BITS F452 (Assignment-3) (20 Marks)

Title: Develop an Extended Version of Blockchain System as Implemented on Assignment-2

Submission Deadline: 23-Nov-2024 (23:59) (Hard Deadline - No extension possible)

Detail:

Task 1: Building on your previous blockchain implementation, extend the project to include a simple peer-to-peer (P2P) network where multiple nodes on different systems can participate in maintaining the blockchain. Your blockchain should include the following features:

1. Block Structure: Define a block with the following attributes:
   - Index (block number)
   - Timestamp (time of block creation)
   - List of transactions (each transaction can be a simple string)
   - Hash of the previous block
   - Current block's hash
   - A nonce (a number used to validate the block)
2. Blockchain Creation: Implement a function to initialize the blockchain with a genesis block (the first block in the chain).
3. Adding New Blocks: Implement a method to add new blocks to the blockchain. Use a proof-of-work algorithm where a block's hash must meet a simple condition (e.g., start with four zeros, "0000") before it is added to the chain.
4. Hashing: Implement a hashing function that takes the block's data as input and produces a hash using the SHA-256 algorithm.
5. Chain Validation: Create a function to verify the integrity of the blockchain by checking:
   - If each block's stored "previous_hash" matches the hash of the previous block.
   - The validity of the proof of work for each block.
6. User Interaction: Allow the user to input transactions, mine a new block, and view the current state of the blockchain.
7. Analyze a) Time taken by step 3 and step 5 in terms of CPU clocks, b) Network latency to broadcast transactions and mined blocks.

You are asked to demonstrate the working of task 1 and its analysis.

Task 2: Transaction Pinning Attack

Demonstrate Transaction Pinning Attack in your blockchain. Submit a presentation file containing screenshots of this attack. You are asked to demonstrate the attack during evaluation.

Objectives of assigning project:

- The project helps students grasp the concept of a decentralized network by implementing a peer-to-peer (P2P) system, a fundamental aspect of real-world blockchain networks.
- By extending the proof-of-work algorithm to work in a P2P network, students learn how distributed nodes reach consensus and maintain a unified blockchain, despite potential forks or conflicting versions.
- Students gain hands-on experience with basic network programming, learning how to implement communication between multiple nodes using basic networking principles.
- The project aims to introduce students to fundamental blockchain security attacks and protection concepts.

Groups:

- *Students are supposed to make group by contacting the contact person:*
  Students's list:
  https://docs.google.com/spreadsheets/d/17FCG49OXNAE4V6It2clG2BJqfCf1KlKM/edit?usp=sharing&ouid=111079531175815544116&rtpof=true&sd=true
  Group detail (to be filled by contact persons):
  https://docs.google.com/spreadsheets/d/1w3S4PejgBZc1bnQIPxGwq6HmFZFPBAYy_3yYVvQi2PI/edit?usp=sharing
- *Groups are to be made by 8-Nov-2024.*

Additional Instructions:

- *You are free to use any programming language and platorm.*
- *You are free to make any relevant assumptions, but be sure to mention them during your presentation.*
- *Include comments in your code to explain each part.*
- *You are free to create three subgroups and divide Task 1 and Task 2 among subgroups. You are free to choose the size of subgroups. SUBGROUPS MUST NOT BE OVERLAPPING.*

Submission Instructions:

- *Submissions are to be done through the following link by the contact person of the group as per the list.*
- *Link:*
  https://docs.google.com/forms/d/e/1FAIpQLSdN5HNglMLm7JV2WiviJSYtxt_GoET_S8BiL9An2fNexBJneg/viewform?usp=sf_link
- *Any false submission will result in lower marks.*

Evaluation Instructions:

- *Evaluation will be based on 1) individual efforts made in this group-assignment and 2) whole team's effort.*
- *All teams with all members will be asked to present their work on the evaluation date, i.e., 24-Nov-2024.*

Evaluation Criteria:

- *Knowledge of the task and Solution: 10 marks*
- *Q/A: 4 marks*
- *Quality of Work: 3 marks*
- *Group Effort: 3 marks*

Note: Absentees will receive NC grade. Any group member may be randomly selected to explain the work/ answer the questions about the assigned task.