Name :- Udoy Saha
ID :- 23341134
Section :- 01

CSE 446
Assignment

Ans to the ques no :- 1

Bitcoin uses the following cryptographic operations :-

1. It uses Public and Private key.
2. Since public keys are long, Bitcoin uses elliptic curve (secp256k1) to hash the public key and generate its address.

—o——x——o—

Ans to the ques no :- 2

A valid owner can claim and spend their Bitcoin using their Private key.

We know a user receives coins with their address. The received coin gets validated with the receivers private key. An incoming request needs a proof to be claimed. With

an incoming request, there comes a ScriptSig key that contains the digital signature from the sender. The ScriptSig needs to be validated using the receivers keys in order to claim the coin.

Similarly, a sender needs to sign the transaction using their private key to spend the Bitcoin. Finally both needs to broadcast the transaction to the network.

—o—×—o—

Ans to the ques no:- 3

A miner gets reward for mining Bitcoin. The reward is halved in every 210000 blocks, which is around 4 years (1 block = 10 minute). So, being like a geometric series, the reward will at some point reach asymptotically to zero. As no rewards will be given, no

coins will be produced. Till that point when the reward will be asymptotically zero, there will be 21 million Bitcoins only.

Bitcoins are fundamentally made to avoid inflation. Therefore, as a deflationary currency, there is no mechanism to create additional bitcoins once 21 million ~~conse~~ coins are mined. Though, ~~thee~~ technically its possible if there is a consensus among the majority of users. But that will violate the scarcity priciple of Bitcoin.

— o — x — o —

Ans to the ques no:- 4

Bitcoin ensures a block is created in every 10 minutes by manipulating the difficulty value.

Bitcoin developers have set the block creation

time to be 10 minutes to ensure atomicity and security. The solved double hash of (V||H||M||T||N) ~~show~~ needs to be less than the difficulty value. The Blockchain network always measures how much coin is generated in any time duration. When there is more than 1 block generated in 10 minutes, the difficulty value gets reduced, making it harder to produce a block the next few minutes. In the same way, when blocks are under-produced, the difficulty value is increased which helps produce more blocks.

In this way Bitcoin ensures a block is created in 10 minutes on an average.

—o— ~ —o—

Ans to the ques no:- 5

The features of Bitcoin that I would like to adopt :

1. Scarcity : There should be a limited amount of supply and no possibility of inflation.
2. Decentralization :- I would adopt the distributed approach, so that no single authority can influence over the whole system.
3. Immutability :- Once a block is validated, I would like to adopt the fact that the block can never be impaired.
4. Private key based encryption :- Integration of the cryptographic abilities to ensure security.

The changes I would like to make :-

1. Energy efficiency :- PoS based validation system instead of PoW to lessen energy consumption.
2. Faster validation :- Would introduce a validation system that works much faster than 10 minutes.
3. More condition on block / transaction validation :-

some automated system that could validate and introduce more conditions while receiving or sending a transaction.

4. Account based ledger:- To make a user's balance more feasible to calculate.

—o— × —o—

Ans to the ques no:-6

The PoW puzzle ensures that some miner has spent computational power and generated a block and added to the blockchain. It prevents malicious actions from the attackers because the puzzle solving is computationally very expensive, making the system secure and reliable.

It solves the puzzle first by concatenating the version(v), hash of Merkle root (m), header

hash (H), time (T), and a random value nonce (N). Then it double-hashes the whole thing like SHA256(SHA256(V||H||M||T||N)), and compares the value with D (difficulty). If the hash value is less than D, the block is validated.

After a miner has found a correct nonce value and generated a block, it broadcasts the block to the network; when the block reaches other miners, the other miners try to validate the block. If the block is valid, all the other miners stop working on that block and adds it to their block-chain. In this process the block gets added to the entire blockchain and acheives consensus.

—o— * —o—

Ans to the ques no:-7

(a)

Bob is sending Tx1. Because, Tx1 uses the input Tx0[0], which was sent for Bob.

Alice is sending Tx2. Because, Tx2 uses Tx1[1], which was sent for Alice.

(b)

For Tx1, fee = (5·25) - (0·2 + 5 + 0·02)

= 0·03 BTC

For Tx2, fee = (5) - (1 + 3·99)

= 0·01 BTC

(c)

To be a valid transaction, fee should be greater on equal to 0.

For Tx3, fee = (0.2 + 1) - (1.18 + 0.11)

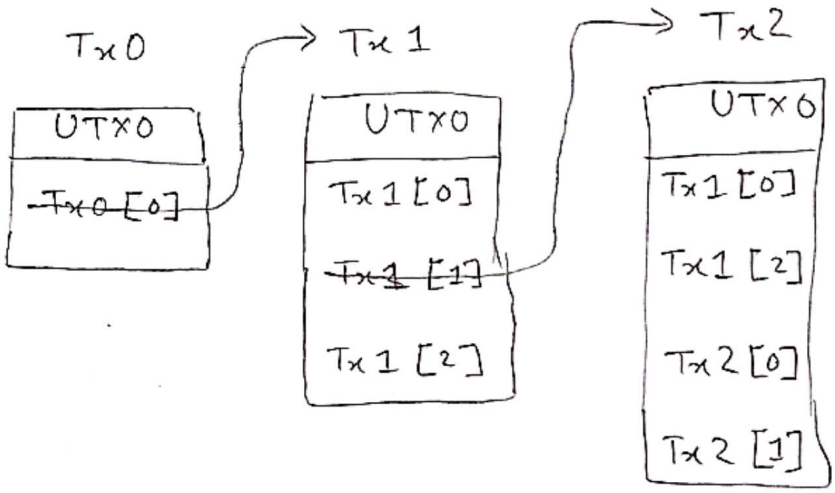
= 1.2 - 1.29

= -0.09

As the fee is negative, Tx3 is invalid.

(d)

The UTXO table after each transaction is shown below :-



So, after Tx1 and Tx2, the UTXO table will look like :-

UTXO table
Tx1 [0]
Tx1 [2]
Tx2 [0]
Tx2 [1]