Bitcoin Scripting Assignment Report

CS 216: Introduction to Blockchain - Assignment 3

Team : wasd

Submitted by:

- Rohan Dhiman (230001069)
- Mani Kaustubh Mathur (230001050)
- Siddharth Singh (230002068)

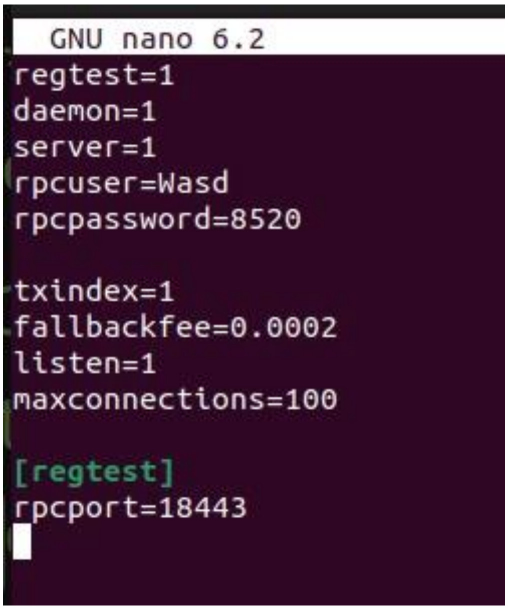
1. Introduction

This report presents our implementation and analysis of Bitcoin transactions using both Legacy (P2PKH) and SegWit (P2SH-P2WPKH) address formats. We developed Python scripts to interact with bitcoind in regtest mode, create and broadcast transactions, and analyze the resulting scripts.

2. Environment Setup

We configured Bitcoin Core to run in regtest mode with the following settings in bitcoin.conf:

```
regtest=1
server=1
rpcuser=Wasd
rpcpassword=8520
paytxfee=0.0001
fallbackfee=0.0002
mintxfee=0.00001
txconfirmtarget=1
```



```
  GNU nano 6.2
regtest=1
daemon=1
server=1
rpcuser=Wasd
rpcpassword=8520

txindex=1
fallbackfee=0.0002
listen=1
maxconnections=100

[regtest]
rpcport=18443
```

For our implementation, we used Python with the python-bitcoinrpc and simplejson libraries to interact with the Bitcoin daemon.

3. Legacy Address Transactions (P2PKH)

3.1 Workflow

1. **Address Generation**: We generated three legacy addresses (A, B, and C) using the Bitcoin Core wallet.

```
"address_a": "mo3Gb91CZh3MtPGdzJbBw8cFNZW4xN8ihT",
"address_b": "mfnzo7byi9R76pf4Ct1eUH5cgf9QSA6qnv",
"address_c": "mgrxiR3r336phqmN2EGuTtMCF25PJsBK4u",
```

2. **Funding Address A**: We funded address A using the sendtoaddress command.

```
    print("Funding Address A")
     txid_funding = rpc.sendtoaddress(address_a, 1.0)
     print(f"Funding transaction ID: {txid_funding}")
```

3. **Transaction from A to B**: We created a raw transaction sending coins from A to B, signed it, and broadcast it to the network.

```
{
        "address_a": "mo3Gb91CZh3MtPGdzJbBw8cFNZW4xN8ihT",
        "address_b": "mfnzo7byi9R76pf4Ct1eUH5cgf9QSA6qnv",
        "address_c": "mgrxiR3r336phqmN2EGuTtMCF25PJsBK4u",
        "tx_a_to_b":
"07b3c2c3e791e11c3faffb0333e207bb016633cf4f727621e56874d1e0f48c9f"
    }
```

4. **Transaction from B to C**: We used the UTXO from the previous transaction to create a new transaction from B to C.

```
{
        "address_a": "mo3Gb91CZh3MtPGdzJbBw8cFNZW4xN8ihT",
        "address_b": "mfnzo7byi9R76pf4Ct1eUH5cgf9QSA6qnv",
        "address_c": "mgrxiR3r336phqmN2EGuTtMCF25PJsBK4u",
        "tx_a_to_b":
"07b3c2c3e791e11c3faffb0333e207bb016633cf4f727621e56874d1e0f48c9f",
        "tx_b_to_c":
"bae2c3576128e35c649ba30538b9e24aecf300aad7063a0e230a344fd35ffa23",
        "scriptSig": {
            "asm":
"3044022073fdb36a203bc0eb4ffa8d2545f26cb4aeec78ff31ae92d79a937073793f1bfb02205
d4441054c0f984cf795deac8e9034e68b20cc323cd3332d45f00666811f8315[ALL]
02a6b47f2ea4d66df2b14b9878c53fe58fec9724500f74390ec45b43994c374bfb",
            "hex":
"473044022073fdb36a203bc0eb4ffa8d2545f26cb4aeec78ff31ae92d79a937073793f1bfb022
05d4441054c0f984cf795deac8e9034e68b20cc323cd3332d45f00666811f8315012102a6b47f2
ea4d66df2b14b9878c53fe58fec9724500f74390ec45b43994c374bfb"
        },
        "previousScriptPubKey": {
            "asm": "OP_DUP OP_HASH160 0308be3f7ded2074b14c477fa18ec0ecfe3e3dfc
OP_EQUALVERIFY OP_CHECKSIG",
            "desc": "addr(mfnzo7byi9R76pf4Ct1eUH5cgf9QSA6qnv)#5d7z884z",
            "hex": "76a9140308be3f7ded2074b14c477fa18ec0ecfe3e3dfc88ac",
            "address": "mfnzo7byi9R76pf4Ct1eUH5cgf9QSA6qnv",
            "type": "pubkeyhash"
        }
    }
```

3.2 Script Analysis

Transaction from A to B

The locking script (ScriptPubKey) for address B follows the P2PKH format:

