National University of Computer and Emerging Sciences, Lahore Campus

Course:	**Blockchain and Cryptocurrency**	**Course Code:**	**CS4049**
Program:	**BS (Computer Science)**	**Semester:**	**Fall-2022**
Duration:	**150 Minutes**	**Total Marks:**	**80**
Paper Date:	**27-12-22**	**Page(s):**	**10**
Section:	**All sections**	**Weightage**	**40**
Exam:	**Final**	**Instructor:**	**Syeda Tayyaba Bukhari**

Student: Name: ___________________________Roll No._____________ Section______

Instructions:

1. Make sure there are total 10 **pages including title page**.
2. All questions are to be attempted on this paper. **No extra Sheets are 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	4	5	6	7	Total
Total Marks	10	6	10	10	26	5	8	80
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 [10 marks]

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

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

1. A block in the blockchain can never have more than one parent block
   A. True
   B. False

2. Bitcoin is based on ……….. blockchain?
   A. Private
   B. Public
   C. Public Permissioned
   D. Permissioned

3. Blockchain forks can result in which of the following?
   A. Multiple Parent Blocks
   B. Multiple Children Blocks

4. In blockchain, blocks are linked:
   A. Backward to the previous block
   B. Forward to the next block
   C. Not linked with each other
   D. None of above

5. What is a node?
   A. A type of cryptocurrency
   B. A blockchain
   C. A computer on a blockchain network
   D. An exchange

6. Which data structure is used to record the order of transactions and then hashed?
   A. Red black trees
   B. AVL trees
   C. Hash tree
   D. Merkle trees

7. Which type of language is solidity?
   A. procedure oriented language
   B. object oriented language
   C. scripting language
   D. low level language

8. Ethereum is best suited for
   A. economic systems
   B. video creation systems
   C. website creation
   D. survey systems

9. Ether based own tokens can be launched on which Ethereum chains?
   A. public chains only
   B. private chains only
   C. Both public and private chains
   D. Both public and private chains

10. Which among the following is true with respect to EVM?
   A. It is designed for specific purposes
   B. ownerless virtual machine
   C. accepts any programming language
   D. its licensed

Question # 2: [4+2=6 marks]

	Name any Bitcoin blockchain network(chain) currently running on it
Draw a Diagram showing Soft Fork	
Draw a Diagram showing Hard Fork	

Question 3: [10 marks]

Complete the following functions highlighted in Bold.

```
 pragma solidity ^0.4.25;
contract MinnionFactory {
   // declare our event here
   event NewMinnion(uint minnionId, string name, uint dna);
   uint dnaDigits = 16;
   uint dnaModulus = 10 ** dnaDigits;
   struct Minnion {
      string name;
      uint dna;
   }
   Minnion[] public minnions;
   function _createMinnion(string _name, uint _dna) private {
      // and fire it here











   }

   function _generateRandomDna(string _str) private view returns (uint) {
      uint rand = uint(keccak256(abi.encodePacked(_str)));
      return rand % dnaModulus;
   }

   function createRandomMinnion(string _name) public {











   }

}
```

Question 4: [10 marks]

UTXOs:

Ali	-> Me	2.1BTC
Hassan	-> Me	3.01BTC
Usama	-> Me	6.3BTC
Hamza	-> Me	2.08BTC
Faiza	-> Me	0.9BTC
Ali	-> Me	1.1BTC
Amina	-> Me	1.08BTC

I want to buy a Car for 9.89 BTC and a bike tire worth of 4.05 with 0.72 traction fee.

Transaction:

Input:	**Output:**

Question # 5: Answer the following [4+2+5+2+2+2+2+7=26 marks]

	Answer:
Write two main security issues of programmable blockchain like Ethereum and how these issues are handled in Ethereum. **[4 marks]**	**Issues:** **1.** **2.** **Solutions to issues:** **1.** **2.**
Define Seed Phrase **[2 marks]**	
Write Signature API **[5 marks]**	

<table>
<tr><td><b>What are the drawbacks of PoW?
[2 marks]</b></td><td></td></tr>
<tr><td><b>What do you know about Ouroboros and Casper?
[2 marks]</b></td><td></td></tr>
<tr><td><b>Write names of any two consensus algorithm other than PoW and PoS.
[2 marks]</b></td><td></td></tr>
<tr><td><b>Write names of four crypto wallet attacks
[2 marks]</b></td><td>1.
2.
3.
4.</td></tr>
<tr><td><b>Write the abbreviations
[7 marks]</b></td><td><table>
<tr><td>IPO</td><td></td></tr>
<tr><td>nonce</td><td></td></tr>
<tr><td>ICO</td><td></td></tr>
<tr><td>PoS</td><td></td></tr>
<tr><td>DAO</td><td></td></tr>
<tr><td>PoB</td><td></td></tr>
<tr><td>PoW</td><td></td></tr>
</table></td></tr>
</table>

Question # 6: [5 marks]
Kashif wants to start his project of Amusement Park. Unfortunately, his initial Capital is low. How ICOs can help him to increase the capital for his project. What steps should he supposed to take?

Question # 7: Complete the following functions: [8 marks]

```
 pragma solidity 0.5.1;

contract MyContract {
    uint256 public peopleCount = 0;
    mapping(uint => Person) public people;
    address owner;
    modifier onlyOwner() {
    //make sure that Calle is owner



       }
    struct Person {
        uint _id;
        string _firstName;
        string _lastName;
    }
    constructor() public {
     //set calle’s address to owner



    }
    function addPerson(
        string memory _firstName,
        string memory _lastName
    )
        public
        onlyOwner
    {
        //update the people array
        incrementCount()



    }
    function incrementCount() internal {
        //increment count



    }
}
```