# Block Consensus – Quiz

20 Multiple-Choice Questions

*Bloom's levels: 4 Understand · 8 Apply · 6 Analyze · 2 Evaluate*

Prof. Dr. Jörg Osterrieder

BSc Blockchain, Crypto Economy & NFTs

Spring 2026

# Quiz Questions 1–5

**Q1. What does “fork resolution” mean in Bitcoin?**
A) The mechanism by which the network chooses one branch when two competing blocks exist
B) A software update process C) A way to create new cryptocurrencies D) A method for increasing block size

# Quiz Questions 1–5

**Q1. What does “fork resolution” mean in Bitcoin?**
A) The mechanism by which the network chooses one branch when two competing blocks exist
B) A software update process C) A way to create new cryptocurrencies D) A method for increasing block size
**Answer: A** – When two miners find valid blocks simultaneously, the network converges on the chain with the most cumulative work.

**Q2. What is an “orphaned” (stale) block in Bitcoin?**
A) A block with no transactions B) A block mined by a solo miner
C) A valid block that lost the chain selection competition and was abandoned D) A block that exceeds the size limit

# Quiz Questions 1–5

**Q1. What does “fork resolution” mean in Bitcoin?**
A) The mechanism by which the network chooses one branch when two competing blocks exist
B) A software update process C) A way to create new cryptocurrencies D) A method for increasing block size
**Answer: A** – When two miners find valid blocks simultaneously, the network converges on the chain with the most cumulative work.

**Q2. What is an “orphaned” (stale) block in Bitcoin?**
A) A block with no transactions B) A block mined by a solo miner
C) A valid block that lost the chain selection competition and was abandoned D) A block that exceeds the size limit
**Answer: C** – Orphaned blocks are valid but discarded when another chain accumulates more cumulative work.

**Q3. What does Bitcoin’s “cumulative work” measure?**
A) The number of transactions processed B) The total computational effort invested in mining all blocks in a chain
C) The number of active nodes D) The total BTC in circulation

# Quiz Questions 1–5

**Q1. What does “fork resolution” mean in Bitcoin?**
A) The mechanism by which the network chooses one branch when two competing blocks exist
B) A software update process C) A way to create new cryptocurrencies D) A method for increasing block size
**Answer: A** – When two miners find valid blocks simultaneously, the network converges on the chain with the most cumulative work.

**Q2. What is an “orphaned” (stale) block in Bitcoin?**
A) A block with no transactions B) A block mined by a solo miner
C) A valid block that lost the chain selection competition and was abandoned D) A block that exceeds the size limit
**Answer: C** – Orphaned blocks are valid but discarded when another chain accumulates more cumulative work.

**Q3. What does Bitcoin’s “cumulative work” measure?**
A) The number of transactions processed B) The total computational effort invested in mining all blocks in a chain
C) The number of active nodes D) The total BTC in circulation
**Answer: B** – Cumulative work sums the expected hashes required for every block; it is the true chain selection criterion.

**Q4. How often do natural forks typically occur on the Bitcoin network?**
A) Every block B) Once per year C) They have never occurred D) Approximately once every 1–2 weeks

# Quiz Questions 1–5

**Q1. What does "fork resolution" mean in Bitcoin?**
A) The mechanism by which the network chooses one branch when two competing blocks exist
B) A software update process C) A way to create new cryptocurrencies D) A method for increasing block size
**Answer: A** – When two miners find valid blocks simultaneously, the network converges on the chain with the most cumulative work.

**Q2. What is an "orphaned" (stale) block in Bitcoin?**
A) A block with no transactions B) A block mined by a solo miner
C) A valid block that lost the chain selection competition and was abandoned D) A block that exceeds the size limit
**Answer: C** – Orphaned blocks are valid but discarded when another chain accumulates more cumulative work.

**Q3. What does Bitcoin's "cumulative work" measure?**
A) The number of transactions processed B) The total computational effort invested in mining all blocks in a chain
C) The number of active nodes D) The total BTC in circulation
**Answer: B** – Cumulative work sums the expected hashes required for every block; it is the true chain selection criterion.

**Q4. How often do natural forks typically occur on the Bitcoin network?**
A) Every block B) Once per year C) They have never occurred D) Approximately once every 1–2 weeks
**Answer: D** – Propagation delays occasionally cause two valid blocks to be found near-simultaneously, creating brief forks.