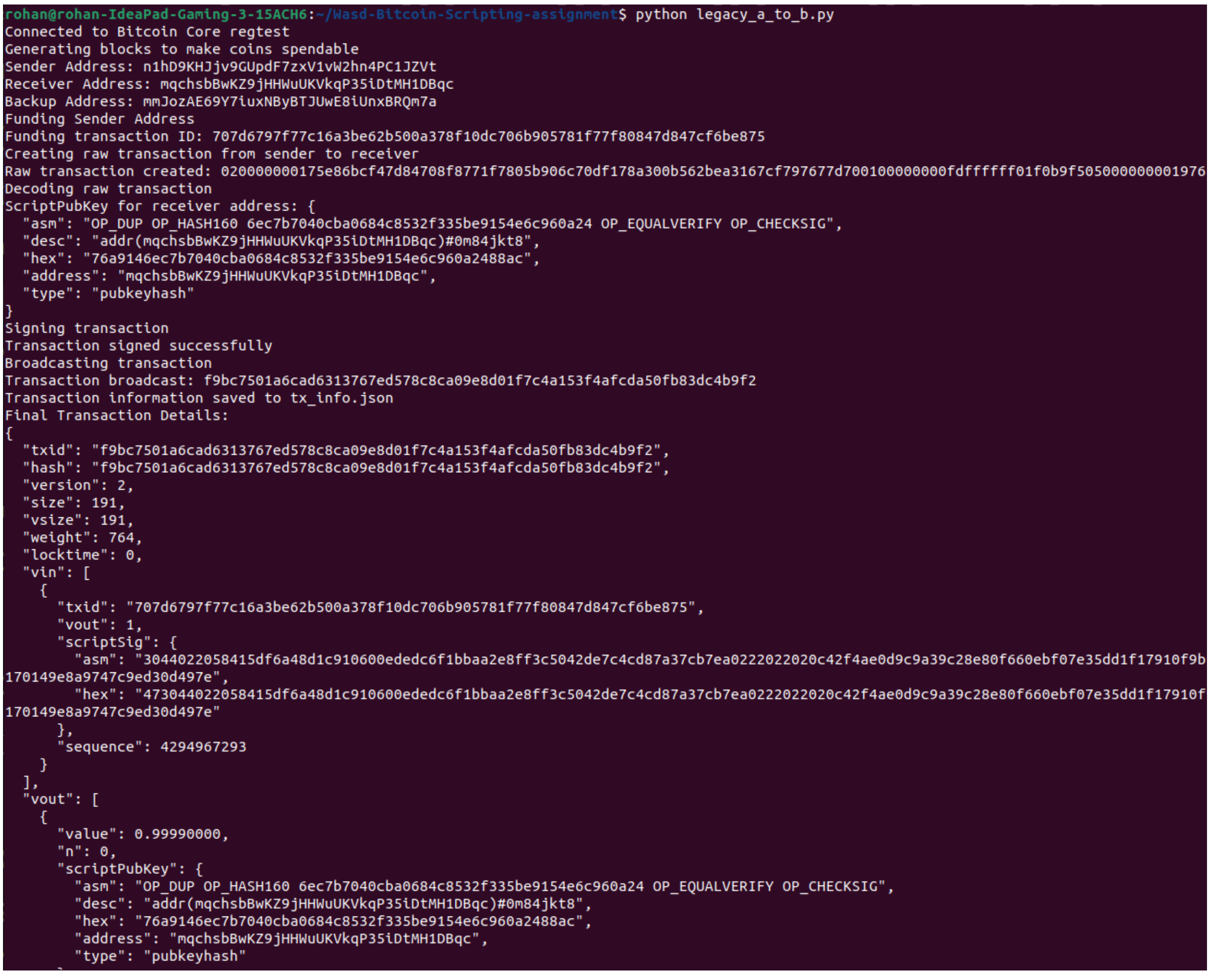
text

```
OP_DUP OP_HASH160 <PubKeyHash of B> OP_EQUALVERIFY OP_CHECKSIG
```

This script locks the funds such that only the owner of the private key corresponding to address B can spend them.

```
"tx_a_to_b": {
            "size": 191,
            "vsize": 191,
            "weight": 764,
            "scriptPubKey": "OP_DUP OP_HASH160
00dd19fff02ba87f0568da1b282a93b1c2d598dc OP_EQUALVERIFY OP_CHECKSIG"
        }
```

```
{
        "address_a": "mo3Gb91CZh3MtPGdzJbBw8cFNZW4xN8ihT",
        "address_b": "mfnzo7byi9R76pf4Ct1eUH5cgf9QSA6qnv",
        "address_c": "mgrxiR3r336phqmN2EGuTtMCF25PJsBK4u",
        "tx_a_to_b":
"07b3c2c3e791e11c3faffb0333e207bb016633cf4f727621e56874d1e0f48c9f"
    }
```



```
rohan@rohan-IdeaPad-Gaming-3-15ACH6:~/Wasd-Bitcoin-Scripting-assignment$ python legacy_a_to_b.py
Connected to Bitcoin Core regtest
Generating blocks to make coins spendable
Sender Address: n1hD9KHJjv9GUpdF7zxV1vW2hn4PC1JZVt
Receiver Address: mqchsbBwKZ9jHHWuUKVkqP35iDtMH1DBqc
Backup Address: mmJozAE69Y7iuxNByBTJUwE8iUnxBRQm7a
Funding Sender Address
Funding transaction ID: 707d6797f77c16a3be62b500a378f10dc706b905781f77f80847d847cf6be875
Creating raw transaction from sender to receiver
Raw transaction created: 020000000175e86bcf47d84708f8771f7805b906c70df178a300b562bea3167cf797677d700100000000fdffffff01f0b9f505000000001976
Decoding raw transaction
ScriptPubKey for receiver address: {
  "asm": "OP_DUP OP_HASH160 6ec7b7040cba0684c8532f335be9154e6c960a24 OP_EQUALVERIFY OP_CHECKSIG",
  "desc": "addr(mqchsbBwKZ9jHHWuUKVkqP35iDtMH1DBqc)#0m84jkt8",
  "hex": "76a9146ec7b7040cba0684c8532f335be9154e6c960a2488ac",
  "address": "mqchsbBwKZ9jHHWuUKVkqP35iDtMH1DBqc",
  "type": "pubkeyhash"
}
Signing transaction
Transaction signed successfully
Broadcasting transaction
Transaction broadcast: f9bc7501a6cad6313767ed578c8ca09e8d01f7c4a153f4afcda50fb83dc4b9f2
Transaction information saved to tx_info.json
Final Transaction Details:
{
  "txid": "f9bc7501a6cad6313767ed578c8ca09e8d01f7c4a153f4afcda50fb83dc4b9f2",
  "hash": "f9bc7501a6cad6313767ed578c8ca09e8d01f7c4a153f4afcda50fb83dc4b9f2",
  "version": 2,
  "size": 191,
  "vsize": 191,
  "weight": 764,
  "locktime": 0,
  "vin": [
    {
      "txid": "707d6797f77c16a3be62b500a378f10dc706b905781f77f80847d847cf6be875",
      "vout": 1,
      "scriptSig": {
        "asm": "3044022058415df6a48d1c910600ededc6f1bbaa2e8ff3c5042de7c4cd87a37cb7ea0222022020c42f4ae0d9c9a39c28e80f660ebf07e35dd1f17910f9b
170149e8a9747c9ed30d497e",
        "hex": "473044022058415df6a48d1c910600ededc6f1bbaa2e8ff3c5042de7c4cd87a37cb7ea0222022020c42f4ae0d9c9a39c28e80f660ebf07e35dd1f17910f
170149e8a9747c9ed30d497e"
      },
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 0.99990000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 6ec7b7040cba0684c8532f335be9154e6c960a24 OP_EQUALVERIFY OP_CHECKSIG",
        "desc": "addr(mqchsbBwKZ9jHHWuUKVkqP35iDtMH1DBqc)#0m84jkt8",
        "hex": "76a9146ec7b7040cba0684c8532f335be9154e6c960a2488ac",
        "address": "mqchsbBwKZ9jHHWuUKVkqP35iDtMH1DBqc",
        "type": "pubkeyhash"
```

