Blockchain Foundations: Trust, Scarcity, and Coordination

Four Problems That Changed Finance

Prof. Dr. J. Osterrieder

BSc Blockchain, Crypto Economy & NFTs

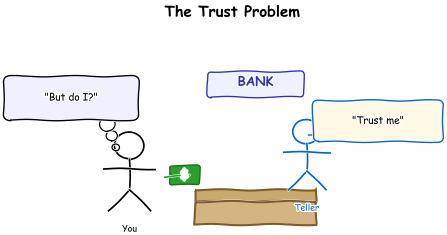
Spring 2026

[Cartoon] Why Do You Trust Your Bank?

You hand your paycheck to a stranger in a building. They write a number in their computer. You believe them. **Why?**

What if that building closes?
What if they change the number?

Every day, billions of people trust institutions they have never audited, run by people they have never met, using systems they cannot inspect.



This is the oldest problem in finance: how do you trust someone with your money?

Learning Objectives

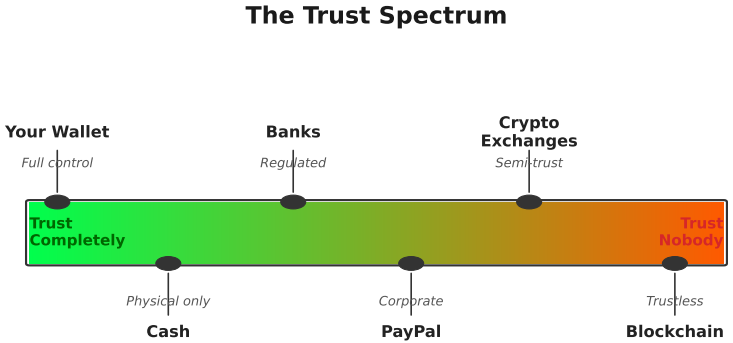
By the end of this lecture, you will be able to:

1. Explain why digital trust requires different solutions than physical trust
2. Describe how blockchain creates digital scarcity without a central authority
3. Compare what is gained and sacrificed by removing intermediaries
4. Illustrate how computers reach agreement without a leader
5. Evaluate when blockchain is (and is not) the right solution

No prerequisites required — we build every concept from everyday experience.

No prerequisites required — we build every concept from everyday experience

Who Do You Trust With Your Money?



- **What you see:** A horizontal spectrum from full trust (cash in your wallet) to zero trust (blockchain)
- **Key pattern:** Each step rightward removes one layer of human trust and replaces it with a technical mechanism
- **Takeaway:** Blockchain is not anti-trust; it moves trust from people to transparent, verifiable rules

Blockchain's radical idea: replace trust in institutions with trust in math

Why Can't You Email a Dollar Bill?

Physical scarcity is free — you cannot photocopy a gold coin. But anything digital can be copied infinitely: music, photos, documents.

This never mattered for cat videos. But it is a **disaster** for money.

The Copy Problem: If Alice emails Bob 1 Bitcoin, what stops her from emailing that same file to Carol?

This is the **double-spending problem**.

Worked Example

Imagine a spreadsheet: Alice has 10 coins. She sends 10 to Bob *and* 10 to Carol at the same time. Who gets paid?

Before Bitcoin, every digital payment system needed a trusted referee (bank, PayPal) to prevent copying

How Can 50,000 Computers Agree Without a Boss?

Imagine 50,000 strangers in different countries all keeping the same notebook. No phone, no email, no leader.

How do they agree on what to write next?

Some might lie. Some might be offline. Some might try to write different things at the same time.

This is the **consensus problem**.

Blockchain solves it — but at a cost: it is *much* slower than just asking one person (a bank) to keep the notebook.

The Trade-off

Bitcoin processes 7 transactions per second.
Visa processes 65,000.
The difference is the price of decentralization.

The decentralization trade-off: trustless agreement is expensive

What Happens When Trust Fails?

2013 Cyprus: Banks froze accounts overnight. People with life savings could not withdraw their own money.

A central authority decided who gets access to their own funds.

2022 Canada: During the trucker protests, the government froze bank accounts of donors — without a court order.

2008 Financial Crisis: Banks made risky bets with depositor money. When those bets failed, governments bailed them out with taxpayer money.

Nobody asked the taxpayers.

Blockchain asks:
What if nobody had that power?

These events drove early Bitcoin adoption — distrust of centralized financial control

What is a Blockchain, Really?

A blockchain is a shared notebook that:

1. **Everyone** can read
2. **Nobody** can erase
3. **No single person** controls

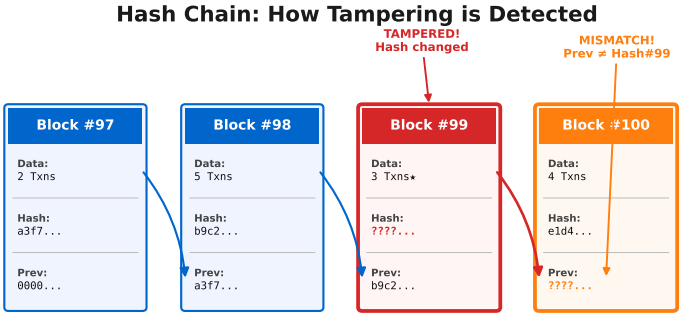
Technically: an append-only, distributed ledger secured by cryptographic hashing.

Intuitive Analogy

Think of it as a Google Doc that 50,000 people share, but once something is written, no one can delete it — not even Google.
Append-only means you can only add new lines. *Distributed* means every participant has a full copy. *Cryptographic hashing* means each page contains a fingerprint of the previous page, so tampering is instantly detectable.

Three words: shared, permanent, decentralized

How Does the Chain in Blockchain Work?



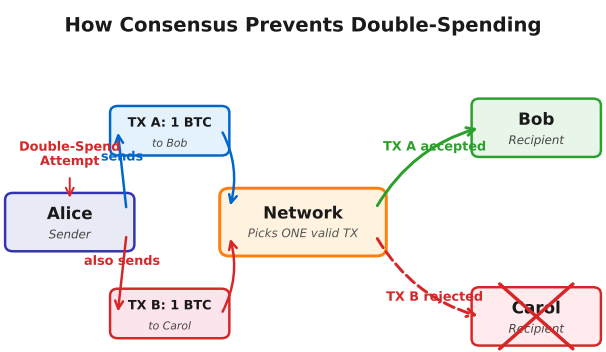
Changing any block breaks all subsequent hashes → tampering is instantly detectable

- **What you see:** Four blocks in sequence, each containing a hash pointer to the previous block
- **Key pattern:** Changing any block's data changes its hash, breaking the link from the next block
- **Takeaway:** Tamper-evidence is automatic and requires zero human oversight

Imagine writing today's page number on yesterday's page. If someone rips out a page, the numbers don't match.

