Shayan Hamidi Dehshali SID: 810197493

Part1-Question1) Generating p2pkh Address:

Step1: generating a 32 byte private key using secret library

Step2: In order to, transform private key to WIF format first extend “0xef” to the left of the private key

Step3: if you want your public key compressed extend “0x01” to the right of the step2 outcome

Step4: find checksum of step3 by getting sha256 twice and then get four first bytes of it.Now extend it to the left of the step3

Step5: Encode to Base58 format the result of Step4, Now you have WIF format.

Step6: In order to find Public key, get the result of Step1 and multiply it in the Spec256k1 generating point

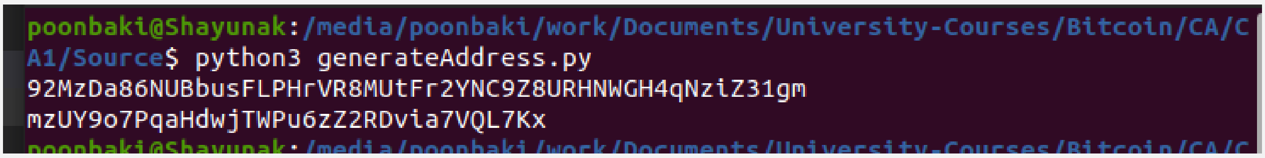
Attention: I have implemented the whole Elliptical Curve functions myself,it is located in ElypticalCurve.py and + and * operators have been overloaded.

Step7: If you want your public key compressed, call the function .to_bytes_compressed().Now take a Sha256 and then a RipeMD160 hash from the public_key.

Step8: Difference: On the Mainnet, Now we extend “0x80” to the left of the hashed public key but on the Testnet, we extend “0x6f” to the left of the hashed public key.

Step9: Extend the checksum of the Step8 result to itself just like Step4.

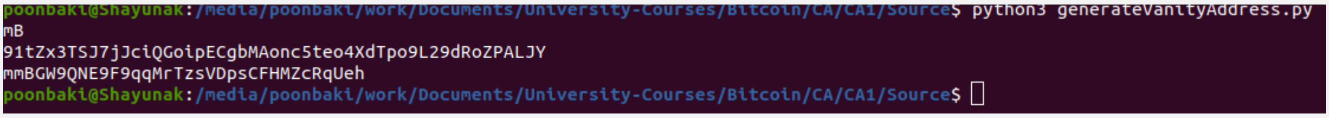
Step10: Now The Base58 format of the result of Step9 is our Address.



```
poonbaki@Shayunak:/media/poonbaki/work/Documents/University-Courses/Bitcoin/CA/C
A1/Source$ python3 generateAddress.py
92MzDa86NUBbusFLPHrVR8MUtFr2YNC9Z8URHNWGH4qNziZ31gm
mzUY9o7PqaHdwjTWPu6zZ2RDvia7VQL7Kx
poonbaki@Shayunak:/media/poonbaki/work/Documents/University-Courses/Bitcoin/CA/C
```

Part1-Question2) Generating Vanity Address:

Our algorithm is brute force based.Using the code from the last question,we keep producing addresses and compare the bytes, that they are in the positions 2..4,to the bytes given in the input.Keep producing addresses till we reach our goal.



```
poonbaki@Shayunak:/media/poonbaki/work/Documents/University-Courses/Bitcoin/CA/CA1/Source$ python3 generateVanityAddress.py
mB
91tZx3TSJ7jJciQGoipECgbMAonc5teo4XdTpo9L29dRoZPALJY
mmBGW9QNE9F9qqMrTzsVDpsCFHMZcRqUeh
poonbaki@Shayunak:/media/poonbaki/work/Documents/University-Courses/Bitcoin/CA/CA1/Source$ 
```

Part1-Question3) Generating Segwit Address:

Step1: According to Question1 get your private key WIF format in compressed form.

Step2: Also get your public key in compressed form(just U_x and an odd/even indicator)(33 bytes)

Step3: Again get a Sha256 and RipeMD160 hash consecutively on the public key

Step4: Using bitcoin.bech32.encode() function, encode your public key hash into bech32 format with “tb” as human readable part(used in Testnet) and witness version 0.Now you have your Segwit address.

Attention: Segwit Addresses separate our signature identity from our block scripts.So we can have:

1) Bigger blocks and storage efficiency
2) Script versioning
3) Offline Signing improvement
4) Signature verification optimization
5) Scalability
6) Transaction Malleability

(Test)Address produced:

`tb1qm83uu3xg7h8s4f026f9n9c8pc0vkpq3hktn9xj`

Private key WIF Format:

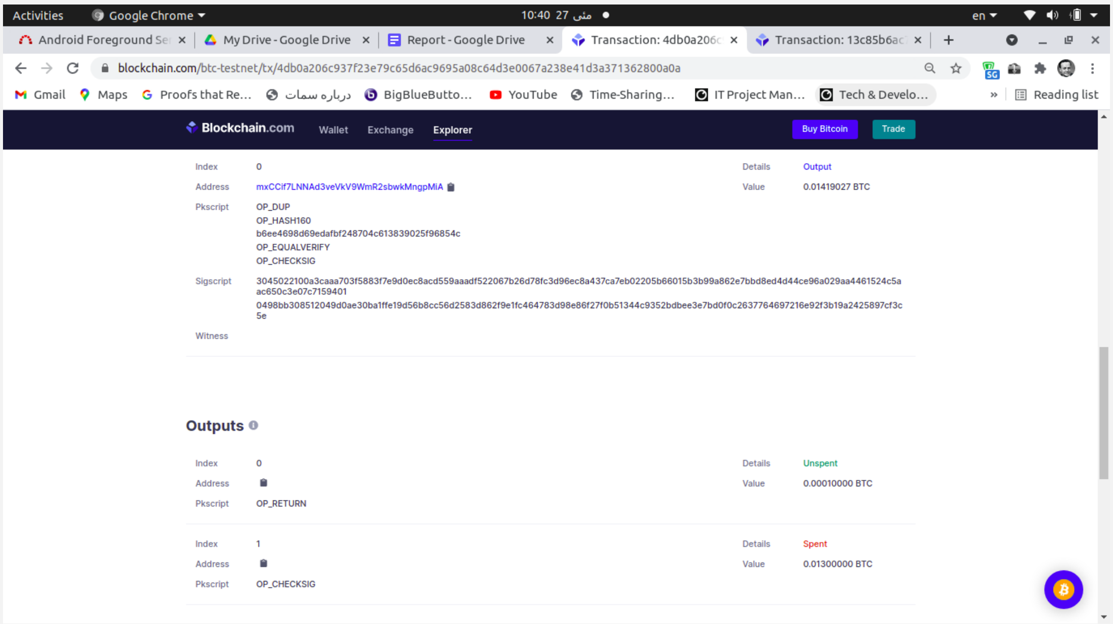
`cSWzxfnTLKAPs5rnVVzTS7fCe68c3kjASg3Ab3T37hf9qbhnY2jx`

Part2) For each Question we use different forms of transaction.py.We also use utils.py, but some extra functions have been added.for each new transaction the main difference is their input/output scripts and also the method to sign the transaction.

Part2-Question1)

1. My Address: mxCCif7LNNAd3veVkV9WmR2sbwkMngpMiA
2. My Private Key(WIF): 91csCMJdVymT5i1YuiPrWkqH9AqZdi2d22bU9oK5ircKYR9saPK
3. Hash Transaction:
   4db0a206c937f23e79c65d6ac9695a08c64d3e0067a238e41d3a371362800a0a
4. Hash Spending Transaction:
   13c85b6ac7fc914883b308693da2cf0810be1491686e8953e276d5decfd5aafd

Our Transaction:



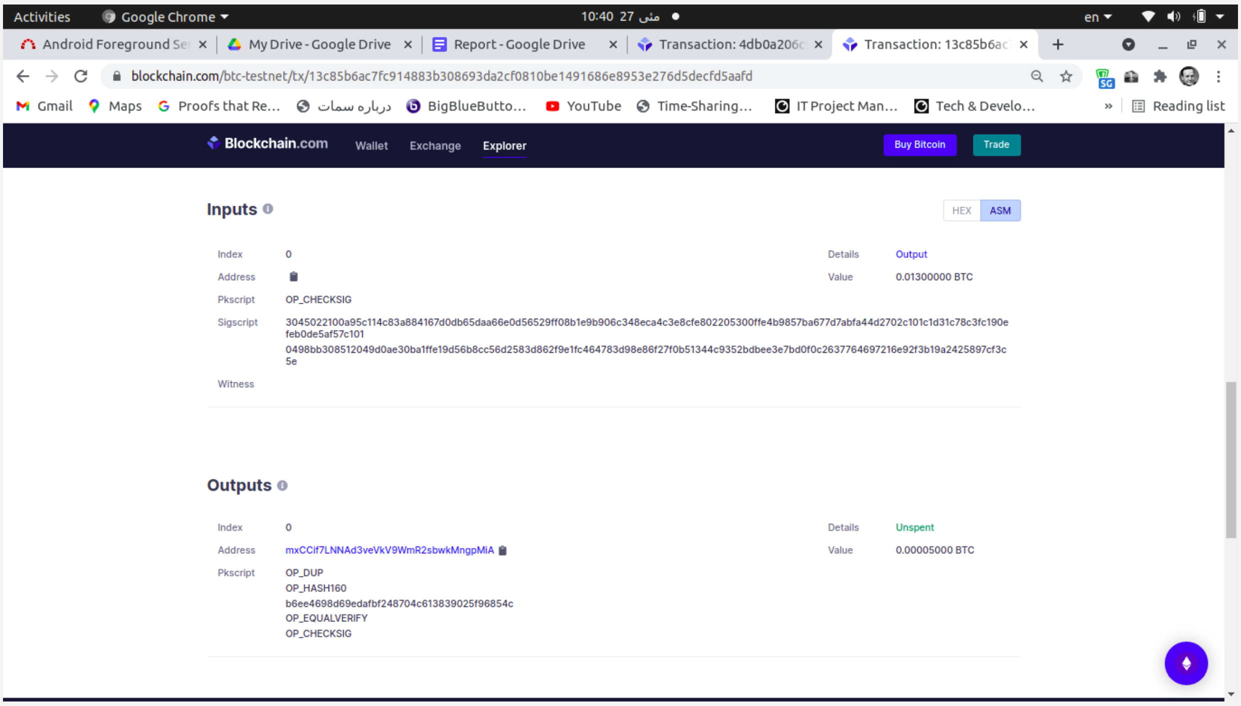
```
Index      0                                              Details   Output
Address    mxCCif7LNNAd3veVkV9WmR2sbwkMngpMiA             Value     0.01419027 BTC
Pkscript   OP_DUP
           OP_HASH160
           b6ee4698d69edafbf248704c613839025f96854c
           OP_EQUALVERIFY
           OP_CHECKSIG
Sigscript  3045022100a3caaa703f5883f7e9d0ec8acd559aaadf522067b26d78fc3d96ec8a437ca7eb02205b66015b3b99a862e7bbd8ed4d44ce96a029aa4461524c5a
           ac650c3e07c7159401
           0498bb308512049d0ae30ba1ffe19d56b8cc56d2583d862f9e1fc464783d98e86f27f0b51344c9352bdbee3e7bd0f0c2637764697216e92f3b19a2425897cf3c
           5e
Witness

Outputs

Index      0                                              Details   Unspent
Address                                                   Value     0.00010000 BTC
Pkscript   OP_RETURN

Index      1                                              Details   Spent
Address                                                   Value     0.01300000 BTC
Pkscript   OP_CHECKSIG
```

