


Electrum testBitcoin

Name: Clemence Goh (1002075)




Question 1

- Seed is needed since it is required to generate a random address
- Seed looks like this:
 - laptop charge clap hawk toy pond pony episode ethics original habit anchor
- "Confirmations" counts the number of blocks which have been mined after the block containing the transaction has been mined in.
- Transactions look like this:



BITCOIN TESTNET TRANSACTION
72c942daddaec91cacfd533f0b7a0e0009548bda8885764100293f8554d5bd40

Estimated TX Value	0.02000000 tBTC	Total Inputs	0.12037509 tBTC
Confirmations	UNCONFIRMED	Total Outputs	0.12037170 tBTC
	OPT-IN RBF	Fee	0.00000339 tBTC
Relay time	Wednesday, October 31st 2018, 11:39:24 +08:00	Fee / KB	0.00001507 tBTC
		Size	225 bytes
		Estimated Change	0.10037170 tBTC
		sent to	n4ceoagCPYx2XFuTAvui17NEwXdrK4mQGx

1 INPUTS	Total Inputs: 0.12037509 tBTC	2 OUTPUTS	0.10037170 tBTC change
 mxewkypxkdDGLWTWG1otsza3qFR7GtTyMD (0.12037509)		my9YzgWGMGuVswr31ufyUSXvXMGzWu49b (0.02000000)	
		n4ceoagCPYx2XFuTAvui17NEwXdrK4mQGx (0.10037170)	

INPUT SCRIPTS	OUTPUT SCRIPTS
30440220648ad98f919f1f189223cd72ddea4499ee4c117d62a1a0bb5e64737dfec1e6cd0 22046a93abf87a44c49333cdf61e851d4647c329f4676fdd6acffac7cc8ff0dbc2201 03ce5c01caad742e4f32883e3dc0a460489dc37a4ebeabab1ef9fc0014ee2f281	OP_DUP OP_HASH160 c16611cf5079678fce6aa63d8a241288b09ddbec OP_EQUALVERIFY OP_CHECKSIG

- Input:
 - Senders and how much they are sending
- Output:
 - Receivers and how much they are receiving
- No. All the balance from the sender will be sent in a transaction. However, since the receiver only receives a part of it, the other "receiver" of the balance would be the sender.

Question 2

Case study:

- Total amount transacted: 3,824.17125018 tBTC (input)
- Receiving addresses:
 - 2N5DKp2kDHoconN3LUtMx8efBQf28BSm3Mt

- n1gen1haVTyg5Ebgoj8kD2HRaxtSGhDCZP

- When did it happen: Wednesday, September 12th 2018, 23:47:03 +08:00
- Yes, it is different. All amount is paid to another account.

Question 3

- The difference lies in the payment only.
- Payment requires all 3 cosigners to agree and create the same transaction

Question 4

- OP_5: 5
- OP_1: 5, 1
- OP_AND: 1
- OP_HASH160: ff056d1a4cf78645eb05ac3c0e0dcaf429de0db3
- 628850cb844fe63c308c62afc8bc5351f1952a7f: ff056d1a4cf78645eb05ac3c0e0dcaf429de0db3, 628850cb844fe63c308c62afc8bc5351f1952a7f
- OP_EQUAL: FALSE