Hash pointers: the cryptographic glue that makes blockchain tamper-evident

How Do You Make Something Digital That Can't Be Copied?



- **What you see:** Alice broadcasts two conflicting transactions; the network validates one, rejects the duplicate
- **Key pattern:** The network achieves consensus on which copy is the "real" one
- **Takeaway:** Digital scarcity is enforced by agreement, not by prevention

Worked example: Alice has 1 BTC. She sends it to Bob (TX A) and Carol (TX B). The network votes: TX A wins. TX B is rejected.

Digital scarcity = consensus on which copy counts, not preventing copies

Physical vs Digital: Why the Rules Change

Property	Physical Asset	Digital Asset	Blockchain Asset
Scarcity	Naturally scarce	Infinitely copiable	Enforced by protocol
Reach	Local / Regional	Global instantly	Global & permissionless
Speed	Days / Weeks	Milliseconds	Seconds / Minutes
Reversibility	Hard to reverse	Easy to reverse (chargeback)	Irreversible by design
Programmability	None	Limited (APIs, apps)	Full: smart contracts
Cost to Transfer	High (logistics, fees)	Near zero (card fees)	Low & flat (gas fees)

- **What you see:** Side-by-side comparison of physical and digital asset properties across six dimensions
- **Key pattern:** Physical and digital worlds have opposite defaults; blockchain selectively imports scarcity into digital
- **Takeaway:** Blockchain adds one missing property (scarcity) while keeping digital advantages

Blockchain's innovation: scarcity in a world of infinite copies

What Was Bitcoin's Very First Transaction?

January 12, 2009: Satoshi Nakamoto sent 10 BTC to Hal Finney. No bank. No intermediary. Just two computers agreeing.

Block #170, Transaction #1.
Still visible on the blockchain today.

The first peer-to-peer digital cash transfer in history.

May 22, 2010: Laszlo Hanyecz paid 10,000 BTC for two pizzas ($41 at the time).

Today: worth over $1 billion.

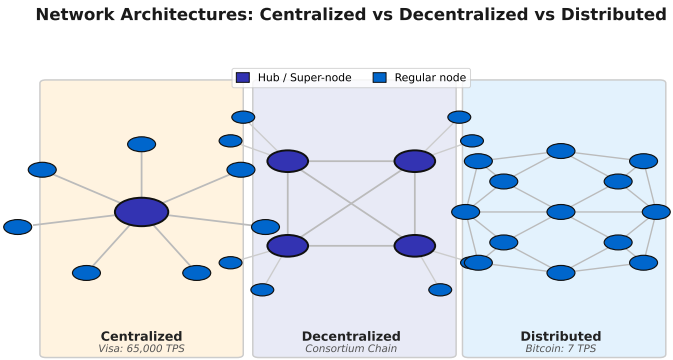
This proved digital scarcity works: those 10,000 BTC could only be spent **once**.

Why It Matters

The pizza transaction was the first real-world purchase using blockchain — proving the technology works outside a lab.

Bitcoin Pizza Day (May 22) is celebrated annually — the first real-world blockchain purchase

Centralized vs Decentralized vs Distributed: What's the Difference?



- **What you see:** Three network topologies with real-world examples and performance numbers
- **Key pattern:** As control spreads, throughput drops but resilience increases
- **Takeaway:** Network architecture is a design choice, not a quality ranking

Bitcoin trades speed for unstoppability — nobody can turn it off

Worked Example: How Does a Hash Fingerprint Work?

A hash function takes any input and produces a fixed-length "fingerprint." Here is SHA-256 in action:

Step 1: Input `"Hello"`
Output: `185f8db3...` *(64 hex characters)*

Step 2: Input `"hello"` (lowercase h)
Output: `2cf24dba...` *(completely different!)*

Step 3: Input `"Hello World"`
Output: `a591a6d4...` *(completely different!)*

Key insight: Tiny change = totally different fingerprint.
This is the **avalanche effect**.

Why this matters for blockchain:

If someone changes even one letter in a block, the fingerprint changes. Everyone on the network notices immediately.

Properties you need to remember:

- **One-way:** You cannot reverse-engineer the input from the output
- **Deterministic:** Same input always gives the same output
- **Collision-resistant:** Practically impossible to find two inputs with the same output

SHA-256 produces a 256-bit fingerprint — more possible values than atoms in the observable universe

Worked Example: Can You Detect Tampering?

Original chain (valid):

Block 100: "Alice pays Bob 5 BTC"
Fingerprint: `abc123`

Block 101: Previous = `abc123`
Fingerprint: `def456`

Block 102: Previous = `def456`

Now tamper with Block 100:
Change to "Alice pays Bob **0** BTC"
New fingerprint: `xyz789`

MISMATCH! Block 101 says "previous = `abc123`" but Block 100 now shows `xyz789`.

The chain breaks at the point of tampering.

To hide the change, the attacker must recompute *every single block* after Block 100.

On Bitcoin, that means racing against 50,000+ computers that are continuously adding new blocks.

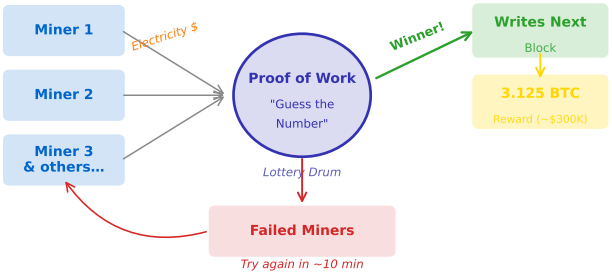
Practical Impossibility

Rewriting 6 blocks deep would require more electricity than a small country uses in a day.

Blockchain is called immutable — not because change is impossible, but because it is impractical

How Do 50,000 Computers Pick Who Writes the Next Page?