Our Spending Transaction:



Inputs

Index 0 Details Output

Address Value 0.01300000 BTC

Pkscript OP_CHECKSIG

Sigscript
```
3045022100a95c114c83a884167d0db65daa66e0d56529ff08b1e9b906c348eca4c3e8cfe802205300ffe4b9857ba677d7abfa44d2702c101c1d31c78c3fc190efeb0de5af57c101
0498bb308512049d0ae30ba1ffe19d56b8cc56d2583d862f9e1fc464783d98e86f27f0b51344c9352bdbee3e7bd0f0c2637764697216e92f3b19a2425897cf3c5e
```

Witness

Outputs

Index 0 Details Unspent

Address mxCCif7LNNAd3veVkV9WmR2sbwkMngpMiA Value 0.00005000 BTC

Pkscript
```
OP_DUP
OP_HASH160
b6ee4698d69edafbf248704c613839025f96854c
OP_EQUALVERIFY
OP_CHECKSIG
```

Part2-Question2)

My Address: mxCCif7LNNAd3veVkV9WmR2sbwkMngpMiA

My Private Key(wif): 91csCMJdVymT5i1YuiPrWkqH9AqZdi2d22bU9oK5ircKYR9saPK

First Private Key(wif): 923qXJ3XEP6Zp2CfDzxAug8rTVrt95Qyv8WKRNPsty7jhuhPNQr

Second Private Key(wif): 935Z9GS9MZGKcd2v6URnPivkW5F9XCt4CYsxe3jui9DYqyexoza

Third Private Key(wif): 92dhsHTLrWC7H8SmctgquXQRrW3c8zVAQAF3V3151GjSwaySDS6

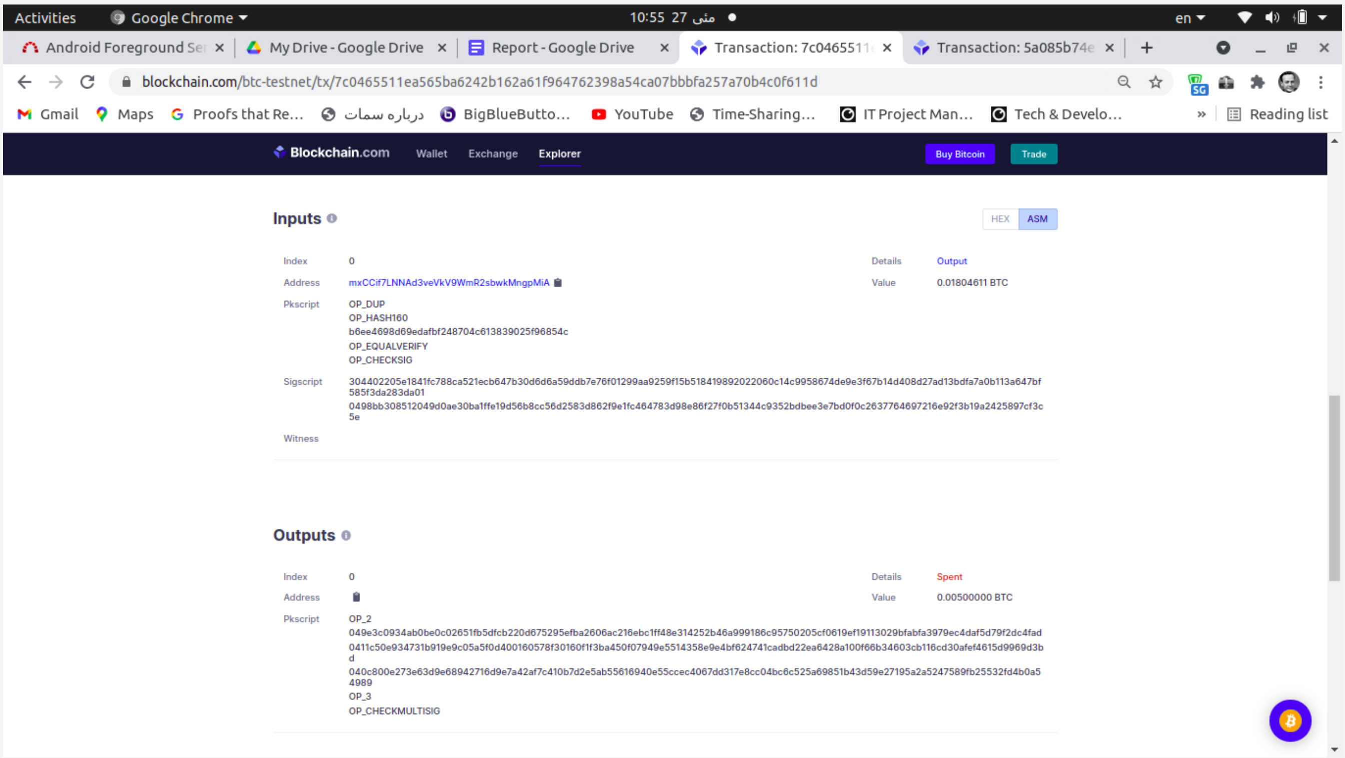
Hash Transaction:

7c0465511ea565ba6242b162a61f964762398a54ca07bbbfa257a70b4c0f611d

Hash Spending Transaction:

5a085b74e174de7de003ff695bb2376ea421f386be6f5a52a439f7861fd97ec6

Our Transaction:



blockchain.com/btc-testnet/tx/7c0465511ea565ba6242b162a61f964762398a54ca07bbbfa257a70b4c0f611d

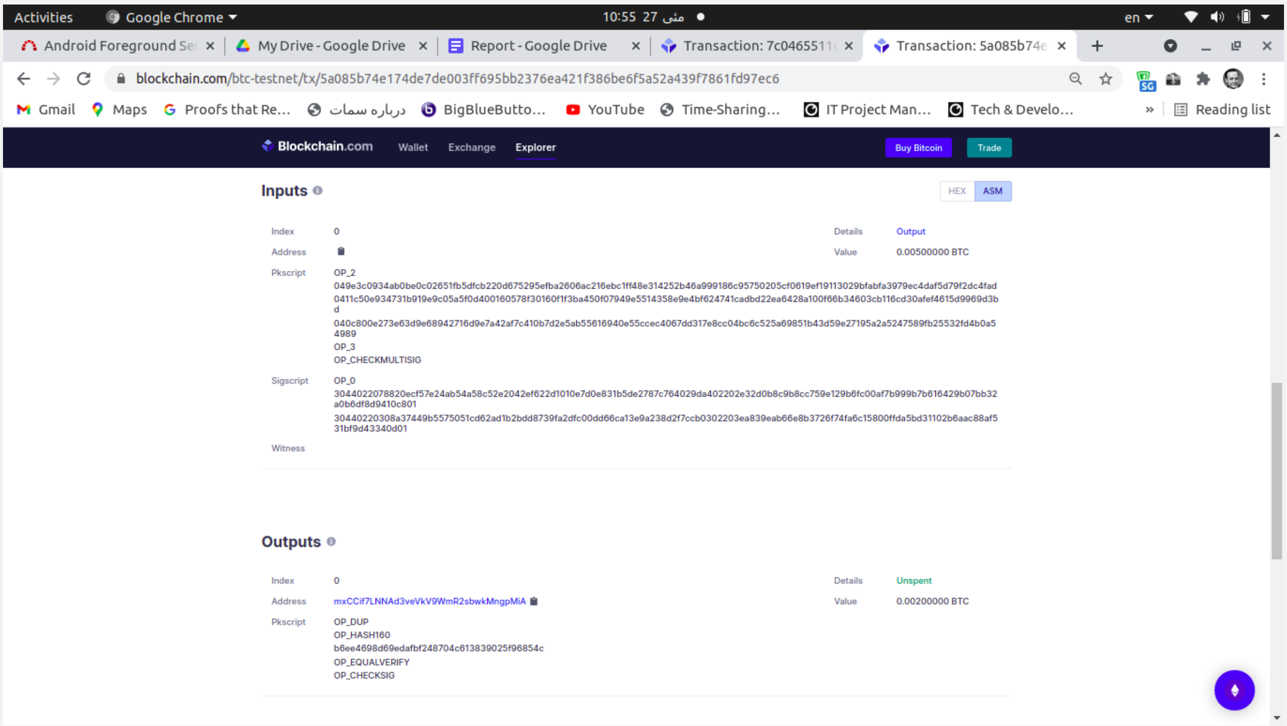
Inputs

```
Index      0                                                   Details   Output
Address    mxCCif7LNNAd3veVkV9WmR2sbwkMngpMiA                  Value     0.01804611 BTC
Pkscript   OP_DUP
           OP_HASH160
           b6ee4698d69edafbf248704c613839025f96854c
           OP_EQUALVERIFY
           OP_CHECKSIG
Sigscript  304402205e1841fc788ca521ecb647b30d6d6a59ddb7e76f01299aa9259f15b518419892022060c14c9958674de9e3f67b14d408d27ad13bdfa7a0b113a647bf
           585f3da283da01
           0498bb308512049d0ae30ba1ffe19d56b8cc56d2583d862f9e1fc464783d98e86f27f0b51344c9352bdbee3e7bd0f0c2637764697216e92f3b19a2425897cf3c
           5e
Witness
```

Outputs

```
Index      0                                                   Details   Spent
Address                                                        Value     0.00500000 BTC
Pkscript   OP_2
           049e3c0934ab0be0c02651fb5dfcb220d675295efba2606ac216ebc1ff48e314252b46a999186c95750205cf0619ef19113029bfabfa3979ec4daf5d79f2dc4fad
           0411c50e934731b919e9c05a5f0d400160578f30160f1f3ba450f07949e5514358e9e4bf624741cadbd22ea6428a100f66b34603cb116cd30afef4615d9969d3b
           d
           040c800e273e63d9e68942716d9e7a42af7c410b7d2e5ab55616940e55ccec4067dd317e8cc04bc6c525a69851b43d59e27195a2a5247589fb25532fd4b0a5
           4989
           OP_3
           OP_CHECKMULTISIG
```

Our Spending Transaction:



blockchain.com/btc-testnet/tx/5a085b74e174de003ff695bb2376ea421f386be6f5a52a439f7861fd97ec6

