MCQ Bank for Blockchain

🟥 **1.CS740_Introduction.pdf**
PDF

🟥 **8b004b4c-f2f0-48fc-87f0-00cac303c22f.pdf**
PDF

We have a class test tomorrow in which all questions will be 1 marks MCQs with negative marking the syllabus is these two ppts. Give me all possible questions that can be asked so that i could not make a single mistake in the paper

Great — since this is **1-mark MCQs with negative marking**, we must eliminate all possible conceptual traps.

Below is a **complete high-probability MCQ bank** covering everything from:

- 📄 PPT 1: Introduction to Blockchain 1.CS740_Introduction
- 📄 PPT 2: Crypto Primitives 8b004b4c-f2f0-48fc-87f0-00cac30…

I have structured this to match exactly your slides.

✅ SECTION 1: BLOCKCHAIN FUNDAMENTALS

1. What is a blockchain?

- Growing list of blocks linked using cryptographic hash
- Each block contains previous block hash, timestamp, transaction data

2. Blockchain is:

- A decentralized distributed ledger

3. Blockchain ensures:

- Tamper-proof
- Transparency
- Distributed consistency

4. Each block contains:

- Previous block hash
- Timestamp
- Transaction data

5. Blockchain resembles:

- Public ledger

6. Blockchain nodes:

- Maintain local copy of ledger
- Local copies must be identical

7. Centralized system disadvantage:

- Single point of failure

8. Decentralized system:

- Multiple coordinators
- Needs consensus
- Slower than centralized

9. Distributed system:

- Coordination distributed
- No single control point

✅ SECTION 2: TYPES OF BLOCKCHAIN

10. Public blockchain is:

- Permission-less
- Anyone can mine
- Anyone can verify

Examples:

- Bitcoin
- Ethereum
- Litecoin

11. Private blockchain:

- Permissioned
- Closed network
- Enterprise use

Examples:

- Hyperledger Fabric
- Sawtooth

- Corda

12. Consortium blockchain:

- Governed by group of organizations

13. Hybrid blockchain:

- Combination of public and private
- Example: Dragonchain

✅ SECTION 3: CRYPTOGRAPHIC HASH FUNCTIONS

(from both PPTs)

14. Hash function properties:

- Collision resistant
- Hiding
- Puzzle friendly

15. Output length in blockchain:

- 256-bit (SHA-256)

16. Avalanche effect:

- Small input change → large output change

17. Hash is:

- Deterministic
- Fixed-length output
- Many-to-one mapping

18. Collision resistance means:

- Hard to find m1 ≠m2 such that H(m1)=H(m2)

19. Birthday attack complexity:

- 2^(n/2)

For SHA-256:

- 2^128 operations

20. SHA:

- Developed by NIST
- SHA-1 → 160-bit
- SHA-256/384/512 introduced in FIPS 180-2
- Based on MD4

✅ SECTION 4: MERKLE TREE

21. Merkle tree:

- Binary tree of hashes
- Leaves = hash of data
- Internal nodes = hash of children

22. Root hash:

- Represents entire dataset

23. Verification complexity:

- O(log n)

24. Sorted Merkle tree:

- Can prove non-membership

25. Changing one transaction requires:

- Recomputing all upper hashes

✅ SECTION 5: BLOCK STRUCTURE

26. Block has:

- Block header
- Transaction list

27. Block header contains:

- Previous block hash
- Merkle root
- Timestamp
- Nonce
- Difficulty

28. Mining formula:

Hk = Hash(Hk−1 || T || Nonce)

29. Mining requires:

- Finding nonce
- Satisfying difficulty (leading zeros)

✅ SECTION 6: CONSENSUS

30. Distributed consensus ensures:

- All correct nodes decide same value
- Value proposed by correct node

31. Permission-less consensus uses:

- Challenge-response

32. Bitcoin consensus:

- Proof of Work (PoW)

33. PoW requirement:

- Computational effort

34. Incentive for miners:

- Cryptocurrency reward

✅ SECTION 7: BITCOIN SPECIFICS

35. Bitcoin is:

- Decentralized
- Peer-to-peer
- Permission-less

36. Inventor:

- Satoshi Nakamoto

37. Bitcoin block size limit:

- ~1 MB (as proposed)

