

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATIONS-2022

B.Tech-VIII Semester (CS/IT/ECE/Civil/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. i. A blockchain network is decentralized in nature then discuss some perspectives to design a system corrected based on the requirements. Also provide a suitable example for each of the perspective that you would like to mention. [3]
- ii. The blockchain network communicates by broadcasting messages from one peer to another peer so that each node will receive the intended message. Now, give the details of the layered approach that the blockchain network used for communication. [3]
- Q2. i. Broadly, there are two kinds of cryptography, mention each of them with their benefits and limitations in a tabular format. [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. i. Blockchain is one of the most disruptive technologies as of today. But due to its decentralized nature it requires a huge computation as in Bitcoin to propose a block of valid transactions through proof of work. Provide some other consensus algorithm that is quite popular without burning a lot electricity and computation power. [3]
- ii. [3]
- iii. Any miner has capability to propose a block in the network then how a network will always have a single chain of blocks. [3]
- iv. [3]
- v. Describe the block structure of Bitcoin blockchain with suitable description of each structure. [3]
- Q4. One of the main issues in Bitcoin is validating a transaction efficiently because one needs to check all the preceding blocks and its hashes to verify. So, which way Bitcoin used to make this kind of validation efficient and even a light node can also perform validation for a given transaction without storing the up-to-date ledger state with sufficient details? [7]
- Q5. Nowadays, DES is not very much popular due to its inherent weaknesses. Provide the reason behind it in points and which algorithms replaced the DES. Also provide the encryption and decryption process with all of its components. [7]