B3.E9-R5 : BLOCKCHAIN TECHNOLOGY

NOTE :
1. **Answer Question 1 and any FOUR Questions from 2 to 7.**
2. **Parts of the same question should be answered together and in the same sequence.**

Total Time : 3 Hours   **Total Marks : 100**

1.   (a)   What are the three pillars of blockchain ?

     (b)   What is a trapdoor function, and why is it needed in blockchain development ?

     (c)   What is a chain fork ?

     (d)   What is traffic padding and what is its purpose ?

     (e)   Explain the difference between Proof-of-Work and Proof-of-Stake.

     (f)   Briefly explain about Practical Byzantine Fault Tolerance (PBFT) mechanism.

     (g)   What is double spending ?   **(7x4)**

2.   (a)   Compute the bits number 1, 16, 33, and 48 at the output of the first round of the DES decryption, assuming that the ciphertext block is composed of all ones and the external key is composed of all ones.

     (b)   Draw a matrix that shows the relationship between security services and attacks.

     (c)   What Front-End Technologies are required for standard blockchain implementations ? Briefly explain about them.   **(9+5+4)**

3.   (a)   How is blockchain helpful for e-commerce ?

     (b)   Differentiate between a public and a private blockchain.

     (c)   Explain what constitutes a blockchain network, including the main property of that network.

     (d)   Discuss how problems with scaling and interoperability affect wider blockchain utilization.   **(5+5+4+4)**

4.   (a)   How do public blockchains ensure the adherence of transaction and block-writing rules ?

     (b)   Discuss the need for predefined mechanisms and rules to modify a public blockchain's protocols.

     (c)   Compare and Contrast Centralized and Distributed Systems. What are the disadvantages of Centralized and Distributed Systems ?   **(6+6+6)**

5. (a) What are the vulnerabilities of a smart contract ?

(b) Why do we need Ganache for Ethereum development ?

(c) What is a DAO? How did the DAO get hacked? How was the DAO hack resolved ?

(d) Differentiate between Blockchain and Hyperledger.

(5+5+4+4)

6. (a) What are function modifiers in Solidity? Explain the most widely used modifiers with examples ?

(b) What is the Ethereum Virtual Machine (EVM)? Is the EVM decentralized ? How does it work ?

(c) Differentiate between Ethereum and Bitcoin.

(6+6+6)

7. (a) What are the components of a blockchain architecture ?

(b) Explain the characteristics of the blockchain applications known as "DApps".

(c) Why do some cryptocurrencies use "Merkle Trees" ?

(6+6+6)

- o 0 o -