Lalita Sharkey; UIN 01063704

CS 764/864: Blockchains and Cryptocurrencies: Fundamentals, Technologies, and Economics

Module 3: Homework 3 Blockchain implementation

Readme

Requirements:

1. The latest JDK version
2. JavaScript runtime (node.js)
3. Install crypto using `npm install –save crypto-js` from terminal
4. Install elliptic using `npm install elliptic` from terminal

Running the program:

1. From command prompt, cd to the location of the source code
2. Using node `.\main.js > result.txt` to save output to a text file

Program constrains:

1. Difficulty level was set to 2.
2. Mining reward was set to 100.

References

[1] https://www.youtube.com/watch?v=OKg4PqD01Z0
[2] https://github.com/dvf/blockchain/blob/master/blockchain.py
[3] https://github.com/julienr/ipynb_playground/blob/master/bitcoin/dumbcoin/dumbcoin.ipynb

Source Code

blockchain.js

```
1. const crypto = require('crypto');
2. const EC = require('elliptic').ec;
3. const ec = new EC('secp256k1');
4. const SHA256 = require('crypto-js/sha256');
5.
6. class Transaction{
7.     constructor(clientPubicKey, merchantPubicKey, amount, timestamp){
8.         this.clientPubicKey = clientPubicKey;
9.         this.merchantPubicKey = merchantPubicKey;
10.        this.amount = amount;
11.        this.timestamp = timestamp;
12.    }
13.
14.    calculateHash(){
15.        return SHA256(this.clientPubicKey, this.merchantPubicKey, this.amount, this.timestamp).toString();
16.    }
17.
18.    signTransaction(signingKey){
19.        if(signingKey.getPublic('hex') !== this.clientPubicKey){
20.            throw new Error('Unable to sign the transaction from other wallets!');
21.        }
22.        const hashTx = this.calculateHash();
23.        const sig = signingKey.sign(hashTx, 'base64');
24.        this.signature = sig.toDER('hex');
25.    }
26.
27.    isValid(){
28.        if(this.clientPubicKey === null) return true;
29.
30.        if(!this.signature || this.signature.length ===0){
31.            throw new Error('No signature in this transaction');
32.        }
33.
34.        const publicKey = ec.keyFromPublic(this.clientPubicKey, 'hex');
35.        return publicKey.verify(this.calculateHash(), this.signature);
36.    }
```

```
}

class Block{
    constructor(transactions, previouHash = ''){
        this.transactions = transactions;
        this.previouHash = previouHash;
        this.hash = this.calculateHash();
        this.nonce = 0;
    }

    calculateHash(){
        return SHA256(this.index + this.previouHash + this.timestamp + JSON.stringify(this.transactions) + this
    .nonce).toString();

    }

    mineBlock(difficulty){
        while(this.hash.substring(0, difficulty) !== Array(difficulty +1).join("0")){
            this.nonce++;
            this.hash = this.calculateHash();
        }

        console.log("Block mined: " + this.hash);
    }

    hasValidTransactions(){
        for(const tx of this.transactions){
            if(!tx.isValid()){
                return false;
            }
        }
        return true;
    }
}

class Blockchain{
    constructor(){
```

```
73.         this.chain = [this.createGenesisBlock()];
74.         this.difficulty = 2;
75.         this.pendingTransactions = [];
76.         this.miningReward = 100;
77.     }
78.
79.     createGenesisBlock(){
80.         return new Block("Genesis Block", "0");
81.     }
82.
83.     getLastestBlock(){
84.         return this.chain[this.chain.length - 1];
85.     }
86.
87.     minePendingTransactions(miningRewardAddress){
88.         const rewardTx = new Transaction(null, miningRewardAddress, this.miningReward);
89.         this.pendingTransactions.push(rewardTx);
90.         const block = new Block(this.pendingTransactions, this.getLastestBlock().hash);
91.         block.mineBlock(this.difficulty);
92.         this.chain.push(block);
93.         this.pendingTransactions = [];
94.     }
95.
96.     addTransaction(transaction){
97.         if(!transaction.clientPubicKey  || !transaction.merchantPubicKey){
98.             throw new Error('Transaction must include client pubic key and merchant pubic key');
99.         }
100.
101.            if(!transaction.isValid()){
102.                throw new Error('Cannot add invalid transaction to chain');
103.            }
104.
105.            this.pendingTransactions.push(transaction);
106.            console.log('Client pubicKey: ', transaction.clientPubicKey);
107.            console.log('Merchant pubicKey: ', transaction.merchantPubicKey);
108.            console.log('Transaction date: ', Date(transaction.timestamp.toString()));
109.            console.log('Transaction amount: ', transaction.amount.toFixed(2), '\n');
```

```
110.        }
111.
112.        getBalanceOfAddress(address){
113.            let balance = 0;
114.
115.            for(const block of this.chain){
116.                for(const trans of block.transactions){
117.                    if(trans.clientPubicKey === address){
118.                        balance -= trans.amount;
119.                    }
120.
121.                    if(trans.merchantPubicKey === address){
122.                        balance += trans.amount;
123.                    }
124.                }
125.            }
126.            return balance;
127.        }
128.
129.        isChainValid(){
130.            for(let i = 1; i < this.chain.length; i++){
131.                const currentBlock = this.chain[i];
132.                const previousBlock = this.chain[i-1];
133.
134.                if(!currentBlock.hasValidTransactions()){
135.                    return false;
136.                }
137.
138.                if(currentBlock.hash !== currentBlock.calculateHash()){
139.                    return false;
140.                }
141.
142.                if(currentBlock.previouHash !== previousBlock.hash){
143.                    return false;
144.                }
145.            }
146.
```

```
147.            return true;
148.        }
149.    }
150.
151.    module.exports.Blockchain = Blockchain;
152.    module.exports.Block = Block;
153.    module.exports.Transaction = Transaction;
```