**Q5. A miner discovers a valid block but it takes 12 seconds to propagate. Another miner also finds a valid block during that window. What is the immediate result?**
A) Both blocks are rejected B) The network experiences a temporary fork with two competing chain tips
C) The second block is automatically invalid D) Nodes shut down until the conflict is resolved

# Quiz Questions 1–5

**Q1. What does "fork resolution" mean in Bitcoin?**
A) The mechanism by which the network chooses one branch when two competing blocks exist
B) A software update process C) A way to create new cryptocurrencies D) A method for increasing block size
**Answer: A** – When two miners find valid blocks simultaneously, the network converges on the chain with the most cumulative work.

**Q2. What is an "orphaned" (stale) block in Bitcoin?**
A) A block with no transactions B) A block mined by a solo miner
C) A valid block that lost the chain selection competition and was abandoned D) A block that exceeds the size limit
**Answer: C** – Orphaned blocks are valid but discarded when another chain accumulates more cumulative work.

**Q3. What does Bitcoin's "cumulative work" measure?**
A) The number of transactions processed B) The total computational effort invested in mining all blocks in a chain
C) The number of active nodes D) The total BTC in circulation
**Answer: B** – Cumulative work sums the expected hashes required for every block; it is the true chain selection criterion.

**Q4. How often do natural forks typically occur on the Bitcoin network?**
A) Every block B) Once per year C) They have never occurred D) Approximately once every 1–2 weeks
**Answer: D** – Propagation delays occasionally cause two valid blocks to be found near-simultaneously, creating brief forks.

**Q5. A miner discovers a valid block but it takes 12 seconds to propagate. Another miner also finds a valid block during that window. What is the immediate result?**
A) Both blocks are rejected B) The network experiences a temporary fork with two competing chain tips
C) The second block is automatically invalid D) Nodes shut down until the conflict is resolved
**Answer: B** – Both blocks are locally valid; nodes hold whichever they saw first until one chain extends and wins.

# Quiz Questions 6–10

**Q6. An online retailer sells a $200 item and wants less than 0.1% reversal risk against a 10% attacker. How many confirmations are needed?**
A) 1 confirmation B) 12 confirmations C) 3 confirmations D) 6 confirmations

# Quiz Questions 6–10

**Q6. An online retailer sells a $200 item and wants less than 0.1% reversal risk against a 10% attacker. How many confirmations are needed?**
A) 1 confirmation B) 12 confirmations C) 3 confirmations D) 6 confirmations
**Answer: C** – Nakamoto's formula shows 3 confirmations reduces reversal probability below 0.1% against a 10% attacker.

**Q7. A node receives Block X from Miner A. Ten seconds later, competing Block Y arrives at the same height. What does the node do?**
A) Replace Block X with Block Y B) Forward both to the network
C) Shut down and restart D) Keep Block X (first-seen) and reject Block Y unless Y's chain later accumulates more work

# Quiz Questions 6–10

**Q6. An online retailer sells a $200 item and wants less than 0.1% reversal risk against a 10% attacker. How many confirmations are needed?**
A) 1 confirmation B) 12 confirmations C) 3 confirmations D) 6 confirmations
**Answer: C** – Nakamoto's formula shows 3 confirmations reduces reversal probability below 0.1% against a 10% attacker.

**Q7. A node receives Block X from Miner A. Ten seconds later, competing Block Y arrives at the same height. What does the node do?**
A) Replace Block X with Block Y B) Forward both to the network
C) Shut down and restart D) Keep Block X (first-seen) and reject Block Y unless Y's chain later accumulates more work
**Answer: D** – Nodes apply the first-seen rule locally but switch if a competing chain grows longer (more cumulative work).

**Q8. Chain A: 10 blocks, difficulty 100 each. Chain B: 8 blocks, difficulty 150 each. Which chain does Bitcoin select?**
A) Chain B (cumulative work 1,200 $>$ 1,000) B) Chain A (10 blocks $>$ 8 blocks)
C) Whichever was created first D) Neither — a tie requires manual resolution

# Quiz Questions 6–10

**Q6. An online retailer sells a $200 item and wants less than 0.1% reversal risk against a 10% attacker. How many confirmations are needed?**
A) 1 confirmation B) 12 confirmations C) 3 confirmations D) 6 confirmations
**Answer: C** – Nakamoto's formula shows 3 confirmations reduces reversal probability below 0.1% against a 10% attacker.

