Block Consensus: How a Distributed Network Agrees on One Truth

Mini-Lecture — 30 Minutes

Prof. Dr. Jörg Osterrieder

Blockchain, Crypto Economy & NFTs

Learning Objectives:

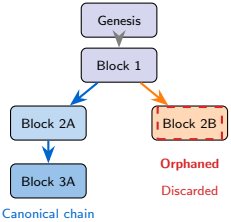
1. Explain how Bitcoin resolves temporary forks when two blocks are found simultaneously
2. Distinguish between "longest chain" and "most cumulative work"
3. Describe why 6 confirmations is the standard finality threshold

The Fork Problem

A Thought Experiment

Two miners in different countries solve the proof-of-work puzzle within milliseconds of each other. Both blocks are valid. The network's 50,000 nodes temporarily disagree about which block is canonical.

This happens roughly **once every 1–2 weeks** in Bitcoin — not an error, but an expected consequence of decentralised mining.



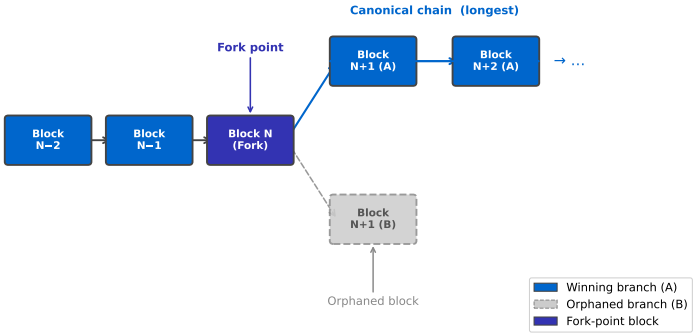
Analogy: Choosing a restaurant without talking. Everyone follows the same rule — *go where the most people are* — and the group converges without coordination.

Bitcoin's fork resolution works the same way: every node applies an identical chain-selection rule, and the network converges automatically.

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

When the Chain Splits

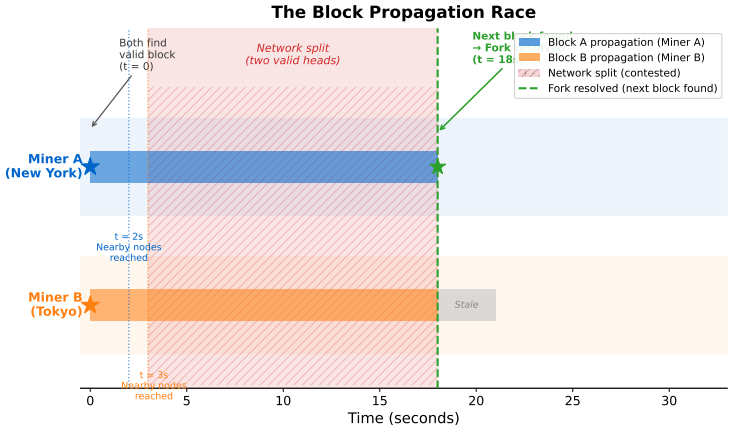
Fork Resolution: Longest Chain Wins



- Each node (circle) represents a valid block proposed by a miner
- Competing branches exist briefly — only one survives as canonical
- Orphaned blocks are discarded; their transactions return to the mempool

Bitcoin experiences natural forks roughly once every 1–2 weeks

The Block Propagation Race



- Block A and Block B race across the network after near-simultaneous discovery
- Nodes adopt whichever block they hear first — network splits temporarily
- The fork resolves when the next block extends one branch, making it longer

Block propagation takes 8–15 seconds — during this window, forks can form

Chain Selection: Length vs. Work

Common misconception: Bitcoin follows the *longest chain*.

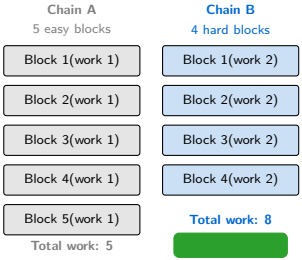
Reality: Bitcoin's code implements *most cumulative proof-of-work*.

Chain	Blocks	Cumulative Work
Chain A	5 blocks @ diff 1	Work = 5
Chain B	4 blocks @ diff 2	Work = 8
Winner		**Chain B**

Why it matters: An attacker cannot cheaply produce many low-difficulty blocks to rewrite history. Each block must represent real, expensive computation.