38. Average transactions per block:

- ~500+

✅ SECTION 8: SMART CONTRACTS

39. Smart contract:

- Program running on blockchain
- Self-enforcing
- Tamper-proof

40. Introduced by:

- Nick Szabo (1994)

41. Bitcoin smart contracts:

- Turing incomplete

42. Ethereum:

- Turing complete smart contracts

43. Characteristics:

- Self-verifying
- Self-enforcing
- Tamper-proof

44. Advantages:

- No intermediary
- Faster
- Secure
- Paper-free

✅ SECTION 9: HASH POINTERS

45. Hash pointer stores:

- Address of data
- Hash of data

46. Used for:

- Tamper-evident logs

✅ SECTION 10: DIGITAL SIGNATURE

47. Digital signature ensures:

- Authentication
- Integrity
- Non-repudiation

48. Only signer can:

- Sign

49. Anyone can:

- Verify

50. Signature is:

- Document-specific
- Cannot be reused

✅ SECTION 11: SHA-256 DETAILS

51. Padding rule:

Append 1 → zeros → 64-bit length
Make total length divisible by 512

52. Block size of SHA-256:

- 512-bit block

53. Initial hash value:

- Fixed IV

54. Compression function:

- Applied iteratively

✅ HIGH-PROBABILITY TRICK MCQs

⚠️ These are commonly confused:

- Blockchain is NOT fully anonymous (it is pseudonymous)
- PoW does NOT guarantee fastest mining — it is probabilistic
- Merkle tree verification is NOT O(n) — it is O(log n)
- Collision resistance ≠ preimage resistance
- Birthday attack works in 2^(n/2), not 2^n
- Public blockchain is slower than private
- Smart contracts are immutable after deployment
- Hash functions are deterministic
- SHA-1 = 160-bit, not 256
- MD5 = 128-bit
- SHA developed by NIST, not RSA

🚀 If You Want 100% Safety

I can now:

- Create 150–200 practice MCQs (with tricky options)
- Give rapid-fire revision sheet
- Prepare 30 ultra-tricky negative-marking traps
- Make a last 10-minute crash revision sheet

Tell me how aggressive you want the practice to be 😄

Sources

> the questions will have 4 options, so generate me all those example questions (along with correct answer - only a single sentence explanation only if required otherwise not) which can be asked (i will study from the questions provided by you and want to score full marks)

Perfect. Below is a **high-coverage MCQ bank (4 options each)** from both PPTs 1.CS740_Introduction 8b004b4c-f2f0-48fc-87f0-00cac30… .

Each has the **correct answer marked**. Short explanation only when necessary.

🔹 BLOCKCHAIN BASICS

1. A blockchain is best described as:
A) Centralized database
B) Distributed ledger linked using cryptographic hashes

C) Encrypted file system
D) Cloud storage system
✅ **Answer: B**

---

2. Each block in a blockchain contains:
A) Previous block hash, timestamp, transaction data
B) Only transaction data
C) Public keys only
D) Only nonce
✅ **Answer: A**

---

3. Blockchain primarily prevents:
A) Network delay
B) Data tampering
C) Bandwidth usage
D) Encryption
✅ **Answer: B**

---

4. In a decentralized system:
A) One central coordinator
B) No coordination
C) Multiple coordinators
D) Offline operation
✅ **Answer: C**

---

5. Main disadvantage of centralized systems:
A) Slow speed
B) High cost
C) Single point of failure
D) Complex mining
✅ **Answer: C**

---

6. In blockchain, every node:
A) Maintains identical ledger copy
B) Maintains partial data
C) Stores only its own transactions
D) Stores encrypted blocks only
✅ **Answer: A**

🔹 TYPES OF BLOCKCHAIN

7. A permission-less blockchain allows:
A) Only authorized validators
B) Anyone to participate

C) Government access only
D) Limited mining
✅ **Answer: B**

---

8. Example of public blockchain:
A) Hyperledger Fabric
B) Bitcoin
C) Corda
D) Private ledger
✅ **Answer: B**

---

9. Private blockchain is mainly used for:
A) Anonymous payments
B) Enterprise collaboration
C) Illegal transactions
D) Open mining
✅ **Answer: B**

