National University of Computer and Emerging Sciences, Lahore Campus

Course:	Blockchain and Cryptocurrency	Course Code:	CS4049
Program:	BS (Data Science)	Semester:	Fall-2023
Duration:	3 hours	Total Marks:	65
Paper Date:	30-December-2023	Page(s):	8
Section:	All sections	Weightage	50
Exam:	Final	Instructor:	Syeda Tayyaba Bukhari

Student: [redacted]

Instructions:

1. Make sure there are total **8 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	4	5	Total
Total Marks	10	10	10	15	20	65
Obtained Marks	10	9	7	15	18	59

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

0004

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	B
2	B
3	C
4	C
5	C

10

1. Which of the following statements best describes a blockchain?
   a) A centralized database maintained by a single entity.
   b) A decentralized, distributed ledger that records transactions across multiple computers.
   c) A peer-to-peer file sharing system.
   d) An encrypted messaging platform for secure communication.

2. What is the purpose of a cryptocurrency wallet?
   a) To mine new coins.
   b) To store private keys used to access and manage digital assets.
   c) To facilitate instant transactions.
   d) To act as a hardware device for crypto storage.

3. Which consensus mechanism is used by Bitcoin?
   a) Proof of Stake (PoS).
   b) Proof of Authority (PoA).
   c) Proof of Work (PoW).
   d) Delegated Proof of Stake (DPoS).

4. What distinguishes Ethereum from Bitcoin?
   a) Ethereum uses a different hashing algorithm.
   b) Ethereum focuses solely on privacy and anonymity.
   c) Ethereum allows for the creation of smart contracts.
   d) Ethereum has a fixed supply of coins.

5. What does "private key" refer to in the context of cryptocurrencies?
   a) The public address of a wallet.
   b) A unique code for identifying the blockchain network.
   c) A secret code granting access to one's cryptocurrency holdings.
   d) The transaction hash stored in the blockchain.

2: Complete the following functions: [10 marks]

```
ct Balance {
apping(address => uint256) public balanceOf;
mapping(uint => uint) private userBalances;

  function transfer (address _to, uint256 _value) {
      //Check if sender has balance and then add and subtract new balaces
```

require (msg.sender._value >0 && msg.sender.userBalances >_value ; "Wrong amount")

Balance [_to, userBalances+_value] // update balance of receiver

Balance [msg.sender, userBalances-_value] // update balance of sender

comment :-
// require check that sender has more than 0 balance and greater than the value transfered..

```
  function withdrawBalance (uint _value) public {
      //withdraw the required amount
```

msg.sender.
~~Balance~~.

require (_value >0 && _value <userBalances ;

"Insufficient amount")

msg.sender
new_amount = userBalances - _value

msg.sender,
Balance [userBalances] = [new_amount]

OR

Balance [msg.sender , userBalances-_value]

```
  }
```

comment
// first i check that value must greater than zero and also that value should less then actual balance

// then minus the amount from actuall amount which user want to withdraw

// then stored new_amount into user balance.

0004

Question 3: (10 marks)

Part a: Write Output of below goLang Code. If there is an error, mention the statement having error. (3 marks)

```
package main

import (
        "fmt"
)

func factorial(n int) int {
        if n == 0 || n == 1 {
                return 1
        }
        result := 1
        for i := 2; i <= n; i++ {
                result *= i
        }
        return result
}

func main() {
        // Example usage
        input := 5
        fmt.Printf("Factorial of %d is: %d\n", input, factorial(input))
}
```

Answer: Code

fmt.Printf line is wrong

we use println in golang to print anything

000

As a policymaker in a government office, describe how blockchain could revolutionize the way citizens access public services ting, identification, or land registry. **(2 marks)**

Blockchain is a temper proof and decentralized so no one can change its data, which is present in Block. Also Blockchain also hold anonymity so no one know anyone so no one can steal your identity because blockchain cannot be reverse (dehashed)

2

Part c: You're a customer support representative for a cryptocurrency wallet provider. Outline the steps you'd guide a user through to recover their funds in case they lose access to their wallet credentials or their device is lost/stolen. **(2 marks)**