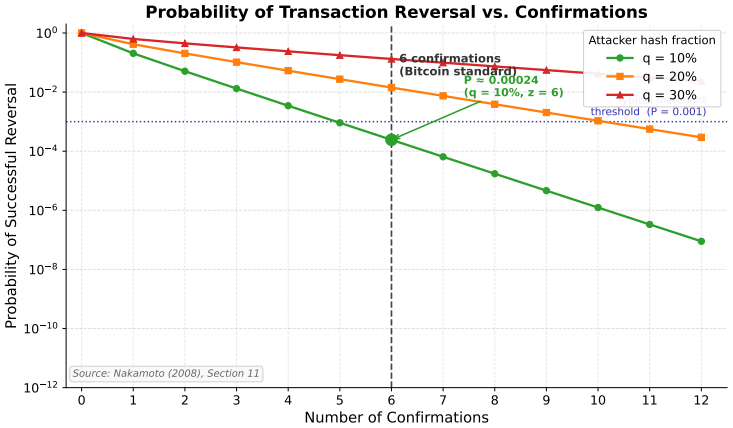
Formula:

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



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

Confirmation Probability



- Each confirmation multiplies the computational cost of a reversal attack
- Probability of successful reversal decays exponentially with confirmations
- Assumes attacker controls 10% of hash rate (Nakamoto 2008, Section 11)

Source: Nakamoto (2008), Section 11

The Math: Why 6 Confirmations?

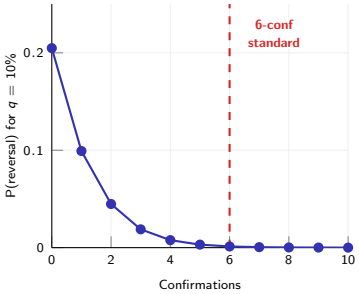
Nakamoto (2008) computed reversal probabilities for an attacker controlling fraction q of total hash rate:

q (attacker)	Confirmations	P(reversal)
10%	1	0.205%
10%	3	0.017%
10%	6	$<$0.002%
30%	6	17.7%

Analogy: Like cement drying — after 10 minutes it is *probably* solid, after 60 minutes it is *practically* solid. The risk never reaches exactly zero.

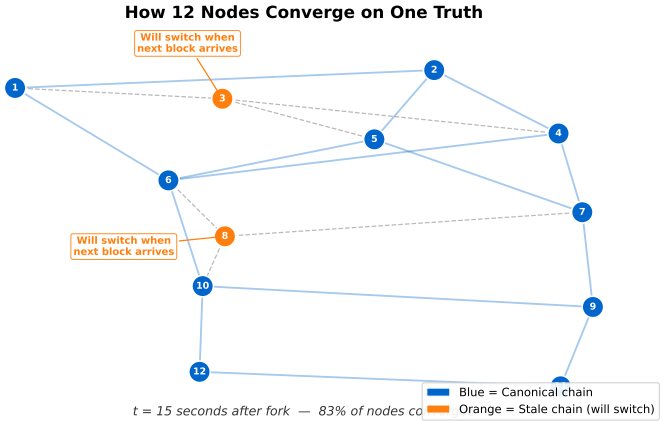
Practical thresholds:

- Coffee shop ($5): 0 confirmations acceptable
- Exchange deposit: 6 confirmations standard
- Large settlement ($1M+): 12+ confirmations



Each confirmation exponentially reduces the probability of reversal

How Nodes Converge



- Across 12 nodes, most converge on the canonical chain within seconds of fork resolution
- Nodes following divergent branches switch automatically once a longer chain is broadcast
- No voting, no leader — agreement emerges from identical rule application

Consensus is emergent — nodes following the same rule produces collective agreement

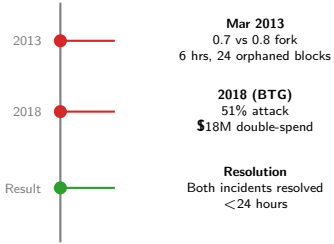
Historical Forks

March 2013 Accidental Fork

Bitcoin 0.7 and 0.8 nodes applied different database lock limits, causing a chain split lasting **6 hours** and orphaning **24 blocks**. Developers coordinated via IRC to downgrade mining pools to 0.7 — the wider-accepted version — allowing the network to converge on a single chain without a hard fork.

Bitcoin Gold 51% Attack (2018)

An attacker rented sufficient hash rate to double-spend **$18M** of Bitcoin Gold across multiple exchanges. The attack succeeded because BTG's hash rate was too low to make renting it expensive. Exchanges were forced to raise their confirmation thresholds to 50+ blocks.

