

Bitcoin Scripting Assignment Report

CS 216: Introduction to Blockchain

Team Name: - CipherSurge

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`

- ```

(wenv) vikrant@vikrant:~/Desktop/bl-25_python -u "/home/vikrant/Desktop/bl-2/Legacy.py"

=== Legacy P2PKH Transactions ===
Address A: muu5GhFLjCoHNpm4YQCjMGua19dsEwbj6Y
Address B: m1StYsMpYn92XHmcz52wMALq5DkwbFn6X
Address C: mhFv5QC8Y8RcR6EKY3UbTtYefNsii8rd

Funded Address A with txid: 16b19d085d46750c82888c71d4e9743ffdf9699bb2b45a4a274e3399fdfad42dd

Creating transaction from muu5GhFLjCoHNpm4YQCjMGua19dsEwbj6Y to m1StYsMpYn92XHmcz52wMALq5DkwbFn6X for 1.0 BTC
Available UTXOs: [{"txid": "16b19d085d46750c82888c71d4e9743ffdf9699bb2b45a4a274e3399fdfad42dd", "vout": 0, "address": "muu5GhFLjCoHNpm4YQCjMGua19dsEwbj6Y",
'Label': '', 'scriptPubKey': '76a9149dc8b6c24771b87c9c951e4d5d208b5040ecd7ae88bac', 'amount': 'Decimal('10.00000000')', 'confirmations': 1, 'spendable': True,
'solvable': True, 'desc': 'pkh([0x0115fa/44h]/1h/0h/0/3)02fca184de28f208380a5f1ec72eb0deb1db23698d09d083796d0d101f0533fcfMkdx871sf', 'parent_descs':
['pkh(tpubD6mZ5VbkrYhZ4WwEhKQ89p6oPoPVXdtOhY64YVP6mXoZj6pUBgEumFy12J3uJbdQX1xpXRFsCmFhs44YbALcmRPLHBj8CjMwg83N2LEpds/44h/1h/0h/0/3)*9g08Rqzmz', 'safe': True]}
Raw transaction created: 0280080001d42add9ff39e374a284452bbb996fd3f74e9d4718c08028c75468d059db16080008000f0fffff0280e1f50500080001976a914208be7ffdd0e1849
f4ad66f85719a637f6ce8e288ac0c1a35000800001976a9149dc8b6c24771b87c9c951e4d5d208b5040ecd7ae88ac08000800
Signed transaction: {'hex': '0280080001d42add9ff39e374a284452bbb996fd3f74e9d4718c08028c75468d059db160800080064730448220647c7cd6dc614729fe1689778f5877717
84a99d1e38ad868d736fb3396e02204241d4c428a7fb2f35e08545b321547edae08017954828a9b5243e77b4b9012102fca184de28f208380a5f1ec72eb0deb1db23698d09d083796d0d101f0533
fcdf0fffff0280e1f50500080001976a914208be7ffdd0e1849f4ad66f85719a637f6ce8e288ac0c1a3500080001976a9149dc8b6c24771b87c9c951e4d5d208b5040ecd7ae88ac08000800', 'complete':
True}
Transaction broadcasted with txid: f0c473628feed0aeb28c9904af7296791058898472db1a17236c9203bfff43c6d

```

- 105 blocks to make coins spendable (first 100 blocks need to mature).
- Address A with 10 BTC:
- Transaction ID:  
16b19d058d46750c02088c71d4e9743ffd9699bb2b45a4a274e3399fdfad42dd
- Address A sent and executed Transaction A→B:
- Sent 1.0 BTC from Address A to Address B
- Transaction ID:  
f0c473628feed0ae20bc9904af7296791058898472d1ba17236c9203bff43c6e
- Address B sent 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):**

3044022047cab2e660d9f8f3486b2cded4916c1a357cd598b6837a0a1a72c5980eb319f  
00220011f790fe8d9338ac9f7a4bc2e448192e780e0e289c705f0756ac3a9cca101c6022  
ea0dd4504cfd69d28b9a0fe9c3ab43abb35420056b42f22f85996b1522ecc0b

### Output Script (ScriptPubKey):

OP\_EQUALVERIFY OP\_CHECKSIG

### Transaction B→C (Legacy P2PKH)

**Input Script (ScriptSig):**

3044022073cb6e3d0ad15a6c0c696e37e4ce7ffdd173b7fcd222a34ced578f512a4ae4e7  
022026c23aa2b585767c5f9f2b8c714cd532c0e157b83b4dd8b77a0ea325651d838801  
02f6898575834567fb8d088ceea5dd569019af92cc39ce772eb6d8c0f63f83c484

