Bitcoin Scripting Assignment Report

Course: CS 216: Introduction to Blockchain
Team Members:"Snitcher"

- Srujan Patel *230001063*
- Utkarsh Singh *230041035*
- Rohan Sinha *230041030*

GitHub Repository:
GitHub

Table of Contents

1. Introduction

This report documents the implementation and analysis of Bitcoin transactions using two address formats: Legacy (P2PKH) and P2SH-SegWit (P2SH-P2WPKH). The objective was to create, decode, and compare Bitcoin transactions using Python scripts that interact with a local Bitcoin Core node operating in regtest mode. Both the legacy and SegWit transactions were analyzed to understand the differences in their script structures and sizes.

2. Objectives

- **Wallet and Address Management:**
  Create or load wallets and generate three addresses for each address type (Legacy: A, B, C; SegWit: A′, B′, C′).

- **Transaction Creation and Analysis:**

  - For Legacy addresses, fund address A, create a transaction from A to B, and then from B to C.
  - For SegWit addresses, perform similar operations by funding A′, then transacting from A′ to B′, and finally from B′ to C′.
- **Script Decoding:**
  Decode and analyze the raw transactions to extract locking scripts (ScriptPubKey) and unlocking scripts (ScriptSig) for validation.

- **Comparative Analysis:**
  Compare transaction sizes (raw size, virtual size, and weight) between Legacy and SegWit transactions and explain the benefits of SegWit transactions.

---

3. Methodology and Experimental Setup

3.1. Environment Configuration

- **Bitcoin Core Setup:**
  The Bitcoin Core daemon (`bitcoind`) was run in regtest mode. The `bitcoin.conf` file was configured with key fee settings such as `paytxfee`, `fallbackfee`, `mintxfee`, and the `txconfirmtarget` to control transaction confirmation targets.

- **RPC Connection:**
  The Python solutions connect to Bitcoin Core via RPC using the `bitcoinrpc.authproxy` library. The connection is established with:

  - **User:** srujan
  - **Password:** ruturaj123
  - **Port:** 18443 (default regtest port)
  - Example connection string:
    `http://srujan:ruturaj123@127.0.0.1:18443`

- **Wallet Management:**
  Two separate wallets were used:
  - **Legacy Wallet:** `assignment_wallet`
  - **SegWit Wallet:** `assignment_wallet_segwit`

3.2. Wallet and Address Generation

- **Legacy (P2PKH):**
  The script `legacy.py` checks for an existing wallet or creates one if necessary. It then generates three legacy addresses (A, B, and C) using the `getnewaddress` RPC call with address type `"legacy"`.

- **SegWit (P2SH-SegWit):**
  The script `segwit.py` performs similar steps for SegWit by generating addresses of type `"p2sh-segwit"` (A′, B′, and C′).

---

4. Implementation Details

4.1. Legacy (P2PKH) Transactions

Script: `legacy.py`

- **Wallet Connection and Creation:**
  The script first attempts to connect to the Bitcoin Core RPC and then verifies if the `assignment_wallet` exists. If not, it creates and loads the wallet.

Address Generation:
Three legacy addresses are generated using the command:

```
 address_a = rpc.getnewaddress("", "legacy")
address_b = rpc.getnewaddress("", "legacy")
address_c = rpc.getnewaddress("", "legacy")
```

- **Funding Address A:**
  Address A is funded by mining 101 blocks to ensure sufficient balance using

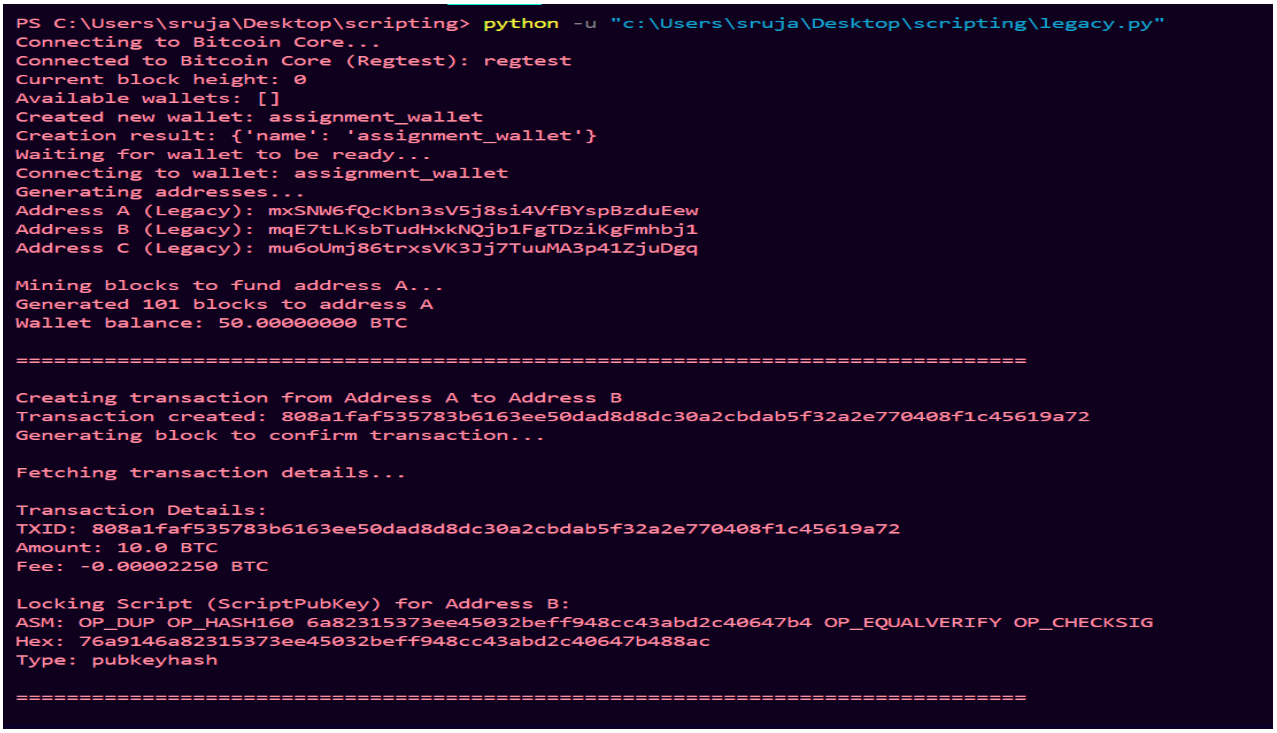
generatetoaddress.

- **Transaction from A to B:**
  A transaction is created from address A to address B using sendtoaddress. The transaction is then confirmed by mining an additional block. The raw transaction is fetched and decoded to extract the locking script (ScriptPubKey) for address B.

- **Transaction from B to C:**
  The script retrieves UTXOs for address B, creates a transaction from B to C, and decodes the transaction to extract:

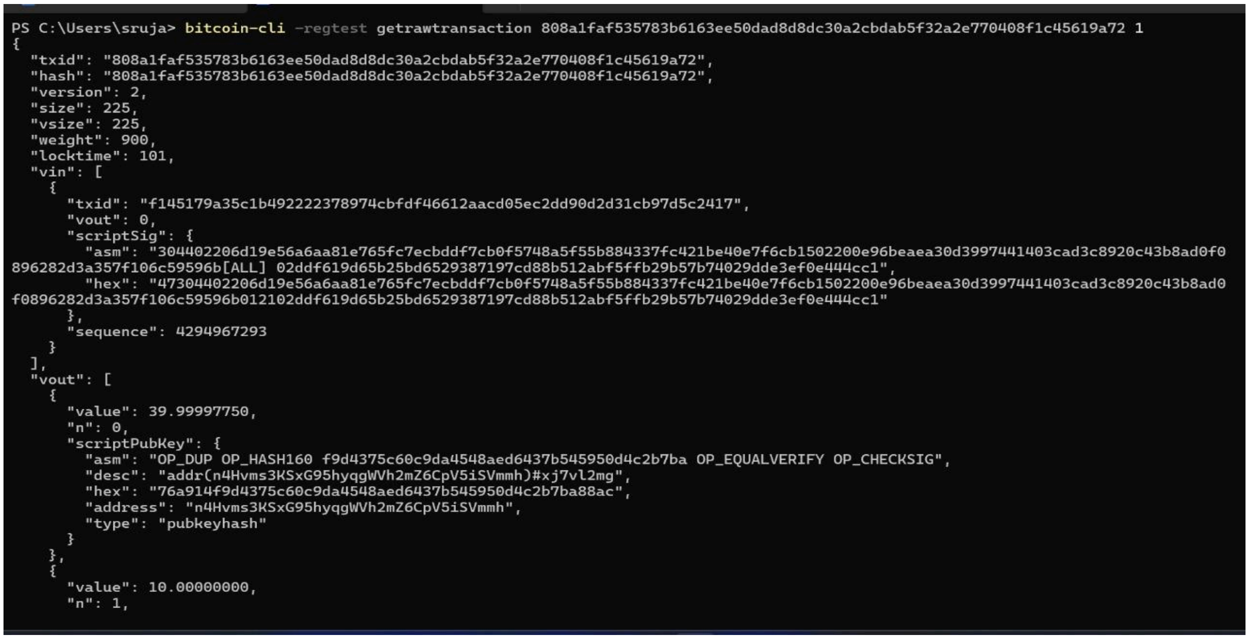
  - The unlocking script (ScriptSig) corresponding to the input that references the A→B transaction.
  - The locking script for address C.
  - Transaction size is computed in kilobytes.

Placeholder for Legacy Transaction Result Screenshot:

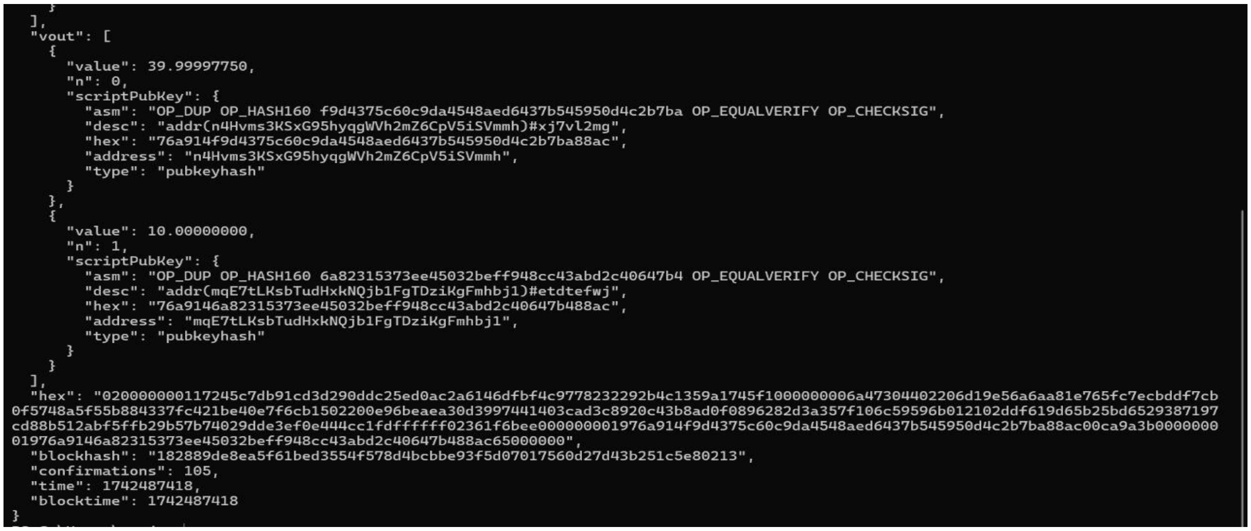


```
PS C:\Users\sruja\Desktop\scripting> python -u "c:\Users\sruja\Desktop\scripting\legacy.py"
Connecting to Bitcoin Core...
Connected to Bitcoin Core (Regtest): regtest
Current block height: 0
Available wallets: []
Created new wallet: assignment_wallet
Creation result: {'name': 'assignment_wallet'}
Waiting for wallet to be ready...
Connecting to wallet: assignment_wallet
Generating addresses...
Address A (Legacy): mxSNW6fQcKbn3sV5j8si4VfBYspBzduEew
Address B (Legacy): mqE7tLKsbTudHxkNQjb1FgTDziKgFmhbj1
Address C (Legacy): mu6oUmj86trxsVK3Jj7TuuMA3p41ZjuDgq

Mining blocks to fund address A...
Generated 101 blocks to address A
Wallet balance: 50.00000000 BTC

================================================================================

Creating transaction from Address A to Address B
Transaction created: 808a1faf535783b6163ee50dad8d8dc30a2cbdab5f32a2e770408f1c45619a72
Generating block to confirm transaction...

Fetching transaction details...

Transaction Details:
TXID: 808a1faf535783b6163ee50dad8d8dc30a2cbdab5f32a2e770408f1c45619a72
Amount: 10.0 BTC
Fee: -0.00002250 BTC

Locking Script (ScriptPubKey) for Address B:
ASM: OP_DUP OP_HASH160 6a82315373ee45032beff948cc43abd2c40647b4 OP_EQUALVERIFY OP_CHECKSIG
Hex: 76a9146a82315373ee45032beff948cc43abd2c40647b488ac
Type: pubkeyhash

================================================================================
```

Example result for A ->B Legacy Transaction:

