Block Header and Mining

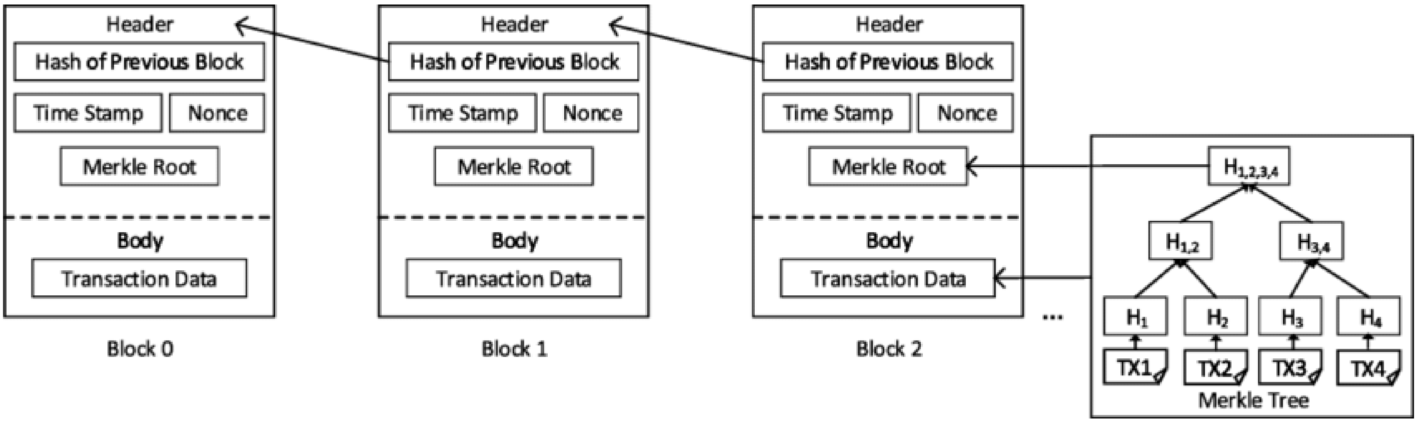
Table of Content

To understand how blockchain creation happens we will first look at what the structure of a Block is like.

Block and Structure of Block

Block in a Blockchain–

- Blockchain is a linear chain of blocks.
- Each block contains a set of transactions and other essential details.
- Blocks are linearly connected and cryptographically secured.
- Each block header contains the previous block hash, current block hash, nonce, Merkle root, and other details.
- For adding a new block to the network, the blockchain follows consensus mechanisms like proof of work (PoW), proof of stake (PoS), etc.



1. Block Header

The Block header is an 80-Byte field that contains the metadata – the data about the block. 6 components of the Block Header are:

- Timestamp:

In blockchain, a timestamp is a crucial component of a block's header. It represents the exact time when a block is created and added to the blockchain. The timestamp is fundamental for several reasons:

a. **Ordering Transactions:** It helps in maintaining the chronological order of transactions within the block. This chronological order is critical for ensuring the integrity and consistency of the blockchain.

b. **Preventing Tampering:** The timestamp, when combined with other block information, contributes to the block's unique hash. Any alteration in the block's content or sequence of transactions would change the hash, making tampering evident.

c. **Difficulty Adjustment:** Some blockchain protocols, like Bitcoin, use timestamps to adjust the difficulty level of mining. The time taken to mine a block influences the complexity of the mathematical puzzles miners need to solve. The timestamp helps regulate this difficulty to ensure a consistent block creation rate.

d. **Network Synchronization:** Timestamps facilitate network synchronization across different nodes in the blockchain network. Nodes use these timestamps to align and verify the correct order of transactions and blocks.

It's important to note that timestamps in blockchain are not just regular time indicators but are often subject to specific rules or protocols within the blockchain network. For instance, there might be rules about how much time can elapse between blocks or rules to prevent nodes from manipulating timestamps for their advantage.

- **Version** – It’s a 4-bytes field representing the version number of the protocol used. Usually, for bitcoin, it’s ‘0x1’.

- **Previous Block Address/ Hash:** It is used to connect the i+1th block to the ith block using the hash. In short, it is a reference to the hash of the previous (parent) block in the chain.

