Block Consensus: How a Distributed Network Agrees on One Truth

Fork Resolution, Chain Selection, and Probabilistic Finality in Bitcoin

Prof. Dr. Jörg Osterrieder

BSc Blockchain, Crypto Economy & NFTs

Spring 2026

Two Miners, One Puzzle, Same Second

A miner in Iceland finds a valid block at 14:32:07 UTC. Two seconds later, a miner in Texas finds a *different* valid block at the same height.

Both blocks are legitimate. Both contain valid transactions. Both miners spent real electricity to earn the right to write.

Which one wins?

How do 50,000 computers pick the same answer — **without talking to each other?**

Key Questions

1. How does the network resolve forks when two valid blocks appear?
2. Why do merchants wait for 6 confirmations before shipping?
3. What does "longest chain" actually mean — and why is it wrong?

Every 10 minutes, Bitcoin faces this coordination problem — and solves it without a leader

Learning Objectives

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

1. Explain how Bitcoin resolves temporary forks when two blocks are found simultaneously
2. Distinguish between "longest chain" and "most cumulative work" as chain selection rules
3. Calculate the probability of transaction reversal given attacker hash power and confirmation depth
4. Describe how nodes converge from disagreement to consensus without central coordination
5. Justify why 6 confirmations is the standard threshold for Bitcoin transaction finality

No prerequisites beyond basic blockchain structure (blocks, hashes, mining).

No prerequisites beyond basic blockchain structure (blocks, hashes, mining)

The Shared Notebook Problem

Imagine 50,000 people around the world all writing in the same notebook. No phone, no leader, no referee.

Two people write a new entry at the exact same moment. Now there are two versions of the notebook.

Which version is the "real" one?

You cannot ask a judge — there is no judge. You cannot vote — identities can be faked. You cannot flip a coin — there is no shared coin.

Blockchain's answer:

Make writing expensive. Let everyone see both versions. Wait. The version that gets extended first wins.

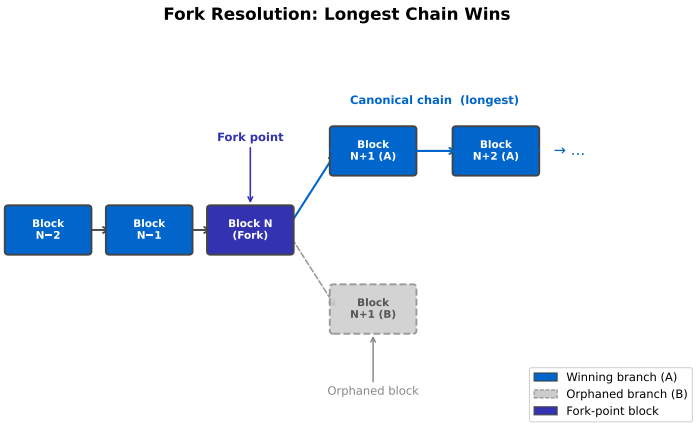
The Rule

If two pages appear at the same time, keep both temporarily. As soon as one version gets a new page added, abandon the other.

No coordination. No communication. Just one rule, followed independently by every participant.

Fork resolution is blockchain's answer to simultaneous writes in a distributed system

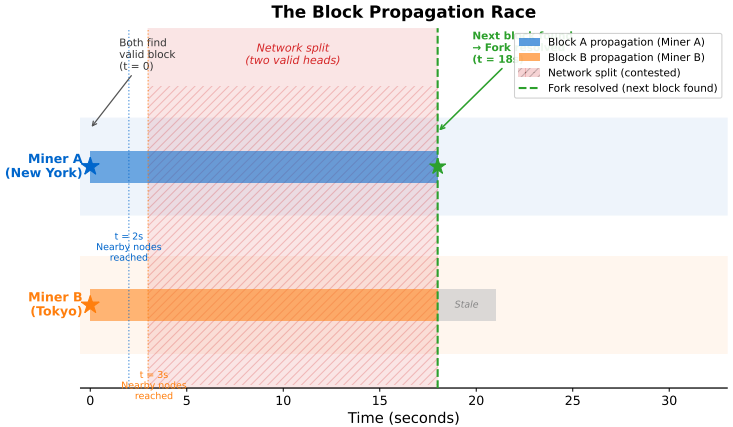
What Happens When the Chain Splits?



- **What you see:** A blockchain that splits into two competing branches at the same block height
- **Key pattern:** Both branches are valid — the network temporarily disagrees on which is canonical
- **Takeaway:** Forks are not errors; they are a natural consequence of decentralized block production

Bitcoin experiences natural forks roughly once every 1–2 weeks — they are a feature, not a bug

Two Valid Blocks: A Race Across the Globe



- **What you see:** Two blocks propagating outward from different geographic origins across the network
- **Key pattern:** Nodes near each miner see "their" block first, creating a temporary partition
- **Takeaway:** Geography and network latency determine which nodes see which block first

Block propagation takes 8–15 seconds across the Bitcoin network — during this window, forks can form

How Does the Fork Get Resolved?

Step 1: Two miners find valid blocks A and B at height N

Step 2: Block A reaches 60% of nodes first; Block B reaches 40%

Step 3: Miners who received A build on A; miners who received B build on B

Step 4: A miner on the A-branch finds block $N+1$ first

Step 5: The A-branch now has more cumulative work

Step 6: B-branch nodes switch to the A-branch (reorganization)

Step 7: Block B becomes orphaned; its transactions return to the mempool

Key Insight

Nobody decided that A was "correct." No vote was taken. No leader announced the winner.

The resolution emerged from thousands of independent nodes all following the same rule: *always build on the chain with the most cumulative work.*

Fork resolution is emergent, not directed — individual rules produce collective agreement

[Analogy] Choosing a Restaurant Without Talking

The scenario:

You arrive in a new city, hungry. Two restaurants face each other. You know nothing about either. No reviews, no recommendations.

Restaurant A has 30 people inside. Restaurant B has 3.

You walk into Restaurant A. So does the next tourist, and the next. Nobody coordinated. Nobody spoke.

This is a **Schelling point**: a focal solution that people converge on independently because it is the obvious choice.

Bitcoin connection:

Each miner follows one rule: build on the chain with the most work.

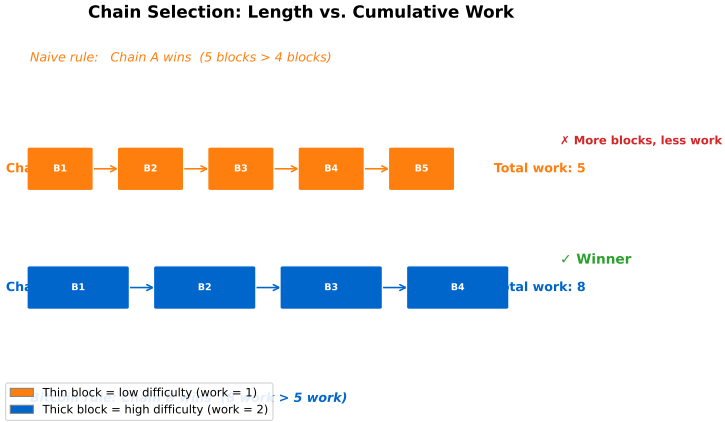
When a fork appears, miners naturally converge on the branch that received the next block first — just like tourists converge on the busier restaurant.

No Communication Needed

The rule is simple enough that everyone follows it independently. Coordination emerges from shared incentives, not shared messages.

Schelling points: when everyone follows the same rule, coordination emerges without communication

Longest Chain or Most Work? (They Are Not the Same)



- **What you see:** Two chains with different block counts but different cumulative work totals
- **Key pattern:** The chain with fewer blocks can have more cumulative work if each block required higher difficulty
- **Takeaway:** Bitcoin selects the chain with the most *work*, not the most *blocks*

Satoshi wrote "longest chain" in the whitepaper, but the code implements "most cumulative work"

Why Cumulative Work Beats Block Count

The problem with counting blocks:

An attacker with slow, cheap hardware could produce many low-difficulty blocks. If the rule were "most blocks wins," the attacker's chain of easy blocks would beat the honest chain of hard blocks.

