COMP5521 DISTRIBUTED LEDGER TECHNOLOGY, CRYPTOCURRENCY AND E-PAYMENT

Project Specification

Objective

Have an in-depth understanding of how the blockchain system works.

Be able to write a customized blockchain platform from the scratch.

Requirements

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

Please write the documents in your own word and make sure that 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: May 14th, 2020 (online in Team)
2. Submission of all project deliverables: May 21st, 2020 in the blackboard

Please see the project submission part for more information about project demonstration and final project deliverables.

Note: Late submission will be penalized unless there is proper reason justified.

Goals

1. Blockchain Prototype: construct the blockchain system according to the following structure.
   a) Index: the height of current block.
   b) Data: any data that is included in the block
   c) Timestamp: the creation time of block (seconds from Unix Epoch).
   d) Previous Block Hash: SHA-256 hash of previous block.
   e) Current Block Hash: SHA-256 hash of current block.
2. Mining: implement a Proof-of-Work algorithm.
   a) Combine all the data in a block.
   b) Calculate a SHA-256 hash value of these information.
   c) If the output is under the target, you mine a new block successfully.
   d) Otherwise, increment nonce by 1 and repeat step c).
3. Transaction:
   a) Structure: one transaction consists of a transaction ID, an input, and an output.
   b) Transaction ID: the transaction ID is calculated by taking a hash of the transaction contents.
   c) Output: the output consists of an address and an amount of coins.
   d) Input: the input consists where the coins are coming from (i.e., previous transaction ID and index) along with a signature.
4. Network: two basic interactions should be realized.
   a) getblock: it is used to get the blocks from the other nodes.
   b) inv: it is used to inform the other nodes what blocks or transactions it has.
   c) You could implement your network via socket, HTTP or different ports.
   d) You could refer to some open source projects to implement your network.
5. Storage: two databases should be implemented.
   a) Blockchain: it stores the raw data of the whole blockchain in disk.
   b) State: it stores the latest state of the blockchain in memory.
   c) You could refer to some open source projects to implement your databases.

Project Submissions

1. Project Presentation and Demonstration

Date: May 14th, 2020

You need to present your project result in Team, and record your presentation in Team.

Note: For ease of online Team presentation management, 1-2 members can do the presentation.

2. Final Deliverables

Deadline: May 21st, 2020

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**, 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. Create the blockchain according to the required structure	3
2. Mine a block successfully	3
3. Generate a transaction according to the requirement	3
4. Different nodes in the blockchain system can get blocks from other nodes	3
5. The blockchain data can be stored in disk and acquired later	3
6. Presentation and demonstration	5
7. Group report	3
8. Individual report	2