

한 번에 끝내는 블록체인 개발 A to Z

Chapter 1

Blockchain 1.0 - Bitcoin

Chapter 1

Blockchain 1.0 - Bitcoin

Block Structure

Block 구조

Size	Field	설명
4 bytes	Block Size	Block의 크기
80 bytes	Block Header	Block Header 정보
1-9 bytes	Transaction Counter	현재 블록 내 Transaction 개수
Variable	Transaction	블록 내 Transaction 리스트

Block Header 구조

Size	Field	설명
4 bytes	Version	버전 정보
32 bytes	Previous Bloc 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)

Genesis Block

Genesis Block은 Block의 최초 검증 데이터로
Genesis Block이 다르게 되면
그 뒤에 연결되는 모든 Blockchain 데이터
검증이 불가능하다.

Block 0

USD BTC

This block was mined on January 04, 2009 at 3:15 AM GMT+9 by [Unknown](#). It currently has 745,725 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 50.00000000 BTC (\$1189,233.00). The reward consisted of a base reward of 50.00000000 BTC (\$1,189,233.00) with an additional 0.00000000 BTC (\$0.00) reward paid as fees of the 1 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this [address](#).

A total of 0.00000000 BTC (\$0.00) were sent in the block with the average transaction being 0.00000000 BTC (\$0.00). Learn more about [how blocks work](#).

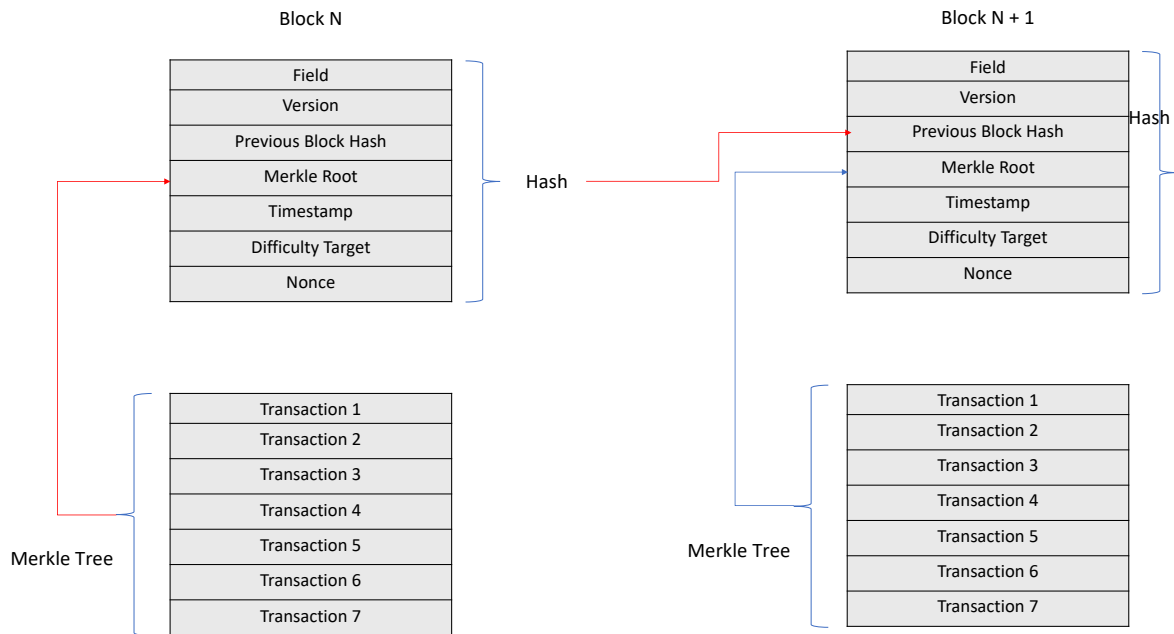
Hash	00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Confirmations	745,725
Timestamp	2009-01-04 03:15
Height	0
Miner	Unknown
Number of Transactions	1
Difficulty	1.00
Merkle root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Version	0x1
Bits	486,604,799
Weight	1,140 WU
Size	285 bytes
Nonce	2,083,236,893
Transaction Volume	0.00000000 BTC
Block Reward	50.00000000 BTC
Fee Reward	0.00000000 BTC

(출처: blockchain.com)

Block 생성



Block 연결 방법



Block Size

현재 기준 Bitcoin 전체 Blockchain Size 는 약 400GB

1개의 Block의 최대 크기는 1MB (1MB 초과는 Witness Data)

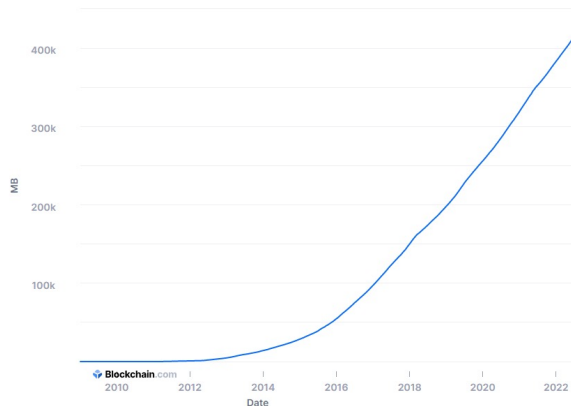
Blocks

validated Bitcoin network transactions.

Height	Hash	Mined	Miner	Size
743565	0..5b39cfe28a01b1054fead102ef1af6bfd221a87ebdb42	33 minutes	Unknown	627,880 bytes
743564	0..83941dcd93e53ecffc35cbdea830be86ba8db67800405	36 minutes	ViaBTC	382,699 bytes
743563	0..3d44a9400ee5a45bfade6dc16bfb0fb6c0426887ab31f	39 minutes	F2Pool	1,098,891 bytes
743562	0..10e7d73d189b931b83d4cd824ba3e8d0cbb29616bde77	51 minutes	SlushPool	1,573,611 bytes

Blockchain Size (MB)

The total size of the blockchain minus database indexes in megabytes.



(출처: blockchain.com)

Bitcoin에서 Block 크기의 제한과 채굴

Bitcoin 에서 Block 크기의 제한을 둔 이유

- Transaction을 처리하기 위한 Database Lock의 성능 때문
 - 이로 인해 1Block 내에 약 2000개의 Tx만 들어가게 됨(3-7 tps)
 - 채굴자들은 이런 Block 크기의 제한으로 인해 거래 수수료를 최대한을 많이 얻는 방법을 구현
 - 수수료가 비싸거나 거래 데이터 용량이 작은 거래만 선택
 - Bitcoin 사용자가 늘어나며, 수수료 가격 증가 (Bitcoin 가격 증가로 인해 더 폭등)
 - 2017년 Hard Fork(Segwit)