perplexity

What Is Blockchain?

A **blockchain** is a decentralized, distributed digital ledger that records transactions across a network of computers. Each record is grouped into a "block," and these blocks are linked together in chronological order using cryptographic hashes. This structure ensures that once data is recorded, it is extremely difficult to alter, making the blockchain secure, transparent, and immutable.

- **Example:** Imagine a public notebook where everyone can write transactions, and each page is glued to the previous one. Changing one page would require changing all subsequent pages, making tampering nearly impossible.

What Is a Block?

A **block** is a fundamental unit of a blockchain. Each block contains:

- A batch of validated transactions
- A timestamp
- A cryptographic hash of the previous block
- A nonce (for mining)
- Other metadata

Blocks are chained together, ensuring the integrity of the entire ledger.

- **Example:** Each block is like a page in a ledger, listing recent transactions and referencing the previous page.

What Are Transactions?

A **transaction** is an action recorded on the blockchain, such as transferring cryptocurrency from one user to another. Transactions are grouped into blocks and validated by the network before being permanently added to the blockchain.

- **Attributes:** Sender and recipient addresses, amount, transaction fee, unique identifier (hash).
- **Example:** Alice sends 1 Bitcoin to Bob; this transaction is included in a block and becomes part of the permanent record.

What Is a Smart Contract?

A **smart contract** is a self-executing program stored on the blockchain. It automatically enforces and executes the terms of an agreement when predefined conditions are met—without needing intermediaries.

- **Bitcoin Smart Contracts:** Bitcoin supports smart contracts through a scripting language called Script, which is intentionally simple. Common uses include:
  - **Multisignature transactions:** Require multiple parties to sign before funds are spent.
  - **Time-locked transactions:** Funds can only be spent after a certain time or block height.
- **Example:** A business sets up a contract that requires both the CEO and CFO to approve a transaction before it is processed[1] [2].

What Is Bitcoin?

Bitcoin is the first widely adopted cryptocurrency, enabling peer-to-peer digital payments without banks or intermediaries. Its blockchain is decentralized, with no single entity in control, and its supply is capped at 21 million coins.

- **Example:** You can use Bitcoin to pay for goods or transfer value globally.

How Many Transactions Does Bitcoin Have?

As of July 11, 2025, the Bitcoin network processed approximately **408,758 transactions per day**[3] [4]. This number fluctuates with network activity.

- **Example:** On some days, Bitcoin has processed over 600,000 transactions[3].

How Many Nodes Does Bitcoin Have?

As of 2025, there are about **18,500 full nodes** running on the Bitcoin network[5]. Nodes are computers that store and update the blockchain, validate transactions, and help maintain the network's decentralization and security.

- **Example:** Each node independently verifies all transactions and blocks, ensuring no single point of failure[5].

What Does "10 Minutes" Mean in Bitcoin?

Bitcoin is designed so that a new block is added to the blockchain roughly every **10 minutes**. This interval, called the **block time**, balances security and transaction throughput.

- **Example:** If you send a Bitcoin transaction, it is usually confirmed within about 10 minutes[6] [7].

What Is Hashing?

Hashing is the process of converting input data of any size into a fixed-length string using a mathematical algorithm (hash function). In Bitcoin, SHA-256 is used. Hashing links blocks together and secures data integrity. Even a small change in input creates a drastically different hash.

- **Example:** Hashing the word "hello" with SHA-256 produces a unique 256-bit string[8] [9].

What Is Mining?

Mining is the process by which new blocks are added to the blockchain. Miners collect pending transactions, bundle them into a block, and compete to solve a complex mathematical puzzle (finding a valid hash). The first miner to solve it broadcasts the block to the network for verification and inclusion.

- **Example:** Miners try different values (nonces) until the block's hash meets the required criteria[10].

What Do Miners Get?

Miners are rewarded with:

- **Newly minted bitcoins** (block reward)
- **Transaction fees** from the transactions included in the block

As of July 2025, the reward per block is **3.125 BTC**, plus transaction fees[4] [11].

