

Topic 1.1: What Is Money, Really?

Trust, Ledgers, and the Double-Spending Problem

Joerg Osterrieder

Digital Finance

2025

What You Will Learn in This Topic

By the end of this session, you will be able to:

1. **Dissolve assumptions** about what money “is”
2. **Understand** why digital money is fundamentally hard
3. **Explain** the double-spending problem and its implications
4. **Distinguish** account-based from token-based money
5. **Analyze** the trade-offs of trusted intermediaries

Hands-On Component

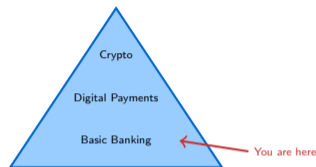
We'll use a Colab notebook to simulate a simple ledger and see double-spending in action.

No prior knowledge required!

- This topic starts from first principles
- We'll build up concepts step by step
- Questions are encouraged

Helpful background:

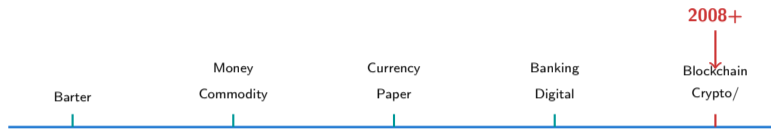
- Basic understanding of banks
- Familiarity with digital payments
- Curiosity about how things work



Key Mindset

Forget everything you “know” about money. We’re going to rebuild the concept from scratch.

The Big Picture: Why This Matters



We're witnessing a fundamental shift:

- Money is being **reinvented** for the digital age
- Old assumptions are being **challenged**
- New possibilities are **emerging**

Course Goal

Understand *why* these changes are happening and *how* they work.

Imagine you're stranded on an island with 9 strangers...

You have skills:

- Alice: fishing
- Bob: building
- Carol: farming
- Dave: medicine
- ...and so on

The problem:

- Alice wants vegetables
- Carol doesn't need fish
- How do you trade?

The Coincidence of Wants Problem

Direct barter requires both parties to want what the other has, at the same time. This almost never happens.

Three Solutions to the Barter Problem

Commodity Money

(shells, gold)

Credit (IOUs)

(trust-based)

Shared Ledger

(recordkeeping)

Key Insight: All three solutions are really about **trust**.

- Commodity: Trust the material has value
- Credit: Trust the person will repay
- Ledger: Trust the recordkeeper is honest

Think about the last time you paid for something...

The Three Functions of Money:

1. Medium of Exchange

Accepted for transactions

Example: Your Starbucks gift card is a medium of exchange—but only within Starbucks

2. Unit of Account

Common measure of value

3. Store of Value

Holds purchasing power over time



What makes something “money”?

Collective belief that others will accept it.

Anthropological Fact

Debt and credit systems (ledgers) predate physical currency by thousands of years. Money is fundamentally about **information**, not objects.

Historical Evolution of Money



Key Pattern:

- Each stage = more **abstract**
- Each stage = more **scalable**
- Each stage = requires more **trust**

The Constant:

- Always about **trust**
- Always about **recordkeeping**
- Always **social technology**

Why did gold win?

- Durable (doesn't rot)
- Divisible (can be split)
- Portable (easy to carry)
- Recognizable (hard to fake)
- Scarce (limited supply)

The Ledger: Humanity's Oldest Financial Technology

THE LEDGER		
From	To	Amount
Alice	Bob	50
Bob	Carol	30
Carol	Alice	20
...

A ledger is simply: A record of who owes what to whom.

The critical question: Who maintains the ledger?

Essential Properties:

1. **Accuracy**
Records match reality
2. **Completeness**
All transactions recorded
3. **Immutability**
History cannot be changed
4. **Availability**
Accessible when needed

Trust Requirements:

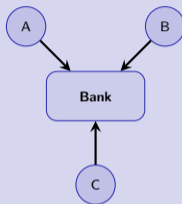
- Keeper won't **lie**
- Keeper won't **steal**
- Keeper won't **disappear**
- Keeper won't **discriminate**

The Core Problem

How do we ensure these properties without trusting any single party?

