CS 216 Scripting Assignment
Team Name - Blockfinity

Members -

1. **Subhankar Das (230001073)**
2. **Salaj Bansal (230002063)**
3. **Nipun Samal (230041025)**

Objective:

The objective of this assignment is to understand the process of creating and validating Bitcoin transactions using Legacy (P2PKH) and SegWit (P2SH-P2WPKH) address formats.

Setup:

We have used Python to interact with bitcoind(Bitcoin-core in regtest mode).
The following parameters were set to the corresponding values in 'bitcoin.conf' file:
paytxfee - 0.0001 (BTC/kB)
fallbackfee - 0.0002 (BTC/kB)
mintxfee - 0.00001 (BTC/kB)
txconfirmtarget - 6

Legacy Address Transaction:

Addresses generated are:
Address A: moFFJr31DfkuKJMhGJVRLXd4TBw8XPaHbT
Address B: n2CTex4hHhmMPK3MGD5SyjKopHGS8MkY1Y
Address C: mj5mFK1PmTJS4NsWCYgvNFwyoPHFs3CCqi

Initially, A is given 1 BTC.
Then, 0.5 BTC is sent from A to B, with a fee of 0.0001 BTC, leaving A with 0.4999 BTC.
TXID for A to B -
3048109b7c2fbee5d7e901d750d6e7b8f9f335c6eb1877a544af76dd2515f4d9

Thus, B has one UTXO containing 0.5 BTC.
UTXO set of B -
{'txid': '3048109b7c2fbee5d7e901d750d6e7b8f9f335c6eb1877a544af76dd2515f4d9', 'vout': 0, 'address': 'n2CTex4hHhmMPK3MGD5SyjKopHGS8MkY1Y', 'label': '', 'scriptPubKey': '76a914e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e88ac', 'amount': Decimal('0.50000000'), 'confirmations': 1, 'spendable': True, 'solvable': True, 'desc': 'pkh([d48c3dee/44h/1h/0h/0/1]03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a)#7rlleftz', 'parent_descs': ['pkh(tpubD6NzVbkrYhZ4YTiPYoTnmQn3VwYXBcgPM9dENFpsijkoiReXJB4WM77q89ZYVW9f253r1WkACKMsRWQ6Syyj9c6r1iTAWxu9s6t1aScxm3D/44h/1h/0h/0/)#wqquptwx'], 'safe': True}*

This UTXO refers to the TXID for A to B and has the address of B along with 1 confirmation, making this UTXO spendable provided the correct response script is provided to the challenge script (scriptPubKey mentioned in the UTXO). Thus, when B spends this UTXO, it uses the previous transaction (from A to B).

Now, 0.25 BTC is sent from B to C along with a fee of 0.0001 BTC, leaving B with 0.2499 BTC. The following command refers to this transaction.
createrawtransaction [[{"txid":
"3048109b7c2fbee5d7e901d750d6e7b8f9f335c6eb1877a544af76dd2515f4d9", "vout": 0}],
{"mj5mFK1PmTJS4NsWCYgvNFwyoPHFs3CCqi": 0.25,
"n2CTex4hHhmMPK3MGD5SyjKopHGS8MkY1Y": 0.2499}]

TXID for B to C -
e12541902639b5992110235a9b538477b650745ef7041385cf1769222c72d860

Decoded Script for A to B -
OP_DUP OP_HASH160 77f8a0ca27b5e20f226754836ff2f266d9e329ae OP_EQUALVERIFY OP_CHECKSIG

Decoded Script for B to C -
OP_DUP OP_HASH160 149b6ecd97dc692a405919c69f640d61b23c7b04 OP_EQUALVERIFY OP_CHECKSIG

Procedure:
In Legacy address transactions, the challenge script and valid response script structures are as follows:
Challenge Script: OP_DUP OP_HASH160 <Public Key Hash> OP_EQUALVERIFY OP_CHECKSIG
Response Script: <Signature> <Public Key>

First, the response script is pushed on the stack and then the challenge script is placed on the stack. Then, one by one the operations are executed

1. Public key is duplicated and hashed.
2. This hash is compared with the hash in the challenge script with OP_EQUALVERIFY.
3. If they are equal, then it is checked if the signature is valid using the public key. If true, then the transaction is valid.

