COMP4087/7200 Blockchain Technology

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 4-5). 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 HKBU plagiarism booklet: http://ar.hkbu.edu.hk/curr/avoid_plagiarism/

Project Schedule

1. Demonstration of the project: Apr. 12, 2021 at lecture room or via zoom
2. Submission of all project deliverables: Apr. 12, 2021 in the Moodle

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

Note: Late submission will be penalized.

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 information in the block and start nonce from 0.
    b) Calculate the SHA-256 hash value of all the information.
    c) If the output is under the target, add the new block to the blockchain.
    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. Mint Coins:
    a) Coinbase Transaction: each block should contain a coinbase transaction at the very first place for transactions to mint 50 coins.
    b) Transaction ID: the transaction ID of coinbase transaction is calculated by taking a hash of the transaction contents.
    c) Input: the input of coinbase transaction is zero.
    d) Output: the output consists of an address and the amount of minted coins.
5. 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.

Project Submissions

1. Project Presentation and Demonstration

Date: Apr. 12, 2021

In the presentation, show how you achieve the above 5 goals.

15 minutes project presentation, demonstration, and Q&A session.

Note: Each member is required to present his/her own part.

2. Final Deliverables

Deadline: Apr. 12, 2021

The final submission (softcopy) contains the following items for each group:

1) Presentation slides and project source code. You could package the project source files as a compressed file.
2) Final group report, which should have 7-8 pages to illustrate how you implemented the blockchain system and how you obtained results. You could also include what you have learnt or tried but not demonstrated or included in this project
3) Meanwhile, each student needs to attach a short individual report after the group report. Each individual report should be 1 page. In the individual report, each team member should describe his responsibility in detail.

Note: The softcopy files should be submitted to the Moodle.

Grading Scheme

Total marks	100
1. Create the blockchain according to the required structure	15
2. Mine blocks successfully	15
3. Generate transactions according to the requirement	15

4. Mint new coins using the coinbase transaction	15
5. Different nodes in the blockchain system can get blocks from other nodes	15
6. Presentation and report	25