Market Talks
EDUCATION CENTER

BLOCKCHAIN · BEGINNER · LESSON 6 OF 13

Blocks and Hashing, Explained Simply

The short codes that hold the chain together, what a block really contains, and why mining is a giant guessing game

7 min read 6 quiz questions with answer key

BLOCKCHAIN · BEGINNER · LESSON 6 OF 13

Blocks and Hashing, Explained Simply

IN ONE SENTENCE

A hash is a short code calculated from any piece of data. Change the data even slightly and the code changes completely. Each block stores the hash of the block before it, so editing old history breaks every link that follows.

A short code that stands for any data

In Lesson 3 we said that each record in a chain carries a digital fingerprint of the one before it. That fingerprint has a proper name: a **hash**.

A **hash function** is a calculation that takes any data, a word, a contract or an entire block of transactions, and turns it into a short code of fixed length. Bitcoin's hash function is called **SHA-256**. Its result is always 64 characters made of the digits 0 to 9 and the letters a to f. It does not matter whether the input is one word or a whole library. The result is always 64 characters.

Any computer can calculate a hash in a fraction of a second, and everyone who hashes the same data gets exactly the same result. That makes a hash a quick way to check whether two copies of something are identical without comparing them line by line.

TRY IT WITH OUR NAME

Here is the SHA-256 hash of the text *Market Talks*:

`16e127cc0d60a230a1f1f80040012fc10164f835b2a99ab8f42b2ea457d9964c`

And here is the hash of *Market talks*, with only one letter changed to lowercase:

`79eaca857fb12aa6db2d1ab5c896ae9a3241eb2c96f99dd0640f2c6517a5a972`

One small change, and nothing in the result looks related. You can check these yourself with any free online SHA-256 tool.

Four things a good hash function guarantees

- **Same input, same output.** The same data always produces the same hash, on any computer, anywhere in the world.
- **Tiny change, totally different output.** Changing a single character scrambles the whole result, as the example above shows. This is called the **avalanche effect**.

- **One-way only.** Going from data to hash is easy. Going from a hash back to the original data is practically impossible. The only way to find an input that matches a hash is to guess again and again.
- **No two alike in practice.** In theory two different inputs could share a hash, but with SHA-256 nobody has ever found such a pair. The number of possible results has 78 digits, roughly as many as the estimated number of atoms in the observable universe.

Together, these four rules mean a hash can act as a seal on data. If the hash still matches, the data has not changed. If it does not match, something was altered, even if it was a single comma.

> **ANALOGY: THE SMOOTHIE**
>
> Put a banana, some milk and five strawberries in a blender. Anyone with the same recipe gets the same smoothie. Add one extra strawberry and the taste changes. But nobody can pour a smoothie back into a whole banana and five separate strawberries. A hash works the same way: easy to make, sensitive to every ingredient, and impossible to reverse.

What a block holds

A Bitcoin block has two parts. The larger part is the **body**: a list of transactions, usually a few thousand of them. The smaller part is the **header**, a short summary that includes:

- **The previous block's hash.** This is the link that makes it a chain.
- **A summary of all its transactions.** The transactions are hashed together into a single code, so changing any one of them changes the summary. The Intermediate level shows exactly how this summary is built.
- **A timestamp** showing roughly when the block was created.
- **The difficulty target**, which sets how hard the mining puzzle is at the time.
- **A nonce**, a number miners change again and again while they search for a valid block. More on this below.

The block's own hash is calculated from its header. Because the header contains both the summary of transactions and the previous block's hash, that one code depends on everything in the block and everything before it.

How hashes lock the chain

Now the pieces fit together. Block 102 stores the hash of block 101. Block 103 stores the hash of block 102. And so on, all the way back to the genesis block.

Suppose someone edits a single transaction in block 101. Its transaction summary changes, so its hash changes. But block 102 still stores the old hash, so the link between them no longer matches, and every node can see it immediately.

To hide the edit, the attacker would have to recalculate block 101, then block 102, then every block after it. And as the next section shows, producing each of those blocks requires an enormous amount of guessing. Meanwhile, the honest network keeps adding new blocks on top. This is why a payment becomes safer with every block added after it.