Screenshots:

Decoded Scripts -


```
Decoded transaction from A to B:
{'txid': '8f8c9522ee24ef14accaaa303a1dc0f488468f50c33c8490fe86681bdc8f3e7a', 'hash':
'8f8c9522ee24ef14accaaa303a1dc0f488468f50c33c8490fe86681bdc8f3e7a', 'version': 2, 'size': 119, 'vsize': 119, 'weight': 476, 'locktime': 0,
'vin': [{'txid': '591e8b95fc28392c43e87d99acb1d55d499e189678c18f224bd2b3acafe4f4a2', 'vout': 1, 'scriptSig': {'asm': '', 'hex': ''},
'sequence': 4294967293}], 'vout': [{'value': Decimal('0.50000000'), 'n': 0, 'scriptPubKey': {'asm': 'OP_DUP OP_HASH160
e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e OP_EQUALVERIFY OP_CHECKSIG', 'desc': 'addr(n2CTex4hHhmMPK3MGD5SyjKopHGS8MkY1Y)#wuvv5a75', 'hex':
'76a914e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e88ac', 'address': 'n2CTex4hHhmMPK3MGD5SyjKopHGS8MkY1Y', 'type': 'pubkeyhash'}}, {'value':
Decimal('0.49990000'), 'n': 1, 'scriptPubKey': {'asm': 'OP_DUP OP_HASH160 54c88d9c796cc9e6ddf4af4215506c6821376c0f OP_EQUALVERIFY
OP_CHECKSIG', 'desc': 'addr(moFFJr31DfkuKJMhGJVRLXd4TBw8XPaHbT)#82d0sdpe', 'hex': '76a91454c88d9c796cc9e6ddf4af4215506c6821376c0f88ac',
'address': 'moFFJr31DfkuKJMhGJVRLXd4TBw8XPaHbT', 'type': 'pubkeyhash'}}]}
```

```
Decoded transaction from B to C:
{'txid': '2376ac1e90e2e20ab69ad94e19e62fff9b5c1e379ebfd76a63ac514b3d81e043', 'hash':
'2376ac1e90e2e20ab69ad94e19e62fff9b5c1e379ebfd76a63ac514b3d81e043', 'version': 2, 'size': 119, 'vsize': 119, 'weight': 476, 'locktime': 0,
'vin': [{'txid': '3048109b7c2fbee5d7e901d750d6e7b8f9f335c6eb1877a544af76dd2515f4d9', 'vout': 0, 'scriptSig': {'asm': '', 'hex': ''},
'sequence': 4294967293}], 'vout': [{'value': Decimal('0.25000000'), 'n': 0, 'scriptPubKey': {'asm': 'OP_DUP OP_HASH160
271ce1dcfc0152e07515fe8fb94719eb53301aa8 OP_EQUALVERIFY OP_CHECKSIG', 'desc': 'addr(mj5mFK1PmTJS4NsWCYgvNFwyoPHFs3CCqi)#m6s4pkfm', 'hex':
'76a914271ce1dcfc0152e07515fe8fb94719eb53301aa888ac', 'address': 'mj5mFK1PmTJS4NsWCYgvNFwyoPHFs3CCqi', 'type': 'pubkeyhash'}}, {'value':
Decimal('0.24990000'), 'n': 1, 'scriptPubKey': {'asm': 'OP_DUP OP_HASH160 e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e OP_EQUALVERIFY
OP_CHECKSIG', 'desc': 'addr(n2CTex4hHhmMPK3MGD5SyjKopHGS8MkY1Y)#wuvv5a75', 'hex': '76a914e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e88ac',
'address': 'n2CTex4hHhmMPK3MGD5SyjKopHGS8MkY1Y', 'type': 'pubkeyhash'}}]}
```

