Quiz: What is Blockchain

Instructions: 23 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates all subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the transaction fee B) Spending the same digital asset twice C) Mining two blocks D) Sending to wrong address

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates all subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the transaction fee B) Spending the same digital asset twice C) Mining two blocks D) Sending to wrong address
Answer: B – Digital files can be copied; blockchain prevents spending same coins twice via consensus.

Q3. What is the verification complexity using a Merkle proof?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates all subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the transaction fee B) Spending the same digital asset twice C) Mining two blocks D) Sending to wrong address
Answer: B – Digital files can be copied; blockchain prevents spending same coins twice via consensus.

Q3. What is the verification complexity using a Merkle proof?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q4. Which network type does blockchain represent?
A) Centralized B) Decentralized C) Distributed D) Hierarchical

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates all subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the transaction fee B) Spending the same digital asset twice C) Mining two blocks D) Sending to wrong address
Answer: B – Digital files can be copied; blockchain prevents spending same coins twice via consensus.

Q3. What is the verification complexity using a Merkle proof?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q4. Which network type does blockchain represent?
A) Centralized B) Decentralized C) Distributed D) Hierarchical
Answer: C – Blockchain is distributed: no central authority, all nodes equal, cryptographic trust.

Q5. The Bitcoin whitepaper was published in:
A) 1991 B) 2001 C) 2008 D) 2015

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates all subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the transaction fee B) Spending the same digital asset twice C) Mining two blocks D) Sending to wrong address
Answer: B – Digital files can be copied; blockchain prevents spending same coins twice via consensus.

Q3. What is the verification complexity using a Merkle proof?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q4. Which network type does blockchain represent?
A) Centralized B) Decentralized C) Distributed D) Hierarchical
Answer: C – Blockchain is distributed: no central authority, all nodes equal, cryptographic trust.

Q5. The Bitcoin whitepaper was published in:
A) 1991 B) 2001 C) 2008 D) 2015
Answer: C – Satoshi Nakamoto published the Bitcoin whitepaper in October 2008.

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed
Answer: B – Collision resistance: $\Pr[H(x) = H(y), x \neq y] \approx 2^{-128}$.

Q7. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency, efficiency D) Mining, staking, governance

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed
Answer: B – Collision resistance: $\Pr[H(x) = H(y), x \neq y] \approx 2^{-128}$.

Q7. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency, efficiency D) Mining, staking, governance
Answer: B – Trilemma: cannot optimize all three simultaneously.

Q8. How many confirmations typically provide $< 0.1\%$ reversal probability?
A) 1 B) 3 C) 6 D) 100

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed
Answer: B – Collision resistance: $\Pr[H(x) = H(y), x \neq y] \approx 2^{-128}$.

Q7. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency, efficiency D) Mining, staking, governance
Answer: B – Trilemma: cannot optimize all three simultaneously.

Q8. How many confirmations typically provide $< 0.1\%$ reversal probability?
A) 1 B) 3 C) 6 D) 100
Answer: C – 6 confirmations give reversal probability $< 0.1\%$ for attacker with $q = 0.3$ hashrate.

Q9. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed
Answer: B – Collision resistance: $\Pr[H(x) = H(y), x \neq y] \approx 2^{-128}$.

Q7. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency, efficiency D) Mining, staking, governance
Answer: B – Trilemma: cannot optimize all three simultaneously.

Q8. How many confirmations typically provide $< 0.1\%$ reversal probability?
A) 1 B) 3 C) 6 D) 100
Answer: C – 6 confirmations give reversal probability $< 0.1\%$ for attacker with $q = 0.3$ hashrate.

Q9. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB
Answer: B – Bitcoin block header is exactly 80 bytes containing metadata.

Q10. The avalanche effect means:
A) Hash output grows exponentially B) 1-bit input change flips 50% of output bits C) Blocks cascade faster D) Network congestion increases

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed
Answer: B – Collision resistance: $\Pr[H(x) = H(y), x \neq y] \approx 2^{-128}$.

