BLOCKCHAIN TECHNOLOGY
(IOT2201)

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 blockchain?
(a) A blockchain is a centralized digital ledger consisting of records called blocks
(b) A blockchain is a decentralized, distributed, digital ledger consisting of records called blocks
(c) A blockchain is a digital database consisting of records called class
(d) None of the above.

(ii) 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.

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

(iv) 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

(v) What is Byzantine fault tolerance?
(a) Resilience against multiple node crashes
(b) Resilience against multiple message losses
(c) Resilience against partitioned network
(d) Resilience against malicious nodes

(vi) How often does Bitcoin ledger reconcile?
(a) Every day (b) Every 3 months
(c) Every 3 Minutes (d) Every 10 Minutes

(vii) How many minutes does it take to mine an Ethereum block?
(a) 0 (b) 10 (c) 30 (d) 12.

(viii) 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.

(ix) What is digital fiat currency?
(a) A digital form of currency, that represents a country's financial reserves
(b) An e-currency, that creates a transparent and borderless debt market
(c) An online system, that enables making transactions without a bank account
(d) All of the above.

(x) How does blockchain technology help to protect intellectual property rights (IP)?
(a) It allows a user to include IP transactions in smart contracts
(b) It allows a user to record an event and establish the timeline
(c) It allows a user to record the creation of software packages
(d) It allows a user to send a transaction and receive IP ownership.

Fill in the blanks with the correct word

(xi) Bitcoin is based on _____ blockchain.

(xii) _____ provides the power to the Ethereum Virtual Machine.

(xiii) In blockchain, a block is consist of _____.

(xiv) Blockchain technology is consists of _____ pillars.

(xv) _____ characteristic makes blockchain tamper-proof.

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) Perform encryption and decryption using the RSA algorithm, for the following: $p = 3$; $q = 11$, $e = 7$; $M = 5$. *[(CO1)(Solve/IOCQ)]*
(b) Explain the steps in digital enveloping. How does digital envelope exploit the advantages of both symmetric and asymmetric key cryptography? *[(CO2)(Explain/LOCQ)]*
7 + 5 = 12

Group - C

4. (a) Illustrate the safety and liveness properties of a distributed system. *[(CO3)(Illustrate/IOCQ)]*

   (b) Sketch the different types of faults in a distributed system. *[(CO3)(Sketch/IOCQ)]*

6 + 6 = 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) Examine the execution of a Bitcoin script with an example. *[(CO4)(Examine/IOCQ)]*

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

6 + 6 = 12

7. (a) Examine the transaction flooding mechanism in a Bitcoin network. *[(CO4)(Examine/IOCQ)]*

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

   (c) Examine the double spending problem in a Bitcoin network and how it can be handled using Blockchain. *[(CO4)(Examine/IOCQ)]*

5 + 5 + 2 = 12

Group - E

8. (a) Evaluate whether it would make sense to extend the scope of the Funds Transfer Regulation and/or the Cash Control Regulation as to include cryptocurrency transactions. *[(CO5)(Evaluate/HOCQ)]*

   (b) Compare the different types of wallet providers in a Bitcoin network. *[(CO5)(Compare/IOCQ)]*

6 + 6 = 12

9. (a) Give your arguments in support of the statement – "There is a need for introducing license requirements for cryptocurrencies". *[(CO5)(Argue/HOCQ)]*

   (b) Write five different applications/use cases of blockchain. *[(CO6)(Write/HOCQ)]*

7 + 5 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	20.83	60.42	18.75