

Implement SBitcoin, a simple version of Bitcoin, which works under the following rules:

1. A block contains the following information

blockNo: Block number

data: Set of transactions

prev: Pointer that points to the previous block

prev_hash: Hash of the previous block

nonce: Block nonce

timestamp: Block creation time

2. There are two kinds of transactions

A. BaseCoins

```
{ "hash": "db9ca9df899e7",  
  "type": "BaseCoins",  
  "coins_created": [  
    { "num": 0, "value": 20, "recipient": "[Miner]" }  
  ],  
  "Timestamp": "2020-07-24 13:54:46.983531" }
```

B. PayCoins

```
{ "hash": "c821f7621208b",  
  "type": "PayCoins",  
  "coins_consumed": [  
    { "hash": "db9ca9df899e7", "num": 0 },  
    { "hash": "772fe5688d766", "num": 2 },  
    { "hash": "8c9b6da77d6cb", "num": 1 }  
  ],  
  "coins_created": [  
    { "num": 0, "value": 3.2, "recipient": "[Alice]" },  
    { "num": 1, "value": 1.4, "recipient": "[Bob]" },  
    { "num": 2, "value": 7.5, "recipient": "[Caleb]" }  
  ],  
  "signatures": [  
    "<signature for { 'hash': 'db9ca9df899e7', 'num': 0 }>",  
    "<signature for { 'hash': '772fe5688d766', 'num': 2 }>",  
    "<signature for { 'hash': '8c9b6da77d6cb', 'num': 1 }>"  
  ],  
  "Timestamp": "2020-07-24 14:34:26.653531" }
```

2. When a user creates a new transaction, this transaction is stored in the pending pool that contains all pending transactions

3. New blocks are created by miners

- A miner collects all transactions in the pending pool and creates a new block that contains these transactions

- A miner receives 20 coins as a reward for each new valid block created

- Time to mine a new block base on the difficulty

difficulty = 20

maxNonce = 2 ** 32

$\text{target} = 2^{(256 - \text{difficulty})}$

Do the following tests to your program.

1. Generate four accounts: Alice, Bob, Caleb and Marry
2. Alice mines a new block
3. Alice transfers 10 coins to Bob and 5 coins to Marry
4. Bob mines the next block
5. Bob transfers 25 coins to Caleb and 5 coins to Alice
6. Alice creates a transaction that Caleb transfers 15 coins to Alice, sign this transaction by Alice private key
7. Marry mines the next block
8. Alice and Marry transfer 5 coins to Bob and 5 coins to Caleb
9. Caleb transfers 15 coins to Bob and 5 coins to Marry
10. Alice creates a transaction that Caleb transfers 10 coins to Alice
11. Alice mines the next block
12. Bob transfers 20 coins to Marry and 5 coins to Alice
13. Caleb mines the next block
14. Marry transfers 10 coins to Alice
15. Alice mines the next block and changes her reward to 30 coins
16. Caleb transfers 5 coins to Marry
17. Alice transfers 20 coins to Bob
18. Bob transfers 15 coins to Alice
19. Marry mines the next block
20. Marry tampers with all blocks mined by her to change the rewards to 25 coins