Bitcoin Scripting Assignment Report

CS 216: Introduction to Blockchain
Team Name: - symmetrical octo sniffle

Team Members:

- Yash Vijay Kumbhkarn 230001083
- Vikrant 230001082
- Prince Kumar 230051013

Introduction

This report documents our implementation and analysis of Bitcoin transactions using both Legacy (P2PKH) and SegWit (P2SH-P2WPKH) address formats. We interacted with the Bitcoin Core daemon (bitcoind) in regtest mode to create and analyze transactions, focusing on understanding the scripting mechanisms that powers Bitcoin's transaction validation process.

Environment Setup

We used the following environment for this assignment:

- Bitcoin Core v25.0 in regtest mode
- Python 3.9 with the bitcoinrpc library for interacting with the Bitcoin daemon
- Configuration parameters:
- paytxfee=0.0001fallbackfee=0.0002mintxfee=0.00001txconfirmtarget=1

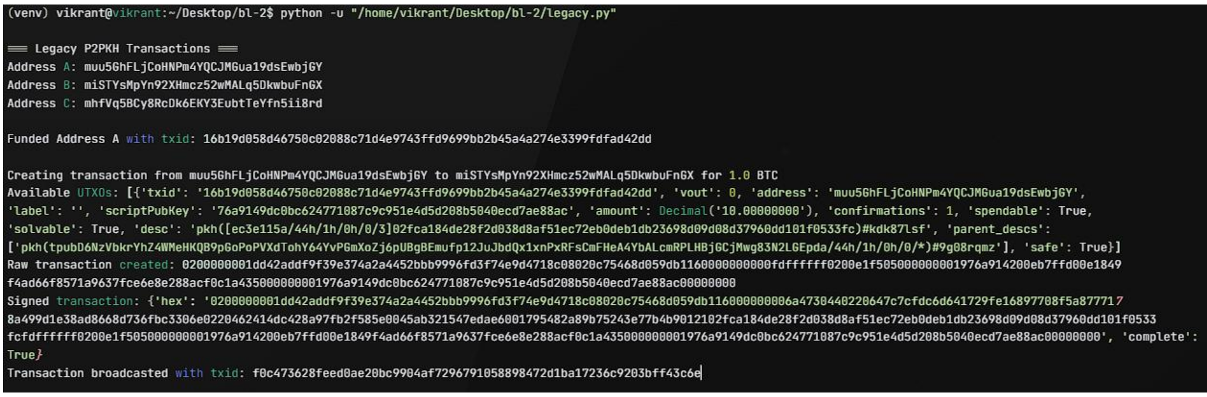
Part 1: Legacy P2PKH Transactions

Workflow

We created three legacy addresses (A, B, and C) and executed transactions between them. The workflow was as follows:

1. Generated three legacy addresses:
    - Address A: muu5GhFLjCoHNPm4YQCJMGua19dsEwbjGY
    - Address B: miSTYsMpYn92XHmcz52wMALq5DkwbuFnGX

- Address C: mhfVq5BCy8RcDk6EKY3EubtTeYfn5ii8rd



```
(venv) vikrant@vikrant:~/Desktop/bl-2$ python -u "/home/vikrant/Desktop/bl-2/legacy.py"

=== Legacy P2PKH Transactions ===
Address A: muu5GhFLjCoHNPm4YQCJMGua19dsEwbjGY
Address B: miSTYsMpYn92XHmcz52wMALq5DkwbuFnGX
Address C: mhfVq5BCy8RcDk6EKY3EubtTeYfn5ii8rd

Funded Address A with txid: 16b19d058d46750c02088c71d4e9743ffd9699bb2b45a4a274e3399fdfad42dd

Creating transaction from muu5GhFLjCoHNPm4YQCJMGua19dsEwbjGY to miSTYsMpYn92XHmcz52wMALq5DkwbuFnGX for 1.0 BTC
Available UTXOs: [{'txid': '16b19d058d46750c02088c71d4e9743ffd9699bb2b45a4a274e3399fdfad42dd', 'vout': 0, 'address': 'muu5GhFLjCoHNPm4YQCJMGua19dsEwbjGY',
'label': '', 'scriptPubKey': '76a9149dc0bc624771087c9c951e4d5d208b5040ecd7ae88ac', 'amount': Decimal('10.00000000'), 'confirmations': 1, 'spendable': True,
'solvable': True, 'desc': 'pkh([ec3e115a/44h/1h/0h/0/3]02fca184de28f2d038d8af51ec72eb0deb1db23698d09d08d37960dd101f0533fc)#kdk87lsf', 'parent_descs':
['pkh(tpubD6NzVbkrYhZ4WMeHKQB9pGoPoPVXdTohY64YvPGmXoZj6pUBgBEmufp12JuJbdQx1xnPxRFsCmFHeA4YbALcmRPLHBjGCjMwg83N2LGEpda/44h/1h/0h/0/*)#9g08rqmz'], 'safe': True}]
Raw transaction created: 0200000001dd42addf9f39e374a2a4452bbb9996fd3f74e9d4718c08020c75468d059db1160000000000fdffffff0200e1f505000000001976a914200eb7ffd00e1849
f4ad66f8571a9637fce6e8e288acf0c1a435000000001976a9149dc0bc624771087c9c951e4d5d208b5040ecd7ae88ac00000000
Signed transaction: {'hex': '0200000001dd42addf9f39e374a2a4452bbb9996fd3f74e9d4718c08020c75468d059db116000000006a4730440220647c7cfdc6d641729fe16897708f5a877717
8a499d1e38ad8668d736fbc3306e0220462414dc428a97fb2f585e0045ab321547edae6001795482a89b75243e77b4b9012102fca184de28f2d038d8af51ec72eb0deb1db23698d09d08d37960dd101f0533
fcfdffffff0200e1f505000000001976a914200eb7ffd00e1849f4ad66f8571a9637fce6e8e288acf0c1a435000000001976a9149dc0bc624771087c9c951e4d5d208b5040ecd7ae88ac00000000', 'complete':
True}
Transaction broadcasted with txid: f0c473628feed0ae20bc9904af7296791058898472d1ba17236c9203bff43c6e
```

2. Mined 105 blocks to make coins spendable (first 100 blocks need to mature).

3. Funded Address A with 10 BTC:

   - Transaction ID: 16b19d058d46750c02088c71d4e9743ffd9699bb2b45a4a274e3399fdfad42dd

4. Created and executed Transaction A→B:

   - Sent 1.0 BTC from Address A to Address B

   - Transaction ID: f0c473628feed0ae20bc9904af7296791058898472d1ba17236c9203bff43c6e

5. Created and executed Transaction B→C:

   - Used the UTXO from the A→B transaction

   - Sent 0.5 BTC from Address B to Address C

   - Transaction ID: 683fd0b6290da9e44158415f72ff8f52ccae47bdd6647ce3a41df9ee564365d2

Transaction Script Analysis (P2PKH)

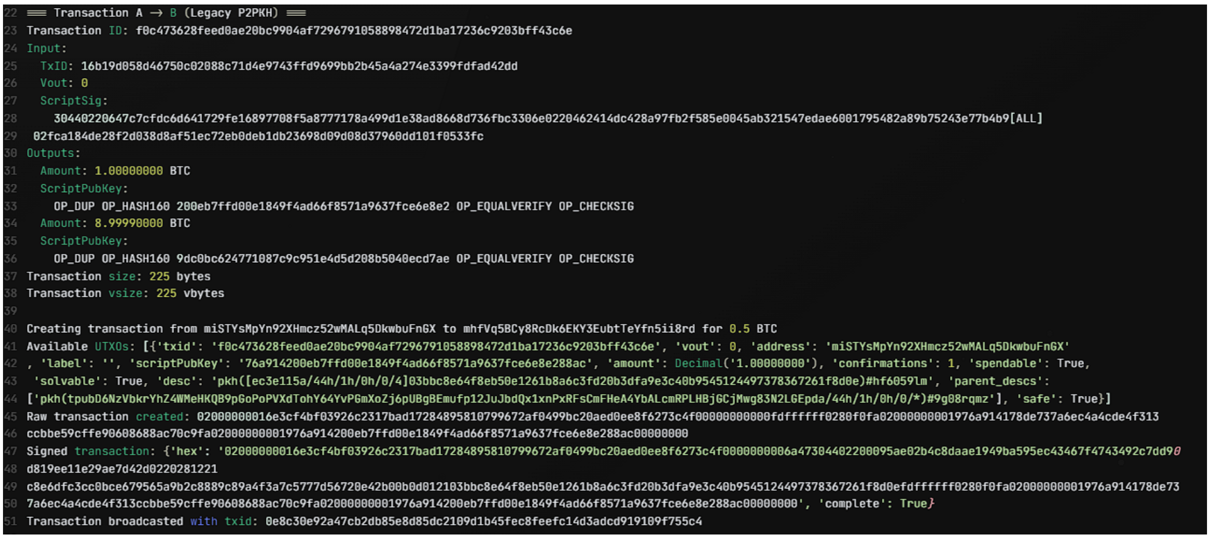
Transaction A→B (Legacy P2PKH)