keyGen.js

```
const EC = require('elliptic').ec;
const ec = new EC('secp256k1');

//Assume that you have 5 customers (C1-C5), 2 merchants (M1-M2), and a single miner (SM)
//Generate 2 public-key/private-key pairs representing 2 merchants
const keyM1 = ec.genKeyPair();
const publicKeyM1 = keyM1.getPublic('hex');
const privateKeyM1 = keyM1.getPrivate('hex');

const keyM2 = ec.genKeyPair();
const publicKeyM2 = keyM2.getPublic('hex');
const privateKeyM2 = keyM2.getPrivate('hex');

//Generate 5 public-key/private-key pairs representing 5 customers
const keyC1 = ec.genKeyPair();
const publicKeyC1 = keyC1.getPublic('hex');
const privateKeyC1 = keyC1.getPrivate('hex');

const keyC2 = ec.genKeyPair();
const publicKeyC2 = keyC2.getPublic('hex');
const privateKeyC2 = keyC2.getPrivate('hex');

const keyC3 = ec.genKeyPair();
const publicKeyC3 = keyC3.getPublic('hex');
const privateKeyC3 = keyC3.getPrivate('hex');

const keyC4 = ec.genKeyPair();
const publicKeyC4 = keyC4.getPublic('hex');
const privateKeyC4 = keyC4.getPrivate('hex');

const keyC5 = ec.genKeyPair();
const publicKeyC5 = keyC5.getPublic('hex');
const privateKeyC5 = keyC5.getPrivate('hex');

//Generate 1 public-key/private-key pair for the single miner
const keySM = ec.genKeyPair();
```

```
const publicKeySM = keySM.getPublic('hex');
const privateKeySM = keySM.getPrivate('hex');


console.log('Public key M1:', publicKeyM1);
console.log('Private key M1: ', privateKeyM1);
console.log();
console.log('Public key M2:', publicKeyM2);
console.log('Private key M2: ', privateKeyM2);
console.log();
console.log('Public key C1:', publicKeyC1);
console.log('Private key C1: ', privateKeyC1);
console.log();
console.log('Public key C2:', publicKeyC2);
console.log('Private key C2: ', privateKeyC2);
console.log();
console.log('Public key C3:', publicKeyC3);
console.log('Private key C3: ', privateKeyC3);
console.log();
console.log('Public key C4:', publicKeyC4);
console.log('Private key C4: ', privateKeyC4);
console.log();
console.log('Public key C5:', publicKeyC5);
console.log('Private key C5: ', privateKeyC5);
console.log();
console.log('Public key SM:', publicKeySM);
console.log('Private key SM: ', privateKeySM);
```

