**Birla Institute of Technology & Science, Pilani**

**Work-Integrated Learning Programmes Division**

**First Semester 2022-2023**

**Mid-Semester Test (EC-2 Regular)**

Course No. : SE ZG569

Course Title : BLOCKCHAIN TECHNOLOGIES & SYSTEMS

Nature of Exam : Open Book

No. of Pages = 1

# No. of Questions = 10

Weightage : 30%

Duration : 2 Hours

Date of Exam : Sunday, 25/09/2022 (AN)

Note:

1. Please follow all the *Instructions to Candidates* given on the cover page of the answer book.
2. All parts of a question should be answered consecutively. Each answer should start from a fresh page.
3. Assumptions made if any, should be stated clearly at the beginning of your answer.
4. Give the example of three different industries that can leverage the potential of blockchain technology to improvise some aspect of their business and how? [3]
5. Discuss the blockchain technology with respect to following terms: leader, cryptography, cryptocurrency, consensus mechanism, scalability, cost and software development. [3]
6. Discuss the various aspects of decentralization in BITCOIN? [3]
7. Describe at least three different security features of a cryptographic hash function and provide examples for each one of these feature. [3]
8. Give at least three reasons with explanation to demonstrate why reaching consensus in a decentralized system is hard? [3]
9. In bitcoin while trying to add a block to the blockchain whether all minors solve the same puzzle. (Justify) Discuss about some built-in limitations to the Bitcoin protocol, and why it’s challenging to improve them. [3]
10. What are some ways to burn bitcoins, i.e., to make a transaction unredeemable? Which of these allow a proof of burn, i.e., convincing any observer that no one can redeem such a transaction? [3]
11. Scalability is one of the major issues with blockchain. Discuss the reasons for this problem and various techniques that can be applied to make blockchain-based solutions more scalable. Critically analyse your answer for scalability in terms of number of nodes, throughput, size of the block, etc. [3]
12. For digital money to be useful, it needs to be transferable. The transfer of money on a blockchain is initiated by the owner, creating a transaction. This transaction informs the network about how much money is changing hands and who the new owner is. UTXO and account based are two most commonly used accounting models used in blockchains.
13. Describe the working of both the model.
14. Mention the similarities and difference between the two models
15. Compare the two models with respect to different performance criterions. [3]
16. In order to prove “Transaction B” and Transaction D are part of the following merkle tree. What all hashes are required to be sent by the prover to the verifier in addition to transaction B and Transaction D itself. [3]

