Blockchain and Cryptocurrencies Final Exam

Divij Singh

10/05/19

1 Q1

The time would be 2019-05-06 03:26:56, according to `https://blockchain.com`

2 Q2

One such h would be 0, i.e the genesis block.

3 Q3

It would be roughly around 575,374, judging by trends on `https://blockexplorer.com`

4 Q4

Judging by statistic from blockchain.com, it would be around 410,849,309 total transactions.

5 Q5

Yes, it is possible. One account could be sending the currency to two or more adresses (not counting the address for change).

6 Q6

Yes, it is possible. The funds could come from a combination of accounts, rather than just one.

7 Q8

Currently, it takes roughly 9.8 minutes for a new block to be mined, according to blockchain.com. Thus, the nLockTime would be roughly 16 hours, 20 minutes from the time of txn creation.

8 Q9

Yes, as the two input scripts have a witness each. Though the ScriptSig field has information, it may be due to the sender using an older format.

9 Q10

Yes, as the input script has a witness. (Verified by checking on `https://yogh.io`)

10 Q11

One such txn is 009f9991bbf6c99596d6cad637040630874a12968c381cec4ebecc11368654d5. It contains a Segwit input (contains a witness) and the output is a Segwit ID (it starts with 'bc1', which according to BIP-173 is a Segwit address type) `https://github.com/bitcoin/bips/blob/master/bip-0173.mediawiki#Segwit_address_format`