The Consensus Lottery: How Bitcoin Picks a Block Writer



- **What you see:** A lottery drum metaphor showing miners feeding electricity; the winner receives the block reward
- **Key pattern:** Cost is paid upfront, creating credible commitment that discourages dishonest entries
- **Takeaway:** Proof of Work converts energy expenditure into network security

Every 10 minutes, Bitcoin runs a global lottery. The "ticket price" is electricity. The "prize" is 3.125 BTC (about $300,000).

Proof of Work: the more electricity you spend, the more lottery tickets you buy

Why Would Anyone Play an Expensive Lottery?

Honest Play

- Spend $50,000 on electricity
- Submit a valid block with real transactions
- Network accepts your block
- Earn $300,000 in block rewards

Profit: $250,000

Cheating

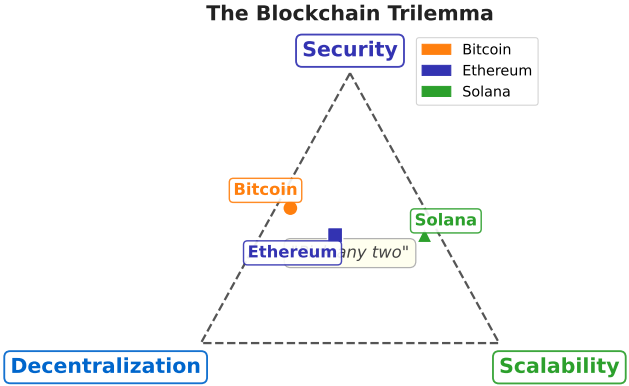
- Spend $50,000 on electricity
- Submit a fake block with fraudulent transactions
- Network rejects your block
- Earn nothing

Loss: $50,000

The math makes honesty more profitable than cheating. This is the core of **cryptoeconomics**: designing systems where the economically rational choice is also the honest choice.

Incentive-compatible design: honest behavior is the Nash equilibrium

Why Can't Blockchain Be Fast, Secure, AND Decentralized?



- **What you see:** A triangle with Bitcoin, Ethereum, and Solana plotted at different positions
- **Key pattern:** No system occupies the center — every blockchain sacrifices one property
- **Takeaway:** The trilemma is a fundamental design trade-off, not a temporary limitation

Pick any two: Bitcoin chose security + decentralization (7 TPS). Solana chose security + scalability (fewer validators).

Layer 2 solutions (Lightning Network, rollups) attempt to break the trilemma

What is Actually Inside a Block?

Block Header (80 bytes):

- Version number
- Previous block fingerprint (hash)
- Merkle root (fingerprint of all transactions)
- Timestamp
- Difficulty target
- Nonce (the lottery guess)

The header is like the front page of a newspaper: date, edition number, and a summary of what is inside.

Block Body (up to 4 MB):

- List of transactions (2,000–3,000 per block)
- Each transaction: sender, receiver, amount, signature

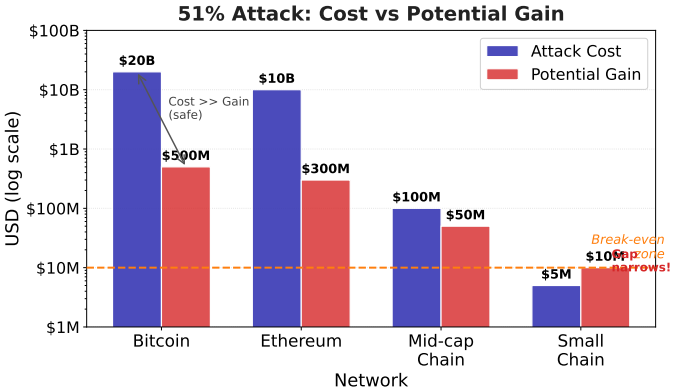
Think of it as a page in a notebook: the header is the page number and date; the body is the actual entries.

Real-World Example

Bitcoin Block #840,000 (April 20, 2024):
3,050 transactions — the 4th halving block.

The block header is only 80 bytes — small enough to verify on a mobile phone

What if Someone Buys Half the Lottery Tickets?



- **What you see:** Grouped bars comparing attack cost vs potential gain for different networks
- **Key pattern:** For large networks, cost dwarfs gain by orders of magnitude; for small networks the gap narrows
- **Takeaway:** Network size is the ultimate security mechanism

2014: GHash.io briefly reached 51%. They voluntarily reduced — attacking would destroy their own bitcoins.

Attack cost rises with network size — Bitcoin's security budget exceeds $15 billion per year

Has Blockchain Ever Failed?

Mt. Gox (2014):
Exchange hacked, $450M in Bitcoin lost.

Not a blockchain failure — the centralized exchange was the weak point. The Bitcoin blockchain itself continued operating without interruption.

Key distinction:
The lock on the vault was fine.
The guard at the door was not.

Terra/Luna (2022):
Algorithmic stablecoin collapsed, $40B wiped out in one week.

The blockchain worked perfectly — the *economic design* was flawed.

Key Lesson

Blockchain secures data.
It does **not** guarantee that the data represents something valuable.

Most "blockchain failures" are actually failures of centralized services built on top of blockchains

Does Blockchain Waste Energy?

Bitcoin's energy use:
Approximately 150 TWh per year — comparable to Argentina.

That sounds enormous. But what does it buy?

- A payment network that cannot be censored
- A store of value that cannot be inflated
- A settlement layer that never closes
- No buildings, no branches, no employees

For comparison:
Global banking system: estimated 260 TWh per year (buildings, ATMs, data centers, armored trucks).

Bitcoin secures $1.8 trillion with no physical infrastructure.

The real question:
Is the energy cost justified by the trust it produces?

The alternative:
Proof of Stake (Ethereum since Sept 2022) reduces energy use by 99.95%.

Proof of Stake (Ethereum since 2022) reduces energy use by 99.95%

Where is Blockchain Actually Used in Finance?

Cryptocurrency Markets (2026):

- Bitcoin market cap: $1.8T
- Stablecoins: $311B
- DeFi protocols: $120B locked
- Daily trading volume: $50B+

These are not toy numbers — stablecoins alone process more daily volume than PayPal.

