Market Talks
EDUCATION CENTER

BLOCKCHAIN · BEGINNER · LESSON 3 OF 13

Before Bitcoin: The Digital Cash Experiments

Twenty-five years of attempts, near misses and failures, and the pieces each one left behind for Bitcoin

8 min read · 6 quiz questions with answer key

BLOCKCHAIN · BEGINNER · LESSON 3 OF 13

Before Bitcoin: The Digital Cash Experiments

IN ONE SENTENCE

Bitcoin did not appear out of nowhere. It combined ideas from earlier digital cash projects, and it was designed to avoid the single weakness that brought most of them down.

A dream older than the web browser

In Lessons 1 and 2 we met two problems: digital money can be copied, and a system run by one party can be frozen, shut down or corrupted. Long before Bitcoin, cryptographers and entrepreneurs were already trying to solve both.

Their projects ran from the early 1980s to the mid-2000s. Some became real businesses with real customers. Others never left the page. None of them fully succeeded, yet almost every one of them added something that Bitcoin would later use. Following their story is the best way to understand why Bitcoin is built the way it is.

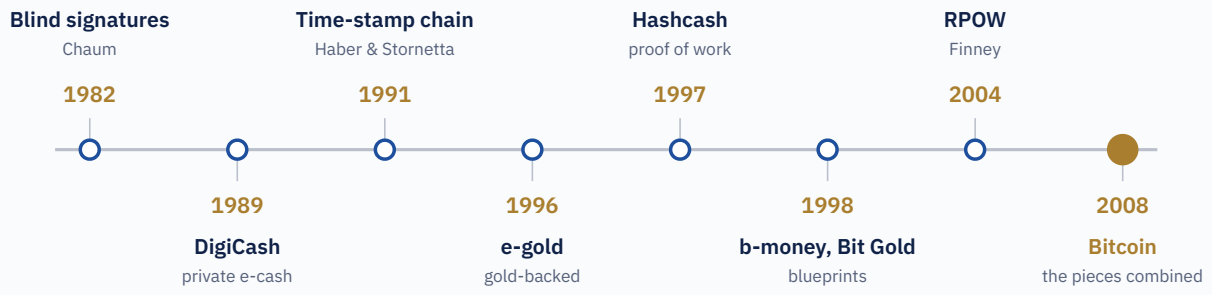


Figure 1. More than 25 years of digital cash experiments came before Bitcoin. Each left behind a piece of the final design.

DigiCash: private, but run by one company

In 1982, the cryptographer David Chaum described a technique called **blind signatures**. It lets a bank sign a digital coin to confirm it is valid without seeing which coin it is signing. The result is

digital money that can be spent privately, much like cash, because the bank cannot link a payment back to the person who withdrew the coin.

Chaum founded DigiCash in 1989 to turn the idea into a product, and in 1995 the Mark Twain Bank in St. Louis began offering its eCash to customers. The technology worked. The business did not: too few banks and merchants signed up, and DigiCash filed for bankruptcy in 1998.

The deeper weakness was structural. Every coin still had to be issued by a central bank or company, and that same central party checked for double spending. When the company failed, the money failed with it.

e-gold: real backing, one point of failure

e-gold, launched in 1996, took a different approach. Every unit was backed by physical gold held in vaults, and users could send gold-backed balances to each other across the world in seconds. It grew fast: by 2006 it was processing more than $2 billion of payments a year.

But e-gold was one company, and that made it one target. Its lack of identity checks made it attractive to criminals, and US authorities charged the company and its directors in 2007. In 2008 they pleaded guilty to conspiracy to commit money laundering and to running an unlicensed money transmitting business, and in 2009 transfers were suspended. Account holders waited years for a process to recover their funds.

The lesson from Lesson 2 played out in real life: a single point of control is also a single point of failure, whether the cause is a hacker, a bankruptcy or a court order.