main.js

```
const { Blockchain, Transaction } = require('./blockchain');
```

```
const EC = require('elliptic').ec;
const ec = new EC('secp256k1');

const m1Key = ec.keyFromPrivate('ba79c4ba6496277f0962c8041c9983b5cf9861934f9b37ad47d0cb110678f52c');
const m2Key = ec.keyFromPrivate('4e61543508d9b20f75fbc8d18b4b9ac7d2ee16bba6237bd1f6ef903138b77af5');
const c1Key = ec.keyFromPrivate('92b0628d411bbcc4957758a90f8848a6f3e60866c8e8ec04c3814c906561f540');
const c2Key = ec.keyFromPrivate('cbc5bcbe325edb45ff43bc0422d64afc14f8e977e2307b4733b5a98cee17e3d3');
const c3Key = ec.keyFromPrivate('8769062d5a26785ee2ac63d8ce97ec8bea270726c7b7e726908605c47b397a98');
const c4Key = ec.keyFromPrivate('fb82a5149fd9f1149d5931f6c613230430bae8deb678df993851cb6a33d53ee1');
const c5Key = ec.keyFromPrivate('c81d723550da9648d031ae9344f72f7cb58e93981bbfae5b275b6886a51b37a3');
const smKey = ec.keyFromPrivate('14c84513562d13a100be9344379680d9ca6932268144872b472866f7aa0c7905');

const m1Wallet = m1Key.getPublic('hex');
const m2Wallet = m2Key.getPublic('hex');
const c1Wallet = c1Key.getPublic('hex');
const c2Wallet = c2Key.getPublic('hex');
const c3Wallet = c3Key.getPublic('hex');
const c4Wallet = c4Key.getPublic('hex');
const c5Wallet = c5Key.getPublic('hex');

let singleMiner = new Blockchain();

//Generate 25 random transactions using the above transaction format
const transaction1 = new Transaction(c1Wallet, m1Wallet, 50, Date.now());
transaction1.signTransaction(c1Key);
singleMiner.addTransaction(transaction1);
singleMiner.minePendingTransactions(c1Wallet);

const transaction2 = new Transaction(c2Wallet, m1Wallet, 100, Date.now());
transaction2.signTransaction(c2Key);
singleMiner.addTransaction(transaction2);
singleMiner.minePendingTransactions(c2Wallet);

const transaction3 = new Transaction(c2Wallet, m1Wallet, 300, Date.now());
transaction3.signTransaction(c2Key);
singleMiner.addTransaction(transaction3);
singleMiner.minePendingTransactions(c2Wallet);
```

```
const transaction4 = new Transaction(c4Wallet, m2Wallet, 10, Date.now());
transaction4.signTransaction(c4Key);
singleMiner.addTransaction(transaction4);
singleMiner.minePendingTransactions(c4Wallet);

const transaction5 = new Transaction(c2Wallet, m1Wallet, 90, Date.now());
transaction5.signTransaction(c2Key);
singleMiner.addTransaction(transaction5);
singleMiner.minePendingTransactions(c2Wallet);

const transaction6 = new Transaction(c1Wallet, m1Wallet, 250, Date.now());
transaction6.signTransaction(c1Key);
singleMiner.addTransaction(transaction6);
singleMiner.minePendingTransactions(c1Wallet);

const transaction7 = new Transaction(c4Wallet, m1Wallet, 45, Date.now());
transaction7.signTransaction(c4Key);
singleMiner.addTransaction(transaction7);
singleMiner.minePendingTransactions(c4Wallet);

const transaction8 = new Transaction(c5Wallet, m1Wallet, 99.99, Date.now());
transaction8.signTransaction(c5Key);
singleMiner.addTransaction(transaction8);
singleMiner.minePendingTransactions(c5Wallet);

const transaction9 = new Transaction(c3Wallet, m2Wallet, 29, Date.now());
transaction9.signTransaction(c3Key);
singleMiner.addTransaction(transaction9);
singleMiner.minePendingTransactions(c3Wallet);

const transaction10 = new Transaction(c3Wallet, m2Wallet, 49, Date.now());
transaction10.signTransaction(c3Key);
singleMiner.addTransaction(transaction10);
singleMiner.minePendingTransactions(c3Wallet);

const transaction11 = new Transaction(c5Wallet, m1Wallet, 69, Date.now());
```

```
transaction11.signTransaction(c5Key);
singleMiner.addTransaction(transaction11);
singleMiner.minePendingTransactions(c5Wallet);

const transaction12 = new Transaction(c5Wallet, m1Wallet, 78, Date.now());
transaction12.signTransaction(c5Key);
singleMiner.addTransaction(transaction12);
singleMiner.minePendingTransactions(c5Wallet);

const transaction13 = new Transaction(c1Wallet, m2Wallet, 69, Date.now());
transaction13.signTransaction(c1Key);
singleMiner.addTransaction(transaction13);
singleMiner.minePendingTransactions(c1Wallet);

const transaction14 = new Transaction(c4Wallet, m2Wallet, 44, Date.now());
transaction14.signTransaction(c4Key);
singleMiner.addTransaction(transaction14);
singleMiner.minePendingTransactions(c4Wallet);

const transaction15 = new Transaction(c1Wallet, m1Wallet, 325.25, Date.now());
transaction15.signTransaction(c1Key);
singleMiner.addTransaction(transaction15);
singleMiner.minePendingTransactions(c1Wallet);

const transaction16 = new Transaction(c1Wallet, m1Wallet, 250.99, Date.now());
transaction16.signTransaction(c1Key);
singleMiner.addTransaction(transaction16);
singleMiner.minePendingTransactions(c1Wallet);

const transaction17 = new Transaction(c3Wallet, m1Wallet, 40, Date.now());
transaction17.signTransaction(c3Key);
singleMiner.addTransaction(transaction17);
singleMiner.minePendingTransactions(c3Wallet);

const transaction18 = new Transaction(c1Wallet, m1Wallet, 5, Date.now());
transaction18.signTransaction(c1Key);
singleMiner.addTransaction(transaction18);
```

```
singleMiner.minePendingTransactions(c1Wallet);

const transaction19 = new Transaction(c4Wallet, m1Wallet, 10.10, Date.now());
transaction19.signTransaction(c4Key);
singleMiner.addTransaction(transaction19);
singleMiner.minePendingTransactions(c4Wallet);

const transaction20 = new Transaction(c3Wallet, m2Wallet, 900, Date.now());
transaction20.signTransaction(c3Key);
singleMiner.addTransaction(transaction20);
singleMiner.minePendingTransactions(c3Wallet);

const transaction21 = new Transaction(c2Wallet, m1Wallet, 210, Date.now());
transaction21.signTransaction(c2Key);
singleMiner.addTransaction(transaction21);
singleMiner.minePendingTransactions(c2Wallet);

const transaction22 = new Transaction(c2Wallet, m2Wallet, 178, Date.now());
transaction22.signTransaction(c2Key);
singleMiner.addTransaction(transaction22);
singleMiner.minePendingTransactions(c2Wallet);

const transaction23 = new Transaction(c1Wallet, m1Wallet, 49, Date.now());
transaction23.signTransaction(c1Key);
singleMiner.addTransaction(transaction23);
singleMiner.minePendingTransactions(c1Wallet);

const transaction24 = new Transaction(c4Wallet, m1Wallet, 5.29, Date.now());
transaction24.signTransaction(c4Key);
singleMiner.addTransaction(transaction24);
singleMiner.minePendingTransactions(c4Wallet);

const transaction25 = new Transaction(c5Wallet, m2Wallet, 190, Date.now());
transaction25.signTransaction(c5Key);
singleMiner.addTransaction(transaction25);
singleMiner.minePendingTransactions(c5Wallet);
```

```
/*Increment the amount in transaction (in block 10) by $10.00, and show how it can be
detected by the customer*/
console.log('\n       ------------------------------------')
console.log('Increment the amount in transaction (in block 10) by $10.00\n');
singleMiner.chain[10].transactions[1].amount += 10;
console.log('Blockchain valid?', singleMiner.isChainValid() ? 'Yes' : 'No');

/*List all transactions for customer 3 (C3)*/
console.log('\n------------------------------------')
console.log('\nList all transactions for customer 3 (C3)\n');
for (let i = 0;  i < singleMiner.chain.length; i++){
    for(let j = 0; j < singleMiner.chain[i].transactions.length; j++){
        if (singleMiner.chain[i].transactions[j].clientPubicKey === c3Wallet){
            console.log(singleMiner.chain[i].transactions[j])
            }
    }
}

/*all transactions for merchant 2 (M2)*/
console.log('\n------------------------------------')
console.log('\nList all transactions for merchant 2 (M2)\n');
for (let i = 0;  i < singleMiner.chain.length; i++){
    for(let j = 0; j < singleMiner.chain[i].transactions.length; j++){
        if (singleMiner.chain[i].transactions[j].merchantPubicKey === m2Wallet){
            console.log(singleMiner.chain[i].transactions[j])
            }
    }
}
```

