Lab 3 Assignment

In this lab, we will implement a mechanism that allows to store transactions in a Blockchain. This Blockchain will be used as a Database. For a seek of simplicity, at this level, transactions will in the form of a single String message.

In order to implement such a Blockchain, there will be mainly 2 classes: a class representing the Block and a class representing the whole Blockchain.

Block:

- A class that represents the Block.
- A Block is characterized by its index, its hash, a previous hash, the data and a nonce.
- The index represents the position of the Block in the Blockchain. The index of the first Block is 0, the second Block is 1, the third block is 2, and so on.
- The Block data is the concatenation of two messages.
- The previous hash is containing the value of the previous block hash. The previous hash of the genesis block will be NULL.
- The nonce is a 32-bit integer whose value represents the PoW.
- Finally, the hash is the result of applying SHA256 to the concatenation of the previous element of the Block as follows:

  Hash = SHA256(index + previous hash + SHA256(data) + nonce)

- This class should implement methods that allows mainly: Mining a block and Computing the Block hash.

Blockchain:

- A class that represents the Blockchain.
- The PoW difficulty is defined in this class.
- This class represents the Log that maintains the blockchain (i.e. an Array list of Blocks linked to each other by their hashes). Note that there should be no direct pointers.
- This class should allow verifying a Block and verifying the validity of the Blockchain.

The main program should read an input text file to initialize the Blockchain.
The file contains a list of messages.