Department of Computer Science and Engineering

Central Institute of Technology Kokrajhar

End Semester Examination

M. Tech

Course Title: **Blockchain Technology and Its Application** Course Code: **MCS218**
Session: **Jan-Jun, 2025** Full Marks: **100** Time: **3:00** hrs

---

Figure in the margin indicates full marks.
Question 1 is compulsory, Attempt any three from the rest!

1 [A] Fill in the blanks 2 x 10 = 20

i. Historically, _____ involved the direct exchange of goods but suffered from issues like lack of "coincidence of scales," "coincidence of time frames," and "coincidence of locations".
ii. Traditional exchange of value is now performed on ledgers managed by _____
iii. A hash function turns data into a _____ of that data called a hash.
iv. Bitcoin uses the _____ hash function, which produces an output of 32 bytes (256 bits).
v. A property of hash functions is _____, meaning you cannot find two different inputs that produce the same hash output.
vi. In asymmetric encryption, each user has two keys: a public key given to everybody and a _____ key kept secret.
vii. A _____ blockchain requires permission to join and participate in the network.
viii. The first widely adopted application of blockchain technology was the cryptocurrency _____ .
ix. A _____ is a digital representation of an asset or value that can be traded and managed on a blockchain.
x. A Decentralized Application (DApp) runs on a blockchain and is characterized as operating in a trustless, transparent, and _____ manner.

[B] Multiple Choice Questions 2 x 10 = 20

i. IPFS identifies files using content-based addressing by means of:
a) Location-based URLs
b) Server IP addresses
c) File names and paths
d) Cryptographic hashes, known as CIDs
ii. ERC20 is a token standard on Ethereum primarily designed for:
a) Unique, indivisible tokens
b) Tokens representing physical assets
c) Fungible tokens that are interchangeable
d) Tokens used solely for voting
iii. The ERC-721 token standard is the technical foundation primarily used for creating:
a) fungible currencies
b) Non-Fungible Tokens (NFTs)
c) security tokens requiring regulatory approval

d) privacy-preserving tokens

iv. A Decentralized Application (DApp) is defined as a software application that runs on a blockchain and operates in a manner that is:

a) Centralized and controlled by a single entity

b) Peer-to-peer, but requires a trusted intermediary

c) Trustless, transparent, and censorship-resistant

d) Primarily designed for offline use

v. A Hierarchical Deterministic (HD) Wallet allows for the generation of a structured tree of private and public key pairs from a single:

a) Transaction ID

b) Smart contract address

c) Seed phrase (or mnemonic)

d) Hardware device identifier

vi. A significant advantage of using an HD Wallet for managing cryptocurrency is:

a) It eliminates the need for transaction fees

b) It guarantees complete anonymity for all transactions

c) It provides simple and secure backup and recovery using a single seed phrase

d) It speeds up the block confirmation process

vii. Which consensus mechanism of Blockchain selects validators based on their identity and reputation, making it suitable for private or consortium networks?

a) Proof-of-Work (PoW)

b) Proof-of-Stake (PoS)

c) Proof-of-Authority (PoA)

d) Delegated Proof-of-Stake (DPoS)

viii. In a Proof-of-Stake (PoS) system, validators are typically chosen to propose and validate blocks based on:

a) Their ability to solve complex mathematical puzzles

b) The amount of computing power they contribute

c) Their real-world identity and reputation

d) The amount of cryptocurrency they have staked or committed

ix. What is a key advantage of using blockchain for supply chain management?

(a) Reduced transparency

(b) Increased risk of counterfeiting

(c) Enhanced traceability and accountability

(d) Slower transaction speeds

x. What is the primary purpose of a hash in a blockchain?

(a) To encrypt the entire block of data

(b) To uniquely identify a block and verify its integrity

(c) To speed up transaction processing

(d) To reward miners for their work

2 a. What is the difference between physical and digital assets in Blockchain? 5 x 4 = 20

b. What is the double-spending problem in the context of digital assets?

c. Why was direct exchange (barter) historically problematic?

d. What are some characteristics of "good money"?

3 a. What is "mining" in the context of blockchain? 5 x 4 = 20

b. What is the purpose of the Nonce in the mining process?

c. How is a new block accepted into the blockchain?

d. What is the incentive for nodes to participate in mining?

4 a. Explain the fundamental principles behind blockchain technology, detailing the roles of decentralization, cryptography (hashing and digital signatures), and consensus mechanisms in ensuring its security and integrity. 15 + 5 = 20
b. Discuss the advantages and disadvantages of this architectural approach compared to traditional centralized systems.

5 Compare and contrast at least three different consensus mechanisms (e.g., Proof-of-Work, Proof-of-Stake, Proof-of-Authority), highlighting their operational principles, energy efficiency, security strengths and weaknesses, and suitability for different types of blockchain applications. 20

6 Analyze the potential of blockchain technology to disrupt traditional financial systems (DeFi). Discuss the key components of DeFi, its benefits and risks compared to traditional finance, and the regulatory challenges it currently faces. 20

xxXxx