Exam Date & Time: 25-Apr-2024 (09:15 AM - 12:30 PM)

**CHAROTAR UNIVERSITY OF SCIENCE AND TECHNOLOGY**

University Theory Examination (Regular) April 2024
Sixth Semester Of B.Tech (IT)

**BLOCKCHAIN TECHNOLOGIES [IT384]**

**Marks: 70** **Duration: 195 mins.**

**1**

**Answer all the questions.** Section Duration: 40 mins

Choose the right answer.

1 Ethereum uses _____ hashing algorithm. (1)

SHA-256 Keccak-256 ECDSA SHA-1

2 Make a match: (1)

1. Proof of Stack ----------> a. Waves
2. Proof of Elapsed Time--> b. Intel
3. Proof of Importance-----> c. NEM
4. Proof of Burn ----------> d. Slimcoin
5. Proof of Capacity--------> e. Burstcoin

1-a, 2-d, 3-e, 4-c, 5-b 1-c, 2-d, 3-e, 4-b, 5-a 1-e, 2-c, 3-b, 4-a, 5-d 1-a, 2-b, 3-c, 4-d, 5-e

3 For a 512 bit hash function, the attacker needs to compute how many hash operations in order to find two matching outputs in the initial round? (1)

2^1024 2^512 2^256 2^128

4 Which of the following field in present in a Bitcoin block summary? (1)

Difficulty Gas limit Gas used Private key of the sender

5 5-ether equals to... (1)

5 x (10^6) wei 5 x (10^8) wei 5 x (10^16) wei 5 x (10^18) wei

6 Which of the following is an open source, enterprise-grade Permissioned DLT platform? (1)

Hyperledger Indy Hyperledger Burrow Hyperledger Fabric Hyperledger Explorer

7 An_____ is defined as a communication node that is responsible for the distribution of blockchain transactions in Hyperledger Fabric. (1)

MSP Client Node Endorsing Node Orderer

8 What type of ledger refers to a distributed ledger that doesn't require a native currency to operate? (1)

Tokenless Public Enterprise Private

9 Level DB is the default database for Hyperledger Fabric and is particularly appropriate when ledger states comprise what type of data? (1)

Complex key-value pairs Rich Queries JSON data pairs Simple key-value pairs

10 If there are 25 faulty nodes in, at least how many nodes needed to reach consensus in the Byzantine Fault Tolerance (BFT) system. (1)

72 76 77 79

11 What is the correct sequence of operations in PBFT algorithm? (1)

i) Prepare ii) Reply iii) Commit iv) Pre-prepare.

iv, i, ii, iii iv, i, iii, i, iv, ii, iii i, ii,iv, iii

i

12 In a decentralized blockchain network, which scenario poses a significant risk known as the "51% Vulnerability"? (1)

- When more than 51% of the nodes in the network experience a temporary outage.
- When a single entity or a group controls more than 51% of the network's computing power.
- When a majority of users hold more than 51% of the cryptocurrency tokens.
- When more than 51% of the transactions in a block are invalid due to cryptographic errors.

13 Which is/are the possible example/s of a double-spending attack? (1)

- Suresh has a total of 90 unspent bitcoins from two different transactions with an equal amount of bitcoins each. He tries to send the entire amount at a time each to Minesh and Nimesh as transactions.
- Naresh bought a car using 'm' bitcoins. On delivery, the bitcoins are transferred from his wallet to the dealer's wallet.
- Paresh has 180 unspent bitcoins. He sends the equal amount each to Devesh and Bhavesh one by one.
- Ramesh has 20 unspent bitcoins. He tries to transfer those 20 bitcoins to his two each of his friends simultaneously.

14 Select the correct statement for Ethereum? (1)

- An address is 20 bytes long, a public key 64 bytes, and the private key 32 bytes
- An address is 20 characters long, a public key 32 characters long, and a private key 64 characters long
- There is no public key, the public key is the address, both are 20 bytes, the private key 32 bytes long
- None of the above

15 Which of the statements is TRUE? (1)

- Gas is a fee paid to miners for mining blocks.
- Gas is the cost of computational work on the blockchain.
- Gas is NOT mandatory when sending ETH transactions.
- Gas fees are based on the size of a transaction.