Cumulative work counts the *total computational effort* across all blocks. A chain of 4 hard blocks beats a chain of 6 easy blocks.

This is why difficulty adjustments matter: they ensure each block represents roughly the same amount of work.

[Analogy] The Essay Problem:

Student A writes 10 pages of filler.
Student B writes 5 pages of rigorous research.

Who did more work?

Counting pages (blocks) is misleading. Measuring effort (cumulative work) reveals the truth.

Bitcoin's Real Rule

```
if (chain.work > best.work)
  best = chain;
```

Cumulative work = sum of difficulty targets across all blocks — this is what Bitcoin's chainwork tracks

Chain Selection: The Formula

How Bitcoin calculates cumulative work:

$$\text{Cumulative Work} = \sum_{i=1}^{n} \frac{2^{256}}{\text{target}_i + 1}$$

Each block's work is inversely proportional to its difficulty target: a lower target (harder puzzle) means more work per block.

Worked Example:

Chain A: 5 blocks, each at difficulty 1
Work per block $= \frac{2^{256}}{T_1+1} \approx 1$ unit
Total work $= 5 \times 1 = 5$

Chain B: 4 blocks, each at difficulty 3
Work per block ≈ 3 units
Total work $= 4 \times 3 = 12$

Result: Chain B wins despite having fewer blocks ($12 > 5$).

The Bitcoin Core variable `chainwork` tracks this sum — you can query it with `getblockchaininfo`

Orphaned Blocks: The Losers of Fork Resolution

What are orphaned blocks?

When a fork resolves, the losing branch's blocks are "orphaned" — valid blocks that the network has moved past.

What happens to their contents:

- Transactions return to the mempool
- Most are re-included within 1–2 blocks
- The miner loses the block reward entirely
- No permanent effect on the network

The orphaned block was real work, wasted. This is the cost of decentralized agreement.

By the Numbers:

- Orphan rate: 0.1–0.5% of blocks
- Typical resolution: 1 block ($\sim$10 min)
- Revenue lost per orphan: 3.125 BTC + fees ($\sim$\$320K)
- Annual orphaned blocks: $\sim$50–250

Economic Impact

Orphaned blocks are economically painful for the miner who produced them, but harmless to the network. Users experience a brief delay, not a loss.

Orphaned blocks are economically costly to miners but harmless to the network — transactions are re-included

[Analogy] Finality Like Drying Cement

Traditional finance: Finality is binary.
A wire transfer is either settled or not. A check either clears or bounces.

Blockchain: Finality is probabilistic.
A transaction becomes *more* final with every new block, but never reaches 100%.

The cement analogy:

- 1 minute: you can still reshape it
- 10 minutes: hard to change, possible with effort
- 1 hour: requires power tools to modify
- 1 day: practically permanent

Bitcoin confirmations work the same way. Each new block is another layer of hardening cement.

Confirmation levels:

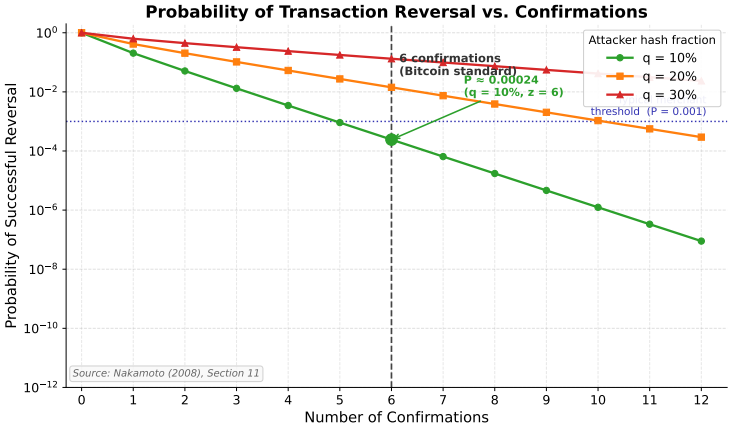
0 conf	Wet cement
1 conf	Setting (10 min)
3 conf	Firm (30 min)
6 conf	Hard (1 hour)
12 conf	Concrete (2 hours)

Key Difference

Banks: "Your payment is final." (Binary)
Bitcoin: "Your payment is 99.9998% final." (Probabilistic)
In practice, the difference is negligible — but the math is fundamentally different.

Probabilistic finality: never 100%, but exponentially approaching it with each confirmation

How Safe Are Your Bitcoins After N Confirmations?



- **What you see:** Reversal probability dropping exponentially as confirmations increase, for different attacker hash rates
- **Key pattern:** At 10% attacker hash power, 6 confirmations reduce reversal probability to $\sim$0.002%
- **Takeaway:** Each additional confirmation makes reversal exponentially harder — not linearly harder

Source: Nakamoto (2008), Section 11 — "Calculations" in the Bitcoin whitepaper

Nakamoto's Probability Formula (Bitcoin Whitepaper, Section 11)

The attacker's success probability after z confirmations, with fraction q of total hash power:

$$P(z) = 1 - \sum_{k=0}^{z} \frac{(\lambda)^k e^{-\lambda}}{k!} \left(1 - (q/p)^{z-k}\right), \quad \lambda = z \cdot \frac{q}{p}$$

where $p = 1 - q$ is the honest miners' share and λ is the expected attacker progress.

Worked examples:

At $q = 10\%$, $z = 6$:
$P \approx 0.00002$ (1 in 50,000)

At $q = 10\%$, $z = 1$:
$P \approx 0.0562$ (1 in 18)

At $q = 30\%$, $z = 6$:
$P \approx 0.0177$ (1 in 56)

At $q = 30\%$, $z = 24$:
$P \approx 0.000003$ (1 in 330,000)

Key insight: The probability decreases *exponentially* with z, but increases *dramatically* with q. A 30% attacker needs 24 confirmations to match a 10% attacker at 6.

This formula is why exchanges wait for more confirmations for large deposits

Why Exactly 6? The Origin of Bitcoin's Standard

Satoshi's reasoning (2008):

At $q = 10\%$ (generous assumption for an attacker):

- 1 confirmation: 5.6% chance of reversal
- 3 confirmations: 0.13% chance
- 6 confirmations: 0.002% chance
- 10 confirmations: 0.00001% chance

At $q = 1\%$ (realistic for Bitcoin today):

- 1 confirmation: effectively zero
- 6 confirmations: astronomically small

6 was chosen as a practical threshold where the risk drops below what any rational attacker would attempt.

In practice, it depends on value:

Situation	Value	Conf.
Coffee	\$5	0
Online purchase	\$100	1–2
Electronics	\$1,000	3
Exchange deposit	\$10K+	6
Settlement	\$1M+	12+

The right number of confirmations depends on how much you stand to lose.

Coinbase requires 3 confirmations for BTC deposits; Kraken requires 4; Binance requires 1

Worked Example: Anatomy of a Double-Spend Attack

The attack in 7 steps:

Step 1: Attacker sends 100 BTC to a merchant (TX A)
Step 2: Simultaneously mines a secret chain sending 100 BTC back to themselves (TX B)
Step 3: Merchant sees TX A confirmed in the public chain
Step 4: Merchant ships the goods after 1 confirmation
Step 5: Attacker's secret chain grows longer (more work)
Step 6: Attacker broadcasts secret chain; network switches to it
Step 7: TX A is orphaned; attacker has both goods and BTC

Why 6 Confirmations Stops This

The attacker must mine 6+ blocks faster than the entire honest network.

With 10% hash power, this requires winning a race where you are 10x slower — six times in a row.

Probability: $\sim 0.002\%$

Each additional confirmation makes the secret chain exponentially harder to extend faster than the public chain.