Transaction from B to C

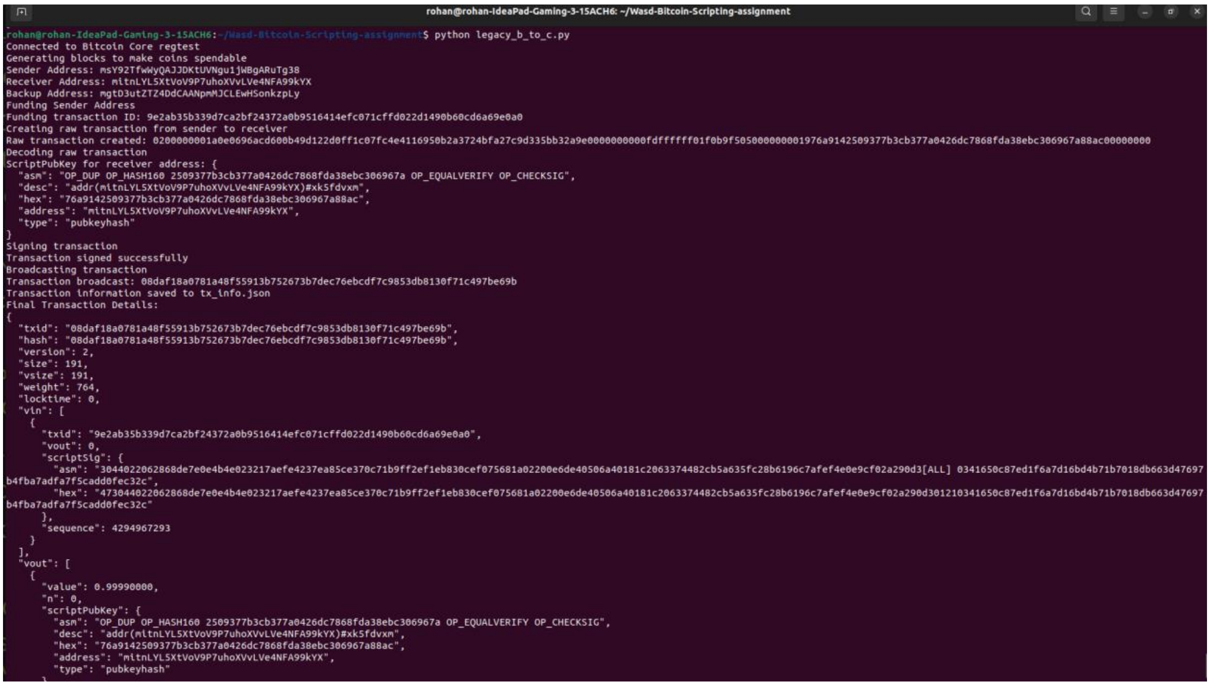
The unlocking script (ScriptSig) for spending from address B contains:

text

```
<Signature> <Public Key of B>
```

When executed with the locking script, this proves ownership of the private key corresponding to address B.

```
"tx_b_to_c": {
            "size": 191,
            "vsize": 191,
            "weight": 764,
            "scriptSig":
"3044022016fd32832079dc113843014b53f3439300eabff1836346e11d30b911da90ec1d02203
851e58d65bff9c29860f051bacb17eff6cf73a22b406566d5e2e8f096a32a7f[ALL]
02cae87b2b5a19279fee686c92490e919662dfc152faabf3049403b18a1ab35133"
        }
```


rohan@rohan-IdeaPad-Gaming-3-15ACH6: ~/Wasd-Bitcoin-Scripting-assignment

```
rohan@rohan-IdeaPad-Gaming-3-15ACH6:~/Wasd-Bitcoin-Scripting-assignment$ python legacy_b_to_c.py
Connected to Bitcoin Core regtest
Generating blocks to make coins spendable
Sender Address: msY92TfwWyQAJJDKtUVNgu1jWBgARuTg38
Receiver Address: mitnLYL5XtVoV9P7uhoXVvLVe4NFA99kYX
Backup Address: mgtD3utZTZ4DdCAANpmMJCLEwHSonkzpLy
Funding Sender Address
Funding transaction ID: 9e2ab35b339d7ca2bf24372a0b9516414efc071cffd022d1490b60cd6a69e0a0
Creating raw transaction from sender to receiver
Raw transaction created: 0200000001a0e0696acd600b49d122d0ff1c07fc4e4116950b2a3724bfa27c9d335bb32a9e0000000000fdffffff01f0b9f505000000001976a9142509377b3cb377a0426dc7868fda38ebc306967a88ac00000000
Decoding raw transaction
ScriptPubKey for receiver address: {
  "asm": "OP_DUP OP_HASH160 2509377b3cb377a0426dc7868fda38ebc306967a OP_EQUALVERIFY OP_CHECKSIG",
  "desc": "addr(mitnLYL5XtVoV9P7uhoXVvLVe4NFA99kYX)#xk5fdvxm",
  "hex": "76a9142509377b3cb377a0426dc7868fda38ebc306967a88ac",
  "address": "mitnLYL5XtVoV9P7uhoXVvLVe4NFA99kYX",
  "type": "pubkeyhash"
}
Signing transaction
Transaction signed successfully
Broadcasting transaction
Transaction broadcast: 08daf18a0781a48f55913b752673b7dec76ebcdf7c9853db8130f71c497be69b
Transaction information saved to tx_info.json
Final Transaction Details:
{
  "txid": "08daf18a0781a48f55913b752673b7dec76ebcdf7c9853db8130f71c497be69b",
  "hash": "08daf18a0781a48f55913b752673b7dec76ebcdf7c9853db8130f71c497be69b",
  "version": 2,
  "size": 191,
  "vsize": 191,
  "weight": 764,
  "locktime": 0,
  "vin": [
    {
      "txid": "9e2ab35b339d7ca2bf24372a0b9516414efc071cffd022d1490b60cd6a69e0a0",
      "vout": 0,
      "scriptSig": {
        "asm": "3044022062868de7e0e4b4e023217aefe4237ea85ce370c71b9ff2ef1eb830cef075681a02200e6de40506a40181c2063374482cb5a635fc28b6196c7afef4e0e9cf02a290d3[ALL] 0341650c87ed1f6a7d16bd4b71b7018db663d47697
b4fba7adfa7f5cadd0fec32c",
        "hex": "473044022062868de7e0e4b4e023217aefe4237ea85ce370c71b9ff2ef1eb830cef075681a02200e6de40506a40181c2063374482cb5a635fc28b6196c7afef4e0e9cf02a290d301210341650c87ed1f6a7d16bd4b71b7018db663d47697
b4fba7adfa7f5cadd0fec32c"
      },
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 0.99990000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 2509377b3cb377a0426dc7868fda38ebc306967a OP_EQUALVERIFY OP_CHECKSIG",
        "desc": "addr(mitnLYL5XtVoV9P7uhoXVvLVe4NFA99kYX)#xk5fdvxm",
        "hex": "76a9142509377b3cb377a0426dc7868fda38ebc306967a88ac",
        "address": "mitnLYL5XtVoV9P7uhoXVvLVe4NFA99kYX",
        "type": "pubkeyhash"
```

