

Jaypee Institute of Information Technology, Noida (U.P)

Test-1, Examinations 2020-21

B.Tech, VI Semester

Course Title: Introduction to Blockchain Technology

Course Code: 21B12CS317

Maximum Marks: 20

Time :01Hr

Note:

- 1) This a paper and pen examinations. Answers has to be written on papers only in your own handwriting. No answers has to give on the google form.
- 2) On the top of your answer sheet, write your Name, Enrollment No., Batch, Date of Examination, Course name, Course Code.
- 3) Answers should be uploaded collectively at the end of Examination.

Q1. The concept of distributed ledgers was introduced way back in 1990's. Still the actual online P2P cash transfer system was not realized till 2009. What were the major 5-6 reasons for this and how were these issues resolved with advent on bitcoin. [CO1, Marks-4]

Q2. Confidentiality and non-repudiation are two major concerns for a P2P system. Which algorithms can be used to achieve these 2 factors? How can one achieve both these factors in a single go. Is it possible that both these factors contradict each other in some scenario? [CO2, Marks-4]

Q3. What is the meaning of having n number of zeros in front of hash value of a block? How does these zeros signify or validate that the miner who mined this block is not malicious and the block mined by him can be accepted in main chain. [CO3, Marks-4]

Q.4 There is a blockchain having a new block added in every 5 minutes with 500 transactions in each block. There are 20 users in the network out of which 4 are active miners. Right now there are 10 blocks in the chain. A hacker wants to update a transaction in second block. What all is required to be done by him. Explain in steps in short. [CO3, Marks-2]

Q5. There is a block with 500 transactions. The transactions are stored in merkle tree. How can you validate the transactions (in terms of double spending) using the Merkle root hash? [CO2, Marks-2]

Q6. Who is paying the rewards to the miners for the mining procedure and on what basis the new bitcoins are created? [CO1, Marks- 2]

Q7. What is the use of avalanche effect in bitcoin transactions? Does it help in keeping the transactions tamper free? [CO2, Marks-2]