### Output Script (ScriptPubKey):

OP\_DUP OP\_HASH160 2d39ea3e1100fe1bf6d71f881b808fbd5451f0c5

OP EQUALVERIFY OP CHECKSIG

```

=== Transaction B → C (Legacy P2PKH) ===
Transaction ID: 0e8c30e92a47cb2db85e8d85dc2109d1b45fec8feefc14d3adcc919109f755c4
Input:
 TxID: f0c473628feed0ae20bc9904af7296791058898472d1ba17236c9203bfff43c6e
 Vout: 0
 ScriptSig:
 304402200895ae02b4c8daae1949ba595ec43467f4743492c7dd98d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b2c8889c89a4f3a7c5777d56720e42b08b0d[ALL]
 83bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
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-69-Workstation-Desktop-PC:~$ btcdeb --
tx=0208080801e3cf4b93926c2317bad17284895810799672af0499bc20aed0ee8f6273cf0808080806a47304402208095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9f
--
txin=0208080801dd42addf9f39e374a2a4452bbb9996fd3f74e9d4718c08020c75468d959db110808080806a47304402208095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9f
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
304402208095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b2c8889c89a4f3a7c5777d56720e42b080d81
03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e |
<<< scriptPubKey >>> |
OP_DUP |
OP_HASH160 |
200eb7ffd08e1849f4ad66f8571a9637fce6e8e2 |
OP_EQUALVERIFY |
OP_CHECKSIG |
#0000 304402208095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b2c8889c89a4f3a7c5777d56720e42b080d81
btcdeb> step
 > PUSH stack 304402208095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b2c8889c89a4f3a7c5777d56720e42b080d81
script | stack
-----|-----
03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e | 304402208095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b2c8889c89a4f3a7c5777d56720e42b080d81
<<< scriptPubKey >>> |
OP_DUP |
OP_HASH160 |
200eb7ffd08e1849f4ad66f8571a9637fce6e8e2 |
OP_EQUALVERIFY |
OP_CHECKSIG |
#0001 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
btcdeb> step
 > PUSH stack 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
script | stack
-----|-----
<<< scriptPubKey >>> | 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
OP_DUP | 304402208095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b2c8889c89a4f3a7c5777d56720e42b080d81
OP_HASH160 |

200eb7ffd08e1849f4ad66f8571a9637fce6e8e2 |
OP_EQUALVERIFY |
OP_CHECKSIG |
#0001 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
btcdeb> step
 > PUSH stack 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
script | stack
-----|-----
<<< scriptPubKey >>> | 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
OP_DUP | 304402208095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b2c8889c89a4f3a7c5777d56720e42b080d81
OP_HASH160 |

200eb7ffd08e1849f4ad66f8571a9637fce6e8e2 |
OP_EQUALVERIFY |
OP_CHECKSIG |
<<< scriptPubKey >>> |
btcdeb> step
script	stack
OP_DUP | 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
OP_HASH160 | 304402208095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b2c8889c89a4f3a7c5777d56720e42b080d81
200eb7ffd08e1849f4ad66f8571a9637fce6e8e2 |
OP_EQUALVERIFY |
OP_CHECKSIG |
#0003 OP_DUP
btcdeb> step
 > PUSH stack 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
script | stack
-----|-----
OP_HASH160 | 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
200eb7ffd08e1849f4ad66f8571a9637fce6e8e2 | 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
OP_EQUALVERIFY | 304402208095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b2c8889c89a4f3a7c5777d56720e42b080d81
OP_CHECKSIG |
#0004 OP_HASH160
btcdeb> step
 > POP stack
 > PUSH stack 200eb7ffd08e1849f4ad66f8571a9637fce6e8e2
script | stack
-----|-----
200eb7ffd08e1849f4ad66f8571a9637fce6e8e2 | 200eb7ffd08e1849f4ad66f8571a9637fce6e8e2
OP_EQUALVERIFY | 03bbc8e64f8eb50e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
OP_CHECKSIG | 304402208095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b2c8889c89a4f3a7c5777d56720e42b080d81
#0005 200eb7ffd08e1849f4ad66f8571a9637fce6e8e2
btcdeb> step
 > PUSH stack 200eb7ffd08e1849f4ad66f8571a9637fce6e8e2
script | stack
-----|-----
```

```

OP_EQUALVERIFY | 208eb7ffd08e1849f4ad66f8571a9637fce6e8e2
OP_CHECKSIG | 208eb7ffd08e1849f4ad66f8571a9637fce6e8e2
| 03bbc8e64f8eb58e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
| 304402208095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e...

#0006 OP_EQUALVERIFY
btcd> step
 > POP stack
 > POP stack
 > PUSH stack 01
 > POP stack

script	stack
OP_CHECKSIG	03bbc8e64f8eb58e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
304402208095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e...	

#0007 OP_CHECKSIG
btcd> step
EvalChecksig() sigversion=0
Eval Checksig Pre-Tapscript
GenericTransactionSignatureChecker::CheckECDSASignature(71 len sig, 33 len pubkey, sigversion=0)
sig = 304402208095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b2c8889c89ae4f3a7c5777d56720e42b0b0d01
pub key = 03bbc8e64f8eb58e1261b8a6c3fd20b3dfa9e3c40b9545124497378367261f8d0e
script code = 76e914208eb7ffd08e1849f4ad66f8571a9637fce6e8e288ac
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:76e914208eb7ffd08e1849f4ad66f8571a9637fce6e8e288ac
<< txTo.vin[nInput].nSequence = 4294967293 [0xffffffff]
sighash = 01273873a4816f52da7d4ed4f6d8edb9d222db562642a9d85fa06f080e77c612
pubkey.VerifyECDSASignature(sig=304402208095ae02b4c8daae1949ba595ec43467f4743492c7dd90d819ee11e29ae7d42d0220281221c8e6dfc3cc0bce679565a9b2c8889c89ae4f3a7c5777d56720e42b0b0d, sighash=01273873a
result: success
 > POP stack
 > POP stack
 > PUSH stack 01

script	stack
01	

btcd> 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:

```
[3045022100f2a3e245ab5af1c76bdad8c0231bb38c3e32fb61c6f8ce073ef86e4f0644cb
2c02203c8fe9e88e5266b7e64ba6fcc8b7c6da68dcb47cfc1c59de4a07a8162cd5f5101
][03a72f82143f639e0147275c3e92e6d643df73e6f44b15fce04e067e7d3a53a210]
```

2. OP\_DUP: Stack:

```
[3045022100f2a3e245ab5af1c76bdad8c0231bb38c3e32fb61c6f8ce073ef86e4f0644cb
2c02203c8fe9e88e5266b7e64ba6fcc8b7c6da68dcb47cfc1c59de4a07a8162cd5f5101
][03a72f82143f639e0147275c3e92e6d643df73e6f44b15fce04e067e7d3a53a210]
[03a72f82143f639e0147275c3e92e6d643df73e6f44b15fce04e067e7d3a53a210]
```

3. OP\_HASH160: Stack:

```
[3045022100f2a3e245ab5af1c76bdad8c0231bb38c3e32fb61c6f8ce073ef86e4f0644cb
2c02203c8fe9e88e5266b7e64ba6fcc8b7c6da68dcb47cfc1c59de4a07a8162cd5f5101
][03a72f82143f639e0147275c3e92e6d643df73e6f44b15fce04e067e7d3a53a210]
[68c6c9e0b1fb2e4747720482f451c8dabb85d600]
```

4. Push [68c6c9e0b1fb2e4747720482f451c8dabb85d600]: Stack:

```
[3045022100f2a3e245ab5af1c76bdad8c0231bb38c3e32fb61c6f8ce073ef86e4f0644cb
2c02203c8fe9e88e5266b7e64ba6fcc8b7c6da68dcb47cfc1c59de4a07a8162cd5f5101
][03a72f82143f639e0147275c3e92e6d643df73e6f44b15fce04e067e7d3a53a210]
[68c6c9e0b1fb2e4747720482f451c8dabb85d600]
[68c6c9e0b1fb2e4747720482f451c8dabb85d600]
```

5. OP\_EQUALVERIFY: Stack:

```
[3045022100f2a3e245ab5af1c76bdad8c0231bb38c3e32fb61c6f8ce073ef86e4f0644cb
2c02203c8fe9e88e5266b7e64ba6fcc8b7c6da68dcb47cfc1c59de4a07a8162cd5f5101
][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': 2NGGeba8r4VJZ3jCV26NNtRr1f2XmTVkrMq

```

P2SH-P2WPKH (SegWit) Transactions ===
Address A': 2MtkxV9k58aJmRLiwx3tK04jeMxChuoH5HF
Address B': 2N8PFN2dJmR81Vxp15HDsdjom6SRdpEzm
Address C': 2N66ebs8r4VJ3zjCV2bNntR1rf12XmTVkrMq

Funded Address A' with txid: f4afa83fd35dec369a839c8f9c297636a0880e8fd0ca799101888d981ac2fb81

Creating transaction from 2MtkxV9k58aJmRLiwx3tK04jeMxChuoH5HF to 2N8PFN2dJmR81Vxp15HDsdjom6SRdpEzm for 1.0 BTC
Available UTXOs: [{"txid": "f4afa83fd35dec369a839c8f9c297636a0880e8fd0ca799101888d981ac2fb81", "vout": 1, "address": "2MtkxV9k58aJmRLiwx3tK04jeMxChuoH5HF", "label": "", "redeemScript": "0014629cdfef982ab4e1a05501f8582e62605614", "scriptPubKey": "a9141097a9fad24689a177c0543bdc05779bee10857987", "amount": Decimal('1.00000000')}, {"confirmations": 1, "spendable": True, "solvable": True, "desc": "sh(wpkh([0a19a30b/49h/1h/0h/8/3]028fd013e9d8c9e6d534c3500d8fe9e35d5915faa959b61caa0eff77ca498c0682))#x1sk7dp0", "parent_descs": ["sh(wpkh(tpub06kzVbkrYhZ4k1cAQM4sh3MRcUomoy5NNHbmi903k3n1P3a9j7fMEXDNVwe0DLy4c28ksT5bhHen6HJRxexXZ6f7LEH61diaV18f9/49h/1h/0h/8/0)#r5pkn5tc")], "safe": True}]
Raw transaction:
020800000181fbc21a988d88019179ca04fe80e086a6397c28f9c839a30cd3d33fa8ff40100000000fdffffff0200e1f505000000017a91460e5c727a34df927898fbd4fec40b499efc87f9c1a4350000000017a9141097a9fad24689a177c0543bdc05779bee1085798700000000
Signed transaction: 'hex':
'02080000000181fbc21a988d88019179ca04fe80e086a6397c28f9c839a30cd3d33fa8ff4010000017160014629cdfef982ab4e1a05501f8582e62605614fdffffff0200e1f505000000017a91460e5c727a34df927898fbd4fec40b499efc87f9c1a4350000000017a9141097a9fad24689a177c0543bdc05779bee1085798702743040d203e4f6c35b9493603b836e42475198f528142dee6f0122c51e165f1823f9147250220527f80e95e49c9accb1c3a05f1b232c190bbcc971bf55db06ea6f179802be0121828fd013e9d8c9e6d534c3500d8fe9e35d5915faa959b61caa0eff77ca498c068200000000', 'complete': True}
Transaction broadcasted with txid: f45ce4634f1d923bb7cddc9869d296bc8b5e8271d5b3e308ca5e768e2e215a7

```

2. Funded Address A' with 10 BTC:

- Transaction ID:  
f4afa83fd3d3ec309a839c8fc297636a080ee8fd04ca799101888d981ac2fb81

3. Created and executed Transaction  $A' \rightarrow B'$ :

- Sent 1.0 BTC from Address A' to Address B'
- Transaction ID:  
f45ce4634f1d923bb7cddc9869d296bc8b5e8e271d5b3e308ca5e768e2e215a7

4. Created and executed Transaction  $B' \rightarrow C'$ :

- 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:



### Output Script (ScriptPubKey):

```
=== Transaction A' -> B' (P2SH-P2WPKH) ===
Transaction ID: f45ce4634f1d923bb7cdcc9869d296bc8b5e8e271d5b3e308ca5e768e2e215a7
Input:
TxID: f4fa83fd3d3ec309a839c8fc29736ba088ee8df84ca799101888d981ac27fb81
Vout: 1
ScriptSig:
 0014629cdfef9082ab4ea1a95501ff8502e6fe2605614
Outputs:
Amount: 1.00000000 BTC
ScriptPubKey:
 OP_HASH160 a60e5cb727a34dfd9f278998fdb4fec40b499efc OP_EQUAL
Amount: 8.99990000 BTC
ScriptPubKey:
 OP_HASH160 1097a9fad24689a177c0543bdc085779bee108579 OP_EQUAL
Transaction size: 247 bytes
Transaction vsize: 166 vbytes

Creating transaction from 2N8PFN2dJmRb1Vxp15HDsdjomGSRpdgEzm to 2N6G8bs8r4VJz3jCV26NWtRr1f2XmTVkrMq for 0.5 BTC
Available UTXOs: [{'txid': 'f45ce4634f1d923bb7cdcc9869d296bc8b5e8e271d5b3e308ca5e768e2e215a7', 'vout': 0, 'address': '2N8PFN2dJmRb1Vxp15HDsdjomGSRpdgEzm', 'label': '',
 'redeemScript': '0014d296b997248ddf6d6dfc08af703278ae83e2355', 'scriptPubKey': 'a914a60e5cb727a34dfd9f278998fdb4fec40b499efc87', 'amount': Decimal('1.00000000')},
 'confirmations': 1, 'spendable': True, 'solvable': True, 'desc':
 'sh(wpkh([9a19a30b]/49h/1h/8h/8/4)[024d2e94aa114a6c0833f73c1ed29fef6d72c39e69f8ec67294e4e63cc5036e])#nu5kt6w',
 'parent_descs': ['sh(wpkh(tpubD0nzVbkrrYhZ4XlKcAQm4h3MRaCoorUmoY5NhHbaim9QnK5ln1P3a9jftfMEXDNVwe6DLy4xk2StShENH6JRxeXX26f7LEh61diwYi8F9/49h/1h/8h/0/*))#Spkn5tc']},
 'safe': True}]
Raw transaction created: 0200000001a715e2c68e7a58c303e5b1d278e5e8bbc96d26998ddcd73b921d4f63e45cf40000000000dfffffff02080ffa0200000000017a914fc8fdaf38d4b7401bdd747c664eb24
5a34511b28770c9Fa020000000017a914a69e5cb727a34dfd9f278998fdb4fec40b499efc8700000000
Signed transactions: {'hex': '02000000000101a715e2c68e7a58c303e5b1d278e5e8bbc96d26998ddcd73b921d4f63e45cf400000000017160014d29b6987248ddfd66dfcc8af703278ae83e2355dffff
ff02080ffa02000000017a914fc
8fda38db47401bdd747c664eb245a34511b28770c9Fa020000000017a914a69e5cb727a34dfd9f278998fdb4fec40b499efc870247304bd220a0501f58f814ac94dc61a113a4560e2200f6be843c8994189a8
3a7cc5dd97302204b5809811a99ea31170d9784c03c73814a231e0872caaa04689f5dc030ef09121024d2e94aa114a6c0833f73c1ed29fef6d72c39e69f8ecf67294e4e63cc5036e0000000', 'complete':
True}
Transaction broadcasted with txid: 972c195f4ac1d6bfc8f39aaf7ac08bf9f6c3296db2f1d5c0211441c1c4e0231
```

