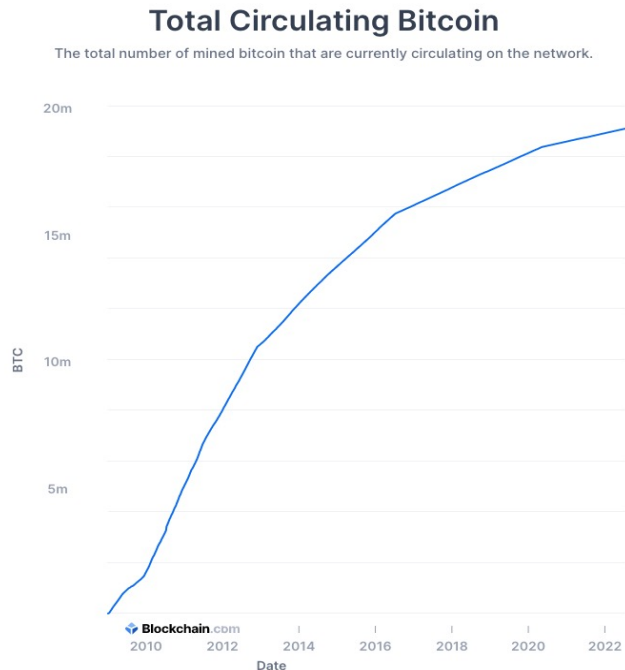
정답 : Header Hash가 Target 보다 작은 값을 만족하는 Nonce를 찾는 것!

이 Difficulty는 Network Hash에 따라 쉬워질 수도 어려워질 수도 있기 때문에 2016 block마다 조정된다.

$$\text{new_difficulty} = \text{old_difficulty} \times (2016 \times 10 \text{ min}) / (\text{실제 } 2016\text{blocks 에 걸린 시간})$$

채굴 보상

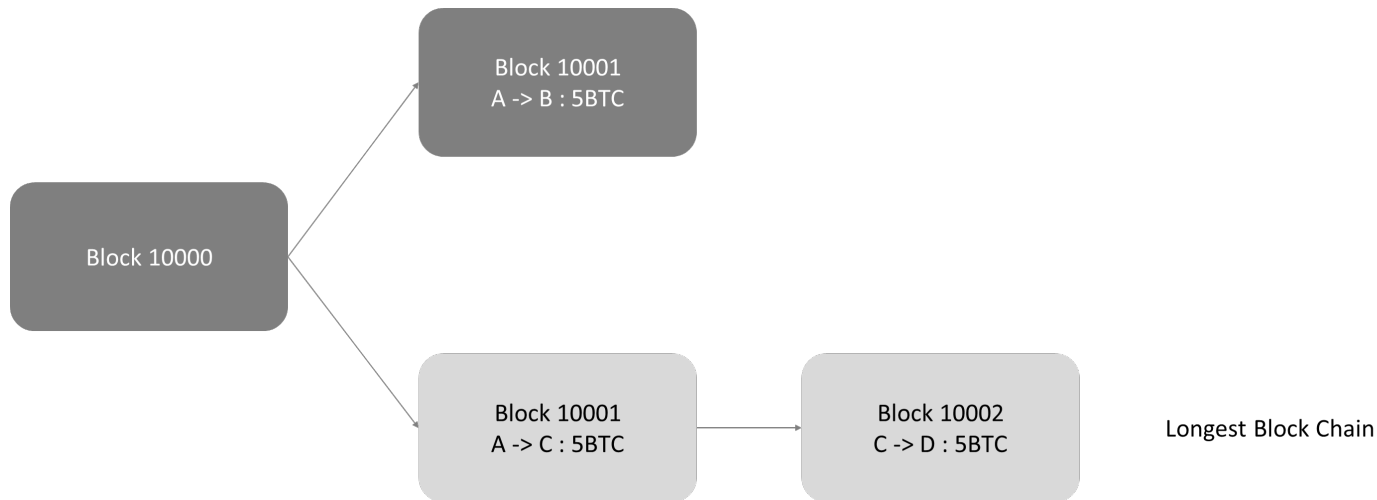
- Block 채굴에 성공하게 되면 Block Reward(신규 발행)와 Transaction Fee를 Coinbase를 통해 채굴자가 얻게 된다.
- Bitcoin 발행량은 2100만개로 제한
- Block Reward는 4년마다 반감기를 통해 보상이 감소
- (50BTC(2009년) → 25 BTC(2013년) → 12.5 BTC(2017년) → 6.25 BTC(2021년) ...
- 2050년 이후로는 블록 신규 발행이 없으므로 채굴자들은 Transaction Fee만 블록 생성 보상으로 가져가게 된다.