Bitcoin Debugger Steps -

```
nipun-samal@nipun-samal-HP-Pavilion-Laptop-14-ec1xxx:~$ btcdeb --tx=0200000001d9f41525dd76af44a57718ebc635f3f9b8e7d650d701e9d7e5be2f7c9b104830000000006a4730440220487af36e6e36125c07dd09b8b65f
e64c6af686e51c656fc4577b649acb966c1a02200c64da187aa96e92037b11d60ae85fe26950dd64e088d14db2ccd010bb4311a6012103a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4afdffffff0240787d
01000000001976a914271ce1dcfc0152e07515fe8fb94719eb53301aa888ac30517d01000000001976a914e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e88ac00000000 --txin=0200000001a2f4e4afacb3d24b228fc17896189e495d
d5b1ac997de8432c3928fc958b1e59010000006a47304402204ce7f0bcc3fc2f885024752b392fef704d72741ec332cdc8b1e256be3d38fc56022049ec7b0aa816b079f33bcf784c504ec3859224a9caf0fb0d873cf9e038547945012102 98
d8bc16dff13eac69fed57f0eac95e4d1695d654222a9380ed181cd9391291ffdfffff0280f0fa02000000001976a914e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e88ac70c9fa02000000001976a91454c88d9c796cc9e6ddf4af4215
506c6821376c0f88ac00000000
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 = 50000000
got witness stack of size 0
8 op script loaded. type `help` for usage information
script                                                          |  stack
----------------------------------------------------------------+--------
30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649... |
03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a |
<<< scriptPubKey >>>                                            |
OP_DUP                                                          |
OP_HASH160                                                      |
e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e                        |
OP_EQUALVERIFY                                                  |
OP_CHECKSIG                                                     |
#0000 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649acb966c1a02200c64da187aa96e92037b11d60ae85fe26950dd64e088d14db2ccd010bb4311a601
btcdeb> step
                <> PUSH stack 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649acb966c1a02200c64da187aa96e92037b11d60ae85fe26950dd64e088d14db2ccd010bb4311a601
script                                                          |                                                                stack
----------------------------------------------------------------+----------------------------------------------------------------
03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a | 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649...
<<< scriptPubKey >>>                                            |
OP_DUP                                                          |
OP_HASH160                                                      |
e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e                        |
OP_EQUALVERIFY                                                  |
OP_CHECKSIG                                                     |
#0001 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
btcdeb> print
    #0000 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649acb966c1a02200c64da187aa96e92037b11d60ae85fe26950dd64e088d14db2ccd010bb4311a601
 -> #0001 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
    <<< scriptPubKey >>>
    #0003 OP_DUP
    #0004 OP_HASH160
    #0005 e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e
```

```
btcdeb> print
    #0000 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649acb966c1a02200c64da187aa96e92037b11d60ae85fe26950dd64e088d14db2ccd010bb4311a601
 -> #0001 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
    <<< scriptPubKey >>>
    #0003 OP_DUP
    #0004 OP_HASH160
    #0005 e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e
    #0006 OP_EQUALVERIFY
    #0007 OP_CHECKSIG
btcdeb> step
                <> PUSH stack 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
script                                                          |                                                                stack
----------------------------------------------------------------+----------------------------------------------------------------
<<< scriptPubKey >>>                                            | 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
OP_DUP                                                          | 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649...
OP_HASH160                                                      |
e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e                        |
OP_EQUALVERIFY                                                  |
OP_CHECKSIG                                                     |
<<< scriptPubKey >>>
btcdeb> print
    #0000 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649acb966c1a02200c64da187aa96e92037b11d60ae85fe26950dd64e088d14db2ccd010bb4311a601
    #0001 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
 -> <<< scriptPubKey >>>
    #0003 OP_DUP
    #0004 OP_HASH160
    #0005 e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e
    #0006 OP_EQUALVERIFY
    #0007 OP_CHECKSIG
btcdeb> step
script                                                          |                                                                stack
----------------------------------------------------------------+----------------------------------------------------------------
OP_DUP                                                          | 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
OP_HASH160                                                      | 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649...
e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e                        |
OP_EQUALVERIFY                                                  |
OP_CHECKSIG                                                     |
#0003 OP_DUP
btcdeb> print
    #0000 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649acb966c1a02200c64da187aa96e92037b11d60ae85fe26950dd64e088d14db2ccd010bb4311a601
    #0001 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
    <<< scriptPubKey >>>
```

```
#0003 OP_DUP
btcdeb> print
    #0000 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649acb966c1a02200c64da187aa96e92037b11d60ae85fe26950dd64e088d14db2ccd010bb4311a601
    #0001 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
    <<< scriptPubKey >>>
 -> #0003 OP_DUP
    #0004 OP_HASH160
    #0005 e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e
    #0006 OP_EQUALVERIFY
    #0007 OP_CHECKSIG
btcdeb> step
               <> PUSH stack 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
script                                                          |                                                                stack
----------------------------------------------------------------+----------------------------------------------------------------
OP_HASH160                                                      | 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e                        | 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
OP_EQUALVERIFY                                                  | 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649...
OP_CHECKSIG                                                     |
#0004 OP_HASH160
btcdeb> print
    #0000 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649acb966c1a02200c64da187aa96e92037b11d60ae85fe26950dd64e088d14db2ccd010bb4311a601
    #0001 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
    <<< scriptPubKey >>>
    #0003 OP_DUP
 -> #0004 OP_HASH160
    #0005 e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e
    #0006 OP_EQUALVERIFY
    #0007 OP_CHECKSIG
btcdeb> step
               <> POP  stack
               <> PUSH stack e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e
script                                                          |                                                                stack
----------------------------------------------------------------+----------------------------------------------------------------
e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e                        |                                 e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e
OP_EQUALVERIFY                                                  | 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
OP_CHECKSIG                                                     | 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649...
#0005 e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e
btcdeb> print
    #0000 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649acb966c1a02200c64da187aa96e92037b11d60ae85fe26950dd64e088d14db2ccd010bb4311a601
    #0001 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
    <<< scriptPubKey >>>
    #0003 OP_DUP
```

```
btcdeb> print
    #0000 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649acb966c1a02200c64da187aa96e92037b11d60ae85fe26950dd64e088d14db2ccd010bb4311a601
    #0001 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
    <<< scriptPubKey >>>
    #0003 OP_DUP
    #0004 OP_HASH160
 -> #0005 e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e
    #0006 OP_EQUALVERIFY
    #0007 OP_CHECKSIG
btcdeb> step
               <> PUSH stack e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e
script                                                          |                                                                stack
----------------------------------------------------------------+----------------------------------------------------------------
OP_EQUALVERIFY                                                  |                         e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e
OP_CHECKSIG                                                     |                         e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e
                                                                | 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
                                                                | 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649...
#0006 OP_EQUALVERIFY
btcdeb> print
    #0000 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649acb966c1a02200c64da187aa96e92037b11d60ae85fe26950dd64e088d14db2ccd010bb4311a601
    #0001 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
    <<< scriptPubKey >>>
    #0003 OP_DUP
    #0004 OP_HASH160
    #0005 e2db3f359ce01b1db3b69eb5a9f631f38af5ea1e
 -> #0006 OP_EQUALVERIFY
    #0007 OP_CHECKSIG
btcdeb> step
               <> POP  stack
               <> POP  stack
               <> PUSH stack 01
               <> POP  stack
script                                                          |                                                                stack
----------------------------------------------------------------+----------------------------------------------------------------
OP_CHECKSIG                                                     | 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
                                                                | 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649...

#0007 OP_CHECKSIG
btcdeb> print
    #0000 30440220487af36e6e36125c07dd09b8b65fe64c6af686e51c656fc4577b649acb966c1a02200c64da187aa96e92037b11d60ae85fe26950dd64e088d14db2ccd010bb4311a601
    #0001 03a1f80d1fdf46751ac19be52c30adfc62b681d7a625e35b93f525e50eeebd7d4a
    <<< scriptPubKey >>>
    #0003 OP_DUP
    #0004 OP_HASH160
```

