Blockchain Foundations

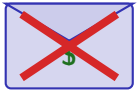
Mini-Lecture: Trust, Scarcity, and Coordination

Prof. Dr. J. Osterrieder

Spring 2026

Why Can't You Email a Dollar Bill?

- Physical cash is scarce by nature – you hand it over and it is gone
- Digital files can be copied infinitely: emails, photos, PDFs
- **The copy problem**: how do you make a digital object *un-copyable*?
- Before 2009, every solution required a trusted middleman (bank, PayPal, Visa)



Cannot copy-paste value

Insight

Before Bitcoin, digital money always needed a referee.

Four problems: trust, scarcity, decentralization, coordination.

What Happens When Trust Fails?

- **Cyprus 2013**: government froze bank accounts overnight – savers lost up to 47.5% of deposits above €100k
- **2008 crisis**: "too big to fail" banks were bailed out with taxpayer money while depositors bore the risk
- Citizens discovered that "your money" is really a promise from an institution
- Bitcoin genesis block embedded the headline: *"Chancellor on brink of second bailout for banks"*

Institutional trust can break

Reflection

"Have you ever been unable to access your own money?"

These events drove early Bitcoin adoption.

What is a Blockchain?

- **Shared**: thousands of identical copies across the network – no single owner
- **Permanent**: once written, data cannot be erased or altered without redoing all subsequent work
- **Decentralized**: no single point of failure or control
- Each block contains a cryptographic hash of the previous block, forming an unbreakable chain

Each hash locks the previous block

Insight

A blockchain is a shared notebook that nobody can erase.

Three properties: shared, permanent, decentralized.

Bitcoin's First Transaction

- **Jan 12, 2009**: Satoshi Nakamoto sends 10 BTC to Hal Finney – the first person-to-person Bitcoin transfer (Block 170)
- **May 22, 2010**: Laszlo Hanyecz pays 10,000 BTC for two pizzas ($41 at the time, worth >$1 billion today)
- These transactions proved that digital scarcity works: each BTC could only be spent once
- No bank, no intermediary – just cryptographic proof

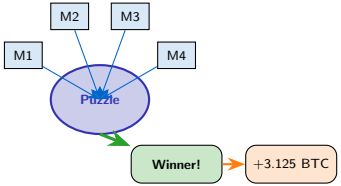
Insight

Those 10,000 BTC for pizza could only be spent once – scarcity works.

Bitcoin Pizza Day (May 22) celebrates the first real-world purchase.

How Do 50,000 Computers Agree?

- **Consensus lottery**: miners compete to solve a cryptographic puzzle – first valid solution wins the right to add the next block
- **Ticket price**: electricity and hardware – real economic cost that deters cheaters
- **Prize**: newly minted BTC (currently 3.125 BTC per block) plus transaction fees
- Honesty pays more than fraud because honest blocks earn rewards while attack blocks get rejected



One winner every ∼10 minutes

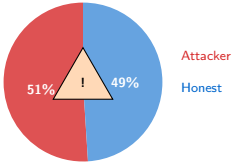
Insight

Proof of Work converts electricity into security.

The math makes honesty more profitable than cheating.

What if Someone Controls 51%?

- A **51% attack** means one entity controls the majority of mining power and can rewrite recent history
- The attacker could double-spend coins but *cannot* steal from arbitrary addresses or create coins from nothing
- **GHash.io (2014)**: mining pool briefly exceeded 51% – voluntarily reduced to preserve network trust and BTC price
- Cost estimate for Bitcoin: $>$ \$20 billion in hardware plus ongoing electricity – far exceeding any potential gain



Attack cost far exceeds potential gain

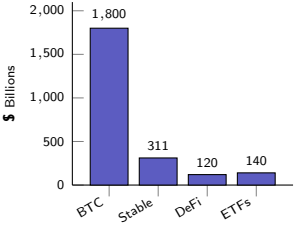
Insight

For Bitcoin, a 51% attack costs billions but gains almost nothing.