Q7. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency, efficiency D) Mining, staking, governance
Answer: B – Trilemma: cannot optimize all three simultaneously.

Q8. How many confirmations typically provide $< 0.1\%$ reversal probability?
A) 1 B) 3 C) 6 D) 100
Answer: C – 6 confirmations give reversal probability $< 0.1\%$ for attacker with $q = 0.3$ hashrate.

Q9. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB
Answer: B – Bitcoin block header is exactly 80 bytes containing metadata.

Q10. The avalanche effect means:
A) Hash output grows exponentially B) 1-bit input change flips 50% of output bits C) Blocks cascade faster D) Network congestion increases
Answer: B – Avalanche: small input change causes large, unpredictable output change.

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q12. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory database C) Supply chain provenance D) Decentralized identity

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q12. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory database C) Supply chain provenance D) Decentralized identity
Answer: B – Single organization control makes blockchain unnecessary; use traditional DB.

Q13. The integrity constraint $B_i.\textbf{prev} = H(B_{i-1})$ ensures:
A) Faster processing B) Each block links to its predecessor cryptographically C) Blocks can be deleted D) Transactions are encrypted

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q12. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory database C) Supply chain provenance D) Decentralized identity
Answer: B – Single organization control makes blockchain unnecessary; use traditional DB.

Q13. The integrity constraint $B_i.\textbf{prev} = H(B_{i-1})$ ensures:
A) Faster processing B) Each block links to its predecessor cryptographically C) Blocks can be deleted D) Transactions are encrypted
Answer: B – Hash pointer links blocks, making tampering detectable.

Q14. Current Bitcoin network hash rate (2024) is approximately:
A) 1 TH/s B) 100 PH/s C) 1,200 EH/s D) 1 ZH/s

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q12. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory database C) Supply chain provenance D) Decentralized identity
Answer: B – Single organization control makes blockchain unnecessary; use traditional DB.

Q13. The integrity constraint $B_i.\textbf{prev} = H(B_{i-1})$ ensures:
A) Faster processing B) Each block links to its predecessor cryptographically C) Blocks can be deleted D) Transactions are encrypted
Answer: B – Hash pointer links blocks, making tampering detectable.

Q14. Current Bitcoin network hash rate (2024) is approximately:
A) 1 TH/s B) 100 PH/s C) 1,200 EH/s D) 1 ZH/s
Answer: C – Bitcoin hash rate reached 1,200 EH/s (1.2×10^{21} hashes/sec).

Q15. SPV (Simplified Payment Verification) clients use:
A) Full blockchain B) Merkle proofs C) Trusted servers only D) No verification

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q12. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory database C) Supply chain provenance D) Decentralized identity
Answer: B – Single organization control makes blockchain unnecessary; use traditional DB.

Q13. The integrity constraint $B_i.\textbf{prev} = H(B_{i-1})$ ensures:
A) Faster processing B) Each block links to its predecessor cryptographically C) Blocks can be deleted D) Transactions are encrypted
Answer: B – Hash pointer links blocks, making tampering detectable.

Q14. Current Bitcoin network hash rate (2024) is approximately:
A) 1 TH/s B) 100 PH/s C) 1,200 EH/s D) 1 ZH/s
Answer: C – Bitcoin hash rate reached 1,200 EH/s (1.2×10^{21} hashes/sec).

Q15. SPV (Simplified Payment Verification) clients use:
A) Full blockchain B) Merkle proofs C) Trusted servers only D) No verification
Answer: B – SPV clients verify transactions using Merkle proofs without full chain.

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption
Answer: B – Distributed: no hubs/hierarchy; Decentralized: multiple hubs but still hierarchy.

Q17. The Merkle root in a Bitcoin block header commits to:
A) Previous block only B) All transactions in the block C) Mining difficulty D) Network nodes

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption
Answer: B – Distributed: no hubs/hierarchy; Decentralized: multiple hubs but still hierarchy.