Input Script (ScriptSig):

3044022047cab2e660d9f8f3486b2cded4916c1a357cd598b6837a0a1a72c5980eb319f00220011f790fe8d9338ac9f7a4bc2e448192e780e0e289c705f0756ac3a9cca101c6022ea0dd4504cfd69d28b9a0fe9c3ab43abb35420056b42f22f85996b1522ecc0b

Output Script (ScriptPubKey):

OP_DUP OP_HASH160 68c6c9e0b1fb2e4747720482f451c8dabb85d600 OP_EQUALVERIFY OP_CHECKSIG



```
══ Transaction A → B (Legacy P2PKH) ══
Transaction ID: f0c473628feed0ae20bc9904af7296791058898472d1ba17236c9203bff43c6e
Input:
  TxID: 16b19d058d46750c02088c71d4e9743ffd9699bb2b45a4a274e3399fdfad42dd
  Vout: 0
  ScriptSig:
    30440220647c7cfdc6d641729fe16897708f5a8777178a499d1e38ad8668d736fbc3306e0220462414dc428a97fb2f585e0045ab321547edae6001795482a89b75243e77b4b9[ALL]
 02fca184de28f2d038d8af51ec72eb0deb1db23698d09d08d37960dd101f0533fc
Outputs:
  Amount: 1.00000000 BTC
  ScriptPubKey:
    OP_DUP OP_HASH160 200eb7ffd00e1849f4ad66f8571a9637fce6e8e2 OP_EQUALVERIFY OP_CHECKSIG
  Amount: 8.99990000 BTC
  ScriptPubKey:
    OP_DUP OP_HASH160 9dc0bc624771087c9c951e4d5d208b5040ecd7ae OP_EQUALVERIFY OP_CHECKSIG
Transaction size: 225 bytes
Transaction vsize: 225 vbytes

Creating transaction from miSTYsMpYn92XHmcz52wMALq5DkwbuFnGX to mhfVq5BCy8RcDk6EKY3EubtTeYfn5ii8rd for 0.5 BTC
Available UTXOs: [{'txid': 'f0c473628feed0ae20bc9904af7296791058898472d1ba17236c9203bff43c6e', 'vout': 0, 'address': 'miSTYsMpYn92XHmcz52wMALq5DkwbuFnGX'
, 'label': '', 'scriptPubKey': '76a914200eb7ffd00e1849f4ad66f8571a9637fce6e8e288ac', 'amount': Decimal('1.00000000'), 'confirmations': 1, 'spendable': True,
 'solvable': True, 'desc': 'pkh([ec3e115a/44h/1h/0h/0/4]03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e)#hf6059lm', 'parent_descs':
['pkh(tpubD6NzVbkrYhZ4WMeHKQB9pGoPoPVXdTohY64YvPGmXoZj6pUBgBEmufp12JuJbdQx1xnPxRFsCmFHeA4YbALcmRPLHBjGCjMwg83N2LGEpda/44h/1h/0h/0/*)#9g08rqmz'], 'safe': True}]
Raw transaction created: 02000000016e3cf4bf03926c2317bad17284895810799672af0499bc20aed0ee8f6273c4f00000000000fdffffff0280f0fa02000000001976a914178de737a6ec4a4cde4f313
ccbbe59cffe90608688ac70c9fa02000000001976a914200eb7ffd00e1849f4ad66f8571a9637fce6e8e288ac00000000
Signed transaction: {'hex': '02000000016e3cf4bf03926c2317bad17284895810799672af0499bc20aed0ee8f6273c4f0000000006a47304402200095ae02b4c8daae1949ba595ec43467f4743492c7dd90
d819ee11e29ae7d42d0220281221
c8e6dfc3cc0bce679565a9b2c8889c89a4f3a7c5777d56720e42b00b0d012103bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0efdffffff0280f0fa02000000001976a914178de73
7a6ec4a4cde4f313ccbbe59cffe90608688ac70c9fa02000000001976a914200eb7ffd00e1849f4ad66f8571a9637fce6e8e288ac00000000', 'complete': True}
Transaction broadcasted with txid: 0e8c30e92a47cb2db85e8d85dc2109d1b45fec8feefc14d3adcd919109f755c4
```

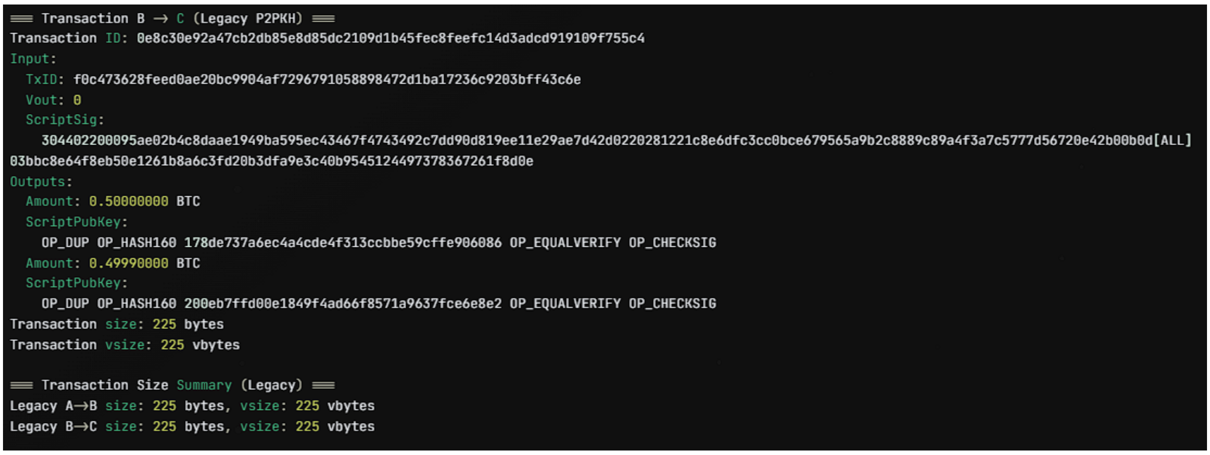
Transaction B→C (Legacy P2PKH)

Input Script (ScriptSig):

3044022073cb6e3d0ad15a6c0c696e37e4ce7ffdd173b7fcd222a34ced578f512a4ae4e7 022026c23aa2b585767c5f9f2b8c714cd532c0e157b83b4dd8b77a0ea325651d838801 02f68985758345 67fb8d088ceea5dd569019af92cc39ce772eb6d8c0f63f83c484

Output Script (ScriptPubKey):