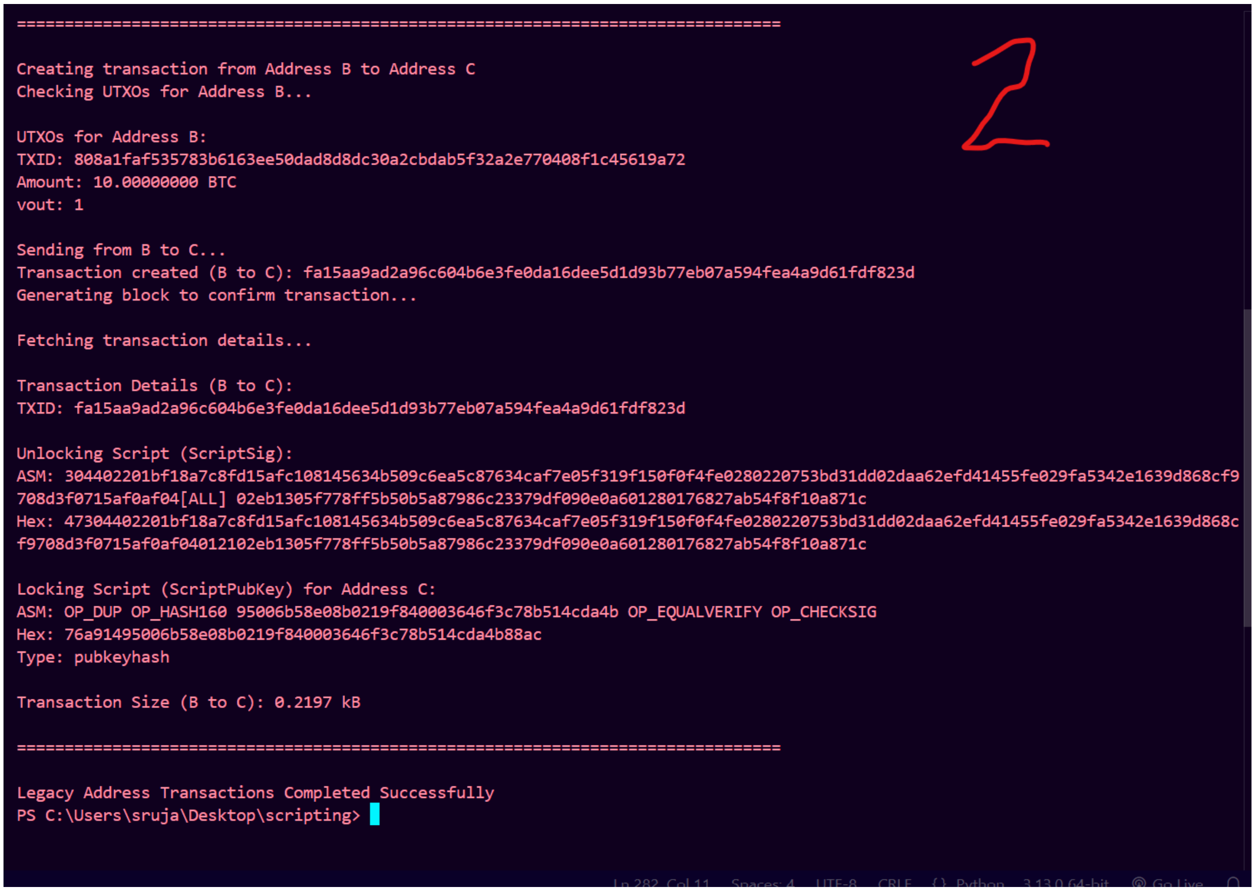


```
PS C:\Users\sruja> bitcoin-cli -regtest getrawtransaction 808a1faf535783b6163ee50dad8d8dc30a2cbdab5f32a2e770408f1c45619a72 1
{
  "txid": "808a1faf535783b6163ee50dad8d8dc30a2cbdab5f32a2e770408f1c45619a72",
  "hash": "808a1faf535783b6163ee50dad8d8dc30a2cbdab5f32a2e770408f1c45619a72",
  "version": 2,
  "size": 225,
  "vsize": 225,
  "weight": 900,
  "locktime": 101,
  "vin": [
    {
      "txid": "f145179a35c1b492222378974cbfdf46612aacd05ec2dd90d2d31cb97d5c2417",
      "vout": 0,
      "scriptSig": {
        "asm": "304402206d19e56a6aa81e765fc7ecbddf7cb0f5748a5f55b884337fc421be40e7f6cb1502200e96beaea30d3997441403cad3c8920c43b8ad0f0
896282d3a357f106c59596b[ALL] 02ddf619d65b25bd6529387197cd88b512abf5ffb29b57b74029dde3ef0e444cc1",
        "hex": "47304402206d19e56a6aa81e765fc7ecbddf7cb0f5748a5f55b884337fc421be40e7f6cb1502200e96beaea30d3997441403cad3c8920c43b8ad0
f0896282d3a357f106c59596b012102ddf619d65b25bd6529387197cd88b512abf5ffb29b57b74029dde3ef0e444cc1"
      },
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 39.99997750,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 f9d4375c60c9da4548aed6437b545950d4c2b7ba OP_EQUALVERIFY OP_CHECKSIG",
        "desc": "addr(n4Hvms3KSxG95hyqgWVh2mZ6CpV5iSVmmh)#xj7vl2mg",
        "hex": "76a914f9d4375c60c9da4548aed6437b545950d4c2b7ba88ac",
        "address": "n4Hvms3KSxG95hyqgWVh2mZ6CpV5iSVmmh",
        "type": "pubkeyhash"
      }
    },
    {
      "value": 10.00000000,
      "n": 1,
```



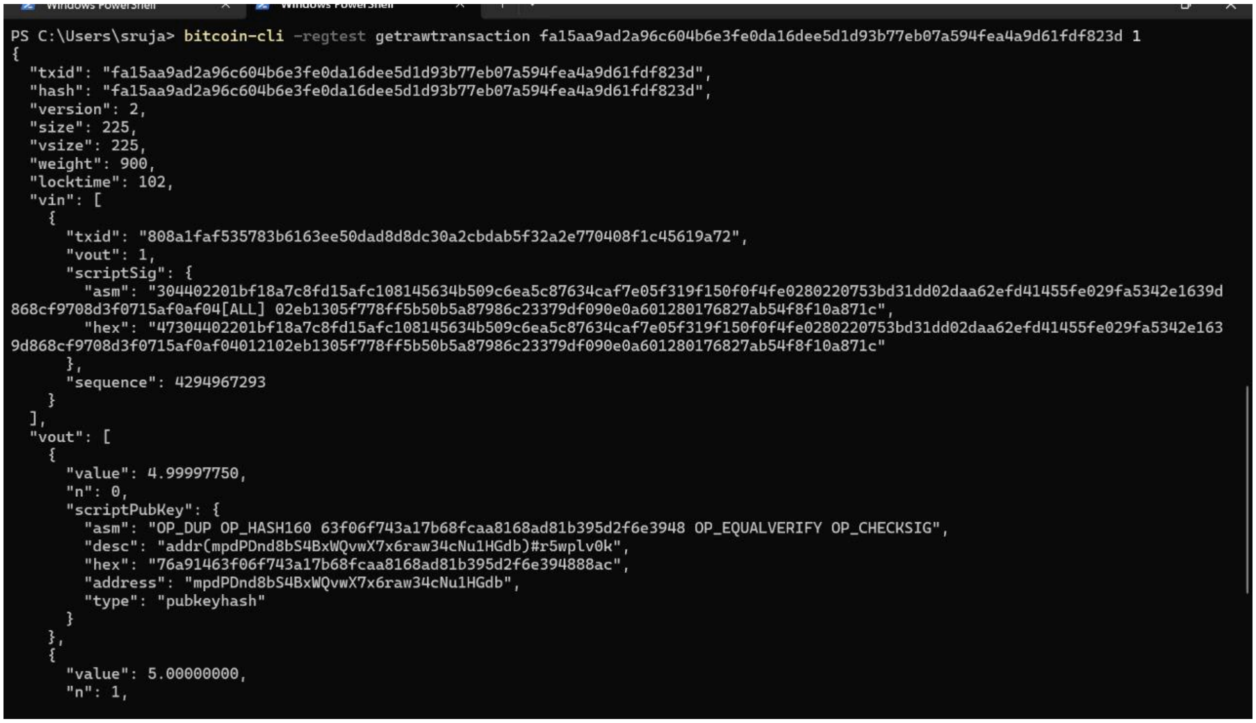
```
  ],
  "vout": [
    {
      "value": 39.99997750,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 f9d4375c60c9da4548aed6437b545950d4c2b7ba OP_EQUALVERIFY OP_CHECKSIG",
        "desc": "addr(n4Hvms3KSxG95hyqgWVh2mZ6CpV5iSVmmh)#xj7vl2mg",
        "hex": "76a914f9d4375c60c9da4548aed6437b545950d4c2b7ba88ac",
        "address": "n4Hvms3KSxG95hyqgWVh2mZ6CpV5iSVmmh",
        "type": "pubkeyhash"
      }
    },
    {
      "value": 10.00000000,
      "n": 1,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 6a82315373ee45032beff948cc43abd2c40647b4 OP_EQUALVERIFY OP_CHECKSIG",
        "desc": "addr(mqE7tLKsbTudHxkNQjb1FgTDziKgFmhbj1)#etdtefwj",
        "hex": "76a9146a82315373ee45032beff948cc43abd2c40647b488ac",
        "address": "mqE7tLKsbTudHxkNQjb1FgTDziKgFmhbj1",
        "type": "pubkeyhash"
      }
    }
  ],
  "hex": "020000000117245c7db91cd3d290ddc25ed0ac2a6146dfbf4c9778232292b4c1359a1745f1000000006a47304402206d19e56a6aa81e765fc7ecbddf7cb
0f5748a5f55b884337fc421be40e7f6cb1502200e96beaea30d3997441403cad3c8920c43b8ad0f0896282d3a357f106c59596b012102ddf619d65b25bd6529387197
cd88b512abf5ffb29b57b74029dde3ef0e444cc1fdffffff02361f6bee000000001976a914f9d4375c60c9da4548aed6437b545950d4c2b7ba88ac00ca9a3b0000000
01976a9146a82315373ee45032beff948cc43abd2c40647b488ac65000000",
  "blockhash": "182889de8ea5f61bed3554f578d4bcbbe93f5d07017560d27d43b251c5e80213",
  "confirmations": 105,
  "time": 1742487418,
  "blocktime": 1742487418
}
```

Example result for B ->C Legacy Transaction:

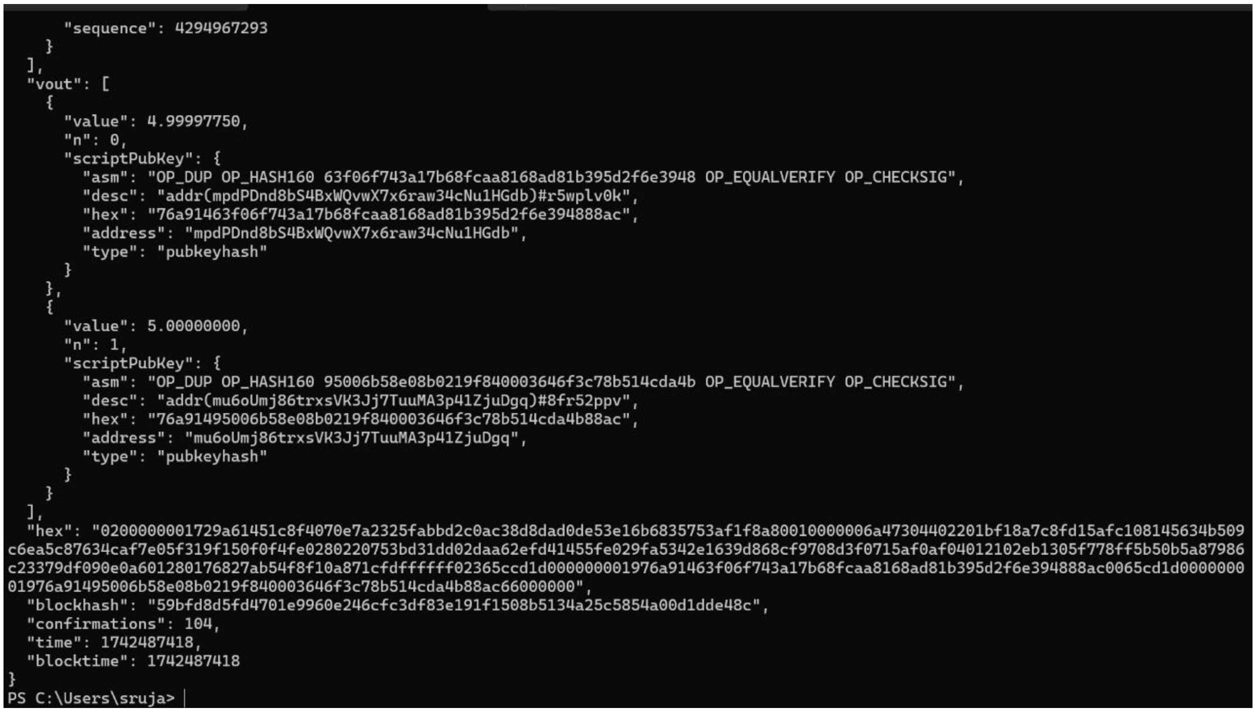


2

```
================================================================================

Creating transaction from Address B to Address C
Checking UTXOs for Address B...

UTXOs for Address B:
TXID: 808a1faf535783b6163ee50dad8d8dc30a2cbdab5f32a2e770408f1c45619a72
Amount: 10.00000000 BTC
vout: 1

Sending from B to C...
Transaction created (B to C): fa15aa9ad2a96c604b6e3fe0da16dee5d1d93b77eb07a594fea4a9d61fdf823d
Generating block to confirm transaction...

Fetching transaction details...

Transaction Details (B to C):
TXID: fa15aa9ad2a96c604b6e3fe0da16dee5d1d93b77eb07a594fea4a9d61fdf823d

Unlocking Script (ScriptSig):
ASM: 304402201bf18a7c8fd15afc108145634b509c6ea5c87634caf7e05f319f150f0f4fe0280220753bd31dd02daa62efd41455fe029fa5342e1639d868cf9
708d3f0715af0af04[ALL] 02eb1305f778ff5b50b5a87986c23379df090e0a601280176827ab54f8f10a871c
Hex: 47304402201bf18a7c8fd15afc108145634b509c6ea5c87634caf7e05f319f150f0f4fe0280220753bd31dd02daa62efd41455fe029fa5342e1639d868c
f9708d3f0715af0af04012102eb1305f778ff5b50b5a87986c23379df090e0a601280176827ab54f8f10a871c

Locking Script (ScriptPubKey) for Address C:
ASM: OP_DUP OP_HASH160 95006b58e08b0219f840003646f3c78b514cda4b OP_EQUALVERIFY OP_CHECKSIG
Hex: 76a91495006b58e08b0219f840003646f3c78b514cda4b88ac
Type: pubkeyhash

Transaction Size (B to C): 0.2197 kB

================================================================================

Legacy Address Transactions Completed Successfully
PS C:\Users\sruja\Desktop\scripting>
```



```
PS C:\Users\sruja> bitcoin-cli -regtest getrawtransaction fa15aa9ad2a96c604b6e3fe0da16dee5d1d93b77eb07a594fea4a9d61fdf823d 1
{
  "txid": "fa15aa9ad2a96c604b6e3fe0da16dee5d1d93b77eb07a594fea4a9d61fdf823d",
  "hash": "fa15aa9ad2a96c604b6e3fe0da16dee5d1d93b77eb07a594fea4a9d61fdf823d",
  "version": 2,
  "size": 225,
  "vsize": 225,
  "weight": 900,
  "locktime": 102,
  "vin": [
    {
      "txid": "808a1faf535783b6163ee50dad8d8dc30a2cbdab5f32a2e770408f1c45619a72",
      "vout": 1,
      "scriptSig": {
        "asm": "304402201bf18a7c8fd15afc108145634b509c6ea5c87634caf7e05f319f150f0f4fe0280220753bd31dd02daa62efd41455fe029fa5342e1639d
868cf9708d3f0715af0af04[ALL] 02eb1305f778ff5b50b5a87986c23379df090e0a601280176827ab54f8f10a871c",
        "hex": "47304402201bf18a7c8fd15afc108145634b509c6ea5c87634caf7e05f319f150f0f4fe0280220753bd31dd02daa62efd41455fe029fa5342e163
9d868cf9708d3f0715af0af04012102eb1305f778ff5b50b5a87986c23379df090e0a601280176827ab54f8f10a871c"
      },
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 4.99997750,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 63f06f743a17b68fcaa8168ad81b395d2f6e3948 OP_EQUALVERIFY OP_CHECKSIG",
        "desc": "addr(mpdPDnd8bS4BxWQvwX7x6raw34cNu1HGdb)#r5wplv0k",
        "hex": "76a91463f06f743a17b68fcaa8168ad81b395d2f6e394888ac",
        "address": "mpdPDnd8bS4BxWQvwX7x6raw34cNu1HGdb",
        "type": "pubkeyhash"
      }
    },
    {
      "value": 5.00000000,
      "n": 1,
```



```
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 4.99997750,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 63f06f743a17b68fcaa8168ad81b395d2f6e3948 OP_EQUALVERIFY OP_CHECKSIG",
        "desc": "addr(mpdPDnd8bS4BxWQvwX7x6raw34cNu1HGdb)#r5wplv0k",
        "hex": "76a91463f06f743a17b68fcaa8168ad81b395d2f6e394888ac",
        "address": "mpdPDnd8bS4BxWQvwX7x6raw34cNu1HGdb",
        "type": "pubkeyhash"
      }
    },
    {
      "value": 5.00000000,
      "n": 1,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 95006b58e08b0219f840003646f3c78b514cda4b OP_EQUALVERIFY OP_CHECKSIG",
        "desc": "addr(mu6oUmj86trxsVK3Jj7TuuMA3p41ZjuDgq)#8fr52ppv",
        "hex": "76a91495006b58e08b0219f840003646f3c78b514cda4b88ac",
        "address": "mu6oUmj86trxsVK3Jj7TuuMA3p41ZjuDgq",
        "type": "pubkeyhash"
      }
    }
  ],
  "hex": "0200000001729a61451c8f4070e7a2325fabbd2c0ac38d8dad0de53e16b6835753af1f8a80010000006a47304402201bf18a7c8fd15afc108145634b509
c6ea5c87634caf7e05f319f150f0f4fe0280220753bd31dd02daa62efd41455fe029fa5342e1639d868cf9708d3f0715af0af04012102eb1305f778ff5b50b5a87986
c23379df090e0a601280176827ab54f8f10a871cfdffffff02365ccd1d000000001976a91463f06f743a17b68fcaa8168ad81b395d2f6e394888ac0065cd1d0000000
01976a91495006b58e08b0219f840003646f3c78b514cda4b88ac66000000",
  "blockhash": "59bfd8d5fd4701e9960e246cfc3df83e191f1508b5134a25c5854a00d1dde48c",
  "confirmations": 104,
  "time": 1742487418,
  "blocktime": 1742487418
}
PS C:\Users\sruja> |
```

4.2. P2SH-SegWit (SegWit) Transactions

Script: `segwit.py`

- **Wallet Connection and Creation:**
  The SegWit wallet (`assignment_wallet_segwit`) is loaded or created. The script then reconnects using the wallet-specific RPC endpoint.

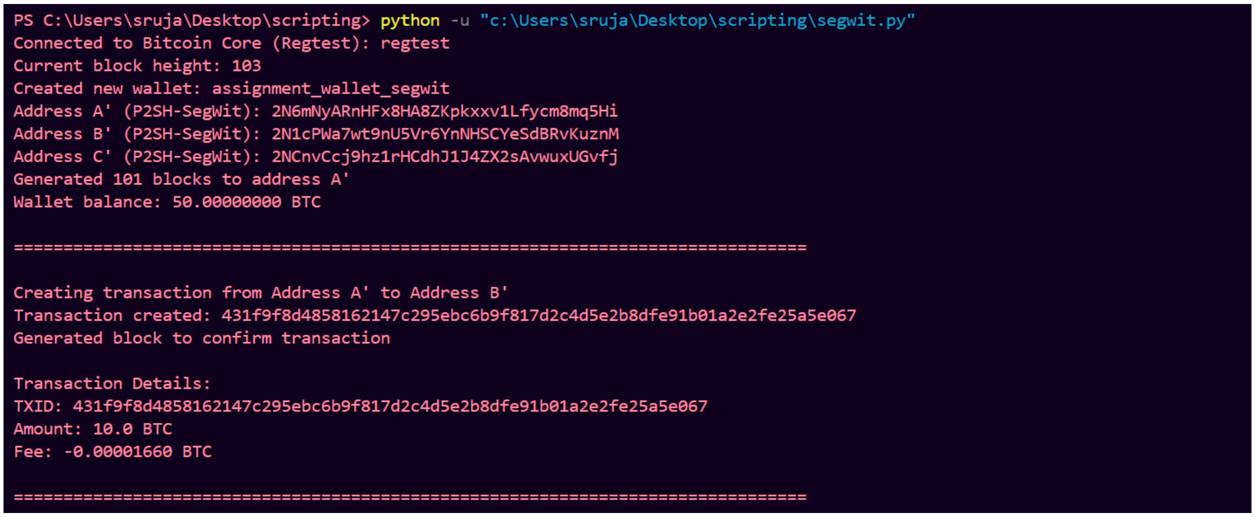
- **Address Generation:**
  Three SegWit addresses (A′, B′, and C′) are generated using the `"p2sh-segwit"` address type.

- **Funding Address A′:**
  Similar to the legacy process, address A′ is funded by mining 101 blocks.

- **Transaction from A′ to B′:**
  A transaction is executed from address A′ to B′, followed by confirmation via block generation. The script decodes the transaction to retrieve the locking script for address B′.

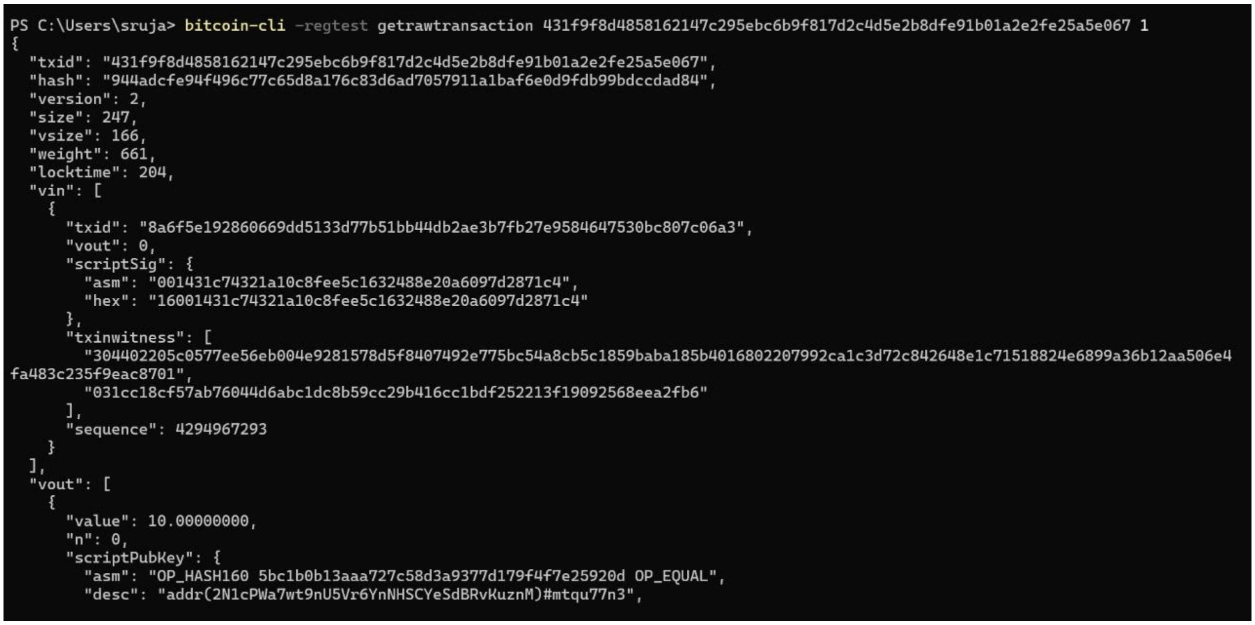
- **Transaction from B′ to C′:**
  After listing UTXOs for address B′, a transaction is created from B′ to C′. The decoding process in this transaction:
  - Extracts the unlocking script (ScriptSig) and includes SegWit-specific witness data if available.
  - Retrieves the locking script for address C′.
  - Computes the transaction size.

Placeholder for SegWit Transaction Result Screenshot:

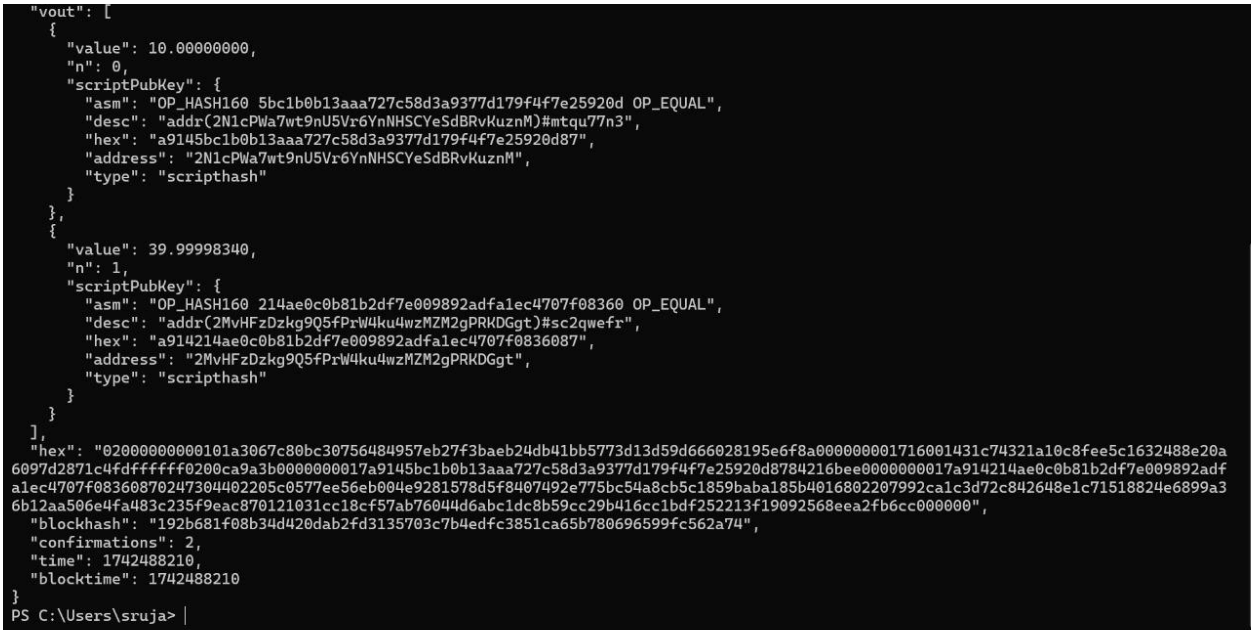


```
PS C:\Users\sruja\Desktop\scripting> python -u "c:\Users\sruja\Desktop\scripting\segwit.py"
Connected to Bitcoin Core (Regtest): regtest
Current block height: 103
Created new wallet: assignment_wallet_segwit
Address A' (P2SH-SegWit): 2N6mNyARnHFx8HA8ZKpkxxv1Lfycm8mq5Hi
Address B' (P2SH-SegWit): 2N1cPWa7wt9nU5Vr6YnNHSCYeSdBRvKuznM
Address C' (P2SH-SegWit): 2NCnvCcj9hz1rHCdhJ1J4ZX2sAvwuxUGvfj
Generated 101 blocks to address A'
Wallet balance: 50.00000000 BTC

================================================================================

Creating transaction from Address A' to Address B'
Transaction created: 431f9f8d4858162147c295ebc6b9f817d2c4d5e2b8dfe91b01a2e2fe25a5e067
Generated block to confirm transaction

Transaction Details:
TXID: 431f9f8d4858162147c295ebc6b9f817d2c4d5e2b8dfe91b01a2e2fe25a5e067
Amount: 10.0 BTC
Fee: -0.00001660 BTC

================================================================================
```