Q17. The Merkle root in a Bitcoin block header commits to:
A) Previous block only B) All transactions in the block C) Mining difficulty D) Network nodes
Answer: B – 32-byte Merkle root is cryptographic commitment to all block transactions.

Q18. Bitcoin ETFs reached what AUM by December 2024?
A) $1B B) $10B C) $129B D) $500B

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption
Answer: B – Distributed: no hubs/hierarchy; Decentralized: multiple hubs but still hierarchy.

Q17. The Merkle root in a Bitcoin block header commits to:
A) Previous block only B) All transactions in the block C) Mining difficulty D) Network nodes
Answer: B – 32-byte Merkle root is cryptographic commitment to all block transactions.

Q18. Bitcoin ETFs reached what AUM by December 2024?
A) \$1B B) \$10B C) \$129B D) \$500B
Answer: C – Bitcoin ETFs reached \$129B AUM, surpassing gold ETFs in Dec 2024.

Q19. To modify block B_k in a chain of n blocks, an attacker must:
A) Change only B_k B) Recompute hashes for all blocks after B_k C) Get permission D) Wait for consensus

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption
Answer: B – Distributed: no hubs/hierarchy; Decentralized: multiple hubs but still hierarchy.

Q17. The Merkle root in a Bitcoin block header commits to:
A) Previous block only B) All transactions in the block C) Mining difficulty D) Network nodes
Answer: B – 32-byte Merkle root is cryptographic commitment to all block transactions.

Q18. Bitcoin ETFs reached what AUM by December 2024?
A) \$1B B) \$10B C) \$129B D) \$500B
Answer: C – Bitcoin ETFs reached \$129B AUM, surpassing gold ETFs in Dec 2024.

Q19. To modify block B_k in a chain of n blocks, an attacker must:
A) Change only B_k B) Recompute hashes for all blocks after B_k C) Get permission D) Wait for consensus
Answer: B – Modifying B_k requires recomputing all $n - k$ subsequent block hashes.

Q20. The formula Value $\propto \frac{\text{Trust Deficit} \times \text{Coordination Benefit}}{\text{Performance Requirements}}$ suggests blockchain is best when:
A) Performance is critical B) Trust is high C) Trust deficit is high with coordination needs D) Single entity controls data

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption
Answer: B – Distributed: no hubs/hierarchy; Decentralized: multiple hubs but still hierarchy.

Q17. The Merkle root in a Bitcoin block header commits to:
A) Previous block only B) All transactions in the block C) Mining difficulty D) Network nodes
Answer: B – 32-byte Merkle root is cryptographic commitment to all block transactions.

Q18. Bitcoin ETFs reached what AUM by December 2024?
A) \$1B B) \$10B C) \$129B D) \$500B
Answer: C – Bitcoin ETFs reached \$129B AUM, surpassing gold ETFs in Dec 2024.

Q19. To modify block B_k in a chain of n blocks, an attacker must:
A) Change only B_k B) Recompute hashes for all blocks after B_k C) Get permission D) Wait for consensus
Answer: B – Modifying B_k requires recomputing all $n - k$ subsequent block hashes.

Q20. The formula Value $\propto \frac{\text{Trust Deficit} \times \text{Coordination Benefit}}{\text{Performance Requirements}}$ suggests blockchain is best when:
A) Performance is critical B) Trust is high C) Trust deficit is high with coordination needs D) Single entity controls data
Answer: C – Blockchain adds value when trust is lacking and coordination benefits are high.

Quiz (21–23)

Q21. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$

Quiz (21–23)

Q21. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q22. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests

Quiz (21–23)

Q21. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q22. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q23. The value formula suggests blockchain is best when:
A) Performance is critical B) Trust is high C) Trust deficit + coordination needs D) Single entity controls

Quiz (21–23)

Q21. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q22. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q23. The value formula suggests blockchain is best when:
A) Performance is critical B) Trust is high C) Trust deficit + coordination needs D) Single entity controls
Answer: C – Blockchain adds value when trust is lacking and coordination benefits are high.