P2SH-SegWit Address Transactions:

Addresses generated are
SegWit Address A': 2MwbY56NSb27hDgoy6MArCSNDSjZ54gMvfG
SegWit Address B': 2NA5G4fvdTpkELh4R75G3GfYNhTG5YHeLS9
SegWit Address C': 2MxgETHK7EMk1zhMhj8NZbSf6ZMtg7pXQdU

Initially, A is given 1 BTC.
Then, 0.5 BTC is sent from A to B, with a fee of 0.0001 BTC, leaving A with 0.4999 BTC.
TXID for A to B -
6aeb004b08abccaa83711adffd47421acd55b81305ac2df27bed8c35187a4c8c

Thus, B has one UTXO containing 0.5 BTC.
Like in the Legacy Address case, here also the UTXO refers to the TXID for A to B and has the address of B along with 1 confirmation, making this UTXO spendable provided the correct response script is provided to the challenge script (scriptPubKey mentioned in the UTXO). Thus, when B spends this UTXO, it uses the previous transaction (from A to B).

Now, 0.25 BTC is sent from B to C along with a fee of 0.0001 BTC, leaving B with 0.2499 BTC. The following command refers to this transaction.

createrawtransaction [[{"txid":
"6aeb004b08abccaa83711adffd47421acd55b81305ac2df27bed8c35187a4c8c", "vout": 0}],
{"2MxgETHK7EMk1zhMhj8NZbSf6ZMtg7pXQdU": 0.25,
*"2NA5*G4fvdTpkELh4R75G3GfYNhTG5YHeLS9": 0.2499}]

TXID for B to C -
502e5ed2dd0d4ceb2bc3977c06664befca03cbb86bdc9ba37f24919562ca5834

Decoded Script for A to B -
OP_HASH160 b897b61cb7cdb951b2a61e0fd8b49ea163c4ef67 OP_EQUAL

Decoded Script for B to C -
OP_HASH160 3b936aa1c056f0418b0ce445d26975977a490780 OP_EQUAL

Procedure:
In P2SH-SegWit address transactions, the challenge script and valid response script structures are as follows:
Challenge Script: OP_HASH160 <Redeem Script Hash> OP_EQUAL
Response Script: <Signature> <Public Key> <Redeem Script>

First, the response script is pushed on the stack and then the challenge script is placed on the stack. Then, one by one the operations are executed

1. Redeem Script is hashed and compared with the hash in challenge script using OP_EQUAL
2. If they are equal, then it is checked if the signature is valid using the public key. If true, then the transaction is valid.

Screenshots:

Decoded Scripts -

