Blockchain - 2

Huipeng ZENG 5156067

December 2018

1 Assignment 1. Bitcoin Various Topics

1.1 Transaction validation

Step 8, because we have to then traverse all txs in the pool, and in the main branch (within 6 blocks i think).
And steps 10, 12 because we have to traverse main branch and pool to find if there is such a output transaction exist. So i think the best basic data structure for the txs in a block would be tree structure. Because the traverse is the most frequent operation.

1.2 Green addresses

When a user attempts a double spending, then the system looks up into the local transaction records, validates the transactions at first if the input already be spent, if so, then while the user arising the double spending, copies the transaction 10000 times and broadcasts them. then the miners would notice this user, and may then block this user.

2 Extra question: more forking

1. They rejected the block which had more than 1000 locks, so i think, the single one largest block, which caused the issue, has been abandoned, since they could not confirm this block, and it use a higher version. (information from https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki) However, I also saw some articles said that, if a hard fork occured, then the coins will be copied and the copied work as usual in new fork.
2.
3.

3 Assignment 2. Transaction fees

1. Assume that Alice has n value v BTC, so the

   $transSize = 148 * n + 34 * 1 + 10 = 148 * n + 44$

   The transaction fee $= n * v = \frac{0.0001 * transSize}{1000} = \frac{148*n+44}{10000000}$

   Let's omit 44 at $148 * n + 44$, regard of the a is a "large number of coins". so, we can get the solution that $v = 1.48 * 10^{-5}$

2. Yes, because Alice has large number of extra small value coins,it can then only fill the third condition if she wants to make a free fee transaction.

   Assume when the priority = 1, means it is large enough. so,$Priority = \frac{n*inputAge*1.48*10^{-5}}{148*n+44} = 1$

   again, we omit 44 at $148 * n + 44$, $inputAge = 10^7$

   So Alice has to wait 10^7 time unit until transaction be involved in block.

3. - User has to wait longer if they made small amount transactions which the transSize is large than 1000 byte.
   - But they can speed the transactions up, if a transaction is urgent, but which also means that they have to pay more fee for it.
   - It would make the system more efficient, since the users will than avoid small amount transactions.

4 Assignment 3. Multi-signature wallet

1. Use another 2 private keys to generate the hash, and compare this hash with the three hashes that we stored, make another two hashes out of use. And regenerate a new private key after that, then regenerate and restored new hashes with other two private keys.

2. Generate another new private key and send it to users, and unable old hash, and replace it with new hash at the same time.

5 Assignment 4. Node in a blockchain

Sorry, my partner dropped out, and I haven't got enough time to finish the test. I creates two coinbase block, and tried to add one transaction in the third block by using blockhandler, but there are still some errors there.