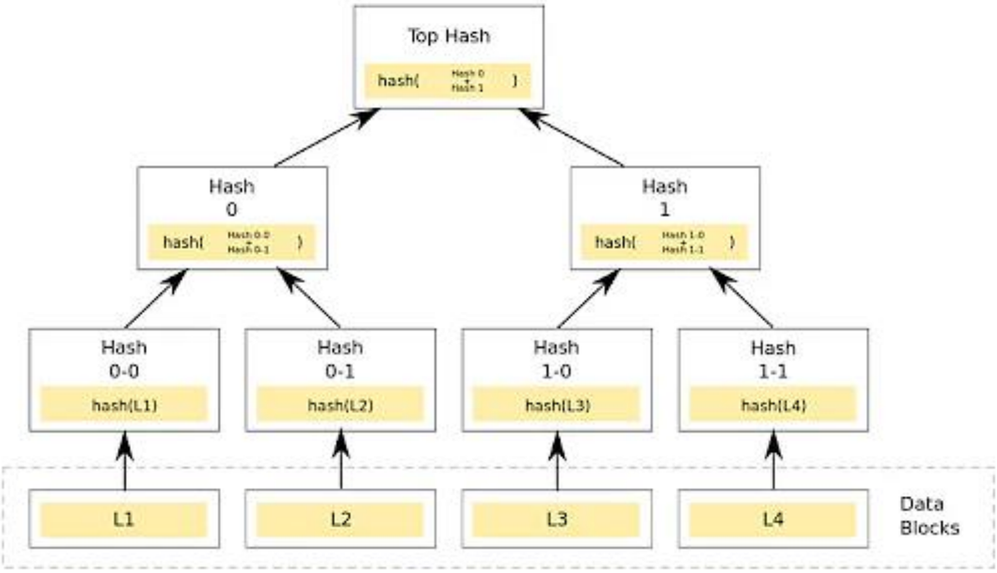
- **Bits** – It’s a 4-bytes field that tells the complexity to add the block. It’s also known as “difficulty bits.” According to PoW, the block hash should be less than the difficulty level.

- **Nonce** –

    - ➢ It’s a 4-bytes field that contains a 32-bit number. These are the only changeable element in a block of transactions. In PoW, miners alter nonce until they find the right block hash.
    - ➢ A Nonce is a random number that is appended to a block of data before it is hashed in the context of blockchain. Miners use this attribute to validate transactions and produce new blocks since the inclusion of the Nonce alters the data’s hash. It ensures that a block’s hash is distinct and deters bad actors from altering the blockchain, as it is only ever used once.
    - ➢ To expand further, the word “Nonce” in the blockchain comes from the phrase “number used once.” Miners must constantly change the Nonce value until they find a hash that satisfies the precise specifications of the network in order to solve the difficult mathematical calculations that are necessary to validate transactions

and create new blocks. The proof-of-work (PoW) consensus mechanism used in this procedure makes sure that miners are compensated for their computational work and that the network is safe.

- **Merkle Root**
    - ➢ A 32-bytes field containing a 256-bit root hash. It's constructed hierarchically combining hashes of the individual transactions in a block.
    - ➢ Merkle trees, also known as Binary hash trees, are a prevalent sort of data structure in computer science.
    - ➢ In bitcoin and other cryptocurrencies, they're used to encrypt blockchain data more efficiently and securely.
    - ➢ It's a mathematical data structure made up of hashes of various data blocks that summarize all the transactions in a block.
    - ➢ It also enables quick and secure content verification across big datasets and verifies the consistency and content of the data.



2. Block Height –

It's the sequence number of the block in the chain of blocks. Block Height: 1 is the genesis block (first block in the network).

3. Block Size –

It's a 4-bytes or 32-bit field that contains the size of the block. It adds size in Bytes. Ex – Block Size: 216 Bytes.