If customer lose access to their wallet credentials or their device is lost

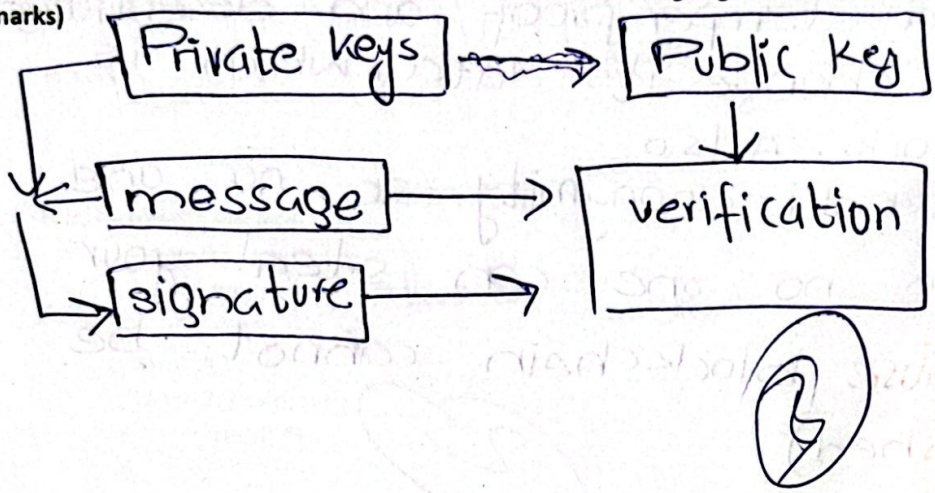
(i) wallet have multiple private keys, so if customer have any of them it can access to the wallet

(ii) if customer don't have any private key then every wallet have one master key so customer can access through master key

(iii) if customer don't have any Private or master then it might not possible to get access of wallet.

2

Part d: How digital Signature works? Draw the diagram ONLY of signing and verification process. No further explanation is needed (3 marks)



3

Question 4: [15 Marks]
Fill-in the below table:

Parameters	Bitcoin	Ethereum	Hyperledger
Cryptocurrency	Bitcoin	ether	None but we can make
Network	Public	Public	Permissioned
Consensus	POW	First POW Now POS	PBFT (Practical byzantine fault tolerance)
Smart Contract	No	(solidity) yes	yes (chaincode)
Language	C++	golang, python	golang, Java

5

0004

ion 5: [20 marks]

end of yours has DAPP running on his/her system. He /She sends you the whole code of DAPP. How can you execute at DAPP on your system having Linux platform?

A. **What tool(s) should you need? (Only mention names of tools not the Linux command to install that tools) [5 marks]**
B. **What steps should you perform? [7 marks]**
C. **What Linux command(s) should you execute? [8 marks]**

NOTE: You can write any assumption, if that assumption carries logical weight, you will be rewarded.

Steps :-

(i) I will download the code and place it into new folder

(ii) Open code folder in any compiler i-e VS code, vmware etc

(iii) Download all the packages and enviroment which needed to run DAPP in virtual env.

(iv) I will look into Ganache, if Ganache is install its good otherwise i will install it

(v) After Ganache, i will look into MetaMask extension if its install its good otherwise i install it

(vi) then i will make local host enviroment on metamask

(vii) Copying a key from metamask and paste into Ganache to connect

(viii) After all i will run code from my compiler

(ix) and at end i will perform some transaction to see all goes well or not i-e transaction is done or not

7

0004

Linux Commands :-

⇒ pip install npm
⇒ pip install truffle
⇒ import truffle
⇒ npm run dev
⇒ truffle migrate
⇒ truffle sol

Tools :-

⇒ Metamask
⇒ Ganache
⇒ Compiler to run (VS code, Vmware..)

Assumption

⇒ if we have to deploy our DAPP on server so we use Winscp or putty to transfer our code to server and assume we use AWS EC2 after sending all files we use Linux command to deploy our contract and after deploying we get p-address of our script and then that IP_address will integrated with our app to use block-chain service.