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

UE18CS324

OCTOBER 2020: IN SEMESTER ASSESSMENT B Tech 5 SEMESTER
TEST – 1
UE18CS324 (4 credit) – BLOCKCHAIN

Time: 2 Hrs	Answer All Questions	Max Marks: 60

1.	a	Define Blockchain with Key features.	3
	b	Assume that, A hospital XYZ is planning to replace the tradition systems with blockchain. So, analyze and tell how effective it will be with some advantageous?	4
	c	In a company, they want to replace current system with blockchain. To be part of this network, certain nodes don't have the more computational requirement and storage capacity. So, how can they take part in blockchain? What is your suggestion?	3
2.	a	Define the immutable property of the blockchain. How the transactions in a block will be organized?	5
	b	Explain blockchain construction and the structure of a block.	5
3.	a	Assume the blockchain with 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 with by considering given input and output.	3
	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?	3
	c	How to reduce the signature size? Explain the mechanism.	4
4.	a	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 $(p - 1)(q - 1)$.	5
	b	Alice perform asset transfer from bank A to Bank D, He would like to track his asset transfer path between Bank A to Bank D. His application is using blockchain to perform this. Which blockchain model will help Alice to track his asset transfer.	2
	c	What is the nonce and how is it used in mining?	3
5.	a	Write any three difference between Proof of Work and Proof of Elapsed time	6
	b	Analyze Proof of Stake, Proof of Burn and Proof of capacity and justify which is	4

		efficient consensus.	
6	a	Consider there exist blockchain network with 6 numbers of nodes. This system 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: A: 1.1, 2.1 B: 1.1, 3.1, 3.2 B: 1.1, 1.2 D: 1.1 E: 1.1, 3.1 F:1.1,2.1,3.1 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?	5
	b	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, The client waits for replies from different backups with the same result. N this scenario the system is using which consensus? If the primary node is byzantine, how the system will work? How it differs from BFT?	5