*Total No. of Questions: 6* *Total No. of Printed Pages:3*

**Enrollment No.....**

# Faculty of Engineering

## End Sem (Odd) Examination Dec-2019

## OE00016 Blockchain Architecture

Programme: B.Tech. Branch/Specialisation: All

**Duration: 3 Hrs.** **Maximum Marks: 60**

Note: All questions are compulsory. Internal choices, if any, are indicated. Answers of Q.1 (MCQs) should be written in full instead of only a, b, c or d.

Q.1 i. Which of the following are properties of blockchain? **1**

(a) Distributed Ledger (b) Integrity and Safety

(c) Decentralized Systems (d) All of these

ii. Which is not an example of cryptocurrency? **1**

(a) Bitcoin (b) Litecoin (c) XRP (d) Ripple

iii. The property of consistency is preserved in blockchain by maintaining _____ **1**

(a) A Global copy of the Total Information

(b) A Local copy of the Global Information

(c) A Global List of transactions

(d) None of these

iv. A block in blockchain is pointed using: **1**

(a) Hash Pointer (b) User ID

(c) Transaction ID (d) Timestamp

v. In distributed consensus, all the correct individuals either reach a value or null. The property is **1**

(a) Termination (b) Validity

(c) Integrity (d) Agreement

vi. Suppose the previous difficulty was set to 20 and the given threshold before the change in difficulty level is 2 weeks. If the last 2016 blocks were mined in 1119100 milliseconds, then after 2 weeks what will be the level of difficulty? [Use ceiling function to provide the answer]. **1**

(a) 22 (b) 20 (c) 19 (d) 21

P.T.O.

vii. Which of the following variable among the components of the block header is computed (or rather obtained) to achieve the difficulty posed by the blockchain network? **1**

(a) Merkle tree root (b) Nonce

(c) Timestamp (d) Previous block hash

viii. What is a Merkle Root in bitcoin? **1**

(a) A hash of all transactions in a block that allows any specific transaction to be verified without downloading the entire blockchain

(b) A series of complex data that uniquely identifies the owner of an address

(c) A program designed by David Merkle that uncovers the largest inactive bitcoin wallets

(d) A cryptocurrency developed by the chancellor of Germany

ix. What is the most prominent future of blockchain? **1**

(a) Hash graph

(b) Tangle

(c) Distributed Ethereum Ledger (DET)

(d) None of these

x. Which of the following advantages are provided by the blockchain based solution for trade logistics? **1**

(a) Tamper proof and digitally signed documents

(b) Process Automation

(c) Real Time Visibility and Analytics

(d) All of these

Q.2 i. What is meant by Double spending? Why is it considered as a problem? **3**

ii. Write down at least five legal aspects of crypto currency, along with diagram. **7**

OR iii. What is meant by Wallets for crypto currency? Give at least five types of crypto currency wallets? How is it different from digital wallets? **7**

Q.3 i. What are the two basic cryptographic primitives behind the blockchain technology? **3**



ii. Write short note on SHA-256. **7**

OR iii. What is Digital signature? What are their requirements? Discuss direct digital signature and arbitrated digital signature. **7**

Q.4 i. What do you understand by difficulty level? Explain what parameters affects the difficulty level? **3**

ii. Differentiate between POW, POB, POS. **7**

OR iii. Explain Ethereum architecture with diagram. Explain the concept of GAS and EVM in Ether's context. **7**

Q.5 i. What is Merkle Tree? Give its significance in Block Chain. **3**

ii. What is Fork? Give at least four differences between Hard and Soft Fork. **7**

OR iii. What do you understand by public blockchain? How is it different from Private blockchain? Give at least three practical aspects of public blockchain. **7**

Q.6 i. What do you understand by Hash graph? **3**

ii. Write a detailed application of blockchain covering Financial Sector and Medical record management system **7**

OR iii. Write a Case study: Government on blockchain. **7**

******

# Marking Scheme
# OE00016 Blockchain Architecture

| | | | | |
|---|---|---|---|---|
| Q.1 | i. | Which of the following are properties of blockchain?<br>(d) All of these | | **1** |
| | ii. | Which is not an example of cryptocurrency?<br>(c) XRP | | **1** |
| | iii. | The property of consistency is preserved in blockchain by maintaining _____<br>(b) A Local copy of the Global Information | | **1** |
| | iv. | A block in blockchain is pointed using:<br>(a) Hash Pointer | | **1** |
| | v. | In distributed consensus, all the correct individuals either reach a value or null. The property is<br>(d) Agreement | | **1** |
| | vi. | Suppose the previous difficulty was set to 20 and the given threshold before the change in difficulty level is 2 weeks. If the last 2016 blocks were mined in 1119100 milliseconds, then after 2 weeks what will be the level of difficulty? [Use ceiling function to provide the answer].<br>(a) 22 | | **1** |
| | vii. | Which of the following variable among the components of the block header is computed (or rather obtained) to achieve the difficulty posed by the blockchain network?<br>(b) Nonce | | **1** |
| | viii. | What is a Merkle Root in bitcoin?<br>(a) A hash of all transactions in a block that allows any specific transaction to be verified without downloading the entire blockchain | | **1** |
| | ix. | What is the most prominent future of blockchain?<br>(d) None of these | | **1** |
| | x. | Which of the following advantages are provided by the blockchain based solution for trade logistics?<br>(d) All of these | | **1** |
| Q.2 | i. | Double spending | 1 mark | **3** |
| | | Why is it considered as a problem | 1 mark | |
| | | Overcome | 1 mark | |
| | ii. | Five legal aspects of crypto currency | 5 marks | **7** |
| | | Diagram. | 2 marks | |
| OR | iii. | Wallets for crypto currency | 1 mark | **7** |
| | | Five types of crypto currency wallets | 5 marks | |
| | | Different from digital wallets | 1 mark | |
| Q.3 | i. | Two basic cryptographic primitives | | **3** |
| | | Cryptographically Secured Hash Function | 1.5 marks | |
| | | Digital Signature | 1.5 marks | |
| | ii. | Short note on SHA-256. | | **7** |
| OR | iii. | Digital signature | 2 marks | **7** |
| | | Their requirements | 2 marks | |
| | | Direct digital and arbitrated digital signature | 3 marks | |
| Q.4 | i. | Difficulty level | 2 marks | **3** |
| | | Parameters affects the difficulty level | 1 mark | |
| | ii. | Differentiate between POW, POB, POS. | | **7** |
| | | 1 mark for each valid point | (1 mark * 7) | |
| OR | iii. | Ethereum architecture with diagram | 4 marks | **7** |
| | | Concept of GAS and EVM in Ether's context | 3 marks | |
| Q.5 | i. | Merkle Tree | 2 marks | **3** |
| | | Its significance in Block Chain | 1 mark | |
| | ii. | Fork | 3 marks | **7** |
| | | At least four differences between Hard and Soft Fork | 4 marks | |
| OR | iii. | Public blockchain | 2 marks | **7** |
| | | Different from Private blockchain | 2 marks | |
| | | At least three practical aspects of public blockchain | 3 marks | |
| Q.6 | i. | Hash graph | | **3** |
| | ii. | Application of blockchain covering | | **7** |
| | | Financial Sector | 3.5 marks | |
| | | Medical record management system | 3.5 marks | |
| OR | iii. | Case study: Government on blockchain. | | **7** |

******