The 2018 Bitcoin Gold 51% attack succeeded because the network had only $70K/hour in mining security

When Forks Made Headlines

March 2013: The Accidental Fork

Bitcoin Core upgraded from BerkeleyDB (v0.7) to LevelDB (v0.8). The new database handled large blocks differently.

Result: v0.7 nodes rejected a block that v0.8 nodes accepted. The network split into two chains for **6 hours**.

24 blocks were orphaned. Developers coordinated miners to downgrade back to v0.7 to reunify the network.

Lesson: Software bugs can cause consensus failures, but the community can coordinate a fix.

August 2010: The Value Overflow Bug

A transaction created **184 billion BTC** out of thin air — exploiting an integer overflow in the code (CVE-2010-5139).

Satoshi Nakamoto deployed a patch within **5 hours**. The network forked to the corrected chain, invalidating the overflow transaction.

Lesson: Even critical bugs can be resolved through coordinated fork resolution.

Common Thread

Both incidents were resolved within hours — demonstrating Bitcoin's practical resilience to unexpected failures.

Both incidents were resolved within hours — demonstrating Bitcoin's practical resilience

Not All Forks Are Equal

Natural Forks (this lecture):

- Cause: two miners find valid blocks simultaneously
- Resolution: automatic via chain selection rule
- Frequency: every 1–2 weeks
- Duration: typically 1 block ($\sim$10 min)
- Impact: harmless; transactions re-included

Natural forks are the expected cost of decentralized block production — they test the protocol constantly.

Intentional Forks (different lectures):

- **Soft fork:** tighten rules (old nodes still compatible)
  Example: SegWit (Aug 2017)
- **Hard fork:** loosen rules (old nodes incompatible)
  Example: Bitcoin Cash (Aug 2017)

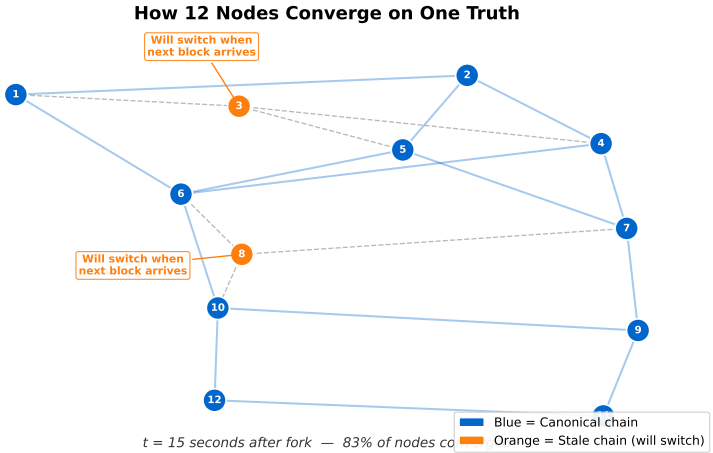
Intentional forks are *political* — they represent disagreements about the protocol's future direction.

Key Distinction

Natural forks: resolved by math.
Intentional forks: resolved by community.

Natural forks test the protocol; intentional forks test the community

From Disagreement to Consensus: A Network in Motion



- **What you see:** The percentage of nodes agreeing on the canonical chain over time after a fork event
- **Key pattern:** Rapid convergence once a new block extends one branch — nearly 100% within minutes
- **Takeaway:** Temporary disagreement is normal; convergence is fast and reliable

Average convergence time: 10–20 minutes for natural forks (one additional block)

Why Does Block Propagation Time Matter?

Faster propagation = fewer forks.

If a block reaches all nodes before the next block is found, no fork can form. Forks only occur when two blocks are found within the propagation window.

The math:
Fork probability $\propto$ propagation time / block interval

Key improvement:
Compact blocks (BIP 152, 2016) reduced propagation from $\sim$40 seconds to $\sim$8 seconds by sending only transaction IDs instead of full transactions.

The trade-off:

Chain	Interval	Fork Rate
Bitcoin	10 min	$\sim$0.3%
Ethereum	15 sec	$\sim$6%
Hypothetical	1 sec	catastrophic

Shorter block intervals mean higher throughput but more forks — another manifestation of the blockchain trilemma.

Design Principle

Block interval must be significantly longer than propagation time to keep forks rare.

Compact blocks (BIP 152) reduced propagation time from $\sim$40s to $\sim$8s — fewer natural forks

What Happens to Transactions in Orphaned Blocks?

When a block is orphaned, its transactions are not lost. They return to the **mempool** — the waiting room where unconfirmed transactions sit until a miner includes them.

Most transactions are re-included within 1–2 blocks. The only exception: if the orphaned block contained a double-spend, the conflicting transaction in the winning chain takes priority.

For honest users, an orphaned block is a brief delay — not a loss of funds.

Transaction Lifecycle

Step 1: User broadcasts transaction
→ Enters mempool
Step 2: Miner includes it in a block
→ 1 confirmation
Step 3: Block is orphaned
→ Transaction returns to mempool
Step 4: Another miner includes it
→ Back to 1 confirmation

For users: orphaned blocks cause a temporary delay, not a loss — unless someone is attempting a double-spend

Real-World Confirmation Requirements (2026)

Service / Scenario	Risk Level	Confirmations	Wait Time
BitPay (small retail)	Low	0	Instant
Binance (BTC deposit)	Medium	1	$\sim$10 min
Coinbase (BTC deposit)	Medium	3	$\sim$30 min
Kraken (BTC deposit)	Medium-High	4	$\sim$40 min
Exchange standard	High	6	$\sim$1 hour
Large settlement	Very High	12+	$\sim$2+ hours

Key patterns:

- Higher value $\rightarrow$ more confirmations required
- Each exchange sets its own threshold based on risk tolerance
- Zero-confirmation is acceptable for small amounts where the cost of a double-spend attack far exceeds the value

Zero-confirmation transactions are accepted for small amounts because the double-spend risk is not worth the effort

What Makes Bitcoin's Consensus Secure?

Three pillars of security:

1. Hash power concentration:
Attacking Bitcoin requires outpacing the combined hash rate of all honest miners worldwide.

2. Energy cost:
Each block requires ∼$50,000–100,000 in electricity. An attacker pays the same cost but earns nothing for invalid blocks.

3. Economic alignment:
Miners who own expensive hardware benefit from Bitcoin's value.
Attacking the network would destroy the value of their own investment.

Security budget math (2026):

Block reward: 3.125 BTC
BTC price: ∼$100,000
Reward per block: ∼$312,500
Average fees: ∼$10,000–50,000

Per block: $320,000–360,000
Per day (144 blocks): $46M–52M
Per year: $17B–19B

The Halving Problem

Block rewards halve every 4 years (next: 2028). Transaction fees must eventually replace rewards as the primary security budget.

As block rewards halve every 4 years, transaction fees must eventually replace them as the security budget

Why Can't Nodes Just Vote on the Correct Chain?

The Sybil problem:

In a permissionless network, anyone can join. Creating a new node costs nothing — just spin up a virtual machine.

If voting were based on "one node, one vote":

- An attacker creates 10,000 fake nodes
- Each fake node gets one vote
- The attacker now controls the election
- Cost: $100 in cloud computing

This is a Sybil attack:
Overwhelming a vote by creating fake identities. There is no passport office in a decentralized network.

Proof of Work's solution:

PoW replaces identity-based voting with *work-based* voting.

- 10,000 fake nodes? Still only the hash power you actually have.
- Each "vote" costs real electricity.
- You cannot counterfeit computational work.

The Key Insight

PoW does not prevent fake identities — it makes them irrelevant. Voting power is proportional to energy spent, not to the number of nodes controlled.

Proof of Work is a Sybil-resistance mechanism: it makes identity fraud expensive, not impossible

The Byzantine Generals Problem, Solved

The classical problem (Lamport, 1982):

Several generals surround a city. They must agree to attack or retreat. But some generals are traitors who send conflicting messages.

Classical result: requires $3f+1$ total generals to tolerate f traitors. With $\frac{1}{3}$ traitors, *no deterministic protocol works*.