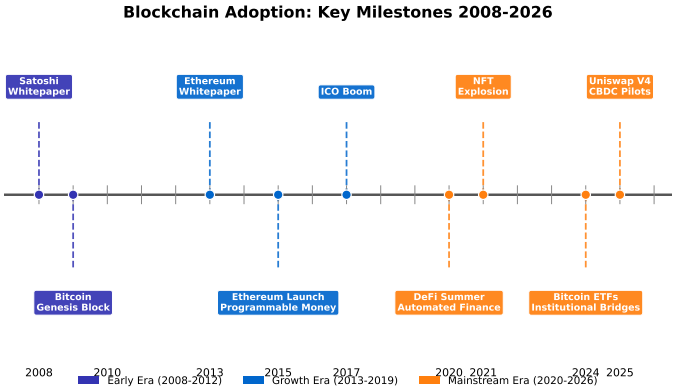
Institutional Adoption:

- Bitcoin ETFs: $140B in assets (surpassed gold ETFs Dec 2024)
- JPMorgan Onyx: $1B+ daily settlements
- BlackRock BUIDL: tokenized Treasury fund

The same banks that dismissed Bitcoin in 2017 are now building on it.

Source: CoinGecko, DefiLlama (Jan 2026) — Institutional adoption accelerating

What Else Can Blockchain Do?



- **What you see:** Timeline from 2008 to 2026 with five major waves annotated
- **Key pattern:** Each wave expanded what blockchain coordinates — from value transfer to full financial systems
- **Takeaway:** Adoption follows a widening pattern; each wave builds on prior infrastructure

Each wave expanded what blockchain can coordinate: money, contracts, markets, institutions

Are Governments and Companies Using Blockchain?

Government CBDCs:

- China e-CNY: 260M+ wallets
- EU Digital Euro: pilot phase
- 130+ countries exploring CBDCs

CBDCs use blockchain technology but are *centrally controlled* — the opposite of Bitcoin's philosophy.

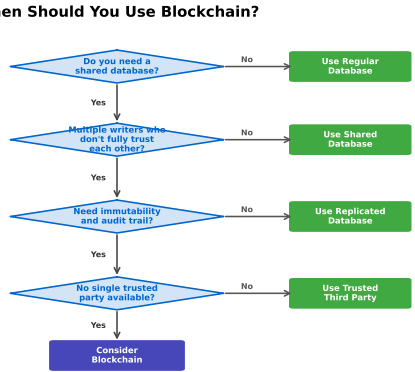
Enterprise Adoption:

- IBM Food Trust: 500+ organizations
- RWA tokenization: $15B+ in real-world assets on-chain
- Supply chain tracking across borders

Companies use blockchain where multiple parties need a shared source of truth without trusting each other.

Irony: governments use blockchain technology to build centralized digital currencies

When is Blockchain the Right Answer?



- **What you see:** A three-question decision tree where each "No" exits to "Use a database"
- **Key pattern:** Most scenarios exit before reaching blockchain — the filter is intentionally strict
- **Takeaway:** The honest starting point is "use a database"; blockchain only when trust, immutability, and multi-party coordination are all required

Most enterprise "blockchain" projects could use a replicated database — be honest about the trade-offs

What Does Blockchain Change About Society?

What blockchain enables:

- Trustless coordination between strangers
- Digital ownership without intermediaries
- Programmable, transparent finance
- Global financial access (1.4B unbanked)

For the first time, you can own a digital asset the way you own a physical object — without asking anyone's permission.

What blockchain does NOT solve:

- Human greed (Terra/Luna)
- Bad governance (The DAO hack, 2016)
- Unequal access (requires internet, devices)
- Climate concerns (Proof of Work energy)

Technology does not fix human problems — it changes the toolkit available to address them.

Blockchain is a tool, not a solution — its value depends on the problem it addresses

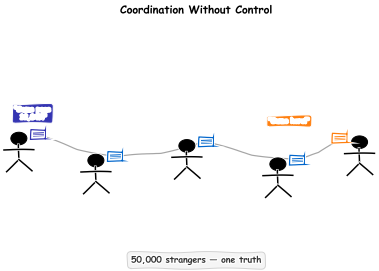
[Cartoon] 50,000 Strangers Keeping the Same Notebook

We started with a question: *how can strangers trust each other without a bank?*

Blockchain's answer:

- Replace the bank with math
- Replace trust with verification
- Replace one notebook with 50,000 identical copies

The cost? Speed, energy, complexity.
The gain? A system that nobody controls and everybody can verify.



From trust to trustless: blockchain's fundamental contribution to coordination

Key Takeaways

Four ideas to remember from today:

1. **Trust:** Blockchain solves the trust problem — strangers can transact without intermediaries
2. **Scarcity:** Digital scarcity is created through consensus, not by preventing copies
3. **Cost:** Decentralization has real costs — slower speed, higher energy, more complexity
4. **Design:** Coordination without control works through incentive-compatible design

Decision Heuristic:

$$\text{Blockchain Value is proportional to } (\text{Trust Deficit} \times \text{Coordination Benefit}) \,/\, \text{Performance Requirements}$$

If the trust deficit is low or performance requirements are high, a traditional database is likely the better choice.

Blockchain is a tool, not a solution — evaluate against specific requirements

Summary and What Comes Next

Today we learned:

- The 4 core tensions: trust, scarcity, coordination, trade-offs
- How hash chains create tamper-evidence
- How consensus turns energy into security
- Why the trilemma forces design choices

Coming next:

- **L02a** — DLT Fundamentals: Byzantine fault tolerance, network models
- **L02b** — DLT Architecture: Merkle trees, block structure, node types
- **L03** — Hash Functions: SHA-256 internals, birthday attacks, mining

Reflection Questions:

1. Why does removing a trusted intermediary make everything slower?
2. Can you name a real-world situation where blockchain's trade-offs are worth it?
3. What is the difference between "trustless" and "no trust required"?

Review the 4 tensions — they will reappear in every topic this semester

Quiz: Questions 1–5

Q1. Which of the following best describes a blockchain?
A) A centralized database managed by a company
B) A distributed, append-only ledger that no single party controls
C) An encrypted file system for storing passwords
D) A cloud computing platform for running applications

Quiz: Questions 1–5

Q1. Which of the following best describes a blockchain?
A) A centralized database managed by a company
B) A distributed, append-only ledger that no single party controls
C) An encrypted file system for storing passwords
D) A cloud computing platform for running applications
Answer: B – A blockchain is a shared, append-only ledger where no single party controls the data.