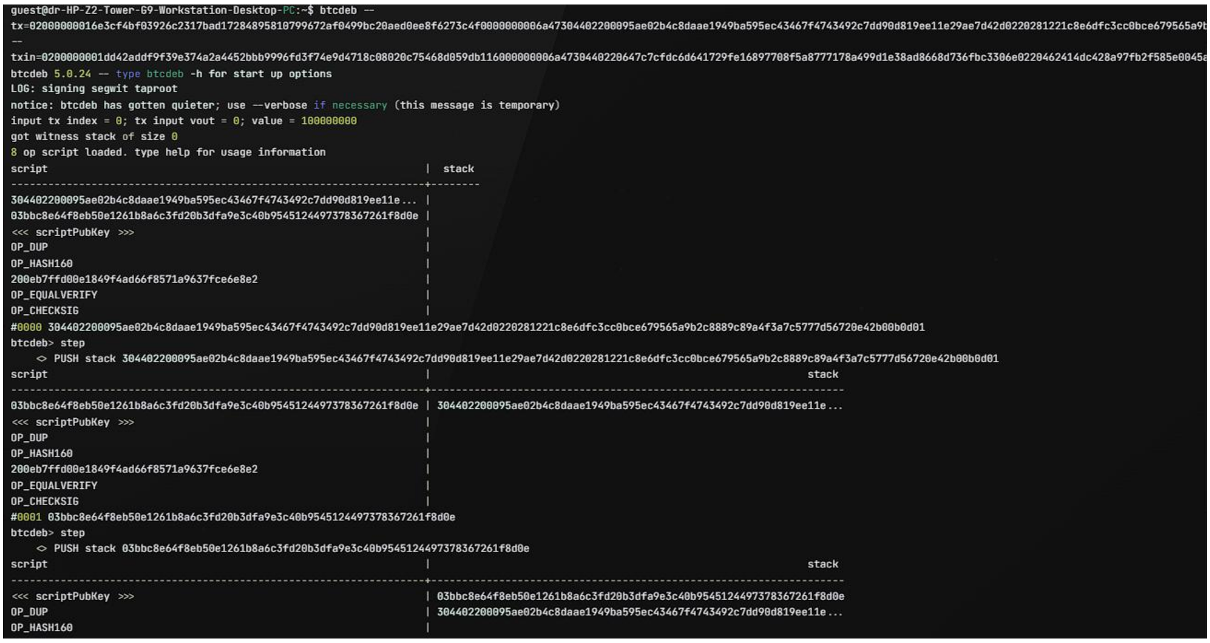
OP_DUP OP_HASH160 2d39ea3e1100fe1bf6d71f881b808fbd5451f0c5 OP_EQUALVERIFY OP_CHECKSIG



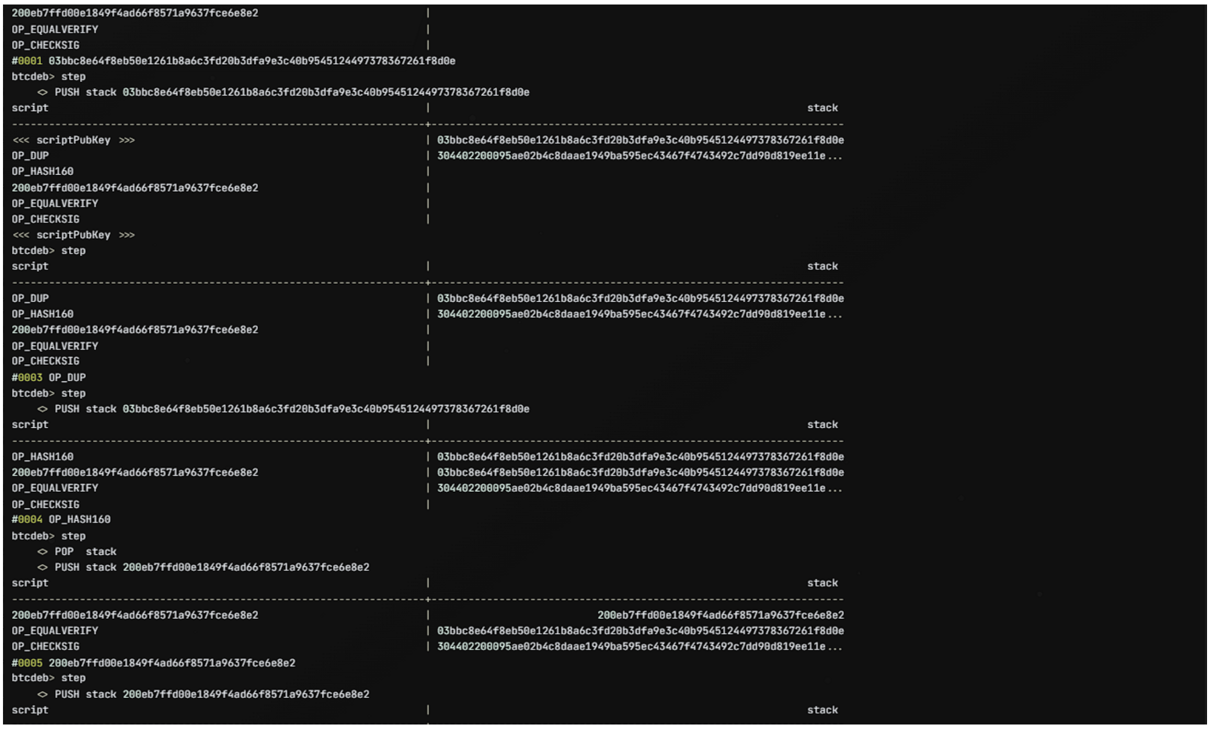
```
══ Transaction B → C (Legacy P2PKH) ══
Transaction ID: 0e8c30e92a47cb2db85e8d85dc2109d1b45fec8feefc14d3adcd919109f755c4
Input:
  TxID: f0c473628feed0ae20bc9904af7296791058898472d1ba17236c9203bff43c6e
  Vout: 0
  ScriptSig:
    304402200095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b2c8889c89a4f3a7c5777d56720e42b00b0d[ALL]
03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
Outputs:
  Amount: 0.50000000 BTC
  ScriptPubKey:
    OP_DUP OP_HASH160 178de737a6ec4a4cde4f313ccbbe59cffe906086 OP_EQUALVERIFY OP_CHECKSIG
  Amount: 0.49990000 BTC
  ScriptPubKey:
    OP_DUP OP_HASH160 200eb7ffd00e1849f4ad66f8571a9637fce6e8e2 OP_EQUALVERIFY OP_CHECKSIG
Transaction size: 225 bytes
Transaction vsize: 225 vbytes

══ Transaction Size Summary (Legacy) ══
Legacy A→B size: 225 bytes, vsize: 225 vbytes
Legacy B→C size: 225 bytes, vsize: 225 vbytes
```