**Q7. A node receives Block X from Miner A. Ten seconds later, competing Block Y arrives at the same height. What does the node do?**
A) Replace Block X with Block Y B) Forward both to the network
C) Shut down and restart D) Keep Block X (first-seen) and reject Block Y unless Y's chain later accumulates more work
**Answer: D** – Nodes apply the first-seen rule locally but switch if a competing chain grows longer (more cumulative work).

**Q8. Chain A: 10 blocks, difficulty 100 each. Chain B: 8 blocks, difficulty 150 each. Which chain does Bitcoin select?**
A) Chain B (cumulative work $1{,}200 > 1{,}000$) B) Chain A (10 blocks $>$ 8 blocks)
C) Whichever was created first D) Neither — a tie requires manual resolution
**Answer: A** – Bitcoin selects by cumulative work, not block count: $8 \times 150 = 1{,}200 > 10 \times 100 = 1{,}000$.

**Q9. After a fork resolves, a transaction from the orphaned block does NOT appear in the winning chain. What is the most likely explanation?**
A) The transaction was permanently destroyed B) A conflicting transaction was already in the winning chain
C) The mempool deleted it D) The transaction fee was too low

# Quiz Questions 6–10

**Q6. An online retailer sells a $200 item and wants less than 0.1% reversal risk against a 10% attacker. How many confirmations are needed?**
A) 1 confirmation B) 12 confirmations C) 3 confirmations D) 6 confirmations
**Answer: C** – Nakamoto's formula shows 3 confirmations reduces reversal probability below 0.1% against a 10% attacker.

**Q7. A node receives Block X from Miner A. Ten seconds later, competing Block Y arrives at the same height. What does the node do?**
A) Replace Block X with Block Y B) Forward both to the network
C) Shut down and restart D) Keep Block X (first-seen) and reject Block Y unless Y's chain later accumulates more work
**Answer: D** – Nodes apply the first-seen rule locally but switch if a competing chain grows longer (more cumulative work).

**Q8. Chain A: 10 blocks, difficulty 100 each. Chain B: 8 blocks, difficulty 150 each. Which chain does Bitcoin select?**
A) Chain B (cumulative work $1{,}200 > 1{,}000$) B) Chain A (10 blocks $>$ 8 blocks)
C) Whichever was created first D) Neither — a tie requires manual resolution
**Answer: A** – Bitcoin selects by cumulative work, not block count: $8 \times 150 = 1{,}200 > 10 \times 100 = 1{,}000$.

**Q9. After a fork resolves, a transaction from the orphaned block does NOT appear in the winning chain. What is the most likely explanation?**
A) The transaction was permanently destroyed B) A conflicting transaction was already in the winning chain
C) The mempool deleted it D) The transaction fee was too low
**Answer: B** – Orphaned-block transactions return to the mempool, but a double-spend in the winning chain prevents re-inclusion.

**Q10. Bitcoin's difficulty adjusts every 2,016 blocks. If miners double hash power, what happens to cumulative work per block after adjustment?**
A) It doubles B) It halves C) It becomes unpredictable
D) It stays the same — difficulty increases to maintain block interval, each block represents more work

# Quiz Questions 6–10

**Q6. An online retailer sells a $200 item and wants less than 0.1% reversal risk against a 10% attacker. How many confirmations are needed?**
A) 1 confirmation B) 12 confirmations C) 3 confirmations D) 6 confirmations
**Answer: C** – Nakamoto's formula shows 3 confirmations reduces reversal probability below 0.1% against a 10% attacker.

**Q7. A node receives Block X from Miner A. Ten seconds later, competing Block Y arrives at the same height. What does the node do?**
A) Replace Block X with Block Y B) Forward both to the network
C) Shut down and restart D) Keep Block X (first-seen) and reject Block Y unless Y's chain later accumulates more work
**Answer: D** – Nodes apply the first-seen rule locally but switch if a competing chain grows longer (more cumulative work).