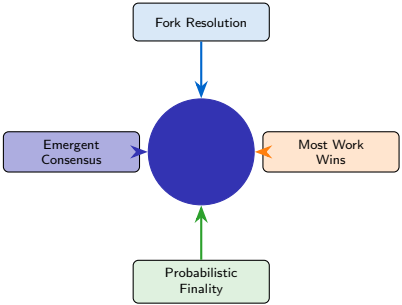


Both incidents resolved within hours — demonstrating Bitcoin's resilience

Key Takeaways

What You Should Now Know

1. **Forks are normal:** Two miners finding valid blocks simultaneously creates a temporary split; the chain-selection rule resolves it automatically within one block.
2. **Most cumulative work wins, not most blocks:** An attacker cannot rewrite history with cheap, low-difficulty blocks — real computation is required.
3. **Finality is probabilistic:** 6 confirmations reduces reversal probability below 0.002% for an attacker with 10% of hash rate — the practical industry standard.
4. **Consensus is emergent:** No voting, no leader, no central coordinator — agreement arises from every node applying the same rule independently.



Fork resolution + chain selection + probabilistic finality = Nakamoto Consensus

Quiz — Questions 1–5

Q1. What is a natural fork in Bitcoin?
A) A planned network upgrade B) Two miners finding valid blocks at approximately the same time C) A software bug D) A 51% attack

Quiz — Questions 1–5

Q1. What is a natural fork in Bitcoin?
A) A planned network upgrade B) Two miners finding valid blocks at approximately the same time C) A software bug D) A 51% attack
B – Natural forks occur when two miners solve the puzzle simultaneously; both blocks are valid and the network temporarily disagrees.

Q2. What does probabilistic finality mean?
A) Finality is guaranteed after 6 blocks B) Finality is impossible on blockchains C) Probability of reversal decreases with each confirmation but never reaches exactly zero D) Nodes vote to confirm finality

Quiz — Questions 1–5

Q1. What is a natural fork in Bitcoin?
A) A planned network upgrade B) Two miners finding valid blocks at approximately the same time C) A software bug D) A 51% attack
B – Natural forks occur when two miners solve the puzzle simultaneously; both blocks are valid and the network temporarily disagrees.

Q2. What does probabilistic finality mean?
A) Finality is guaranteed after 6 blocks B) Finality is impossible on blockchains C) Probability of reversal decreases with each confirmation but never reaches exactly zero D) Nodes vote to confirm finality
C – Each additional confirmation makes reversal exponentially harder but never mathematically impossible.

Q3. Chain A has 6 blocks at difficulty 1 (total work 6). Chain B has 4 blocks at difficulty 2 (total work 8). Which chain does Bitcoin follow?
A) Chain A — more blocks B) Chain B — more cumulative work C) Both chains equally D) The older chain

Quiz — Questions 1–5

Q1. What is a natural fork in Bitcoin?
A) A planned network upgrade B) Two miners finding valid blocks at approximately the same time C) A software bug D) A 51% attack
B – Natural forks occur when two miners solve the puzzle simultaneously; both blocks are valid and the network temporarily disagrees.

Q2. What does probabilistic finality mean?
A) Finality is guaranteed after 6 blocks B) Finality is impossible on blockchains C) Probability of reversal decreases with each confirmation but never reaches exactly zero D) Nodes vote to confirm finality
C – Each additional confirmation makes reversal exponentially harder but never mathematically impossible.

Q3. Chain A has 6 blocks at difficulty 1 (total work 6). Chain B has 4 blocks at difficulty 2 (total work 8). Which chain does Bitcoin follow?
A) Chain A — more blocks B) Chain B — more cumulative work C) Both chains equally D) The older chain
B – Bitcoin selects the chain with the most cumulative proof-of-work, not the most blocks.

Q4. A merchant accepts a $500 purchase after just 1 confirmation. How risky is this?
A) Moderately risky — limited protection against a determined double-spend attempt B) Zero risk C) Extremely risky, equivalent to no confirmation D) Safe because miners already validated it

Quiz — Questions 1–5

Q1. What is a natural fork in Bitcoin?
A) A planned network upgrade B) Two miners finding valid blocks at approximately the same time C) A software bug D) A 51% attack
B – Natural forks occur when two miners solve the puzzle simultaneously; both blocks are valid and the network temporarily disagrees.

Q2. What does probabilistic finality mean?
A) Finality is guaranteed after 6 blocks B) Finality is impossible on blockchains C) Probability of reversal decreases with each confirmation but never reaches exactly zero D) Nodes vote to confirm finality
C – Each additional confirmation makes reversal exponentially harder but never mathematically impossible.