For 40 years, this was considered unsolvable in open networks where you do not know how many participants exist.

Nakamoto's insight (2008):

Replace "honest majority of generals" with **honest majority of computational work.**

Key differences from classical BFT:

- Open membership (anyone can join)
- No fixed number of participants
- Probabilistic guarantee (not deterministic)
- Works at any scale

Trade-off

Classical BFT: 100% finality, closed group.
Nakamoto: 99.998% finality, open to the world.

Bitcoin does not solve BFT in the classical sense — it provides probabilistic guarantees, which is sufficient in practice

The Complete Consensus Cycle

How Bitcoin reaches agreement, step by step:

1. Users broadcast transactions to the network
2. Transactions propagate to nodes and enter the mempool
3. Miners select transactions (prioritizing higher fees)
4. Miners race to solve the Proof of Work puzzle ($\sim$10 minutes on average)
5. Winner broadcasts the new block to all nodes
6. Nodes verify: valid PoW? Valid transactions? Correct previous hash?
7. If valid, nodes add the block to their chain and begin mining the next block
8. If a fork exists, nodes follow the chain with the most cumulative work
9. Orphaned blocks' transactions return to the mempool
10. New miners join or leave; difficulty adjusts every 2,016 blocks ($\sim$2 weeks)
11. Cycle repeats at the new chain tip

Repeat every $\sim$10 minutes, 24/7, since January 3, 2009.

---

144 blocks per day, 52,560 blocks per year — Bitcoin's consensus has not failed since launch

Key Takeaways

Five ideas to remember from today:

1. **Forks are normal:** Simultaneous block discovery is expected in a decentralized network — resolution is automatic
2. **Most work, not most blocks:** Bitcoin selects the chain with the highest cumulative computational work, not the longest
3. **Finality is probabilistic:** Each confirmation makes reversal exponentially harder, but never mathematically impossible
4. **6 confirmations:** At 10% attacker hash power, 6 confirmations reduce reversal probability to $\sim$0.002%
5. **No leader needed:** Convergence emerges from individual nodes following the same simple rule independently

Decision Heuristic:

$$\text{Required Confirmations} \propto \text{Value at Risk} \;/\; \text{Network Security Budget}$$

When the cost of attack exceeds the value of the prize, the system is secure.

Fork resolution + chain selection + probabilistic finality = Nakamoto Consensus

Summary and What Comes Next

Today we learned:

- How Bitcoin resolves forks through cumulative work, not voting
- Why "longest chain" is technically imprecise
- How Nakamoto's formula quantifies transaction security
- Why emergent consensus works without central coordination

Related topics:

- **L02a** — DLT Fundamentals: Byzantine fault tolerance
- **L07** — Mining: hash rate, difficulty, economics
- **L09** — Consensus Mechanisms: PoS, DPoS, BFT variants
- **L10** — Attacks: 51%, selfish mining, eclipse

Reflection Questions:

1. If Bitcoin's block time were reduced to 1 minute, what would happen to the fork rate?
2. Why might a merchant accept 0 confirmations for a $3 coffee but not a $30,000 car?
3. If transaction fees replace block rewards, who ultimately pays for Bitcoin's security?

Nakamoto Consensus: the simplest idea that works at planetary scale

Further Reading and Resources

Primary Sources:

- Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." Section 11: Calculations.
- Garay, J., Kiayias, A., & Leonardos, N. (2015). "The Bitcoin Backbone Protocol." *Eurocrypt 2015*.
- Sompolinsky, Y. & Zohar, A. (2015). "Secure High-Rate Transaction Processing in Bitcoin." *Financial Cryptography*.

Tools for Exploration:

- `blockchain.com/explorer` — View real blocks and orphaned chains
- `bitcoin-cli getblockchaininfo` — Query chainwork from a full node
- `mempool.space` — Real-time mempool and block visualization

Key Numbers to Remember:

- Block interval: ∼10 minutes — 6 confirmations: ∼1 hour
- Propagation time: 8–15 seconds — Natural fork rate: 0.1–0.5%

The Bitcoin whitepaper is only 9 pages — Section 11 (Calculations) is the mathematical foundation of this lecture

Quiz: Questions 1–5

Q1. What triggers a natural fork in Bitcoin? % Bloom: Understand
A) A software bug in Bitcoin Core causes nodes to reject valid blocks
B) Two miners find valid blocks at approximately the same time
C) A miner intentionally creates a competing chain to earn double rewards
D) The difficulty adjustment algorithm produces conflicting targets

Quiz: Questions 1–5

Q1. What triggers a natural fork in Bitcoin? % Bloom: Understand
A) A software bug in Bitcoin Core causes nodes to reject valid blocks
B) Two miners find valid blocks at approximately the same time
C) A miner intentionally creates a competing chain to earn double rewards
D) The difficulty adjustment algorithm produces conflicting targets
Answer: B – Natural forks occur when two miners independently solve the PoW puzzle near-simultaneously.

Q2. What happens to transactions in an orphaned block? % Bloom: Understand
A) They are permanently lost and must be resubmitted by the sender
B) They are automatically refunded to the sender's wallet
C) They return to the mempool and are typically re-included in the next block
D) They are moved to a special "orphan transaction" database

Quiz: Questions 1–5

Q1. What triggers a natural fork in Bitcoin? % Bloom: Understand
A) A software bug in Bitcoin Core causes nodes to reject valid blocks
B) Two miners find valid blocks at approximately the same time
C) A miner intentionally creates a competing chain to earn double rewards
D) The difficulty adjustment algorithm produces conflicting targets
Answer: B – Natural forks occur when two miners independently solve the PoW puzzle near-simultaneously.

Q2. What happens to transactions in an orphaned block? % Bloom: Understand
A) They are permanently lost and must be resubmitted by the sender
B) They are automatically refunded to the sender's wallet
C) They return to the mempool and are typically re-included in the next block
D) They are moved to a special "orphan transaction" database
Answer: C – Transactions from orphaned blocks re-enter the mempool and are usually mined within 1–2 blocks.

Q3. What is the main difference between a natural fork and a hard fork? % Bloom: Understand
A) Natural forks only occur on testnets, while hard forks occur on mainnet
B) Natural forks require more hash power to resolve than hard forks
C) Natural forks are caused by network latency, while hard forks increase block size
D) Natural forks result from simultaneous discovery and resolve automatically, while hard forks are intentional rule changes

Quiz: Questions 1–5

Q1. What triggers a natural fork in Bitcoin? % Bloom: Understand
A) A software bug in Bitcoin Core causes nodes to reject valid blocks
B) Two miners find valid blocks at approximately the same time
C) A miner intentionally creates a competing chain to earn double rewards
D) The difficulty adjustment algorithm produces conflicting targets
Answer: B – Natural forks occur when two miners independently solve the PoW puzzle near-simultaneously.

Q2. What happens to transactions in an orphaned block? % Bloom: Understand
A) They are permanently lost and must be resubmitted by the sender
B) They are automatically refunded to the sender's wallet
C) They return to the mempool and are typically re-included in the next block
D) They are moved to a special "orphan transaction" database
Answer: C – Transactions from orphaned blocks re-enter the mempool and are usually mined within 1–2 blocks.

Q3. What is the main difference between a natural fork and a hard fork? % Bloom: Understand
A) Natural forks only occur on testnets, while hard forks occur on mainnet
B) Natural forks require more hash power to resolve than hard forks
C) Natural forks are caused by network latency, while hard forks increase block size
D) Natural forks result from simultaneous discovery and resolve automatically, while hard forks are intentional rule changes
Answer: D – Natural forks are resolved by the chain selection rule; hard forks require community consensus on new rules.