**Q8. Chain A: 10 blocks, difficulty 100 each. Chain B: 8 blocks, difficulty 150 each. Which chain does Bitcoin select?**
A) Chain B (cumulative work $1{,}200 > 1{,}000$) B) Chain A (10 blocks $>$ 8 blocks)
C) Whichever was created first D) Neither — a tie requires manual resolution
**Answer: A** – Bitcoin selects by cumulative work, not block count: $8 \times 150 = 1{,}200 > 10 \times 100 = 1{,}000$.

**Q9. After a fork resolves, a transaction from the orphaned block does NOT appear in the winning chain. What is the most likely explanation?**
A) The transaction was permanently destroyed B) A conflicting transaction was already in the winning chain
C) The mempool deleted it D) The transaction fee was too low
**Answer: B** – Orphaned-block transactions return to the mempool, but a double-spend in the winning chain prevents re-inclusion.

**Q10. Bitcoin's difficulty adjusts every 2,016 blocks. If miners double hash power, what happens to cumulative work per block after adjustment?**
A) It doubles B) It halves C) It becomes unpredictable
D) It stays the same — difficulty increases to maintain block interval, each block represents more work
**Answer: D** – Difficulty rises to keep block time at 10 minutes; cumulative work per block is unchanged at target.

# Quiz Questions 11–15

**Q11. A Bitcoin ATM processes $50 purchases with 0 confirmations. A customer attempts a double-spend. Why is this economically irrational?**
A) The protocol prevents all double-spends B) ATMs are exempt from double-spends
C) The cost of the attack far exceeds the $50 value D) Zero-confirmation transactions cannot be reversed

# Quiz Questions 11–15

**Q11. A Bitcoin ATM processes $50 purchases with 0 confirmations. A customer attempts a double-spend. Why is this economically irrational?**
A) The protocol prevents all double-spends B) ATMs are exempt from double-spends
C) The cost of the attack far exceeds the $50 value D) Zero-confirmation transactions cannot be reversed
**Answer: C** – Mining hardware, electricity, and risk of detection far outweigh a $50 gain; the incentives deter attack.

**Q12. Compact Blocks (BIP 152) reduces propagation time from seconds to milliseconds. How does this affect fork rates?**
A) Fewer forks — shorter propagation window reduces the chance of simultaneous discoveries
B) No effect — forks are random C) More forks — faster propagation confuses nodes
D) Eliminates all forks permanently

# Quiz Questions 11–15

**Q11. A Bitcoin ATM processes $50 purchases with 0 confirmations. A customer attempts a double-spend. Why is this economically irrational?**
A) The protocol prevents all double-spends B) ATMs are exempt from double-spends
C) The cost of the attack far exceeds the $50 value D) Zero-confirmation transactions cannot be reversed
**Answer: C** – Mining hardware, electricity, and risk of detection far outweigh a $50 gain; the incentives deter attack.

**Q12. Compact Blocks (BIP 152) reduces propagation time from seconds to milliseconds. How does this affect fork rates?**
A) Fewer forks — shorter propagation window reduces the chance of simultaneous discoveries
B) No effect — forks are random C) More forks — faster propagation confuses nodes
D) Eliminates all forks permanently
**Answer: A** – Faster block relay shrinks the window in which two valid blocks can coexist, reducing fork probability.

**Q13. Bitcoin's whitepaper says "longest chain" but the code implements "most cumulative work." When do they differ?**
A) They always agree B) Only during software upgrades
C) When competing chains have blocks mined at different difficulty levels D) Only when the mempool is full

# Quiz Questions 11–15

**Q11. A Bitcoin ATM processes $50 purchases with 0 confirmations. A customer attempts a double-spend. Why is this economically irrational?**
A) The protocol prevents all double-spends B) ATMs are exempt from double-spends
C) The cost of the attack far exceeds the $50 value D) Zero-confirmation transactions cannot be reversed
**Answer: C** – Mining hardware, electricity, and risk of detection far outweigh a $50 gain; the incentives deter attack.

**Q12. Compact Blocks (BIP 152) reduces propagation time from seconds to milliseconds. How does this affect fork rates?**
A) Fewer forks — shorter propagation window reduces the chance of simultaneous discoveries
B) No effect — forks are random C) More forks — faster propagation confuses nodes
D) Eliminates all forks permanently
**Answer: A** – Faster block relay shrinks the window in which two valid blocks can coexist, reducing fork probability.

