Bitcoin Scripting Assignment Report CS 216:

Introduction to Blockchain Assignment 2: Bitcoin Scripting

Team Name: Rafale

Team Members:

- Vasav Jain (230001081)
- Rudra Pratap Singh Jadon (230004043)
- Yash Vardhan Solanki (230005052)

Introduction

The objective of this assignment is to understand the process of creating and validating Bitcoin transactions using both Legacy (P2PKH) and SegWit (P2SH-P2WPKH) address formats. This report outlines the implementation details, transaction analysis, and comparison of transaction sizes between these formats.

Legacy Address Transactions (P2PKH)

- Workflow
  - **Wallet Setup**: Connected to bitcoind via RPC and created a new wallet.
  - **Address Generation**: Generated three legacy addresses (A, B, C).
  - **Funding Address A**: Sent Bitcoin to address A using `sendtoaddress`.
  - **Transaction A → B**:
    - Created a raw transaction from A to B.
    - Decoded the transaction and extracted `ScriptPubKey` for B.
    - Signed the transaction and broadcasted it.

```
task2praveshjain@Vasav-Jain Rafale_Task2_CS216 % cd part1
task2praveshjain@Vasav-Jain part1 % python3 run1.py

✅ Connected to bitcoind

✅ Wallet 'test_wallet' already loaded

Address A: mgGH2g6u6JdCcLxsef5yVAkRsCpJu6bAVi
Address B: mzterncNFFYWpSzrc9rb3zrSkadazSUD5x
Address C: mfpwnU9QYoSHQHkVgRGTbJQH2QVYVTSY89

✅ Funded Address A with 0.5 BTC. TxID: d2477b1212b6f75a5a88e747632bcd3a3748cad90c60a1c03f0adfa4c1965d52

✅ Transaction confirmed

✅ Raw Transaction Created

✅ Transaction Signed

✅ Transaction Broadcasted! TxID: 08f971388b7d45fcaba8879387d677b871b8cf6f90a05f7f3474227af6ff8c0c

✅ Decoded Transaction:
{'txid': '08f971388b7d45fcaba8879387d677b871b8cf6f90a05f7f3474227af6ff8c0c', 'hash': 'be66f061548f0bfb196a5bca9
034607002bd625b0e7eea2edf30a77bac14e976', 'version': 2, 'size': 228, 'vsize': 147, 'weight': 585, 'locktime': 0
, 'vin': [{'txid': '28f4f9035a7304bab758152384310bb71d2e0896f50df56d0ff4ec3d3116501a', 'vout': 0, 'scriptSig':
{'asm': '', 'hex': ''}, 'txinwitness': ['3044022074d6d38291a6ac1f0449cb1bd86536cfd818f0374d06e9233b74458f1043bf
e40220153302d1c805357f17563361d11fa3fb4d4a9abde9cad44e7e8ac5cc2a8d485e01', '02191f976271ffd2ac4d576ebfac821eda7
be31f0e63ea034bc2a00bdacd2f8046'], 'sequence': 4294967293}], 'vout': [{'value': Decimal('0.50000000'), 'n': 0,
'scriptPubKey': {'asm': 'OP_DUP OP_HASH160 d484fc8c50431a0fbc988f47a836eea78be722ec OP_EQUALVERIFY OP_CHECKSIG'
, 'desc': 'addr(mzterncNFFYWpSzrc9rb3zrSkadazSUD5x)#yj2cs870', 'hex': '76a914d484fc8c50431a0fbc988f47a836eea78b
e722ec88ac', 'address': 'mzterncNFFYWpSzrc9rb3zrSkadazSUD5x', 'type': 'pubkeyhash'}}, {'value': Decimal('49.499
99000'), 'n': 1, 'scriptPubKey': {'asm': 'OP_DUP OP_HASH160 08318681bf4f219407959fbc05b878bdf0115d53 OP_EQUALVE
RIFY OP_CHECKSIG', 'desc': 'addr(mgGH2g6u6JdCcLxsef5yVAkRsCpJu6bAVi)#7uyqyfet', 'hex': '76a91408318681bf4f21940
7959fbc05b878bdf0115d5388ac', 'address': 'mgGH2g6u6JdCcLxsef5yVAkRsCpJu6bAVi', 'type': 'pubkeyhash'}}]}

🔐 Locking Script for Address B:
  OP_DUP OP_HASH160 d484fc8c50431a0fbc988f47a836eea78be722ec OP_EQUALVERIFY OP_CHECKSIG

💰 Final Wallet Balance: 99.99996060 BTC

✅ Block mined: 6d1ce8283117659862aa01df3839e52c940943186c1722aaf5ec612d2aa9ade8

✅ Task Complete!
```