Network size is the ultimate security mechanism.

Where is Blockchain Used Today?

- **Bitcoin market cap**: ∼$1.8 trillion – larger than most countries' GDP
- **Stablecoins**: $311 billion in circulation (USDT, USDC) – the "dollar rails" of crypto
- **DeFi TVL**: $120 billion locked in decentralized lending, trading, and derivatives
- **Bitcoin ETFs**: $140 billion AUM – surpassed gold ETFs in December 2024



Insight

Institutional adoption is accelerating – ETFs surpassed gold in 2024.

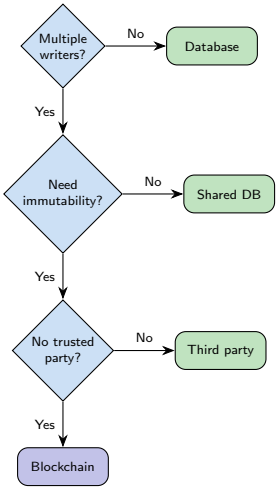
Source: CoinGecko, DefiLlama (Jan 2026).

When Should You Use Blockchain?

- Start with a simple question: **do multiple parties need to write to the same ledger?**
- If one party controls the data, a database is simpler, faster, and cheaper
- If you need immutability but trust exists, a shared database with audit logs suffices
- Blockchain is justified only when *all three* conditions hold: multiple writers, immutability required, no trusted third party

Insight

Most use cases exit the tree before reaching blockchain.



The honest starting point is always "use a database."

4 Things to Remember

1. **Trust via math**: Blockchain replaces institutional trust with cryptographically verifiable rules – no referee needed
2. **Scarcity via consensus**: Digital scarcity is enforced by network-wide agreement, not by preventing copies
3. **Decentralization has costs**: Slower speed, higher energy consumption, greater complexity than centralized alternatives
4. **Incentives align honesty**: The economic math makes cheating unprofitable – honest participation earns rewards while attacks cost more than they gain

Remember

These 4 tensions will reappear in every topic this semester.

Blockchain is a tool, not a solution – evaluate against specific requirements.

Your Challenge

1. Pick any financial service you used this week (payment app, bank transfer, online purchase). Where does it sit on the trust spectrum – fully centralized, partially decentralized, or trustless?
2. Could that service work *without* a central authority? What would you gain (censorship resistance, transparency)? What would you lose (speed, consumer protection, convenience)?
3. Apply the 3-question decision tree from this lecture: Does your chosen service actually *need* a blockchain?

Coming next:

- L02a – DLT Fundamentals: taxonomy, Byzantine Generals, network topologies
- L02b – DLT Architecture: block structure, Merkle trees, node types
- L03 – Hash Functions: the cryptographic glue that holds it all together

Bring your answers to class – we'll discuss in groups.

Quiz – Questions 1–5

Q1. Which best describes a blockchain?
A) Centralized database B) Shared, append-only ledger C) Encrypted file on one server D) Cloud storage

Quiz – Questions 1–5

Q1. Which best describes a blockchain?
A) Centralized database B) Shared, append-only ledger C) Encrypted file on one server D) Cloud storage
B – Shared (distributed), permanent (append-only), maintained by many nodes.

Q2. What is the double-spending problem?
A) Spending more than your balance B) Paying twice for one item C) Sending same token to two people D) A banking bug

Quiz – Questions 1–5

Q1. Which best describes a blockchain?
A) Centralized database B) Shared, append-only ledger C) Encrypted file on one server D) Cloud storage
B – Shared (distributed), permanent (append-only), maintained by many nodes.

Q2. What is the double-spending problem?
A) Spending more than your balance B) Paying twice for one item C) Sending same token to two people D) A banking bug
C – Digital data can be copied; without consensus, the same coin goes to two recipients.