**Q13. Bitcoin's whitepaper says "longest chain" but the code implements "most cumulative work." When do they differ?**
A) They always agree B) Only during software upgrades
C) When competing chains have blocks mined at different difficulty levels D) Only when the mempool is full
**Answer: C** – Block count and cumulative work agree only when all blocks share identical difficulty; variable difficulty breaks this equivalence.

**Q14. GHash.io briefly exceeded 50% of Bitcoin's hash power in 2014 but did not attack the network. Why?**
A) The protocol prevented any attack B) They were unaware of their hash power share
C) The government was monitoring them
D) An attack would crash Bitcoin's price, destroying the value of their own mining rewards and held BTC

# Quiz Questions 11–15

**Q11. A Bitcoin ATM processes $50 purchases with 0 confirmations. A customer attempts a double-spend. Why is this economically irrational?**
A) The protocol prevents all double-spends B) ATMs are exempt from double-spends
C) The cost of the attack far exceeds the $50 value D) Zero-confirmation transactions cannot be reversed
**Answer: C** – Mining hardware, electricity, and risk of detection far outweigh a $50 gain; the incentives deter attack.

**Q12. Compact Blocks (BIP 152) reduces propagation time from seconds to milliseconds. How does this affect fork rates?**
A) Fewer forks — shorter propagation window reduces the chance of simultaneous discoveries
B) No effect — forks are random C) More forks — faster propagation confuses nodes
D) Eliminates all forks permanently
**Answer: A** – Faster block relay shrinks the window in which two valid blocks can coexist, reducing fork probability.

**Q13. Bitcoin's whitepaper says "longest chain" but the code implements "most cumulative work." When do they differ?**
A) They always agree B) Only during software upgrades
C) When competing chains have blocks mined at different difficulty levels D) Only when the mempool is full
**Answer: C** – Block count and cumulative work agree only when all blocks share identical difficulty; variable difficulty breaks this equivalence.

**Q14. GHash.io briefly exceeded 50% of Bitcoin's hash power in 2014 but did not attack the network. Why?**
A) The protocol prevented any attack B) They were unaware of their hash power share
C) The government was monitoring them
D) An attack would crash Bitcoin's price, destroying the value of their own mining rewards and held BTC
**Answer: D** – A successful 51% attack destroys confidence in Bitcoin, collapsing the very asset the attacker mines and holds.

**Q15. The 2010 Value Overflow bug created 184 billion BTC. The community released a fix and built a competing chain. What type of consensus resolved this?**
A) Proof of Work consensus only B) Social consensus overriding protocol rules
C) Proof of Stake consensus D) Automatic protocol self-healing

# Quiz Questions 11–15

**Q11. A Bitcoin ATM processes $50 purchases with 0 confirmations. A customer attempts a double-spend. Why is this economically irrational?**
A) The protocol prevents all double-spends B) ATMs are exempt from double-spends
C) The cost of the attack far exceeds the $50 value D) Zero-confirmation transactions cannot be reversed
**Answer: C** – Mining hardware, electricity, and risk of detection far outweigh a $50 gain; the incentives deter attack.

**Q12. Compact Blocks (BIP 152) reduces propagation time from seconds to milliseconds. How does this affect fork rates?**
A) Fewer forks — shorter propagation window reduces the chance of simultaneous discoveries
B) No effect — forks are random C) More forks — faster propagation confuses nodes
D) Eliminates all forks permanently
**Answer: A** – Faster block relay shrinks the window in which two valid blocks can coexist, reducing fork probability.

**Q13. Bitcoin's whitepaper says "longest chain" but the code implements "most cumulative work." When do they differ?**
A) They always agree B) Only during software upgrades
C) When competing chains have blocks mined at different difficulty levels D) Only when the mempool is full
**Answer: C** – Block count and cumulative work agree only when all blocks share identical difficulty; variable difficulty breaks this equivalence.

**Q14. GHash.io briefly exceeded 50% of Bitcoin's hash power in 2014 but did not attack the network. Why?**
A) The protocol prevented any attack B) They were unaware of their hash power share
C) The government was monitoring them
D) An attack would crash Bitcoin's price, destroying the value of their own mining rewards and held BTC
**Answer: D** – A successful 51% attack destroys confidence in Bitcoin, collapsing the very asset the attacker mines and holds.

