BRAC UNIVERSITY
Department of Computer Science and Engineering

Submission Deadline: **September 13, 2024**

Semester: Summer 2024
Full Marks: 25

CSE 446: Blockchain and Cryptocurrencies

Figures in the right margin indicate marks.

1. **What** cryptographic operations are used in Bitcoin? 2

2. **How** a valid owner can claim and spend their Bitcoin? 3

3. **Why** is only there 21M Bitcoin? Is it possible to increase the Bitcoin supply when all Bitcoins are mined? 1 + 2

4. **How** Bitcoin ensures a block is created in average in every 10 minutes? 2

5. Imagine you are creating a Bitcoin like system. **Explain** the features you would adopt from Bitcoin along with their justification. **What** changes would you make in your system and **why**? 5

6. **What** is the purpose of solving the PoW puzzle**? How** is it solved? **How** PoW is used to achieve consensus in Bitcoin? 1 + 2 + 2

7. Samples for a few transactions are given below. 1+1+1+2

Tx0	
ø	Amount: 5.25 To: Bob

Tx1	
Tx0[0]	Amount: 0.20 To: Bob
	Amount: 5.00 To: Alice
	Amount: 0.02 To: Carol

Tx2	
Tx1[1]	Amount: 1.00 To: Bob
	Amount: 3.99 To: Alice

Tx3	
Tx1[0]	Amount: 1.18 To: Bob
Tx2[0]	Amount: 0.11 To: Alice

Now **answer** the following questions:

a) **Who** are sending Tx1 and Tx2?

b) **Determine** the fee (if any) for Tx1 and Tx2.

c) **Justify** if Tx3 is a valid transaction.

d) **Show** the UTXO table after transactions Tx1 and Tx2.