National University of Computer and Emerging Sciences, Lahore Campus

Course:	**Blockchain and Cryptocurrency**	**Course Code:**	**CS4049**
Program:	**BS (Computer Science)**	**Semester:**	**Spring-2023**
Duration:	**3 hours**	**Total Marks:**	**45**
Paper Date:	**29-May-2023**	**Page(s):**	**7**
Section:	**All sections**	**Weightage**	**45**
Exam:	**Final**	**Instructor:**	**Syeda Tayyaba Bukhari**

Student: Name: _____Roll No._____ Section_____

Instructions:

1. Make sure there are total **7 pages including title page**.
2. All questions are to be attempted on this paper. **Extra/Rough Sheets are NOT allowed.**
3. Understanding of questions is the part of the exam.
4. If there is any ambiguity in the paper, benefit will be given to students.

Question No.	1	2	3	Total
Total Marks	20	15	10	45
Obtained Marks				

DO NOT OPEN UNTIL YOU ARE TOLD TO DO SO…..GOOD LUCK 😊

Question 1: Choose the Best Answer. Write your choice in the table either A, B, C or D [20 marks]

Answer Section for Q1 (Any type of overwriting is not allowed):

1		11	
2		12	
3		13	
4		14	
5		15	
6		16	
7		17	
8		18	
9		19	
10		20	

1. What is the main benefit of blockchain technology?
   a) Increased transaction speed
   b) Centralized control over data
   c) Improved data security and integrity
   d) Lower energy consumption
2. What is a smart contract in the context of blockchain?
   a) A legally binding agreement between blockchain participants
   b) A digital certificate that verifies the identity of a user
   c) A private key used for encryption in blockchain networks
   d) A self-executing code that runs on the blockchain
3. What does immutability mean in the context of blockchain?
   a) The ability to modify data on the blockchain
   b) The capability to upgrade the blockchain protocol
   c) The permanence and inability to alter recorded data
   d) The feature that allows for anonymous transactions
4. What is a 51% attack in blockchain?
   a) A situation where more than half of the network nodes fail simultaneously
   b) A type of cybersecurity attack targeting blockchain wallets
   c) A scenario where an individual or group controls the majority of network computing power
   d) A protocol upgrade that introduces significant changes to the blockchain
5. How are new transactions added to a blockchain?
   a) By a central authority validating and adding the transactions
   b) Through a majority vote by network participants
   c) By conducting regular audits of the blockchain data
   d) By performing complex mathematical calculations (mining)
6. What is the purpose of a Merkle tree in a blockchain?
   a) To encrypt sensitive data on the blockchain
   b) To ensure the privacy of transaction information
   c) To store a compact representation of all transactions in a block
   d) To prevent double-spending attacks

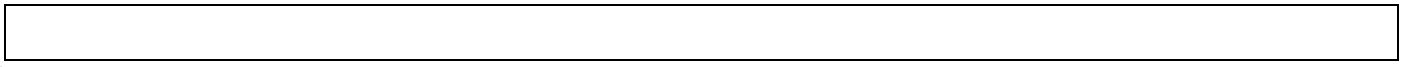
7. What is the purpose of a hash function in blockchain?
   a) To encrypt private keys
   b) To secure the blockchain against attacks
   c) To convert data into a fixed-size string of characters
   d) To validate smart contracts
8. What is the role of a miner in a proof-of-work blockchain network?
   a) Verifying transactions and adding them to the blockchain
   b) Creating new cryptocurrencies
   c) Facilitating peer-to-peer transactions
   d) Establishing consensus among network participants
9. What is the purpose of a timestamp in a blockchain transaction?
   a) To record the exact time when the transaction occurred
   b) To encrypt transaction data for enhanced security
   c) Both a and b
   d) To identify the transaction sender and receiver
10. What is a hard fork in the context of blockchain?
   a) A software update that introduces new features to the blockchain
   b) A temporary network interruption affecting blockchain transactions
   c) A consensus mechanism that requires multiple nodes to validate transactions
   d) A permanent divergence in the blockchain resulting in two separate chains
11. What is the purpose of a nonce in the mining process of a blockchain?
   a) To identify the block's position in the blockchain
   b) To ensure the privacy of transactions
   c) To prevent double-spending attacks
   d) To find a valid hash for the block
12. What is the purpose of the migrations directory in a Truffle project?
   a) It contains Solidity source files for smart contracts.
   b) It handles the deployment of smart contracts.
   c) It stores JavaScript and Solidity tests.
   d) It contains configuration files for Truffle.
13. How is the web3 object instantiated in the front-end code?
   a) By using the web3.currentProvider property
   b) By calling the enable() function of the ethereum object
   c) By creating a new instance of the Web3.providers.HttpProvider class
   d) By using the window.ethereum object
14. In context of PetShop Scenario: What is the purpose of the getJSON() function in the front-end code?
   a) It retrieves the pet data from the Ethereum blockchain.
   b) It requests access to the user's Ethereum account.
   c) It retrieves the contract artifact for the Adoption contract.
   d) It sends a transaction to adopt a pet.
15. IP spoofing is commonly used in which type of attack that tricks users into visiting a fake website and disclosing sensitive information?
   a) Loader Attacks
   b) Second-factor Authentication