3.3 Script Validation

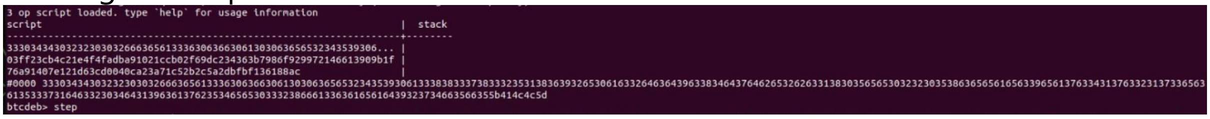
The validation process works as follows:

1. The unlocking script provides the signature and public key
2. The locking script verifies that:
    - The hash of the public key matches the expected hash
    - The signature is valid for the transaction and public key

```
{
        "address_a": "mo3Gb91CZh3MtPGdzJbBw8cFNZW4xN8ihT",
        "address_b": "mfnzo7byi9R76pf4Ct1eUH5cgf9QSA6qnv",
        "address_c": "mgrxiR3r336phqmN2EGuTtMCF25PJsBK4u",
        "tx_a_to_b":
"07b3c2c3e791e11c3faffb0333e207bb016633cf4f727621e56874d1e0f48c9f",
        "tx_b_to_c":
"bae2c3576128e35c649ba30538b9e24aecf300aad7063a0e230a344fd35ffa23",
        "scriptSig": {
            "asm":
"3044022073fdb36a203bc0eb4ffa8d2545f26cb4aeec78ff31ae92d79a937073793f1bfb02205
d4441054c0f984cf795deac8e9034e68b20cc323cd3332d45f00666811f8315[ALL]
02a6b47f2ea4d66df2b14b9878c53fe58fec9724500f74390ec45b43994c374bfb",
            "hex":
"473044022073fdb36a203bc0eb4ffa8d2545f26cb4aeec78ff31ae92d79a937073793f1bfb022
05d4441054c0f984cf795deac8e9034e68b20cc323cd3332d45f00666811f8315012102a6b47f2
ea4d66df2b14b9878c53fe58fec9724500f74390ec45b43994c374bfb"
        },
        "previousScriptPubKey": {
            "asm": "OP_DUP OP_HASH160 0308be3f7ded2074b14c477fa18ec0ecfe3e3dfc
OP_EQUALVERIFY OP_CHECKSIG",
            "desc": "addr(mfnzo7byi9R76pf4Ct1eUH5cgf9QSA6qnv)#5d7z884z",
            "hex": "76a9140308be3f7ded2074b14c477fa18ec0ecfe3e3dfc88ac",
            "address": "mfnzo7byi9R76pf4Ct1eUH5cgf9QSA6qnv",
            "type": "pubkeyhash"
        }
    }
```

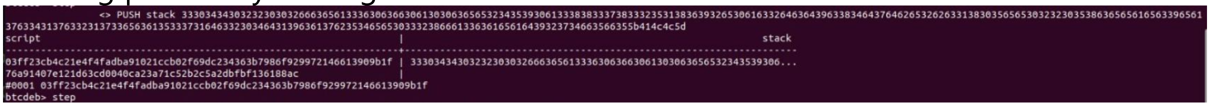
- **Validation of tx a to b**

1. Loading the script:



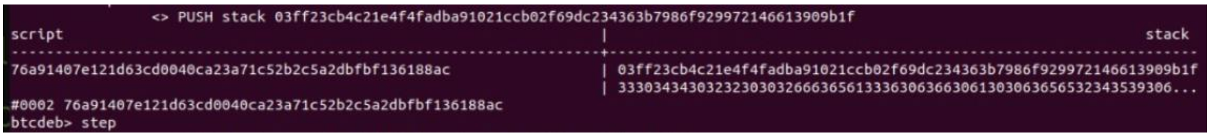
```
3 op script loaded. type `help` for usage information
script                                                            |  stack
------------------------------------------------------------------+--------
3330343430323230303266636561333630636630613030636565323435393306... |
03ff23cb4c21e4f4fadba91021ccb02f69dc234363b7986f929972146613909b1f |
76a91407e121d63cd0040ca23a71c52b2c5a2dbfbf136188ac                 |
#0000 3330343430323230303266636561333630636630613030636565323435393061333838333738333235313836393265306163326463643963383464376462653262633138303565653032323035386365656165633965613763343137633231373365 63
61353337316463323034643139636137623534656530333238666133636165616439323734663566355b414c4c5d
btcdeb> step
```

2. Pushing public key and signature:



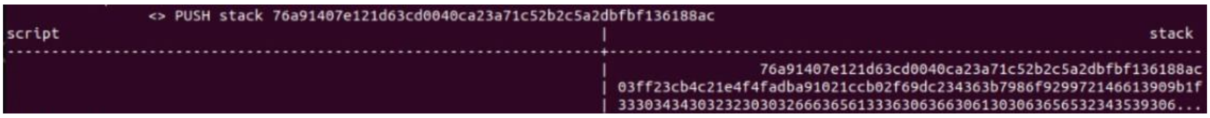
```
                <> PUSH stack 33303434303232303032666365613336306366306130306365653234353930613338383337383332353138363932653061633264636439633834643764626532626331383035656530323230353863656561656339656 1
37633431376332313733656361353337316463323034643139636137623534656530333238666133636165616439323734663566355b414c4c5d
script                                                            |                                                                  stack
------------------------------------------------------------------+------------------------------------------------------------------
03ff23cb4c21e4f4fadba91021ccb02f69dc234363b7986f929972146613909b1f | 3330343430323230303266636561333630636630613030636565323435393306...
76a91407e121d63cd0040ca23a71c52b2c5a2dbfbf136188ac                 |
#0001 03ff23cb4c21e4f4fadba91021ccb02f69dc234363b7986f929972146613909b1f
btcdeb> step
```

3. Duplicating the public key:



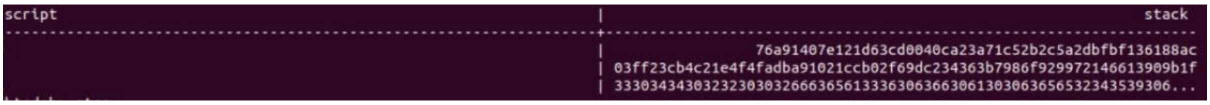
```
                <> PUSH stack 03ff23cb4c21e4f4fadba91021ccb02f69dc234363b7986f929972146613909b1f
script                                                            |                                                                  stack
------------------------------------------------------------------+------------------------------------------------------------------
76a91407e121d63cd0040ca23a71c52b2c5a2dbfbf136188ac                 | 03ff23cb4c21e4f4fadba91021ccb02f69dc234363b7986f929972146613909b1f
                                                                   | 3330343430323230303266636561333630636630613030636565323435393306...
#0002 76a91407e121d63cd0040ca23a71c52b2c5a2dbfbf136188ac
btcdeb> step
```