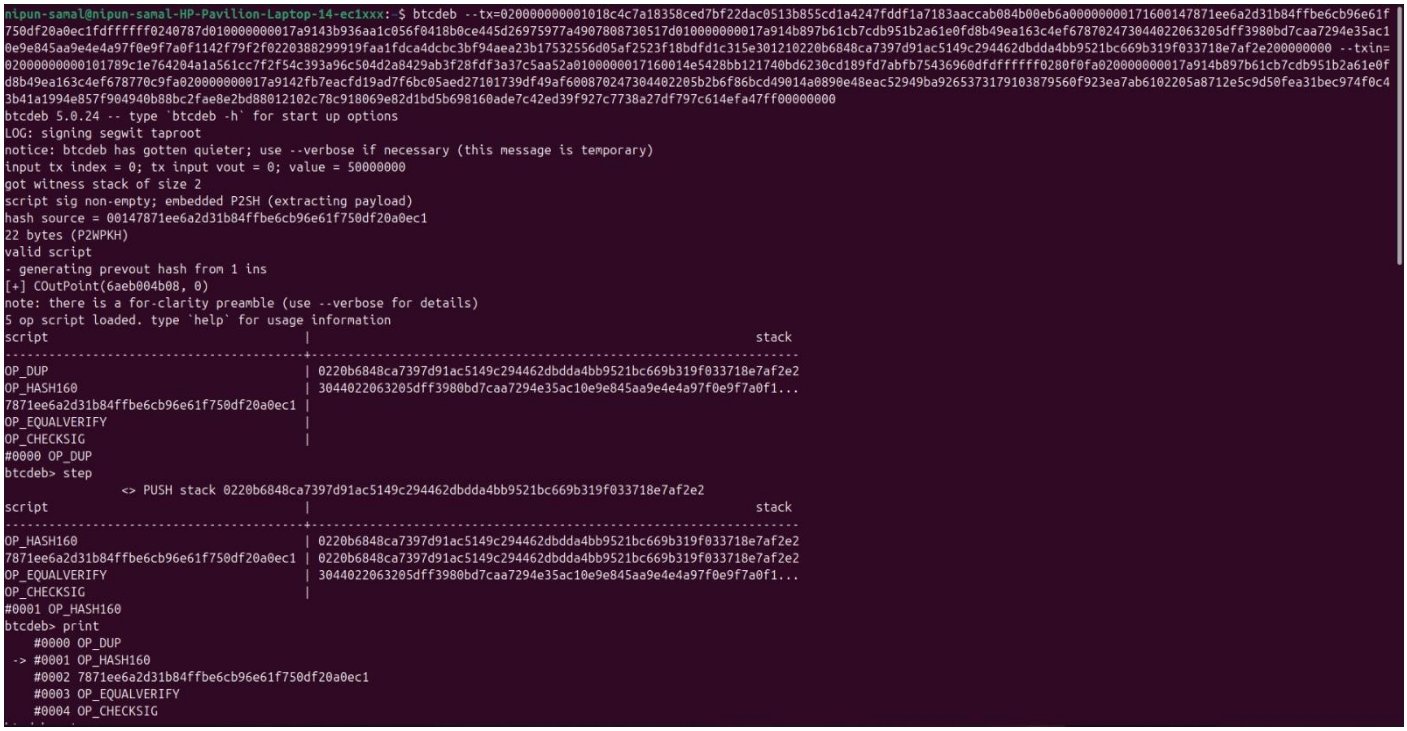
Transaction from A' to B' -


```
DEBUG:BitcoinRPC:<-16- {"txid": "6aeb004b08abccaa83711adffd47421acd55b81305ac2df27bed8c35187a4c8c", "hash":
"a4103189bb2a6ae3bdbf9e873bce5152e24c116e4c3af36baafb885c7fda265b", "version": 2, "size": 247, "vsize": 166, "weight": 661, "locktime": 0,
"vin": [{"txid": "2aa55a7ca3f3fd283fab29842a4d506ca993c3542f7fcc61a5a10442761e9c78", "vout": 1, "scriptSig": {"asm":
"0014e5428bb121740bd6230cd189fd7abfb75436960d", "hex": "160014e5428bb121740bd6230cd189fd7abfb75436960d"}, "txinwitness":
["304402205b2b6f86bcd49014a0890e48eac52949ba9265373179103879560f923ea7ab6102205a8712e5c9d50fea31bec974f0c43b41a1994e857f904940b88bc2fae8e2bd8
801", "02c78c918069e82d1bd5b698160ade7c42ed39f927c7738a27df797c614efa47ff"], "sequence": 4294967293}], "vout": [{"value": 0.5, "n": 0,
"scriptPubKey": {"asm": "OP_HASH160 b897b61cb7cdb951b2a61e0fd8b49ea163c4ef67 OP_EQUAL", "desc": "addr(2NA5G4fvdTpkELh4R75G3GfYNhTG5YHeLS9)
#c9zffurh", "hex": "a914b897b61cb7cdb951b2a61e0fd8b49ea163c4ef6787", "address": "2NA5G4fvdTpkELh4R75G3GfYNhTG5YHeLS9", "type":
"scripthash"}}, {"value": 0.4999, "n": 1, "scriptPubKey": {"asm": "OP_HASH160 2fb7eacfd19ad7f6bc05aed27101739df49af600 OP_EQUAL", "desc":
"addr(2MwbY56NSb27hDgoy6MArCSNDSjZ54gMvfG)#sp6js4zh", "hex": "a9142fb7eacfd19ad7f6bc05aed27101739df49af60087", "address":
"2MwbY56NSb27hDgoy6MArCSNDSjZ54gMvfG", "type": "scripthash"}}], "hex":
"02000000000101789c1e764204a1a561cc7f2f54c393a96c504d2a8429ab3f28fdf3a37c5aa52a0100000017160014e5428bb121740bd6230cd189fd7abfb75436960dfdffff
ff0280f0fa020000000017a914b897b61cb7cdb951b2a61e0fd8b49ea163c4ef678770c9fa020000000017a9142fb7eacfd19ad7f6bc05aed27101739df49af60087024730440
2205b2b6f86bcd49014a0890e48eac52949ba9265373179103879560f923ea7ab6102205a8712e5c9d50fea31bec974f0c43b41a1994e857f904940b88bc2fae8e2bd88012102
c78c918069e82d1bd5b698160ade7c42ed39f927c7738a27df797c614efa47ff00000000", "blockhash":
"0fa2ac2204992ef2217c22e0090078f883ecc812785ec0115f70485551857ab4", "confirmations": 1, "time": 1742725707, "blocktime": 1742725707}
```