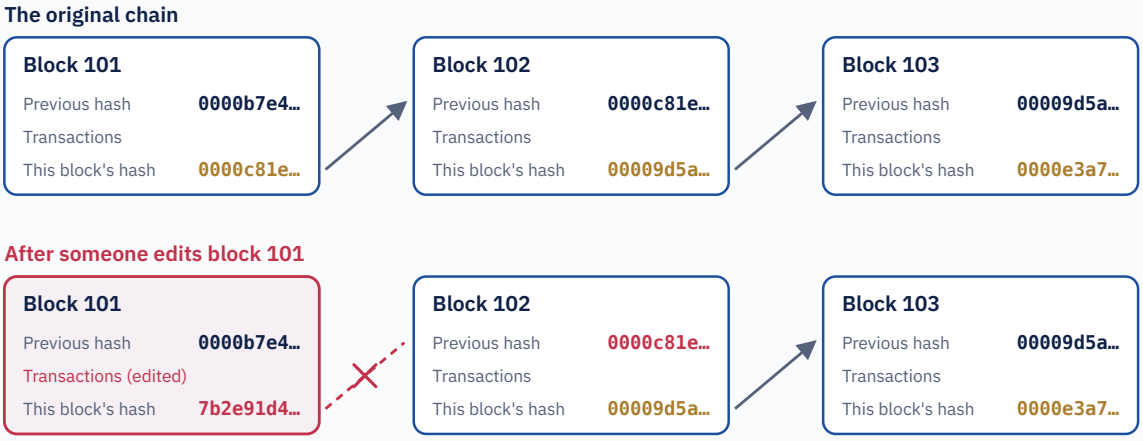


Figure 1. Each block stores the hash of the block before it. Editing block 101 changes its hash, so the link to block 102 no longer matches, and everyone can see the chain was tampered with.

Mining: a giant guessing game

Lesson 4 said miners race to solve a puzzle. Here is what that puzzle actually is. For a block to be valid, its hash must be below a target number set by the network, which in simple terms means the hash must start with a certain number of zeros.

Because hashes are one-way, there is no clever way to produce a hash with many zeros. Miners change the nonce, hash the header, check the result, and try again, billions of times per second. Each extra zero required makes the search about 16 times harder.

We ran this experiment ourselves, hashing *Market Talks* followed by a counting number until the result started with enough zeros:

Zeros required	Guesses it took us	Average guesses expected
1	15	16
2	262	256
3	5,931	4,096
4	120,539	65,536
5	129,996	1,048,576
6	13,591,130	16,777,216

Notice the five-zero row: we got lucky. Mining is a lottery, and any single guess can win. But on average, the work grows fast. Bitcoin's very first block needed a hash starting with 10 zeros. Blocks today need about 19 or 20, which is why the whole network now makes around a billion trillion guesses every second.

Why this matters for traders

- **Every transaction has a hash too.** It is called the **transaction ID**, or TXID. When an exchange or a counterparty says a payment has been sent, ask for the TXID and look it up on a block explorer. It shows whether the transaction exists, how much was sent and how many new blocks now sit on top of it.
- **Hashrate is a health signal.** Hashrate is the total number of guesses the network makes per second. Bitcoin's hashrate first passed one zettahash per second, a 1 followed by 21 zeros, in April 2025. A rising hashrate means miners are investing in the network. A sudden drop, like when a US winter storm forced miners to switch off a large share of machines in January 2026, can put miners under pressure.
- **Stressed miners can become sellers.** Miners pay for electricity and machines, often by selling the bitcoin they earn. When their income falls, some sell more or shut down. That is why some traders follow hashrate-based indicators alongside price charts.

Key terms

Hash	A short, fixed-length code calculated from any data. The same data always gives the same hash.
SHA-256	The hash function Bitcoin uses. Its results are always 64 characters long.