4. Hashing the public key:

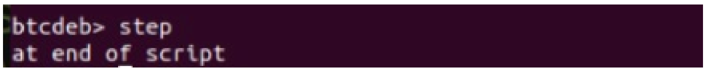


```
                  <> PUSH stack 76a91407e121d63cd0040ca23a71c52b2c5a2dbfbf136188ac
script                                                            |                                                                  stack
------------------------------------------------------------------+-------------------------------------------------------------------
                                                                  |                        76a91407e121d63cd0040ca23a71c52b2c5a2dbfbf136188ac
                                                                  | 03ff23cb4c21e4f4fadba91021ccb02f69dc234363b7986f929972146613909b1f
                                                                  | 333034343032323030326663656133363063663061303063656532343539306...
```

5. Comparing the hash with the stored hashkey:



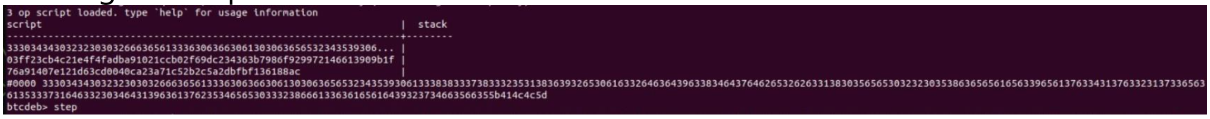
```
script                                                            |                                                                  stack
------------------------------------------------------------------+-------------------------------------------------------------------
                                                                  |                        76a91407e121d63cd0040ca23a71c52b2c5a2dbfbf136188ac
                                                                  | 03ff23cb4c21e4f4fadba91021ccb02f69dc234363b7986f929972146613909b1f
                                                                  | 333034343032323030326663656133363063663061303063656532343539306...
```



```
btcdeb> step
at end of script
```

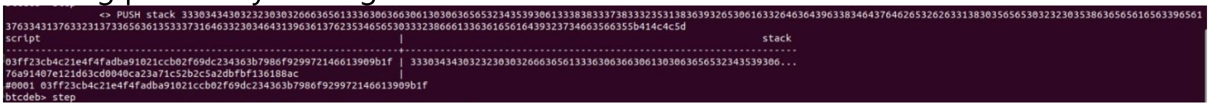
- **Validation of tx b to c**

1. Loading the script:



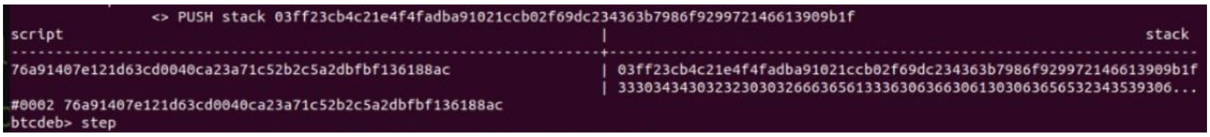
```
3 op script loaded. type `help` for usage information
script                                                            |  stack
------------------------------------------------------------------+--------
333034343032323030326663656133363063663061303063656532343539306... |
03ff23cb4c21e4f4fadba91021ccb02f69dc234363b7986f929972146613909b1f |
76a91407e121d63cd0040ca23a71c52b2c5a2dbfbf136188ac                 |
#0000 33303434303232303032666365613336306366306130306365653234353930613338383337383332353138363932653061633264636439633834643764626532626331383035656530323230353863656561656339656137633431376332313733656563
613533373164633230346431396361376235346565303332386661333636165616439323734663566355b414c4c5d
btcdeb> step
```

2. Pushing public key and signature:



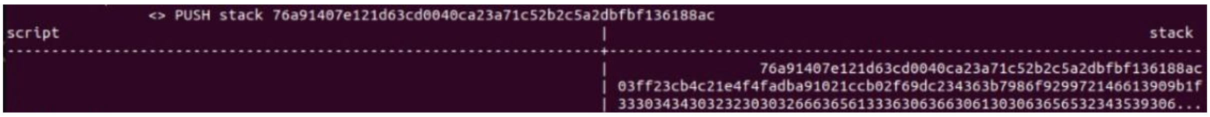
```
                  <> PUSH stack 33303434303232303032666365613336306366306130306365653234353930613338383337383332353138363932653061633264636439633834643764626532626331383035656530323230353863656561656339656561
376334313763323137336563613533373164633230346431396361376235346565303332386661333636165616439323734663566355b414c4c5d
script                                                            |                                                                  stack
------------------------------------------------------------------+-------------------------------------------------------------------
03ff23cb4c21e4f4fadba91021ccb02f69dc234363b7986f929972146613909b1f | 333034343032323030326663656133363063663061303063656532343539306...
76a91407e121d63cd0040ca23a71c52b2c5a2dbfbf136188ac                 |
#0001 03ff23cb4c21e4f4fadba91021ccb02f69dc234363b7986f929972146613909b1f
btcdeb> step
```

3. Duplicating the public key:



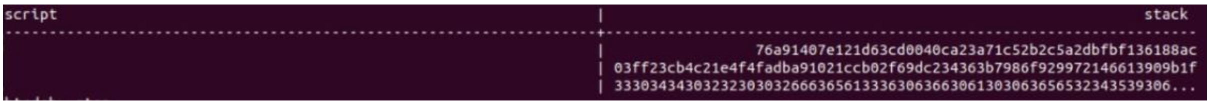
```
                  <> PUSH stack 03ff23cb4c21e4f4fadba91021ccb02f69dc234363b7986f929972146613909b1f
script                                                            |                                                                  stack
------------------------------------------------------------------+-------------------------------------------------------------------
76a91407e121d63cd0040ca23a71c52b2c5a2dbfbf136188ac                 | 03ff23cb4c21e4f4fadba91021ccb02f69dc234363b7986f929972146613909b1f
                                                                  | 333034343032323030326663656133363063663061303063656532343539306...
#0002 76a91407e121d63cd0040ca23a71c52b2c5a2dbfbf136188ac
btcdeb> step
```

4. Hashing the public key:

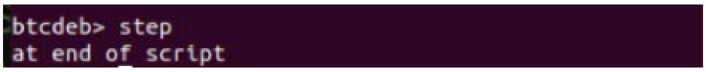


```
                  <> PUSH stack 76a91407e121d63cd0040ca23a71c52b2c5a2dbfbf136188ac
script                                                            |                                                                  stack
------------------------------------------------------------------+-------------------------------------------------------------------
                                                                  |                        76a91407e121d63cd0040ca23a71c52b2c5a2dbfbf136188ac
                                                                  | 03ff23cb4c21e4f4fadba91021ccb02f69dc234363b7986f929972146613909b1f
                                                                  | 333034343032323030326663656133363063663061303063656532343539306...
```