keys.txt

Public key M1:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea9284345d2c533cbf108119588dd0e6f5642
Private key M1: ba79c4ba6496277f0962c8041c9983b5cf9861934f9b37ad47d0cb110678f52c

Public key M2:
04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a961cb72366f2c564cd10e33e1bb194817f890c88
Private key M2: 4e61543508d9b20f75fbc8d18b4b9ac7d2ee16bba6237bd1f6ef903138b77af5

Public key C1:
04a709bce3d44f25cb3bd8a57a3412879ff971d5de6522bca10aa553b32507165c1440ff615dbc147c43787d259acfe383b536d27c8e11291c457128eacb738e09
Private key C1: 92b0628d411bbcc4957758a90f8848a6f3e60866c8e8ec04c3814c906561f540

Public key C2:
04465c2cd7091736b07bee1c3a17759846eef730e250baca5a68c077e3a09ce4ec507bc5b34cffcc8fc653086b4d4106271d7cabbfc5b55d8f7d17f3643354d211
Private key C2: cbc5bcbe325edb45ff43bc0422d64afc14f8e977e2307b4733b5a98cee17e3d3

Public key C3:
044dd948ed7fdd98a7938cdc56de1e50faf36624b43942604a531dc3fe7af2e62f4f911c76e7c763a51c097162ee8f631a309e665bad40f99f4a764b0fe52ba773
Private key C3: 8769062d5a26785ee2ac63d8ce97ec8bea270726c7b7e726908605c47b397a98

Public key C4:
04355d5df8305ba120b8c0fc40cea8364e30df520f7e96ae0e4b70e5c2dd0f0abd367102a69222f0d926b975e1f9378f00471b244e19d4001b4ddaf1c9cf2cfd08
Private key C4: fb82a5149fd9f1149d5931f6c613230430bae8deb678df993851cb6a33d53ee1

Public key C5:
047b823fd722e0ade40438b94f3d4658e1d6632835436de8ecf8c757f1245f0237d4120b1310b8fb084be6afe3849550dc6a797ea77501952a30eb66472d95449e
Private key C5: c81d723550da9648d031ae9344f72f7cb58e93981bbfae5b275b6886a51b37a3

Public key SM:
0492e3dc4431d8ac998c2272444f6d46107e1589bf54d01deb7b1e1409cf999daa11a35882342df5fc0893646dedf4e35b569560db555601b07de579f57de7cf24
Private key SM: 14c84513562d13a100be9344379680d9ca6932268144872b472866f7aa0c7905