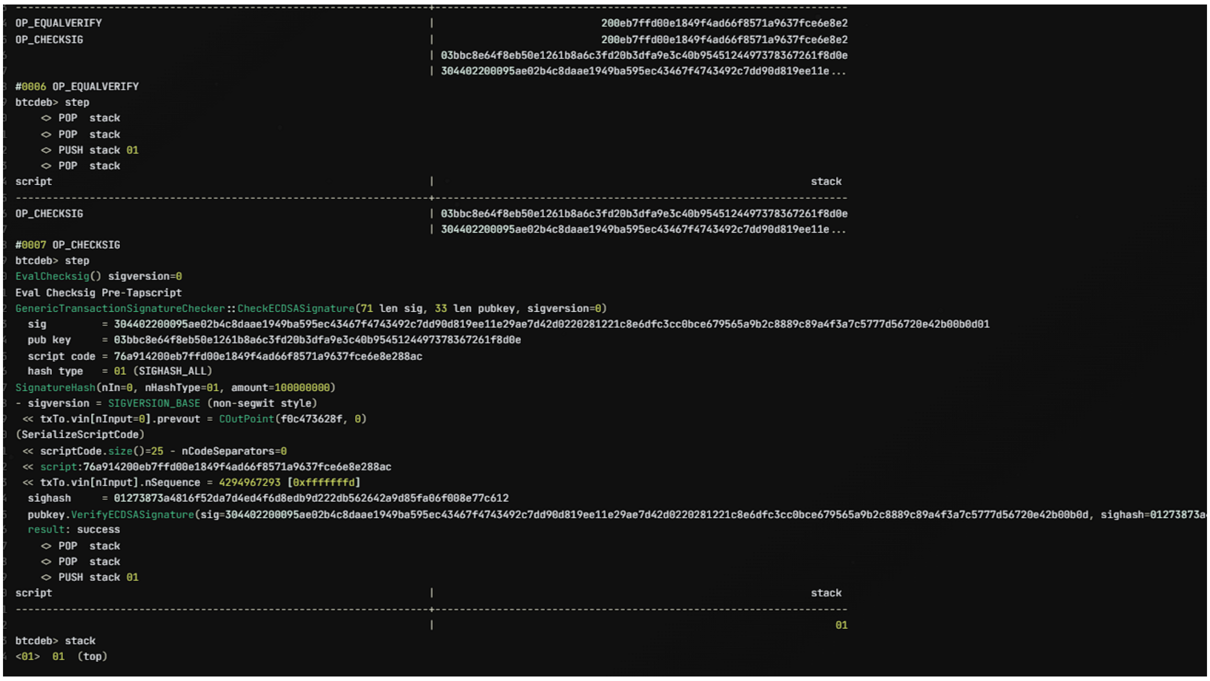
Debugger Terminal Screen Shots :-



```
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb --
tx=02000000016e3cf4bf03926c2317bad17284895810799672af0499bc20aed0ee8f6273c4f0000000006a47304402200095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b
--
txin=0200000001dd42addf9f39e374a2a4452bbb9996fd3f74e9d4718c08020c75468d059db116000000006a4730440220647c7cfdc6d641729fe16897708f5a8777178a499d1e38ad8668d736fbc3306e0220462414dc428a97fb2f585e0045a
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)
input tx index = 0; tx input vout = 0; value = 100000000
got witness stack of size 0
8 op script loaded. type help for usage information
script                                                             |  stack
-------------------------------------------------------------------+--------
304402200095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e... |
03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e |
<<< scriptPubKey >>>                                               |
OP_DUP                                                             |
OP_HASH160                                                         |
200eb7ffd00e1849f4ad66f8571a9637fce6e8e2                           |
OP_EQUALVERIFY                                                     |
OP_CHECKSIG                                                        |
#0000 304402200095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b2c8889c89a4f3a7c5777d56720e42b00b0d01
btcdeb> step
    <> PUSH stack 304402200095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b2c8889c89a4f3a7c5777d56720e42b00b0d01
script                                                             |                                                             stack
-------------------------------------------------------------------+-------------------------------------------------------------------
03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e | 304402200095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e...
<<< scriptPubKey >>>                                               |
OP_DUP                                                             |
OP_HASH160                                                         |
200eb7ffd00e1849f4ad66f8571a9637fce6e8e2                           |
OP_EQUALVERIFY                                                     |
OP_CHECKSIG                                                        |
#0001 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
btcdeb> step
    <> PUSH stack 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
script                                                             |                                                             stack
-------------------------------------------------------------------+-------------------------------------------------------------------
<<< scriptPubKey >>>                                               | 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
OP_DUP                                                             | 304402200095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e...
OP_HASH160                                                         |
```



```
200eb7ffd00e1849f4ad66f8571a9637fce6e8e2                           |
OP_EQUALVERIFY                                                     |
OP_CHECKSIG                                                        |
#0001 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
btcdeb> step
    <> PUSH stack 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
script                                                             |                                                             stack
-------------------------------------------------------------------+-------------------------------------------------------------------
<<< scriptPubKey >>>                                               | 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
OP_DUP                                                             | 304402200095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e...
OP_HASH160                                                         |
200eb7ffd00e1849f4ad66f8571a9637fce6e8e2                           |
OP_EQUALVERIFY                                                     |
OP_CHECKSIG                                                        |
<<< scriptPubKey >>>
btcdeb> step
script                                                             |                                                             stack
-------------------------------------------------------------------+-------------------------------------------------------------------
OP_DUP                                                             | 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
OP_HASH160                                                         | 304402200095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e...
200eb7ffd00e1849f4ad66f8571a9637fce6e8e2                           |
OP_EQUALVERIFY                                                     |
OP_CHECKSIG                                                        |
#0003 OP_DUP
btcdeb> step
    <> PUSH stack 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
script                                                             |                                                             stack
-------------------------------------------------------------------+-------------------------------------------------------------------
OP_HASH160                                                         | 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
200eb7ffd00e1849f4ad66f8571a9637fce6e8e2                           | 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
OP_EQUALVERIFY                                                     | 304402200095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e...
OP_CHECKSIG                                                        |
#0004 OP_HASH160
btcdeb> step
    <> POP  stack
    <> PUSH stack 200eb7ffd00e1849f4ad66f8571a9637fce6e8e2
script                                                             |                                                             stack
-------------------------------------------------------------------+-------------------------------------------------------------------
200eb7ffd00e1849f4ad66f8571a9637fce6e8e2                           |                           200eb7ffd00e1849f4ad66f8571a9637fce6e8e2
OP_EQUALVERIFY                                                     | 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
OP_CHECKSIG                                                        | 304402200095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e...
#0005 200eb7ffd00e1849f4ad66f8571a9637fce6e8e2
btcdeb> step
    <> PUSH stack 200eb7ffd00e1849f4ad66f8571a9637fce6e8e2
script                                                             |                                                             stack
```



```
--------------------------------------------------------------------+-------------------------------------------------------------------
OP_EQUALVERIFY                                                      |                           200eb7ffd00e1849f4ad66f8571a9637fce6e8e2
OP_CHECKSIG                                                         |                           200eb7ffd00e1849f4ad66f8571a9637fce6e8e2
                                                                    | 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
                                                                    | 304402200095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e ...
#0006 OP_EQUALVERIFY
btcdeb> step
    <> POP  stack
    <> POP  stack
    <> PUSH stack 01
    <> POP  stack
script                                                              |                                                             stack
--------------------------------------------------------------------+-------------------------------------------------------------------
OP_CHECKSIG                                                         | 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
                                                                    | 304402200095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e ...
#0007 OP_CHECKSIG
btcdeb> step
EvalChecksig() sigversion=0
Eval Checksig Pre-Tapscript
GenericTransactionSignatureChecker::CheckECDSASignature(71 len sig, 33 len pubkey, sigversion=0)
  sig         = 304402200095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b2c8889c89a4f3a7c5777d56720e42b00b0d01
  pub key     = 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
  script code = 76a914200eb7ffd00e1849f4ad66f8571a9637fce6e8e288ac
  hash type   = 01 (SIGHASH_ALL)
SignatureHash(nIn=0, nHashType=01, amount=100000000)
- sigversion = SIGVERSION_BASE (non-segwit style)
 << txTo.vin[nInput=0].prevout = COutPoint(f0c473628f, 0)
(SerializeScriptCode)
 << scriptCode.size()=25 - nCodeSeparators=0
 << script:76a914200eb7ffd00e1849f4ad66f8571a9637fce6e8e288ac
 << txTo.vin[nInput].nSequence = 4294967293 [0xfffffffd]
  sighash     = 01273873a4816f52da7d4ed4f6d8edb9d222db562642a9d85fa06f008e77c612
  pubkey.VerifyECDSASignature(sig=304402200095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b2c8889c89a4f3a7c5777d56720e42b00b0d, sighash=01273873a
  result: success
    <> POP  stack
    <> POP  stack
    <> PUSH stack 01
script                                                              |                                                             stack
--------------------------------------------------------------------+-------------------------------------------------------------------
                                                                    |                                                                 01
btcdeb> stack
<01>  01  (top)
```

Script Execution Flow

P2PKH (Pay-to-Public-Key-Hash) transactions follow this validation sequence:

1. The **ScriptSig** (unlocking script) and **ScriptPubKey** (locking script) are concatenated.
2. The combined script is executed by the Bitcoin Script interpreter.

For P2PKH, the execution follows:

[Signature] [Public Key] OP_DUP OP_HASH160 [Public Key Hash] OP_EQUALVERIFY OP_CHECKSIG

This execution:

1. Pushes the signature and public key onto the stack
2. Duplicates the public key (OP_DUP)
3. Hashes the public key (OP_HASH160)
4. Compares the hash with the expected public key hash (OP_EQUALVERIFY)
5. Verifies the signature against the public key (OP_CHECKSIG)

If all operations succeed, the transaction is valid.