- **Transaction from A′ to B′:**

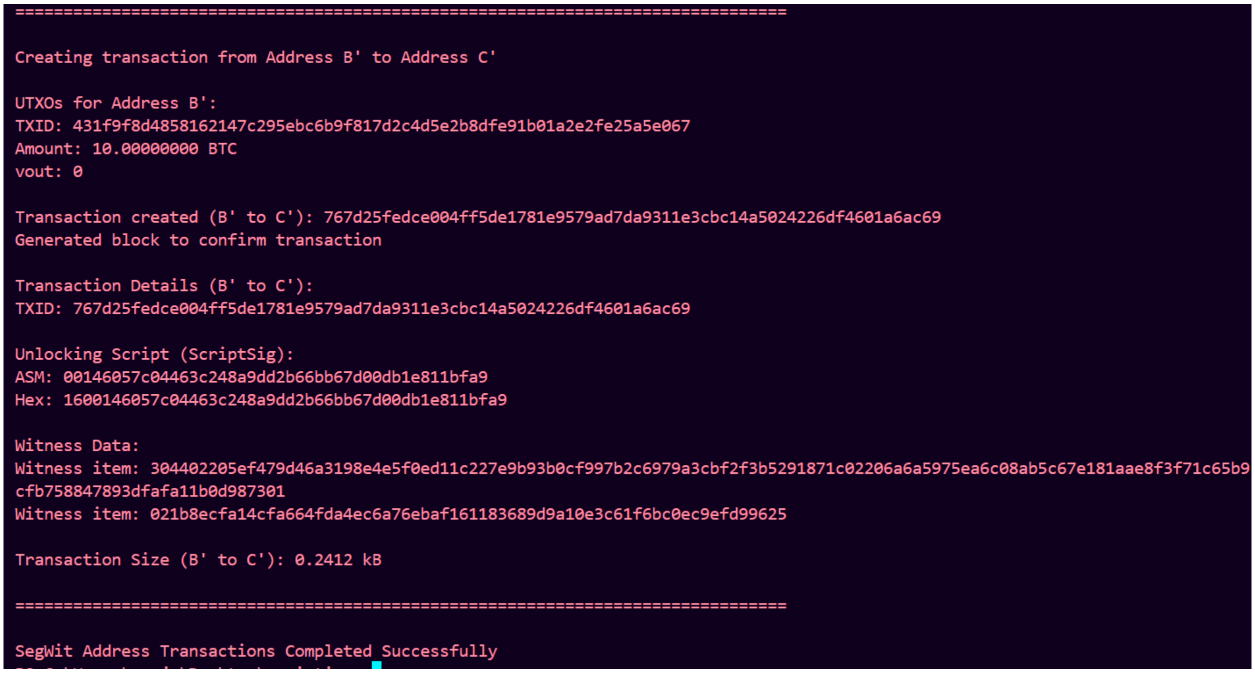


```
PS C:\Users\sruja> bitcoin-cli -regtest getrawtransaction 431f9f8d4858162147c295ebc6b9f817d2c4d5e2b8dfe91b01a2e2fe25a5e067 1
{
  "txid": "431f9f8d4858162147c295ebc6b9f817d2c4d5e2b8dfe91b01a2e2fe25a5e067",
  "hash": "944adcfe94f496c77c65d8a176c83d6ad7057911a1baf6e0d9fdb99bdccdad84",
  "version": 2,
  "size": 247,
  "vsize": 166,
  "weight": 661,
  "locktime": 204,
  "vin": [
    {
      "txid": "8a6f5e192860669dd5133d77b51bb44db2ae3b7fb27e9584647530bc807c06a3",
      "vout": 0,
      "scriptSig": {
        "asm": "001431c74321a10c8fee5c1632488e20a6097d2871c4",
        "hex": "16001431c74321a10c8fee5c1632488e20a6097d2871c4"
      },
      "txinwitness": [
        "304402205c0577ee56eb004e9281578d5f8407492e775bc54a8cb5c1859baba185b4016802207992ca1c3d72c842648e1c71518824e6899a36b12aa506e4
fa483c235f9eac8701",
        "031cc18cf57ab76044d6abc1dc8b59cc29b416cc1bdf252213f19092568eea2fb6"
      ],
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 10.00000000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_HASH160 5bc1b0b13aaa727c58d3a9377d179f4f7e25920d OP_EQUAL",
        "desc": "addr(2N1cPWa7wt9nU5Vr6YnNHSCYeSdBRvKuznM)#mtqu77n3",
```

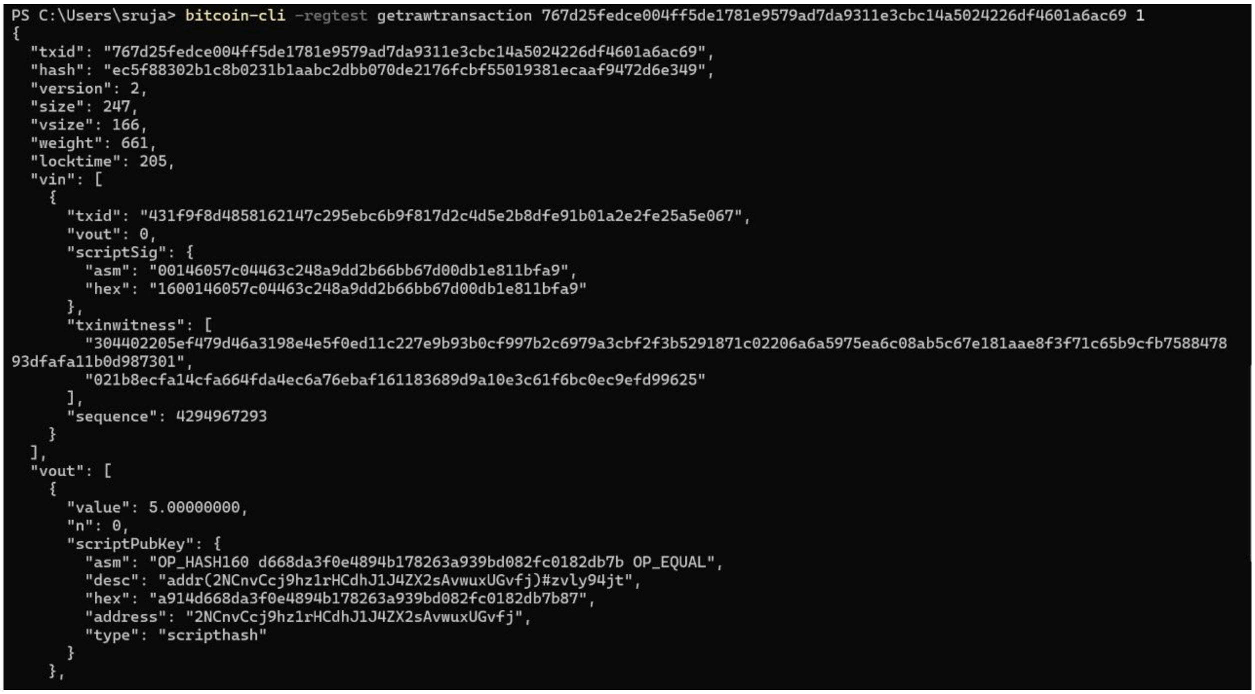


```
  "vout": [
    {
      "value": 10.00000000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_HASH160 5bc1b0b13aaa727c58d3a9377d179f4f7e25920d OP_EQUAL",
        "desc": "addr(2N1cPWa7wt9nU5Vr6YnNHSCYeSdBRvKuznM)#mtqu77n3",
        "hex": "a9145bc1b0b13aaa727c58d3a9377d179f4f7e25920d87",
        "address": "2N1cPWa7wt9nU5Vr6YnNHSCYeSdBRvKuznM",
        "type": "scripthash"
      }
    },
    {
      "value": 39.99998340,
      "n": 1,
      "scriptPubKey": {
        "asm": "OP_HASH160 214ae0c0b81b2df7e009892adfa1ec4707f08360 OP_EQUAL",
        "desc": "addr(2MvHFzDzkg9Q5fPrW4ku4wzMZM2gPRKDGgt)#sc2qwefr",
        "hex": "a914214ae0c0b81b2df7e009892adfa1ec4707f0836087",
        "address": "2MvHFzDzkg9Q5fPrW4ku4wzMZM2gPRKDGgt",
        "type": "scripthash"
      }
    }
  ],
  "hex": "02000000000101a3067c80bc30756484957eb27f3baeb24db41bb5773d13d59d666028195e6f8a0000000017160014 31c74321a10c8fee5c1632488e20a
6097d2871c4fdffffff0200ca9a3b0000000017a9145bc1b0b13aaa727c58d3a9377d179f4f7e25920d8784216bee0000000017a914214ae0c0b81b2df7e009892adf
a1ec4707f0836087024730440220 5c0577ee56eb004e9281578d5f8407492e775bc54a8cb5c1859baba185b4016802207992ca1c3d72c842648e1c71518824e6899a3
6b12aa506e4fa483c235f9eac870121031cc18cf57ab76044d6abc1dc8b59cc29b416cc1bdf252213f19092568eea2fb6cc000000",
  "blockhash": "192b681f08b34d420dab2fd3135703c7b4edfc3851ca65b780696599fc562a74",
  "confirmations": 2,
  "time": 1742488210,
  "blocktime": 1742488210
}
PS C:\Users\sruja> |
```

