**Teo Yong Quan**

**1002828**

**Question 1**

Why do we need seeds?

* Seeds act as our wallet recovery key sand allows us to get our wallet bacck in case anything happens to our computers. By downloading the software (electrum) and supplying the seed we can get the same wallet back, preventing the loss of bitcoins.
* The seeds are 12 word long sentences and are as follows
  + (BTC) giggle scene inquiry sense model explain solve icon coil slam abstract teach
  + (ETH) oven anchor buddy pet name travel wisdom essay ten mystery crop arctic

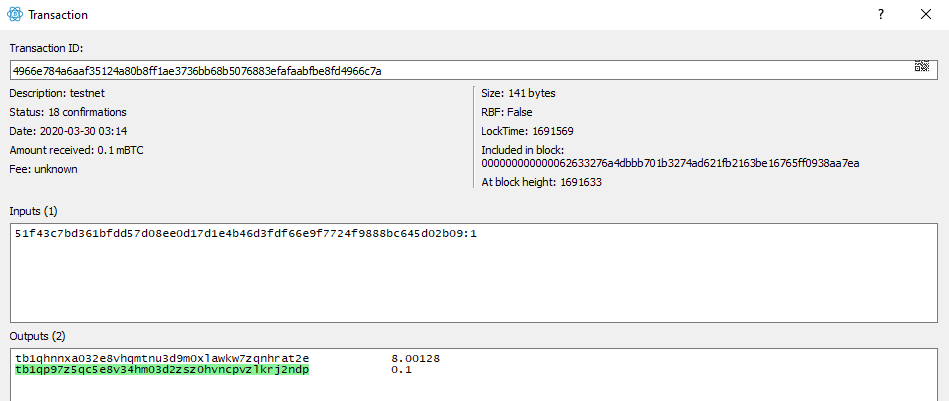
What does it mean by confirmations when you send and receive coins?

When one sends and receive coins, we have to wait for miners to add to mine the block and publish it to the blockchain network. Each time a miner adds a subsequent block, it is counted as 1 confirmation. When there are 6 confirmations, the transactions becomes successful and is counted as confirmed as it is deep in the blockchain and resilient to forks.

Is the total amount transacted in a transaction the same amount that you receive? Why? What is an input? How does a transaction look like? What is an input ? What is an output?

It is not the same. If they sender does not have the exact change, there is another output which is the sender’s remaining bitcoin.

Attached is how a transaction looks like. An input is the pubkey of the sender and an output is the pubkey of myself and the change of the sender.



**Question 2**

1. What is the total amount transacted?

* 0.45297571 BTC / $3,030.68

1. What is/are the receiving address(es)?

* 2MwVzE43EeqCRRbGGAYukTxgsVUvvwN1n5K

1. What is the miner's fee?

* 0.00252621 BTC

1. How the inputs were spent?

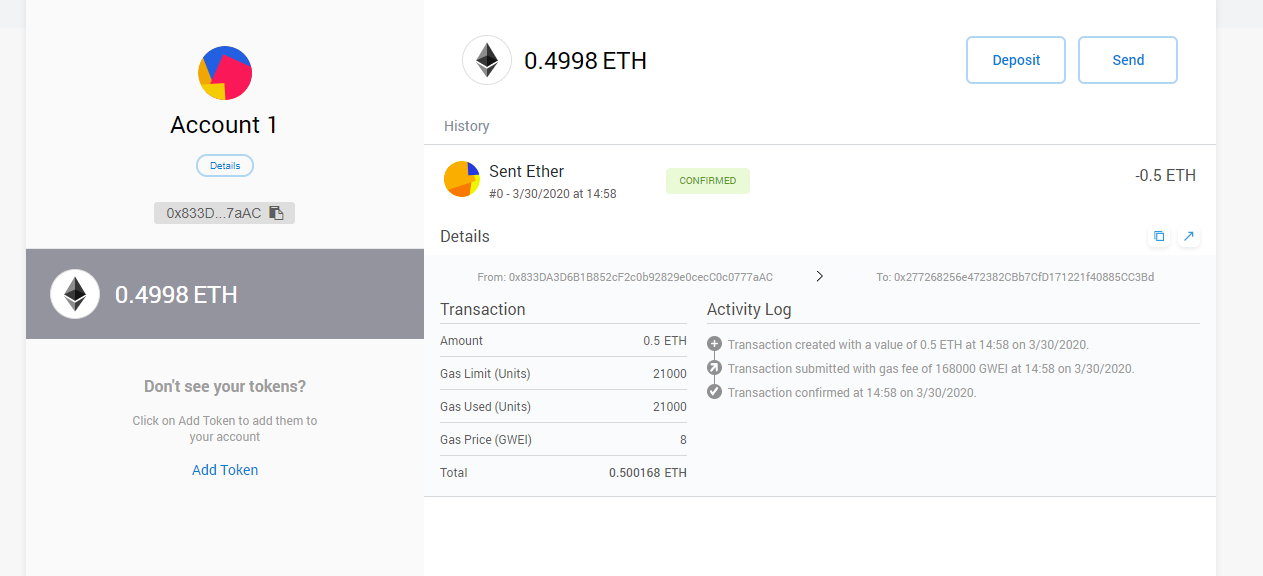
* The inputs from 2 UTXOs were combined to make the transfer.