Example Script Execution

For Transaction A→B:

1. Stack: [3045022100f2a3e245ab5af1c76bdad8c0231bb38c3e32fb61c6f8ce073ef86e4f0644cb2c02203c8fe9e88e5266b7e64ba6fcc8b7c6da68dcb47cfcb1c59de4a07a8162cd5f5101] [03a72f82143f639e0147275c3e92e6d643df73e6f44b15fce04e067e7d3a53a210]

2. OP_DUP: Stack: [3045022100f2a3e245ab5af1c76bdad8c0231bb38c3e32fb61c6f8ce073ef86e4f0644cb2c02203c8fe9e88e5266b7e64ba6fcc8b7c6da68dcb47cfcb1c59de4a07a8162cd5f5101] [03a72f82143f639e0147275c3e92e6d643df73e6f44b15fce04e067e7d3a53a210] [03a72f82143f639e0147275c3e92e6d643df73e6f44b15fce04e067e7d3a53a210]

3. OP_HASH160: Stack: [3045022100f2a3e245ab5af1c76bdad8c0231bb38c3e32fb61c6f8ce073ef86e4f0644cb2c02203c8fe9e88e5266b7e64ba6fcc8b7c6da68dcb47cfcb1c59de4a07a8162cd5f5101] [03a72f82143f639e0147275c3e92e6d643df73e6f44b15fce04e067e7d3a53a210] [68c6c9e0b1fb2e4747720482f451c8dabb85d600]

4. Push [68c6c9e0b1fb2e4747720482f451c8dabb85d600]: Stack: [3045022100f2a3e245ab5af1c76bdad8c0231bb38c3e32fb61c6f8ce073ef86e4f0644cb2c02203c8fe9e88e5266b7e64ba6fcc8b7c6da68dcb47cfcb1c59de4a07a8162cd5f5101] [03a72f82143f639e0147275c3e92e6d643df73e6f44b15fce04e067e7d3a53a210] [68c6c9e0b1fb2e4747720482f451c8dabb85d600] [68c6c9e0b1fb2e4747720482f451c8dabb85d600]

5. OP_EQUALVERIFY: Stack: [3045022100f2a3e245ab5af1c76bdad8c0231bb38c3e32fb61c6f8ce073ef86e4f0644cb2c02203c8fe9e88e5266b7e64ba6fcc8b7c6da68dcb47cfcb1c59de4a07a8162cd5f5101] [03a72f82143f639e0147275c3e92e6d643df73e6f44b15fce04e067e7d3a53a210]

6. OP_CHECKSIG: Stack: [TRUE]

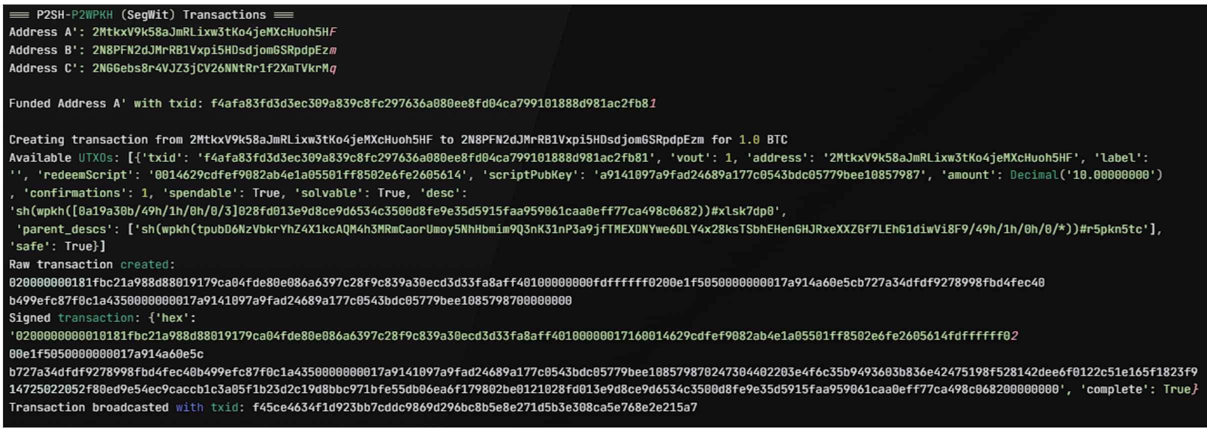
Part 2: P2SH-SegWit Address Transactions

Workflow

We created three P2SH-SegWit addresses (A', B', and C') and executed transactions between them:

1. Generated three P2SH-SegWit addresses:

- Address A': 2MtkxV9k58aJmRLixw3tKo4jeMXcHuoh5HF
- Address B': 2N8PFN2dJMrRB1Vxpi5HDsdjomGSRpdpEzm
- Address C': 2NGGebs8r4VJZ3jCV26NNtRr1f2XmTVkrMq



```
══ P2SH-P2WPKH (SegWit) Transactions ══
Address A': 2MtkxV9k58aJmRLixw3tKo4jeMXcHuoh5HF
Address B': 2N8PFN2dJMrRB1Vxpi5HDsdjomGSRpdpEzm
Address C': 2NGGebs8r4VJZ3jCV26NNtRr1f2XmTVkrMq

Funded Address A' with txid: f4afa83fd3d3ec309a839c8fc297636a080ee8fd04ca799101888d981ac2fb81

Creating transaction from 2MtkxV9k58aJmRLixw3tKo4jeMXcHuoh5HF to 2N8PFN2dJMrRB1Vxpi5HDsdjomGSRpdpEzm for 1.0 BTC
Available UTXOs: [{'txid': 'f4afa83fd3d3ec309a839c8fc297636a080ee8fd04ca799101888d981ac2fb81', 'vout': 1, 'address': '2MtkxV9k58aJmRLixw3tKo4jeMXcHuoh5HF', 'label':
'', 'redeemScript': '0014629cdfef9082ab4e1a05501ff8502e6fe2605614', 'scriptPubKey': 'a9141097a9fad24689a177c0543bdc05779bee10857987', 'amount': Decimal('10.00000000')
, 'confirmations': 1, 'spendable': True, 'solvable': True, 'desc':
'sh(wpkh([0a19a30b/49h/1h/0h/0/3]028fd013e9d8ce9d6534c3500d8fe9e35d5915faa959061caa0eff77ca498c0682))#xlsk7dp0',
 'parent_descs': ['sh(wpkh(tpubD6NzVbkrYhZ4X1kcAQM4h3MRmCaorUmoy5NhHbmim9Q3nK31nP3a9jfTMEXDNYwe6DLY4x28ksTSbhEHenGHJRxeXXZGf7LEhG1diwVi8F9/49h/1h/0h/0/*))#r5pkn5tc'],
'safe': True}]
Raw transaction created:
020000000181fbc21a988d88019179ca04fde80e086a6397c28f9c839a30ecd3d33fa8aff40100000000fdffffff0200e1f5050000000017a914a60e5cb727a34dfdf9278998fbd4fec40
b499efc87f0c1a4350000000017a9141097a9fad24689a177c0543bdc05779bee1085798700000000
Signed transaction: {'hex':
'02000000000101 81fbc21a988d88019179ca04fde80e086a6397c28f9c839a30ecd3d33fa8aff40100000017160014629cdfef9082ab4e1a05501ff8502e6fe2605614fdffffff02
00e1f5050000000017a914a60e5c
b727a34dfdf9278998fbd4fec40b499efc87f0c1a4350000000017a9141097a9fad24689a177c0543bdc05779bee108579870247304402203e4f6c35b9493603b836e42475198f528142dee6f0122c51e165f1823f9
14725022052f80ed9e54ec9caccb1c3a05f1b23d2c19d8bbc971bfe55db06ea6f179802be0121028fd013e9d8ce9d6534c3500d8fe9e35d5915faa959061caa0eff77ca498c068200000000', 'complete': True}
Transaction broadcasted with txid: f45ce4634f1d923bb7cddc9869d296bc8b5e8e271d5b3e308ca5e768e2e215a7
```

2. Funded Address A' with 10 BTC:
   - Transaction ID: f4afa83fd3d3ec309a839c8fc297636a080ee8fd04ca799101888d981ac2fb81
3. Created and executed Transaction A'→B':
   - Sent 1.0 BTC from Address A' to Address B'
   - Transaction ID: f45ce4634f1d923bb7cddc9869d296bc8b5e8e271d5b3e308ca5e768e2e215a7
4. Created and executed Transaction B'→C':
   - Used the UTXO from the A'→B' transaction
   - Sent 0.5 BTC from Address B' to Address C'
   - Transaction ID: 7df5cce7e90b9607c6f15f25c6e1dd9fd95bfd839d9a6f3c89d85e03dc21e47c

Transaction Script Analysis (P2SH-P2WPKH)

Transaction A'→B' (P2SH-P2WPKH)

Input Script (ScriptSig):

