ASSIGNMENT 4

CS 454: Principles of Concurrent Programming / Spring 2024

Description

In this assignment, you will implement a cryptocurrency based on coins, wallets, and a blockchain. A coin can be mined and then registered with the blockchain. Coins can be present in one wallet at most. Our sample cryptocurrency features three novel technologies. First, wallets need to pay rent to the blockchain by giving up coins. Second, coins can be redeemed by the blockchain for direct access to goods and services. Coins used to pay rent, as well as redeemed coins, leave circulation and cannot be used anymore in any operation. Finally, wallets have a maximum number of coins that they can hold (like physical wallets that hold physical coins).

Changes between Assignment 4 and Assignment 1 are highlighted in this document.

Your submission should extend the following abstract class:

```
abstract class Blockchain {
  abstract Wallet createWallet(int capacity);

  abstract Coin createCoin(int id);

  abstract boolean addCoins(Wallet w, Set coins);

  abstract boolean transferCoins(Wallet from, wallet to, Set coins);

  abstract boolean payRent(Wallet w, Set coins);

  abstract boolean redeemCoins(Wallet w, Set coins);

  abstract Set getCoins();

  abstract Set getCoins(Wallet w);

  abstract Result<Boolean> addCoinsAsync(Wallet w, Set coins);

  abstract Result<Boolean> payRentAsync (Wallet w, Set coins);

  abstract Result<Boolean> redeemCoinsAsync (Wallet w, Set coins);
```

```
  abstract Result<Boolean> transferCoinsAsync (Wallet w, Set coins);

  abstract Result<Set> getCoinsAsync ();

  abstract Result<Set> getCoinsAsync (Wallet w);

  abstract List<Action< Wallet>> audit(Coin c);

  abstract List<Action< Coin>> audit(Wallet w);
}
```

Each operation (method) behaves as follows:

- **createWallet**: Creates a wallet that can store a number of coins – `capacity`
- **createCoin**: Registers a new mined coin with a given `id`. The `id` is unique across the same `Blockchain`.
- **addCoins**: Adds all coins `coins` to the wallet `w`.
  - This operation either adds all the coins, if the wallet has enough capacity, or none.
  - For instance, attempting to add two coins to a wallet that only has room for one should not change the contents of the wallet.
  - If all the coins are added to the wallet, this operation returns `true`. If the wallet remains unchanged, this operation returns `false`.
- **transferCoins**: Moves `coins` currently present in the `from` wallet to the `to` wallet.
  - If there is not enough room in the `to` wallet, this operation should fail and return `false`.
  - If any coin is not present in the `from` wallet, this operation should fail and return `false`.
  - This operation returns `true` if it succeeds in moving all the coins between wallets.
- **redeemCoin**: Marks all the given `coins` provided as redeemed, which should be present on the given `wallet`.
  - Similarly to **addCoins**, this operation either marks all the coins or none.
  - Trying to redeem a coin that is not in the current wallet results in failure of the whole operation (i.e., no coins are redeemed).
  - If all the coins are redeemed, this operation returns `true`. If any coin was not redeemed, then no coins are modified and this operation returns `false`.
- **payRent**: Similar to redeem described above, but marks all coins as used in rent payments
- **getCoins**: Gets the coins in a given wallet (i.e., added to the wallet, and not redeemed or used for rent).
  - Without arguments, this operation lists all the coins that the blockchain produced that are still in circulation.

    - With a `wallet` argument, this operation lists all the coins currently in that wallet that are still in circulation.
- **Asynchronous methods**: Each method described above has an asynchronous version
    - The asynchronous methods should return as fast as possible
    - The asynchronous methods return a Result object, which the caller can then use to retrieve the result of the operation
    - The asynchronous methods do not wait for the operation to be performed
- ~~**audit**: Returns an audit log that tracks coins and wallets.~~
    - ~~With a `coin` argument, returns a list of all the wallets in which the coin ever was~~
        - ~~The order of the list matters~~
        - ~~When transferring, coins should be removed from one wallet before being added to another wallet~~
    - ~~With a `wallet` argument, returns a list of all the coins that passed by that wallet~~
        - ~~The order of the list matters~~
            - ~~If an operation changes many coins at once, the order between those coins does not matter.~~
            - ~~However, all those coins should be on the list after preceding operations and before later operations~~

Besides the `Blockchain` interface, your solution should also implement the `Coin` interface for each coin, which defines the **getStatus** operation:

```
interface Coin {
    enum Status { MINED, IN_CIRCULATION, RENT , REDEEMED }
    Status getStatus();
}
```

Each coins should behave as follows:

- All coins are created as `MINED`
- A `MINED` coin can be added to a wallet, in which case it becomes `IN_CIRCULATION`
- Once a coin is in circulation, it cannot become `MINED` again
- A `IN_CIRCULATION` coin can be used to pay rent, and become `RENT`
- A `IN_CIRCULATION` coin can be redeemed, and become `REDEEMED`
- Once a coin is not in circulation, it cannot go back in circulation

Correctness Requirements

Your implementation should keep the following properties at all times:

1. **getCoins** operations never list more coins than a wallet's capacity

2. **getCoins** operations never list more items for the whole blockchain than the sum of the capacity of all the wallets.
3. Adding mined coins to a wallet successfully results in those coins being listed in later **getCoins** operations.
4. Once a coin is used to pay rent or redeemed, that coin is not listed in later **getCoins** operations.
5. ~~Each coin is listed in one wallet at most by **getCoins** operations.~~
6. ~~Coins are never "in-transit" due to transfer operations (i.e., **getCoins** operations not listing coins removed from the `from` wallet and still not added to the `to` wallet).~~
7. Once the status of a coin is observed to be `RENT` or `REDEEMED`, it cannot be observed to be anything else from that point on.
8. ~~It is not possible to observe partial results of any operation on a single wallet. Each operation either happens completely, or not at all.~~
9. ~~The current contents of any wallet can be explained by following the entries in the audit log, by the order in which they appear in the log.~~
10. ~~The current state and location of any coin can be explained by following the entries in the audit log, by the order in which they appear in the log.~~
11. Move operations cannot lose any of the coins being moved. Eventually, all the coins will be either in the destination wallet (success) or in the source wallet (fail).

Concurrency Requirements

In this assignment, you are provided with an implementation of `Wallet` that has the following properties:

- The provided wallet already has a set contents to contain all the coins in the wallet that are in circulation
- Each wallet is associated with its own worker thread
- Each wallet's contents can be modified only by the worker thread of that wallet
    - If any other thread attempts to add/remove coins from a wallet, the code throws an exception that will cause all tests to fail
- Asynchronous methods must preserve order: If a thread adds a coin to a wallet and then uses it to pay rent using `addCoinsAsync` followed by `payRentAsync`, then both results should (eventually) be true
- Your implementation cannot use busy-waiting

Bonus Extra Functionality

Besides implementing all of the above, you can claim a 10% bonus by ensuring that **Blockchain.getCoins()** is as fast as possible, taking full advantage of as much concurrency as possible.

Entry Point

You should create a new class, on a new file, where you will implement your solution. You should change method Blockchain.createBlockchain so that it creates an instance of the class you added. You cannot change any other part of the code that is provided to you.

```
abstract class Blockchain {
    static Blockchain createBlockchain() {
        throw new Error("Not implemented");
    }
}
```

You should also implement your own result, returned by the asynchronous operations.

Due Date and Resubmission Policy

This assignment is due on **March 30 2024** (Saturday) at **5pm CST**. There is no late policy.

The code and date used for your submission is defined by the last commit to your Git repository.

To resubmit this assignment, your **original grade** (as defined by the autograder) should be **equal to or higher than 30%** for undergraduate students, and **50%** for graduate students. You can resubmit your assignment until **April 6 2024** (following Saturday) at **5pm CST**. Together with your resubmission, you will have to submit a written description of what you changed from the original submission (on Gradescope).

Bonus Points

This assignment has a total of **10% bonus points**, which you can earn by using Piazza as described in the syllabus. Your posts should be public, tagged with the `assignment-4` label, and non-anonymous to the instructors to count towards the bonus.

Submission and Grading

This assignment is submitted through Github, and has an automatic grade component of 70%. You can check your current grade at any point by submitting your code and checking the autograder. The automatic grade is determined by 7 tests, that will check if your submission outputs the expected result. Each test is worth 10%.

Together with the code, you should submit three video screen-cast (**through Gradescope**) that answers the three questions below by explaining how your code works (one video per question). The questions focus on concurrency/multi-threading and are worth 10% each. You can record such a video without installing any software by using the following website: https://screenapp.io/#/

1. How do you avoid busy-waiting in your implementation?
2. Is it correct to modify `Wallet.contents` without grabbing a lock? Why?
3. How do you ensure that a failing transfer operation does not result in coins being lost?
4. (bonus) What steps did you take to ensure Blockchain.getCoins() is as fast and concurrent as possible?

The maximum length for each video is 1 minute, instructors will stop watching at the 1 minute mark (nothing past that point in the video will be graded). This video should be a screencast of your IDE open on the code submitted, and you should highlight the code. Note that longer videos are not better videos, and you should record a video as short as needed to show all the expressions and answer the questions above.

The final grade for the assignment will be the grade of the original submission, for assignments without a resubmission; or the average between the original grade and the resubmission grade, for assignments with a resubmission. The grade of the original submission includes any bonus points.

Errors and Omissions

If you find an error or an omission, please post it on Piazza as soon as you find it.

Hardcoding and Academic Integrity

Any hardcoding will result in a 0% grade. Hardcoding is when you submit code that detects which test is being run, and simply outputs the expected result. For instance, detecting that test 22 is running, and replacing the usual execution of your submission with `System.out.println("expected result").`

The academic integrity policy described in the syllabus applies to this assignment. You are responsible for writing all the code that you submit. We will use an automatic tool that detects plagiarism on all submitted code, and we will investigate all instances where plagiarism is more than likely.

Please refer to the syllabus for the full academic integrity policy.