Indian Statistical Institute

Semestral Examination
M.Tech.(CrS)-II, 2025-26

Blockchains & Cryptocurrencies

Date: 19.11.2025 **Duration: 3 hours** **Maximum marks: 100**

Only precise and to the point answer will get full mark(s).

1. (a) Define Byzantine Agreement and Byzantine Broadcast. Show that they are equivalent. [6 + 8]

   (b) Write the time and message complexity of the Dolev-Strong's Byzantine Broadcast protocol. [6]

   (c) In the "vote" protocol discussed in class, prove that if any honest node outputs a bit b, then every other honest node outputs either b or $\perp$. [5]

2. (a) Write the structure of a Bitcoin block, describing each of its components. [6]

   (b) Explain the concept of Proof of Work (PoW) in Bitcoin. How does PoW secure the Bitcoin network, and why is it necessary for reaching consensus? [10+5]

   (c) Explain Proof of stake and the key comparison with PoW. [10]

   (d) Suppose Alice wants to buy a car from Bob. Bob waits for 6 confirmations on a Bitcoin payment before transferring the car to Alice. Describe how a majority attacker (i.e., more than 51%) can execute a double spend attack on Bob. [6]

   (e) Suppose the miners decide which transactions to include in the current block to be mined based on the transaction fee. The higher the transaction fee, the greater the chances of being included in the block. Thus, the transaction fees depends on the transaction queue size; if the queue is large, users in a hurry may pay a higher fee to ensure their transaction is processed quickly. An easy way (for a malicious user) to increase the transaction fee is to create dummy transactions (between two accounts owned by the malicious user) with higher transaction fees. However, this strategy results in the malicious party losing its Bitcoins, as the transaction fee is paid to the miner. Nonetheless, the increase in the transaction queue size will result in higher fees for other users. How could all miners collude to use this strategy and earn higher transaction fees from users (without losing their transaction fee)? [5]

3. (a) Describe the Streamlet blockchain protocol (with the required assumptions). Prove that there cannot be a conflicting block notarized at the same height, i.e., same distance from the genesis block. [7 + 8]

   (b) Describe the Fruitchain blockchain protocol. Explain the high-level ideas. [10]

4. (a) Explain the Ethereum blockchain protocol. Compare and contrast the design principles and applications of Ethereum and Bitcoin. [5 + 7]

   (b) Explain Escrow Smart Contracts and Micropayments. [6 + 6]

--- END of the Question Paper ---