---

10. Consortium blockchain is governed by:
A) One company
B) Public miners
C) Group of organizations
D) Anonymous users
✅ **Answer: C**

🔹 HASH FUNCTIONS

11. SHA-256 produces output of:
A) 128 bits
B) 160 bits
C) 256 bits
D) 512 bits
✅ **Answer: C**

---

12. Collision resistance means:
A) Hard to compute hash
B) Hard to find two inputs with same hash
C) Hash is random
D) Hash is encrypted
✅ **Answer: B**

---

13. Birthday attack complexity on n-bit hash is:
A) 2^n
B) $2^n/2$

C) n^2

D) log n

✅ **Answer: B**

---

14. Avalanche effect means:

A) Large input causes large output

B) Small input change causes big output change

C) Hash decreases

D) Hash becomes reversible

✅ **Answer: B**

---

15. Hash functions are:

A) Reversible

B) Non-deterministic

C) Deterministic

D) Symmetric keys

✅ **Answer: C**

---

16. Hiding property ensures:

A) Hash collision

B) Preimage resistance

C) Blockchain speed

D) Fast mining

✅ **Answer: B**

---

17. Puzzle-friendly property is required for:

A) Encryption

B) Digital signature

C) Bitcoin mining

D) Private blockchain

✅ **Answer: C**

🔹 MERKLE TREE

18. In Merkle tree, leaf nodes store:

A) Raw public keys

B) Hash of data

C) Nonce

D) Timestamp

✅ **Answer: B**

---

19. Internal nodes in Merkle tree store:

A) Transaction

B) Nonce

C) Hash of children
D) Block height
✅ **Answer: C**

---

20. Membership verification in Merkle tree takes:
A) O(n)
B) O(1)
C) O(log n)
D) $O(n^2)$
✅ **Answer: C**

---

21. Changing one transaction affects:
A) Only that transaction
B) Entire chain forward
C) Nothing
D) Only Merkle root of same block
✅ **Answer: B**

🔹 BLOCK STRUCTURE

22. Bitcoin block consists of:
A) Header + Transactions
B) Only hash
C) Only signature
D) Only nonce
✅ **Answer: A**

---

23. Block header contains:
A) Previous hash
B) Merkle root
C) Timestamp
D) All of the above
✅ **Answer: D**

---

24. Mining requires finding:
A) Private key
B) Hash function
C) Nonce
D) Signature
✅ **Answer: C**

---

25. Mining difficulty controls:
A) Network size
B) Number of users

C) Number of leading zeros
D) Gas fees
✅ **Answer: C**

🔹 CONSENSUS

26. Proof of Work is based on:
A) Identity
B) Stake
C) Challenge-response
D) Voting
✅ **Answer: C**

27. In PoW, winner is the node that:
A) Has highest money
B) Solves puzzle first
C) Has permission
D) Is government
✅ **Answer: B**

28. Incentive for miners:
A) Signature
B) Storage
C) Cryptocurrency reward
D) Consensus authority
✅ **Answer: C**

🔹 DIGITAL SIGNATURE

29. Digital signature provides:
A) Confidentiality
B) Authentication & Non-repudiation
C) Speed
D) Compression
✅ **Answer: B**

30. Only ___ can sign, but ___ can verify:
A) Anyone, anyone
B) Signer, anyone
C) Miner, node
D) Public, private
✅ **Answer: B**

31. Digital signature is:
A) Transferable
B) Document-specific
C) Reusable
D) Anonymous
✅ **Answer: B**

◆ SMART CONTRACTS

32. Smart contract executes when:
A) Miner approves
B) Conditions are satisfied
C) Government approves
D) Hash changes
✅ **Answer: B**

---

33. Smart contracts were proposed by:
A) Satoshi Nakamoto
B) Nick Szabo
C) NIST
D) Ron Rivest
✅ **Answer: B**

---

34. Bitcoin scripting language is:
A) Turing complete
B) Turing incomplete
C) AI-based
D) Object-oriented
✅ **Answer: B**

---

35. Ethereum supports:
A) Turing incomplete contracts
B) Turing complete smart contracts
C) No contracts
D) Only payments
✅ **Answer: B**