Q2. What is the purpose of a hash pointer in a blockchain?
A) To encrypt transaction data so only the sender can read it
B) To link each block to the previous one and detect tampering
C) To store the wallet addresses of all participants
D) To calculate the transaction fees for each block

Quiz: Questions 1–5

Q1. Which of the following best describes a blockchain?
A) A centralized database managed by a company
B) A distributed, append-only ledger that no single party controls
C) An encrypted file system for storing passwords
D) A cloud computing platform for running applications
Answer: B – A blockchain is a shared, append-only ledger where no single party controls the data.

Q2. What is the purpose of a hash pointer in a blockchain?
A) To encrypt transaction data so only the sender can read it
B) To link each block to the previous one and detect tampering
C) To store the wallet addresses of all participants
D) To calculate the transaction fees for each block
Answer: B – Hash pointers create tamper-evident links; changing any block invalidates all subsequent hashes.

Q3. The double-spending problem refers to:
A) Paying twice the normal transaction fee
B) Spending the same digital coin more than once
C) Two miners finding a block at the same time
D) A user creating two separate wallets

Quiz: Questions 1–5

Q1. Which of the following best describes a blockchain?
A) A centralized database managed by a company
B) A distributed, append-only ledger that no single party controls
C) An encrypted file system for storing passwords
D) A cloud computing platform for running applications
Answer: B – A blockchain is a shared, append-only ledger where no single party controls the data.

Q2. What is the purpose of a hash pointer in a blockchain?
A) To encrypt transaction data so only the sender can read it
B) To link each block to the previous one and detect tampering
C) To store the wallet addresses of all participants
D) To calculate the transaction fees for each block
Answer: B – Hash pointers create tamper-evident links; changing any block invalidates all subsequent hashes.

Q3. The double-spending problem refers to:
A) Paying twice the normal transaction fee
B) Spending the same digital coin more than once
C) Two miners finding a block at the same time
D) A user creating two separate wallets
Answer: B – Without a mechanism to prevent it, digital money can be copied and spent multiple times.

Q4. What does Proof of Work achieve for the Bitcoin network?
A) It encrypts all transactions for privacy
B) It makes honest block creation more profitable than cheating
C) It increases transaction speed to match Visa
D) It eliminates the need for internet connectivity

Quiz: Questions 1–5

Q1. Which of the following best describes a blockchain?
A) A centralized database managed by a company
B) A distributed, append-only ledger that no single party controls
C) An encrypted file system for storing passwords
D) A cloud computing platform for running applications
Answer: B – A blockchain is a shared, append-only ledger where no single party controls the data.

Q2. What is the purpose of a hash pointer in a blockchain?
A) To encrypt transaction data so only the sender can read it
B) To link each block to the previous one and detect tampering
C) To store the wallet addresses of all participants
D) To calculate the transaction fees for each block
Answer: B – Hash pointers create tamper-evident links; changing any block invalidates all subsequent hashes.

Q3. The double-spending problem refers to:
A) Paying twice the normal transaction fee
B) Spending the same digital coin more than once
C) Two miners finding a block at the same time
D) A user creating two separate wallets
Answer: B – Without a mechanism to prevent it, digital money can be copied and spent multiple times.

Q4. What does Proof of Work achieve for the Bitcoin network?
A) It encrypts all transactions for privacy
B) It makes honest block creation more profitable than cheating
C) It increases transaction speed to match Visa
D) It eliminates the need for internet connectivity
Answer: B – PoW ensures that miners who follow the rules earn rewards, while cheaters waste their electricity.

Q5. Alice has 1 BTC. She sends it to Bob and Carol at the same time. What happens?
A) Both receive 1 BTC (the coin is duplicated)
B) The network rejects both transactions
C) The network accepts one transaction and rejects the other
D) Alice's wallet automatically splits the coin in half

Quiz: Questions 1–5

Q1. Which of the following best describes a blockchain?
A) A centralized database managed by a company
B) A distributed, append-only ledger that no single party controls
C) An encrypted file system for storing passwords
D) A cloud computing platform for running applications
Answer: B – A blockchain is a shared, append-only ledger where no single party controls the data.

Q2. What is the purpose of a hash pointer in a blockchain?
A) To encrypt transaction data so only the sender can read it
B) To link each block to the previous one and detect tampering
C) To store the wallet addresses of all participants
D) To calculate the transaction fees for each block
Answer: B – Hash pointers create tamper-evident links; changing any block invalidates all subsequent hashes.

Q3. The double-spending problem refers to:
A) Paying twice the normal transaction fee
B) Spending the same digital coin more than once
C) Two miners finding a block at the same time
D) A user creating two separate wallets
Answer: B – Without a mechanism to prevent it, digital money can be copied and spent multiple times.

Q4. What does Proof of Work achieve for the Bitcoin network?
A) It encrypts all transactions for privacy
B) It makes honest block creation more profitable than cheating
C) It increases transaction speed to match Visa
D) It eliminates the need for internet connectivity
Answer: B – PoW ensures that miners who follow the rules earn rewards, while cheaters waste their electricity.

Q5. Alice has 1 BTC. She sends it to Bob and Carol at the same time. What happens?
A) Both receive 1 BTC (the coin is duplicated)
B) The network rejects both transactions
C) The network accepts one transaction and rejects the other
D) Alice's wallet automatically splits the coin in half
Answer: C – Consensus determines which transaction is valid; the duplicate is rejected.

Quiz: Questions 6–10

Q6. You hash "Hello" and get `185f...`. You hash "hello" and get `2cf2...`. This demonstrates:
A) A hash collision B) The avalanche effect
C) Preimage resistance D) A broken hash function

Quiz: Questions 6–10

Q6. You hash "Hello" and get `185f...`. You hash "hello" and get `2cf2...`. This demonstrates:
A) A hash collision B) The avalanche effect
C) Preimage resistance D) A broken hash function
Answer: B – The avalanche effect means a tiny input change produces a completely different output.

