## Department of Computer Science and Engineering -SVNIT, Surat

## Mid Semester Examinations, September 2022

[U19CSO12]

## B Tech IV(CSE) - Semester VII Course: Blockchain Technology (CS467)

Date: 27-Sep-2022 Time: 2:00 PM - 3:30 PM Marks: 30

Instructions: 1. Answer all questions. 2. Figures to the right indicate max. marks. a) List and discuss role of Cryptographic Security primitives used in Blockchain? QA [4] b) Answer the following (Any three) [6] 1. Explain Bitcoin difficulty adjustment. 2. How crypto-currencies are different than Fiat currencies? 3. Give your comments on Bitcoin energy usage. 4. Discuss Forks in blockchain. 5. List design properties of Blockchain and their technology implications. Q.2 a) Answer the following (Choose only one correct answer out of A,B,C,D) [2] 1. What is genesis block? A. The first transaction of a blockchain B. The first block of a blockchain C. The last block of a blockchain D. A block created by Founder 2. What is the coinbase blocke reward for miners currently in Bitcoin blockchain. A. 6.25 BTC B. 12.5 BTC C. 25.00 BTC D. 50.00 BTC 3. Which of these fields is present in Bitcoin Blockchain summary? A. Gas limit B. Difficulty C. Private key of Sender D. None of the above 4. What is the smallest denomination of crypto-currency ether? A. Satoshi B. Wei C. Uni D. Luna b) Answer in detail - any two. [8] 1. Discuss DeFi and NFT. 2. Compare Bitcoin and Ethereum – as currency, as blockchain, and transaction components. 3. What is Mining and what is Validation? Discuss Proof of Work and Proof of Stake. Q.3 a) Answer any one of the following [5] 1. For an elliptic curve  $y^2 = x^3 + ax + b$ , prove that Sum of the roots have to be equal to negative coefficient of x<sup>2</sup>. 2. For an elliptic curve  $E: y^2 = x^3 - 25x$  perform following operations i. For points  $P = (x_1, y_1) = (0,0)$  and  $Q = (x_2, y_2) = (-5,0)$ , find  $P + Q = (x_3, y_3)$ ii. For point  $P = (x_1, y_1) = (-4,6)$ , find  $2P = (x_2, y_2)$ b) Answer any two. [5] V. Explain Merkle tree and its advantages in context of the Blockchain technology. 2. Explain properties of hash function. 3. Discuss smart contracts and their advantages.