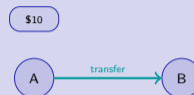
Account-Based vs. Token-Based Money

Account-Based (Ledger)



- Identity verified
- Balances in database
- Transfers update records
- **Example:** Bank app showing your balance

Token-Based (Bearer)



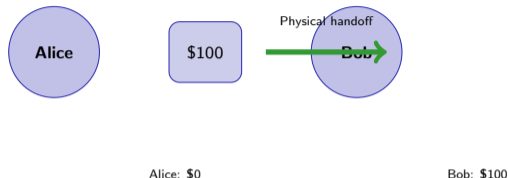
- Possession = ownership
- No identity needed
- Physical handoff
- **Example:** Cash in your wallet

Visual comparison: Checking your bank app balance (account-based) vs. counting cash in your wallet (token-based)

The Digital Dilemma

Physical tokens can be handed over. Digital files can be **copied**. How do you hand over a digital token without copying it?

Why Physical Money Works



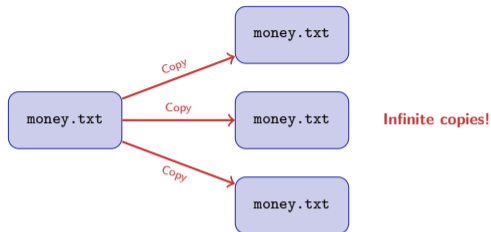
Physics enforces scarcity:

- A physical object can only be in **one place** at a time
- Giving it away means you **no longer have it**
- No need to check a database—possession is proof

Key Insight

Physical money is **self-proving**. The laws of physics prevent double-spending automatically.

The Problem with Digital Files



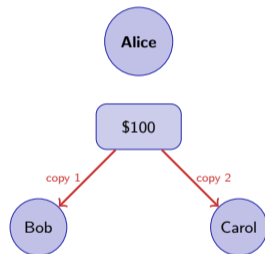
Digital information is fundamentally different:

- **Perfect copies** cost nothing to make
- **No scarcity**—bits can be duplicated infinitely
- **No physics** to enforce “giving it away”

The Digital Money Problem

If money is just a file, what stops someone from copying it and spending it twice?

The Fundamental Challenge of Digital Money



Both get “paid”!

Why is this hard?

- Digital = perfectly copyable
- No physical scarcity
- Can't “hand over” a file
- Need to prevent copies from both being valid

How ledgers solve this:

By keeping a single record everyone trusts

Before 2008, only one solution existed:

A trusted central authority

Double-Spending: A Concrete Example



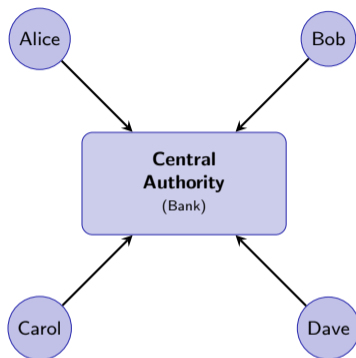
Without a central authority:

- Bob checks his copy of the ledger: "Alice paid me \$100" ✓
- Carol checks her copy: "Alice paid me \$100" ✓
- Neither knows about the other transaction!

The Core Question

How do Bob and Carol **agree** on which transaction is valid?

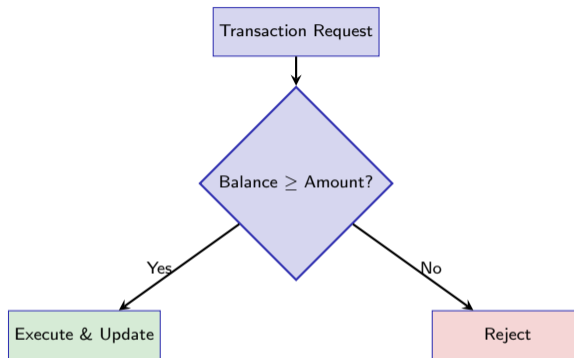
The Traditional Solution: Trusted Third Parties



Account	Balance
Alice	\$100
Bob	\$250
Carol	\$75
Dave	\$180

How it prevents double-spending:

1. Alice requests: "Send \$100 to Bob"
2. Bank checks: Does Alice have \$100?
3. Bank updates: Alice $-\$100$, Bob $+\$100$
4. Transaction complete—Alice can't spend it again

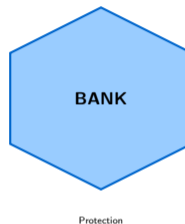


Key Properties:

- **Sequential processing:** One transaction at a time
- **Atomic execution:** All-or-nothing (no partial transfers)
- **Single source of truth:** Only the bank's ledger matters

Benefits of Trusted Intermediaries:

- ✓ **Double-spending prevented**
Central validation ensures no duplicate spending
- ✓ **Transaction records**
Complete audit trail maintained
- ✓ **Dispute resolution**
Authority can mediate conflicts
- ✓ **Reversibility**
Chargebacks possible for fraud



The Value Proposition

“Trust us, and we’ll protect your money.”