- **Transaction B → C**:
  - Used `listunspent` to obtain the txid from A to B.
  - Created and broadcasted a transaction from B to C.

```
task2praveshjain@Vasav-Jain part1 % python3 run2.py

🔎 Fetching UTXOs for Address B...
✅ UTXO found for Address B:
  Address: mzterncNFFYWpSzrc9rb3zrSkadazSUD5x
  TxID: 08f971388b7d45fcaba8879387d677b871b8cf6f90a05f7f3474227af6ff8c0c
  Amount: 0.50000000 BTC


🛠️ Creating Transaction from B to C...
✅ Raw Transaction Created: 02000000010c8cfff67a2274347f5fa0906fcfb871b877d6879387a8abfc457d8b3871f9080000000000fdffffff02
404b4c00000000001976a91403670fbf2ee614f2703f4ecc0e6220eeb786b47388ac58a1ae02000000001976a914d484fc8c50431a0fbc988f47a836ee
a78be722ec88ac00000000

✅ Transaction Signed: 02000000010c8cfff67a2274347f5fa0906fcfb871b877d6879387a8abfc457d8b3871f908000000006a47304402205cf69
7cd70808b0fef2a92251ed0a9aff6b90f245f15794394a350d500939623022025e98c265337e5bf669c03adfcdf7e41cfcb83e10f1245606ab8b8c43c0
45c01012103d3712f9e1f2fc188b81d88bece00d6135ab85dd5c4b50fb32e84dc2c0656004bfdffffff02404b4c00000000001976a91403670fbf2ee61
4f2703f4ecc0e6220eeb786b47388ac58a1ae02000000001976a914d484fc8c50431a0fbc988f47a836eea78be722ec88ac00000000

✅ Transaction Broadcasted! TxID: 45498715062637a105e0d2eddacc44bc716fe026c426134c58280cf53d777c5c


🔎 Decoding Transaction...
✅ Decoded Transaction: {'txid': '45498715062637a105e0d2eddacc44bc716fe026c426134c58280cf53d777c5c', 'hash': '454987150626
37a105e0d2eddacc44bc716fe026c426134c58280cf53d777c5c', 'version': 2, 'size': 225, 'vsize': 225, 'weight': 900, 'locktime':
 0, 'vin': [{'txid': '08f971388b7d45fcaba8879387d677b871b8cf6f90a05f7f3474227af6ff8c0c', 'vout': 0, 'scriptSig': {'asm': '
304402205cf697cd70808b0fef2a92251ed0a9aff6b90f245f15794394a350d500939623022025e98c265337e5bf669c03adfcdf7e41cfcb83e10f1245
606ab8b8c43c045c01[ALL] 03d3712f9e1f2fc188b81d88bece00d6135ab85dd5c4b50fb32e84dc2c0656004b', 'hex': '47304402205cf697cd708
08b0fef2a92251ed0a9aff6b90f245f15794394a350d500939623022025e98c265337e5bf669c03adfcdf7e41cfcb83e10f1245606ab8b8c43c045c010
12103d3712f9e1f2fc188b81d88bece00d6135ab85dd5c4b50fb32e84dc2c0656004b'}, 'sequence': 4294967293}], 'vout': [{'value': Deci
mal('0.05000000'), 'n': 0, 'scriptPubKey': {'asm': 'OP_DUP OP_HASH160 03670fbf2ee614f2703f4ecc0e6220eeb786b473 OP_EQUALVER
IFY OP_CHECKSIG', 'desc': 'addr(mfpwnU9QYoSHQHkVgRGTbJQH2QVYVTSY89)#rgaequ2x', 'hex': '76a91403670fbf2ee614f2703f4ecc0e622
0eeb786b47388ac', 'address': 'mfpwnU9QYoSHQHkVgRGTbJQH2QVYVTSY89', 'type': 'pubkeyhash'}}, {'value': Decimal('0.44999000')
, 'n': 1, 'scriptPubKey': {'asm': 'OP_DUP OP_HASH160 d484fc8c50431a0fbc988f47a836eea78be722ec OP_EQUALVERIFY OP_CHECKSIG',
 'desc': 'addr(mzterncNFFYWpSzrc9rb3zrSkadazSUD5x)#yj2cs870', 'hex': '76a914d484fc8c50431a0fbc988f47a836eea78be722ec88ac',
 'address': 'mzterncNFFYWpSzrc9rb3zrSkadazSUD5x', 'type': 'pubkeyhash'}}]}

🔒 ScriptSig (Unlocking Script): 304402205cf697cd70808b0fef2a92251ed0a9aff6b90f245f15794394a350d500939623022025e98c265337e
5bf669c03adfcdf7e41cfcb83e10f1245606ab8b8c43c045c01[ALL] 03d3712f9e1f2fc188b81d88bece00d6135ab85dd5c4b50fb32e84dc2c0656004
b
ScriptSig (Hex): 47304402205cf697cd70808b0fef2a92251ed0a9aff6b90f245f15794394a350d500939623022025e98c265337e5bf669c03adfcd
f7e41cfcb83e10f1245606ab8b8c43c045c01012103d3712f9e1f2fc188b81d88bece00d6135ab85dd5c4b50fb32e84dc2c0656004b

🔑 ScriptPubKey (Locking Script) for Address C: OP_DUP OP_HASH160 03670fbf2ee614f2703f4ecc0e6220eeb786b473 OP_EQUALVERIFY
OP_CHECKSIG
ScriptPubKey (Hex): 76a91403670fbf2ee614f2703f4ecc0e6220eeb786b47388ac

💰 Final Wallet Balance: 149.99995060 BTC

✅ Block mined: 1509470d2dd434b459cf38f2c2f768dccd0b4f42d5d4e3f3fa22c9deae2866c2

✅ Task Complete!
```

