Market Talks
EDUCATION CENTER

BLOCKCHAIN · BEGINNER · LESSON 1 OF 13

The Trust Problem

Why every digital payment needs a middleman, and why blockchain was invented to change that

7 min read 6 quiz questions with answer key

BLOCKCHAIN · BEGINNER · LESSON 1 OF 13

The Trust Problem

IN ONE SENTENCE

Every digital payment today depends on a trusted middleman keeping the books. Blockchain is an attempt to keep shared books that nobody has to trust.

Money is a record, not a thing

Most of the money you own is not cash in a drawer. It is a number in a bank's database. When you pay someone from your account, nothing physical travels anywhere. Your bank lowers one entry in its records, and the recipient's bank raises another.

So what you really hold is a *promise*: the bank's promise that its records are correct and that it will honor them when you ask. The same is true for card balances, payment apps and funds sitting on a trading exchange. Digital money is, at its core, a record kept by someone.

Why we rely on a middleman

Imagine paying a seller on the other side of the world whom you have never met. You cannot check their records, and they cannot check yours. Neither of you has a reason to trust the other. A middleman solves this by doing three jobs at once:

- **Keeping the official record** of who owns what.
- **Checking every payment**, for example that you actually have the funds you are sending.
- **Settling disagreements**, including reversing mistakes and fraud.

Banks, card networks, payment apps and exchanges all play this role. Most of the time the arrangement works well, which is exactly why it dominates the financial world.

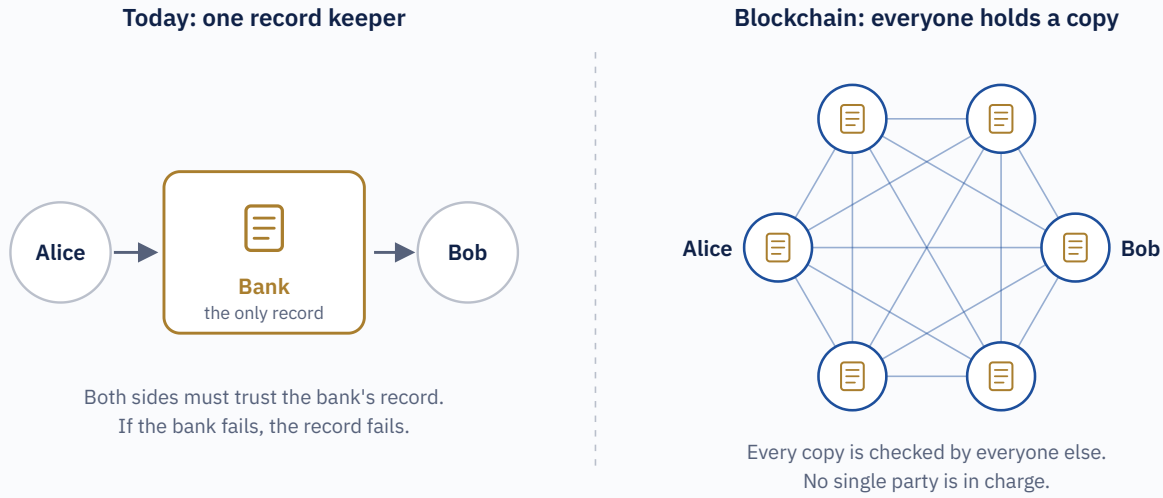


Figure 1. With a middleman, one party holds the only record. With a blockchain, every participant holds and checks an identical copy.

The hidden cost of trusting someone

Relying on a middleman is convenient, but it is never free. The costs show up in four ways:

- **Fees and delays.** An international transfer can pass through a chain of banks, each adding time and charges. According to the World Bank, sending $200 abroad cost 6.49% on average in early 2025, more than double the 3% global target.
- **Gatekeeping.** A middleman can freeze, close or refuse an account. According to the World Bank, more than a billion adults worldwide still have no bank account at all.
- **A single point of failure.** If the middleman is hacked, goes offline or collapses, everyone who relied on it is affected at once.
- **Records you cannot check.** You see the balance the middleman chooses to show you. You cannot audit its books yourself.