Hashcash: making things costly on purpose

In 1997, the cryptographer Adam Back proposed **Hashcash** as a defence against email spam. Before sending a message, the sender's computer had to solve a small puzzle, taking a moment of computing work. For one email, the cost is invisible. For a spammer sending millions, it adds up fast.

The clever part is the asymmetry: the puzzle is slow to solve but instant to check. Anyone receiving the email can confirm the work was done without redoing it. This idea is called **proof of work**, and Bitcoin's whitepaper names Hashcash as a direct influence.

ANALOGY: THE SUDOKU TEST

A hard sudoku can take an hour to solve, but checking a finished grid takes a minute. If someone hands you a completed puzzle, you know they put in the effort, even though you never watched them do it. Proof of work turns that idea into a digital stamp of effort that any computer can verify.

b-money, Bit Gold and RPOW: the blueprints

In 1998, two proposals came strikingly close to Bitcoin on paper. The computer engineer Wei Dai described **b-money**, in which every participant keeps a copy of who owns what, and new money is created by solving computational problems. Around the same time, the legal scholar and computer scientist Nick Szabo proposed **Bit Gold**, which chained proof-of-work solutions together with timestamps to create something scarce and costly to produce, a kind of digital gold.

Neither was ever launched. Both left an important question open: if many independent people keep the records, how do they agree on which record is correct without someone in charge?

In 2004, the cryptographer Hal Finney built **RPOW** (reusable proofs of work), which let proof-of-work tokens be passed from person to person. It actually ran, but to stop double spending it relied on a trusted server running on special secure hardware. One trusted party was still at the center. Five years later, Finney would receive the first bitcoin ever sent from one person to another.

The chain of time-stamps

One more piece came from outside the world of money. In 1991, the researchers Stuart Haber and W. Scott Stornetta asked how to prove when a digital document was created, and that it has not been changed since.

Their answer was to link records into a chain. Each new record carries a digital fingerprint of the one before it, so changing any old record would break every link that follows. History becomes **tamper-evident**: you can still try to rewrite it, but everyone can see that you did. Bitcoin's whitepaper cites their work three times, and the idea of linking records in this way became the "chain" in blockchain. Lesson 6 explains exactly how these fingerprints work.

A REAL EXAMPLE

To make their chain impossible to quietly rewrite, Haber and Stornetta's company began publishing a fingerprint of its latest records in the classified ads of The New York Times in 1995. Anyone could compare a printed newspaper with the chain, and no one could change thousands of printed copies after the fact.

The missing piece

By the mid-2000s, almost all the parts existed. What was still missing was the hardest one:

Project	What it added	What was still missing
DigiCash (1989)	Private digital payments	Depended on a central issuer
Time-stamp chain (1991)	Records linked so history cannot be quietly changed	Not designed for money
e-gold (1996)	Global transfers at scale	One company that could be shut down
Hashcash (1997)	Proof of work: costly to create, cheap to verify	Not money, just a stamp
b-money, Bit Gold (1998)	Shared records and money created through work	No way to agree without a leader; never launched
RPOW (2004)	Proof-of-work tokens people could pass on	Relied on one trusted server

Every attempt either depended on someone in charge or never solved how strangers could agree on one history without one. In 2008, an anonymous author put the pieces together and added the missing one. That is the story of Lesson 4.

Why this matters for traders

- **Central issuers fail in familiar ways.** DigiCash went bankrupt and e-gold was closed by prosecutors. The same pattern returned in 2013, when US authorities shut down Liberty Reserve, another centrally run digital currency. Any asset that depends on one issuer carries that issuer's business and legal risk.
- **Today's stablecoins echo e-gold.** A dollar-backed stablecoin follows a similar model: a company holds reserves and issues tokens against them. That makes the issuer's reserves, licensing and legal standing worth understanding before relying on one.
- **The "digital gold" narrative has deep roots.** Bit Gold's idea of something scarce because it is costly to create still shapes how many investors compare Bitcoin with gold. Knowing where a narrative comes from helps you judge how much weight it deserves when it moves the market.