Q3. In PoW, what is the "ticket price" for the consensus lottery?
A) Coins held B) Bandwidth C) Electricity and hardware D) Transaction fees

Quiz – Questions 1–5

Q1. Which best describes a blockchain?
A) Centralized database B) Shared, append-only ledger C) Encrypted file on one server D) Cloud storage
B – Shared (distributed), permanent (append-only), maintained by many nodes.

Q2. What is the double-spending problem?
A) Spending more than your balance B) Paying twice for one item C) Sending same token to two people D) A banking bug
C – Digital data can be copied; without consensus, the same coin goes to two recipients.

Q3. In PoW, what is the "ticket price" for the consensus lottery?
A) Coins held B) Bandwidth C) Electricity and hardware D) Transaction fees
C – Real energy cost deters cheaters by making attacks expensive.

Q4. Bitcoin chose which two trilemma properties?
A) Scalability + decentralization B) Security + scalability C) Security + decentralization D) Speed + security

Quiz – Questions 1–5

Q1. Which best describes a blockchain?
A) Centralized database B) Shared, append-only ledger C) Encrypted file on one server D) Cloud storage
B – Shared (distributed), permanent (append-only), maintained by many nodes.

Q2. What is the double-spending problem?
A) Spending more than your balance B) Paying twice for one item C) Sending same token to two people D) A banking bug
C – Digital data can be copied; without consensus, the same coin goes to two recipients.

Q3. In PoW, what is the "ticket price" for the consensus lottery?
A) Coins held B) Bandwidth C) Electricity and hardware D) Transaction fees
C – Real energy cost deters cheaters by making attacks expensive.

Q4. Bitcoin chose which two trilemma properties?
A) Scalability + decentralization B) Security + scalability C) Security + decentralization D) Speed + security
C – Security and decentralization, sacrificing scalability ($\sim$7 TPS).

Q5. Alice sends her only 1 BTC to both Bob and Carol. What happens?
A) Both receive 1 BTC B) Network rejects one via consensus C) Alice is banned D) Both reversed

Quiz – Questions 1–5

Q1. Which best describes a blockchain?
A) Centralized database B) Shared, append-only ledger C) Encrypted file on one server D) Cloud storage
B – Shared (distributed), permanent (append-only), maintained by many nodes.

Q2. What is the double-spending problem?
A) Spending more than your balance B) Paying twice for one item C) Sending same token to two people D) A banking bug
C – Digital data can be copied; without consensus, the same coin goes to two recipients.

Q3. In PoW, what is the "ticket price" for the consensus lottery?
A) Coins held B) Bandwidth C) Electricity and hardware D) Transaction fees
C – Real energy cost deters cheaters by making attacks expensive.

Q4. Bitcoin chose which two trilemma properties?
A) Scalability + decentralization B) Security + scalability C) Security + decentralization D) Speed + security
C – Security and decentralization, sacrificing scalability ($\sim$7 TPS).

Q5. Alice sends her only 1 BTC to both Bob and Carol. What happens?
A) Both receive 1 BTC B) Network rejects one via consensus C) Alice is banned D) Both reversed
B – Consensus confirms only one transaction; the other is rejected.

Answers reveal on click. Review any incorrect answers before proceeding.

Quiz – Questions 6–10

Q6. Block 100 is tampered. What happens to Blocks 101–110?
A) Nothing B) Only Block 101 changes C) All subsequent hashes become invalid D) Network auto-repairs

Quiz – Questions 6–10

Q6. Block 100 is tampered. What happens to Blocks 101–110?
A) Nothing B) Only Block 101 changes C) All subsequent hashes become invalid D) Network auto-repairs
C – Each hash depends on the previous block; changing one breaks the entire chain after it.

Q7. Why did GHash.io voluntarily drop below 51% in 2014?
A) Regulation forced them B) Equipment overheated C) Preserving trust protected their revenue D) Satoshi asked

Quiz – Questions 6–10

Q6. Block 100 is tampered. What happens to Blocks 101–110?
A) Nothing B) Only Block 101 changes C) All subsequent hashes become invalid D) Network auto-repairs
C – Each hash depends on the previous block; changing one breaks the entire chain after it.

