**SUTDcoin Project**

**50.037 Blockchain Technology**

**Presented by: GOLD EXPERIENCE**

**How to run**

1. Simulate miners running Nakamoto consensus and making transactions
   1. new blocks arrive every few (2-5) seconds
   2. coinbase transaction of 100 SUTDcoins
   3. random transactions occur
   4. validation checks (no double spending, validated sender, sender must have enough money)
   5. forks resolved
2. Demonstrate interaction of SPV clients with miners
   1. associated key pairs
   2. receive block headers
   3. receive transactions and verify them
   4. send transactions
3. Demonstrate double-spending via 51% attack
4. Demonstrate selfish-mining

**Major differences between Bitcoin and SUTDcoin**

**Week 3-6 questions**

**Question 1**

Design and implement a Miner class realizing miner's functionalities. Then, implement a simple simulator with miners running Nakamoto consensus and making transactions:

* Adjust the TARGET (global and static) parameter, such that on average new blocks arrive every few (2-5) seconds.
* A miner who found a new block should be rewarded with 100 SUTDcoins.
* Introduce random transactions, such that miners (with coins) can send transactions to other miners.
* Make sure that coins cannot be double-spent.
  + consider the addr:balance model and the UTXO model. What are pros and cons?
  + do you need to modify (why, if so) the transaction format introduced in the first week? *Hint:* yes, you need.
* Extend the verification checks.
* Simulate miners competition.

**Question 1**

Design and implement an SPVClient class. SPV clients should implement a simple SPV logic, i.e., they should:

* have their key pairs associated
* be able to receive block headers (not full blocks)
* be able to receive transactions (with their presence proofs) and verify them
* be able to send transactions

Integrate your implementation with your simulator from the previous exercise. Test your implementation.

**Question 2**

Move actors of your protocol (i.e., miners and SPV clients) to stand-alone applications. For their communication, design and implement a simple network protocol. Your protocol should be able to handle different kind of messages (e.g., SPV clients need only headers, miners need to synchronize entire blocks, ...).

To implement the network protocol you can use your favorite tools (e.g., the HTTP protocol and Flask). You can simplify some functionalities (but ask before) like node discovery (e.g., a file with participants' addresses is good enough).

### Question 1

Implement and demonstrate double-spending via the 51% attack.

### Question 2

Implement and demonstrate the selfish-mining attack.

**Question 1**

Prepare your code for a demonstration including:

* mining and coin creation
* fork resolution
* transaction resending protection
* payments between miners and SPV clients
  + transaction validation (for miners and SPV clients)
* the attacks from the previous week

Conduct a demonstration and prepare a document reporting on it. In your report please also document how to reproduce your demonstration and highlight major differences between Bitcoin and your SUTDcoin.