None of this means banks are bad. It means trust has a price, and you pay it whether you notice it or not.

A REAL EXAMPLE

In November 2022, the crypto exchange FTX collapsed and filed for bankruptcy. Customers who believed they held bitcoin and dollars on the platform discovered they actually held a claim against a failing company. Their funds were frozen for years while the bankruptcy was worked out.

Why not simply create digital money? The double-spending problem

Digital things copy perfectly. When you email a photo to a friend, you do not lose the photo. You both have it now. That is fine for photos, but it is a disaster for money. If money were just a file, you could send the same file to a hundred different people and pay all of them with it.

A physical coin cannot be in two pockets at once. Digital money can, unless something stops it. This is called the **double-spending problem**, and it is the central challenge of digital money.

Until 2008, the only reliable solution was a central record keeper that decides which payment came first and rejects the copy. So every attempt at digital cash still needed a middleman, and when that middleman failed or was shut down, the money disappeared with it. We look at those early attempts in Lesson 3.

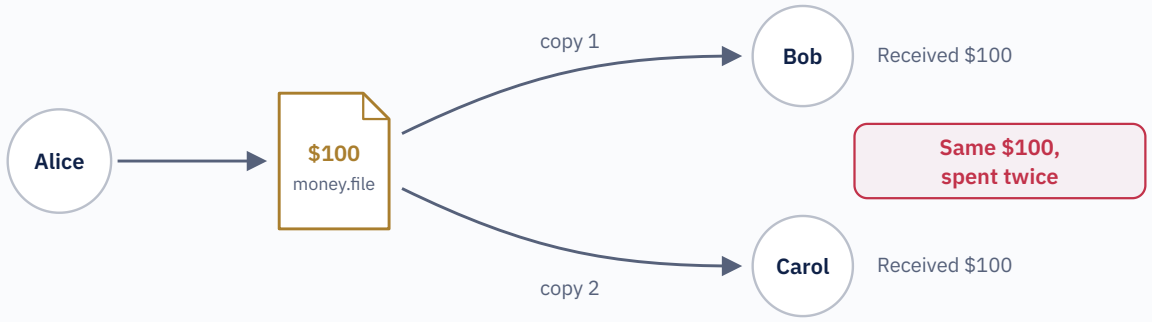


Figure 2. A digital file can be copied, so without a safeguard the same money could be sent to two people at once.

The question blockchain was built to answer

Put everything above together and you arrive at one question:

> Can a group of strangers who do not trust each other keep one shared record that everyone accepts, with nobody in charge?

That is the problem blockchain was designed to solve. In 2008, a paper published under the name Satoshi Nakamoto proposed an answer, and Bitcoin went live a few months later. We cover that story in Lesson 4.

The core idea, in short:

- Instead of one record held by one keeper, **many identical copies** are held by anyone who wants one.

- Every new entry is **checked by everyone** against the same public rules.
- Changing past entries is made **extremely expensive**, so the history can be relied on.

Trust moves away from an institution and toward rules, mathematics and open verification. The crypto community sums this up in three words: *don't trust, verify*.

ANALOGY: THE SHARED SPREADSHEET

Think of an online spreadsheet that one company hosts. The company can lock you out, edit rows or lose the file. Now picture a different spreadsheet: everyone has a full copy, a new row is only added when the whole group confirms it follows the rules, and old rows are sealed so they can no longer be edited. Nobody owns it, and anyone can check it. That second spreadsheet is the basic idea behind a blockchain.

What blockchain does not remove

It is important to be honest about the limits from the start. A blockchain removes the need to trust a *single record keeper*, but it does not remove trust entirely. You still rely on the software being correct, on your own care in protecting your keys, and often on new middlemen such as exchanges and wallet apps.

It also removes the safety nets. There is usually no customer service to reverse a mistaken payment. Over the rest of this track, you will see both sides of these trade-offs in detail.