- **Decoded Scripts**
  - **ScriptPubKey (Locking Script) for Address B**:
    - OP_DUP OP_HASH160 d484fc8c50431a0fbc988f47a836eea78be722ec OP_EQUALVERIFY OP_CHECKSIG
  - **ScriptPubKey (Locking Script) for Address C**:
    - OP_DUP OP_HASH160 03670fbf2ee614f2703f4ecc0e6220eeb786b473 OP_EQUALVERIFY OP_CHECKSIG

- **Debugger Script(Legacy Transaction A->B and B->C)**

```
task2praveshjain@Vasav-Jain part1 % ssh -x guest@10.206.4.201
guest@10.206.4.201's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

12 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sun Mar 23 02:02:11 2025 from 10.18.3.240
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb -v -s "3044022074d6d38291a6ac1f0449cb1bd86536cfd
818f0374d06e9233b74458f1043bfe40220153302d1c805357f17563361d11fa3fb4d4a9abde9cad44e7e8ac5cc2a8d485e01 021
91f976271ffd2ac4d576ebfac821eda7be31f0e63ea034bc2a00bdacd2f8046" OP_DUP OP_HASH160 d484fc8c50431a0fbc988f
47a836eea78be722ec OP_EQUALVERIFY OP_CHECKSIG
btcdeb 5.0.24 -- type `btcdeb -h` for start up options
LOG: signing segwit taproot
notice: btcdeb has gotten quieter; use --verbose if necessary (this message is temporary)
valid script
1 op script loaded. type `help` for usage information
script  |                                       stack
--------+---------------------------------------
OP_DUP  |                                         ac
        |                                         88
        | d484fc8c50431a0fbc988f47a836eea78be722ec
        |                                         a9
#0000 OP_DUP
btcdeb> ^C
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb -v -s "304402205cf697cd70808b0fef2a92251ed0a9aff
6b90f245f15794394a350d500939623022025e98c265337e5bf669c03adfcdf7e41cfcb83e10f1245606ab8b8c43c045c01[ALL]
03d3712f9e1f2fc188b81d88bece00d6135ab85dd5c4b50fb32e84dc2c0656004b" OP_DUP OP_HASH160 03670fbf2ee614f2703
f4ecc0e6220eeb786b473 OP_EQUALVERIFY OP_CHECKSIG
btcdeb 5.0.24 -- type `btcdeb -h` for start up options
LOG: signing segwit taproot
notice: btcdeb has gotten quieter; use --verbose if necessary (this message is temporary)
valid script
1 op script loaded. type `help` for usage information
script  |                                       stack
--------+---------------------------------------
OP_DUP  |                                         ac
        |                                         88
        | 03670fbf2ee614f2703f4ecc0e6220eeb786b473
        |                                         a9
#0000 OP_DUP
btcdeb>
```

SegWit Address Transactions (P2SH-P2WPKH)

- **Workflow**
  - **Wallet Setup**: Created a new wallet and generated three SegWit addresses (A', B', C').
  - **Funding Address A'**: Sent Bitcoin to A' using `sendtoaddress`.
  - **Transaction A' → B'**:
    - Created a raw transaction and extracted the `ScriptPubKey`.
    - Signed and broadcasted the transaction.