5. Comparing the hash with the stored hashkey:



```
script                                                            |                                                                  stack
------------------------------------------------------------------+-------------------------------------------------------------------
                                                                  |                        76a91407e121d63cd0040ca23a71c52b2c5a2dbfbf136188ac
                                                                  | 03ff23cb4c21e4f4fadba91021ccb02f69dc234363b7986f929972146613909b1f
                                                                  | 333034343032323030326663656133363063663061303063656532343539306...
```



```
btcdeb> step
at end of script
```

4. SegWit Address Transactions (P2SH-P2WPKH)

4.1 Workflow

1. **Address Generation**: We generated three P2SH-SegWit addresses (A', B', and C').
2. **Funding Address A'**: We funded address A' using the sendtoaddress command.
3. **Transaction from A' to B'**: We created a raw transaction sending coins from A' to B', signed it, and broadcast it.
4. **Transaction from B' to C'**: We used the UTXO from the previous transaction to create a new transaction from B' to C'.

```
{
        "address_a": "mo3Gb91CZh3MtPGdzJbBw8cFNZW4xN8ihT",
        "address_b": "mfnzo7byi9R76pf4Ct1eUH5cgf9QSA6qnv",
        "address_c": "mgrxiR3r336phqmN2EGuTtMCF25PJsBK4u",
        "tx_a_to_b":
"07b3c2c3e791e11c3faffb0333e207bb016633cf4f727621e56874d1e0f48c9f",
        "tx_b_to_c":
"bae2c3576128e35c649ba30538b9e24aecf300aad7063a0e230a344fd35ffa23"
    }
```

4.2 Script Analysis

Transaction from A' to B'

The locking script for a P2SH-P2WPKH address B' has the format:

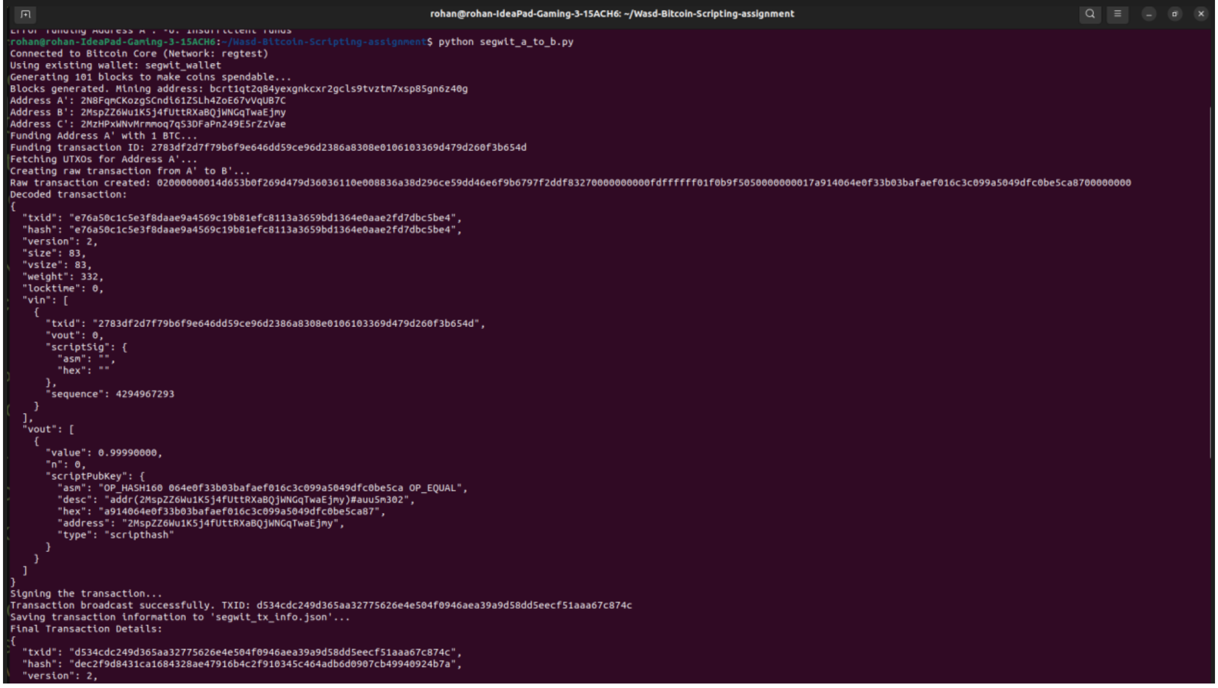
```
OP_HASH160 <Hash of redeemScript> OP_EQUAL
```

Where the redeemScript is:

```
0 <PubKeyHash of B'>

"tx_a_to_b": {
            "size": 215,
            "vsize": 134,
            "weight": 533,
            "scriptPubKey": "OP_HASH160
4f7e3fbf192f9e4838ceb2232f46d13df9694023 OP_EQUAL"
        }
```

```
{
    "address_a_prime": "2N5YVgeVK8JaxDNeEja4vPMSXDDruPaSbe8",
    "address_b_prime": "2MxN4iffihUoJ8WkqgnDCHpdTu6vrGnzeks",
    "address_c_prime": "2N6RSDWaE9FmzrYAn8rA2mzK4PHuAapS3LD",
    "tx_a_to_b":
"15f00e0da6d82c54054ea3939fce946338d03ac306fe87172271759b00871c30"
}
```


rohan@rohan-IdeaPad-Gaming-3-15ACH6: ~/Wasd-Bitcoin-Scripting-assignment

```
Error funding Address A': -6: Insufficient funds
rohan@rohan-IdeaPad-Gaming-3-15ACH6:~/Wasd-Bitcoin-Scripting-assignment$ python segwit_a_to_b.py
Connected to Bitcoin Core (Network: regtest)
Using existing wallet: segwit_wallet
Generating 101 blocks to make coins spendable...
Blocks generated. Mining address: bcrt1qt2q84yexgnkcxr2gcls9tvztm7xsp85gn6z40g
Address A': 2N8FqmCKozgSCndi61ZSLh4ZoE67vVqUB7C
Address B': 2MspZZ6Wu1K5j4fUttRXaBQjWNGqTwaEjmy
Address C': 2MzHPxWNvMrmmoq7qS3DFaPn249E5rZzVae
Funding Address A' with 1 BTC...
Funding transaction ID: 2783df2d7f79b6f9e646dd59ce96d2386a8308e0106103369d479d260f3b654d
Fetching UTXOs for Address A'...
Creating raw transaction from A' to B'...
Raw transaction created: 02000000014d653b0f269d479d36036110e008836a38d296ce59dd46e6f9b6797f2ddf83270000000000fdffffff01f0b9f5050000000017a914064e0f33b03bafaef016c3c099a5049dfc0be5ca8700000000
Decoded transaction:
{
  "txid": "e76a50c1c5e3f8daae9a4569c19b81efc8113a3659bd1364e0aae2fd7dbc5be4",
  "hash": "e76a50c1c5e3f8daae9a4569c19b81efc8113a3659bd1364e0aae2fd7dbc5be4",
  "version": 2,
  "size": 83,
  "vsize": 83,
  "weight": 332,
  "locktime": 0,
  "vin": [
    {
      "txid": "2783df2d7f79b6f9e646dd59ce96d2386a8308e0106103369d479d260f3b654d",
      "vout": 0,
      "scriptSig": {
        "asm": "",
        "hex": ""
      },
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 0.99990000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_HASH160 064e0f33b03bafaef016c3c099a5049dfc0be5ca OP_EQUAL",
        "desc": "addr(2MspZZ6Wu1K5j4fUttRXaBQjWNGqTwaEjmy)#auu5m302",
        "hex": "a914064e0f33b03bafaef016c3c099a5049dfc0be5ca87",
        "address": "2MspZZ6Wu1K5j4fUttRXaBQjWNGqTwaEjmy",
        "type": "scripthash"
      }
    }
  ]
}
Signing the transaction...
Transaction broadcast successfully. TXID: d534cdc249d365aa32775626e4e504f0946aea39a9d58dd5eecf51aaa67c874c
Saving transaction information to 'segwit_tx_info.json'...
Final Transaction Details:
{
  "txid": "d534cdc249d365aa32775626e4e504f0946aea39a9d58dd5eecf51aaa67c874c",
  "hash": "dec2f9d8431ca1684328ae47916b4c2f910345c464adb6d0907cb49940924b7a",
  "version": 2,
```