- **Example:** If transaction fees total 0.03 BTC, a miner earns 3.155 BTC for mining a block.

What Is a Nonce?

A **nonce** (number used once) is a variable in the block header that miners change to try to find a hash meeting the network's difficulty requirement. It is essential for mining.

- **Example:** A miner starts with nonce = 0, hashes the block, checks if it meets the target, and increments the nonce until successful[12] [13].

Why Is the Nonce Required?

The nonce allows miners to generate new hashes for the same block data, enabling the trial-and-error process of mining. Without a nonce, miners would have only one chance per block, making mining impossible.

Can Miners Precompute Nonce of Leading Zeros?

No, miners **cannot precompute** nonces that will result in hashes with leading zeros. The SHA-256 hash function is designed to be unpredictable and one-way, so the only way to find a valid nonce is by brute-force—trying different values until the hash meets the difficulty target[12] [13].

- **Example:** There is no shortcut; miners must try billions of nonces per second.

What Is SHA?

SHA stands for **Secure Hash Algorithm**. Bitcoin uses **SHA-256**, producing a 256-bit fixed-length hash. SHA-256 is cryptographically secure, one-way, and collision-resistant, making it essential for blockchain security[8] [9].

- **Example:** SHA-256("blockchain") produces a unique 256-bit hash.

What Is Proof of Work?

Proof of Work (PoW) is a consensus mechanism requiring miners to solve computationally difficult puzzles to add a new block. This process secures the network, prevents spam and attacks, and ensures only valid transactions are recorded.

- **Example:** In Bitcoin, PoW means finding a nonce so that the block's hash is below a certain target (starts with a set number of zeros)[10] [14].

Summary Table

Concept	Definition & Example
Blockchain	Decentralized ledger of blocks; e.g., Bitcoin's transaction record
Block	Group of transactions with hash link to previous block
Transaction	Action like sending Bitcoin from Alice to Bob
Smart Contract	Self-executing code; e.g., multisig or time-locked transactions on Bitcoin
Bitcoin	First cryptocurrency; capped at 21 million coins
Transactions/day	~408,758 on July 11, 2025
Nodes	~18,500 full nodes in 2025
10 Minutes	Average time to add a new block in Bitcoin
Hashing	Converts data to fixed-length hash (SHA-256)
Mining	Adding new blocks by solving puzzles; miners earn rewards
Miner Rewards	Block reward (3.125 BTC) + transaction fees
Nonce	Value miners change to find valid hash
Why Nonce Needed	Enables repeated hash attempts for mining
Precompute Nonce?	Not possible due to hash unpredictability
SHA	Secure Hash Algorithm, used for hashing in Bitcoin
Proof of Work	Requires solving puzzles to add blocks, secures the network

⁂

1. https://www.blockchain-council.org/cryptocurrency/bitcoin-smart-contracts/
2. https://river.com/learn/what-are-bitcoin-smart-contracts/

3. https://ycharts.com/indicators/bitcoin_transactions_per_day
4. https://bitinfocharts.com/bitcoin/
5. https://pocketoption.com/blog/en/knowledge-base/learning/how-many-bitcoin-nodes-are-there/
6. https://www.linkedin.com/pulse/why-block-time-bitcoin-10-mins-introduction-pow-1-tara-annison
7. https://www.nadcab.com/blog/block-time-in-bitcoin
8. https://www.youtube.com/watch?v=FJUacc_tw-M
9. https://komodoplatform.com/en/academy/sha-256-algorithm/
10. https://strike.me/learn/what-is-proof-of-work/
11. https://bitbo.io/tools/mining-profitable/
12. https://pmc.ncbi.nlm.nih.gov/articles/PMC8946996/
13. https://www.investopedia.com/terms/n/nonce.asp
14. https://www.investopedia.com/terms/p/proof-work.asp