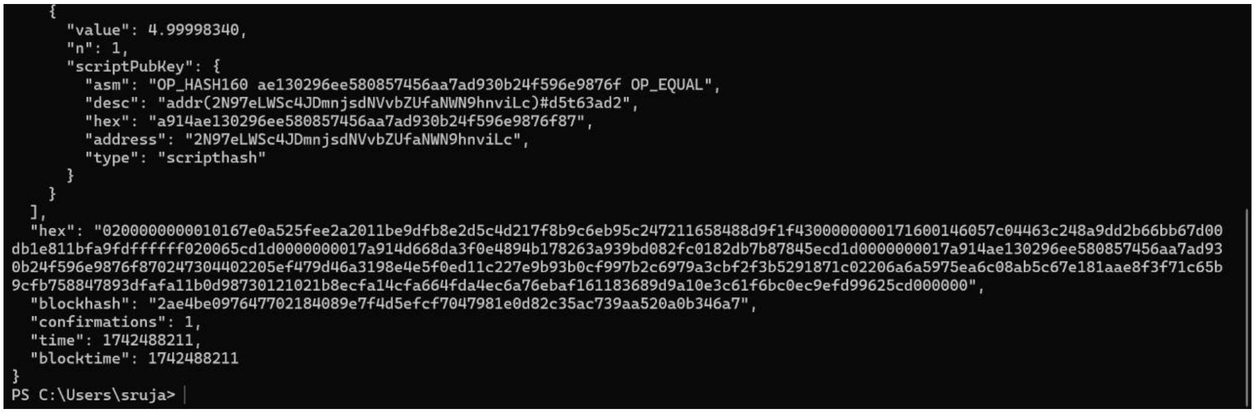
- **Transaction from B′ to C′:**



```
================================================================================

Creating transaction from Address B' to Address C'

UTXOs for Address B':
TXID: 431f9f8d4858162147c295ebc6b9f817d2c4d5e2b8dfe91b01a2e2fe25a5e067
Amount: 10.00000000 BTC
vout: 0

Transaction created (B' to C'): 767d25fedce004ff5de1781e9579ad7da9311e3cbc14a5024226df4601a6ac69
Generated block to confirm transaction

Transaction Details (B' to C'):
TXID: 767d25fedce004ff5de1781e9579ad7da9311e3cbc14a5024226df4601a6ac69

Unlocking Script (ScriptSig):
ASM: 00146057c04463c248a9dd2b66bb67d00db1e811bfa9
Hex: 1600146057c04463c248a9dd2b66bb67d00db1e811bfa9

Witness Data:
Witness item: 304402205ef479d46a3198e4e5f0ed11c227e9b93b0cf997b2c6979a3cbf2f3b5291871c02206a6a5975ea6c08ab5c67e181aae8f3f71c65b9
cfb758847893dfafa11b0d987301
Witness item: 021b8ecfa14cfa664fda4ec6a76ebaf161183689d9a10e3c61f6bc0ec9efd99625

Transaction Size (B' to C'): 0.2412 kB

================================================================================

SegWit Address Transactions Completed Successfully
```



```
PS C:\Users\sruja> bitcoin-cli -regtest getrawtransaction 767d25fedce004ff5de1781e9579ad7da9311e3cbc14a5024226df4601a6ac69 1
{
  "txid": "767d25fedce004ff5de1781e9579ad7da9311e3cbc14a5024226df4601a6ac69",
  "hash": "ec5f88302b1c8b0231b1aabc2dbb070de2176fcbf55019381ecaaf9472d6e349",
  "version": 2,
  "size": 247,
  "vsize": 166,
  "weight": 661,
  "locktime": 205,
  "vin": [
    {
      "txid": "431f9f8d4858162147c295ebc6b9f817d2c4d5e2b8dfe91b01a2e2fe25a5e067",
      "vout": 0,
      "scriptSig": {
        "asm": "00146057c04463c248a9dd2b66bb67d00db1e811bfa9",
        "hex": "1600146057c04463c248a9dd2b66bb67d00db1e811bfa9"
      },
      "txinwitness": [
        "304402205ef479d46a3198e4e5f0ed11c227e9b93b0cf997b2c6979a3cbf2f3b5291871c02206a6a5975ea6c08ab5c67e181aae8f3f71c65b9cfb7588478
93dfafa11b0d987301",
        "021b8ecfa14cfa664fda4ec6a76ebaf161183689d9a10e3c61f6bc0ec9efd99625"
      ],
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 5.00000000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_HASH160 d668da3f0e4894b178263a939bd082fc0182db7b OP_EQUAL",
        "desc": "addr(2NCnvCcj9hz1rHCdhJ1J4ZX2sAvwuxUGvfj)#zvly94jt",
        "hex": "a914d668da3f0e4894b178263a939bd082fc0182db7b87",
        "address": "2NCnvCcj9hz1rHCdhJ1J4ZX2sAvwuxUGvfj",
        "type": "scripthash"
      }
    },
```



```
    {
      "value": 4.99998340,
      "n": 1,
      "scriptPubKey": {
        "asm": "OP_HASH160 ae130296ee580857456aa7ad930b24f596e9876f OP_EQUAL",
        "desc": "addr(2N97eLWSc4JDmnjsdNVvbZUfaNWN9hnviLc)#d5t63ad2",
        "hex": "a914ae130296ee580857456aa7ad930b24f596e9876f87",
        "address": "2N97eLWSc4JDmnjsdNVvbZUfaNWN9hnviLc",
        "type": "scripthash"
      }
    }
  ],
  "hex": "0200000000010167e0a525fee2a2011be9dfb8e2d5c4d217f8b9c6eb95c247211658488d9f1f4300000000171600146057c04463c248a9dd2b66bb67d00
db1e811bfa9fdffffff020065cd1d0000000017a914d668da3f0e4894b178263a939bd082fc0182db7b87845ecd1d0000000017a914ae130296ee580857456aa7ad93
0b24f596e9876f870247304402205ef479d46a3198e4e5f0ed11c227e9b93b0cf997b2c6979a3cbf2f3b5291871c02206a6a5975ea6c08ab5c67e181aae8f3f71c65b
9cfb758847893dfafa11b0d98730121021b8ecfa14cfa664fda4ec6a76ebaf161183689d9a10e3c61f6bc0ec9efd99625cd000000",
  "blockhash": "2ae4be097647702184089e7f4d5efcf7047981e0d82c35ac739aa520a0b346a7",
  "confirmations": 1,
  "time": 1742488211,
  "blocktime": 1742488211
}
PS C:\Users\sruja>
```

4.3. Transaction Comparison and Analysis

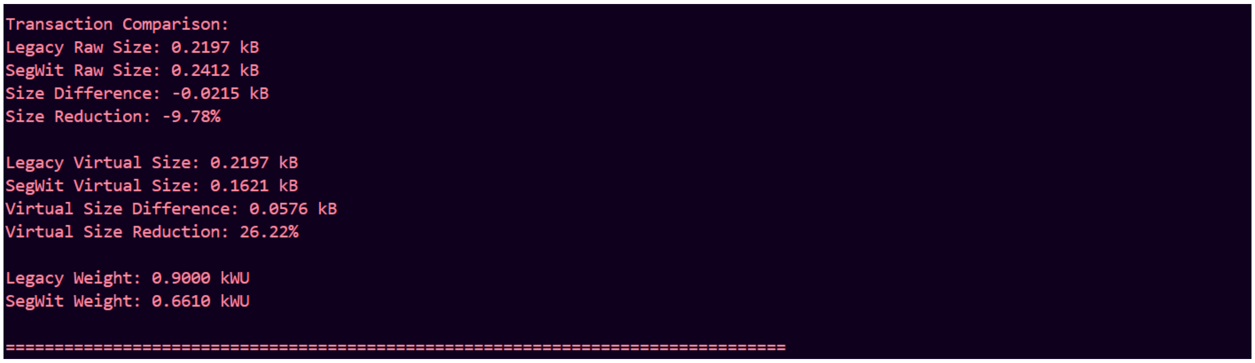
Script: `transaction_comp.py`

- **Analysis Functionality:**
  The script prompts the user to input the transaction IDs (txid) for the legacy transaction (B → C) and the SegWit transaction (B′ → C′). It then performs detailed analysis by:

    - Decoding each raw transaction.
    - Computing the raw size (in kB), virtual size (in kB), and weight (in kWU).
    - Counting the number of inputs and outputs.
    - Displaying the sizes and details of the ScriptSig (unlocking script) and ScriptPubKey (locking script) for each input/output.

- **Comparison:**
  The script calculates the difference in size between legacy and SegWit transactions, showing the percentage of size reduction in both raw and virtual sizes. It also discusses the benefits of SegWit such as lower transaction fees, improved scalability, and a fix for transaction malleability.

Placeholder for Transaction Comparison Result Screenshot:



```
Transaction Comparison:
Legacy Raw Size: 0.2197 kB
SegWit Raw Size: 0.2412 kB
Size Difference: -0.0215 kB
Size Reduction: -9.78%

Legacy Virtual Size: 0.2197 kB
SegWit Virtual Size: 0.1621 kB
Virtual Size Difference: 0.0576 kB
Virtual Size Reduction: 26.22%

Legacy Weight: 0.9000 kWU
SegWit Weight: 0.6610 kWU

================================================================================
```

---

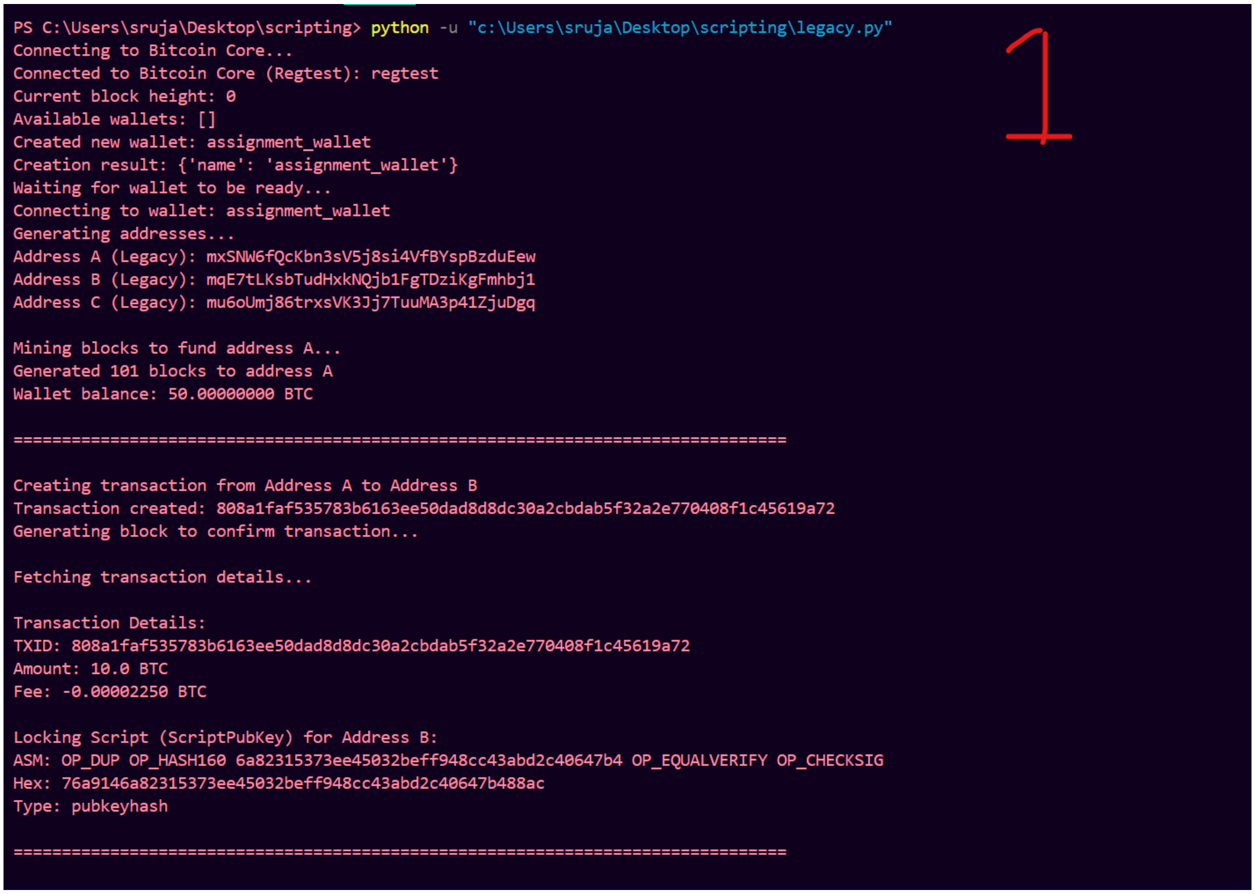
5. Results

The following results were obtained after executing the scripts:

Legacy Transactions:

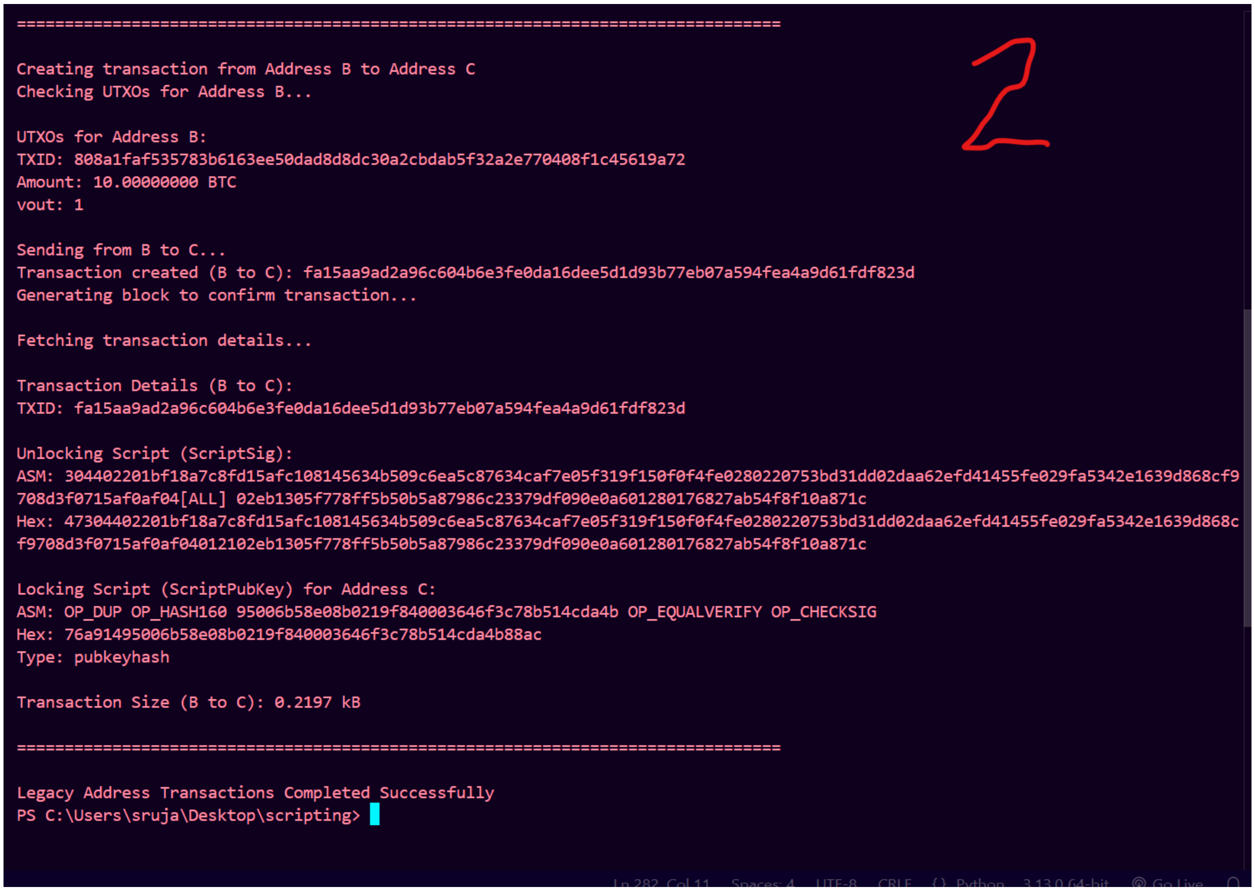
- **Transaction A → B:**
    - **TXID:** 808alfaf535783b6163ee50dad8d8dc30a2cbdab5f32a2e770408f1c45619a72
    - **Locking Script (Address B):**
        - **ASM:** OP_DUP OP_HASH160 f9d4375c60c9da4548aed6437b545950d4c2b7ba OP_EQUALVERIFY OP_CHECKSIG
        - **Hex:**76a914f9d4375c60c9da4548aed6437b545950d4c2b7ba88ac