Q3. Chain A has 6 blocks at difficulty 1 (total work 6). Chain B has 4 blocks at difficulty 2 (total work 8). Which chain does Bitcoin follow?
A) Chain A — more blocks B) Chain B — more cumulative work C) Both chains equally D) The older chain
B – Bitcoin selects the chain with the most cumulative proof-of-work, not the most blocks.

Q4. A merchant accepts a $500 purchase after just 1 confirmation. How risky is this?
A) Moderately risky — limited protection against a determined double-spend attempt B) Zero risk C) Extremely risky, equivalent to no confirmation D) Safe because miners already validated it
A – One confirmation significantly reduces risk but an attacker with sufficient hash rate could still attempt a reversal.

Q5. What happens to transactions in an orphaned block?
A) They are permanently lost B) They are automatically refunded C) They return to the mempool and are re-included in the next block D) They are penalised with a fee

Quiz — Questions 1–5

Q1. What is a natural fork in Bitcoin?
A) A planned network upgrade B) Two miners finding valid blocks at approximately the same time C) A software bug D) A 51% attack
B – Natural forks occur when two miners solve the puzzle simultaneously; both blocks are valid and the network temporarily disagrees.

Q2. What does probabilistic finality mean?
A) Finality is guaranteed after 6 blocks B) Finality is impossible on blockchains C) Probability of reversal decreases with each confirmation but never reaches exactly zero D) Nodes vote to confirm finality
C – Each additional confirmation makes reversal exponentially harder but never mathematically impossible.

Q3. Chain A has 6 blocks at difficulty 1 (total work 6). Chain B has 4 blocks at difficulty 2 (total work 8). Which chain does Bitcoin follow?
A) Chain A — more blocks B) Chain B — more cumulative work C) Both chains equally D) The older chain
B – Bitcoin selects the chain with the most cumulative proof-of-work, not the most blocks.

Q4. A merchant accepts a $500 purchase after just 1 confirmation. How risky is this?
A) Moderately risky — limited protection against a determined double-spend attempt B) Zero risk C) Extremely risky, equivalent to no confirmation D) Safe because miners already validated it
A – One confirmation significantly reduces risk but an attacker with sufficient hash rate could still attempt a reversal.

Q5. What happens to transactions in an orphaned block?
A) They are permanently lost B) They are automatically refunded C) They return to the mempool and are re-included in the next block D) They are penalised with a fee
C – Orphaned transactions re-enter the mempool and are typically re-confirmed within the next few blocks.

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

Quiz — Questions 6–10

Q6. Why is Bitcoin's 10-minute block target deliberate?
A) To limit energy use B) To maximise miner revenue C) To slow transaction throughput D) It makes propagation delay negligible compared to block interval, minimising forks

Quiz — Questions 6–10

Q6. Why is Bitcoin's 10-minute block target deliberate?
A) To limit energy use B) To maximise miner revenue C) To slow transaction throughput D) It makes propagation delay negligible compared to block interval, minimising forks
D – With 8–15 second propagation and 10-minute blocks, the fork window is less than 2.5% of the block interval.

Q7. Why does Bitcoin measure cumulative work rather than block count?
A) An attacker could cheaply produce many low-difficulty blocks to create a longer chain B) Block count is harder to verify C) Cumulative work is easier to compute D) Satoshi made an implementation error

Quiz — Questions 6–10

Q6. Why is Bitcoin's 10-minute block target deliberate?
A) To limit energy use B) To maximise miner revenue C) To slow transaction throughput D) It makes propagation delay negligible compared to block interval, minimising forks
D – With 8–15 second propagation and 10-minute blocks, the fork window is less than 2.5% of the block interval.

Q7. Why does Bitcoin measure cumulative work rather than block count?
A) An attacker could cheaply produce many low-difficulty blocks to create a longer chain B) Block count is harder to verify C) Cumulative work is easier to compute D) Satoshi made an implementation error
A – Counting blocks would allow an attacker with low-difficulty hardware to outrun honest miners; cumulative work requires real, expensive computation.

Q8. In the March 2013 fork, why did developers instruct miners to downgrade to version 0.7?
A) Version 0.8 had a critical security vulnerability B) Version 0.7 produced longer blocks C) The widest-accepted chain version wins, minimising disruption to the broader network D) Regulators required it

Quiz — Questions 6–10

Q6. Why is Bitcoin's 10-minute block target deliberate?
A) To limit energy use B) To maximise miner revenue C) To slow transaction throughput D) It makes propagation delay negligible compared to block interval, minimising forks
D – With 8–15 second propagation and 10-minute blocks, the fork window is less than 2.5% of the block interval.