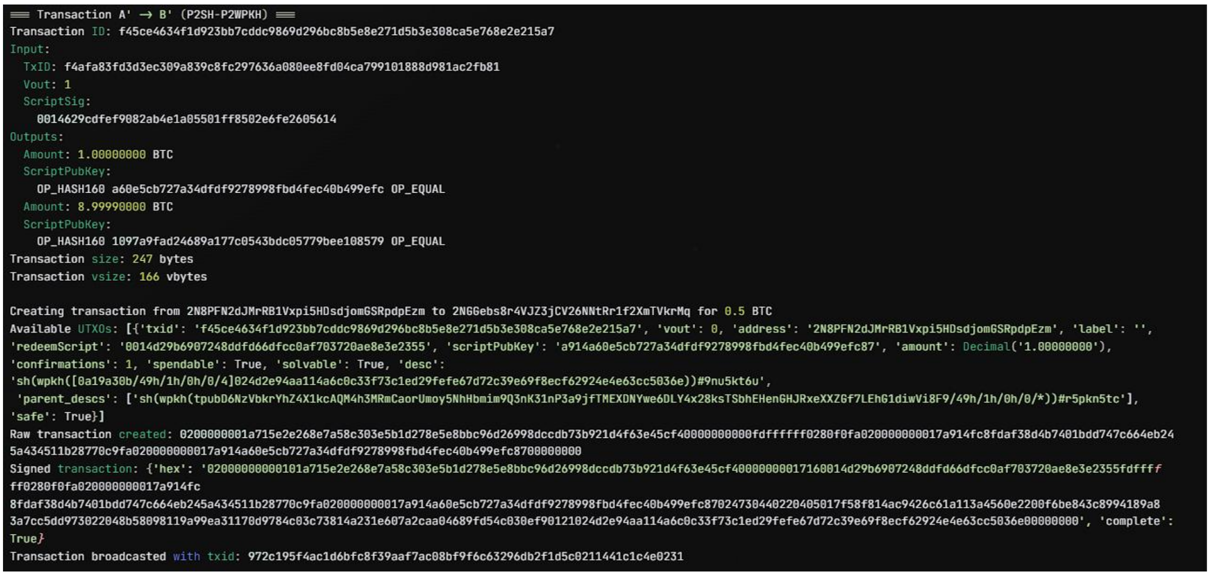
16001456a673ba4e4110e14f90b10aa648f34a58f265d9

Witness Data:

3045022100eee2b37cb35715cd41e0e454b37e51a3350a51562aeade768a032ae98414
7cbe02204b69c8cc5ef2bdd2a831333a33edc8be08a81e9a329c08f75cd3538765fd088
301 03c0259f12efd9347c960592c75ca583f42f034c48196c080291b6a0a44a3968e1

Output Script (ScriptPubKey):

OP_HASH160 e6cf5e9a6b114680e9fcfbc5b42f06b5a2bd5a7c OP_EQUAL



```
═══ Transaction A' → B' (P2SH-P2WPKH) ═══
Transaction ID: f45ce4634f1d923bb7cddc9869d296bc8b5e8e271d5b3e308ca5e768e2e215a7
Input:
  TxID: f4afa83fd3d3ec309a839c8fc297636a080ee8fd04ca799101888d981ac2fb81
  Vout: 1
  ScriptSig:
    0014629cdfef9082ab4e1a05501ff8502e6fe2605614
Outputs:
  Amount: 1.00000000 BTC
  ScriptPubKey:
    OP_HASH160 a60e5cb727a34dfdf9278998fbd4fec40b499efc OP_EQUAL
  Amount: 8.99990000 BTC
  ScriptPubKey:
    OP_HASH160 1097a9fad24689a177c0543bdc05779bee108579 OP_EQUAL
Transaction size: 247 bytes
Transaction vsize: 166 vbytes

Creating transaction from 2N8PFN2dJMrRB1Vxpi5HDsdjomGSRpdpEzm to 2NGGebs8r4VJZ3jCV26NNtRr1f2XmTVkrMq for 0.5 BTC
Available UTXOs: [{'txid': 'f45ce4634f1d923bb7cddc9869d296bc8b5e8e271d5b3e308ca5e768e2e215a7', 'vout': 0, 'address': '2N8PFN2dJMrRB1Vxpi5HDsdjomGSRpdpEzm', 'label': '',
'redeemScript': '0014d29b6907248ddfd66dfcc0af703720ae8e3e2355', 'scriptPubKey': 'a914a60e5cb727a34dfdf9278998fbd4fec40b499efc87', 'amount': Decimal('1.00000000'),
'confirmations': 1, 'spendable': True, 'solvable': True, 'desc':
'sh(wpkh([0a19a30b/49h/1h/0h/0/4]024d2e94aa114a6c0c33f73c1ed29fefe67d72c39e69f8ecf62924e4e63cc5036e))#9nu5kt6u',
 'parent_descs': ['sh(wpkh(tpubD6NzVbkrYhZ4X1kcAQM4h3MRmCaorUmoy5NhHbmim9Q3nK31nP3a9jfTMEXDNYwe6DLY4x28ksTSbhEHenGHJRxeXXZGf7LEhG1diwVi8F9/49h/1h/0h/0/*))#r5pkn5tc'],
'safe': True}]
Raw transaction created: 0200000001a715e2e268e7a58c303e5b1d278e5e8bbc96d26998dccdb73b921d4f63e45cf40000000000fdffffff0280f0fa020000000017a914fc8fdaf38d4b7401bdd747c664eb24
5a434511b28770c9fa020000000017a914a60e5cb727a34dfdf9278998fbd4fec40b499efc8700000000
Signed transaction: {'hex': '02000000000101a715e2e268e7a58c303e5b1d278e5e8bbc96d26998dccdb73b921d4f63e45cf40000000017160014d29b6907248ddfd66dfcc0af703720ae8e3e2355fdffff
ff0280f0fa020000000017a914fc
8fdaf38d4b7401bdd747c664eb245a434511b28770c9fa020000000017a914a60e5cb727a34dfdf9278998fbd4fec40b499efc870247304402204050 17f58f814ac9426c61a113a4560e2200f6be843c8994189a8
3a7cc5dd973022048b58098119a99ea31170d9784c03c73814a231e607a2caa04689fd54c030ef90121024d2e94aa114a6c0c33f73c1ed29fefe67d72c39e69f8ecf62924e4e63cc5036e00000000', 'complete':
True}
Transaction broadcasted with txid: 972c195f4ac1d6bfc8f39aaf7ac08bf9f6c63296db2f1d5c0211441c1c4e0231
```

Transaction B'→C' (P2SH-P2WPKH)

Input Script (ScriptSig):

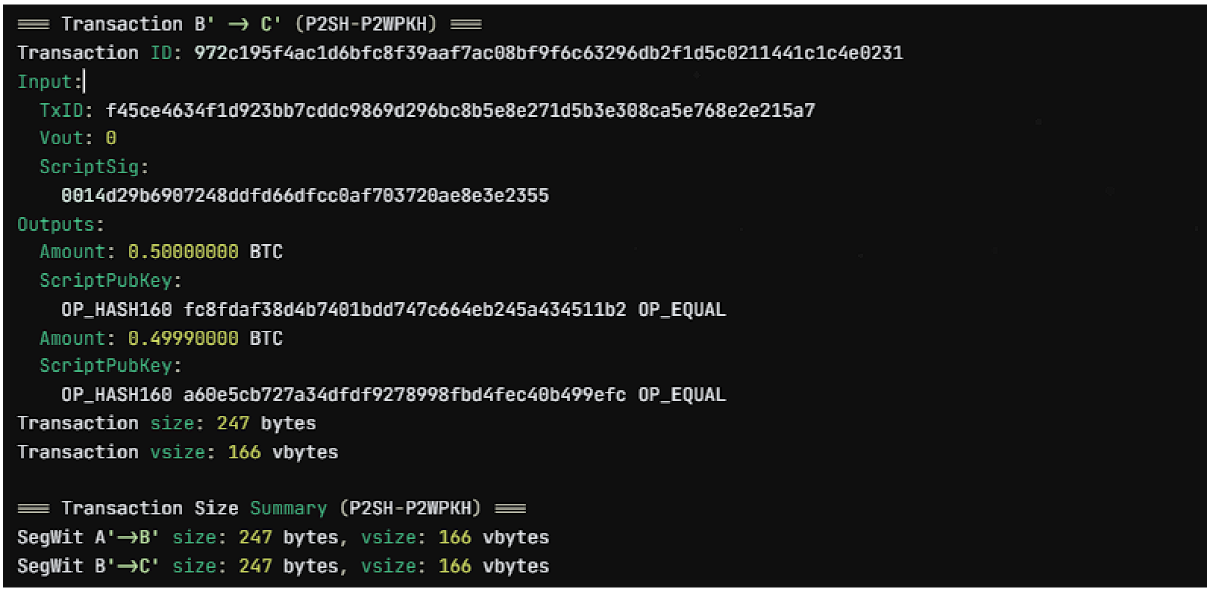
16001469f01650696e8fcd2b5a11183f5d6c7431defb5c