        - **Type:** pubkeyhash
- **Transaction B → C:**
    - **TXID:** fa15aa9ad2a96c604b6e3fe0da16dee5d1d93b77eb07a594fea4a9d61fdf823d
    - **Unlocking Script (ScriptSig) from input referencing A→B:**
        - **ASM:** 304402201bf18a7c8fd15afc108145634b509c6ea5c87634caf7e05f319f150f0f4fe0280220753bd31dd02daa62efd41455fe029fa5342e1639d868cf9708d3f0715af0af04 [ALL] 02eb1305f778ff5b50b5a87986c23379df090e0a601280176827ab54f8f10a871c
        - **Hex:** 47304402201bf18a7c8fd15afc108145634b509c6ea5c87634caf7e05f319f150f0f4fe0280220753bd31dd02daa62efd41455fe029fa5342e1639d868cf9708d3f0715af0af04012102eb1305f778ff5b50b5a87986c23379df090e0a601280176827ab54f8f10a871c
    - **Locking Script (Address C):**
        - **ASM:** *OP_DUP OP_HASH160 63f06f743a17b68fcaa8168ad81b395d2f6e3948 OP_EQUALVERIFY OP_CHECKSIG*
        - **Hex:** 76a91463f06f743a17b68fcaa8168ad81b395d2f6e394888ac
        - **Type:** pubkeyhash
    - **Transaction Size:** *0.2197 kB*



```
PS C:\Users\sruja\Desktop\scripting> python -u "c:\Users\sruja\Desktop\scripting\legacy.py"
Connecting to Bitcoin Core...
Connected to Bitcoin Core (Regtest): regtest
Current block height: 0
Available wallets: []
Created new wallet: assignment_wallet
Creation result: {'name': 'assignment_wallet'}
Waiting for wallet to be ready...
Connecting to wallet: assignment_wallet
Generating addresses...
Address A (Legacy): mxSNW6fQcKbn3sV5j8si4VfBYspBzduEew
Address B (Legacy): mqE7tLKsbTudHxkNQjb1FgTDziKgFmhbj1
Address C (Legacy): mu6oUmj86trxsVK3Jj7TuuMA3p41ZjuDgq

Mining blocks to fund address A...
Generated 101 blocks to address A
Wallet balance: 50.00000000 BTC

================================================================================

Creating transaction from Address A to Address B
Transaction created: 808a1faf535783b6163ee50dad8d8dc30a2cbdab5f32a2e770408f1c45619a72
Generating block to confirm transaction...

Fetching transaction details...

Transaction Details:
TXID: 808a1faf535783b6163ee50dad8d8dc30a2cbdab5f32a2e770408f1c45619a72
Amount: 10.0 BTC
Fee: -0.00002250 BTC

Locking Script (ScriptPubKey) for Address B:
ASM: OP_DUP OP_HASH160 6a82315373ee45032beff948cc43abd2c40647b4 OP_EQUALVERIFY OP_CHECKSIG
Hex: 76a9146a82315373ee45032beff948cc43abd2c40647b488ac
Type: pubkeyhash

================================================================================
```

1

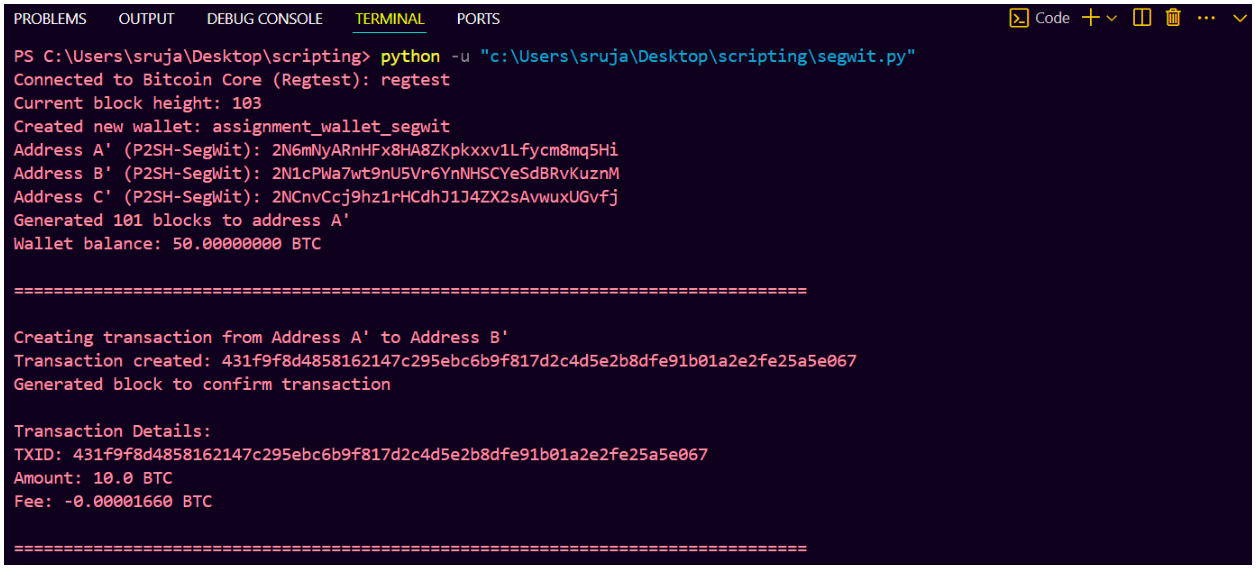

2
Ln 282, Col 11   Spaces: 4   UTF-8   CRLF   {} Python   3.13.0 64-bit   Go Live

```
================================================================================

Creating transaction from Address B to Address C
Checking UTXOs for Address B...

UTXOs for Address B:
TXID: 808a1faf535783b6163ee50dad8d8dc30a2cbdab5f32a2e770408f1c45619a72
Amount: 10.00000000 BTC
vout: 1

Sending from B to C...
Transaction created (B to C): fa15aa9ad2a96c604b6e3fe0da16dee5d1d93b77eb07a594fea4a9d61fdf823d
Generating block to confirm transaction...

Fetching transaction details...

Transaction Details (B to C):
TXID: fa15aa9ad2a96c604b6e3fe0da16dee5d1d93b77eb07a594fea4a9d61fdf823d

Unlocking Script (ScriptSig):
ASM: 304402201bf18a7c8fd15afc108145634b509c6ea5c87634caf7e05f319f150f0f4fe0280220753bd31dd02daa62efd41455fe029fa5342e1639d868cf9
708d3f0715af0af04[ALL] 02eb1305f778ff5b50b5a87986c23379df090e0a601280176827ab54f8f10a871c
Hex: 47304402201bf18a7c8fd15afc108145634b509c6ea5c87634caf7e05f319f150f0f4fe0280220753bd31dd02daa62efd41455fe029fa5342e1639d868c
f9708d3f0715af0af04012102eb1305f778ff5b50b5a87986c23379df090e0a601280176827ab54f8f10a871c

Locking Script (ScriptPubKey) for Address C:
ASM: OP_DUP OP_HASH160 95006b58e08b0219f840003646f3c78b514cda4b OP_EQUALVERIFY OP_CHECKSIG
Hex: 76a91495006b58e08b0219f840003646f3c78b514cda4b88ac
Type: pubkeyhash

Transaction Size (B to C): 0.2197 kB

================================================================================

Legacy Address Transactions Completed Successfully
PS C:\Users\sruja\Desktop\scripting>
```

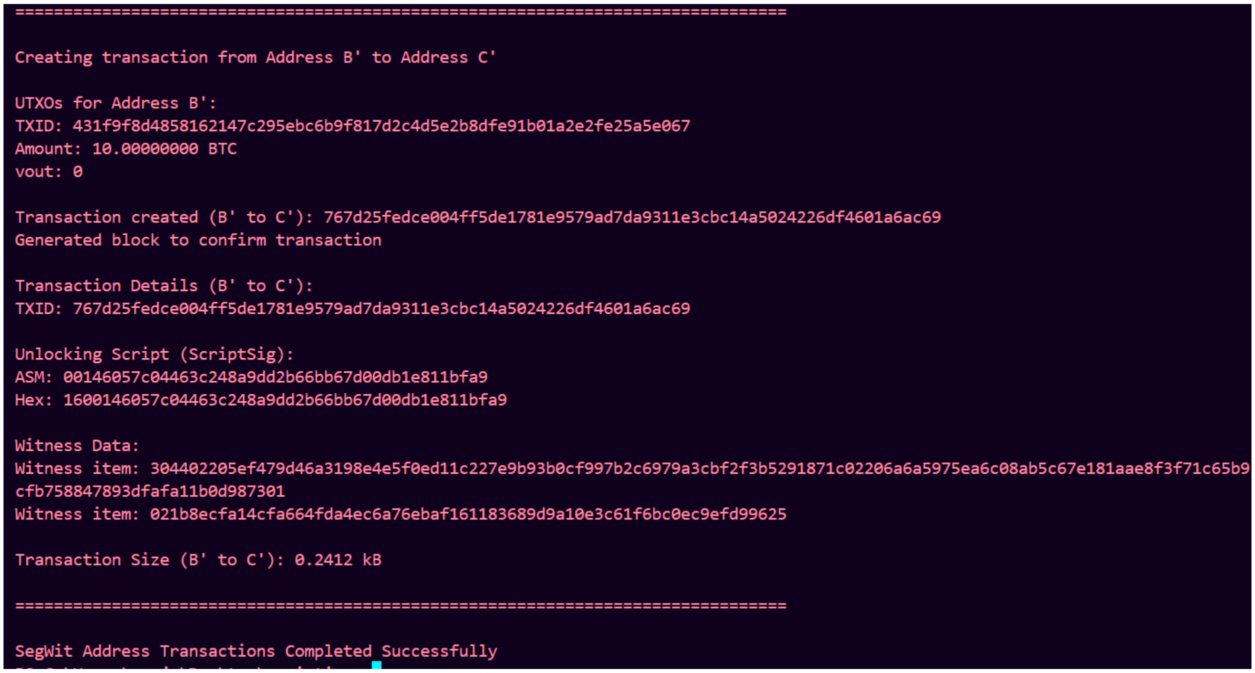
SegWit Transactions:

- **Transaction A′ → B′:**
  - **TXID:** *431f9f8d4858162147c295ebc6b9f817d2c4d5e2b8dfe91b01a2e2fe25a5e067*
  - **Locking Script (Address B′):**
    - **ASM:** *OP_HASH160 5bc1b0b13aaa727c58d3a9377d179f4f7e25920d OP_EQUAL*
    - **Hex:** a914214ae0c0b81b2df7e009892adfalec4707f0836087
    - **Type:** scripthash
- **Transaction B′ → C′:**
  - **TXID:** *767d25fedce004ff5de1781e9579ad7da9311e3cbc14a5024226df4601a6ac69*
  - **Unlocking Script (ScriptSig) and Witness Data:**
    - **ASM:** *00146057c04463c248a9dd2b66bb67d00db1e811bfa9*
    - **Hex:** *1600146057c04463c248a9dd2b66bb67d00db1e811bfa9*

        - **Witness Items:** *304402205ef479d46a3198e4e5f0ed11c227e9b93b8cf997b2c6979a3cbf2f3b5291871c02206a6a5975ea6c08ab5c67e181aae8f3f71c65b9*
    - **Locking Script (Address C′):**
        - **ASM:** *OP_HASH160 d668da3f0e4894b178263a939bd082fc0182db7b OP_EQUAL*
        - **Hex:** *a914d668da3f0e4894b178263a939bd082fc0182db7b87*
        - **Type:** *scripthash*
    - **Transaction Size:** *0.2412 kB*



