## **National University of Computer and Emerging Sciences, Lahore Campus**



Course: Blockchain and Cryptocurrency Course Code: CS4049
Program: BS (Data Science) Semester: Fall-2023
Duration: 60 Minutes 30

Duration:60 MinutesTotal Marks:30Paper Date:14-10-23Page(s):6Section:All sectionsInstructor:Syed

Section: All sections Instructor: Syeda Tayyaba Bukhari
Exam: Mid-I

Name:	_ Roll No	
-------	-----------	--

## Instructions:

- 1. Make sure there are total 6 pages including title page.
- 2. All questions are to be attempted on this paper. No extra Sheets are allowed
- 3. Understanding of question is the part of exam.
- 4. If there is any ambiguity in the paper, benefit will be given to students.

Question No.	1	2	3	Total
Total Marks	10	15	5	30
Obtained				
Marks				

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

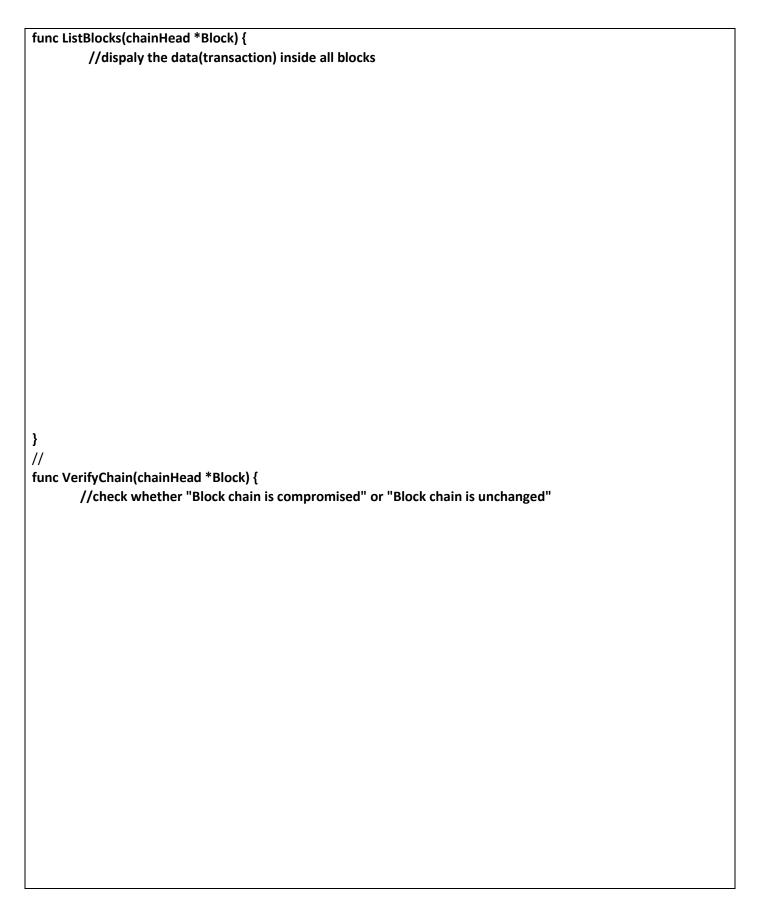
## Question 1: Choose the Best Answer. Write your choice in above table either A, B, C or D

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

1	
2	
3	
4	

- 1. What is a node?
  - A. A type of cryptocurrency
  - B. A blockchain
  - C. A computer on a blockchain network
  - D. An exchange
- 2. 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
- 3. We can modify the mining reward of traditional Bitcoin network by consensus (majority-based decision).
  - A. True
  - B. False
- 4. Is it possible to create a collision free hash function for hashing fixed length passcode for mobile devices?
  - A. No, it is possible to create collision resistant instead of collision free hash function
  - B. Yes, this can be done.
  - C. All above
  - D. None of above

```
Question 2: (15 marks)
Complete the three highlighted functions (You cannot change the signature of any function):
package Mid1
import (
        "crypto/sha256"
        "encoding/hex"
        "fmt"
)
// Block
type Block struct {
        transactions []string
        prevPointer *Block
        prevHash string
        currentHash string
}
//
func CalculateHash(inputBlock *Block) string {
        hash := sha256.Sum256([]byte(fmt.Sprintln(inputBlock)))
        return hex.EncodeToString(hash[:])
}
//
func ChangeBlock(oldTrans string, newTrans string, chainHead *Block) {
        //change transaction data inside block
}
```



}			

Question 3 (5marks)
What is nonce and how mining works? Cover all technical points to get full marks.