

BLOCKCHAIN TECHNOLOGY & APPLICATIONS
(MCAP 2254)

Time Allotted : 3 hrs

Full Marks : 70

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and any 5 (five) from Group B to E, taking at least one from each group.

Candidates are required to give answer in their own words as far as practicable.

Group - A
(Multiple Choice Type Questions)

1. Choose the correct alternative for the following: **10 × 1 = 10**
- (i) Blockchain is a
(a) centralized digital ledger consisting of records called blocks
(b) decentralized, distributed, digital ledger consisting of records called blocks
(c) digital database consisting of records called class
(d) none of the above.
- (ii) _____ is the part of asymmetric encryption.
(a) Public key
(b) Private Key
(c) Passphrase
(d) All of the above
- (iii) _____ is the type of ledger present in Blockchain.
(a) Distributed Ledger
(b) Decentralized Ledger
(c) Both (a) and (b)
(d) None of the above
- (iv) The maximum number of bitcoins that can be created is _____
(a) 11 million
(b) 25 million
(c) 21 million
(d) 100 million.
- (v) _____ characteristic makes blockchain tamper-proof.
(a) Cryptocurrency
(b) VPN
(c) Immutability
(d) All of the above
- (vi) _____ is used for storing bitcoins.
(a) Block
(b) Wallet
(c) Both (a) and (b)
(d) None of the above
- (vii) In blockchain, a block is consist of _____
(a) a timestamp
(b) transaction data
(c) a hash pointer
(d) all of the above.
- (viii) Smart contracts are not the legal documents
(a) Yes
(b) No
(c) May be
(d) Can't say.

- (ix) Genesis block is
(a) the first block of a blockchain
(b) a famous block that hardcoded a hash of the Book of Genesis onto the blockchain
(c) the first block after each block halving
(d) the 2nd transaction of a blockchain.
- (x) What is the purpose of a nonce?
(a) Follows nouns
(b) A hash function
(c) Prevents double spending
(d) Sends information to the blockchain network.

Group- B

2. (a) Recall the different types of hashing. Reproduce the utility of a hash pointer. *[[CO1](Remember/LOCQ)]*
(b) Reproduce the RSA key generation, encryption and decryption process. *[[CO1](Remember/LOCQ)]*
(3 + 3) + 6 = 12
3. (a) Explain how Hashing is used to resist tampering in a blockchain. *[[CO2](Understand/LOCQ)]*
(b) Discuss, how blockchain eradicates the problems with a classical centralized approach of storing data. *[[CO2](Understand/LOCQ)]*
6 + 6 = 12

Group - C

4. (a) Write the properties of distributed consensus. Interpret the correctness of a distributed consensus protocol. *[[CO3](Apply/IOCQ)]*
(b) Interpret the FLP impossibility theorem for asynchronous deterministic consensus. *[[CO3](Apply/IOCQ)]*
(4 + 2) + 6 = 12
5. (a) Examine the applicability of Hashcash as a proof of work. *[[CO4](Analyze/IOCQ)]*
(b) Demonstrate the Lamport Shostak Pease algorithm with an example. *[[CO3](Apply/IOCQ)]*
6 + 6 = 12

Group - D

6. (a) What is an uncle block in an Ethereum block? How are rewards for uncle blocks calculated? *[[CO4](Analyze/IOCQ)]*
(b) Distinguish between external account and contract account in an Ethereum blockchain. *[[CO4](Analyze/IOCQ)]*
(2 + 4) + 6 = 12

7. (a) Distinguish between the following Bitcoin scripts – *provably unspendable output* and *anyone can spend*. [[CO4](Analyze/IOCQ)]
 (b) Examine the block propagation mechanism in a Bitcoin network. [[CO4](Analyze/IOCQ)]
4 + 8 = 12

Group - E

8. (a) Evaluate the ways in which a cryptocurrency user can obtain his coins. [[CO5](Evaluate/HOCQ)]
 (b) Evaluate the regulatory challenges in the fight against money laundering, terrorist financing and tax evasion via cryptocurrencies. [[CO5](Evaluate/HOCQ)]
6 + 6 = 12
9. (a) Write five different applications/use cases of blockchain. [[CO6](Create/HOCQ)]
 (b) Develop a Blockchain solution for handling double selling problem in land registration. [[CO6](Create/HOCQ)]
5 + 7 = 12

<i>Cognition Level</i>	<i>LOCQ</i>	<i>IOCQ</i>	<i>HOCQ</i>
<i>Percentage distribution</i>	<i>25</i>	<i>50</i>	<i>25</i>

Course Outcome (CO):

After the completion of the course students will be able to

- CO1: Recall basic cryptographic mechanisms like encryption, hashing and digital signature required for blockchain
- CO2: Understand blockchain network, mining mechanism, distributed consensus, transactions, anonymity, reward, fork, private and public blockchain
- CO3: Demonstrate different distributed consensus models like proof of work (PoW) and proof of stake (PoS)
- CO4: Examine the working principle of cryptocurrencies like Bitcoin and Ethereum
- CO5: Evaluate the current cryptocurrency regulations, legal aspects, cryptocurrency exchange, black market and global economy
- CO6: Create blockchain applications in the domain of internet of things, e-governance, land registration, medical record management, domain name service, etc.

**LOCQ: Lower Order Cognitive Question; IOCQ: Intermediate Order Cognitive Question; HOCQ: Higher Order Cognitive Question.*