Costs of Centralization:

- ✗ **Privacy**
Bank sees all transactions
- ✗ **Autonomy**
Bank can freeze accounts
- ✗ **Inclusion**
Need bank approval to participate
- ✗ **Speed**
Bank's hours and processes
- ✗ **Cost**
Fees of 1–5% or more

The Trust Assumption

We must trust that the central authority:

- Won't steal our money
- Won't censor transactions
- Won't fail or get hacked
- Will always be available
- Will treat everyone fairly

2008 Financial Crisis:

Many questioned whether this trust was warranted.

What is Counterparty Risk?

The risk that the other party (bank) might fail to fulfill its obligations.

Examples:

- Bank becomes insolvent
- Bank run depletes reserves
- Government seizes assets
- Cyberattack compromises systems



Your Balance: \$10,000



Bank fails...
Your money?

2008 Financial Crisis: In 2008, banks didn't trust each other's IOUs—the interbank lending system froze

Fractional Reserve Banking

Simple example: You deposit \$100. The bank keeps \$10 and lends \$90 to someone else. Your account still shows \$100. If everyone withdraws at once, the bank cannot pay. This is called a **bank run**.

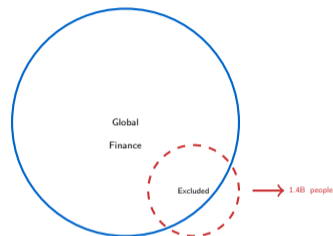
Censorship Risk:

- Accounts can be frozen
- Transactions can be blocked
- Access can be revoked
- No permission = no participation

What happens when the TTP fails? Example: What if PayPal freezes your account?

Financial Exclusion:

- **1.4 billion adults** worldwide lack bank access
- Requirements: ID, minimum balance, credit check
- Geographic limitations
- 3–5 day international transfers



Key Question

Should access to money require permission?

The Coordination Problem: Byzantine Generals

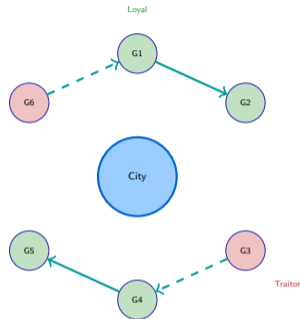
The Thought Experiment:

Several generals surround an enemy city. They must coordinate to attack together or retreat together. But:

- Generals can only communicate via messengers
- Some messengers might be **traitors**
- Some generals might be **traitors**

The Challenge:

How do loyal generals agree on a plan when they can't trust all messages or all participants?



Key Insight

This is the fundamental problem of **consensus without trust**.

“How do strangers agree on who owns what without trusting each other?”

The Parallel:

- **Generals** = Network participants
- **City attack plan** = Transaction history
- **Traitors** = Malicious actors trying to double-spend
- **Messages** = Transaction broadcasts

The Challenge:

- Alice sends conflicting messages: “I paid Bob” and “I paid Carol”
- Bob and Carol each see one message
- Who should they believe?
- How do they agree on what really happened?

Why This Matters

Before Bitcoin (2008), there was **no known solution** to the Byzantine Generals Problem for large, open networks. This is why digital money required trusted banks. Blockchain changed everything.

Can we have the benefits of cash in digital form?

Cash Properties:

- ✓ No permission needed
- ✓ Instant settlement
- ✓ Privacy (no tracking)
- ✓ No counterparty risk
- ✓ No censorship

Digital Requirements:

- Works over the internet
- Globally accessible
- Divisible to small amounts
- Programmable
- Secure against copying

The Challenge

How do you prevent double-spending digitally **without** a central authority?



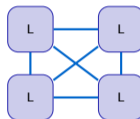
Why did earlier attempts fail?

- Still relied on central parties (company, servers)
- Legal/regulatory shutdown
- No solution to Byzantine consensus

What if we could prevent double-spending without a central authority?

Satoshi Nakamoto's insight:

1. Replicate the ledger everywhere
2. Use cryptography to verify
3. Use economic incentives to secure
4. Achieve consensus without trust



Everyone has the ledger

We'll Explore This in Topic 1.2

For now, understand that **blockchain** is one answer to: "How do we have digital money without trusting a single party?"