Q7. Why did GHash.io voluntarily drop below 51% in 2014?
A) Regulation forced them B) Equipment overheated C) Preserving trust protected their revenue D) Satoshi asked
C – Attacking would crash BTC's price, destroying the value of their own rewards.

Q8. Mt. Gox's collapse was a failure of...
A) Bitcoin protocol B) Centralized exchange security C) Proof of Work D) Hash functions

Quiz – Questions 6–10

Q6. Block 100 is tampered. What happens to Blocks 101–110?
A) Nothing B) Only Block 101 changes C) All subsequent hashes become invalid D) Network auto-repairs
C – Each hash depends on the previous block; changing one breaks the entire chain after it.

Q7. Why did GHash.io voluntarily drop below 51% in 2014?
A) Regulation forced them B) Equipment overheated C) Preserving trust protected their revenue D) Satoshi asked
C – Attacking would crash BTC's price, destroying the value of their own rewards.

Q8. Mt. Gox's collapse was a failure of...
A) Bitcoin protocol B) Centralized exchange security C) Proof of Work D) Hash functions
B – Mt. Gox was a centralized custodian; Bitcoin's protocol worked correctly throughout.

Q9. When should you NOT use a blockchain?
A) Cross-border payments, no trust B) Company internal inventory C) Charity donation tracking D) Voting under censorship

Quiz – Questions 6–10

Q6. Block 100 is tampered. What happens to Blocks 101–110?
A) Nothing B) Only Block 101 changes C) All subsequent hashes become invalid D) Network auto-repairs
C – Each hash depends on the previous block; changing one breaks the entire chain after it.

Q7. Why did GHash.io voluntarily drop below 51% in 2014?
A) Regulation forced them B) Equipment overheated C) Preserving trust protected their revenue D) Satoshi asked
C – Attacking would crash BTC's price, destroying the value of their own rewards.

Q8. Mt. Gox's collapse was a failure of...
A) Bitcoin protocol B) Centralized exchange security C) Proof of Work D) Hash functions
B – Mt. Gox was a centralized custodian; Bitcoin's protocol worked correctly throughout.

Q9. When should you NOT use a blockchain?
A) Cross-border payments, no trust B) Company internal inventory C) Charity donation tracking D) Voting under censorship
B – Single company, one writer, trusted party – a standard database suffices.

Q10. "Bitcoin's energy is wasteful." Best counterargument?
A) Uses less than gaming B) Energy cost is the security mechanism C) Will switch to solar D) Decreases over time

Quiz – Questions 6–10

Q6. Block 100 is tampered. What happens to Blocks 101–110?
A) Nothing B) Only Block 101 changes C) All subsequent hashes become invalid D) Network auto-repairs
C – Each hash depends on the previous block; changing one breaks the entire chain after it.

Q7. Why did GHash.io voluntarily drop below 51% in 2014?
A) Regulation forced them B) Equipment overheated C) Preserving trust protected their revenue D) Satoshi asked
C – Attacking would crash BTC's price, destroying the value of their own rewards.

Q8. Mt. Gox's collapse was a failure of...
A) Bitcoin protocol B) Centralized exchange security C) Proof of Work D) Hash functions
B – Mt. Gox was a centralized custodian; Bitcoin's protocol worked correctly throughout.

Q9. When should you NOT use a blockchain?
A) Cross-border payments, no trust B) Company internal inventory C) Charity donation tracking D) Voting under censorship
B – Single company, one writer, trusted party – a standard database suffices.

Q10. "Bitcoin's energy is wasteful." Best counterargument?
A) Uses less than gaming B) Energy cost is the security mechanism C) Will switch to solar D) Decreases over time
B – Energy expenditure is the security budget; it makes rewriting history prohibitively expensive.

Score: 9–10 Excellent | 7–8 Good | 5–6 Review slides | <5 Re-watch lecture.