Transaction from B' to C'

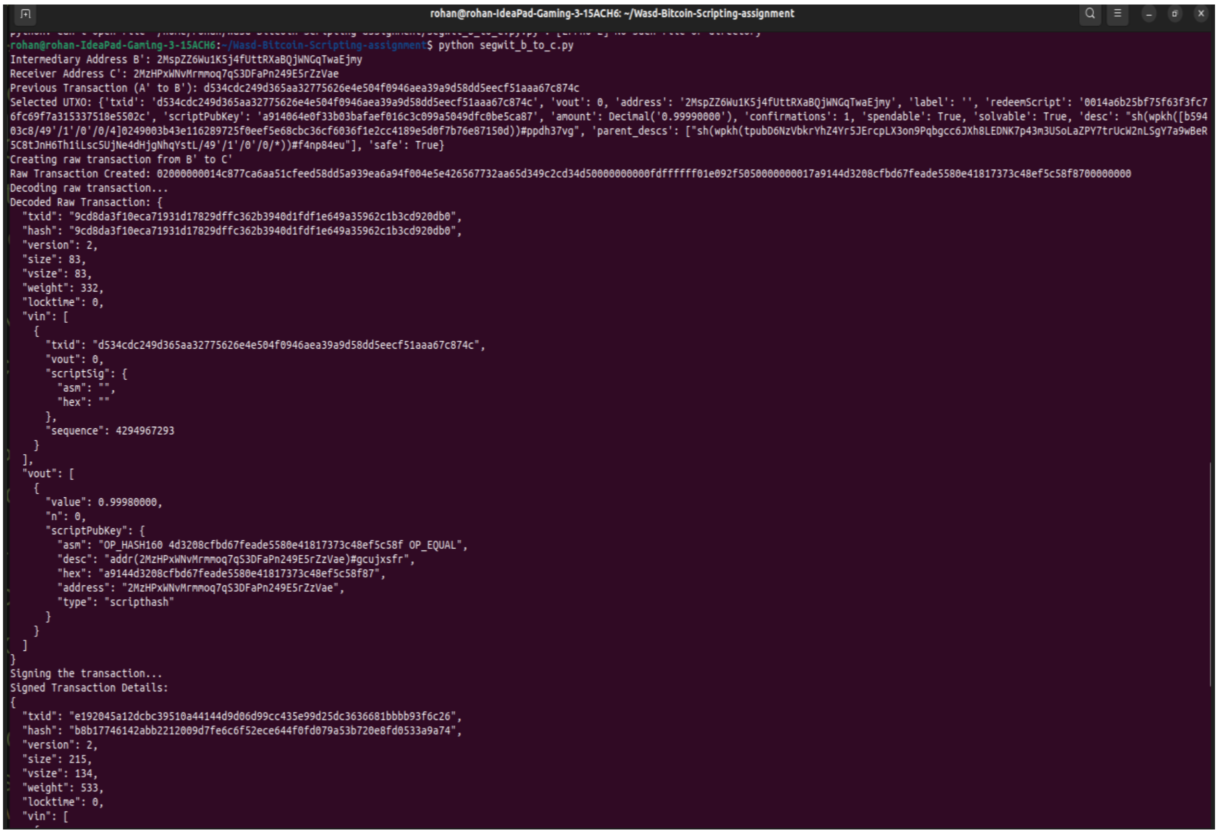
For a P2SH-P2WPKH transaction, the unlocking script is:

```
<redeemScript>
```

The witness data (not part of the scriptSig) contains:

```
<Signature> <Public Key of B'>

"tx_b_to_c": {
            "size": 215,
            "vsize": 134,
            "weight": 533,
            "scriptSig": "0014f004744611840f3536b244c8b29d5e3b0b5852f4"
        }
```



```
rohan@rohan-IdeaPad-Gaming-3-15ACH6:~/Wasd-Bitcoin-Scripting-assignment$ python segwit_b_to_c.py
Intermediary Address B': 2MspZZ6Wu1K5j4fUttRXaBQjWNGqTwaEjmy
Receiver Address C': 2MzHPxWNvMrmmoq7qS3DFaPn249E5rZzVae
Previous Transaction (A' to B'): d534cdc249d365aa32775626e4e504f0946aea39a9d58dd5eecf51aaa67c874c
Selected UTXO: {'txid': 'd534cdc249d365aa32775626e4e504f0946aea39a9d58dd5eecf51aaa67c874c', 'vout': 0, 'address': '2MspZZ6Wu1K5j4fUttRXaBQjWNGqTwaEjmy', 'label': '', 'redeemScript': '0014a6b25bf75f63f3fc7
6fc69f7a315337518e5502c', 'scriptPubKey': 'a914064e0f33b03bafaef016c3c099a5049dfc0be5ca87', 'amount': Decimal('0.99990000'), 'confirmations': 1, 'spendable': True, 'solvable': True, 'desc': "sh(wpkh([b594
03c8/49'/1'/0'/0/4]0249003b43e116289725f0eef5e68cbc36cf6036f1e2cc4189e5d0f7b76e87150d))#ppdh37vg", 'parent_descs': ["sh(wpkh(tpubD6NzVbkrYhZ4Yr5JErcpLX3on9Pqbgcc6JXh8LEDNK7p43m3USoLaZPY7trUcW2nLSgY7a9wBeR
5C8tJnH6Th1iLsc5UjNe4dHjgNhqYstL/49'/1'/0'/0/*))#f4np84eu"], 'safe': True}
Creating raw transaction from B' to C'
Raw Transaction Created: 02000000014c877ca6aa51cfeed58dd5a939ea6a94f004e5e426567732aa65d349c2cd34d50000000000fdffffff01e092f5050000000017a9144d3208cfbd67feade5580e41817373c48ef5c58f8700000000
Decoding raw transaction...
Decoded Raw Transaction: {
  "txid": "9cd8da3f10eca71931d17829dffc362b3940d1fdf1e649a35962c1b3cd920db0",
  "hash": "9cd8da3f10eca71931d17829dffc362b3940d1fdf1e649a35962c1b3cd920db0",
  "version": 2,
  "size": 83,
  "vsize": 83,
  "weight": 332,
  "locktime": 0,
  "vin": [
    {
      "txid": "d534cdc249d365aa32775626e4e504f0946aea39a9d58dd5eecf51aaa67c874c",
      "vout": 0,
      "scriptSig": {
        "asm": "",
        "hex": ""
      },
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 0.99980000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_HASH160 4d3208cfbd67feade5580e41817373c48ef5c58f OP_EQUAL",
        "desc": "addr(2MzHPxWNvMrmmoq7qS3DFaPn249E5rZzVae)#gcujxsfr",
        "hex": "a9144d3208cfbd67feade5580e41817373c48ef5c58f87",
        "address": "2MzHPxWNvMrmmoq7qS3DFaPn249E5rZzVae",
        "type": "scripthash"
      }
    }
  ]
}
Signing the transaction...
Signed Transaction Details:
{
  "txid": "e192045a12dcbc39510a44144d9d06d99cc435e99d25dc3636681bbbb93f6c26",
  "hash": "b8b17746142abb2212009d7fe6c6f52ece644f0fd079a53b720e8fd0533a9a74",
  "version": 2,
  "size": 215,
  "vsize": 134,
  "weight": 533,
  "locktime": 0,
  "vin": [
```

