**Practical 1F**

**Aim: Add blocks to the miner and dump the blockchain.**

# following imports are required by PKI

import hashlib

import random

import binascii

import datetime

import collections

from Crypto.PublicKey import RSA

from Crypto import Random

from Crypto.Cipher import PKCS1\_v1\_5

from collections import OrderedDict

import Crypto

import Crypto.Random

from Crypto.Hash import SHA

from Crypto.Signature import PKCS1\_v1\_5

class Client:

    def \_\_init\_\_(self):

      random = Random.new().read

      self.\_private\_key = RSA.generate(1024, random)

      self.\_public\_key = self.\_private\_key.publickey()

      self.\_signer = PKCS1\_v1\_5.new(self.\_private\_key)

    @property

    def identity(self):

      return binascii.hexlify(self.\_public\_key.exportKey(format='DER')).decode('ascii')

class Transaction:

    def \_\_init\_\_(self, sender, recipient, value):

       self.sender = sender

       self.recipient = recipient

       self.value = value

       self.time = datetime.datetime.now()

    def to\_dict(self):

       if self.sender == "Genesis":

          identity = "Genesis"

       else:

          identity = self.sender.identity

       return collections.OrderedDict({

          'sender': identity,

          'recipient': self.recipient,

          'value': self.value,

          'time' : self.time})

    def sign\_transaction(self):

       private\_key = self.sender.\_private\_key

       signer = PKCS1\_v1\_5.new(private\_key)

       h = SHA.new(str(self.to\_dict()).encode('utf8'))

       return binascii.hexlify(signer.sign(h)).decode('ascii')

def display\_transaction(transaction):

       #for transaction in transactions:

       dict = transaction.to\_dict()

       print ("sender: " + dict['sender'])

       print ('-----')

       print ("recipient: " + dict['recipient'])

       print ('-----')

       print ("value: " + str(dict['value']))

       print ('-----')

       print ("time: " + str(dict['time']))

       print ('-----')

def dump\_blockchain (self):

   print ("Number of blocks in the chain: " + str(len (self)))

   for x in range (len(TPCoins)):

      block\_temp = TPCoins[x]

      print ("block # " + str(x))

      for transaction in block\_temp.verified\_transactions:

         display\_transaction (transaction)

         print ('--------------')

      print ('=====================================')

class Block:

   def \_\_init\_\_(self):

      self.verified\_transactions = []

      self.previous\_block\_hash = ""

      self.Nonce = ""

def sha256(message):

      return hashlib.sha256(message.encode('ascii')).hexdigest()

def mine(message, difficulty=1):

   assert difficulty >= 1

   #if(difficulty <1):

   #        return

   #'1'\*3=> '111'

   prefix = '1' \* difficulty

   for i in range(1000):

      digest = sha256(str(hash(message)) + str(i))

      if digest.startswith(prefix):

         return i #i= nonce value

A = Client()

B =Client()

C =Client()

t0 = Transaction (

   "Genesis",

   A.identity,

   500.0

)

t1 = Transaction (

   A,

   B.identity,

   40.0

)

t2 = Transaction (

   A,

   C.identity,

   70.0

)

t3 = Transaction (

   B,

   C.identity,

   700.0

)

#blockchain

TPCoins = []

block0 = Block()

block0.previous\_block\_hash = None

Nonce = None

block0.verified\_transactions.append (t0)

digest = hash (block0)

last\_block\_hash = digest #last\_block\_hash it is hash of block0

TPCoins.append (block0)

block1 = Block()

block1.previous\_block\_hash = last\_block\_hash

block1.verified\_transactions.append (t1)

block1.verified\_transactions.append (t2)

block1.Nonce=mine (block1, 2)

digest = hash (block1)

last\_block\_hash = digest

TPCoins.append (block1)

block2 = Block()

block2.previous\_block\_hash = last\_block\_hash

block2.verified\_transactions.append (t3)

Nonce = mine (block2, 2)

block2.Nonce=mine (block2, 2)

digest = hash (block2)

last\_block\_hash = digest

TPCoins.append (block2)

dump\_blockchain(TPCoins)

#####################################################################

Output:

Number of blocks in the chain: 3

block # 0

sender: Genesis

-----

recipient: 30819f300d0609…..

-----

value: 500.0

-----

time: 2022-04-26 04:30:59.070952

-----

--------------

=====================================

block # 1

sender: 30819f300d06092a86…..

-----

recipient: 30819f300d06092a…..

-----

value: 40.0

-----

time: 2022-04-26 04:30:59.071076

-----

--------------

sender: 30819f300d06092a86….

-----

recipient: 30819f300d06092a….

-----

value: 70.0

-----

time: 2022-04-26 04:30:59.071174

-----

--------------

=====================================

block # 2

sender: 30819f300d06092a….

-----

recipient: 30819f300d06092a….

-----

value: 700.0

-----

time: 2022-04-26 04:30:59.071272

-----

--------------

=====================================