COMP4142 E-PAYMENT AND CRYPTOCURRENCY

Project Specification

Objective

Have an in-depth understanding on how the blockchain system works.
Be able to write a UTXO (unspent transaction output) blockchain platform.

Requirements

This is a group project (group size 4-6 recommended). Please allocate among yourselves the tasks and indicate the contributions made by each one of you. All team members need to have fairly equal contributions in this project. A workload table and contribution list need to be included in the project report.

A group of 3 students or less can have full marks even with less functions implemented (this will be judged by TA/instructor). We still hope you can finish most functions, which is the purpose of the group project. To be fair, with less students, some difficult functions may not be finished.

Please write the documents in your own word and make sure the materials used have been properly referenced. Please notice the PolyU plagiarism booklet: http://edc.polyu.edu.hk/PSP/Plagiarism_Booklet.pdf

Project Schedule

1. Demonstration: Nov. 24, 2022 (In the class)
2. Submission of all project deliverables: Nov. 29, 2022, in the blackboard

Please see the project submission part for more information about the project demonstration and final project deliverables.
Note: Late submission will be penalized unless there is a proper reason justified.

Goals

1. Blockchain Prototype: construct the blockchain system according to the following structure. The block should have the following **basic content**. (2 points)
   a) Index: the height of the current block.
   b) Timestamp.
   c) Previous Block Hash.
   d) Current Block Hash.
   e) Difficulty: the number of bits at the beginning of block hash.

f) Nonce: the random number used to calculate the block hash.
g) Merkle root of transactions.
h) Data: transaction.

2. Mining: implement a dynamic-difficulty Proof-of-Work algorithm. (3 points)
   a) Design a **Proof-of-Work algorithm**. For example, adjust the nonce and generate hash until having a hash with a leading number of zeros. (2 points)
   b) **Achieve dynamic difficulty**. For example, adjusting the difficulty of the current block dynamically based on the time taken to generate the previous (10, 20, or more) blocks. (1 point)
3. Transaction: implement pay-to-public-key-hash (P2PKH) transactions and verify transactions. (2 points)
   a) Implement pay-to-public-key-hash (P2PKH) transactions**.** (1 point)
   b) Use asymmetric cryptography to create **digital signatures and verify transactions**. (1 point)
4. Network: basic interactions and validation should be realized. (2 points)
   a) Create an API to **broadcast** the new blocks and **get the blocks** from the other nodes. The API should allow a user to interact with the blockchain by the HTTP request, socket, or different ports. (1 point)
   b) Achieve a function to check if the new blocks that we receive from other miners are valid or not. (Hint: recompute the hash of the block and compare it with the given hash of the block.) (1 point)
5. Storage: choose your database in the implementation. (3 points)
   a) Store the raw data of the whole blockchain in the disk. (1 point)
   b) Store the latest state (e.g., chain height, full node list, neighbor list) of the blockchain in memory. (1 point)
   c) Store the transactions (UTXO) in a transaction pool. (1 point)
6. Attack: Implement the 51% attack and double spending in your demo. (2 points)

You could refer to some open-source projects to implement your blockchain system but you must refer to them in your report. Otherwise, it could be seen as plagiarism.

Project Submissions

1. Project Presentation and Demonstration

Date: Nov. 24, 2022
In the class. 2-3 members can do the presentation.

2. Final Deliverables

Deadline: Nov. 29, 2022
The final submission (softcopy) contains the following items for each group:

1) A **group report** (pdf format, no page limits) to show how you implemented the blockchain system and how you achieved the 5 goals. You could also include what you have learnt or tried but not demonstrated or included in this project

2) Each student needs to submit a short **individual report** (no more than half a page), where you should describe your responsibility and contribution in detail.

You should include all the required documents in a compressed file (.rar, .7z, etc.). Each group only needs to submit once and name it after one group mate.
Note: The softcopy files should be submitted to the blackboard.

Grading Scheme

Total marks	25
1. Blockchain Prototype	2
2. Dynamic-difficulty Proof-of-Work algorithm	3
3. Transaction	2
4. Network	2
5. Storage	3
6. Attack	2
7. Presentation and demonstration (e.g., interface design)	5
8. Group report and individual contribution (e.g., coding referring to other sources)	6