

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST-3 EXAMINATIONS-2023

B.Tech-VIII Semester (BI/BT)

COURSE CODE (CREDITS): 19B1WCI839

MAX. MARKS: 35

COURSE NAME: Foundation of Blockchain

COURSE INSTRUCTORS: Dr. Amit Kumar

MAX. TIME: 2 Hours

*Note: All questions are compulsory. Marks are indicated against each question in square brackets.*

- Q1. [CO4] i. Blockchain is designed to work with limited data due to huge computation requirements but we are also using it in many heavy loaded applications and that can create an issue of scalability. Now you will mention at least one approach to address the same. [3]
- [CO3] ii. In the blockchain network broadcasting messages with the peer nodes is the only way to have communication, because each node should get the current state of the ledger as soon as possible. Mention the details of the layered approach that the blockchain network used for communication. [3]
- Q2. [CO2] i. Generally, two category of cryptography is used for the security purposes. Mention both categories and differentiate them with their benefits and limitations. [3]
- ii. Game theory is playing a vital role in the blockchain to achieve consensus among nodes via setting some difficulty target. So, what is this difficulty target and how it can be achieved with proper example. [3]
- Q3. [CO4] i. Blockchain is one of the most disruptive technologies in decentralized nature. So, mention the steps that are involved in discovery of a network for a new node when it wants to join the network. [3]
- [CO5] ii. Many miners are working to solve a given puzzle and more than one may propose a block in the network then how a network will ensure that only single chain of blocks will be considered as a part of extended blockchain. [3]
- [CO7] iii. Describe the various Bitcoin transactions with pictorial description of each of them. [3]
- Q4. [CO7] The main problems in Bitcoin are validating a transaction in a faster way because it is required to check all the previous blocks. So, what strategy the Bitcoin uses to make perform validation efficiently. Moreover, a light node can verify a given transaction without storing the up-to-date ledger state, How? [7]
- Q5. [CO6] Recently, data encryption standard is not accepted due to its design faults. Mention the algorithm that actually utilized for providing security over the communication with its encryption and decryption process with all of its components. [7]