Why this matters for traders

- **Counterparty risk is everywhere.** When your funds sit on an exchange or with a broker, you hold that firm's promise, not the asset itself. The FTX collapse showed what that difference means in practice.
- **Settlement works differently.** US stock trades settle one business day after the trade (T+1, since May 2024), and only on business days. A Bitcoin transfer settles under the network's own rules, around the clock, including weekends.
- **Trust shapes market narratives.** Bitcoin was born in the aftermath of the 2008 banking crisis. When several US regional banks failed in March 2023, Bitcoin rose sharply over the following weeks, and many market commentators linked the move to renewed doubts about banks. Understanding the trust problem helps you understand why stories like these move prices.

Key terms

Intermediary	A middleman, such as a bank or exchange, that keeps records and processes payments between two parties.
Ledger	A record of transactions and balances. A blockchain is a special kind of ledger.
Counterparty risk	The risk that the other party in an arrangement fails to keep its side of the deal.
Double spending	Spending the same digital money more than once. Preventing it is the core challenge of digital cash.
Settlement	The point at which a payment or trade is complete and the ownership change is final.
Trustless	A system in which you do not need to trust any single party, because the rules can be checked by anyone. It does not mean no trust at all.

Key takeaways

1. Digital money is a record, and today a middleman keeps that record for us.
2. Middlemen bring convenience but also fees, delays, gatekeeping and a single point of failure.
3. Because digital files copy perfectly, digital money faces the double-spending problem.
4. Before 2008, only a central record keeper could prevent double spending.
5. Blockchain lets many independent parties keep one shared record that anyone can verify, without anyone in charge.

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 you pay someone from your bank account, what actually happens?

- A Physical cash is moved between bank vaults
- B The bank updates entries in its records
- C A digital coin file is sent to the recipient
- D The central bank prints new money for the recipient

2. What is the double-spending problem?

A. Paying two fees for one transaction
B. Being charged twice by mistake
C. Spending the same digital money more than once, because digital files can be copied
D. Sending money to two banks at the same time

3. Before 2008, how did digital payment systems usually prevent double spending?

A. By relying on a central authority that kept the official record
B. By limiting payments to small amounts
C. By using physical coins alongside digital ones
D. They could not prevent it at all

4. Which of these is NOT a cost of relying on a middleman?

A. Fees and delays
B. The risk of an account being frozen
C. A single point of failure
D. Payments that can never be reversed

5. If you keep funds on an exchange, what do you actually hold?

A. The assets themselves, stored in your name on the blockchain
B. A claim against the exchange, which depends on the exchange staying solvent
C. Insurance that guarantees full repayment
D. A copy of the exchange's private keys

6. In blockchain, what does "trustless" mean?

A. Nobody trusts anybody, so nothing works
B. No trust of any kind is needed
C. You do not have to trust any single party, because anyone can verify the rules and records
D. Only trusted members can join the network

Answer key

1 B

The bank updates entries in its records

Nothing physical moves. The bank lowers your balance and raises the recipient's in its records. Your money is really the bank's record and its promise to honor it.

2 C

Spending the same digital money more than once, because digital files can be copied

Digital files copy perfectly, so without a safeguard the same digital money could be sent to many people. Preventing this is the core challenge of digital cash.

3 A

By relying on a central authority that kept the official record

A central record keeper decided which payment came first and rejected copies. That worked, but it meant every system depended on a middleman.

4 D

Payments that can never be reversed

Middlemen can usually reverse mistakes and fraud. Irreversible payments are a feature, and a risk, of blockchains, not of traditional middlemen.

5 B

A claim against the exchange, which depends on the exchange staying solvent

You hold the exchange's promise. If the exchange fails, as FTX did in 2022, that promise can be frozen or lost. This is counterparty risk.

6 C

You do not have to trust any single party, because anyone can verify the rules and records

Trustless means you do not have to rely on one institution's word. Some trust remains, for example in the software and in your own key handling.

SOURCES

- World Bank, Remittance Prices Worldwide, Q1 2025 report: https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q125_1_0.pdf

Market Talks

CONTINUE LEARNING

Up next: Lesson 2 Centralized, Distributed, Decentralized

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.