Course: CSL7490: Introduction to Blockchain

Assignment 1

Max. Marks: 25 **Due Date: 15.09.2022**

Consider the following scenario: you and your friends are transferring money from one account to another. You go to your bank and request that a particular amount be transferred from your account to your friend's account. This is recorded on the bank's internal servers. This record must be updated on both the receiver's and sender's accounts.

There are few issues which may generates in banking system are:

- Intermediation.
- Failure of centralized server.
- Transaction alteration.
- Fake entry in the transactions.

To solve these problems you need to implement blockchain technology by satisfying following criteria:

- Create at least 10 nodes as miners who are connected to each other. Each miner is connected to at least 2 usres. (5 Marks)
- Create a wallet which contains private and public keys. (4 Marks)
- Use the hash of the public key as the address of each user’s wallet. (2 Marks)
- Using digital signatures verify the sender and receiver. (4 Marks)
- The header of a block in the blockchain should contain: block index, timestamp, previous block hash, and merkle root. (4 Marks)
- The body of the block should contain the hash of each transaction. (2 Marks)
- Store the transactions in UTXO format (w.r.t. Bitcoin wallet). (4 Marks)