- **Transaction B' → C'**:
  - Used `listunspent` to obtain the txid from A' to B'.
  - Created and broadcasted a transaction from B' to C'.

```
task2praveshjain@Vasav-Jain Rafale_Task2_CS216 % cd part2
task2praveshjain@Vasav-Jain part2 % py
thon3 run3.py

✅ Connected to bitcoind

✅ Wallet 'test_wallet' already loaded

Address A': 2N5xPDzgEJM7BG61omjFfB2ADbFR5Zaq3fP
Address B': 2MvFcTr2Pr9k6XMykHxoxGGDE4cMU7Jdf6o
Address C': 2MyKRYfr44zK2rpKuRhccNmkdRKhsWrPWt3

✅ Funded Address A' with 0.5 BTC. TxID: 8068b30a5407a4deaac75979e907a2d8e89717104b94ad3c277dd211f6244aae

✅ Transaction confirmed (Block mined: 6aca7a86e7ffbcc721346da8708f9e5b1efcfae2750162238177c57e4d169847)

✅ Raw Transaction Created

✅ Transaction Broadcasted! TxID: b5751e555781cfcc742aac92314b55cc20c3b323b08104e73673246bc45561ba

✅ Decoded Transaction:
{'txid': 'b5751e555781cfcc742aac92314b55cc20c3b323b08104e73673246bc45561ba', 'hash': '304358f1d18fb1a00ef3e74009741db7a2db12abf21ccbcdfc1c4c22a9eb6823', 'version':
 'size': 247, 'vsize': 166, 'weight': 661, 'locktime': 0, 'vin': [{'txid': '8068b30a5407a4deaac75979e907a2d8e89717104b94ad3c277dd211f6244aae', 'vout': 0, 'scriptSig
 {'asm': '0014061051df7961222037c360717bcf31cb73038d85', 'hex': '160014061051df7961222037c360717bcf31cb73038d85'}, 'txinwitness': ['304402201f181a169fbbbfcf4f2be01f
efaf57b1a5eaa7764567bd6b16c1adf9b25ca8022027bbd54187f401477fe591b3def364b6c8077a803fbeedb2c2d5262911190b0c01', '03a319431b891a609a10a94494d8d68ecdb1a95bd25681e29d2e
f57e6f59d572'], 'sequence': 4294967293}], 'vout': [{'value': Decimal('0.30000000'), 'n': 0, 'scriptPubKey': {'asm': 'OP_HASH160 20fb23828c764f7cdf32e5beb87ac8584fc6
2f OP_EQUAL', 'desc': 'addr(2MvFcTr2Pr9k6XMykHxoxGGDE4cMU7Jdf6o)#2yax9dr2', 'hex': 'a91420fb23828c764f7cdf32e5beb87ac8584fc6482f87', 'address': '2MvFcTr2Pr9k6XMykHx
GGDE4cMU7Jdf6o', 'type': 'scripthash'}}, {'value': Decimal('0.19999000'), 'n': 1, 'scriptPubKey': {'asm': 'OP_HASH160 8b6a4624c17160676821164868dbe7b315504c16 OP_EQ
L', 'desc': 'addr(2N5xPDzgEJM7BG61omjFfB2ADbFR5Zaq3fP)#veq3rl4e', 'hex': 'a9148b6a4624c17160676821164868dbe7b315504c1687', 'address': '2N5xPDzgEJM7BG61omjFfB2ADbFR5
