SRN □□□□□□□□□□□□

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

UE18CS324

## DECEMBER 2020: END SEMESTER ASSESSMENT (ESA) B TECH V SEMESTER

## UE18CS324 - BLOCKCHAIN

| | | |
|---|---|---|
| Time: 3 Hrs | Answer All Questions | Max Marks: 100 |

| | | | |
|---|---|---|---|
| 1 | a) | How can you identify a block in blockchain? Explain with structure and content of each block. | 8M |
| | b) | How a Blockchain distributed ledger different from a traditional ledger? | 6M |
| | c) | Assume the implementation of blockchain for GST collection and write any three advantageous and one disadvantage. | 6M |
| | | | |
| 2 | a) | Suppose Ram wants to encrypt email messages before receiving them from his friends. He started using RSA Encryption Scheme to encrypt and then decrypt electronic communications. Ram set up his own public and private keys and broadcasted them to his friends. He had message of 20 and chosen p = 11 and q = 3 with e = 3 and d=7. Illustrate e-mail exchange with plain text and cipher text conversion. | 8M |
| | b) | What is Merkel Tree? What is the need for the Markle tree in blockchain? How hash code will be processed? Explain with one example. | 6M |
| | c) | How the digital signature is created and verified? Explain with any scenario. | 6M |
| | | | |
| 3 | a) | Consider the blockchain network with 8 nodes using the RAFT consensus algorithm. While electing leader node, two nodes A and B send Request vote message with term 23 at the same time. So which mechanism will be used to elect a leader? Following shows the state of the node logs:<br>A: 1.1, 4.1<br>B: 1.1, 3.1, 3.2<br>C: 1.1, 1.2<br>D: 1.1,3.1<br>E: 1.1, 4.1<br>F: 1.1,2.1,4.1<br>G: 1.1,2.2,3.2<br>H: 1.2,3.2,3.4<br>If the system is searching for a new leader, then is there any chance of committing the transaction 1.2 of the 3rd log in the future? Among these nodes, if three nodes behaving maliciously, then how the system will manage this failure? If your system identifies that the leader is Byzantine, then what will the system do now? | 8M |

SRN

| | | | |
|---|---|---|---|
| | b) | Say, three independent miners propose the following three blocks (containing the transactions enclosed in [])<br>B1=[T91, T92, T93, T94],<br>B2=[T88,T89,T91], and<br>B3=[T88, T89,T91,T92,T93].<br>Considering the consensus algorithm is Proof of Work (PoW). Once the network achieves consensus, which of the following blocks is likely to get added to the main chain, given the last block in the blockchain has transactions T86, T87 and T90? | 3M |
| | c) | Suppose in a distributed network, running Paxos as the underlying consensus algorithm, has 3 proposers and 5 acceptors and 1 learner. Say, 3 of the acceptors have failed, which of the following is true about the network? | 3M |
| | d) | Considering the Proof of Elapsed Time (PoET) adapted in Hyperledger Sawtooth framework, what mechanism is used to ensure that the miner (or block leader) is a legitimate participant and not an attacker and has waited for the random amount of time assigned by the network? Define the concept of Proof of Elapsed Time (PoET) with an example. | 6M |
| | | | |
| 4 | a) | How smart contract can be considered as logically behaved algorithm? And What is the logic behind the one size fits all smart contracts? | 6M |
| | b) | Differentiate between the Decentralized Autonomous Organization and Traditional Organizations. | 6M |
| | c) | With the help of neat diagram, explain the Hyperledger fabric V1 architecture. | 8M |
| | | | |
| 5 | a) | What are the attack vectors on the smart contract? List any four vulnerabilities on smart contract virtual machine. | 7M |
| | b) | Discuss any five attacks that can exploit vulnerabilities on blockchain network. | 5M |
| | c) | List any three challenges with current DNS and explain any 2 blockchain frameworks which provides solution for these challenges. | 8M |