

**FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGY
(INFO 4231)**

Time Allotted : 2½ hrs

Full Marks : 60

Figures out of the right margin indicate full marks.

*Candidates are required to answer Group A and
any4 (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 are the different types of blockchain?
 - (a) Public, private, generic
 - (b) Public, secret, consortium
 - (c) Generic, secret, consortium
 - (d) Public, private, consortium
- (ii) What is the incentive for miners to validate transactions?
 - (a) Appreciation of the community
 - (b) Nonce
 - (c) Additional memory
 - (d) Block rewards
- (iii) What is the genesis block?
 - (a) Any block created by the founder
 - (b) The last block created in the Blockchain
 - (c) The first block of a Blockchain
 - (d) The first transaction in each block
- (iv) If a hacker wanted to alter a blockchain, what percentage of the block copies would he have to alter?
 - (a) Only his copy
 - (b) 1%
 - (c) 51%
 - (d) 100%
- (v) What powers the Ethereum Virtual Machine?
 - (a) Gas
 - (b) Ether
 - (c) Bitcoin
 - (d) Block Rewards

- (vi) The transaction Merkle Tree root value in a Bitcoin block is calculated using,
 - (a) Hash of transactions
 - (b) Previous block's hash
 - (c) Number of transactions
 - (d) None of the above
- (vii) What is a DApp?
 - (a) A type of cryptocurrency
 - (b) A condiment
 - (c) A type of blockchain
 - (d) A decentralized application
- (viii) What is a fork?
 - (a) The copy of a block
 - (b) The creation of an alternative version of a blockchain
 - (c) The creation of a new distributed ledger
 - (d) The copy of a cryptocurrency wallet
- (ix) Hash, identifying each block in the blockchain, is generated using which of the following cryptographic algorithm?
 - (a) SHA128
 - (b) SHA256
 - (c) Both of them
 - (d) None of them
- (x) What is Proof of Stake?
 - (a) A certificate needed to use the blockchain
 - (b) A password needed to access an exchange
 - (c) How private keys are made
 - (d) A transaction and Block Verification Protocol

Fill in the blanks with the correct word

- (xi) _____ occurs when several nodes (usually most nodes on the network) have the same blocks in their locally-validated best blockchain.
- (xii) _____ receive, verify, gather and execute transactions.
- (xiii) Proof-of-Work (PoW) and Proof-of-Stake (PoS) are used in blockchain networks as _____ protocol.
- (xiv) In a Blockchain, _____ stores all the transactions in a block by producing a digital fingerprint of the entire set of transactions.
- (xv) Ethereum smart contract can be written using _____ language.

Group - B

2. (a) Compare and contrast between Proof-of-work and Proof-of-stake.

[(C01)(Analyse/IOCQ)]

- (b) Describe the entities involved and steps followed in a blockchain network to include a transaction into the blockchain? [[CO2](Understand/LOCQ)]
6 + 6 = 12
3. (a) “Blockchain is a decentralized, distributed, append-only digital ledger” – Justify with example. [[CO1](Analyse/IOCQ)]
 (b) Describe the significance of Nonce in the following statement:
 $H_k = \text{Hash}(H_{k-1} || T || \text{Nonce})$. [[CO2](Understand/LOCQ)]
6 + 6 = 12

Group - C

4. (a) How does consensus work in the Bitcoin blockchain and why is it essential? [[CO3](Remember/LOCQ)]
 (b) Illustrate some examples of FORTH script instructions used in Bitcoin transactions. [[CO3](Apply/IOCQ)]
6 + 6 = 12
5. (a) Illustrate the concept of a Merkle Tree with the help of a diagram and justify its role in blockchain? [[CO3](Analyse/IOCQ)]
 (b) Explain the concept of Pay-to-Public-Key-Hash (P2PKH). [[CO3](Understand/LOCQ)]
6 + 6 = 12

Group - D

6. (a) What is Ethereum Network? Differentiate between Mainnet and Testnet? [[CO4](Remember/LOCQ)]
 (b) Explain the role of EVM in Ethereum ecosystem. [[CO4](Understand/LOCQ)]
(2 + 4) + 6 = 12
7. (a) What is Gas limit in Solidity? Discuss two famous smart contract frameworks for Solidity. [[CO4](Remember/LOCQ)]
 (b) Outline some differences between the Ethereum blockchain and Bitcoin. [[CO4](Understand/LOCQ)]
(2 + 3 + 3) + 4 = 12

Group - E

8. (a) Analyze the suitability of blockchain technology in realizing supply chain management. [[CO5](Analyse/IOCQ)]
 (b) Evaluate blockchain scalability issues? [[CO6](Evaluate/HOCQ)]
6 + 6 = 12
9. (a) Discuss an use-cases of blockchain technology in Education Sector. [[CO5](Analyse/IOCQ)]
 (b) Evaluate the probable challenges in adoption of blockchain technology? [[CO6](Evaluate/HOCQ)]
6 + 6 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	50	37.5	12.5

Course Outcome (CO):

After the completion of the course students will be able to

INF04231.1 Understand the abstract models for Blockchain Technology, its benefits and challenges

INF04231.2 Learn the use the basic crypto primitives to secure Blockchain

INF04231.3 Describe the functional/operational aspects of cryptocurrency ecosystem

INF04231.4 Explain the features and functional aspects of smart contract ecosystem

INF04231.5 Discuss the practical use-cases of Blockchain

INF04231.6 Identify the major research challenges in Blockchain domain

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