◆ SHA DETAILS

36. SHA standard was developed by:
A) RSA
B) NIST
C) IBM

D) Google
✅ **Answer: B**

---

37. SHA-1 produces:
A) 128-bit
B) 160-bit
C) 256-bit
D) 512-bit
✅ **Answer: B**

---

38. SHA-256 block size:
A) 256 bits
B) 128 bits
C) 512 bits
D) 1024 bits
✅ **Answer: C**

---

39. Padding in SHA ensures message length becomes multiple of:
A) 128
B) 256
C) 512
D) 1024
✅ **Answer: C**

🔥 HIGH-RISK TRAP QUESTIONS

40. Public blockchains are usually:
A) Faster than private
B) Slower than private
C) Same speed
D) Offline
✅ **Answer: B**

---

41. Blockchain is completely anonymous:
A) True
B) False
C) Depends on miner
D) Depends on government
✅ **Answer: B**

(It's pseudonymous.)

---

42. Collision resistance strength of 256-bit hash is:
A) 2^{256}
B) 2^{128}

C) 2^{512}
D) 2^{64}
✅ **Answer: B**

---

43. If previous block hash changes, then:
A) Nothing happens
B) Only one block changes
C) Entire chain becomes invalid
D) Only nonce changes
✅ **Answer: C**

---

44. Hash pointer stores:
A) Only data
B) Data + key
C) Address + hash
D) Signature
✅ **Answer: C**

---

45. Consensus ensures:
A) Encryption
B) All honest nodes agree on same state
C) Fast mining
D) Zero attacks
✅ **Answer: B**

If you want, I can now:

- 🔥 Generate 100 more tricky ones
- 🧠 Make ultra-confusing negative marking traps
- ⚡ Create a rapid-fire revision sheet for last 20 minutes

Tell me how hard your professor makes MCQs 😄

Sources

🧠 Make ultra-confusing negative marking traps

Perfect 😈
Now I'll give you **ultra-confusing negative marking traps** — these are designed exactly the way professors try to cut marks.

Read **every word carefully**. Many options will look correct but differ by a single phrase.

🔥 SECTION 1: HASH FUNCTION TRAPS

1. Which statement about hash functions is CORRECT?

A) Collision resistance means no two inputs can have same hash
B) Collision resistance guarantees impossibility of collision
C) It is computationally infeasible to find two inputs with same hash
D) Hash functions are reversible

✅ **Answer: C**
(“Infeasible”, not impossible.)

---

2. For a 256-bit hash function, birthday attack requires approximately:

A) 2^{256} operations
B) 2^{128} operations
C) 256 operations
D) 128 operations

✅ **Answer: B**

---

3. Avalanche effect implies:

A) Hash output changes slightly if input changes slightly
B) Hash output changes significantly if input changes slightly
C) Hash becomes non-deterministic
D) Hash becomes longer

✅ **Answer: B**

---

4. Which property is used in Bitcoin mining?

A) Collision resistance
B) Hiding
C) Puzzle friendliness
D) Determinism

✅ **Answer: C**

---

5. Hiding property ensures:

A) Given hash h, finding *any* input is easy
B) Given hash h, finding original message is computationally hard
C) Hash cannot be computed
D) Hash is encrypted

✅ **Answer: B**

🔥 SECTION 2: MERKLE TREE TRAPS

6. Verifying transaction in Merkle tree requires:

A) O(n) hashes
B) O(1) hashes
C) O(log n) hashes
D) n^2 hashes

✅ **Answer: C**

---

7. Changing a transaction in a block requires:

A) Changing only that transaction
B) Changing Merkle root only
C) Recomputing that block and all subsequent blocks
D) Changing nonce only

✅ **Answer: C**

---

8. Merkle root depends on:

A) Only first transaction
B) Only last transaction
C) All transactions
D) Miner identity

✅ **Answer: C**

🔥 SECTION 3: BLOCKCHAIN ARCHITECTURE TRAPS

9. In blockchain, decentralization implies:

A) No coordination
B) Multiple coordinators and need for consensus
C) Faster than centralized systems
D) No failures possible

✅ **Answer: B**

---

10. Blockchain is tamper-proof because:

A) It is encrypted
B) Every node has a copy

C) Blocks contain previous hash
D) It uses cloud storage

✅ **Answer: C**

---

11. Blockchain is fully anonymous:

A) True
B) False
C) Only in Bitcoin
D) Only in Ethereum

✅ **Answer: B**
(It is pseudonymous.)