4. Block Reward –

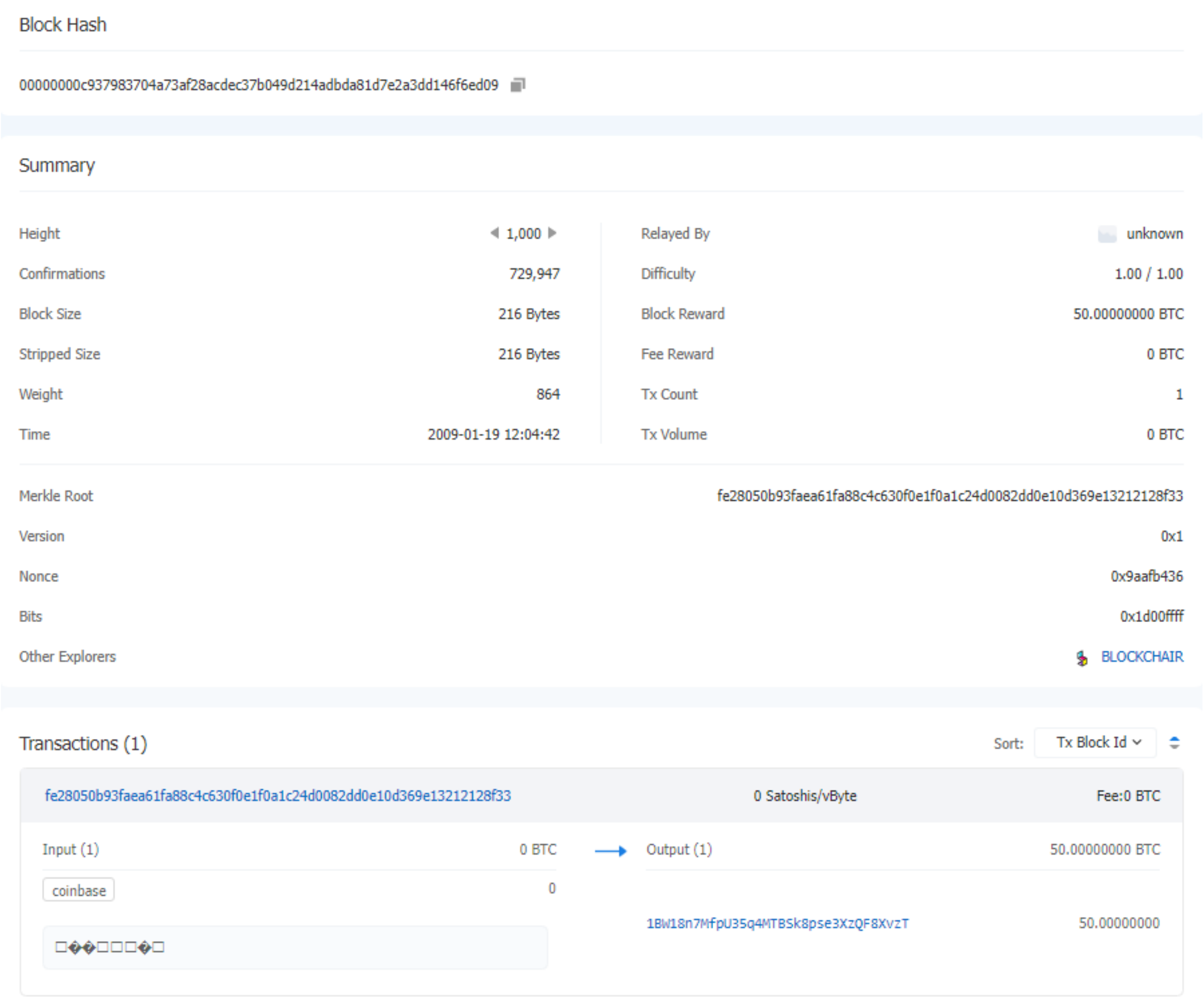
This field contains the amount rewarded to the miner for adding a block of transactions.

5. Tx Count –

The transaction counter shows the number of transactions contained by the block. The field has a maximum size of 9 bytes.
Transactions

It’s a variable-size field that includes the list of all transactions contained in the block.

FYI, each bitcoin block contains about 2000 transactions. The size of each block is approx 1MB. The size and number of transactions in a block vary in blockchains. It’s decided based on network congestion and communication overhead.
Let’s see what an actual bitcoin block looks like. This image contains a block summary of a transaction.



Block Hash

00000000c937983704a73af28acdec37b049d214adbda81d7e2a3dd146f6ed09

Summary

Height	◀ 1,000 ▶	Relayed By	unknown
Confirmations	729,947	Difficulty	1.00 / 1.00
Block Size	216 Bytes	Block Reward	50.00000000 BTC
Stripped Size	216 Bytes	Fee Reward	0 BTC
Weight	864	Tx Count	1
Time	2009-01-19 12:04:42	Tx Volume	0 BTC

Merkle Root	fe28050b93faea61fa88c4c630f0e1f0a1c24d0082dd0e10d369e13212128f33
Version	0x1
Nonce	0x9aafb436
Bits	0x1d00ffff
Other Explorers	BLOCKCHAIR

