

BITS F452 (Assignment-2) (20 Marks)

Title: Develop a Basic Blockchain System

Submission Deadline: 10-Oct-2024 (23:59) (Hard Deadline - No extension possible)

Detail:

Task 1: Create a simple blockchain system using programming language of your choice. 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 two zeros, "00") 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.

Task 2: Race Attack

Demonstrate Race Attack in the absence of proof of work/consensus. Submit a presentation file containing screenshots of this attack.

Task 3: Finney Attack

Demonstrate Finney Attack in the absence of proof of work/consensus. Submit a presentation file containing screenshots of this attack.

Objectives of assigning project:

- The project aims to help students grasp the core concepts of blockchain, including blocks, the chain structure, hashing, proof of work, and the decentralized nature of blockchain.
- Implementing the validation method allows students to learn how blockchains self-verify, reinforcing concepts such as consensus.
- The task encourages students to break down a complex problem into manageable parts, fostering problem-solving skills and logical thinking.
- Encouraging students to work together helps them develop teamwork skills, such as effective communication, cooperation, conflict resolution, and adaptability. These are essential skills for real-world work environments.

Groups:

- You may find group-related information here:
https://drive.google.com/open?id=1q_fhU_4lyZY0K1qgP_REdcEcU-7lldkJ&usp=drive_fs
- There is no change possible in the randomly created groups.

Additional Instructions:

- You are free to use any programming language and platform.
- 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, Task 2, and Task 3 among subgroups. You are free to choose the size of subgroups. SUBGROUPS MUST NOT BE OVERLAPPING (i.e., a student in subgroup-1 must not be in subgroup-2/subgroup-3.)

Submission Instructions:

- Submissions are to be done through the following link by the first person of the group as per the list.
- Link:
https://docs.google.com/forms/d/e/1FAIpQLSccZ4mrY8QWVr2UDfcfLwA2bvbO2iaQTKAcYyFKrUmIwipt-A/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 will be asked to present their work on the evaluation date.

Evaluation Date: To be announced...