Q4. How does Bitcoin's chain selection rule determine the canonical chain? % Bloom: Understand
A) By measuring total cumulative computational work across all blocks
B) By counting the number of blocks in each competing chain
C) By selecting the chain that was broadcast first to the network
D) By having miners vote on which chain to extend

Quiz: Questions 1–5

Q1. What triggers a natural fork in Bitcoin? % Bloom: Understand
A) A software bug in Bitcoin Core causes nodes to reject valid blocks
B) Two miners find valid blocks at approximately the same time
C) A miner intentionally creates a competing chain to earn double rewards
D) The difficulty adjustment algorithm produces conflicting targets
Answer: B – Natural forks occur when two miners independently solve the PoW puzzle near-simultaneously.

Q2. What happens to transactions in an orphaned block? % Bloom: Understand
A) They are permanently lost and must be resubmitted by the sender
B) They are automatically refunded to the sender's wallet
C) They return to the mempool and are typically re-included in the next block
D) They are moved to a special "orphan transaction" database
Answer: C – Transactions from orphaned blocks re-enter the mempool and are usually mined within 1–2 blocks.

Q3. What is the main difference between a natural fork and a hard fork? % Bloom: Understand
A) Natural forks only occur on testnets, while hard forks occur on mainnet
B) Natural forks require more hash power to resolve than hard forks
C) Natural forks are caused by network latency, while hard forks increase block size
D) Natural forks result from simultaneous discovery and resolve automatically, while hard forks are intentional rule changes
Answer: D – Natural forks are resolved by the chain selection rule; hard forks require community consensus on new rules.

Q4. How does Bitcoin's chain selection rule determine the canonical chain? % Bloom: Understand
A) By measuring total cumulative computational work across all blocks
B) By counting the number of blocks in each competing chain
C) By selecting the chain that was broadcast first to the network
D) By having miners vote on which chain to extend
Answer: A – Bitcoin selects the chain with the most cumulative work (sum of difficulty), not the most blocks.

Q5. Chain A has 6 blocks at difficulty 1. Chain B has 4 blocks at difficulty 2. Which chain does Bitcoin select? % Bloom: Apply
A) Chain A, because 6 blocks is more than 4 blocks
B) Chain B, because cumulative work 8 exceeds cumulative work 6
C) Neither; the network waits for both chains to reach equal length
D) Chain A, because it was created first chronologically

Quiz: Questions 1–5

Q1. What triggers a natural fork in Bitcoin? % Bloom: Understand
A) A software bug in Bitcoin Core causes nodes to reject valid blocks
B) Two miners find valid blocks at approximately the same time
C) A miner intentionally creates a competing chain to earn double rewards
D) The difficulty adjustment algorithm produces conflicting targets
Answer: B – Natural forks occur when two miners independently solve the PoW puzzle near-simultaneously.

Q2. What happens to transactions in an orphaned block? % Bloom: Understand
A) They are permanently lost and must be resubmitted by the sender
B) They are automatically refunded to the sender's wallet
C) They return to the mempool and are typically re-included in the next block
D) They are moved to a special "orphan transaction" database
Answer: C – Transactions from orphaned blocks re-enter the mempool and are usually mined within 1–2 blocks.

Q3. What is the main difference between a natural fork and a hard fork? % Bloom: Understand
A) Natural forks only occur on testnets, while hard forks occur on mainnet
B) Natural forks require more hash power to resolve than hard forks
C) Natural forks are caused by network latency, while hard forks increase block size
D) Natural forks result from simultaneous discovery and resolve automatically, while hard forks are intentional rule changes
Answer: D – Natural forks are resolved by the chain selection rule; hard forks require community consensus on new rules.

Q4. How does Bitcoin's chain selection rule determine the canonical chain? % Bloom: Understand
A) By measuring total cumulative computational work across all blocks
B) By counting the number of blocks in each competing chain
C) By selecting the chain that was broadcast first to the network
D) By having miners vote on which chain to extend
Answer: A – Bitcoin selects the chain with the most cumulative work (sum of difficulty), not the most blocks.

Q5. Chain A has 6 blocks at difficulty 1. Chain B has 4 blocks at difficulty 2. Which chain does Bitcoin select? % Bloom: Apply
A) Chain A, because 6 blocks is more than 4 blocks
B) Chain B, because cumulative work 8 exceeds cumulative work 6
C) Neither; the network waits for both chains to reach equal length
D) Chain A, because it was created first chronologically
Answer: B – Cumulative work: Chain A $= 6 \times 1 = 6$; Chain B $= 4 \times 2 = 8$. Chain B wins.

Quiz: Questions 6–10

Q6. You sell a $500 laptop for Bitcoin and wait for 1 confirmation. The buyer controls 15% of hash power. What is the approximate reversal risk? % Bloom: Apply
A) Essentially zero — 1 confirmation is always safe
B) About 50% — it is a coin flip at 15% hash power
C) Roughly 5% — significant enough to warrant more confirmations for this value
D) Over 30% — 1 confirmation provides almost no security

Quiz: Questions 6–10

Q6. You sell a $500 laptop for Bitcoin and wait for 1 confirmation. The buyer controls 15% of hash power. What is the approximate reversal risk? % Bloom: Apply
A) Essentially zero — 1 confirmation is always safe
B) About 50% — it is a coin flip at 15% hash power
C) Roughly 5% — significant enough to warrant more confirmations for this value
D) Over 30% — 1 confirmation provides almost no security
Answer: C – At 15% hash power and 1 confirmation, the reversal probability is approximately 5%.

Q7. A coffee shop accepts 0 confirmations for purchases under $10. Is this reasonable? % Bloom: Apply
A) Yes, because the cost of a double-spend attack far exceeds the $10 at risk
B) No, because zero confirmations always means zero security
C) Yes, but only if the shop uses a Lightning Network channel
D) No, because any transaction can be reversed before 6 confirmations

Quiz: Questions 6–10

Q6. You sell a $500 laptop for Bitcoin and wait for 1 confirmation. The buyer controls 15% of hash power. What is the approximate reversal risk? % Bloom: Apply
A) Essentially zero — 1 confirmation is always safe
B) About 50% — it is a coin flip at 15% hash power
C) Roughly 5% — significant enough to warrant more confirmations for this value
D) Over 30% — 1 confirmation provides almost no security
Answer: C – At 15% hash power and 1 confirmation, the reversal probability is approximately 5%.

Q7. A coffee shop accepts 0 confirmations for purchases under $10. Is this reasonable? % Bloom: Apply
A) Yes, because the cost of a double-spend attack far exceeds the $10 at risk
B) No, because zero confirmations always means zero security
C) Yes, but only if the shop uses a Lightning Network channel
D) No, because any transaction can be reversed before 6 confirmations
Answer: A – A double-spend attack requires significant hash power; no rational attacker would spend thousands to steal $10.

Q8. If Bitcoin's total hash power suddenly doubles overnight, what happens to mining difficulty? % Bloom: Apply
A) It remains constant — difficulty only changes during hard forks
B) It halves to maintain the 10-minute block interval
C) It increases immediately with the next block
D) It doubles at the next difficulty adjustment (within $\sim$2 weeks) to restore the 10-minute target

Quiz: Questions 6–10

Q6. You sell a $500 laptop for Bitcoin and wait for 1 confirmation. The buyer controls 15% of hash power. What is the approximate reversal risk? % Bloom: Apply
A) Essentially zero — 1 confirmation is always safe
B) About 50% — it is a coin flip at 15% hash power
C) Roughly 5% — significant enough to warrant more confirmations for this value
D) Over 30% — 1 confirmation provides almost no security
Answer: C – At 15% hash power and 1 confirmation, the reversal probability is approximately 5%.

Q7. A coffee shop accepts 0 confirmations for purchases under $10. Is this reasonable? % Bloom: Apply
A) Yes, because the cost of a double-spend attack far exceeds the $10 at risk
B) No, because zero confirmations always means zero security
C) Yes, but only if the shop uses a Lightning Network channel
D) No, because any transaction can be reversed before 6 confirmations
Answer: A – A double-spend attack requires significant hash power; no rational attacker would spend thousands to steal $10.