Q7. Block 50 has fingerprint `abc`. Block 51 stores "previous = `abc`". If someone changes Block 50, what happens?
A) Block 51 automatically updates its "previous" field
B) Block 50's fingerprint changes, creating a mismatch with Block 51
C) Nothing — blocks are independent of each other
D) The network deletes both blocks

Quiz: Questions 6–10

Q6. You hash "Hello" and get `185f...`. You hash "hello" and get `2cf2...`. This demonstrates:
A) A hash collision B) The avalanche effect
C) Preimage resistance D) A broken hash function
Answer: B – The avalanche effect means a tiny input change produces a completely different output.

Q7. Block 50 has fingerprint `abc`. Block 51 stores "previous = `abc`". If someone changes Block 50, what happens?
A) Block 51 automatically updates its "previous" field
B) Block 50's fingerprint changes, creating a mismatch with Block 51
C) Nothing — blocks are independent of each other
D) The network deletes both blocks
Answer: B – The chain breaks at the tampered block because the stored hash no longer matches.

Q8. A new blockchain wants maximum transactions per second and strong security, but accepts fewer validators. Where on the trilemma does it sit?
A) High decentralization, low scalability B) High scalability, low decentralization
C) High decentralization, high scalability D) Low security, high scalability

Quiz: Questions 6–10

Q6. You hash "Hello" and get `185f...`. You hash "hello" and get `2cf2...`. This demonstrates:
A) A hash collision B) The avalanche effect
C) Preimage resistance D) A broken hash function
Answer: B – The avalanche effect means a tiny input change produces a completely different output.

Q7. Block 50 has fingerprint `abc`. Block 51 stores "previous = `abc`". If someone changes Block 50, what happens?
A) Block 51 automatically updates its "previous" field
B) Block 50's fingerprint changes, creating a mismatch with Block 51
C) Nothing — blocks are independent of each other
D) The network deletes both blocks
Answer: B – The chain breaks at the tampered block because the stored hash no longer matches.

Q8. A new blockchain wants maximum transactions per second and strong security, but accepts fewer validators. Where on the trilemma does it sit?
A) High decentralization, low scalability B) High scalability, low decentralization
C) High decentralization, high scalability D) Low security, high scalability
Answer: B – Sacrificing decentralization (fewer validators) is how chains like Solana achieve high throughput.

Q9. Bitcoin's total market capitalization in early 2026 is approximately:
A) \$180 million B) \$18 billion C) \$180 billion D) \$1.8 trillion

Quiz: Questions 6–10

Q6. You hash "Hello" and get `185f...`. You hash "hello" and get `2cf2...`. This demonstrates:
A) A hash collision B) The avalanche effect
C) Preimage resistance D) A broken hash function
Answer: B – The avalanche effect means a tiny input change produces a completely different output.

Q7. Block 50 has fingerprint `abc`. Block 51 stores "previous = `abc`". If someone changes Block 50, what happens?
A) Block 51 automatically updates its "previous" field
B) Block 50's fingerprint changes, creating a mismatch with Block 51
C) Nothing — blocks are independent of each other
D) The network deletes both blocks
Answer: B – The chain breaks at the tampered block because the stored hash no longer matches.

Q8. A new blockchain wants maximum transactions per second and strong security, but accepts fewer validators. Where on the trilemma does it sit?
A) High decentralization, low scalability B) High scalability, low decentralization
C) High decentralization, high scalability D) Low security, high scalability
Answer: B – Sacrificing decentralization (fewer validators) is how chains like Solana achieve high throughput.

Q9. Bitcoin's total market capitalization in early 2026 is approximately:
A) $180 million B) $18 billion C) $180 billion D) $1.8 trillion
Answer: D – Bitcoin's market cap reached approximately $1.8 trillion by January 2026.

Q10. Why is a 51% attack on Bitcoin impractical today?
A) The Bitcoin software prevents it with a built-in lock
B) The cost of acquiring enough computing power far exceeds any potential gain
C) There are laws against it in every country
D) Bitcoin uses Proof of Stake, which makes it impossible

Quiz: Questions 6–10

Q6. You hash "Hello" and get `185f...`. You hash "hello" and get `2cf2...`. This demonstrates:
A) A hash collision B) The avalanche effect
C) Preimage resistance D) A broken hash function
Answer: B – The avalanche effect means a tiny input change produces a completely different output.

Q7. Block 50 has fingerprint `abc`. Block 51 stores "previous = `abc`". If someone changes Block 50, what happens?
A) Block 51 automatically updates its "previous" field
B) Block 50's fingerprint changes, creating a mismatch with Block 51
C) Nothing — blocks are independent of each other
D) The network deletes both blocks
Answer: B – The chain breaks at the tampered block because the stored hash no longer matches.

Q8. A new blockchain wants maximum transactions per second and strong security, but accepts fewer validators. Where on the trilemma does it sit?
A) High decentralization, low scalability B) High scalability, low decentralization
C) High decentralization, high scalability D) Low security, high scalability
Answer: B – Sacrificing decentralization (fewer validators) is how chains like Solana achieve high throughput.

Q9. Bitcoin's total market capitalization in early 2026 is approximately:
A) \$180 million B) \$18 billion C) \$180 billion D) \$1.8 trillion
Answer: D – Bitcoin's market cap reached approximately \$1.8 trillion by January 2026.

Q10. Why is a 51% attack on Bitcoin impractical today?
A) The Bitcoin software prevents it with a built-in lock
B) The cost of acquiring enough computing power far exceeds any potential gain
C) There are laws against it in every country
D) Bitcoin uses Proof of Stake, which makes it impossible
Answer: B – The attack cost exceeds \$15 billion per year, far more than any double-spend could earn.

Quiz: Questions 11–15

Q11. A miner spends $50,000 on electricity and earns $300,000 in block rewards. Their profit is:
A) $50,000 B) $250,000 C) $300,000 D) $350,000

Quiz: Questions 11–15

Q11. A miner spends $50,000 on electricity and earns $300,000 in block rewards. Their profit is:
A) $50,000 B) $250,000 C) $300,000 D) $350,000
Answer: B – Profit = Revenue ($300K) minus Cost ($50K) = $250,000.

Q12. A hospital wants to store patient records. Only the hospital accesses the data. Should they use blockchain?
A) Yes — blockchain is more secure than any database
B) No — a single organization controlling data does not need blockchain
C) Yes — patients should own their data on-chain
D) No — blockchain cannot store medical records

Quiz: Questions 11–15

Q11. A miner spends $50,000 on electricity and earns $300,000 in block rewards. Their profit is:
A) $50,000 B) $250,000 C) $300,000 D) $350,000
Answer: B – Profit = Revenue ($300K) minus Cost ($50K) = $250,000.