Transactions (1)

fe28050b93faea61fa88c4c630f0e1f0a1c24d0082dd0e10d369e13212128f33 0 Satoshis/vByte Fee:0 BTC

Input (1)	0 BTC	Output (1)	50.00000000 BTC
coinbase	0	1BW18n7MfpU35q4MTBSk8pse3XzQF8XvzT	50.00000000
□��□□□�□			

Blockchain Explorer: https://btc.com/btc/block/1000

Transaction Inclusion

Transactions are included in a block based on specific criteria to ensure the integrity, security, and efficiency of the blockchain network. The criteria for transaction inclusion typically involve the following aspects:

- **Validity:**

Transactions must be valid according to the network's protocol. This involves checking if the transaction adheres to the rules of the blockchain (e.g., correct format, digital signatures, correct inputs and outputs for the transaction).

- **Sufficient Fees:**
  Many blockchain networks prioritize transactions based on the fees attached to them. Transactions offering higher fees are often processed more quickly as an incentive for miners to include them in the next block.
- **Space Availability:**
  Each block has a limited capacity for transactions due to block size constraints. Transactions compete for space within a block. Transactions with higher fees per byte or those that optimize space usage (smaller in size) are preferred for inclusion.
- **Non-Conflicting Transactions:**
  Conflicting transactions (e.g., double-spending attempts) or transactions that reference the same input cannot be included together in a block. Miners typically prioritize the transaction that appeared first or the one with higher fees.
- **Priority of Transactions:**
  Some networks might give priority to certain types of transactions or transactions from specific addresses (e.g., network-based rules or protocols might favor transactions related to smart contracts, network governance, etc.).

How do you create a block?

Block mining process

To create a new block, miners must go through a process to solve a math problem. When finding a valid solution for the network, a new block can be taken for granted that will be added to the blockchain by consensus. And for which, the miner who found the solution, will receive a reward for the new block. This reward is known as the block reward.

A new Bitcoin block is generated approximately every 10 minutes. So, every time one is found, it means the start of mining for another. Since these are mathematically related or chained together. But let's see in more detail how this process is performed:

- **First stage: Transaction**
  The process of mining a new block starts when a user wants to send a certain amount of cryptocurrency to another person. So send bliss transaction with the data from your wallet, waiting for the network to do and confirm. They remain there until a block is mined where they can be included and validated.

- **Second stage: Compilation**
  These pending transactions on the network are collected and grouped into a block of transactions by mining nodes. Multiple miners are likely to collect the same transactions. And they will all be unconfirmed until the block is mined.

- **Third stage: Training**
  Each miner will select the transactions they want to include and build their own block. If there are transactions already validated and included in the previous block, they will be removed from this one. This new block is known as a candidate, since it is not yet valid because it does not have a valid proof of work.

  In the formation of this new block, a header must be included that contains the hash from the previous block, the merkle root and data for mining competition. I mean, the timestamp, the objective of the algorithm of PoW for that block (the bits), the software version and the nuncio.

- **Stage Four: Proof of Work**

  Once each miner has formed their own transaction block, they will need to find a valid signature for that block. In other words, carry out a proof of work. Each miner must carry out a mathematical calculation process that is unique to each block they formed. So, although the procedure is the same, the result will be totally different for each one. This complex calculation involves a lot of computational power, and therefore, a large expenditure of electrical energy. Which will also depend on the system difficulty for the time of mining.

  The solution miners must find is known as hash. This function is very difficult to find, but once found, it is easy to verify by others nodes. So that they can verify that the output hash complies with the established system conditions.

  To find a valid output hash, the miners perform the mathematical calculations repetitively over and over again using a nuncio. Which is a random number that they use and constantly change until they find an output signature or hash that is valid based on the condition. There is no way to predict which nonce will solve the problem, so they must use as many as necessary. And we are talking about billions of values! Incredible, right?

  In the case of the Bitcoin network, the system determines that the output hash must contain a certain number of zeros at the beginning of the hash.

- **Fifth stage: Transmission**

  When a mining node manages to find a valid output hash for a block, it transmits that block together with the signature to the other nodes in the network so that they can validate it.

  At this time, as long as the 21 million bitcoins have not been issued, the miner receives the reward established for mining, putting new bitcoins into circulation. This is registered on its own node, the other nodes on the network will do so in the next step.

