BLOCKCHAIN TECHNOLOGY & APPLICATIONS
(MCAP 2254)

Time Allotted : 2½ hrs **Full Marks : 60**

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and any 4 (four) from Group B to E, taking one from each group.

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

Group – A

1. Answer any twelve: **12 × 1 = 12**

Choose the correct alternative for the following

(i) _____ is the part of asymmetric encryption.
(a) Public key (b) Private Key
(c) Passphrase (d) All of the above

(ii) UTXO stands for _____.
(a) Unspent Transaction Office (b) United Transaction Office
(c) United Transaction Output (d) Unspent Transaction Output

(iii) _____ characteristic makes blockchain tamper-proof.
(a) Cryptocurrency (b) VPN
(c) Immutability (d) All of the above

(iv) The process of creating new bitcoins is known as
(a) Financing (b) Sourcing
(c) Mining (d) None of the above

(v) _____ is used for storing bitcoins.
(a) Block (b) Wallet
(c) Both (a) and (b) (d) None of the above

(vi) _____ is the type of ledger present in Blockchain.
(a) Distributed Ledger (b) Decentralized Ledger
(c) Both (a) and (b) (d) None of the above

(vii) The maximum number of bitcoins that can be created is _____.
(a) 11 million (b) 25 million
(c) 21 million (d) 100 million

(viii) In blockchain, a block is consist of _____.
(a) A Timestamp (b) Transaction data
(c) A Hash pointer (d) All of the above

(ix) Smart contracts are not the legal documents.
(a) Yes (b) No
(c) May be (d) Can't say

(x) 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.

Fill in the blanks with the correct word

(xi) A hash function converts an input of arbitrary length to an output of _____ length.

(xii) Safety and _____ are the two important properties of distributed consensus.

(xiii) Paxos, Raft and Byzantine Fault Tolerance are _____ consensus protocols.

(xiv) In a distributed system, a node starts behaving maliciously is called a _____ fault.

(xv) Bitcoin protocol runs on TCP port _____.

Group - B

2. (a) List the properties of a cryptographic hash function. *[(CO1)(Remember/LOCQ)]*
(b) Reproduce the signature generation and signature verification steps of digital signature. *[(CO1)(Remember/LOCQ)]*
4 + 8 = 12

3. (a) Explain the different types of hashing with suitable diagrams. *[(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) Interpret the difference between proof of work, proof of stake and proof of burn. *[(CO3)(Apply/IOCQ)]*
(b) Write the basic idea of practical Byzantine fault tolerance. *[(CO3)(Apply/IOCQ)]*
6 + 6 = 12

5. (a) Examine the utility of proof of elapsed time as a consensus protocol. *[(CO4) (Analyze/IOCQ)]*
(b) Demonstrate the Lamport Shostak Pease Algorithm with an example. *[(CO3)(Apply/IOCQ)]*
6 + 6 = 12

Group - D

6. (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

7. (a) Examine the different Ether denominations. *[(CO4)(Analyze/IOCQ)]*

   (b) Appraise the development workflow of smart contract programming. *[(CO4)(Analyze/IOCQ)]*

4 + 8 = 12

Group - E

8. (a) Defend if there is a need for a more comprehensive approach, introducing license requirements for cryptocurrencies? *[(CO5)(Evaluate/HOCQ)]*

   (b) Appraise the different types of wallet providers in a Bitcoin network. *[(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 Validation of Education and Professional Qualifications. *[(CO6)(Create/HOCQ)]*

5 + 7 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	25	50	25

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.*