Let's See Double-Spending in Action

In the Colab notebook (NB01), we will:

1. Build a simple ledger with account balances
2. Process valid transactions
3. Attempt a double-spend attack
4. See how a central authority prevents it
5. Discuss: What happens without the authority?

Access the Notebook

`day_01/notebooks/NB01_ledger_simulation.ipynb`

Or scan QR code / click link provided

Time: 15-20 minutes for guided exploration

Part 1: Build a Ledger

- Create accounts with balances
- Implement transfer function
- Add balance validation

Part 2: Test Double-Spending

- Create a malicious transaction
- Observe the attack
- Understand why it works/fails

Part 3: Explore Trade-offs

- Centralized vs. no central authority
- Speed vs. security
- Privacy vs. auditability

Key Takeaway

Understanding *why* the problem is hard helps you appreciate blockchain's solution.

Questions to Consider:

1. Is Bitcoin “real money”? Why or why not?
2. What makes you trust your bank?
3. If you could design money from scratch, what would it look like?
4. Is privacy a feature or a bug?

Key Takeaways:

- Money = trust infrastructure
- Digital money needs double-spend protection
- Central authorities work but have costs
- Blockchain offers an alternative

The Central Question of This Course

How should we build the trust infrastructure for a digital economy?

Property	Cash	Bank	PayPal	Bitcoin	Stablecoin
Speed	Fast	Slow	Medium	Slow	Fast
Privacy	High	Low	Low	Medium	Medium
Reversibility	No	Yes	Yes	No	Varies
Permission	No	Yes	Yes	No	No
Censorship	Hard	Easy	Easy	Hard	Medium
Global	No	Limited	Yes	Yes	Yes

Key Insight: No single system is “best.” Each optimizes for different properties.

Design Trade-offs

Every money system makes choices about what to prioritize. Understanding these trade-offs is essential for evaluating new financial technologies.

Where This Matters:

Remittances

- \$700B+ sent globally per year
- Fees average 6–7%
- 3–5 days for settlement

Financial Inclusion

- 1.4B unbanked adults
- Mobile phones more common than banks
- Crypto as access point

Cross-Border Commerce

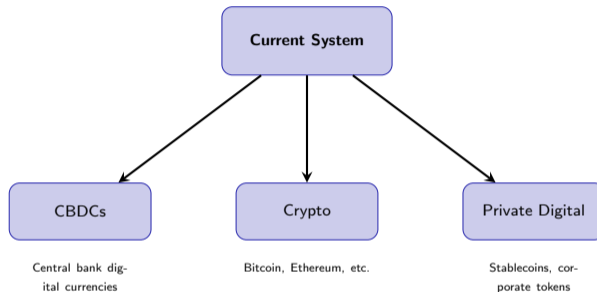
- Currency conversion costs
- Settlement delays
- Regulatory friction

Economic Instability

- Hyperinflation (Venezuela, Zimbabwe)
- Capital controls
- Currency devaluation

Implication

Understanding money's foundations helps evaluate proposed solutions.



Emerging Questions:

- Who should control digital money?
- How do we balance privacy and regulation?
- Can different systems coexist?

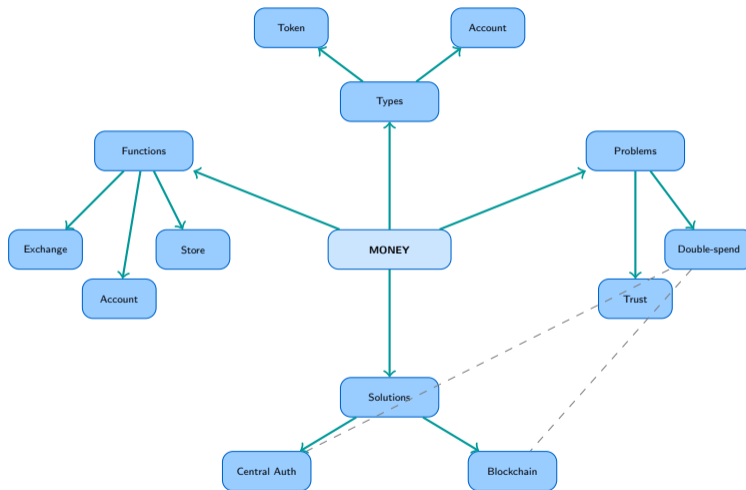
Key Takeaways from Topic 1.1

1. **Money is information, not objects**
Ledgers and trust predate physical currency
2. **The double-spending problem is fundamental**
Digital files can be copied; money cannot be
3. **Traditional solution: trusted intermediaries**
Banks prevent double-spending but introduce costs
4. **Costs include:** fees, delays, exclusion, censorship, counterparty risk
5. **Blockchain proposes an alternative**
Decentralized consensus without central trust

The Big Idea

Understanding *why* digital money is hard helps you appreciate *how* blockchain solves it.

