**PES University, Bengaluru**
(Established under Karnataka Act No. 16 of 2013)

December 2020: End Semester Assessment
B.TECH. VII Semester Elective CSE
UE17CS414: Blockchain Technologies

Time: 180 Mins | Answer All Questions | Max Marks: 100

| Q. N. | | Questions and scheme | Marks |
|---|---|---|---|
| 1 | a. | Define the immutable property of the blockchain. With the help of Markle tree structure, explain the organization of transactions in a block. | 7M |
| | b. | Explain the blockchain construction with the cryptographic functions and the structure of a block. | 7M |
| | c. | Assume that, a hospital XYZ is planning to replace the existing data storing and management system with blockchain. So, analyze and describe the design and tell how effective it will be with some advantageous? | 6M |
| 2 | **a.** | Assume that the blockchain is using 256 bits hash function, M is the input message and H(M) is the output message digest. Explain three important properties of this hash function by considering above given input and output with an example. | 6M |
| | b. | In a blockchain, there exist 10 peers. Among 10 peers Alice and Bob acting as miners. Both collected same set of transactions and mined separate blocks. If both attached their blocks to blockchain, how these two blocks uniquely identified? If they implement digital signature, then how to reduce the signature size? Explain the mechanism. | 7M |
| | **c.** | Suppose john wants to encrypt email messages before sending them to friends. The RSA Encryption Scheme is often used to encrypt and then decrypt electronic communications. John wants to set up his own public and private keys. He chooses p = 23 and q = 19 with e = 283. Find d so that ed has a remainder of 1 when divided by (p − 1)(q − 1). | 7M |
| 3 | **a.** | Analyse Proof of Stake, Proof of Burn and Proof of capacity and justify which is efficient consensus. | 6M |
| | b. | Consider there exist blockchain network with 6 number of nodes, this system is using RAFT consensus algorithm. While electing leader node, two nodes A and B send Request vote message with term 21 at the same time. So which mechanism will be used to elect leader? Following shows the state of the node logs:<br>A: 1.1, 2.1<br>B: 1.1, 3.1, 3.2<br>B: 1.1, 1.2<br>D: 1.1<br>E: 1.1, 3.1 | 7M |

| | | | |
|---|---|---|---|
| | | F:1.1,2.1,3.1<br>Here 1.2 represents the 2nd log from the 1st term. If the system is searching for a new leader,then is there any chance of committing the transaction of 1.2 in future? Among these nodes 2 nodes get failed. How the system will manage this failure? If your system identifies that the leader is Byzantine, then what will the system do now? | |
| | c. | In a system, a client sends a request to invoke a service operation to the primary. The primary multicasts the request to the backups, the backups execute the request and send a reply to the client and the client waits for replies from different backups with the same result. In this scenario the system is using which consensus? If the primary node is byzantine, how will the system work? How does it differ from Byzantine Fault Tolerance? | 7M |
| 4 | a. | What is smart contract? How does it provide trust? Differentiate it from centralized crowd funding platform? | 6M |
| | b. | How Decentralized Application (DApp) fit in the real world? Explain with an example. | 6M |
| | c. | Explain the basic transaction flow of Hyperledger fabric with different nodes with Hyperledger architecture. | 8M |
| 5 | a. | How will you achieve confidentiality, integrity, and availability with blockchain solution? | 6M |
| | b. | List and explain the various stages involved in cyber-kill chain. | 6M |
| | c. | List any five attack surfaces on blockchain and discuss any five attacks that can exploit smart contract vulnerabilities. | 8M |