q3fP', 'type': 'scripthash'}}]}

🔐 Locking Script for Address B':
  OP_HASH160 20fb23828c764f7cdf32e5beb87ac8584fc6482f OP_EQUAL

✅ Block mined: 62f10c4c2d4b362129b13bdf3f6afe07f5cc6e48f70b342269441870a17aba4a

✅ Raw Transaction Created

✅ Transaction Broadcasted! TxID: a556d7de85d92490247a2a5807f5006035a38c55347c40a0dc97f29ab4f499bf

✅ Decoded Transaction:
{'txid': 'a556d7de85d92490247a2a5807f5006035a38c55347c40a0dc97f29ab4f499bf', 'hash': 'dc977e1e5c899e6c8a5eadb3b42819079e21d7fcfb12135711f37c1c8bbb64da', 'version':
 'size': 247, 'vsize': 166, 'weight': 661, 'locktime': 0, 'vin': [{'txid': 'b5751e555781cfcc742aac92314b55cc20c3b323b08104e73673246bc45561ba', 'vout': 0, 'scriptSig
 {'asm': '0014c59f599ddf12eacc5cc848d4fc8dbd13a3f4670a', 'hex': '160014c59f599ddf12eacc5cc848d4fc8dbd13a3f4670a'}, 'txinwitness': ['30440220615a9cd70389708c8befb147
6911a4f1320a3e564e901d0427ceaca0fffab402207f883c67b509b3a2df0f11ef6f3a9574d7d32d66742b4553b6d4f5c523bb87b301', '0311d6929740a7c3cd723e0e86537a0476684e32d5e4aa2513a9
2c9395cdef21'], 'sequence': 4294967293}], 'vout': [{'value': Decimal('0.20000000'), 'n': 0, 'scriptPubKey': {'asm': 'OP_HASH160 429c11276daddd6299e7134815f8accf6576
bf OP_EQUAL', 'desc': 'addr(2MyKRYfr44zK2rpKuRhccNmkdRKhsWrPWt3)#qh6gw8py', 'hex': 'a914429c11276daddd6299e7134815f8accf6576c9bf87', 'address': '2MyKRYfr44zK2rpKuRh
NmkdRKhsWrPWt3', 'type': 'scripthash'}}, {'value': Decimal('0.09999000'), 'n': 1, 'scriptPubKey': {'asm': 'OP_HASH160 20fb23828c764f7cdf32e5beb87ac8584fc6482f OP_EQ
L', 'desc': 'addr(2MvFcTr2Pr9k6XMykHxoxGGDE4cMU7Jdf6o)#2yax9dr2', 'hex': 'a91420fb23828c764f7cdf32e5beb87ac8584fc6482f87', 'address': '2MvFcTr2Pr9k6XMykHxoxGGDE4cMU
df6o', 'type': 'scripthash'}}]}

🔒 ScriptSig (Unlocking Script): 0014c59f599ddf12eacc5cc848d4fc8dbd13a3f4670a
ScriptSig (Hex): 160014c59f599ddf12eacc5cc848d4fc8dbd13a3f4670a

🔑 ScriptPubKey (Locking Script) for Address C': OP_HASH160 429c11276daddd6299e7134815f8accf6576c9bf OP_EQUAL
ScriptPubKey (Hex): a914429c11276daddd6299e7134815f8accf6576c9bf87

💰 Final Wallet Balance: 299.99990200 BTC

✅ Block mined: 1a8a6fb1495d07c7107fe5afd629eaea1c2001aedeb605958faa01e94c3fbe1d

✅ Task Complete!
```