Avalanche effect	The property that a tiny change in the input produces a completely different hash.
Block header	The short summary at the top of a block. It holds the previous block's hash, a summary of transactions, a timestamp and the nonce.
Nonce	A number miners change repeatedly while searching for a block hash that meets the target.
Hashrate	The total number of hash guesses the network makes per second. A common measure of mining power.

Key takeaways

1. A hash is a short, fixed-length code calculated from any data. Bitcoin relies on SHA-256, whose results are 64 characters long.
2. Good hashes are consistent, change completely with any edit, cannot be reversed and do not repeat in practice.
3. A block has a body of transactions and a header that includes the previous block's hash and a summary of its transactions.
4. Because each block stores the hash of the one before, editing an old block breaks every link after it.
5. Mining means guessing nonces until the block hash starts with enough zeros, and each extra zero makes the search about 16 times harder.

Test yourself

Circle one answer for each question. The answer key with explanations is on the next page. You can also take this quiz online at markettalks.info and see your score instantly.

1. What does a hash function do?

- (A) It encrypts data so only the owner can read it
- (B) It turns any data into a short code of fixed length
- (C) It compresses files so they take up less space
- (D) It stores transactions in a database

2. You change one letter in a document and hash it again. What happens to the hash?

A It changes by one character
B It stays the same
C It becomes completely different
D It becomes longer

3. Why can't someone work backwards from a hash to the original data?

A Hash functions are one-way, so the only option is guessing
B The hash is kept secret by the network
C The original data is deleted after hashing
D Only miners have the key to reverse it

4. What links one block to the block before it?

A The same miner creates both blocks
B Both blocks have the same timestamp
C Both blocks contain the same transactions
D Each block's header stores the previous block's hash

5. What is the nonce?

A The reward a miner receives
B A number miners keep changing while searching for a valid block hash
C The ID of a transaction
D The number of transactions in a block

6. What happens to the mining search each time one more leading zero is required?

A It becomes twice as hard
B It does not change
C It becomes about 16 times harder
D It becomes easier

Answer key

1 B

It turns any data into a short code of fixed length

A hash function calculates a short, fixed-length code from any input. With SHA-256, the result is always 64 characters, whatever the size of the input.

2 C

It becomes completely different

This is the avalanche effect. Any change, however small, scrambles the whole result, which makes even tiny edits easy to detect.

3 A

Hash functions are one-way, so the only option is guessing

Hashing is easy in one direction and practically impossible in reverse. That is exactly why mining has to be done by trial and error.

4 D

Each block's header stores the previous block's hash

Each header includes the previous block's hash. If an old block is edited, its hash changes and no longer matches what the next block stores.

5 B

A number miners keep changing while searching for a valid block hash

Miners change the nonce, hash the header and check the result, again and again, until the hash starts with enough zeros.

6 C

It becomes about 16 times harder

Each character of a hash can be one of 16 values, so requiring one more zero makes a valid result about 16 times rarer.

SOURCES

- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008): https://bitcoin.org/bitcoin.pdf
- NIST, FIPS 180-4 Secure Hash Standard (SHA-256): https://csrc.nist.gov/files/pubs/fips/180-4/final/docs/fips180-4.pdf
- Forklog, Bitcoin hashrate surpasses one zettahash for the first time (April 2025): https://forklog.com/en/bitcoin-hashrate-surpasses-one-zettahash-for-the-first-time/
- KuCoin, Bitcoin hashrate in 2026: trends, mining difficulty and network security: https://www.kucoin.com/blog/in-bitcoin-hashrate-in-2026-latest-trends-mining-difficulty-network-security-analysis

Market Talks

CONTINUE LEARNING

Up next: Lesson 7 Nodes and the Peer-to-Peer Network

This lesson is part of the free Blockchain track at the MARKET TALKS Education Center: Beginner, Intermediate and Advanced lessons, each with a quiz and a downloadable PDF.

Education Center
Lessons from first principles to advanced topics

Markets Analysis
Technical and fundamental analysis on major markets

Reports
Bitcoin, Gold, Silver, SPX and more

markettalks.info

Telegram @MARKET_TALKS

For education only. Nothing in this document is financial advice. © 2026 MARKET TALKS. You are welcome to share this PDF unchanged.