Market Talks
EDUCATION CENTER

BLOCKCHAIN · BEGINNER · LESSON 4 OF 13

# 2008 and the Birth of Bitcoin

A nine-page paper, a newspaper headline hidden in the first block, and a founder who walked away

8 min read  6 quiz questions with answer key

BLOCKCHAIN · BEGINNER · LESSON 4 OF 13

# 2008 and the Birth of Bitcoin

IN ONE SENTENCE

In 2008, an unknown author called Satoshi Nakamoto combined the pieces from earlier experiments and solved the one problem none of them could: getting strangers to agree on a single history with no one in charge.

## Nine pages in the middle of a crisis

In September 2008, the investment bank Lehman Brothers collapsed, and governments around the world rushed to rescue their banks with public money. Trust in the financial system was at a low point.

Six weeks later, on 31 October 2008, a message appeared on a mailing list read by cryptographers. Its author, using the name **Satoshi Nakamoto**, announced a new kind of electronic cash that worked directly between users, with no trusted third party. Attached was a link to a short paper: *Bitcoin: A Peer-to-Peer Electronic Cash System*. It was only nine pages long.

The paper did not hide its roots. It cited b-money, Hashcash and the time-stamping research you met in Lesson 3. What it added was a way to make those parts work together without a company, a bank or a trusted server at the center. Many readers on the list were doubtful. Some argued it could never handle enough payments. Others simply ignored it.

## Solving the missing piece

Lesson 3 ended with an open question: if thousands of independent computers each keep a copy of the record, how do they agree on which version is correct when nobody is in charge? Bitcoin's answer has three parts.

First, payments are grouped into batches called **blocks**, and each block is linked to the one before it, like the time-stamp chain from Lesson 3. Second, the right to add the next block is won through **proof of work**, the idea first used by Hashcash. Computers called **miners** race to solve a puzzle, and the winner's block is checked by everyone else before they build on it. Third, if two versions of the history ever compete, every computer follows the chain that has the most work behind it.

Put together, these rules make cheating very expensive. To rewrite a payment that is already buried in the chain, an attacker would have to redo the work for that block and every block after it, and do it faster than the rest of the network combined. The winning miner also receives newly created

bitcoins as a reward, so the same work that protects the record also issues the money. No company is needed for either job.

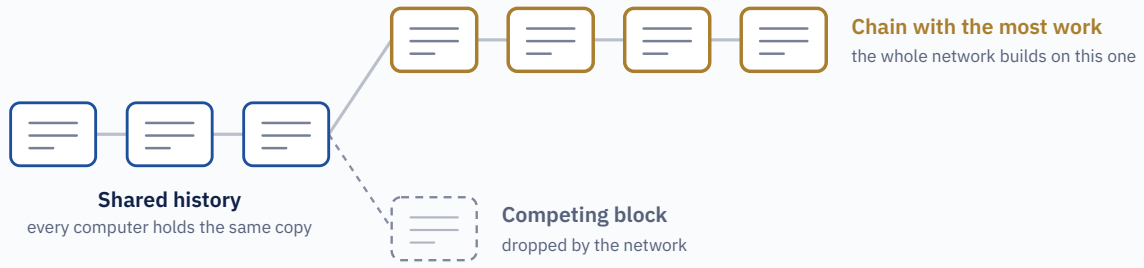



Figure 1. Sometimes two miners find a block at almost the same time. The network keeps building on the chain with the most work, and the competing block is dropped.

**ANALOGY: THE EXPENSIVE RAFFLE**

Picture a shared notebook that only one person may write in at a time. To decide who writes the next page, everyone buys raffle tickets, and each ticket costs real electricity. One winner is drawn about every ten minutes. Anyone who wants to forge old pages must win the raffle over and over, which means buying more tickets than everyone else put together. Honest writers keep winning because there are far more of them.

## 3 January 2009: the first block

On 3 January 2009, Satoshi created the very first block in Bitcoin's chain, known as the **genesis block**. Its reward was 50 bitcoins, and by a quirk of the code those coins can never be spent. Six days later the software was released for anyone to download and run.