Results

Client publicKey:
04a709bce3d44f25cb3bd8a57a3412879ff971d5de6522bca10aa553b32507165c1440ff615dbc147c43787d259acfe383b536d27c8e11291c457128eacb738e09

Merchant publicKey:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea9284345d2c533cbf108119588dd0e6f5642

Transaction date: Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 50.00

Block mined: 00ba41ec58b6b2abc8a3f29894462eb2e9a230ba53ffb583ef6a8106ece890d2

Client publicKey:
04465c2cd7091736b07bee1c3a17759846eef730e250baca5a68c077e3a09ce4ec507bc5b34cffcc8fc653086b4d4106271d7cabbfc5b55d8f7d17f3643354d211

Merchant publicKey:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea9284345d2c533cbf108119588dd0e6f5642

Transaction date: Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 100.00

Block mined: 003bf0d70e3e26420abdd71674454aaa2365ecd84d2f3754e63a33f2d50e7f86

Client publicKey:
04465c2cd7091736b07bee1c3a17759846eef730e250baca5a68c077e3a09ce4ec507bc5b34cffcc8fc653086b4d4106271d7cabbfc5b55d8f7d17f3643354d211

Merchant publicKey:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea9284345d2c533cbf108119588dd0e6f5642

Transaction date: Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 300.00

Block mined: 000ef4fd9c1ded51b67034aad72a6d31870029323f97963abd2c0aa3d6dadbd6

Client publicKey:
04355d5df8305ba120b8c0fc40cea8364e30df520f7e96ae0e4b70e5c2dd0f0abd367102a69222f0d926b975e1f93
78f00471b244e19d4001b4ddaf1c9cf2cfd08

Merchant publicKey:
04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a96
1cb72366f2c564cd10e33e1bb194817f890c88

Transaction date: Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 10.00

Block mined: 00b42b3dadaeca0f5add194060f6e3695dd4f466d792bf22cf490e842d75e257

Client publicKey:
04465c2cd7091736b07bee1c3a17759846eef730e250baca5a68c077e3a09ce4ec507bc5b34cffcc8fc653086b4d41
06271d7cabbfc5b55d8f7d17f3643354d211

Merchant publicKey:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea
9284345d2c533cbf108119588dd0e6f5642

Transaction date: Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 90.00

Block mined: 0072846ec4e62e37adf93e849c6f02d4e36cf69a3fb4bc72250a1d84ee0a3b96

Client publicKey:
04a709bce3d44f25cb3bd8a57a3412879ff971d5de6522bca10aa553b32507165c1440ff615dbc147c43787d259ac
fe383b536d27c8e11291c457128eacb738e09

Merchant publicKey:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea
9284345d2c533cbf108119588dd0e6f5642

Transaction date: Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 250.00

Block mined: 00263b4d8775852c4ec899607e2ee0c5d2667c6f15152a8d85460b167096329b

Client publicKey:
04355d5df8305ba120b8c0fc40cea8364e30df520f7e96ae0e4b70e5c2dd0f0abd367102a69222f0d926b975e1f93
78f00471b244e19d4001b4ddaf1c9cf2cfd08

Merchant publicKey:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea9284345d2c533cbf108119588dd0e6f5642

Transaction date: Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 45.00

Block mined: 001a8553d3c805207636bf509caf5770405172356e04b709d4c5ed5e63485d68

Client publicKey:
047b823fd722e0ade40438b94f3d4658e1d6632835436de8ecf8c757f1245f0237d4120b1310b8fb084be6afe3849550dc6a797ea77501952a30eb66472d95449e

Merchant publicKey:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea9284345d2c533cbf108119588dd0e6f5642

Transaction date: Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 99.99

Block mined: 00104e3f653ba871dde765c82d3c927ef7a9919b98aad5111a98f9f7ac855827

Client publicKey:
044dd948ed7fdd98a7938cdc56de1e50faf36624b43942604a531dc3fe7af2e62f4f911c76e7c763a51c097162ee8f631a309e665bad40f99f4a764b0fe52ba773

Merchant publicKey:
04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a961cb72366f2c564cd10e33e1bb194817f890c88

Transaction date: : Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 29.00

Block mined: 006de46dba1e935a609dac829530a2b2e0c8dae868fca78b7d34f963203c8eda

Client publicKey:
044dd948ed7fdd98a7938cdc56de1e50faf36624b43942604a531dc3fe7af2e62f4f911c76e7c763a51c097162ee8f631a309e665bad40f99f4a764b0fe52ba773

Merchant publicKey:
04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a961cb72366f2c564cd10e33e1bb194817f890c88

Transaction date: : Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 49.00

Block mined: 00056a92a18ff83510ec9c5ed87c937053116708bb2ea45e88a3da78df91f370

Client publicKey:
047b823fd722e0ade40438b94f3d4658e1d6632835436de8ecf8c757f1245f0237d4120b1310b8fb084be6afe3849550dc6a797ea77501952a30eb66472d95449e

Merchant publicKey:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea9284345d2c533cbf108119588dd0e6f5642

