CS731: Blockchain Technology & Applications Report

1. Name: Mayank Sharma
2. Roll No. 160392

“I did not violate any honor code to do this assignment. All the code is written by me only”

What I did?

For debugging purposes, I introduced a `DEBUG` flag in the `Makefile` which I used throughout my code to enable/disable debugging. Just an `export DEBUG=1` turns on debugging.

For `txn_t::validate()` function:

1. First of all I had to calculate the hash of public_key which needs to be the source address. A check was performed for this.
2. Secondly, by using various SHA256* functions, I calculated the overall transaction hash, and then verified it with the `tx_hash` property on `txn_t` object.
3. Finally, I verified the signature of the transaction. If atleast one of these conditions returned false, then transacation was invalid and further processing (update_balance) of that transaction won’t happen.

For `txn_t::update_balances()` function:

1. I replaced the assert statements with `if` conditions.
2. *Optimization Performed* : Earlier, I was storing the `source_addr` in the `balance_map` even though `source_addr` will have `0` balance after a transaction. So, I erased the `source_addr` from the `balance_map`, and this vastly improved the performance of my code.

For `block_t::validate()` function:

1. I looped over all the transactions in block, verified them, updated the balances based on transaction validity and then finally checked the present `block_hash` with the calculated `block_hash`. If these were equal, I awarded the `reward_addr` with a `BLOCK_REWARD`.

`test1.sh` file output

```
PASS t1
PASS t2
PASS t3
```

`test2.sh` file output

```
t4/1


real	0m3.276s
user	0m2.795s
```

```
sys 0m0.033s
PASS t4
t4/2

real    0m2.845s
user    0m2.812s
sys 0m0.023s
PASS t4
t4/3

real    0m3.077s
user    0m3.022s
sys 0m0.033s
PASS t4
t5/1

real    0m11.975s
user    0m11.794s
sys 0m0.139s
PASS t5
t5/2

real    0m11.751s
user    0m11.632s
sys 0m0.100s
PASS t5
t5/3

```

```
real    0m11.847s
user    0m11.688s
sys 0m0.140s
PASS t5
t6/1

real    0m46.773s
user    0m46.256s
sys 0m0.388s
PASS t6
t6/2

real    0m45.462s
user    0m44.969s
sys 0m0.426s
PASS t6
t6/3

real    0m46.201s
user    0m45.709s
sys 0m0.415s
PASS t6
```