On 12 January 2009, Satoshi sent 10 bitcoins to Hal Finney, the cryptographer behind RPOW from Lesson 3. It was the first payment from one person to another on the network. For months after that, the users were a small group of hobbyists running the program on their home computers.

**A MESSAGE IN THE FIRST BLOCK**

Satoshi wrote a line of text into the genesis block: *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*. It was the front-page headline of the British newspaper that day. Like the newspaper fingerprints in Lesson 3, it proves the block could not have been made before that date. Many readers also see it as a comment on why Bitcoin was built.

## Rules written in from day one

Unlike DigiCash or e-gold, Bitcoin has no issuer that decides how much money to create. The supply follows rules built into the software from the start:

- **A new block about every 10 minutes.** Every 2,016 blocks, roughly every two weeks, the puzzle automatically gets harder or easier to keep that pace, whether miners add or remove machines.
- **A shrinking reward.** The reward for each block started at 50 bitcoins and is cut in half every 210,000 blocks, roughly every four years. This event is called the **halving**. After the halving of April 2024, the reward is 3.125 bitcoins.
- **A fixed limit.** Because the reward keeps halving, the total supply can never go above 21 million bitcoins. The last fractions are expected to be mined around the year 2140.

Changing these rules is not something one person can do. Every computer on the network checks every block against the rules it runs, so a block that breaks them is simply rejected. Lesson 7 looks at these computers in more detail.

## From hobby to first price

For most of 2009, bitcoins had no price at all. In October 2009, a user calling himself New Liberty Standard published the first dollar exchange rate: 1,309.03 bitcoins for one US dollar. He arrived at it by working out how much electricity his computer used to mine coins.

On 22 May 2010, a programmer in Florida, Laszlo Hanyecz, paid 10,000 bitcoins for two pizzas, one of the first purchases of real goods with the currency. During 2010 the first exchanges appeared, and Bitcoin began to have a market price that changed every day. A trading market had been born.

## The founder who walked away

Satoshi never revealed a real name, face or location, and wrote only through forum posts and emails. During 2010, Satoshi slowly handed control of the code to other volunteer developers. The last confirmed message, an email dated 23 April 2011, said that Satoshi had "moved on to other things". The identity behind the name is still unknown.

Researchers who studied the earliest blocks estimate that a single miner, widely believed to be Satoshi, collected around 1.1 million bitcoins in the first year. The evidence is circumstantial, and those coins have never moved.

The disappearance turned out to matter. DigiCash and e-gold each had a founder and a company that could go bankrupt, be charged or be pressured. Bitcoin has neither. There is no head office to close and no leader whose decisions everyone must follow.

| Earlier weakness | Bitcoin's answer |
|---|---|
| **Digital money could be copied** | Every payment is checked against one shared history |
| **A company decided how much money exists** | New coins come only from fixed rules in the software |
| **One trusted server stopped double spending** | Thousands of independent computers check every block |
| **No way to agree without a leader** | Proof of work picks who adds the next block, and the chain with the most work wins |
| **A founder who could be charged or pressured** | An anonymous creator who stepped away |

## Why this matters for traders

- **A crisis is part of the story.** Bitcoin was launched during a banking crisis, with a bailout headline in its first block. That story returns whenever banks are under stress. In March 2023, when several US banks failed, bitcoin rose sharply as some investors looked for assets outside the banking system. Narratives like this can move prices, even if they do not last.
- **The supply schedule is public.** Every halving date can be estimated years in advance, and many traders track a roughly four-year cycle around them. Remember that a known event can already be priced in, and past cycles are no guarantee for the next one.
- **Old coins are watched closely.** Coins from the earliest years make headlines whenever they move. In September 2026, 600 bitcoins mined in 2010 moved after 16 years, and analysts quickly found no clear link to Satoshi. Checking the on-chain evidence before reacting to a headline can save you from trading on a rumor.