Q8. If Bitcoin's total hash power suddenly doubles overnight, what happens to mining difficulty? % Bloom: Apply
A) It remains constant — difficulty only changes during hard forks
B) It halves to maintain the 10-minute block interval
C) It increases immediately with the next block
D) It doubles at the next difficulty adjustment (within $\sim$2 weeks) to restore the 10-minute target
Answer: D – Difficulty adjusts every 2,016 blocks ($\sim$2 weeks) to maintain the target block interval.

Q9. Bitcoin has 10-minute blocks and $\sim$0.3% fork rate. Ethereum has 15-second blocks and $\sim$6% fork rate. Why? % Bloom: Analyze
A) Ethereum has fewer miners, so collisions are more likely
B) With shorter block intervals, propagation time is a larger fraction of the block time, increasing fork probability
C) Ethereum's PoS consensus intentionally creates more forks for security
D) Ethereum blocks are larger, so they take longer to validate

Quiz: Questions 6–10

Q6. You sell a $500 laptop for Bitcoin and wait for 1 confirmation. The buyer controls 15% of hash power. What is the approximate reversal risk? % Bloom: Apply
A) Essentially zero — 1 confirmation is always safe
B) About 50% — it is a coin flip at 15% hash power
C) Roughly 5% — significant enough to warrant more confirmations for this value
D) Over 30% — 1 confirmation provides almost no security
Answer: C – At 15% hash power and 1 confirmation, the reversal probability is approximately 5%.

Q7. A coffee shop accepts 0 confirmations for purchases under $10. Is this reasonable? % Bloom: Apply
A) Yes, because the cost of a double-spend attack far exceeds the $10 at risk
B) No, because zero confirmations always means zero security
C) Yes, but only if the shop uses a Lightning Network channel
D) No, because any transaction can be reversed before 6 confirmations
Answer: A – A double-spend attack requires significant hash power; no rational attacker would spend thousands to steal $10.

Q8. If Bitcoin's total hash power suddenly doubles overnight, what happens to mining difficulty? % Bloom: Apply
A) It remains constant — difficulty only changes during hard forks
B) It halves to maintain the 10-minute block interval
C) It increases immediately with the next block
D) It doubles at the next difficulty adjustment (within $\sim$2 weeks) to restore the 10-minute target
Answer: D – Difficulty adjusts every 2,016 blocks ($\sim$2 weeks) to maintain the target block interval.

Q9. Bitcoin has 10-minute blocks and $\sim$0.3% fork rate. Ethereum has 15-second blocks and $\sim$6% fork rate. Why? % Bloom: Analyze
A) Ethereum has fewer miners, so collisions are more likely
B) With shorter block intervals, propagation time is a larger fraction of the block time, increasing fork probability
C) Ethereum's PoS consensus intentionally creates more forks for security
D) Ethereum blocks are larger, so they take longer to validate
Answer: B – Fork probability $\propto$ propagation time / block interval. Shorter intervals make the ratio worse.

Q10. In the March 2013 fork, developers asked miners to downgrade from v0.8 to v0.7. Why not stay on v0.8? % Bloom: Analyze
A) v0.8 had a security vulnerability that allowed double-spending
B) v0.7 was faster and more efficient than v0.8
C) Satoshi Nakamoto personally requested the downgrade
D) The widest-accepted version defines consensus; switching to v0.7 minimized orphaned blocks and user disruption

Quiz: Questions 6–10

Q6. You sell a $500 laptop for Bitcoin and wait for 1 confirmation. The buyer controls 15% of hash power. What is the approximate reversal risk? % Bloom: Apply
A) Essentially zero — 1 confirmation is always safe
B) About 50% — it is a coin flip at 15% hash power
C) Roughly 5% — significant enough to warrant more confirmations for this value
D) Over 30% — 1 confirmation provides almost no security
Answer: C – At 15% hash power and 1 confirmation, the reversal probability is approximately 5%.

Q7. A coffee shop accepts 0 confirmations for purchases under $10. Is this reasonable? % Bloom: Apply
A) Yes, because the cost of a double-spend attack far exceeds the $10 at risk
B) No, because zero confirmations always means zero security
C) Yes, but only if the shop uses a Lightning Network channel
D) No, because any transaction can be reversed before 6 confirmations
Answer: A – A double-spend attack requires significant hash power; no rational attacker would spend thousands to steal $10.

Q8. If Bitcoin's total hash power suddenly doubles overnight, what happens to mining difficulty? % Bloom: Apply
A) It remains constant — difficulty only changes during hard forks
B) It halves to maintain the 10-minute block interval
C) It increases immediately with the next block
D) It doubles at the next difficulty adjustment (within $\sim$2 weeks) to restore the 10-minute target
Answer: D – Difficulty adjusts every 2,016 blocks ($\sim$2 weeks) to maintain the target block interval.

Q9. Bitcoin has 10-minute blocks and $\sim$0.3% fork rate. Ethereum has 15-second blocks and $\sim$6% fork rate. Why? % Bloom: Analyze
A) Ethereum has fewer miners, so collisions are more likely
B) With shorter block intervals, propagation time is a larger fraction of the block time, increasing fork probability
C) Ethereum's PoS consensus intentionally creates more forks for security
D) Ethereum blocks are larger, so they take longer to validate
Answer: B – Fork probability $\propto$ propagation time / block interval. Shorter intervals make the ratio worse.

Q10. In the March 2013 fork, developers asked miners to downgrade from v0.8 to v0.7. Why not stay on v0.8? % Bloom: Analyze
A) v0.8 had a security vulnerability that allowed double-spending
B) v0.7 was faster and more efficient than v0.8
C) Satoshi Nakamoto personally requested the downgrade
D) The widest-accepted version defines consensus; switching to v0.7 minimized orphaned blocks and user disruption
Answer: D – The network needed to converge on one rule set; v0.7 was more widely deployed and accepted.

Quiz: Questions 11–15

Q11. Why does Bitcoin use cumulative work instead of block count for chain selection? % Bloom: Analyze
A) Block count is harder to compute than cumulative work
B) Cumulative work allows miners to skip the difficulty adjustment
C) Block count would make the blockchain incompatible with light clients
D) An attacker could cheaply produce many low-difficulty blocks to create a longer chain

Quiz: Questions 11–15

Q11. Why does Bitcoin use cumulative work instead of block count for chain selection? % Bloom: Analyze
A) Block count is harder to compute than cumulative work
B) Cumulative work allows miners to skip the difficulty adjustment
C) Block count would make the blockchain incompatible with light clients
D) An attacker could cheaply produce many low-difficulty blocks to create a longer chain
Answer: D – Counting blocks rewards volume; counting work rewards effort. An attacker's easy blocks cannot outwork honest mining.

Q12. How does Proof of Work prevent Sybil attacks in Bitcoin's consensus? % Bloom: Analyze
A) PoW requires every node to register with a central authority before mining
B) PoW limits the number of nodes that can connect to the network
C) Creating fake nodes does not help because each block requires real computational work regardless of node count
D) PoW encrypts all communication between nodes to prevent impersonation

Quiz: Questions 11–15

Q11. Why does Bitcoin use cumulative work instead of block count for chain selection? % Bloom: Analyze
A) Block count is harder to compute than cumulative work
B) Cumulative work allows miners to skip the difficulty adjustment
C) Block count would make the blockchain incompatible with light clients
D) An attacker could cheaply produce many low-difficulty blocks to create a longer chain
Answer: D – Counting blocks rewards volume; counting work rewards effort. An attacker's easy blocks cannot outwork honest mining.

Q12. How does Proof of Work prevent Sybil attacks in Bitcoin's consensus? % Bloom: Analyze
A) PoW requires every node to register with a central authority before mining
B) PoW limits the number of nodes that can connect to the network
C) Creating fake nodes does not help because each block requires real computational work regardless of node count
D) PoW encrypts all communication between nodes to prevent impersonation
Answer: C – PoW makes identity irrelevant; voting power comes from hash power, not from the number of nodes.