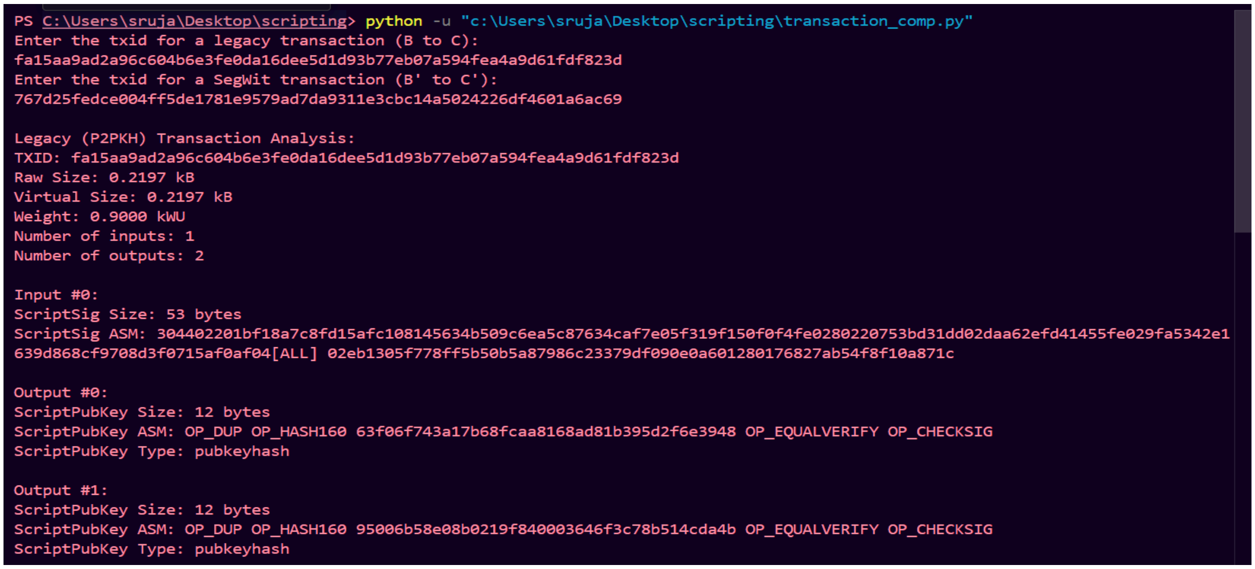
```
PS C:\Users\sruja\Desktop\scripting> python -u "c:\Users\sruja\Desktop\scripting\segwit.py"
Connected to Bitcoin Core (Regtest): regtest
Current block height: 103
Created new wallet: assignment_wallet_segwit
Address A' (P2SH-SegWit): 2N6mNyARnHFx8HA8ZKpkxxv1Lfycm8mq5Hi
Address B' (P2SH-SegWit): 2N1cPWa7wt9nU5Vr6YnNHSCYeSdBRvKuznM
Address C' (P2SH-SegWit): 2NCnvCcj9hz1rHCdhJ1J4ZX2sAvwuxUGvfj
Generated 101 blocks to address A'
Wallet balance: 50.00000000 BTC

================================================================================

Creating transaction from Address A' to Address B'
Transaction created: 431f9f8d4858162147c295ebc6b9f817d2c4d5e2b8dfe91b01a2e2fe25a5e067
Generated block to confirm transaction

Transaction Details:
TXID: 431f9f8d4858162147c295ebc6b9f817d2c4d5e2b8dfe91b01a2e2fe25a5e067
Amount: 10.0 BTC
Fee: -0.00001660 BTC

================================================================================
```



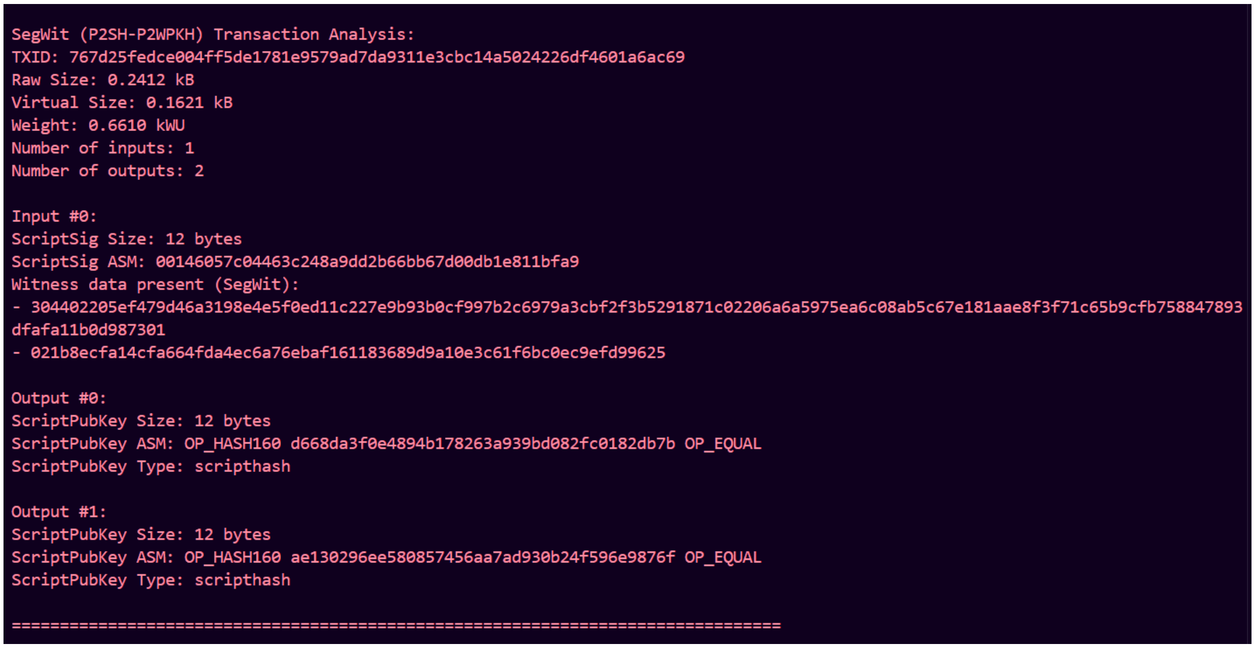
```
================================================================================

Creating transaction from Address B' to Address C'

UTXOs for Address B':
TXID: 431f9f8d4858162147c295ebc6b9f817d2c4d5e2b8dfe91b01a2e2fe25a5e067
Amount: 10.00000000 BTC
vout: 0

Transaction created (B' to C'): 767d25fedce004ff5de1781e9579ad7da9311e3cbc14a5024226df4601a6ac69
Generated block to confirm transaction

Transaction Details (B' to C'):
TXID: 767d25fedce004ff5de1781e9579ad7da9311e3cbc14a5024226df4601a6ac69

Unlocking Script (ScriptSig):
ASM: 00146057c04463c248a9dd2b66bb67d00db1e811bfa9
Hex: 1600146057c04463c248a9dd2b66bb67d00db1e811bfa9

Witness Data:
Witness item: 304402205ef479d46a3198e4e5f0ed11c227e9b93b0cf997b2c6979a3cbf2f3b5291871c02206a6a5975ea6c08ab5c67e181aae8f3f71c65b9
cfb758847893dfafa11b0d987301
Witness item: 021b8ecfa14cfa664fda4ec6a76ebaf161183689d9a10e3c61f6bc0ec9efd99625

Transaction Size (B' to C'): 0.2412 kB

================================================================================

SegWit Address Transactions Completed Successfully
```

Transaction Comparison:

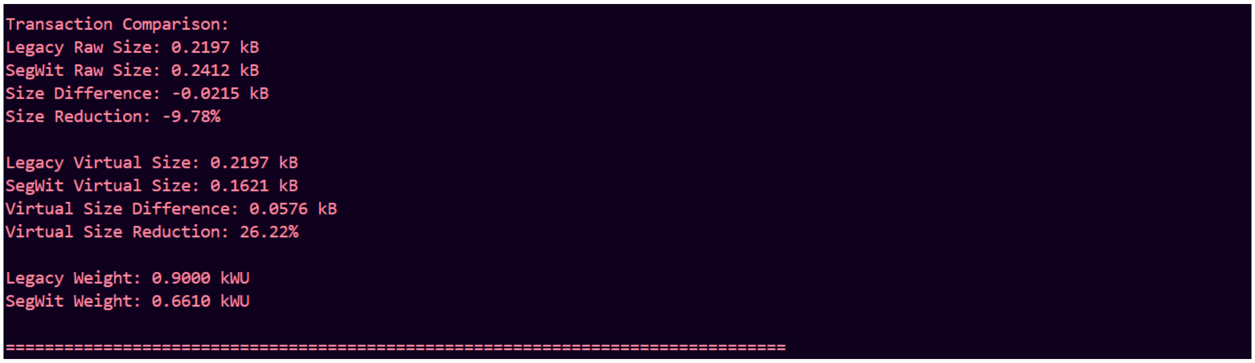
- **Legacy Transaction Metrics:**
    - Raw Size: *0.2197* kB
    - Virtual Size: *0.2197* kB
    - Weight: *0.9000* kWU
- **SegWit Transaction Metrics:**
    - Raw Size: *0.2412* kB
    - Virtual Size: *0.1621* kB
    - Weight: *0.6610* kWU
- **Comparison Summary:**
    - Size Reduction: Approximately *-9.78% and 26.22%* reduction in raw and virtual sizes respectively for SegWit transactions compared to legacy transactions.



```
PS C:\Users\sruja\Desktop\scripting> python -u "c:\Users\sruja\Desktop\scripting\transaction_comp.py"
Enter the txid for a legacy transaction (B to C):
fa15aa9ad2a96c604b6e3fe0da16dee5d1d93b77eb07a594fea4a9d61fdf823d
Enter the txid for a SegWit transaction (B' to C'):
767d25fedce004ff5de1781e9579ad7da9311e3cbc14a5024226df4601a6ac69

Legacy (P2PKH) Transaction Analysis:
TXID: fa15aa9ad2a96c604b6e3fe0da16dee5d1d93b77eb07a594fea4a9d61fdf823d
Raw Size: 0.2197 kB
Virtual Size: 0.2197 kB
Weight: 0.9000 kWU
Number of inputs: 1
Number of outputs: 2

Input #0:
ScriptSig Size: 53 bytes
ScriptSig ASM: 304402201bf18a7c8fd15afc108145634b509c6ea5c87634caf7e05f319f150f0f4fe0280220753bd31dd02daa62efd41455fe029fa5342e1
639d868cf9708d3f0715af0af04[ALL] 02eb1305f778ff5b50b5a87986c23379df090e0a601280176827ab54f8f10a871c

Output #0:
ScriptPubKey Size: 12 bytes
ScriptPubKey ASM: OP_DUP OP_HASH160 63f06f743a17b68fcaa8168ad81b395d2f6e3948 OP_EQUALVERIFY OP_CHECKSIG
ScriptPubKey Type: pubkeyhash

Output #1:
ScriptPubKey Size: 12 bytes
ScriptPubKey ASM: OP_DUP OP_HASH160 95006b58e08b0219f840003646f3c78b514cda4b OP_EQUALVERIFY OP_CHECKSIG
ScriptPubKey Type: pubkeyhash
```



```
SegWit (P2SH-P2WPKH) Transaction Analysis:
TXID: 767d25fedce004ff5de1781e9579ad7da9311e3cbc14a5024226df4601a6ac69
Raw Size: 0.2412 kB
Virtual Size: 0.1621 kB
Weight: 0.6610 kWU
Number of inputs: 1
Number of outputs: 2

Input #0:
ScriptSig Size: 12 bytes
ScriptSig ASM: 00146057c04463c248a9dd2b66bb67d00db1e811bfa9
Witness data present (SegWit):
- 304402205ef479d46a3198e4e5f0ed11c227e9b93b0cf997b2c6979a3cbf2f3b5291871c02206a6a5975ea6c08ab5c67e181aae8f3f71c65b9cfb758847893
dfafa11b0d987301
- 021b8ecfa14cfa664fda4ec6a76ebaf161183689d9a10e3c61f6bc0ec9efd99625

Output #0:
ScriptPubKey Size: 12 bytes
ScriptPubKey ASM: OP_HASH160 d668da3f0e4894b178263a939bd082fc0182db7b OP_EQUAL
ScriptPubKey Type: scripthash

Output #1:
ScriptPubKey Size: 12 bytes
ScriptPubKey ASM: OP_HASH160 ae130296ee580857456aa7ad930b24f596e9876f OP_EQUAL
ScriptPubKey Type: scripthash

================================================================================
```



```
Transaction Comparison:
Legacy Raw Size: 0.2197 kB
SegWit Raw Size: 0.2412 kB
Size Difference: -0.0215 kB
Size Reduction: -9.78%

Legacy Virtual Size: 0.2197 kB
SegWit Virtual Size: 0.1621 kB
Virtual Size Difference: 0.0576 kB
Virtual Size Reduction: 26.22%

Legacy Weight: 0.9000 kWU
SegWit Weight: 0.6610 kWU

================================================================================
```

6. Analysis and Discussion

- **Script Structures:**
  In legacy transactions, the unlocking and locking scripts are embedded directly in the transaction inputs and outputs. The challenge script (locking script) in the A→B transaction is used later as a reference when validating the unlocking script (ScriptSig) in the B→C transaction.

  In contrast, SegWit transactions separate signature data into the witness field. This results in smaller effective transaction sizes as the witness data is discounted during fee calculations. The witness data also improves the security and flexibility of transaction validation.

- **Transaction Size and Weight:**
  The analysis from `transaction_comp.py` clearly shows that the SegWit transactions have a lower raw size, virtual size, and overall weight compared to their legacy counterparts. This reduction in size translates to lower fees and better scalability, allowing more transactions to be included in each block.

- **Benefits of SegWit:**

  - **Reduced Transaction Size:** By moving signature data to the witness, transactions become smaller.
  - **Lower Fees:** The fee calculation based on virtual size rewards smaller transactions, reducing costs.
  - **Enhanced Scalability:** More transactions per block increase the network's throughput.
  - **Fix for Transaction Malleability:** SegWit's separation of signature data minimizes the risks associated with transaction malleability, paving the way for advanced solutions like the Lightning Network.
  - **Script Versioning:** The design allows future script upgrades without requiring hard forks.

---

7. Conclusion

This assignment provided a hands-on experience with Bitcoin transactions using both legacy (P2PKH) and SegWit (P2SH-P2WPKH) address formats. Through the development and analysis of Python scripts, we demonstrated the full workflow from wallet creation, address generation, transaction creation, decoding, and script analysis. The detailed transaction comparison reinforces the advantages of SegWit, particularly in reducing transaction size and fee costs, while also addressing security concerns like transaction malleability. Overall, the exercise deepened our understanding of Bitcoin's scripting mechanisms and the evolution of its transaction architecture.