Q12. A hospital wants to store patient records. Only the hospital accesses the data. Should they use blockchain?
A) Yes — blockchain is more secure than any database
B) No — a single organization controlling data does not need blockchain
C) Yes — patients should own their data on-chain
D) No — blockchain cannot store medical records
Answer: B – When one trusted party controls the data, a traditional database is simpler and faster.

Q13. What is the fundamental trade-off between centralized and distributed architectures?
A) Cost vs. profit B) Throughput vs. resilience
C) Encryption vs. transparency D) Storage vs. bandwidth

Quiz: Questions 11–15

Q11. A miner spends $50,000 on electricity and earns $300,000 in block rewards. Their profit is:
A) $50,000 B) $250,000 C) $300,000 D) $350,000
Answer: B – Profit = Revenue ($300K) minus Cost ($50K) = $250,000.

Q12. A hospital wants to store patient records. Only the hospital accesses the data. Should they use blockchain?
A) Yes — blockchain is more secure than any database
B) No — a single organization controlling data does not need blockchain
C) Yes — patients should own their data on-chain
D) No — blockchain cannot store medical records
Answer: B – When one trusted party controls the data, a traditional database is simpler and faster.

Q13. What is the fundamental trade-off between centralized and distributed architectures?
A) Cost vs. profit B) Throughput vs. resilience
C) Encryption vs. transparency D) Storage vs. bandwidth
Answer: B – Centralized systems are fast but fragile; distributed systems are slow but resilient.

Q14. Mt. Gox lost $450M in Bitcoin. Why is this NOT a blockchain failure?
A) The amount was too small to matter
B) The exchange (centralized service) was hacked, not the Bitcoin blockchain
C) Mt. Gox was not a real exchange
D) The Bitcoin was later recovered

Quiz: Questions 11–15

Q11. A miner spends $50,000 on electricity and earns $300,000 in block rewards. Their profit is:
A) $50,000 B) $250,000 C) $300,000 D) $350,000
Answer: B – Profit = Revenue ($300K) minus Cost ($50K) = $250,000.

Q12. A hospital wants to store patient records. Only the hospital accesses the data. Should they use blockchain?
A) Yes — blockchain is more secure than any database
B) No — a single organization controlling data does not need blockchain
C) Yes — patients should own their data on-chain
D) No — blockchain cannot store medical records
Answer: B – When one trusted party controls the data, a traditional database is simpler and faster.

Q13. What is the fundamental trade-off between centralized and distributed architectures?
A) Cost vs. profit B) Throughput vs. resilience
C) Encryption vs. transparency D) Storage vs. bandwidth
Answer: B – Centralized systems are fast but fragile; distributed systems are slow but resilient.

Q14. Mt. Gox lost $450M in Bitcoin. Why is this NOT a blockchain failure?
A) The amount was too small to matter
B) The exchange (centralized service) was hacked, not the Bitcoin blockchain
C) Mt. Gox was not a real exchange
D) The Bitcoin was later recovered
Answer: B – The blockchain continued operating; the centralized exchange's security was the weak point.

Q15. Ethereum switched from Proof of Work to Proof of Stake in 2022. What was the primary benefit?
A) Faster transaction speed (10x improvement)
B) Energy reduction of approximately 99.95%
C) Complete elimination of all attacks
D) Removal of transaction fees

Quiz: Questions 11–15

Q11. A miner spends $50,000 on electricity and earns $300,000 in block rewards. Their profit is:
A) $50,000 B) $250,000 C) $300,000 D) $350,000
Answer: B – Profit = Revenue ($300K) minus Cost ($50K) = $250,000.

Q12. A hospital wants to store patient records. Only the hospital accesses the data. Should they use blockchain?
A) Yes — blockchain is more secure than any database
B) No — a single organization controlling data does not need blockchain
C) Yes — patients should own their data on-chain
D) No — blockchain cannot store medical records
Answer: B – When one trusted party controls the data, a traditional database is simpler and faster.

Q13. What is the fundamental trade-off between centralized and distributed architectures?
A) Cost vs. profit B) Throughput vs. resilience
C) Encryption vs. transparency D) Storage vs. bandwidth
Answer: B – Centralized systems are fast but fragile; distributed systems are slow but resilient.

Q14. Mt. Gox lost $450M in Bitcoin. Why is this NOT a blockchain failure?
A) The amount was too small to matter
B) The exchange (centralized service) was hacked, not the Bitcoin blockchain
C) Mt. Gox was not a real exchange
D) The Bitcoin was later recovered
Answer: B – The blockchain continued operating; the centralized exchange's security was the weak point.

Q15. Ethereum switched from Proof of Work to Proof of Stake in 2022. What was the primary benefit?
A) Faster transaction speed (10x improvement)
B) Energy reduction of approximately 99.95%
C) Complete elimination of all attacks
D) Removal of transaction fees
Answer: B – The Merge reduced Ethereum's energy consumption by 99.95% while maintaining security.

Quiz: Questions 16–20

Q16. On the trust spectrum, where does a mobile payment app (like Venmo) sit relative to blockchain?
A) Same position — both are digital
B) Closer to the "full trust" end — you trust the company behind the app
C) Closer to the "zero trust" end — it uses encryption
D) Outside the spectrum entirely

Quiz: Questions 16–20

Q16. On the trust spectrum, where does a mobile payment app (like Venmo) sit relative to blockchain?
A) Same position — both are digital
B) Closer to the "full trust" end — you trust the company behind the app
C) Closer to the "zero trust" end — it uses encryption
D) Outside the spectrum entirely
Answer: B – Venmo requires trusting a centralized company; blockchain removes that requirement.

Q17. A Bitcoin block header is 80 bytes. The block body can be up to 4 MB. Why is this separation useful?
A) It allows deleting old transactions to save space
B) Light clients can verify block headers without downloading the full body
C) The header is encrypted while the body is public
D) Miners only need to process the header

Quiz: Questions 16–20

Q16. On the trust spectrum, where does a mobile payment app (like Venmo) sit relative to blockchain?
A) Same position — both are digital
B) Closer to the "full trust" end — you trust the company behind the app
C) Closer to the "zero trust" end — it uses encryption
D) Outside the spectrum entirely
Answer: B – Venmo requires trusting a centralized company; blockchain removes that requirement.