### Transaction B'→C' (P2SH-P2WPKH)

**Input Script (ScriptSig):**

### Witness Data:

### 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 a60e5cb727a34dfd9278998fbd4fec40b499efc 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:-

```

1 guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb --
tx=020808080808181a715e268e7a58c383e5b1d278e5e8bbc96d26998dccb73b921d4f63e45cf40808080817168014d29b6987248ddf66dfcc8af783728ae8e3e2355feffffff0280f8fa020808080817a914fc8fda38d4b7481bd4747c66
-
txin=020808080808181a715e268e7a58c383e5b1d278e5e8bbc96d26998dccb73b921d4f63e45cf40808080817168014d29b6987248ddf66dfcc8af783728ae8e3e2355feffffff0280f8fa020808080817a914fc8fda38d4b7481bd4747c66
2 btcdeb 5.0.24 -- type btcdeb -h for start up options
3 LOG: signing segwit taproot
4 notice: btcdeb has gotten quieter; use --verbose if necessary (this message is temporary)
5 input tx index = 0; tx input vout = 0; value = 100000000
6 got witness stack of size 2
7 script sig non-empty; embedded P2SH (extracting payload)
8 hash source = 0814d29b6987248ddf66dfcc8af783728ae8e3e2355
9 22 bytes (P2WPKH)
10 valid script
11 - generating prevout hash from 1 ins
12 [+] COutPoint(f45ce4634f, 0)
13 note: there is a for-clarity preamble (use --verbose for details)
14 5 op script loaded. type help for usage information
15 script | stack
16 -----|-----
17 OP_DUP | 024d2e94aa114a6c8c33f73c1ed29fefe67d72c39e69f8ecf62924e4e63cc5836e
18 OP_HASH160 | 384402204805017f58f814ac9426c61a113e4560e2208f6be843c8994189a83a ...
19 d29b6987248ddf66dfcc8af783728ae8e3e2355 |
20 OP_EQUALVERIFY |
21 OP_CHECKSIG |
22 #0000 OP_DUP
btcdeb> step
23 ↳ PUSH stack 024d2e94aa114a6c8c33f73c1ed29fefe67d72c39e69f8ecf62924e4e63cc5836e
24 script | stack
25 -----|-----
26 OP_HASH160 | 024d2e94aa114a6c8c33f73c1ed29fefe67d72c39e69f8ecf62924e4e63cc5836e
27 d29b6987248ddf66dfcc8af783728ae8e3e2355 | 024d2e94aa114a6c8c33f73c1ed29fefe67d72c39e69f8ecf62924e4e63cc5836e
28 OP_EQUALVERIFY | 384402204805017f58f814ac9426c61a113e4560e2208f6be843c8994189a83a ...
29 OP_CHECKSIG |
30 #0001 OP_HASH160
btcdeb> step
31 ↳ POP stack
32 ↳ PUSH stack d29b6987248ddf66dfcc8af783728ae8e3e2355
33 script | stack
34 -----|-----
35 d29b6987248ddf66dfcc8af783728ae8e3e2355 | d29b6987248ddf66dfcc8af783728ae8e3e2355
36 OP_EQUALVERIFY | 024d2e94aa114a6c8c33f73c1ed29fefe67d72c39e69f8ecf62924e4e63cc5836e
37 OP_CHECKSIG | 384402204805017f58f814ac9426c61a113e4560e2208f6be843c8994189a83a ...
38 #0002 d29b6987248ddf66dfcc8af783728ae8e3e2355
btcdeb> step
39 ↳ PUSH stack d29b6987248ddf66dfcc8af783728ae8e3e2355
40 script | stack
41 -----|-----
42 OP_EQUALVERIFY | d29b6987248ddf66dfcc8af783728ae8e3e2355
43 OP_CHECKSIG | d29b6987248ddf66dfcc8af783728ae8e3e2355
44 #0003 OP_EQUALVERIFY
btcdeb> step
45 ↳ POP stack
46 ↳ POP stack
47 ↳ PUSH stack 01
48 ↳ POP stack
49 script | stack
50 -----|-----
51 OP_CHECKSIG | 024d2e94aa114a6c8c33f73c1ed29fefe67d72c39e69f8ecf62924e4e63cc5836e
52 #0004 OP_CHECKSIG | 384402204805017f58f814ac9426c61a113e4560e2208f6be843c8994189a83a ...
53 btcdeb> step
54 ↳ EvalChecksig() sigversion=1
55 ↳ EvalChecksig Pre-Tapscript
56 GenericTransactionSignatureChecker::CheckECDSASignature(71 len sig, 33 len pubkey, sigversion=1)
57 sig = 384402204805017f58f814ac9426c61a113e4560e2208f6be843c8994189a83a7cc5dd973022048058098119a99ea31170d9784c83c73814a231e6072caa04689fd54c830ef901
58 pub key = 024d2e94aa114a6c8c33f73c1ed29fefe67d72c39e69f8ecf62924e4e63cc5836e
59 script code = 76a914d29b6987248ddf66dfcc8af783728ae8e3e235588ac
60 hash type = 01 (SIGHASH_ALL)
61 SignatureHash(nIn=0, nHashType=01, amount=100000000)
62 sigversion = SIGVERSION_WITNESS_V0
63 sighash = 6ee42bd069e6c5b1465d0199e02fca86273531cb3dc8fb6886cf9ffaacd179d
64 pubkey.VerifyECDSASignature(sig=384402204805017f58f814ac9426c61a113e4560e2208f6be843c8994189a83a7cc5dd973022048058098119a99ea31170d9784c83c73814a231e6072caa04689fd54c830ef901, sighash=6ee42bd069e6c5b1465d0199e02fca86273531cb3dc8fb6886cf9ffaacd179d)
65 result: success
66 ↳ POP stack
67 ↳ POP stack
68 ↳ PUSH stack 01
69 script | stack
70 -----|-----
71 |
72 |
73 |
74 |
75 |
76 |
77 |
78 |
79 btcdeb> stack
80 <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.