**Q15. The 2010 Value Overflow bug created 184 billion BTC. The community released a fix and built a competing chain. What type of consensus resolved this?**
A) Proof of Work consensus only B) Social consensus overriding protocol rules
C) Proof of Stake consensus D) Automatic protocol self-healing
**Answer: B** – Nodes chose to upgrade and follow the patched chain, demonstrating that social consensus underlies the technical layer.

# Quiz Questions 16–20

**Q16. A blockchain with 2-second blocks has a 15% fork rate vs Bitcoin's 0.3%. What causes the difference?**
A) The difference is coincidental B) The 2-second chain has weaker cryptography
C) Shorter block times mean propagation delay is a much larger fraction of block interval D) Bitcoin has more nodes

# Quiz Questions 16–20

**Q16. A blockchain with 2-second blocks has a 15% fork rate vs Bitcoin's 0.3%. What causes the difference?**
A) The difference is coincidental B) The 2-second chain has weaker cryptography
C) Shorter block times mean propagation delay is a much larger fraction of block interval D) Bitcoin has more nodes
**Answer: C** – If propagation takes 1 second and block time is 2 seconds, a 50% overlap chance exists vs. $<1\%$ at 10 minutes.

**Q17. Why do exchanges require different confirmation counts (e.g., Coinbase 3, Kraken 4, Binance 1)?**
A) They use different blockchains B) Regulatory requirements differ by jurisdiction
C) Technical limitations of their software
D) Each makes its own risk-reward calculation based on typical deposit values and attacker assumptions

# Quiz Questions 16–20

**Q16. A blockchain with 2-second blocks has a 15% fork rate vs Bitcoin's 0.3%. What causes the difference?**
A) The difference is coincidental B) The 2-second chain has weaker cryptography
C) Shorter block times mean propagation delay is a much larger fraction of block interval D) Bitcoin has more nodes
**Answer: C** – If propagation takes 1 second and block time is 2 seconds, a 50% overlap chance exists vs. $<1\%$ at 10 minutes.

**Q17. Why do exchanges require different confirmation counts (e.g., Coinbase 3, Kraken 4, Binance 1)?**
A) They use different blockchains B) Regulatory requirements differ by jurisdiction
C) Technical limitations of their software
D) Each makes its own risk-reward calculation based on typical deposit values and attacker assumptions
**Answer: D** – Confirmation thresholds are business decisions: higher-value deposits or lower risk tolerance require more confirmations.

**Q18. In Nakamoto's formula, what happens as attacker hash power $q$ approaches 50%?**
A) The required confirmations drop to zero B) Confirmations needed increase dramatically as attacker's rate approaches honest rate
C) Nothing changes D) The formula becomes undefined

# Quiz Questions 16–20

**Q16. A blockchain with 2-second blocks has a 15% fork rate vs Bitcoin's 0.3%. What causes the difference?**
A) The difference is coincidental B) The 2-second chain has weaker cryptography
C) Shorter block times mean propagation delay is a much larger fraction of block interval D) Bitcoin has more nodes
**Answer: C** – If propagation takes 1 second and block time is 2 seconds, a 50% overlap chance exists vs. $<1\%$ at 10 minutes.

**Q17. Why do exchanges require different confirmation counts (e.g., Coinbase 3, Kraken 4, Binance 1)?**
A) They use different blockchains B) Regulatory requirements differ by jurisdiction
C) Technical limitations of their software
D) Each makes its own risk-reward calculation based on typical deposit values and attacker assumptions
**Answer: D** – Confirmation thresholds are business decisions: higher-value deposits or lower risk tolerance require more confirmations.

**Q18. In Nakamoto's formula, what happens as attacker hash power $q$ approaches 50%?**
A) The required confirmations drop to zero B) Confirmations needed increase dramatically as attacker's rate approaches honest rate
C) Nothing changes D) The formula becomes undefined
**Answer: B** – Near 50%, the attacker can almost keep pace with the honest chain; exponentially more confirmations are needed.