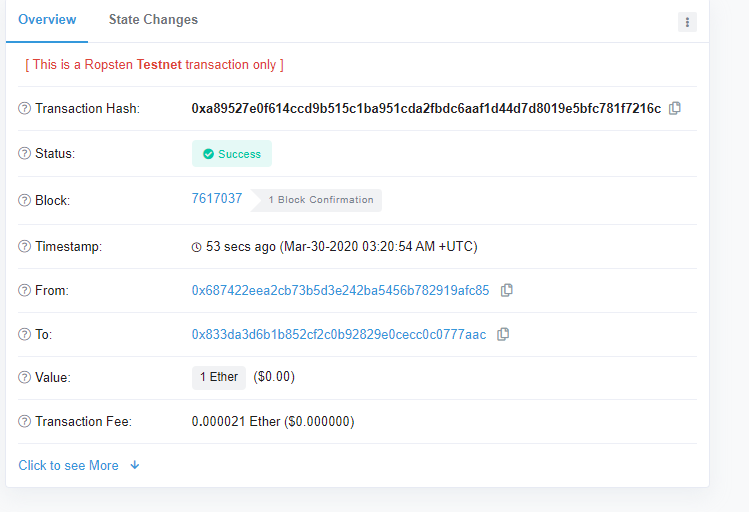
1. Now check the transaction ID 27eb699a9ab24876858bd29c42f3831f036a57c72a3dc701c187d196291afbc8 and compare how these two transactions spent their inputs.

* In this second transaction, there is only 1 input. That means the sender had the exact UTXO for the transaction.

**Question 3**

Using Mist/Metamask, create an Ethereum account, then get and spend some coins. Note: Make sure you are using a Testnet network (e.g., Ropsten).





**Question 4**

Using an Ethereum testnet blockchain explorer (e.g., <https://ropsten.etherscan.io/>), find information about the account with ID: 0xDE314df1A5241D38E9603d784b8A186E0543521E

What is the account's balance?

* 0.999838187 Ether

When was the last transaction performed?

* 11 hrs and 25mins ago

Does it have any smart contract created?

* 1 smart contract created 559 days ago.

**Question 5**

In Bitcoin, we have an option of creating multisig transactions. How it can be realized in Ethereum?

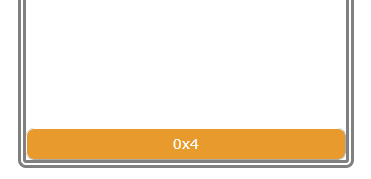
The use of smart contracts can allow multisig transactions.

**Question 6**

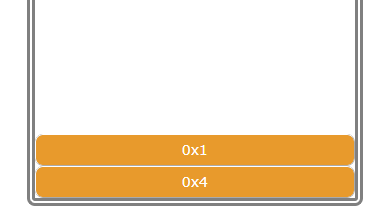
For the following Bitcoin script, draw stages of the stack and determine the outcome (true or false).

* OP\_4 OP\_1 OP\_AND OP\_SHA256 e77b9a9ae9e30b0dbdb6f510a264ef9de781501d7b6b92ae89eb059c5ab743db OP\_EQUAL

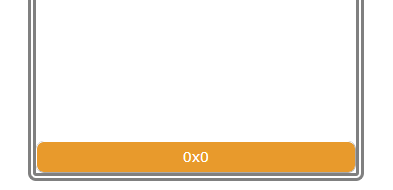
OP\_4 (push 4 into the stack)



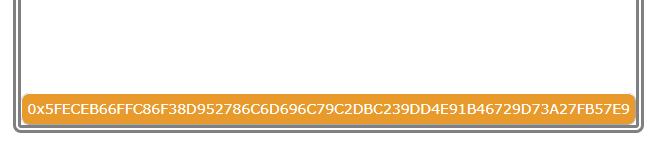
OP\_1 (push 1 into the stack)



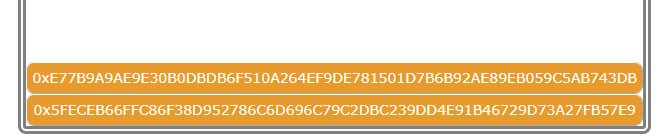
OP\_AND (bitwise and operator on the two elements in the stack)



OP\_SHA256 (performs a sha256 hash on the stack)



Putting e77b9a9ae9e30b0dbdb6f510a264ef9de781501d7b6b92ae89eb059c5ab743db



OP\_EQUAL (check if the contents of the stack are equal)



The script returns false as the two hashes are not the same.