Transaction date: : Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 69.00

Block mined: 005038a52b7aa940a96eb0953bf8745d86622f4f635fe537eb089b9f0f5dc28e

Client publicKey:
047b823fd722e0ade40438b94f3d4658e1d6632835436de8ecf8c757f1245f0237d4120b1310b8fb084be6afe3849550dc6a797ea77501952a30eb66472d95449e

Merchant publicKey:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea9284345d2c533cbf108119588dd0e6f5642

Transaction date: : Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 78.00

Block mined: 00e0072ec807bd525015034b0291e56fe92e00f719d834046519a4a7facf174d

Client publicKey:
04a709bce3d44f25cb3bd8a57a3412879ff971d5de6522bca10aa553b32507165c1440ff615dbc147c43787d259acfe383b536d27c8e11291c457128eacb738e09

Merchant publicKey:
04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a961cb72366f2c564cd10e33e1bb194817f890c88

Transaction date: : Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 69.00

Block mined: 005e877fb544fbbb50547d0fe3231ae9e5c89ba9e045da574c054ee4d0d5ffe9

Client publicKey:
04355d5df8305ba120b8c0fc40cea8364e30df520f7e96ae0e4b70e5c2dd0f0abd367102a69222f0d926b975e1f9378f00471b244e19d4001b4ddaf1c9cf2cfd08

Merchant publicKey:
04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a961cb72366f2c564cd10e33e1bb194817f890c88

Transaction date: : Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 44.00

Block mined: 002fea05e43ad709b62cd8e227fe0c6a2d001025975f5b1d20b8a244387e59d7

Client publicKey:
04a709bce3d44f25cb3bd8a57a3412879ff971d5de6522bca10aa553b32507165c1440ff615dbc147c43787d259acfe383b536d27c8e11291c457128eacb738e09

Merchant publicKey:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea9284345d2c533cbf108119588dd0e6f5642

Transaction date: : Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 325.25

Block mined: 009b7ed61d1282e8ec8edcd64b1962e601ae0a9757affa0f5fb6f39142418b66

Client publicKey:
04a709bce3d44f25cb3bd8a57a3412879ff971d5de6522bca10aa553b32507165c1440ff615dbc147c43787d259acfe383b536d27c8e11291c457128eacb738e09

Merchant publicKey:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea9284345d2c533cbf108119588dd0e6f5642

Transaction date: : Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 250.99

Block mined: 00c97f7830c93a62b9dc0d15a797c1fc39fa2ea3b7f10199c3c39e6a33c07126

Client publicKey:
044dd948ed7fdd98a7938cdc56de1e50faf36624b43942604a531dc3fe7af2e62f4f911c76e7c763a51c097162ee8f631a309e665bad40f99f4a764b0fe52ba773

Merchant publicKey:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea9284345d2c533cbf108119588dd0e6f5642

Transaction date: : Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 40.00

Block mined: 0084b0168c54f3aac50f355eae1f4d834836a9d2558ca4d18fb3d1ead5f9475f

Client publicKey:
04a709bce3d44f25cb3bd8a57a3412879ff971d5de6522bca10aa553b32507165c1440ff615dbc147c43787d259acfe383b536d27c8e11291c457128eacb738e09

Merchant publicKey:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea9284345d2c533cbf108119588dd0e6f5642

Transaction date: : Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 5.00

Block mined: 0054c41187831e8084319c97bb64674ce0e37024f527a0ed6d66dbac7a911b5d

Client publicKey:
04355d5df8305ba120b8c0fc40cea8364e30df520f7e96ae0e4b70e5c2dd0f0abd367102a69222f0d926b975e1f9378f00471b244e19d4001b4ddaf1c9cf2cfd08

Merchant publicKey:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea9284345d2c533cbf108119588dd0e6f5642

Transaction date: : Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 10.10

Block mined: 00d8dd6e7fe4e1c919627ff19acedccbce2220e38f4c515c85dc06541235101a

Client publicKey:
044dd948ed7fdd98a7938cdc56de1e50faf36624b43942604a531dc3fe7af2e62f4f911c76e7c763a51c097162ee8f631a309e665bad40f99f4a764b0fe52ba773

Merchant publicKey:
04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a961cb72366f2c564cd10e33e1bb194817f890c88

Transaction date: : Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 900.00

Block mined: 003f52ea6498c60efdd3a978464ebf514e2aac4cf917cbba29c4f7424aaaee8b

Client publicKey:
04465c2cd7091736b07bee1c3a17759846eef730e250baca5a68c077e3a09ce4ec507bc5b34cffcc8fc653086b4d4106271d7cabbfc5b55d8f7d17f3643354d211

Merchant publicKey:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea9284345d2c533cbf108119588dd0e6f5642

Transaction date: : Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 210.00

Block mined: 0019bb231ac38b7c7a9e6d57c7847a79c9ee6b61464b83e4234c5b1fadbd6f21

Client publicKey:
04465c2cd7091736b07bee1c3a17759846eef730e250baca5a68c077e3a09ce4ec507bc5b34cffcc8fc653086b4d4106271d7cabbfc5b55d8f7d17f3643354d211