Inputs

```
Index      0                                                   Details   Output
Address                                                        Value     0.00500000 BTC
Pkscript   OP_2
           049e3c0934ab0be0c02651fb5dfcb220d675295efba2606ac216ebc1ff48e314252b46a999186c95750205cf0619ef19113029bfabfa3979ec4daf5d79f2dc4fad
           0411c50e934731b919e9c05a5f0d400160578f30160f1f3ba450f07949e5514358e9e4bf624741cadbd22ea6428a100f66b34603cb116cd30afef4615d9969d3b
           d
           040c800e273e63d9e68942716d9e7a42af7c410b7d2e5ab55616940e55ccec4067dd317e8cc04bc6c525a69851b43d59e27195a2a5247589fb25532fd4b0a5
           4989
           OP_3
           OP_CHECKMULTISIG
Sigscript  OP_0
           3044022078820ecf57e24ab54a58c52e2042ef622d1010e7d0e831b5de2787c764029da402202e32d0b8c9b8cc759e129b6fc00af7b999b7b616429b07bb32
           a0b6df8d9410c801
           30440220308a37449b5575051cd62ad1b2bdd8739fa2dfc00dd66ca13e9a238d2f7ccb0302203ea839eab66e8b3726f74fa6c15800ffda5bd31102b6aac88af5
           31bf9d43340d01
Witness
```

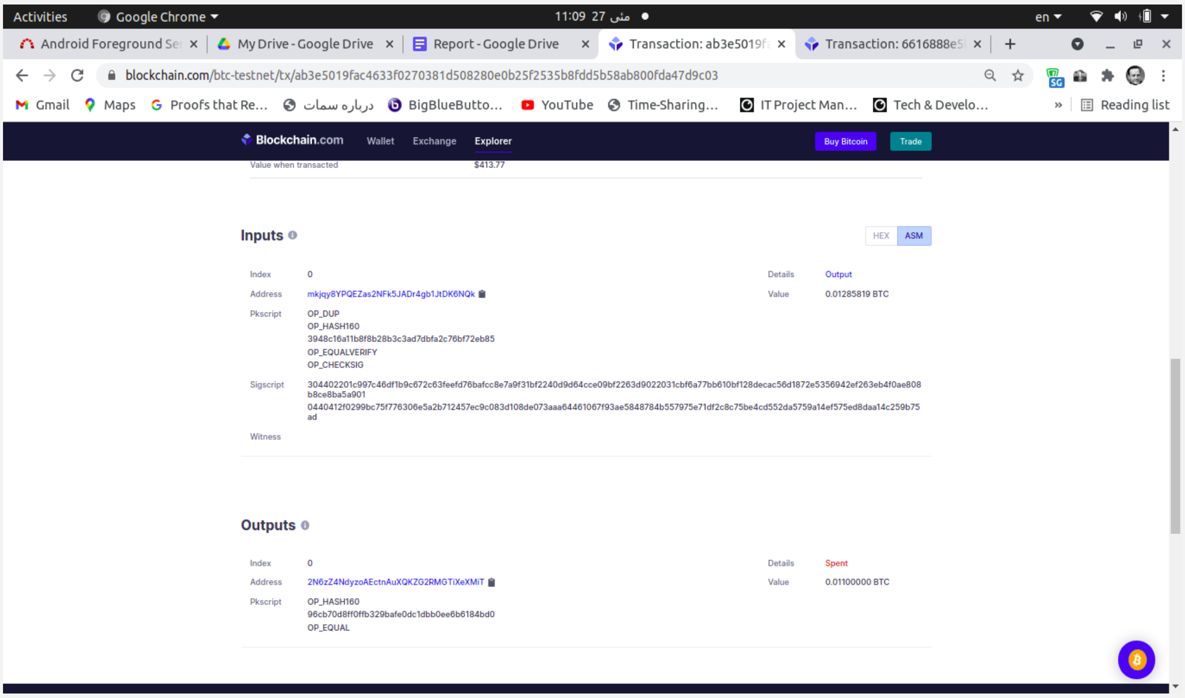
Outputs

```
Index      0                                                   Details   Unspent
Address    mxCCif7LNNAd3veVkV9WmR2sbwkMngpMiA                  Value     0.00200000 BTC
Pkscript   OP_DUP
           OP_HASH160
           b6ee4698d69edafbf248704c613839025f96854c
           OP_EQUALVERIFY
           OP_CHECKSIG
```

Part2-Question3)

1. My Address: mkjqy8YPQEZas2NFk5JADr4gb1JtDK6NQk
2. My Private Key(wif): 93QEpDA2c9i3Zkk1q3cuAxTvsH1kbzijY63ky5VWGJtrkaXerMS
3. P2SH Address: 2N6zZ4NdyzoAEctnAuXQKZG2RMGTiXeXMiT
4. Hash Transaction:
   ab3e5019fac4633f0270381d508280e0b25f2535b8fdd5b58ab800fda47d9c03
5. Hash Spending Transaction:
   6616888e5b966cd38a3dd9ea28617d6a50ae1c6b975539a0a685e629a397e0c4

Our P2SH Transaction:



