BLOCKCHAIN TECHNOLOGY AND APPLICATIONS
(MCA2132)

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) What is a genesis block?
(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

(ii) Which of the following characteristics best defines the primary purpose of blockchain technology?
(a) To provide centralised control of data
(b) To enable peer-to-peer transactions without intermediaries
(c) To replace all traditional databases
(d) To enhance cloud storage capabilities

(iii) Proof of Stake is _____.
(a) A transaction and block verification protocol
(b) A certificate needed to use the blockchain
(c) Both (a) and (b)
(d) None of the above

(iv) POW stands for
(a) Proof of Wisdom (b) Proof of Work
(c) Proof of Word (d) None of the above

(v) What is the purpose of a nonce?
(a) Follows nouns (b) A hash function
(c) Prevents double spending (d) Sends information to the blockchain networ

(vi) What is the primary purpose of a consensus mechanism in blockchain networks?
(a) To increase transaction fees for network participants
(b) To ensure network nodes agree on the validity of transactions
(c) To centralize control of the blockchain
(d) To prevent the creation of multiple blockchains at once

(vii) Which among the following is a difference between Bitcoin and Ethereum?
(a) Ethereum uses PoS while Bitcoin uses PoW.
(b) Bitcoin scrypt is turing-complete while Ethereum's Solidity is turing-incomplete.
(c) Ethereum is more accepted compared to Bitcoin.
(d) Ethereum is deflationary while Bitcoin is inflationary.

(viii) Which method is used by lightweight Bitcoin clients to verify transactions without downloading the entire blockchain?
(a) Proof-of-Stake (b) SPV (Simplified Payment Verification)
(c) Full node validation (d) Lightning Protocol

(ix) How does blockchain technology benefit the insurance industry?
(a) By avoiding compliance requirements of national authorities, which reduces overhead
(b) By ensuring accuracy of data and automating micro insurances, which reduces costs
(c) By introducing flexible premiums to be paid by customers, which increases profits
(d) By setting up a digital mode of payment, which simplifies claims settlement

(x) What is ERC20?
(a) The ISO standard for the implementation of public blockchains
(b) The European standard for the implementation of smart contracts
(c) The technical standard used for smart contracts on the Ethereum blockchain for implementing tokens
(d) The European Central Bank governance standard controlling the value of the bitcoin

Fill in the blanks with the correct word

(xi) In blockchain, blocks are linked _____?

(xii) _____ is the type of ledger present in Blockchain.

(xiii) The process of creating new bitcoins is known as _____.

(xiv) A blockchain that anyone can join and participate in is called a _____ blockchain.

(xv) The process by which a network of computers agrees on the validity of transactions and new blocks is known as _____.

Group - B

2. (a) List the properties of a cryptographic hash function. *[(CO1)(List/LOCQ)]*
(b) Explain how a node in a Blockchain network decides on which block to relay. *[(CO2)(Explain/LOCQ)]*
(c) Describe the utility of the different components of a block hash. *[(CO2)(Describe/LOCQ)]*

4 + 4 + 4 = 12

3. (a) Suppose we want to use the RSA scheme for an encryption and have chosen the integer value *77* as the product of two (2) prime numbers p and q. For the private key *d* and public key *e*, we have the relation *e*d = 1 modulo (p-1) (q-1).*
(i) What is the public key *e* for a private key with *d = 43*?
(ii) What is the cipher C for a message with M =5? *[(CO1)(Solve/IOCQ)]*

(b) Explain how Hashing is used to resist tampering in a blockchain? *[(CO2)(Explain/LOCQ)]*

(4 + 4) + 4 = 12

Group - C

4. (a) Illustrate the concept of distributed consensus with a real life example. *[(CO3)(Illustrate/IOCQ)]*

(b) Distinguish between permissioned and permissionless consensus. *[(CO3)(Distinguish/IOCQ)]*

(c) Sketch the challenges of consensus in a permissionless model. *[(CO3)(Sketch/IOCQ)]*

4 + 4 + 4 = 12

5. (a) Distinguish between proof of work and proof of stake. *[(CO3)(Distinguish/IOCQ)]*

(b) Recall the different types of faults that may be encountered in distributed consensus. *[(CO3)(Recall/LOCQ)]*

(c) Elucidate view change in Practical Byzantine Fault Tolerance. *[(CO3)(Sketch/IOCQ)]*

6 + 3 + 3 = 12

Group - D

6. (a) What is an uncle block in an Ethereum block? How are rewards for uncle blocks calculated? *[(CO4)(Examine/IOCQ)]*

(b) Distinguish between external account and contract account in an Ethereum blockchain. *[(CO4)(Distinguish/IOCQ)]*

(c) Distinguish between the following Bitcoin scripts – provably unspendable output and anyone can spend. *[(CO4)(Distinguish/IOCQ)]*

4 + 4 + 4 = 12

7. (a) Elucidate the concept of smart contracts with appropriate examples. *[(CO4)(Appraise/IOCQ)]*

(b) Write a smart contract that sets the value of a variable and exposes it for other contracts to access. *[(CO4)(Write/HOCQ)]*

5 + 7 = 12

Group - E

8. (a) Evaluate the ways in which a cryptocurrency user can obtain his coins. *[(CO5)(Evaluate/HOCQ)]*

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

6 + 6 = 12

9. Design a blockchain leveraged post disaster relief allocation system over smartphone-based delay tolerant network, elaborating the network architecture, system architecture and flow of activities. *[(CO6)(Design/HOCQ)]* **12**

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	19.8	47.9	32.3