Concept Map: Money and Trust



Money A social technology that serves as medium of exchange, unit of account, and store of value—fundamentally based on trust.

Ledger A record of transactions showing who owes what to whom; humanity's oldest financial technology.

Double-Spending The fundamental challenge of digital money: spending the same digital value multiple times because files can be copied.

Token-Based Money Bearer instruments where possession equals ownership (e.g., cash, gold coins).

Account-Based Money Systems where identity is verified and balances are tracked in a central database (e.g., bank accounts).

Trusted Third Party A central authority (like a bank) that validates transactions and maintains the authoritative ledger.

Counterparty Risk The risk that the other party (e.g., bank) might fail to fulfill its obligations.

Fractional Reserve Banking practice where banks keep only a fraction (e.g., 10%) of deposits as reserves and lend the rest.

Censorship Risk The ability of authorities to freeze accounts, block transactions, or deny service.

Atomic Execution Transactions that complete fully or not at all—no partial states allowed.

Single Source of Truth One authoritative ledger that all parties must accept as correct.

Misconception

“Money is backed by gold”

“Banks store your exact dollars”

“Digital = automatically better”

“Blockchain solves everything”

Reality

Most currencies are fiat—backed by government promise and collective belief

Banks lend most deposits out (fractional reserve); your “balance” is an IOU

Digital creates the double-spend problem; requires new solutions

Blockchain is one solution with its own trade-offs; not universally superior

Critical Thinking

Always ask: What problem does this solve? What trade-offs does it introduce?

Question

Which of the following is NOT one of the three fundamental functions of money?

- A. Medium of exchange
- B. Unit of account
- C. Source of government revenue
- D. Store of value

Question

Which of the following is NOT one of the three fundamental functions of money?

- A. Medium of exchange
- B. Unit of account
- C. Source of government revenue
- D. Store of value

Answer: C

Explanation: The three fundamental functions of money are: (1) medium of exchange (facilitating trade), (2) unit of account (measuring value), and (3) store of value (preserving purchasing power over time). While governments may collect taxes using money, generating revenue is not a core function of money itself.

Question 2

How do banks solve the double-spending problem in digital finance?

Answer: By maintaining a **centralized ledger** and validating every transaction against available balances before execution.

Question 3

What is fractional reserve banking?

Answer: A system where banks keep only a fraction (e.g., 10%) of deposits as reserves and lend out the rest.

Key Insight: This enables economic growth but creates vulnerability during bank runs—not all depositors can withdraw simultaneously.

Preview: From Ledgers to Blockchains

In Topic 1.2, we'll explore:

- How **cryptographic hashing** creates tamper-proof records
- The structure of **blockchain** as a data structure
- **Consensus mechanisms**—how strangers agree without trust
- **Decentralization**—distributing the ledger to everyone

Connection

Topic 1.1 established the *problem* (double-spending).

Topic 1.2 introduces the *solution* (blockchain).

Preparation: Review the concepts of trust and ledgers from today's session.

Essential Reading:

- Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System"
- Graeber, D. (2011). "Debt: The First 5,000 Years" (Ch. 1-3)

Online Resources:

- Course notebook: `NB01_ledger_simulation.ipynb`
- World Bank Global Findex Database (unbanked statistics)
- Bitcoin whitepaper: bitcoin.org/bitcoin.pdf

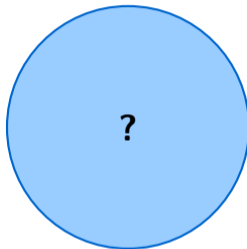
Videos:

- 3Blue1Brown: "But how does bitcoin actually work?"
- Antonopoulos: "What is Money?" (YouTube)

Course Materials

All slides and notebooks available on the course website.

Questions & Discussion



What Is Money, Really?

Contact: joerg.osterrieder@gmail.com

Next Topic: T1.2 — From Ledgers to Blockchains