c) Phishing Attack
d) Dictionary Attacks

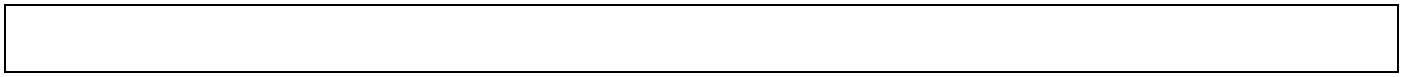
16. Which type of wallet provides the highest level of security?
    a) Hot wallet
    b) Cold wallet
    c) Exchange wallet
    d) Paper wallet
17. What is the purpose of a seed phrase in a cryptocurrency wallet?
    a) To generate public and private keys
    b) To recover the wallet in case of loss or theft
    c) To facilitate transactions on the blockchain
    d) To encrypt the wallet data
18. How are ICOs typically conducted?
    a) By selling tokens or coins to investors
    b) By issuing shares of a company
    c) Through traditional stock exchanges
    d) By offering dividends to shareholders
19. What is the purpose of a whitepaper in an ICO?
    a) To outline the technical specifications of a cryptocurrency
    b) To provide legal documentation for the ICO
    c) To summarize the investment potential of the ICO
    d) To describe the business plan and vision of the project
20. What lessons were learned from the DAO attack?
    a) The importance of centralized control in blockchain systems
    b) The need for better governance and code auditing in DAOs
    c) The irreversibility of blockchain transactions
    d) The limitations of smart contracts in decentralized systems

Question 2: [15 marks] Complete the below code.

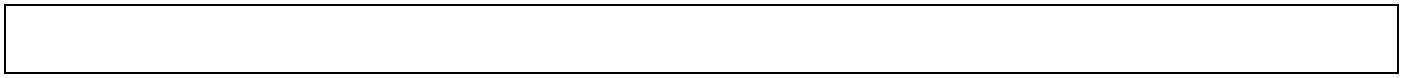
```
pragma solidity ^0.8.0;
contract Marketplace {
    struct Product {
        uint256 id;
        string name;
        uint256 price;
        address payable seller;
        bool isAvailable;
    }
    // Mapping to store products by their IDs
    mapping(uint256 => Product) public products;
    // Counter for generating unique product IDs
    uint256 public productCount;
    // Event emitted when a product is added to the marketplace
    event ProductAdded(uint256 id, string name, uint256 price, address seller);
    // Event emitted when a product is purchased from the marketplace
    event ProductPurchased(uint256 id, string name, uint256 price, address buyer);
    constructor() {
        productCount = 0;
    }
    // Function to add a new product to the marketplace
    function addProduct(string memory _name, uint256 _price) public {
        // Require that the price is greater than zero
```



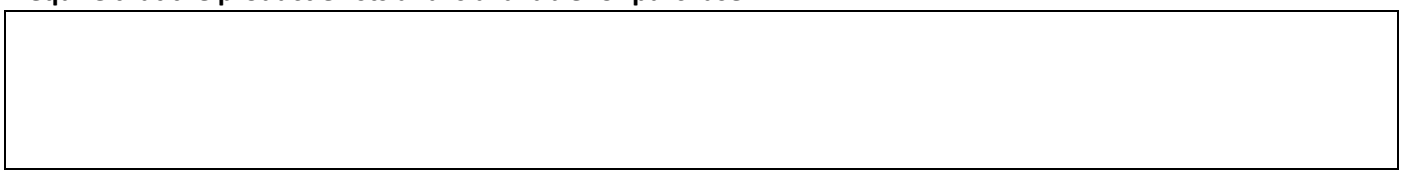
```
        // Increment the product count and assign the new ID
        productCount++;
        // Create a new product and store it in the mapping
```



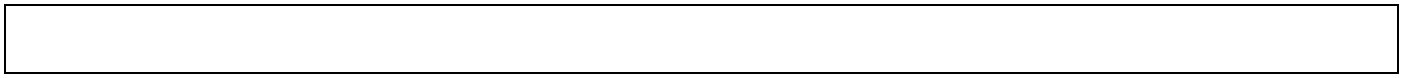
```
        // Emit the ProductAdded event
```



```
    }
    // Function to purchase a product from the marketplace
    function purchaseProduct(uint256 _id) public payable {
        // Retrieve the product based on the provided ID
        Product storage product = products[_id];
        // Require that the product exists and is available for purchase
```



```
        // Require that the buyer sends sufficient funds
```



```
        // Update the availability status of the product
```

```
        // Transfer the payment to the seller
        product.seller.transfer(product.price);
        // Emit the ProductPurchased event
    }
}
```

Question 3: (10 marks)

a. Describe a potential use case for blockchain in the music industry. **(4 marks)**

b. A blockchain network wants to introduce a new feature that requires changes to the underlying data structure of blocks and transactions. The new feature is not compatible with the existing protocol. Which type of fork, hard or soft, would be more suitable in this scenario (Just name, no description)? **(2 marks)**

c. Below are some scenarios in which you have to determine which characteristic/property/feature of blockchain technology is particularly beneficial. **Answers should be from one of these: (Decentralization, transparency, immutability, Digital Signatures) with precise explanation**

Scenario 1: (2 marks)
A consortium of banks wants to explore the potential of blockchain technology to streamline cross-border transactions and improve settlement times. Which characteristic of blockchain technology is particularly beneficial in this scenario?

Scenario 2: (2 marks)
A decentralized application (DApp) wants to ensure that its smart contracts can execute transactions in a reliable and deterministic manner. Which characteristic of blockchain technology addresses this requirement?