Q13. An exchange requires 6 confirmations for a $10,000 deposit but only 1 for a $100 deposit. What principle drives this? % Bloom: Apply
A) Larger amounts require more bandwidth to verify on the network
B) Required confirmations should be proportional to the value at risk
C) The Bitcoin protocol mandates different confirmation counts based on transaction size
D) Smaller transactions are processed faster by miners

Quiz: Questions 11–15

Q11. Why does Bitcoin use cumulative work instead of block count for chain selection? % Bloom: Analyze
A) Block count is harder to compute than cumulative work
B) Cumulative work allows miners to skip the difficulty adjustment
C) Block count would make the blockchain incompatible with light clients
D) An attacker could cheaply produce many low-difficulty blocks to create a longer chain
Answer: D – Counting blocks rewards volume; counting work rewards effort. An attacker's easy blocks cannot outwork honest mining.

Q12. How does Proof of Work prevent Sybil attacks in Bitcoin's consensus? % Bloom: Analyze
A) PoW requires every node to register with a central authority before mining
B) PoW limits the number of nodes that can connect to the network
C) Creating fake nodes does not help because each block requires real computational work regardless of node count
D) PoW encrypts all communication between nodes to prevent impersonation
Answer: C – PoW makes identity irrelevant; voting power comes from hash power, not from the number of nodes.

Q13. An exchange requires 6 confirmations for a $10,000 deposit but only 1 for a $100 deposit. What principle drives this? % Bloom: Apply
A) Larger amounts require more bandwidth to verify on the network
B) Required confirmations should be proportional to the value at risk
C) The Bitcoin protocol mandates different confirmation counts based on transaction size
D) Smaller transactions are processed faster by miners
Answer: B – Higher value = higher incentive for an attacker = more confirmations needed to reach acceptable risk.

Q14. BIP 152 (Compact Blocks) reduced block propagation from $\sim$40s to $\sim$8s. What is the primary benefit? % Bloom: Apply
A) Fewer natural forks, because the window for simultaneous block discovery is shorter
B) Lower transaction fees, because blocks are smaller
C) Faster transaction confirmation, because blocks are validated more quickly
D) Increased block size, allowing more transactions per block

Quiz: Questions 11–15

Q11. Why does Bitcoin use cumulative work instead of block count for chain selection? % Bloom: Analyze
A) Block count is harder to compute than cumulative work
B) Cumulative work allows miners to skip the difficulty adjustment
C) Block count would make the blockchain incompatible with light clients
D) An attacker could cheaply produce many low-difficulty blocks to create a longer chain
Answer: D – Counting blocks rewards volume; counting work rewards effort. An attacker's easy blocks cannot outwork honest mining.

Q12. How does Proof of Work prevent Sybil attacks in Bitcoin's consensus? % Bloom: Analyze
A) PoW requires every node to register with a central authority before mining
B) PoW limits the number of nodes that can connect to the network
C) Creating fake nodes does not help because each block requires real computational work regardless of node count
D) PoW encrypts all communication between nodes to prevent impersonation
Answer: C – PoW makes identity irrelevant; voting power comes from hash power, not from the number of nodes.

Q13. An exchange requires 6 confirmations for a $10,000 deposit but only 1 for a $100 deposit. What principle drives this? % Bloom: Apply
A) Larger amounts require more bandwidth to verify on the network
B) Required confirmations should be proportional to the value at risk
C) The Bitcoin protocol mandates different confirmation counts based on transaction size
D) Smaller transactions are processed faster by miners
Answer: B – Higher value = higher incentive for an attacker = more confirmations needed to reach acceptable risk.

Q14. BIP 152 (Compact Blocks) reduced block propagation from ∼40s to ∼8s. What is the primary benefit? % Bloom: Apply
A) Fewer natural forks, because the window for simultaneous block discovery is shorter
B) Lower transaction fees, because blocks are smaller
C) Faster transaction confirmation, because blocks are validated more quickly
D) Increased block size, allowing more transactions per block
Answer: A – Shorter propagation time means less chance that two blocks are found during the same window.

Q15. What does "probabilistic finality" mean in Bitcoin? % Bloom: Analyze
A) Transactions are final only after a random number of confirmations determined by the network
B) The probability of a transaction being included in a block varies randomly
C) The probability of reversal decreases exponentially with each confirmation but never reaches exactly zero
D) Miners probabilistically select which transactions to include based on fee size

Quiz: Questions 11–15

Q11. Why does Bitcoin use cumulative work instead of block count for chain selection? % Bloom: Analyze
A) Block count is harder to compute than cumulative work
B) Cumulative work allows miners to skip the difficulty adjustment
C) Block count would make the blockchain incompatible with light clients
D) An attacker could cheaply produce many low-difficulty blocks to create a longer chain
Answer: D – Counting blocks rewards volume; counting work rewards effort. An attacker's easy blocks cannot outwork honest mining.

Q12. How does Proof of Work prevent Sybil attacks in Bitcoin's consensus? % Bloom: Analyze
A) PoW requires every node to register with a central authority before mining
B) PoW limits the number of nodes that can connect to the network
C) Creating fake nodes does not help because each block requires real computational work regardless of node count
D) PoW encrypts all communication between nodes to prevent impersonation
Answer: C – PoW makes identity irrelevant; voting power comes from hash power, not from the number of nodes.

Q13. An exchange requires 6 confirmations for a $10,000 deposit but only 1 for a $100 deposit. What principle drives this? % Bloom: Apply
A) Larger amounts require more bandwidth to verify on the network
B) Required confirmations should be proportional to the value at risk
C) The Bitcoin protocol mandates different confirmation counts based on transaction size
D) Smaller transactions are processed faster by miners
Answer: B – Higher value = higher incentive for an attacker = more confirmations needed to reach acceptable risk.

Q14. BIP 152 (Compact Blocks) reduced block propagation from $\sim$40s to $\sim$8s. What is the primary benefit? % Bloom: Apply
A) Fewer natural forks, because the window for simultaneous block discovery is shorter
B) Lower transaction fees, because blocks are smaller
C) Faster transaction confirmation, because blocks are validated more quickly
D) Increased block size, allowing more transactions per block
Answer: A – Shorter propagation time means less chance that two blocks are found during the same window.

Q15. What does "probabilistic finality" mean in Bitcoin? % Bloom: Analyze
A) Transactions are final only after a random number of confirmations determined by the network
B) The probability of a transaction being included in a block varies randomly
C) The probability of reversal decreases exponentially with each confirmation but never reaches exactly zero
D) Miners probabilistically select which transactions to include based on fee size
Answer: C – Each confirmation makes reversal exponentially harder, but mathematical certainty is never achieved.

Quiz: Questions 16–20

Q16. Miner C built on Block A during a fork. Block B's branch wins with more cumulative work. What does Miner C do? % Bloom: Apply
A) Continue mining on Block A's branch to try to overtake Block B
B) Shut down and wait for the fork to resolve naturally
C) Appeal to a network administrator to restore Block A's branch
D) Abandon Block A's branch, switch to the canonical chain (Block B's branch), and start mining there

Quiz: Questions 16–20

Q16. Miner C built on Block A during a fork. Block B's branch wins with more cumulative work. What does Miner C do? % Bloom: Apply
A) Continue mining on Block A's branch to try to overtake Block B
B) Shut down and wait for the fork to resolve naturally
C) Appeal to a network administrator to restore Block A's branch
D) Abandon Block A's branch, switch to the canonical chain (Block B's branch), and start mining there
Answer: D – Rational miners always switch to the chain with the most cumulative work to maximize their rewards.

Q17. Why is the phrase "longest chain" technically imprecise when describing Bitcoin's consensus rule? % Bloom: Analyze
A) Bitcoin selects the chain with the most cumulative computational work, not the one with the most blocks
B) "Longest" refers to byte size, not block count, which is confusing
C) Some blocks are longer than others due to variable transaction counts
D) The phrase was never used by Satoshi and is a common misconception

Quiz: Questions 16–20

Q16. Miner C built on Block A during a fork. Block B's branch wins with more cumulative work. What does Miner C do? % Bloom: Apply
A) Continue mining on Block A's branch to try to overtake Block B
B) Shut down and wait for the fork to resolve naturally
C) Appeal to a network administrator to restore Block A's branch
D) Abandon Block A's branch, switch to the canonical chain (Block B's branch), and start mining there
Answer: D – Rational miners always switch to the chain with the most cumulative work to maximize their rewards.