Q17. A Bitcoin block header is 80 bytes. The block body can be up to 4 MB. Why is this separation useful?
A) It allows deleting old transactions to save space
B) Light clients can verify block headers without downloading the full body
C) The header is encrypted while the body is public
D) Miners only need to process the header
Answer: B – Small headers enable mobile phones and light clients to verify the chain efficiently.

Q18. China's e-CNY (CBDC) uses blockchain technology but is centrally controlled. How does this differ from Bitcoin?
A) No difference — both are digital currencies
B) e-CNY can be censored and accounts frozen; Bitcoin cannot
C) Bitcoin is faster than e-CNY
D) e-CNY is more decentralized than Bitcoin

Quiz: Questions 16–20

Q16. On the trust spectrum, where does a mobile payment app (like Venmo) sit relative to blockchain?
A) Same position — both are digital
B) Closer to the "full trust" end — you trust the company behind the app
C) Closer to the "zero trust" end — it uses encryption
D) Outside the spectrum entirely
Answer: B – Venmo requires trusting a centralized company; blockchain removes that requirement.

Q17. A Bitcoin block header is 80 bytes. The block body can be up to 4 MB. Why is this separation useful?
A) It allows deleting old transactions to save space
B) Light clients can verify block headers without downloading the full body
C) The header is encrypted while the body is public
D) Miners only need to process the header
Answer: B – Small headers enable mobile phones and light clients to verify the chain efficiently.

Q18. China's e-CNY (CBDC) uses blockchain technology but is centrally controlled. How does this differ from Bitcoin?
A) No difference — both are digital currencies
B) e-CNY can be censored and accounts frozen; Bitcoin cannot
C) Bitcoin is faster than e-CNY
D) e-CNY is more decentralized than Bitcoin
Answer: B – CBDCs use blockchain technology but retain central control — the opposite of Bitcoin's design.

Q19. A charity wants transparent donation tracking across 50 international partners. Is blockchain appropriate?
A) No — charities should not use technology
B) Yes — multiple untrusted parties need a shared, immutable record
C) No — a spreadsheet is always sufficient
D) Yes — but only if they use Bitcoin specifically

Quiz: Questions 16–20

Q16. On the trust spectrum, where does a mobile payment app (like Venmo) sit relative to blockchain?
A) Same position — both are digital
B) Closer to the "full trust" end — you trust the company behind the app
C) Closer to the "zero trust" end — it uses encryption
D) Outside the spectrum entirely
Answer: B – Venmo requires trusting a centralized company; blockchain removes that requirement.

Q17. A Bitcoin block header is 80 bytes. The block body can be up to 4 MB. Why is this separation useful?
A) It allows deleting old transactions to save space
B) Light clients can verify block headers without downloading the full body
C) The header is encrypted while the body is public
D) Miners only need to process the header
Answer: B – Small headers enable mobile phones and light clients to verify the chain efficiently.

Q18. China's e-CNY (CBDC) uses blockchain technology but is centrally controlled. How does this differ from Bitcoin?
A) No difference — both are digital currencies
B) e-CNY can be censored and accounts frozen; Bitcoin cannot
C) Bitcoin is faster than e-CNY
D) e-CNY is more decentralized than Bitcoin
Answer: B – CBDCs use blockchain technology but retain central control — the opposite of Bitcoin's design.

Q19. A charity wants transparent donation tracking across 50 international partners. Is blockchain appropriate?
A) No — charities should not use technology
B) Yes — multiple untrusted parties need a shared, immutable record
C) No — a spreadsheet is always sufficient
D) Yes — but only if they use Bitcoin specifically
Answer: B – This scenario has multiple parties, a trust deficit, and a need for transparency — ideal for blockchain.

Q20. Is Bitcoin's energy consumption of 150 TWh/year justified?
A) Yes — it secures $1.8T and provides censorship-resistant payments globally
B) No — all energy use for cryptocurrency is wasteful
C) It depends on whether the trust and censorship resistance it provides are valued by users
D) The question is irrelevant because Proof of Stake has replaced Proof of Work everywhere

Quiz: Questions 16–20

Q16. On the trust spectrum, where does a mobile payment app (like Venmo) sit relative to blockchain?
A) Same position — both are digital
B) Closer to the "full trust" end — you trust the company behind the app
C) Closer to the "zero trust" end — it uses encryption
D) Outside the spectrum entirely
Answer: B – Venmo requires trusting a centralized company; blockchain removes that requirement.

Q17. A Bitcoin block header is 80 bytes. The block body can be up to 4 MB. Why is this separation useful?
A) It allows deleting old transactions to save space
B) Light clients can verify block headers without downloading the full body
C) The header is encrypted while the body is public
D) Miners only need to process the header
Answer: B – Small headers enable mobile phones and light clients to verify the chain efficiently.

Q18. China's e-CNY (CBDC) uses blockchain technology but is centrally controlled. How does this differ from Bitcoin?
A) No difference — both are digital currencies
B) e-CNY can be censored and accounts frozen; Bitcoin cannot
C) Bitcoin is faster than e-CNY
D) e-CNY is more decentralized than Bitcoin
Answer: B – CBDCs use blockchain technology but retain central control — the opposite of Bitcoin's design.

Q19. A charity wants transparent donation tracking across 50 international partners. Is blockchain appropriate?
A) No — charities should not use technology
B) Yes — multiple untrusted parties need a shared, immutable record
C) No — a spreadsheet is always sufficient
D) Yes — but only if they use Bitcoin specifically
Answer: B – This scenario has multiple parties, a trust deficit, and a need for transparency — ideal for blockchain.

Q20. Is Bitcoin's energy consumption of 150 TWh/year justified?
A) Yes — it secures $1.8T and provides censorship-resistant payments globally
B) No — all energy use for cryptocurrency is wasteful
C) It depends on whether the trust and censorship resistance it provides are valued by users
D) The question is irrelevant because Proof of Stake has replaced Proof of Work everywhere
Answer: C – Energy justification depends on the value users place on trustless, censorship-resistant money. Reasonable people disagree.