Merchant publicKey:
04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a961cb72366f2c564cd10e33e1bb194817f890c88

Transaction date: : Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 178.00

Block mined: 00fdb14a46aaa1d895175af0f6c0ff5a8259f501c79a7046a7bf695a8ce7978a

Client publicKey:
04a709bce3d44f25cb3bd8a57a3412879ff971d5de6522bca10aa553b32507165c1440ff615dbc147c43787d259acfe383b536d27c8e11291c457128eacb738e09

Merchant publicKey:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea9284345d2c533cbf108119588dd0e6f5642

Transaction date: : Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 49.00

Block mined: 00d2e132b36d7ae5e02414f9a51a656aae9946075c21bac04b9fb1d4457ec955

Client publicKey:
04355d5df8305ba120b8c0fc40cea8364e30df520f7e96ae0e4b70e5c2dd0f0abd367102a69222f0d926b975e1f9378f00471b244e19d4001b4ddaf1c9cf2cfd08

Merchant publicKey:
045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea9284345d2c533cbf108119588dd0e6f5642

Transaction date: : Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 5.29

Block mined: 0004b7f8bcad809c20df1cd40eb3b7681a7505fd54890fb980c9045c20143989

Client publicKey:
047b823fd722e0ade40438b94f3d4658e1d6632835436de8ecf8c757f1245f0237d4120b1310b8fb084be6afe3849550dc6a797ea77501952a30eb66472d95449e

Merchant publicKey:
04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a961cb72366f2c564cd10e33e1bb194817f890c88

Transaction date: : Fri Feb 07 2020 03:45:21 GMT-0500 (Eastern Standard Time)

Transaction amount: 190.00

Block mined: 0056597cacf421a50610c311fc12c9e776e5c117684d8395adfa911ccf43c6f7

Increment the amount in transaction (in block 10) by $10.00

Blockchain valid? No

List all transactions for customer 3 (C3)

Transaction {

clientPubicKey:
'044dd948ed7fdd98a7938cdc56de1e50faf36624b43942604a531dc3fe7af2e62f4f911c76e7c763a51c097162ee8f631a309e665bad40f99f4a764b0fe52ba773',

merchantPubicKey:
'04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a961cb72366f2c564cd10e33e1bb194817f890c88',

amount: 29,

timestamp: 1581237921193,

signature:
'3045022053f9cc7905e1b561220194dc4471bd70c5b9d2590d403a3b36427a428bc17d040221008ce8862ce5eca927337ab51f2a372d3e013cd5afc05811c953bc7e3b4465c40e'

}

Transaction {

clientPubicKey:
'044dd948ed7fdd98a7938cdc56de1e50faf36624b43942604a531dc3fe7af2e62f4f911c76e7c763a51c097162ee8f631a309e665bad40f99f4a764b0fe52ba773',

merchantPubicKey:
'04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a961cb72366f2c564cd10e33e1bb194817f890c88',

amount: 49,

timestamp: 1581237921197,

signature:
'3045022053f9cc7905e1b561220194dc4471bd70c5b9d2590d403a3b36427a428bc17d040221008ce8862ce5eca927337ab51f2a372d3e013cd5afc05811c953bc7e3b4465c40e'

}

Transaction {

clientPubicKey:
'044dd948ed7fdd98a7938cdc56de1e50faf36624b43942604a531dc3fe7af2e62f4f911c76e7c763a51c097162ee8f631a309e665bad40f99f4a764b0fe52ba773',

merchantPubicKey:
'045cff4fd0ed8035e0fa9609697f53cd982c6ec16af02f6255557919351fb16b830df10c7a3d8ccc0adc93369ea7bea9284345d2c533cbf108119588dd0e6f5642',

amount: 40,

timestamp: 1581237921269,

signature:
'3045022053f9cc7905e1b561220194dc4471bd70c5b9d2590d403a3b36427a428bc17d040221008ce8862ce5eca927337ab51f2a372d3e013cd5afc05811c953bc7e3b4465c40e'

}

Transaction {

clientPubicKey:
'044dd948ed7fdd98a7938cdc56de1e50faf36624b43942604a531dc3fe7af2e62f4f911c76e7c763a51c097162ee8f631a309e665bad40f99f4a764b0fe52ba773',

merchantPubicKey:
'04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a961cb72366f2c564cd10e33e1bb194817f890c88',

amount: 900,

timestamp: 1581237921293,

signature:
'3045022053f9cc7905e1b561220194dc4471bd70c5b9d2590d403a3b36427a428bc17d040221008ce8862ce5eca927337ab51f2a372d3e013cd5afc05811c953bc7e3b4465c40e'

}

List all transactions for merchant 2 (M2)

Transaction {

clientPubicKey:
'04355d5df8305ba120b8c0fc40cea8364e30df520f7e96ae0e4b70e5c2dd0f0abd367102a69222f0d926b975e1f9378f00471b244e19d4001b4ddaf1c9cf2cfd08',

merchantPubicKey:
'04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a961cb72366f2c564cd10e33e1bb194817f890c88',

amount: 10,

timestamp: 1581237921118,

signature:
'304502201dc4d00b86a9af7bbb0dc808ffc3bf3205aa33b55f12612b1e7b469db50cd315022100d954d247740c5193f23c751f22cfb05e9a0281c30a9b04a47aea7cdd1a95bcb7'