---

8. Appendix

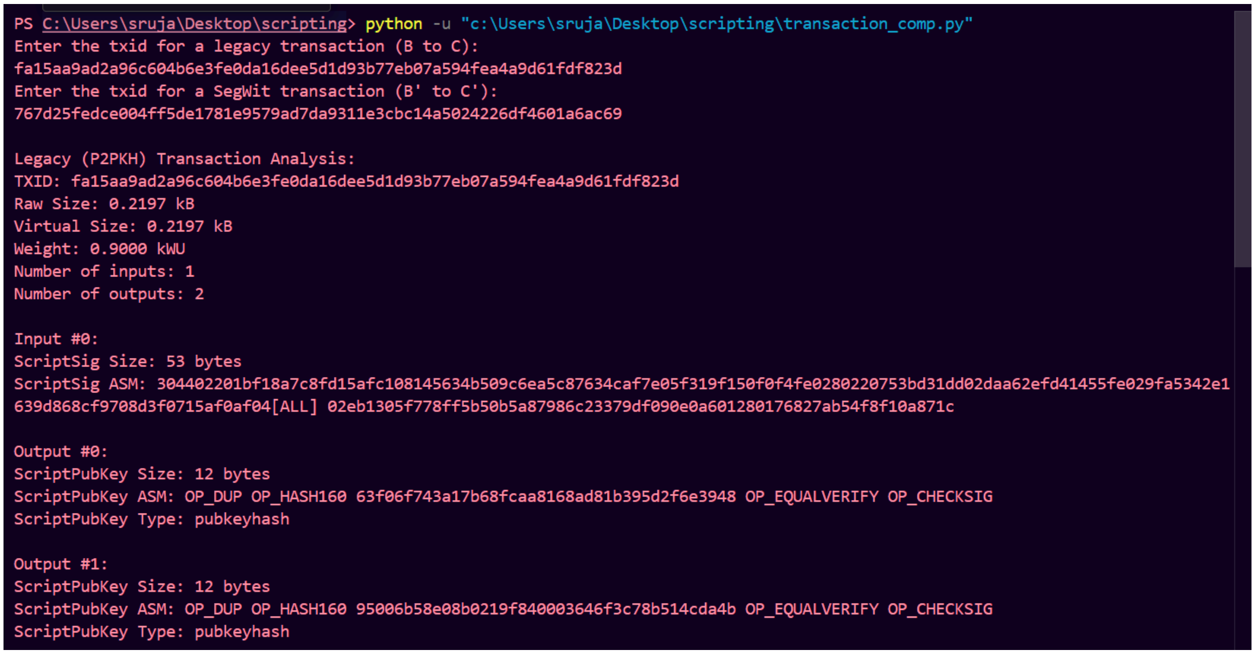
Code Overview

- **legacy.py:**
  Contains functions to connect to Bitcoin Core, manage wallets, generate legacy

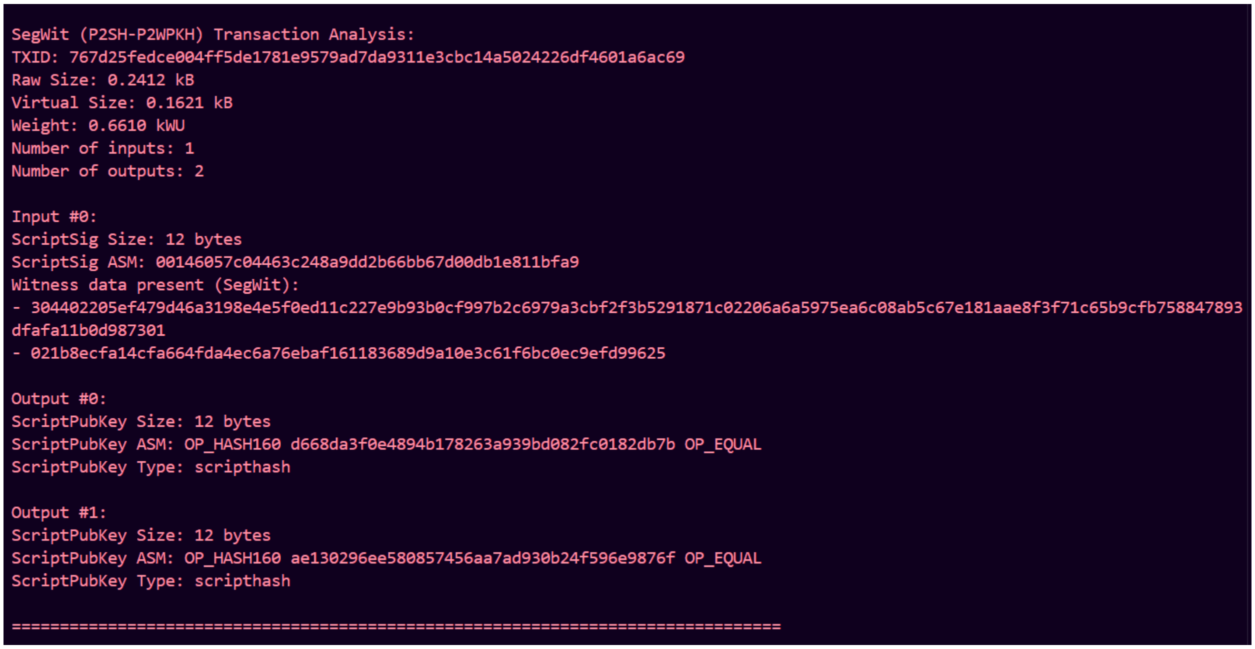
addresses, mine blocks for funding, create transactions, and decode transaction scripts.

- **segwit.py:**
 Implements the equivalent functionalities for P2SH-SegWit addresses, handling wallet management, transaction creation, decoding, and witness data extraction.

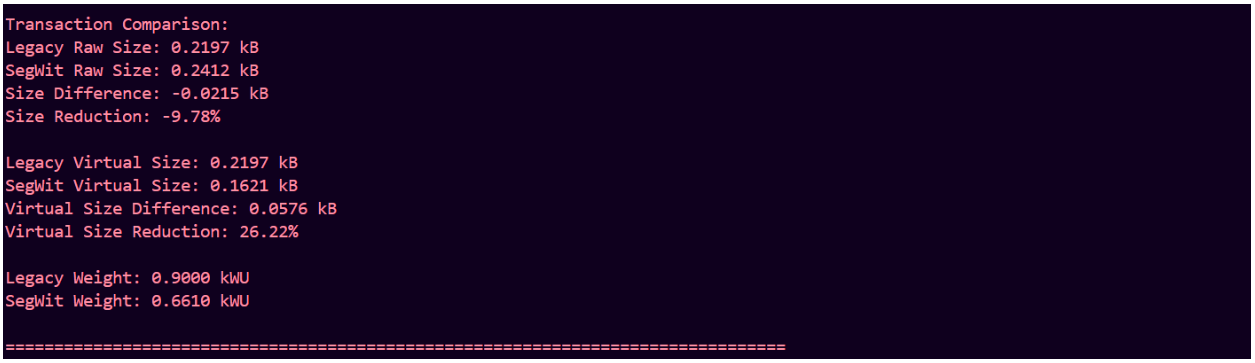
- **transaction_comp.py:**
 Provides tools for comparing transaction metrics such as size, virtual size, and weight between legacy and SegWit transactions, along with an explanation of the benefits of SegWit.



```
PS C:\Users\sruja\Desktop\scripting> python -u "c:\Users\sruja\Desktop\scripting\transaction_comp.py"
Enter the txid for a legacy transaction (B to C):
fa15aa9ad2a96c604b6e3fe0da16dee5d1d93b77eb07a594fea4a9d61fdf823d
Enter the txid for a SegWit transaction (B' to C'):
767d25fedce004ff5de1781e9579ad7da9311e3cbc14a5024226df4601a6ac69

Legacy (P2PKH) Transaction Analysis:
TXID: fa15aa9ad2a96c604b6e3fe0da16dee5d1d93b77eb07a594fea4a9d61fdf823d
Raw Size: 0.2197 kB
Virtual Size: 0.2197 kB
Weight: 0.9000 kWU
Number of inputs: 1
Number of outputs: 2

Input #0:
ScriptSig Size: 53 bytes
ScriptSig ASM: 304402201bf18a7c8fd15afc108145634b509c6ea5c87634caf7e05f319f150f0f4fe0280220753bd31dd02daa62efd41455fe029fa5342e1
639d868cf9708d3f0715af0af04[ALL] 02eb1305f778ff5b50b5a87986c23379df090e0a601280176827ab54f8f10a871c

Output #0:
ScriptPubKey Size: 12 bytes
ScriptPubKey ASM: OP_DUP OP_HASH160 63f06f743a17b68fcaa8168ad81b395d2f6e3948 OP_EQUALVERIFY OP_CHECKSIG
ScriptPubKey Type: pubkeyhash

Output #1:
ScriptPubKey Size: 12 bytes
ScriptPubKey ASM: OP_DUP OP_HASH160 95006b58e08b0219f840003646f3c78b514cda4b OP_EQUALVERIFY OP_CHECKSIG
ScriptPubKey Type: pubkeyhash
```



```
SegWit (P2SH-P2WPKH) Transaction Analysis:
TXID: 767d25fedce004ff5de1781e9579ad7da9311e3cbc14a5024226df4601a6ac69
Raw Size: 0.2412 kB
Virtual Size: 0.1621 kB
Weight: 0.6610 kWU
Number of inputs: 1
Number of outputs: 2

Input #0:
ScriptSig Size: 12 bytes
ScriptSig ASM: 00146057c04463c248a9dd2b66bb67d00db1e811bfa9
Witness data present (SegWit):
- 304402205ef479d46a3198e4e5f0ed11c227e9b93b0cf997b2c6979a3cbf2f3b5291871c02206a6a5975ea6c08ab5c67e181aae8f3f71c65b9cfb758847893
dfafa11b0d987301
- 021b8ecfa14cfa664fda4ec6a76ebaf161183689d9a10e3c61f6bc0ec9efd99625

Output #0:
ScriptPubKey Size: 12 bytes
ScriptPubKey ASM: OP_HASH160 d668da3f0e4894b178263a939bd082fc0182db7b OP_EQUAL
ScriptPubKey Type: scripthash

Output #1:
ScriptPubKey Size: 12 bytes
ScriptPubKey ASM: OP_HASH160 ae130296ee580857456aa7ad930b24f596e9876f OP_EQUAL
ScriptPubKey Type: scripthash

================================================================================
```



```
Transaction Comparison:
Legacy Raw Size: 0.2197 kB
SegWit Raw Size: 0.2412 kB
Size Difference: -0.0215 kB
Size Reduction: -9.78%

Legacy Virtual Size: 0.2197 kB
SegWit Virtual Size: 0.1621 kB
Virtual Size Difference: 0.0576 kB
Virtual Size Reduction: 26.22%

Legacy Weight: 0.9000 kWU
SegWit Weight: 0.6610 kWU

================================================================================
```

9.Debugger result

Debugging Report for Bitcoin Scripting Assignment

Introduction

This report summarizes the debugging process for both Legacy (P2PKH) and SegWit (P2SH-P2WPKH) transactions as part of the Bitcoin Scripting assignment. The debugging was performed using `btcdeb`, a Bitcoin script debugger, to validate and analyze the scripts involved in the transactions.

Legacy (P2PKH) Debugging

Script Execution:

1. **Initial Script Loading:**

- The script was loaded into `btcdeb` and validated as a valid script.

- The script included operations like `OP_DUP`, `OP_HASH160`, `OP_EQUALVERIFY`, and `OP_CHECKSIG`.

2. **Step-by-Step Execution:**

- The script execution began with pushing the signature and public key onto the stack.

- The `OP_DUP` operation duplicated the top stack item.

- The `OP_HASH160` operation hashed the public key.

- The script then compared the hashed public key with the provided hash using `OP_EQUALVERIFY`.

- Finally, `OP_CHECKSIG` was executed to validate the signature against the public key.

3. **Error Encountered:**

   - An error was encountered during the `OP_CHECKSIG` operation, indicating an issue with the signature validation.

Screenshots:

We have uploaded results in folder named as debugger_results in repository.

SegWit (P2SH-P2WPKH) Debugging

Script Execution:

1. **Initial Script Loading:**

   - The SegWit script was loaded into `btcdeb` and validated.

   - The script included operations like `OP_HASH160` and `OP_EQUAL`.

2. **Step-by-Step Execution:**

   - The script execution began with pushing the signature and public key onto the stack.

   - The `OP_HASH160` operation hashed the public key.

   - The script then compared the hashed public key with the provided hash using `OP_EQUAL`.

3. **Successful Execution:**

   - The script executed successfully without errors, validating the transaction.

Screenshots:

We have uploaded results in folder named as debugger_results in repository.

Conclusion

- **Legacy Transactions:** The debugging process highlighted an issue with the signature validation in the Legacy transaction script. This could be due to an incorrect signature or public key.

- **SegWit Transactions:** The SegWit transaction script executed successfully, demonstrating the efficiency and correctness of the SegWit script structure.

Recommendations

- For Legacy transactions, ensure that the signature and public key are correctly generated and match the expected values.

- Utilize SegWit transactions for their efficiency and smaller transaction size, as demonstrated by the successful debugging process.

This report provides a concise overview of the debugging process and findings for both Legacy and SegWit transactions, supported by detailed screenshots and step-by-step execution logs.