SRN | | | | | | | | | | | | |

PES University, Bangalore

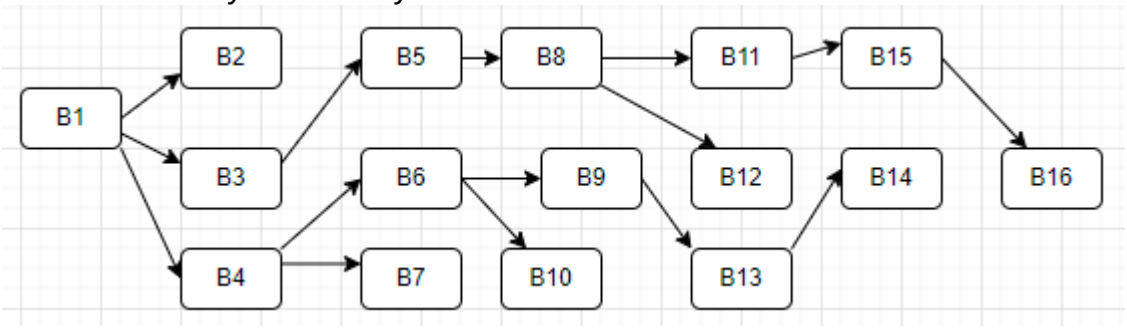
(Established under Karnataka Act No. 16 of 2013)

UE19CS335

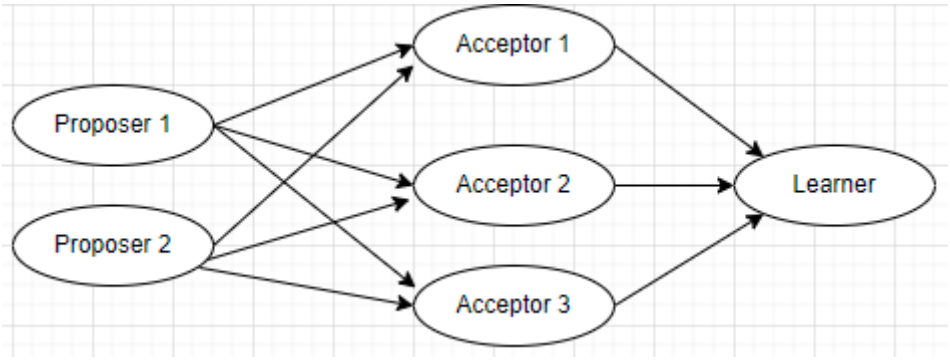
END SEMESTER ASSESSMENT (ESA) B.TECH. 6Th SEMESTER-Jan-May 2022

UE19CS335- Blockchain

Time: 3 hours | Answer All Questions | Max Marks: 100

1.	a	What is the need of blockchain technology? Can blockchain be used for any application? Give some myths that are common with respect to blockchain.	**5**
	b	Give the difference between: i. Full nodes and light weight nodes ii. Transparency and immutability	**5**
	c	i. What is the role of public leger and P2P network in blockchain? Explain with an example. ii. What do you mean by soft forks? Given below a blockchain:  I. When a block Bx has to be inserted, where will it get inserted? II. What are orphaned blocks here?	5+5 =**10**
2.	a	What is difference between symmetric and asymmetric key cryptography? Why symmetric key cryptographic algorithms cannot be used in a blockchain setup?	5
	b	Let us assume that Alice wants to give 10 bitcoins to bob. Alice (public key: Pu_A; private key: Pr_A) initially has 20 bitcoins and bob (public key: Pu_B; private key: Pr_B) has 10 bitcoins. Give a step-by-step procedure how this transaction can be made between them, considering two important factors: encryption/decryption and authenticity. Please note: representation of transaction with authenticity should be given in terms of keys.	5
	c	i. Discuss any two hash function properties with example. ii. What are the steps of joining a node to the bitcoin network? Explain with proper diagrams.	5+5 = **10**
3.	a	What do you mean by distributed consensus? What is the limitation of distributed consensus with respect to blockchain?	5
	b	Consider one organisation *"ABC"*, who supports Proof of work and another organisation *"XYZ"*, who supports Proof of stake. How *ABC* can prove to *XYZ* that proof of work is better that proof of stake. Are these fault tolerant algorithms?	5

SRN | | | | | | | | | | | | |

	c	i. Give the difference between: proof of authority and proof of elapsed time. ii. Consider a scenario from PAXOS:  What will happen if (consider each scenario independently, for example, ii question's answer is not dependent on i question's answer): I. Proposer 1 crashes II. Proposer 2 crashes III. Both proposer 1 and 2 crashes IV. Acceptor 2 crashes V. Learner crashes	5+5 =10
4.	a	What are the benefits of using smart contracts? Give an example with respect to any application where the working of smart contract can be explained.	6
	b	Explain different types of DAPPs. Give an example of each.	6
	c	What do you mean by channel in Hyperledger fabric? Explain the different steps of making a transaction in Hyperledger fabric architecture.	8
5.	a	Explain any three smart contract attacks.	6
	b	Give any two DDOS attack targeting server resources.	6
	c	What do mean by selfish mining? Explain with an example.	8