**Q19. Bitcoin's $15B/year mining cost is called "wasteful." What is the strongest economic counter-argument?**
A) This is the cost of providing trustless, censorship-resistant finality for a $1.8T network
B) Energy comes entirely from renewables C) Banks waste more energy D) Mining energy decreases over time

# Quiz Questions 16–20

**Q16. A blockchain with 2-second blocks has a 15% fork rate vs Bitcoin's 0.3%. What causes the difference?**
A) The difference is coincidental B) The 2-second chain has weaker cryptography
C) Shorter block times mean propagation delay is a much larger fraction of block interval D) Bitcoin has more nodes
**Answer: C** – If propagation takes 1 second and block time is 2 seconds, a 50% overlap chance exists vs. $<1\%$ at 10 minutes.

**Q17. Why do exchanges require different confirmation counts (e.g., Coinbase 3, Kraken 4, Binance 1)?**
A) They use different blockchains B) Regulatory requirements differ by jurisdiction
C) Technical limitations of their software
D) Each makes its own risk-reward calculation based on typical deposit values and attacker assumptions
**Answer: D** – Confirmation thresholds are business decisions: higher-value deposits or lower risk tolerance require more confirmations.

**Q18. In Nakamoto's formula, what happens as attacker hash power $q$ approaches 50%?**
A) The required confirmations drop to zero B) Confirmations needed increase dramatically as attacker's rate approaches honest rate
C) Nothing changes D) The formula becomes undefined
**Answer: B** – Near 50%, the attacker can almost keep pace with the honest chain; exponentially more confirmations are needed.

**Q19. Bitcoin's $15B/year mining cost is called "wasteful." What is the strongest economic counter-argument?**
A) This is the cost of providing trustless, censorship-resistant finality for a $1.8T network
B) Energy comes entirely from renewables C) Banks waste more energy D) Mining energy decreases over time
**Answer: A** – Security spend should be evaluated relative to the value secured; $15B protects a $1.8T asset with no trusted third party.

**Q20. A proposal replaces "most cumulative work" with "most cumulative coin-days-destroyed." What is the strongest objection?**
A) It is mathematically impossible B) Nobody has proposed this
C) It would make mining faster
D) Shifting to an in-protocol metric manipulable by large holders undermines the physical-cost security guarantee

# Quiz Questions 16–20

**Q16. A blockchain with 2-second blocks has a 15% fork rate vs Bitcoin's 0.3%. What causes the difference?**
A) The difference is coincidental B) The 2-second chain has weaker cryptography
C) Shorter block times mean propagation delay is a much larger fraction of block interval D) Bitcoin has more nodes
**Answer: C** – If propagation takes 1 second and block time is 2 seconds, a 50% overlap chance exists vs. $<1\%$ at 10 minutes.

**Q17. Why do exchanges require different confirmation counts (e.g., Coinbase 3, Kraken 4, Binance 1)?**
A) They use different blockchains B) Regulatory requirements differ by jurisdiction
C) Technical limitations of their software
D) Each makes its own risk-reward calculation based on typical deposit values and attacker assumptions
**Answer: D** – Confirmation thresholds are business decisions: higher-value deposits or lower risk tolerance require more confirmations.

**Q18. In Nakamoto's formula, what happens as attacker hash power $q$ approaches 50%?**
A) The required confirmations drop to zero B) Confirmations needed increase dramatically as attacker's rate approaches honest rate
C) Nothing changes D) The formula becomes undefined
**Answer: B** – Near 50%, the attacker can almost keep pace with the honest chain; exponentially more confirmations are needed.

**Q19. Bitcoin's $15B/year mining cost is called "wasteful." What is the strongest economic counter-argument?**
A) This is the cost of providing trustless, censorship-resistant finality for a $1.8T network
B) Energy comes entirely from renewables C) Banks waste more energy D) Mining energy decreases over time
**Answer: A** – Security spend should be evaluated relative to the value secured; $15B protects a $1.8T asset with no trusted third party.

**Q20. A proposal replaces "most cumulative work" with "most cumulative coin-days-destroyed." What is the strongest objection?**
A) It is mathematically impossible B) Nobody has proposed this
C) It would make mining faster
D) Shifting to an in-protocol metric manipulable by large holders undermines the physical-cost security guarantee
**Answer: D** – Physical energy cost is exogenous and unfakeable; coin-days-destroyed can be gamed by wealthy insiders at low marginal cost.