Witness Data:

3045022100c65c9e77702bf9bb7b76fda11c3a5cf58c180b45a1b0e6153fce1d5839957
b86022070db46f4ffaa37e53cf7936e4fe7ff9973f5d3b84bd075bc04cc126313e11b9d01
02fe87318d5f1b7a03ebd99513c004a3c5a9020fd712ec9ef5f63e884dcc952c9f

Output Script (ScriptPubKey):

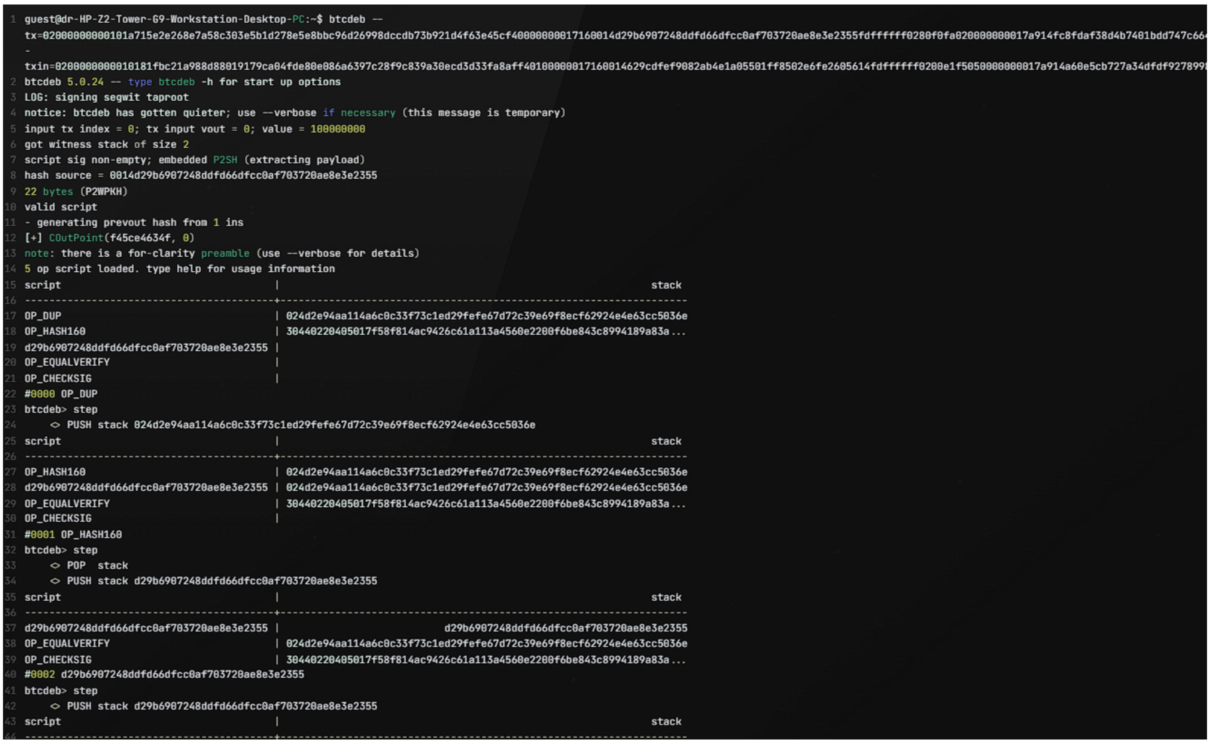
OP_HASH160 b19392a1913a93b935b58df63acbe88cf7411219 OP_EQUAL



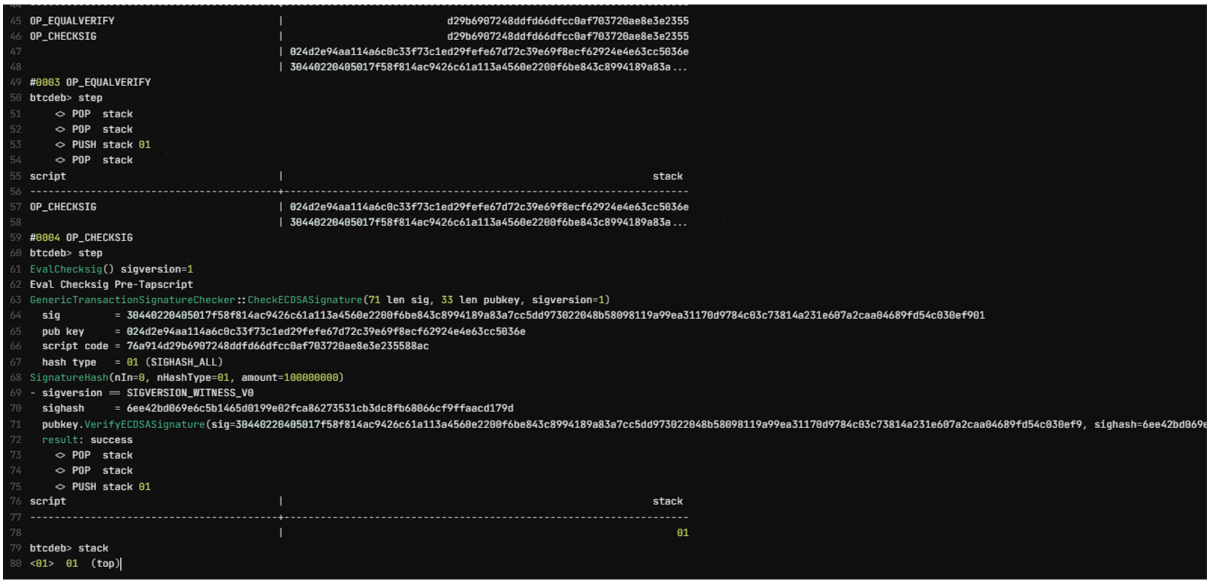
```
══ Transaction B' → C' (P2SH-P2WPKH) ══
Transaction ID: 972c195f4ac1d6bfc8f39aaf7ac08bf9f6c63296db2f1d5c0211441c1c4e0231
Input:
  TxID: f45ce4634f1d923bb7cddc9869d296bc8b5e8e271d5b3e308ca5e768e2e215a7
  Vout: 0
  ScriptSig:
    0014d29b6907248ddfd66dfcc0af703720ae8e3e2355
Outputs:
  Amount: 0.50000000 BTC
  ScriptPubKey:
    OP_HASH160 fc8fdaf38d4b7401bdd747c664eb245a434511b2 OP_EQUAL
  Amount: 0.49990000 BTC
  ScriptPubKey:
    OP_HASH160 a60e5cb727a34dfdf9278998fbd4fec40b499efc OP_EQUAL
Transaction size: 247 bytes
Transaction vsize: 166 vbytes

══ Transaction Size Summary (P2SH-P2WPKH) ══
SegWit A'→B' size: 247 bytes, vsize: 166 vbytes
SegWit B'→C' size: 247 bytes, vsize: 166 vbytes
```