Value when transacted $413.77

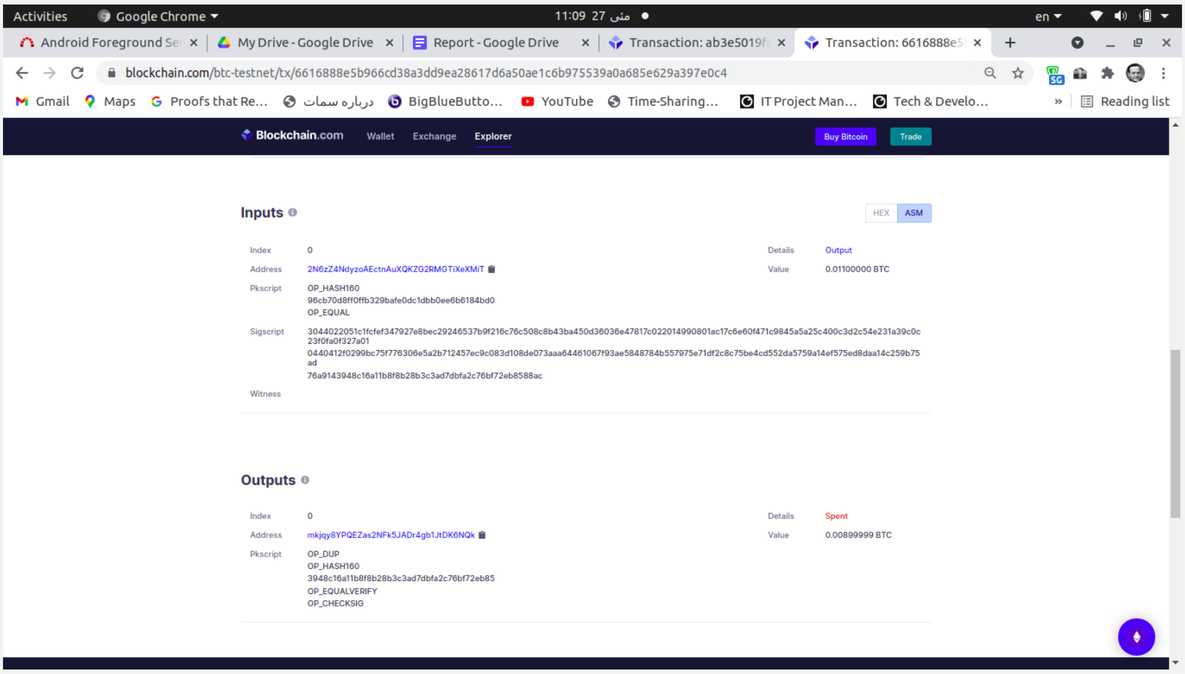
Inputs

Index 0
Details Output
Address mkjqy8YPQEZas2NFk5JADr4gb1JtDK6NQk
Value 0.01285819 BTC
Pkscript
OP_DUP
OP_HASH160
3948c16a11b8f8b28b3c3ad7dbfa2c76bf72eb85
OP_EQUALVERIFY
OP_CHECKSIG
Sigscript
304402201c997c46df1b9c672c63feefd76bafcc8e7a9f31bf2240d9d64cce09bf2263d9022031cbf6a77bb610bf128decac56d1872e5356942ef263eb4f0ae808b8ce8ba5a901
0440412f0299bc75f776306e5a2b712457ec9c083d108de073aaa64461067f93ae5848784b557975e71df2c8c75be4cd552da5759a14ef575ed8daa14c259b75ad
Witness

Outputs

Index 0
Details Spent
Address 2N6zZ4NdyzoAEctnAuXQKZG2RMGTiXeXMiT
Value 0.01100000 BTC
Pkscript
OP_HASH160
96cb70d8ff0ffb329bafe0dc1dbb0ee6b6184bd0
OP_EQUAL

Our P2PKH Spending Transaction:



Inputs

Index 0
Details Output
Address 2N6zZ4NdyzoAEctnAuXQKZG2RMGTiXeXMiT
Value 0.01100000 BTC
Pkscript
OP_HASH160
96cb70d8ff0ffb329bafe0dc1dbb0ee6b6184bd0
OP_EQUAL
Sigscript
3044022051c1fcfef347927e8bec29246537b9f216c76c508c8b43ba450d36036e47817c022014990801ac17c6e60f471c9845a5a25c400c3d2c54e231a39c0c23f0fa0f327a01
0440412f0299bc75f776306e5a2b712457ec9c083d108de073aaa64461067f93ae5848784b557975e71df2c8c75be4cd552da5759a14ef575ed8daa14c259b75ad
76a9143948c16a11b8f8b28b3c3ad7dbfa2c76bf72eb8588ac
Witness