---

12. In public blockchain:

A) Only authorized nodes can validate
B) Anyone can participate in validation
C) Only government can mine
D) Identity verification mandatory

✅ **Answer: B**

🔥 SECTION 4: CONSENSUS TRAPS

---

13. Proof of Work selects miner based on:

A) Identity
B) Voting power
C) Computational power
D) Random assignment

✅ **Answer: C**

---

14. The challenge-response mechanism is used in:

A) Permissioned systems only
B) Permission-less consensus
C) Private blockchain only
D) Digital signatures

✅ **Answer: B**

---

15. If two miners produce blocks simultaneously:

A) Blockchain immediately stops
B) Both chains coexist temporarily
C) Blocks are discarded permanently
D) Mining ends

✅ **Answer: B**

🔥 SECTION 5: BLOCK STRUCTURE TRAPS

---

16. Block header contains:

A) Entire transaction data
B) Merkle root
C) Digital signatures
D) Private keys

✅ **Answer: B**

---

17. Mining requires:

A) Finding block height
B) Finding nonce satisfying difficulty
C) Encrypting transactions
D) Verifying signature

✅ **Answer: B**

---

18. Difficulty adjustment controls:

A) Block size
B) Transaction amount
C) Probability of hash satisfying prefix condition
D) Network delay

✅ **Answer: C**

🔥 SECTION 6: SMART CONTRACT TRAPS

---

19. Smart contracts are:

A) Legal documents stored digitally
B) Programs running on blockchain
C) Encrypted PDFs
D) Voting protocols

✅ **Answer: B**

---

20. Smart contracts once deployed:

A) Can be modified
B) Cannot be modified
C) Can be overwritten by miners
D) Auto-expire

✅ **Answer: B**

---

21. Bitcoin supports smart contracts that are:

A) Fully Turing complete
B) Turing incomplete
C) AI-based
D) Java-based

✅ **Answer: B**

---

22. Ethereum smart contracts are:

A) Permissioned
B) Turing complete
C) Centralized
D) Non-executable

✅ **Answer: B**

🔥 SECTION 7: DIGITAL SIGNATURE TRAPS

---

23. Digital signature provides confidentiality:

A) True
B) False

✅ **Answer: B**
(It provides authentication + non-repudiation, not confidentiality.)

---

24. Anyone can forge a digital signature if they know the public key:

A) True
B) False

✅ **Answer: B**

---

25. Signature of one document can be reused on another:

A) True
B) False

✅ **Answer: B**

🔥 SECTION 8: ULTRA-CONFUSION QUESTIONS

---

26. If a hash function has n-bit output, collision probability becomes significant after:

A) 2^n inputs
B) $2^{n/2}$ inputs
C) n inputs
D) log n inputs

✅ **Answer: B**

---

27. Which ensures blockchain immutability MOST directly?

A) Encryption
B) Merkle root
C) Previous block hash
D) Timestamp

✅ **Answer: C**

---

28. Blockchain ledger is:

A) Centralized but replicated
B) Distributed and append-only
C) Encrypted database
D) Mutable

✅ **Answer: B**

---

29. In SHA-256 preprocessing, padding makes message multiple of:

A) 128 bits
B) 256 bits
C) 512 bits
D) 1024 bits

✅ **Answer: C**

---

30. Mining complexity depends on:

A) Number of transactions
B) Number of nodes
C) Target difficulty
D) Wallet size

✅ **Answer: C**

🧠 FINAL PROFESSOR-LEVEL TRAP

31. Which statement is MOST accurate?

A) Blockchain prevents all attacks
B) Blockchain removes need for trust entirely
C) Blockchain reduces trust requirement using cryptographic mechanisms
D) Blockchain works without consensus

✅ **Answer: C**

If you can confidently answer every one of these without hesitation,
negative marking cannot hurt you.

If you want, I can now:

- 🧬 Create “Select the INCORRECT statement” traps
- 💀 Create Assertion–Reason traps
- ⚡ Give final 15-minute memory compression sheet

Tell me how evil your professor is 😄