Printed Page:- Subject Code:- AMTAI0214

Roll. No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA

(An Autonomous Institute Affiliated to AKTU, Lucknow)

M.Tech.

SEM: II - CARRY OVER THEORY EXAMINATION - JUNE (2021 - 2022)

Subject: Introduction to Blockchain

Time: 3 Hours Max. Marks: 100

General Instructions:

1. The question paper comprises three sections, A, B, and C. You are expected to answer them as directed.
2. Section A - Question No- 1 is 1 marker & Question No- 2 carries 2 mark each.
3. Section B - Question No-3 is based on external choice carrying 4 marks each.
4. Section C - Questions No. 4-8 are within unit choice questions carrying 7 marks each.
5. No sheet should be left blank. Any written material after a blank sheet will not be evaluated/checked.

SECTION A 15

1. Attempt all parts:-

1-a. Blocks hold batches of valid transactions that are hashed and encoded into a? (CO1) 1

(a) merkle tree

(b) cryptographic hash

(c) genesis block

(d) temporary fork

1-b. When encrypting a message with the public key, which key is required to decrypt the message? (CO2) 1

(a) Both Public key and Private key

(b) Private Key

(c) Public Key

(d) Inverted Public Key

1-c. The synchronous consensus technique(s) is (are): (CO3) 1

(a) PAXOS

(b) RAFT

(c) Byzantine General Model

(d) All of the above

1-d. In Ethereum, which algorithm is applied to the private key in order to get a unique public key? (CO4) 1

(a) RSA

(b) SHA 256

(c) ECC

(d) Keccak

1-e. What is miner? (CO5) 1

(a) A cryptographic algorithm

(b) A secured distributed ledger

(c) A person doing calculation

(d) Computers that validate and process blockchain transactions

2. Attempt all parts:-

2.a. What do you mean by Distributed Consensus? (CO1) 2

2.b. Explain Zero Knowledge systems in detail. (CO2) 2

2.c. How is PoW better than PoS? (CO3) 2

2.d.	What are the components of Block chain architecture? (CO4)	2
2.e.	What are the limitations of Smart Contracts? (CO5)	2

SECTION B 20

3. Answer any five of the following:-

3-a.	How is RSA used to create digital signature? (CO1)	4
3-b.	What is Merkle tree? Discuss its properties. (CO1)	4
3-c.	Discuss the properties of hash functions.(CO2)	4
3-d.	Is it possible to modify the data once it is written in a block? Explain.(CO2)	4
3.e.	What are the key requirements for a consensus algorithm? (CO3)	4
3.f.	Differentiate Between Public, Private and hybrid Blockchain. (CO4)	4
3.g.	What is a node in Ethereum? How can you connect with a node? (CO5)	4

SECTION C 35

4. Answer any one of the following:-

4-a.	How is Blockchain distributed ledger different from a traditional ledger? (CO1)	7
4-b.	What are the different types of Blockchain? Explain in detail. (CO1)	7

5. Answer any one of the following:-

5-a.	What is message digest and which key of PKI is used to sign it ? (CO2)	7
5-b.	What is SHA-256? Explain with an algorithm. (CO2)	7

6. Answer any one of the following:-

6-a.	How proof of work based blockchain network defers attacks? (CO3)	7
6-b.	Explain Paxos consensus for permissioned block chain .(CO3)	7

7. Answer any one of the following:-

7-a.	Describe in detail the components of Hyperledger Fabric. What are the security and privacy controls provided by hyperledger fabric? (CO4)	7
7-b.	Explain the mining principle behind bitcoin and Ethereum.(CO4)	7

8. Answer any one of the following:-

8-a.	Elaborate following designs limitations imposed on smart contracts: (CO5) a)Sequential Execution b)Deterministic Execution.	7
8-b.	Discuss how smart contracts developed with blockchain that can be used to achieve crowd funding platform. (CO5)	7