(출처: Blockchain.info)

Double Spending Attack(51% Attack)

동일한 UTXO로 두 개의 거래를 생성하고 Fork를 통해서 공격자가 원하는 거래만 블록에 포함되게 하는 공격
공격자가 더 긴 블록체인을 만들기 위해서는 전체 네트워크 HashRate의 51%를 가져야 성공 가능성이 높음

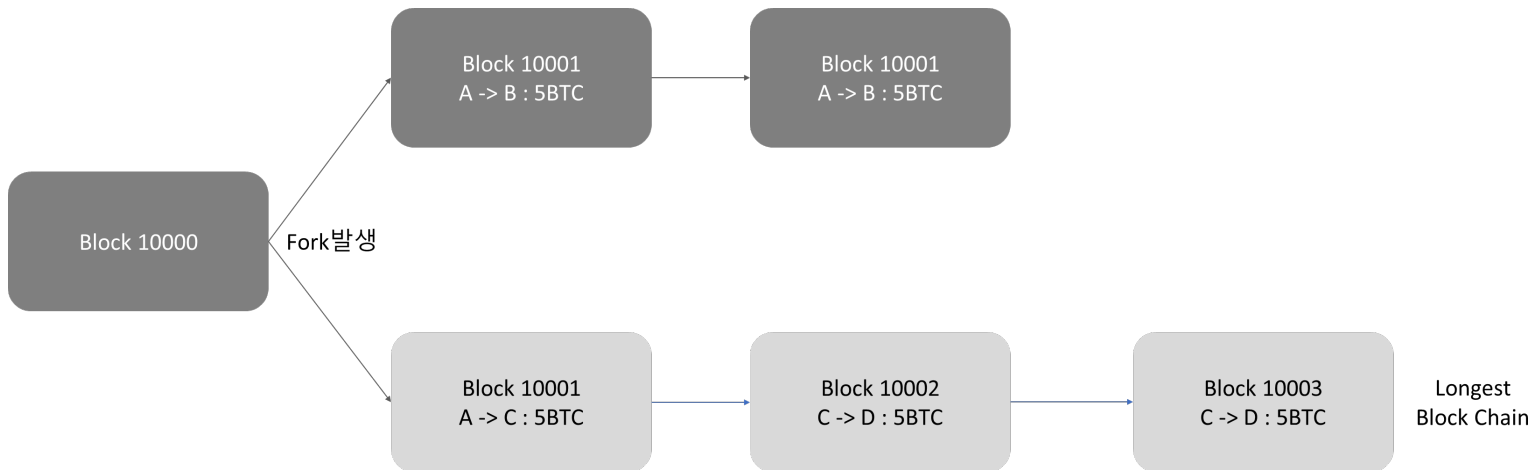


Sybil Attack / DoS(Denial of Service) Attack

- Sybil Attack이란 공격자가 수 많은 노드를 운영하면서 비트코인 네트워크 Block 전파를 방해하거나 잘못된 Block Data를 인접노드들에게 전송하는 공격
 - Sybil Attack 을 하게 된 노드는 비정상적인 행동을 하는 노드로 판단되어 인접 노드들과의 연결이 끊어지게 되고 자연스럽게 Bitcoin 네트워크에서 분리되게 된다.
- DoS Attack 이란 특정 노드들에 비정상적인 거래를 무한정 생성되어 네트워크 전체의 마비를 이르는 공격
 - Bitcoin 에서는 아래와 같은 방법으로 예방
 - 1) 비정상적인 거래, 블록은 전파하지 않음
 - 2) 이중 지불 공격은 전파하지 않음
 - 3) 같은 노드에서 전송된 동일 블록과 거래는 전파하지 않음
 - 4) 아주 작은 단위의 거래를 전송(Mempool Flooding Attack)

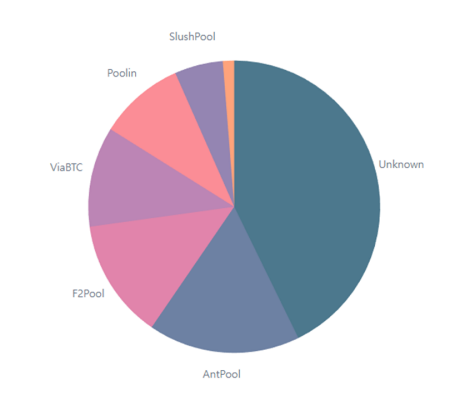
Longest Chain Rule

- Longest Chain Rule은 Bitcoin Network 전체가 Fork가 발생할 때, 하나의 블록체인만을 유지하기 위한 방법
- 실제 Rule은 전체 Blockchain Fork 중 Blockchain 생성에 가장 많은 Computing Power가 사용된 Chain이 Main Chain이 되게 된다.



ASIC과 Mining Pool

- ASIC(Application-specific integrated circuit)이란 특정 용도에 맞게 맞춤 제작된 집적 회로를 의미함
- Proof-of-Work는 Brute Force 방식으로 단순 연산만 이루어지게 됨으로, 이에 맞는 칩을 제작하게 되면 성능이 대폭 향상됨
- 대표적인 ASIC 채굴기인 AntMiner는 13.5 TH/s의 성능을 보여줌(GTX3090 115MH/s)
- Mining Pool은 고성능의 장비를 구매하기 힘든 일반 사용자들이 모여서, 채굴에 참여하기 위해 등장
- BIP-0023으로 제안된 내용
- 현재 대부분의 채굴 순위를 보면 mining pool이 차지하는 중



출처) blockchain.info

Mining Pool

Share

Share는 Mining Pool 내에서의 지분(HashRate) 투입정도를 뜻한다.

Pay-per-Share

항상 Block 채굴 보상에 대해서 지분에 따라 지급하는 방식이다. Mining Pool에 작은 지분으로 참여하여도 보상이 가능하다.

Solo Mining Pool

채굴 가능성이 높은 고HashRate 채굴자들이 선호하는 방식으로 Mining Pool에서 Block을 찾은 miner에게 모든 보상을 제공한다.

Bitcoin Pooled Mining

채굴시 일정 지분 등록을 하고 Mining Pool을 옮겨다니는 Miner의 혜택을 제하기 위해서 블록 보상 후 Submit한 share를 확인 후에 share만큼 보상을 지급한다.