**Design Document- Assignment 1**

**Crypto-Currency**

There will be a DNS server which will be responsible for the maintenance of DHT servers and handle the addition of new nodes in the network. All the DHT servers will be responsible for maintaining hash table of addresses and public keys of all the accounts.

In order to commit the transaction using a 2 phase commit protocol there will be a sender, a receiver and a witness. The sender will send the transaction details to witness and receiver which then send a response back to the sender once they are ready to commit. After getting confirmation from the sender they commit the transaction.

If a transaction is successfully committed, the sender will broadcast it to all the online nodes. A transaction contains transaction id, account numbers of all the 3 parties (sender, receiver, witness) involved, amount to be transferred, list of input transactions and a digital signature.

Each Node will verify transaction is valid.

Verification

1. If the input transaction is in UTXO pool.
2. Run the public script to verify that transaction follows the rules.
3. If correct then it will it to its block.

Each node will be computing the hash puzzle to find the **NOUNCE** of the block so that it could add it to the block chain. Once nounce is found then it will broadcast nounce and block to all other node. Other nodes will verify the block and add it to its block chain.

DNS Server

Addresses of all the nodes and DHT servers

**Modules**

1. DNS Server
2. DHT Servers
3. P2P Nodes