}

Transaction {

clientPubicKey:
'044dd948ed7fdd98a7938cdc56de1e50faf36624b43942604a531dc3fe7af2e62f4f911c76e7c763a51c097162ee8f631a309e665bad40f99f4a764b0fe52ba773',

merchantPubicKey:
'04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a961cb72366f2c564cd10e33e1bb194817f890c88',

amount: 29,

timestamp: 1581237921193,

signature:
'3045022053f9cc7905e1b561220194dc4471bd70c5b9d2590d403a3b36427a428bc17d040221008ce8862ce5eca927337ab51f2a372d3e013cd5afc05811c953bc7e3b4465c40e'

}

Transaction {

clientPubicKey:
'044dd948ed7fdd98a7938cdc56de1e50faf36624b43942604a531dc3fe7af2e62f4f911c76e7c763a51c097162ee8f631a309e665bad40f99f4a764b0fe52ba773',

merchantPubicKey:
'04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a961cb72366f2c564cd10e33e1bb194817f890c88',

amount: 49,

timestamp: 1581237921197,

signature:
'3045022053f9cc7905e1b561220194dc4471bd70c5b9d2590d403a3b36427a428bc17d040221008ce8862ce5eca927337ab51f2a372d3e013cd5afc05811c953bc7e3b4465c40e'

}

Transaction {

clientPubicKey:
'04a709bce3d44f25cb3bd8a57a3412879ff971d5de6522bca10aa553b32507165c1440ff615dbc147c43787d259acfe383b536d27c8e11291c457128eacb738e09',

merchantPubicKey:
'04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a96
1cb72366f2c564cd10e33e1bb194817f890c88',

amount: 69,

timestamp: 1581237921231,

signature:
'3046022100e1e41b83fa6c5ed7de049a27a099d32a854896d9d57f159961904530aa2ebe85022100a8405bf9623
88618bc7c2f1756bcf31e67ec940109f305c8af09799c6d1949f6'

}

Transaction {

clientPubicKey:
'04355d5df8305ba120b8c0fc40cea8364e30df520f7e96ae0e4b70e5c2dd0f0abd367102a69222f0d926b975e1f93
78f00471b244e19d4001b4ddaf1c9cf2cfd08',

merchantPubicKey:
'04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a96
1cb72366f2c564cd10e33e1bb194817f890c88',

amount: 44,

timestamp: 1581237921236,

signature:
'304502201dc4d00b86a9af7bbb0dc808ffc3bf3205aa33b55f12612b1e7b469db50cd315022100d954d247740c51
93f23c751f22cfb05e9a0281c30a9b04a47aea7cdd1a95bcb7'

}

Transaction {

clientPubicKey:
'044dd948ed7fdd98a7938cdc56de1e50faf36624b43942604a531dc3fe7af2e62f4f911c76e7c763a51c097162ee8f
631a309e665bad40f99f4a764b0fe52ba773',

merchantPubicKey:
'04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a96
1cb72366f2c564cd10e33e1bb194817f890c88',

amount: 900,

timestamp: 1581237921293,

signature:
'3045022053f9cc7905e1b561220194dc4471bd70c5b9d2590d403a3b36427a428bc17d040221008ce8862ce5eca
927337ab51f2a372d3e013cd5afc05811c953bc7e3b4465c40e'

}

Transaction {

clientPubicKey:
'04465c2cd7091736b07bee1c3a17759846eef730e250baca5a68c077e3a09ce4ec507bc5b34cffcc8fc653086b4d4106271d7cabbfc5b55d8f7d17f3643354d211',

merchantPubicKey:
'04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a961cb72366f2c564cd10e33e1bb194817f890c88',

amount: 178,

timestamp: 1581237921325,

signature:
'3045022100af926376add4f533860c02b8ff8ebd61095442ec0f4cd9186288c72d9b69b690022078230d871606f4163573eb98041e97d35b1df6a0d8bfbfbae65328e196af9e87'

}

Transaction {

clientPubicKey:
'047b823fd722e0ade40438b94f3d4658e1d6632835436de8ecf8c757f1245f0237d4120b1310b8fb084be6afe3849550dc6a797ea77501952a30eb66472d95449e',

merchantPubicKey:
'04e66d26b7141f8177cfbc9d04c8ef2521bc9e8ba27e3e57b8b4ba60b891e4430be89a74e2d9d4b3fb77ad0e1a961cb72366f2c564cd10e33e1bb194817f890c88',

amount: 190,

timestamp: 1581237921371,

signature:
'3045022040130b8242f9018c115ee4e198d2a0628357a813d93153e4908dd6af194a6394022100f142bbc9edd5f8015d631bc84b931892cabb6ff7f8517c64f904317a4e1e1522'

}