## Key terms

| | |
|---|---|
| **Whitepaper** | A short document that explains how a new system or project is meant to work. Bitcoin's was nine pages long. |
| **Genesis block** | The first block of a blockchain. Bitcoin's was created on 3 January 2009. |
| **Miner** | A computer, or its operator, that competes to add the next block by doing proof of work, in exchange for a reward. |

| | |
|---|---|
| **Block reward** | The new bitcoins the winning miner receives for adding a block. It is how all new bitcoins are created. |
| **Halving** | The cut in the block reward by half every 210,000 blocks, roughly every four years. |
| **Most-work chain** | The rule that when versions of the history compete, the network follows the one with the most proof of work behind it. |

## Key takeaways

1. Satoshi Nakamoto published the nine-page Bitcoin whitepaper on 31 October 2008, in the middle of a banking crisis.
2. Bitcoin combined blocks linked in a chain, proof of work and the most-work rule, so strangers can agree on one history with no one in charge.
3. The genesis block of 3 January 2009 carries a newspaper headline about bank bailouts, proving the date it was made.
4. New bitcoins come only from block rewards that halve about every four years, and the total can never exceed 21 million.
5. Satoshi left in 2011 without revealing an identity, leaving no founder or company that could be shut down.

## 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. When was the Bitcoin whitepaper published?**

- A January 2009
- B 31 October 2008
- C May 2010
- D April 2011

**2. If two versions of the blockchain compete, which one does the network follow?**

A The one created by the oldest computer
B The one chosen by a vote of exchanges
C The one with the most proof of work behind it
D The one with the most payments in it

**3. What does the newspaper headline in the genesis block prove?**

A That the block could not have been made before 3 January 2009
B That a bank approved Bitcoin
C That Satoshi lived in the UK
D That the first bitcoins were backed by pounds

**4. How are new bitcoins created?**

A A central bank prints them on demand
B Satoshi releases them each year
C Exchanges create them when demand rises
D Miners receive them as a reward for adding blocks

**5. What happens at a halving?**

A The price of bitcoin is cut in half
B The reward for adding a block is cut in half
C Half of all bitcoins are destroyed
D Blocks are added twice as fast

**6. Why did Satoshi's disappearance help Bitcoin?**

A It made bitcoin cheaper to mine
B It removed all rules from the system
C It left no founder or company that could be shut down or pressured
D It allowed Satoshi to sell coins in secret

# Answer key

1 B

**31 October 2008**

Satoshi shared the nine-page paper on a cryptography mailing list on 31 October 2008, about six weeks after Lehman Brothers collapsed.

2 C

**The one with the most proof of work behind it**

Every computer follows the chain with the most work behind it. To replace it, an attacker would need more computing power than the rest of the network combined.

3 A

**That the block could not have been made before 3 January 2009**

The headline was printed on 3 January 2009, so the block cannot be older than that. Who Satoshi was and where Satoshi lived remain unknown.

4 D

**Miners receive them as a reward for adding blocks**

The block reward is the only way new bitcoins come into existence. It follows fixed rules in the software, so no one can decide to issue more.

5 B

**The reward for adding a block is cut in half**

Every 210,000 blocks, roughly every four years, the block reward halves. That is why the total supply can never go above 21 million.

6 C

**It left no founder or company that could be shut down or pressured**

DigiCash and e-gold failed with their companies. With no known leader, Bitcoin has no head office to close and no single person whose decisions everyone must follow.

SOURCES


- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008): https://bitcoin.org/bitcoin.pdf
- Cryptography mailing list, Bitcoin P2P e-cash paper (31 October 2008): https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html
- Cointelegraph, Bitcoin turns ten on anniversary of genesis block: https://cointelegraph.com/news/bitcoin-turns-ten-on-anniversary-of-genesis-block
- Bitcoin Magazine, Bitcoin is up 6.5 billion percent since it was first priced in USD: https://bitcoinmagazine.com/culture/bitcoin-is-up-6-5-billion-percent-since-it-was-first-priced-in-usd
- The Defiant, Satoshi Nakamoto sent final email to Mike Hearn on April 23, 2011: https://thedefiant.io/news/people/bitcoin-creator-satoshi-nakamoto-sent-final-email-to-mike-hearn-on-april-23-2011-6735013c
- Cointelegraph, Does Satoshi actually own 1 million bitcoin?: https://cointelegraph.com/news/big-questions-does-satoshi-actually-own-1-million-bitcoin

Market Talks

CONTINUE LEARNING

# Up next: Lesson 5 What a Blockchain Actually Is

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.