Q7. Why does Bitcoin measure cumulative work rather than block count?
A) An attacker could cheaply produce many low-difficulty blocks to create a longer chain B) Block count is harder to verify C) Cumulative work is easier to compute D) Satoshi made an implementation error
A – Counting blocks would allow an attacker with low-difficulty hardware to outrun honest miners; cumulative work requires real, expensive computation.

Q8. In the March 2013 fork, why did developers instruct miners to downgrade to version 0.7?
A) Version 0.8 had a critical security vulnerability B) Version 0.7 produced longer blocks C) The widest-accepted chain version wins, minimising disruption to the broader network D) Regulators required it
C – Coordinating on the most widely-adopted version restored consensus with minimum disruption.

Q9. A coffee shop accepts 0-confirmations for a $5 purchase. Is this reasonable?
A) No — always wait for 6 confirmations B) No — double-spend attacks are common C) Only if the customer shows ID D) Yes — the cost of executing a double-spend far exceeds the value at risk

Quiz — Questions 6–10

Q6. Why is Bitcoin's 10-minute block target deliberate?
A) To limit energy use B) To maximise miner revenue C) To slow transaction throughput D) It makes propagation delay negligible compared to block interval, minimising forks
D – With 8–15 second propagation and 10-minute blocks, the fork window is less than 2.5% of the block interval.

Q7. Why does Bitcoin measure cumulative work rather than block count?
A) An attacker could cheaply produce many low-difficulty blocks to create a longer chain B) Block count is harder to verify C) Cumulative work is easier to compute D) Satoshi made an implementation error
A – Counting blocks would allow an attacker with low-difficulty hardware to outrun honest miners; cumulative work requires real, expensive computation.

Q8. In the March 2013 fork, why did developers instruct miners to downgrade to version 0.7?
A) Version 0.8 had a critical security vulnerability B) Version 0.7 produced longer blocks C) The widest-accepted chain version wins, minimising disruption to the broader network D) Regulators required it
C – Coordinating on the most widely-adopted version restored consensus with minimum disruption.

Q9. A coffee shop accepts 0-confirmations for a $5 purchase. Is this reasonable?
A) No — always wait for 6 confirmations B) No — double-spend attacks are common C) Only if the customer shows ID D) Yes — the cost of executing a double-spend far exceeds the value at risk
D – For tiny amounts, the economics of mounting an attack do not justify the reward; 0-conf is a rational business decision.

Q10. Block rewards will eventually halve toward zero. What sustains network security long-term?
A) Transaction fees must replace block rewards as the primary miner incentive B) Mining hardware becomes cheaper over time C) The Bitcoin foundation funds miners D) Security becomes less necessary as adoption grows

Quiz — Questions 6–10

Q6. Why is Bitcoin's 10-minute block target deliberate?
A) To limit energy use B) To maximise miner revenue C) To slow transaction throughput D) It makes propagation delay negligible compared to block interval, minimising forks
D – With 8–15 second propagation and 10-minute blocks, the fork window is less than 2.5% of the block interval.

Q7. Why does Bitcoin measure cumulative work rather than block count?
A) An attacker could cheaply produce many low-difficulty blocks to create a longer chain B) Block count is harder to verify C) Cumulative work is easier to compute D) Satoshi made an implementation error
A – Counting blocks would allow an attacker with low-difficulty hardware to outrun honest miners; cumulative work requires real, expensive computation.

Q8. In the March 2013 fork, why did developers instruct miners to downgrade to version 0.7?
A) Version 0.8 had a critical security vulnerability B) Version 0.7 produced longer blocks C) The widest-accepted chain version wins, minimising disruption to the broader network D) Regulators required it
C – Coordinating on the most widely-adopted version restored consensus with minimum disruption.

Q9. A coffee shop accepts 0-confirmations for a $5 purchase. Is this reasonable?
A) No — always wait for 6 confirmations B) No — double-spend attacks are common C) Only if the customer shows ID D) Yes — the cost of executing a double-spend far exceeds the value at risk
D – For tiny amounts, the economics of mounting an attack do not justify the reward; 0-conf is a rational business decision.

Q10. Block rewards will eventually halve toward zero. What sustains network security long-term?
A) Transaction fees must replace block rewards as the primary miner incentive B) Mining hardware becomes cheaper over time C) The Bitcoin foundation funds miners D) Security becomes less necessary as adoption grows
A – As block subsidies decay, transaction fees are the intended long-run security budget — an open research question in Bitcoin economics.

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