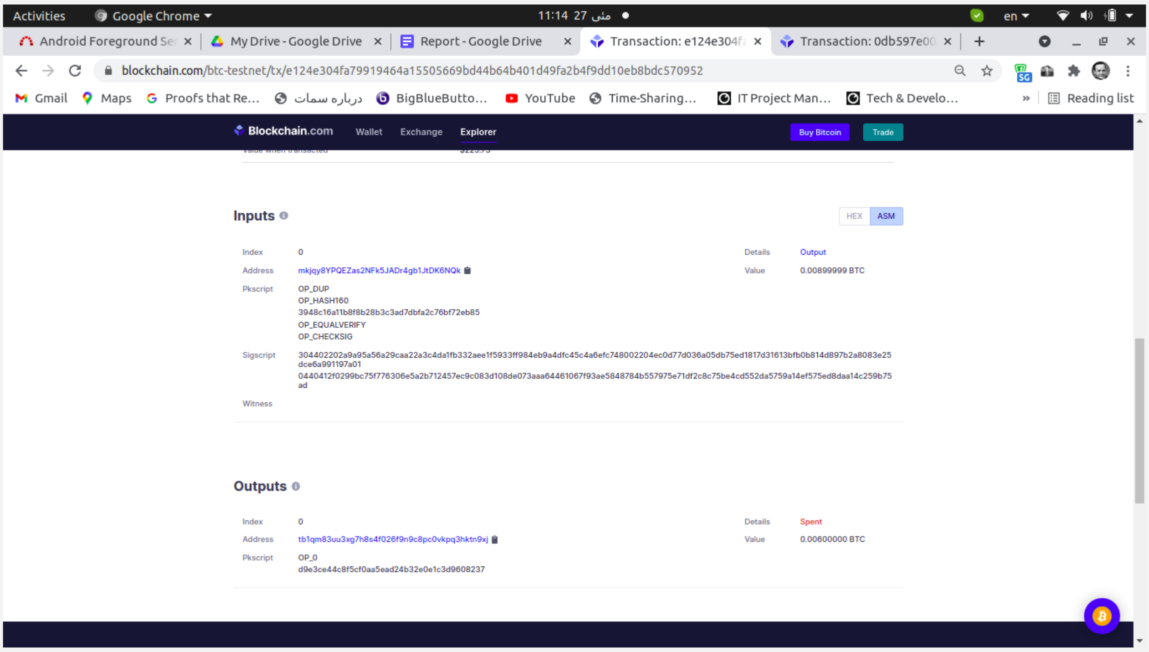
Outputs

Index 0
Details Spent
Address mkjqy8YPQEZas2NFk5JADr4gb1JtDK6NQk
Value 0.00899999 BTC
Pkscript
OP_DUP
OP_HASH160
3948c16a11b8f8b28b3c3ad7dbfa2c76bf72eb85
OP_EQUALVERIFY
OP_CHECKSIG

Part2-Question4)

6. My Address: mkjqy8YPQEZas2NFk5JADr4gb1JtDK6NQk
7. My Private Key(wif): 93QEpDA2c9i3Zkk1q3cuAxTvsH1kbzijY63ky5VWGJtrkaXerMS
8. Segwit Address: tb1qm83uu3xg7h8s4f026f9n9c8pc0vkpq3hktn9xj
9. Segwit Private Key(wif): cSWzxfnTLKAPs5rnVVzTS7fCe68c3kjASg3Ab3T37hf9qbhnY2jx
10. Hash Transaction:
    e124e304fa79919464a15505669bd44b64b401d49fa2b4f9dd10eb8bdc570952
11. Hash Spending Transaction:
    0db597e00a0954cf7e64637dabe723bd1e81b7d936efd863ebdf4012672b88f1

Our P2PWKH Transaction:



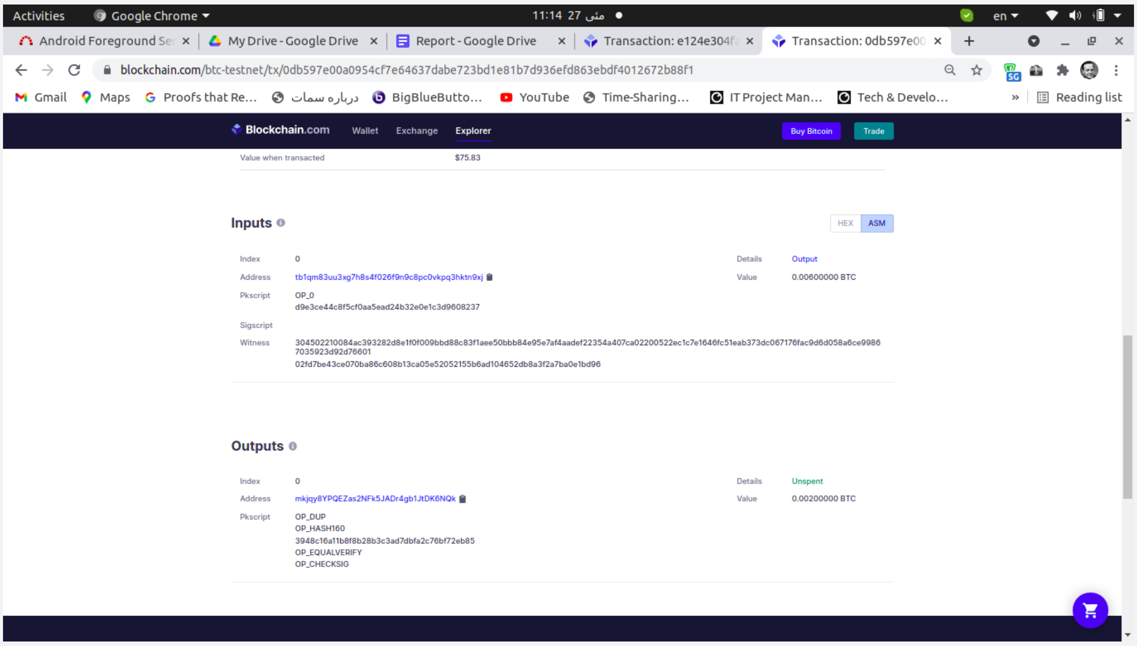
Inputs

Index 0
Details Output
Address mkjqy8YPQEZas2NFk5JADr4gb1JtDK6NQk
Value 0.00899999 BTC
Pkscript
OP_DUP
OP_HASH160
3948c16a11b8f8b28b3c3ad7dbfa2c76bf72eb85
OP_EQUALVERIFY
OP_CHECKSIG
Sigscript
304402202a9a95a56a29caa22a3c4da1fb332aee1f5933ff984eb9a4dfc45c4a6efc748002204ec0d77d036a05db75ed1817d31613bfb0b814d897b2a8083e25dce6a991197a01
0440412f0299bc75f776306e5a2b712457ec9c083d108de073aaa64461067f93ae5848784b557975e71df2c8c75be4cd552da5759a14ef575ed8daa14c259b75ad
Witness