4.3 Script Validation

The validation process for P2SH-P2WPKH works as follows:

1. The unlocking script provides the redeemScript
2. The locking script verifies that the hash of the redeemScript matches the expected hash
3. The witness data provides the signature and public key
4. The redeemScript is executed with the witness data to verify ownership

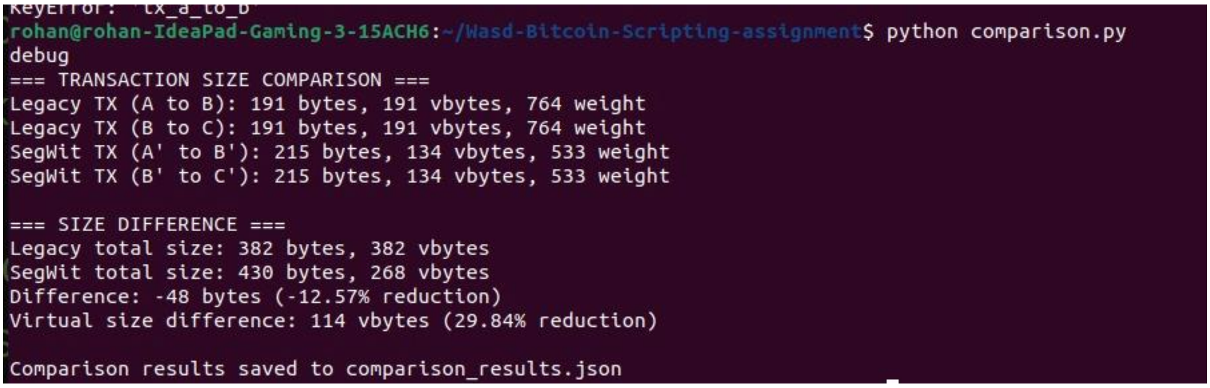
```
{
        "address_a_prime": "2N5YVgeVK8JaxDNeEja4vPMSXDDruPaSbe8",
        "address_b_prime": "2MxN4iffihUoJ8WkqgnDCHpdTu6vrGnzeks",
        "address_c_prime": "2N6RSDWaE9FmzrYAn8rA2mzK4PHuAapS3LD",
        "tx_a_to_b":
"15f00e0da6d82c54054ea3939fce946338d03ac306fe87172271759b00871c30",
        "tx_b_to_c":
"229ed081cf9af34e05122018084139b7e05d40ae4b3893357e99ca6c555e5916",
        "scriptSig": {
            "asm": "0014263e7f5fbb9155682a1af5621c00937d01b4bc5d",
            "hex": "160014263e7f5fbb9155682a1af5621c00937d01b4bc5d"
        },
        "previousScriptPubKey": {
            "asm": "OP_HASH160 3823cd961dce36366cbcdc63ace32b1fe5bb0ec0
OP_EQUAL",
            "desc": "addr(2MxN4iffihUoJ8WkqgnDCHpdTu6vrGnzeks)#x23gvyn5",
            "hex": "a9143823cd961dce36366cbcdc63ace32b1fe5bb0ec087",
            "address": "2MxN4iffihUoJ8WkqgnDCHpdTu6vrGnzeks",
            "type": "scripthash"
        }
    }
```

5. Comparison of Legacy and SegWit Transactions

5.1 Transaction Size Comparison

Transaction Type	Size (bytes)	Weight Units	Virtual Bytes
P2PKH (Legacy)	191 + 191	764 + 764	191 + 191
P2SH-P2WPKH	215 + 215	533 + 533	134 + 134

```
"comparison": {
        "size_reduction": "-12.57%",
        "vsize_reduction": "29.84%"
    }
```



```
KeyError: 'tx_a_to_b'
rohan@rohan-IdeaPad-Gaming-3-15ACH6:~/Wasd-Bitcoin-Scripting-assignment$ python comparison.py
debug
=== TRANSACTION SIZE COMPARISON ===
Legacy TX (A to B): 191 bytes, 191 vbytes, 764 weight
Legacy TX (B to C): 191 bytes, 191 vbytes, 764 weight
SegWit TX (A' to B'): 215 bytes, 134 vbytes, 533 weight
SegWit TX (B' to C'): 215 bytes, 134 vbytes, 533 weight

=== SIZE DIFFERENCE ===
Legacy total size: 382 bytes, 382 vbytes
SegWit total size: 430 bytes, 268 vbytes
Difference: -48 bytes (-12.57% reduction)
Virtual size difference: 114 vbytes (29.84% reduction)

Comparison results saved to comparison_results.json
```

The size in bytes increased by 12.5% but the vsize reduced by about 30%.

5.2 Script Structure Comparison

P2PKH (Legacy):

- ScriptPubKey: `OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG`
- ScriptSig: `<Signature> <Public Key>`

P2SH-P2WPKH (SegWit):

- ScriptPubKey: `OP_HASH160 <Hash of redeemScript> OP_EQUAL`
- ScriptSig: `<redeemScript>`
- Witness: `<Signature> <Public Key>`

5.3 Benefits of SegWit Transactions

1. **Reduced Transaction Size**: By moving signature data to the witness, SegWit transactions are smaller in terms of virtual bytes, resulting in lower fees.
2. **Malleability Fix**: SegWit addresses the transaction malleability issue by separating the witness data from the transaction hash calculation.
3. **Increased Block Capacity**: SegWit effectively increases the block capacity without changing the block size limit.
4. **Script Versioning**: SegWit introduces a version field that allows for future script upgrades.