16 What is an advantage of using the consensus algorithm Proof of Elapsed Time (PoET) instead of Proof of Work (PoW)? (1)

- PoET can often be used in a permissionless blockchain more easily than PoW, because PoET's lottery system for node selection is secure.
- PoET has generally lower transaction costs than PoW, because the hardware needed is more generic than the hardware needed for PoW.
- PoET is much more secure than PoW, because PoET supports the trusted execution environment (TEE) by time-stamping the transactions.
- PoET is usually faster than PoW, because fewer nodes compete for validation than in PoW, since PoET randomly selects the nodes.

17 Which network would incentivize hackers most to break the network? (1)

Bitcoin Fabric Ripple Ethereum

18 How can blockchain technology best help securing identity data? (1)

- By eliminating third parties through providing secured-data storage at a user's server
- By encoding all the health data and save it on a private and permissionless blockchain
- By providing information personal data without disclosing the actual data that proves it
- By protecting data that has been submitted on the internet using a cryptographic algorithm

19 Which characteristic of a blockchain network is also its protection? (1)

- The greater the number of full independent nodes, the harder it is to
- The lower the number of miners in the blockchain, the higher
- The more centralized the control of the blockchain is, the harder
- The more complicated the Proof of Work (PoW) algorithm is, the more

| | | | | |
|---|---|---|---|---|
| | compromise the data in the blockchain. | the incentive is for securing the network. | it is to secure the data and avoid fraud. | rewarding it is to secure the network. |

| | | | |
|---|---|---|---|
| 20 | | | In which scenario smart contract is the best solution to the problem. (1) |

| | | | |
|---|---|---|---|
| A bartender wants to force customers to pay for their drinks by transferring cryptocurrency to his wallet. | A chief financial officer wants her smart watch to notify her when her partner enters their front door. | An energy company wants to automatically buy power when the price reaches a predetermined rate. | An insurance company wants to pay out a farmer whenever the case manager feels it is best to do so. |

**2**

**Answer 5 out of 7 questions.**

Attempt any five.

| | | | | |
|---|---|---|---|---|
| 1 | | | Discuss the role of hashing in Blockchain. How does it ensure data integrity and security? | (5) |
| 2 | | | Illustrate with examples how Merkle Trees contribute to the immutability and integrity of blockchain data. | (5) |
| 3 | | | Write a note on Delayed Proof of Work and Delegated Proof of Stack. | (5) |
| 4 | | | Explain types of accounts and describe how private key and public address generated in Ethereum network? | (5) |
| 5 | | | What is smart contract? What are the benefits of smart contract? | (5) |
| 6 | | | Define Hyperledger, and draw the reference architecture services of Hyperledger and explain each component. | (5) |
| 7 | | | Define: i) Importance of nonce, ii) Process of mining, iii) Verification of transactions v) Difficulty level, vii) Consortium Blockchain. | (5) |

**3**

**Answer 5 out of 7 questions.**

Attempt any five.

| | | | | |
|---|---|---|---|---|
| 1 | | | Explain the concept of Asynchronous Byzantine Models of fault tolerance in the context of blockchain technology. | (5) |
| 2 | | | Describe Proof of Capacity and Proof of Burn. | (5) |
| 3 | | | Differentiate between public and private blockchains. Provide examples of each type and discuss their respective use cases. | (5) |
| 4 | | | How Invoke and Query works in Hyperledger for making the transaction. Explain with diagram. | (5) |
| 5 | | | Describe the role of endorsing peers in the transaction endorsement process of Hyperledger Fabric. How does it ensure transaction validity and integrity? | (5) |
| 6 | | | Discuss cases of Blockchain technology in the supply chain management. | (5) |
| 7 | | | Define: i) 51% attack ii) Sybil attack iii) Double-spending attack iv) Selfish Mining v) Zero-knowledge | (5) |

-----End-----