Outputs

Index 0
Details Spent
Address tb1qm83uu3xg7h8s4f026f9n9c8pc0vkpq3hktn9xj
Value 0.00600000 BTC
Pkscript
OP_0
d9e3ce44c8f5cf0aa5ead24b32e0e1c3d9608237

Our P2PKH Spending Transaction:



Value when transacted $75.83

Inputs

Index 0
Details Output
Address tb1qm83uu3xg7h8s4f026f9n9c8pc0vkpq3hktn9xj
Value 0.00600000 BTC
Pkscript
OP_0
d9e3ce44c8f5cf0aa5ead24b32e0e1c3d9608237
Sigscript
Witness
3045022100084ac393282d8e1f0f009bbd88c83f1aee50bbb84e95e7af4aadef22354a407ca02200522ec1c7e1646fc51eab373dc067176fac9d6d058a6ce99867035923d92d76601
02fd7be43ce070ba86c608b13ca05e52052155b6ad104652db8a3f2a7ba0e1bd96

Outputs

Index 0
Details Unspent
Address mkjqy8YPQEZas2NFk5JADr4gb1JtDK6NQk
Value 0.00200000 BTC
Pkscript
OP_DUP
OP_HASH160
3948c16a11b8f8b28b3c3ad7dbfa2c76bf72eb85
OP_EQUALVERIFY
OP_CHECKSIG

Part3)Mining:

Step1: First we get block n height and it’s hash from the input

My_block_height: 7493

My_block_hash: `000000000e07b8b1072caa57878b8943dc27fa398cbb57e7d45f4084d4773ca1`

Step2: Then we need to make the Coinbase transaction with this information:

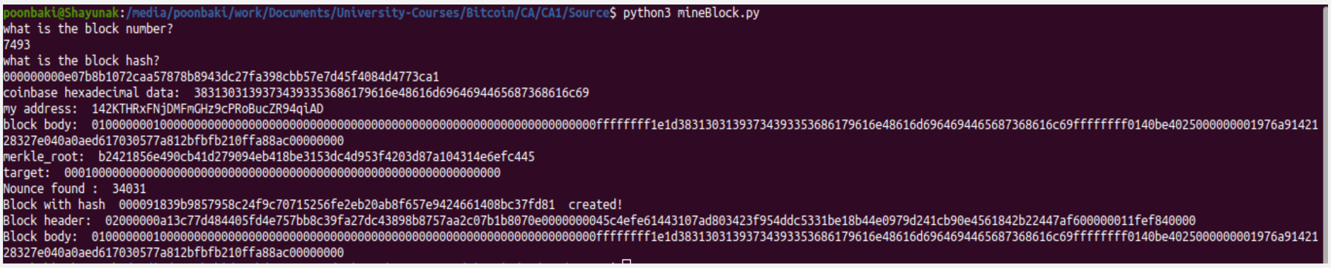
1. Txid_to_spend: 0000000000000000000000000000000000000000000000000000000000000000
2. Txid_to_spend_index: 0xFFFFFFFF
3. scriptSig_input: 810197493ShayanHamidiDehshali (to hex string)
4. Output Script: A P2PKH output script to our address sending 6.25 BTC

Step3: Now we should calculate merkle root.In order to do that,we need to use .serialize() function to get stream format because merkle root equals to the coinbase when we have one transaction.

Step4: In order to mine we need to calculate the target.The target is calculated nBits that need to be set according to the number of zeros as difficulty.For four zeros we use “0x1f010000” as bits.

Step5: Then we need to build the block header partially,because most of the header remains intact except nounce.so we make it partially and in mining process we attach nounce to the header and hash it.

Step6: Now we start mining.From nounce 0 to Max,which is a 4 byte integer,we attach the nounce to the partial_header, calculate sha256 twice on the header and see if it is less than the target.If yes,we have successfully mined a block.



```
poonbaki@Shayunak:/media/poonbaki/work/Documents/University-Courses/Bitcoin/CA/CA1/Source$ python3 mineBlock.py
what is the block number?
7493
what is the block hash?
000000000e07b8b1072caa57878b8943dc27fa398cbb57e7d45f4084d4773ca1
coinbase hexadecimal data:  383130313937343933536861796616e48616d6964694465687368616c69
my address:  142KTHRxFNjDMFmGHz9cPRoBucZR94qiAD
block body:  01000000010000000000000000000000000000000000000000000000000000000000000000ffffffff1e1d3831303139373439333536861796616e48616d6964694465687368616c69ffffffff0140be4025000000001976a91421
28327e040a0aed617030577a812bfbfb210ffa88ac00000000
merkle_root:  b2421856e490cb41d279094eb418be3153dc4d953f4203d87a104314e6efc445
target:  0001000000000000000000000000000000000000000000000000000000000000
Nounce found :  34031
Block with hash  000091839b9857958c24f9c70715256fe2eb20ab8f657e9424661408bc37fd81  created!
Block header:  02000000a13c77d484405fd4e757bb8c39fa27dc43898b8757aa2c07b1b8070e0000000045c4efe61443107ad803423f954ddc5331be18b44e0979d241cb90e4561842b22447af600000011fef840000
Block body:  01000000010000000000000000000000000000000000000000000000000000000000000000ffffffff1e1d3831303139373439333536861796616e48616d6964694465687368616c69ffffffff0140be4025000000001976a91421
28327e040a0aed617030577a812bfbfb210ffa88ac00000000
```