Debugger Terminal Screen Shots:-



```
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb --
tx=02000000000101a715e2e268e7a58c303e5b1d278e5e8bbc96d26998dccdb73b921d4f63e45cf40000000000017160014d29b6907248ddfd66dfcc0af703720ae8e3e2355fdffffff0280f0fa020000000017a914fc8fdaf38d4b7401bdd747c66
-
txin=0200000000010181fbc21a988d88019179ca04fde80e086a6397c28f9c839a30ecd3d33fa8aff4010000000017160014629cdfef9082ab4e1a05501ff8502e6fe2605614fdffffff0200e1f5050000000017a914a60e5cb727a34dfdf927899
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)
input tx index = 0; tx input vout = 0; value = 100000000
got witness stack of size 2
script sig non-empty; embedded P2SH (extracting payload)
hash source = 0014d29b6907248ddfd66dfcc0af703720ae8e3e2355
22 bytes (P2WPKH)
valid script
- generating prevout hash from 1 ins
[+] COutPoint(f45ce4634f, 0)
note: there is a for-clarity preamble (use --verbose for details)
5 op script loaded. type help for usage information
script                                   |                                                            stack
-----------------------------------------+-------------------------------------------------------------------
OP_DUP                                   | 024d2e94aa114a6c0c33f73c1ed29fefe67d72c39e69f8ecf62924e4e63cc5036e
OP_HASH160                               | 30440220405017f58f814ac9426c61a113a4560e2200f6be843c8994189a83a...
d29b6907248ddfd66dfcc0af703720ae8e3e2355 |
OP_EQUALVERIFY                           |
OP_CHECKSIG                              |
#0000 OP_DUP
btcdeb> step
        <> PUSH stack 024d2e94aa114a6c0c33f73c1ed29fefe67d72c39e69f8ecf62924e4e63cc5036e
script                                   |                                                            stack
-----------------------------------------+-------------------------------------------------------------------
OP_HASH160                               | 024d2e94aa114a6c0c33f73c1ed29fefe67d72c39e69f8ecf62924e4e63cc5036e
d29b6907248ddfd66dfcc0af703720ae8e3e2355 | 024d2e94aa114a6c0c33f73c1ed29fefe67d72c39e69f8ecf62924e4e63cc5036e
OP_EQUALVERIFY                           | 30440220405017f58f814ac9426c61a113a4560e2200f6be843c8994189a83a...
OP_CHECKSIG                              |
#0001 OP_HASH160
btcdeb> step
        <> POP  stack
        <> PUSH stack d29b6907248ddfd66dfcc0af703720ae8e3e2355
script                                   |                                                            stack
-----------------------------------------+-------------------------------------------------------------------
d29b6907248ddfd66dfcc0af703720ae8e3e2355 |                           d29b6907248ddfd66dfcc0af703720ae8e3e2355
OP_EQUALVERIFY                           | 024d2e94aa114a6c0c33f73c1ed29fefe67d72c39e69f8ecf62924e4e63cc5036e
OP_CHECKSIG                              | 30440220405017f58f814ac9426c61a113a4560e2200f6be843c8994189a83a...
#0002 d29b6907248ddfd66dfcc0af703720ae8e3e2355
btcdeb> step
        <> PUSH stack d29b6907248ddfd66dfcc0af703720ae8e3e2355
script                                   |                                                            stack
-----------------------------------------+-------------------------------------------------------------------
```



```
OP_EQUALVERIFY                           |                           d29b6907248ddfd66dfcc0af703720ae8e3e2355
OP_CHECKSIG                              |                           d29b6907248ddfd66dfcc0af703720ae8e3e2355
                                         | 024d2e94aa114a6c0c33f73c1ed29fefe67d72c39e69f8ecf62924e4e63cc5036e
                                         | 30440220405017f58f814ac9426c61a113a4560e2200f6be843c8994189a83a...
#0003 OP_EQUALVERIFY
btcdeb> step
        <> POP  stack
        <> POP  stack
        <> PUSH stack 01
        <> POP  stack
script                                   |                                                            stack
-----------------------------------------+-------------------------------------------------------------------
OP_CHECKSIG                              | 024d2e94aa114a6c0c33f73c1ed29fefe67d72c39e69f8ecf62924e4e63cc5036e
                                         | 30440220405017f58f814ac9426c61a113a4560e2200f6be843c8994189a83a...
#0004 OP_CHECKSIG
btcdeb> step
EvalChecksig() sigversion=1
Eval Checksig Pre-Tapscript
GenericTransactionSignatureChecker::CheckECDSASignature(71 len sig, 33 len pubkey, sigversion=1)
  sig         = 30440220405017f58f814ac9426c61a113a4560e2200f6be843c8994189a83a7cc5dd973022048b58098119a99ea31170d9784c03c73814a231e607a2caa04689fd54c030ef901
  pub key     = 024d2e94aa114a6c0c33f73c1ed29fefe67d72c39e69f8ecf62924e4e63cc5036e
  script code = 76a914d29b6907248ddfd66dfcc0af703720ae8e3e235588ac
  hash type   = 01 (SIGHASH_ALL)
SignatureHash(nIn=0, nHashType=01, amount=100000000)
- sigversion == SIGVERSION_WITNESS_V0
  sighash     = 6ee42bd069e6c5b1465d0199e02fca86273531cb3dc8fb68066cf9ffaacd179d
  pubkey.VerifyECDSASignature(sig=30440220405017f58f814ac9426c61a113a4560e2200f6be843c8994189a83a7cc5dd973022048b58098119a99ea31170d9784c03c73814a231e607a2caa04689fd54c030ef9, sighash=6ee42bd069e
  result: success
        <> POP  stack
        <> POP  stack
        <> PUSH stack 01
script                                   |                                                            stack
-----------------------------------------+-------------------------------------------------------------------
                                         |                                                                 01
btcdeb> stack
<01>  01  (top)
```

Script Execution Flow

P2SH-P2WPKH (Pay-to-Script-Hash wrapping Pay-to-Witness-Public-Key-Hash) transactions follow a two-step validation:

1. First, the P2SH validation:
2. [Redeemscript] OP_HASH160 [Redeemscript Hash] OP_EQUAL

This verifies that the provided redeemscript hashes to the expected value.

3. Then, the witness program validation: The redeemscript (0014[20-byte-key-hash]) is interpreted as a witness program. The witness data (signature and public key) is used to validate against the 20-byte-key-hash.

Part 3: Analysis and Comparison

Transaction Size Comparison

Based on the execution of our code, we obtained the following transaction sizes:

Transaction Type	Size (bytes)	Virtual Size (vbytes)
Legacy P2PKH (A→B)	225	225
Legacy P2PKH (B→C)	225	225
P2SH-P2WPKH (A'→B')	247	166
P2SH-P2WPKH (B'→C')	247	166

Structural Differences

1. **Script Structure**:
   - **P2PKH**: The input script (ScriptSig) contains both the signature and public key. The output script (ScriptPubKey) contains the challenge script.
   - **P2SH-P2WPKH**: The input script only contains the redeemscript. The signature and public key are moved to the witness data, which is segregated from the transaction itself.
2. **Transaction Weight**:
   - P2SH-P2WPKH transactions have smaller virtual sizes (166 vbytes) compared to P2PKH transactions (224-225 vbytes), approximately 25-26% smaller.
   - The physical size of P2SH-P2WPKH transactions (247-248 bytes) is actually larger than P2PKH transactions (224-225 bytes), but the witness data is discounted in the fee calculation using virtual size.

Benefits of SegWit Transactions

1. **Reduced Transaction Size**:

  - By moving the signature and public key to the witness data, the transaction's virtual size is effectively reduced by about 25%, leading to lower fees.
  - Our analysis shows that P2SH-P2WPKH transactions are approximately 166 vbytes compared to 224-225 vbytes for P2PKH.

2. **Transaction Malleability Fix**:
   - SegWit addresses the transaction malleability issue by segregating the witness data from the transaction hash calculation. This makes the transaction ID immune to signature manipulations.
   - Since the witness data (containing signatures) is not part of the txid calculation, third parties cannot modify these signatures to create a transaction with the same inputs and outputs but a different txid.
3. **Increased Block Capacity**:
   - The witness discount allows more transactions to fit in a block without increasing the block size limit.
   - With the discount factor of 0.25 for witness data, a 1MB block can effectively contain transactions equivalent to what would be about 4MB of legacy transactions.
4. **Script Versioning**:
   - SegWit introduces a version field, enabling future script upgrades without requiring hard forks.
   - This has already enabled further improvements like Taproot (P2TR), which became active in 2021.
5. **Linear Scaling of Signature Operations**:
   - SegWit changes how signature operations are counted, preventing potential DoS attacks.
   - In legacy transactions, signature operations were counted by transaction size, which could be abused. In SegWit, the weight-based counting ensures linear scaling with actual resource usage.

Conclusion

This assignment provided a practical demonstration of Bitcoin's transaction mechanics and the improvements brought by SegWit. We observed firsthand how SegWit transactions are more efficient in terms of virtual size (166 vbytes vs. 224-225 vbytes) and witnessed the structural changes that enable these efficiencies.

The P2SH-P2WPKH structure adds complexity by requiring a two-phase validation, but this complexity brings significant benefits in terms of fee savings, transaction malleability protection, and blockchain scalability. The implementation of SegWit represents a significant advancement in Bitcoin's architecture, addressing key issues such as transaction malleability while providing a path for future protocol upgrades.