- **Decoded Scripts**
  - **ScriptPubKey (Locking Script) for Address B'**:

    OP_HASH160 20fb23828c764f7cdf32e5beb87ac8584fc6482f OP_EQUAL

- **ScriptPubKey (Locking Script) for Address C'**:

  OP_HASH160 429c11276daddd6299e7134815f8accf6576c9bf OP_EQUAL

- **Debugger Script(Legacy Transaction A->B and B->C)**

```
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb -v -s "304402201f181a169fbbbfcf4f2be01f
dbefaf57b1a5eaa7764567bd6b16c1adf9b25ca8022027bbd54187f401477fe591b3def364b6c8077a803fbeedb2c2d5
262911190b0c01 03a319431b891a609a10a94494d8d68ecdb1a95bd25681e29d2e5cf57e6f59d572" OP_HASH160 20
fb23828c764f7cdf32e5beb87ac8584fc6482f OP_EQUAL
btcdeb 5.0.24 -- type `btcdeb -h` for start up options
LOG: signing segwit taproot
notice: btcdeb has gotten quieter; use --verbose if necessary (this message is temporary)
valid script
1 op script loaded. type `help` for usage information
script     |                                   stack
-----------+-----------------------------------------
OP_HASH160 |                                      87
           | 20fb23828c764f7cdf32e5beb87ac8584fc6482f
#0000 OP_HASH160
btcdeb> ^C
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb -v -s "30440220615a9cd70389708c8befb147
8e6911a4f1320a3e564e901d0427ceaca0fffab402207f883c67b509b3a2df0f11ef6f3a9574d7d32d66742b4553b6d4
f5c523bb87b301 0311d6929740a7c3cd723e0e86537a0476684e32d5e4aa2513a9912c9395cdef21" OP_HASH160 42
9c11276daddd6299e7134815f8accf6576c9bf OP_EQUAL
btcdeb 5.0.24 -- type `btcdeb -h` for start up options
LOG: signing segwit taproot
notice: btcdeb has gotten quieter; use --verbose if necessary (this message is temporary)
valid script
1 op script loaded. type `help` for usage information
script     |                                   stack
-----------+-----------------------------------------
OP_HASH160 |                                      87
           | 429c11276daddd6299e7134815f8accf6576c9bf
#0000 OP_HASH160
btcdeb>
```

Analysis and Comparison

- **Transaction Size Comparison**

Transaction Type **(For A->B)**	Size (Bytes)	Virtual Size (vsize)	Weight
P2PKH (Legacy)	247	147	585
P2SH-P2WPKH (SegWit)	228	166	661

Transaction Type **(For B->C)**	Size (Bytes)	Virtual Size (vsize)	Weight
P2PKH (Legacy)	247	225	900
P2SH-P2WPKH (SegWit)	225	166	661

- **Script Structure Comparison**

Feature	P2PKH (Legacy)	P2SH-P2WPKH (SegWit)
Locking Script	OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	OP_0 <PubKeyHash>
Unlocking Script	<Signature> <Public Key>	<Signature> <Public Key> (Stored in Witness)
Script Size	Larger due to scriptSig inclusion	Smaller due to witness segregation

Why SegWit Transactions Are Smaller & Their Benefits

- **Separate Data:** SegWit separates witness data (signatures) from base transaction data.
- **Discount Applied:** Witness data gets a 75% discount in weight, reducing the effective (virtual) size.

- **Network Benefits:** This results in lower fees and more transactions per block, enhancing scalability.
- **Increased Block Capacity**: Allows more transactions per block, improving efficiency.

Workflow and Transaction Analysis

- **Transaction IDs and Flow**
  - **A to B Transaction**:
    - TXID:b5751e555781cfcc742aac92314b55cc20c3b323b08104e73673246bc45561ba
    - Output used as input for transaction B to C.
  - **B to C Transaction**:
    - TXID:a556d7de85d92490247a2a5807f5006035a38c55347c40a0dc97f29ab4f499bf
    - Used the unspent output from A to B.

- **Challenge-Response Script Analysis**
  - **P2PKH Challenge Script (Locking Script for B):**

    OP_DUP OP_HASH160 03670fbf2ee614f2703f4ecc0e6220eeb786b473 OP_EQUALVERIFY OP_CHECKSIG

  - **P2PKH Response Script (Unlocking Script for B → C Transaction):**

    304402205cf697cd70808b0fef2a92251ed0a9aff6b90f245f15794394a350d500939623022025e98c265337e5bf669c03adfcdf7e41cfcb83e10f1245606ab8b8c43c045c01[ALL] 03d3712f9e1f2fc188b81d88bece00d6135ab85dd5c4b50fb32e84dc2c0656004b

  - **P2PKH Challenge Script (Locking Script for C):**

    OP_DUP OP_HASH160 03670fbf2ee614f2703f4ecc0e6220eeb786b473 OP_EQUALVERIFY OP_CHECKSIG

- **SegWit Challenge Script (Locking Script for B')**:

  OP_HASH160 429c11276daddd6299e7134815f8accf6576c9bf OP_EQUAL

- **SegWit Response Script (Unlocking Script for B' → C' Transaction):**

  <0014c59f599ddf12eacc5cc848d4fc8dbd13a3f4670a><160014c59f599ddf12eacc5cc848d4fc8dbd13a3f4670a>

- **SegWit Challenge Script (Locking Script for C')**:

  OP_HASH160 429c11276daddd6299e7134815f8accf6576c9bf OP_EQUAL