IT486: Blockchains and Cryptocurrencies Autumn 2020-21
Homework 2 (12 marks)
Due: Dec 9 23:59 via Google classroom

Instructions. This homework is a programming assignment. You are to work individually. Be sure to include your full name and email address in the comment at the top of `merkle_proof.py`. Late submissions will not be accepted.

Refer to the following link: https://github.com/Blockchain-for-Developers/merkle-tree. You are given skeleton of merkle tree, edit the `merkle_proof.py` file and write `merkle_proof` and `verify_proof` functions. The `test.py` file consist of test cases, your code should pass all the test cases. The function `merkle_proof` takes a merkle tree and a transaction as input, and outputs a list consist of transactions (sequence of transaction in list matters). These transactions are minimum required nodes in the tree to generate the block header. The function `verify_proof` takes the list obtained from `merkle_proof` and a transaction (`tx`). It will check if the block header can be re-generated from transactions included in the list along with input `tx`.

Hints: Use height of tree to find how many nodes should be there in the list (output of `merkle_proof` function). `HashLeaf` object in `hash_data_structure.py` have `left` and `right` variables which can be used to find `siblings` if you need them.