Key terms

Blind signature — A way for a bank or issuer to approve a digital coin without seeing which coin it approves, so payments can stay private.

Proof of work	Evidence that a computer spent real effort solving a puzzle. Slow to produce, instant to check.
Asset-backed	Money or tokens whose value is supported by a real asset, such as gold or dollars, held by an issuer.
Time-stamping	Proving when a digital record was created and that it has not been changed since.
Tamper-evident	Built so that any change to past records is visible to everyone, even if it cannot be physically prevented.
Digital scarcity	A limited supply of something digital that cannot simply be copied or created for free.

Key takeaways

1. Digital cash experiments began in the early 1980s, more than 25 years before Bitcoin.
2. DigiCash brought privacy and e-gold brought global scale, but both depended on one company and failed with it.
3. Hashcash introduced proof of work: effort that is slow to produce but instant to verify.
4. b-money, Bit Gold and RPOW sketched shared records and work-based money, but none solved how strangers could agree without a trusted party.
5. Linked time-stamps showed how to make history tamper-evident. Bitcoin combined these pieces and added the one that was missing.

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 was the key innovation behind DigiCash?

- (A) Gold held in vaults
- (B) Blind signatures that made digital payments private
- (C) Proof of work to stop spam
- (D) A ledger copied by every user

2. Why did e-gold come to an end?

A Legal action against the single company that ran it
B Its gold reserves were stolen
C A bug allowed users to copy coins
D Its users moved to Bitcoin

3. What was Hashcash originally designed to do?

A Make online payments private
B Store gold-backed balances
C Make sending email spam expensive
D Time-stamp legal documents

4. Which property makes proof of work useful?

A It can be produced instantly by anyone
B It can only be checked by a central server
C It is easy to copy
D It is slow to produce but instant to verify

5. What did Haber and Stornetta's 1991 work contribute?

A Gold-backed digital money
B Linking records in a chain so that changing history becomes visible
C Anonymous email
D The first cryptocurrency exchange

6. Before 2008, what piece was still missing?

A Faster internet connections
B A way to make payments private
C A way for strangers to agree on one shared history without anyone in charge
D Computers powerful enough to do proof of work

Answer key

1 B

Blind signatures that made digital payments private

David Chaum's blind signatures let a bank approve a coin without seeing which coin it was, so payments could stay private, much like cash.

2 A

Legal action against the single company that ran it

e-gold was run by one company. After prosecutors charged it and its directors, they pleaded guilty in 2008 and transfers were suspended in 2009. One company meant one point of failure.

3 C

Make sending email spam expensive

Adam Back proposed Hashcash to fight spam. Each email required a little computing work: nothing for one message, very costly for millions.

4 D

It is slow to produce but instant to verify

Like a finished sudoku, proof of work takes effort to create but only a moment to check. That lets anyone confirm the work was done without redoing it.

5 B

Linking records in a chain so that changing history becomes visible

Each record carries a fingerprint of the previous one, so changing an old record breaks every later link. This idea became the "chain" in blockchain.

6 C

A way for strangers to agree on one shared history without anyone in charge

Earlier systems either relied on a trusted party or never solved how many independent participants could agree on one record. Bitcoin added that missing piece, as Lesson 4 explains.

SOURCES

- US Department of Justice, e-gold guilty pleas (July 2008): https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html
- Wikipedia, DigiCash: https://en.wikipedia.org/wiki/DigiCash
- Wikipedia, e-gold: https://en.wikipedia.org/wiki/E-gold
- Satoshi Nakamoto Institute, Hal Finney: RPOW: https://nakamotoinstitute.org/finney/rpow/
- Cointelegraph, Co-inventor of blockchain on why he is not Satoshi Nakamoto: https://cointelegraph.com/news/co-inventor-of-blockchain-on-why-he-is-not-satoshi-nakamoto

Market Talks

CONTINUE LEARNING

Up next: Lesson 4
2008 and the Birth of Bitcoin

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.