Q17. Why is the phrase "longest chain" technically imprecise when describing Bitcoin's consensus rule? % Bloom: Analyze
A) Bitcoin selects the chain with the most cumulative computational work, not the one with the most blocks
B) "Longest" refers to byte size, not block count, which is confusing
C) Some blocks are longer than others due to variable transaction counts
D) The phrase was never used by Satoshi and is a common misconception
Answer: A – A shorter chain with higher-difficulty blocks can have more cumulative work than a longer chain of easy blocks.

Q18. A 10% attacker tries to reverse a transaction with 6 confirmations. $P \approx 0.002\%$. What does this mean practically? % Bloom: Apply
A) The attack will succeed once every 500 attempts
B) The attacker would need approximately 50,000 attempts to expect one success
C) The attack is guaranteed to fail every time
D) The attacker needs 10% more hash power to have any chance

Quiz: Questions 16–20

Q16. Miner C built on Block A during a fork. Block B's branch wins with more cumulative work. What does Miner C do? % Bloom: Apply
A) Continue mining on Block A's branch to try to overtake Block B
B) Shut down and wait for the fork to resolve naturally
C) Appeal to a network administrator to restore Block A's branch
D) Abandon Block A's branch, switch to the canonical chain (Block B's branch), and start mining there
Answer: D – Rational miners always switch to the chain with the most cumulative work to maximize their rewards.

Q17. Why is the phrase "longest chain" technically imprecise when describing Bitcoin's consensus rule? % Bloom: Analyze
A) Bitcoin selects the chain with the most cumulative computational work, not the one with the most blocks
B) "Longest" refers to byte size, not block count, which is confusing
C) Some blocks are longer than others due to variable transaction counts
D) The phrase was never used by Satoshi and is a common misconception
Answer: A – A shorter chain with higher-difficulty blocks can have more cumulative work than a longer chain of easy blocks.

Q18. A 10% attacker tries to reverse a transaction with 6 confirmations. P $\approx$ 0.002%. What does this mean practically? % Bloom: Apply
A) The attack will succeed once every 500 attempts
B) The attacker would need approximately 50,000 attempts to expect one success
C) The attack is guaranteed to fail every time
D) The attacker needs 10% more hash power to have any chance
Answer: B – 0.002% $= 1/50{,}000$. The attacker would need $\sim$50,000 attempts, each costing millions in electricity.

Q19. As Bitcoin's block reward approaches zero through halvings, what is the strongest argument for continued security? % Bloom: Evaluate
A) Miners will continue mining at a loss because they believe in Bitcoin's mission
B) The Bitcoin protocol will switch to Proof of Stake like Ethereum did
C) Transaction fees must grow to provide sufficient incentive for miners to secure the network
D) Governments will subsidize mining to maintain the network's security

Quiz: Questions 16–20

Q16. Miner C built on Block A during a fork. Block B's branch wins with more cumulative work. What does Miner C do? % Bloom: Apply
A) Continue mining on Block A's branch to try to overtake Block B
B) Shut down and wait for the fork to resolve naturally
C) Appeal to a network administrator to restore Block A's branch
D) Abandon Block A's branch, switch to the canonical chain (Block B's branch), and start mining there
Answer: D – Rational miners always switch to the chain with the most cumulative work to maximize their rewards.

Q17. Why is the phrase "longest chain" technically imprecise when describing Bitcoin's consensus rule? % Bloom: Analyze
A) Bitcoin selects the chain with the most cumulative computational work, not the one with the most blocks
B) "Longest" refers to byte size, not block count, which is confusing
C) Some blocks are longer than others due to variable transaction counts
D) The phrase was never used by Satoshi and is a common misconception
Answer: A – A shorter chain with higher-difficulty blocks can have more cumulative work than a longer chain of easy blocks.

Q18. A 10% attacker tries to reverse a transaction with 6 confirmations. $P \approx 0.002\%$. What does this mean practically? % Bloom: Apply
A) The attack will succeed once every 500 attempts
B) The attacker would need approximately 50,000 attempts to expect one success
C) The attack is guaranteed to fail every time
D) The attacker needs 10% more hash power to have any chance
Answer: B – $0.002\% = 1/50{,}000$. The attacker would need $\sim$50,000 attempts, each costing millions in electricity.

Q19. As Bitcoin's block reward approaches zero through halvings, what is the strongest argument for continued security? % Bloom: Evaluate
A) Miners will continue mining at a loss because they believe in Bitcoin's mission
B) The Bitcoin protocol will switch to Proof of Stake like Ethereum did
C) Transaction fees must grow to provide sufficient incentive for miners to secure the network
D) Governments will subsidize mining to maintain the network's security
Answer: C – The security budget must transition from block rewards to transaction fees as rewards diminish.

Q20. Critics argue Bitcoin's $15B annual mining cost is "wasteful." What is the strongest counter-argument? % Bloom: Evaluate
A) It is the cost of providing trustless, censorship-resistant finality for a $1.8 trillion network
B) The energy is fully renewable and has zero environmental impact
C) Traditional banks spend even more, so Bitcoin is actually cheaper
D) Mining costs will drop to zero once all 21 million BTC are mined

Quiz: Questions 16–20

Q16. Miner C built on Block A during a fork. Block B's branch wins with more cumulative work. What does Miner C do? % Bloom: Apply
A) Continue mining on Block A's branch to try to overtake Block B
B) Shut down and wait for the fork to resolve naturally
C) Appeal to a network administrator to restore Block A's branch
D) Abandon Block A's branch, switch to the canonical chain (Block B's branch), and start mining there
Answer: D – Rational miners always switch to the chain with the most cumulative work to maximize their rewards.

Q17. Why is the phrase "longest chain" technically imprecise when describing Bitcoin's consensus rule? % Bloom: Analyze
A) Bitcoin selects the chain with the most cumulative computational work, not the one with the most blocks
B) "Longest" refers to byte size, not block count, which is confusing
C) Some blocks are longer than others due to variable transaction counts
D) The phrase was never used by Satoshi and is a common misconception
Answer: A – A shorter chain with higher-difficulty blocks can have more cumulative work than a longer chain of easy blocks.

Q18. A 10% attacker tries to reverse a transaction with 6 confirmations. P $\approx$ 0.002%. What does this mean practically? % Bloom: Apply
A) The attack will succeed once every 500 attempts
B) The attacker would need approximately 50,000 attempts to expect one success
C) The attack is guaranteed to fail every time
D) The attacker needs 10% more hash power to have any chance
Answer: B – 0.002% $= 1/50{,}000$. The attacker would need $\sim$50,000 attempts, each costing millions in electricity.

Q19. As Bitcoin's block reward approaches zero through halvings, what is the strongest argument for continued security? % Bloom: Evaluate
A) Miners will continue mining at a loss because they believe in Bitcoin's mission
B) The Bitcoin protocol will switch to Proof of Stake like Ethereum did
C) Transaction fees must grow to provide sufficient incentive for miners to secure the network
D) Governments will subsidize mining to maintain the network's security
Answer: C – The security budget must transition from block rewards to transaction fees as rewards diminish.

Q20. Critics argue Bitcoin's $15B annual mining cost is "wasteful." What is the strongest counter-argument? % Bloom: Evaluate
A) It is the cost of providing trustless, censorship-resistant finality for a $1.8 trillion network
B) The energy is fully renewable and has zero environmental impact
C) Traditional banks spend even more, so Bitcoin is actually cheaper
D) Mining costs will drop to zero once all 21 million BTC are mined
Answer: A – The mining cost buys a specific service (trustless finality) that no cheaper alternative currently provides.