  In addition, regardless of whether all the bitcoins have been issued or not, the miner also receives all the mining commissions that users have put in the transactions that make up this block.

- **Sixth stage: Verification**

  The other nodes in the network are in charge of validate and verify that the block and hash meet the system conditions, verifying its legitimacy and if it actually contains the stated number of zeros.

  Here also the proof of work is confirmed, that is, the computational power spent to find the solution, and it is noted that the miner who discovered the block can effectively make use of the recently received bitcoins.

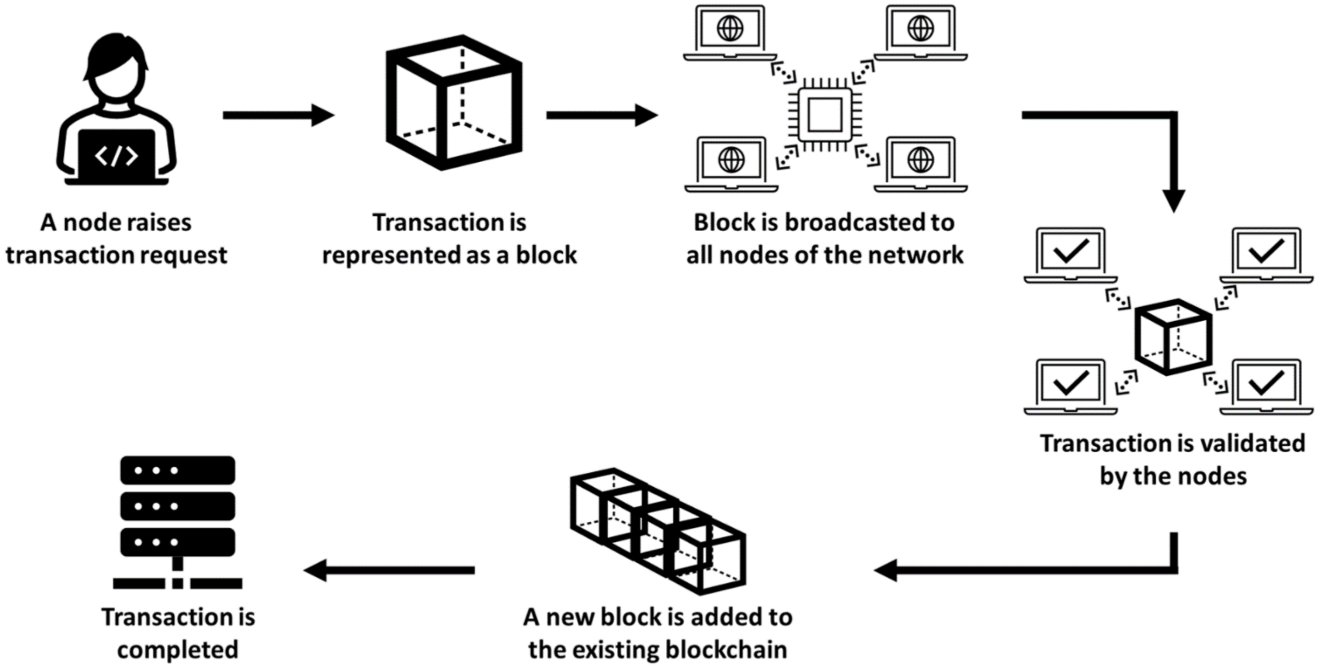
- **Seventh stage: Confirmation**

  Once the new block is added to the blockchain, all the others that are added on top of it will count as a confirmation. At this point, we can come to think that since each miner started the process with their own block, they can continue mining. But it's not like that. Once a block is generated, all mining nodes must start the process by forming a new block of transactions. They cannot continue mining the previous block because each block must add the output hash of the block that precedes it.

This is why we know this technology as a chain of blocks or blockchain. Then, by the time the miner gets a valid hash, another number of new blocks may have been mined. So the output hash of your mined block will not match the output hash of the last added block in the chain. It will be rejected.

In addition, it is very likely that all or most of the transactions included in that block have already been added to others. Even if you succeed in mining the block most of your included transactions will not be able to be validated or confirmed.

https://www.youtube.com/watch?v=WmugrLm2wd0


A node raises transaction request
Transaction is represented as a block
Block is broadcasted to all nodes of the network
Transaction is validated by the nodes
A new block is added to the existing blockchain
Transaction is completed