End-Term Examination

CS577: Introduction to Blockchain and Cryptocurrency

Full Marks: 100 Time: 3 hours

(Make assumptions whenever necessary)

1. Choose the correct answer(s): **(10*1=10 points)**

a. Which of the following is first distributed blockchain implementation?

i. Bitcoin

ii. Ethereum

b. Bitcoin is based on ________ blockchain?

i. Private

ii. Public

iii. Public Permissioned

iv. Permissioned

c. Blockchain can be stored as which of the following?

i. A flat file

ii. A Database

iii. Both of the above

iv. None of the above

d. In blockchain, blocks are linked ________?

i. Backward to the previous block

ii. Forward to next block

iii. Not linked with each other

e. The primary benefit of immutability is

i. Scalability

ii. Improved Security

iii. Tamper Proof

iv. Increased Efficiency

f. Hash identifying each block in the Blockchain is generated using which of the following cryptographic algorithm?

i. SHA128

ii. SHA256

g. A block in the blockchain can never have more than one parent block?

i. True

ii. False

h. Where is the LEAST SAFE place to keep your cryptocurrency?

i. In your pocket

ii. On an exchange

iii. On a hot wallet

iv. At your work desk

i. Cold storage is

i. A place to hang your coat

ii. A private key connected to the Internet

iii. A private key not connected to the Internet
iv. A desktop wallet

j. A genesis block is
   i. The first block of a Blockchain
   ii. A famous block that hardcoded a hash of the Book of Genesis onto the blockchain
   iii. The first block after each block halving
   iv. The second transaction of a Blockchain

2. Define blockchain. Describe key characteristics of blockchain. Briefly describe the structure of a block in bitcoin blockchain. What are coinbase-transaction and locktime in bitcoin blocks?

(2+4+5+4=15 points)

3. Describe all the steps which take place in bitcoin-network starting from the initiation of a transaction to its commit into the blockchain. Compare PoW, PoS and DPoS.

(10+6=16 points)

4. How are the membership and non-membership of an element in a given Merkle Tree determined? Why there is a need to change the difficulty level in PoW? Explain Hard fork and Soft fork in bitcoin blockchain with suitable example in each case.

(4+2+4*2=14 points)

5. Describe any FIVE: **(5*5 =25 points)**
   a. Proof of burn,
   b. Pay-to-script-hash,
   c. Pay-to-MULTISIG vs. Secret Sharing,
   d. Fully-validating Nodes Vs. Thin Clients,
   e. Public Vs. Private Vs. Consortium Blockchain.
   f. Smart Contracts

6. How does bitcoin network deal with the following attacks? **(4*5=20 points)**
   a. Double-spend attack.
   b. Denial of service attack,
   c. Forking attack,
   d. Block-withholding attack.