Transaction from B’ to C’ -


```
DEBUG:BitcoinRPC:<-24- {"txid": "502e5ed2dd0d4ceb2bc3977c06664befca03cbb86bdc9ba37f24919562ca5834", "hash":
"bef8e2552f943d7ae62a9a12ede2282c6330c35f0409b2e6594003c8fd6f2dc7", "version": 2, "size": 247, "vsize": 166, "weight": 661, "locktime": 0,
"vin": [{"txid": "6aeb004b08abccaa83711adffd47421acd55b81305ac2df27bed8c35187a4c8c", "vout": 0, "scriptSig": {"asm":
"00147871ee6a2d31b84ffbe6cb96e61f750df20a0ec1", "hex": "1600147871ee6a2d31b84ffbe6cb96e61f750df20a0ec1"}, "txinwitness":
["3044022063205dff3980bd7caa7294e35ac10e9e845aa9e4e4a97f0e9f7a0f1142f79f2f0220388299919faa1fdca4dcbc3bf94aea23b17532556d05af2523f18bdfd1c315e
301", "0220b6848ca7397d91ac5149c294462dbdda4bb9521bc669b319f033718e7af2e2"], "sequence": 4294967293}], "vout": [{"value": 0.25, "n": 0,
"scriptPubKey": {"asm": "OP_HASH160 3b936aa1c056f0418b0ce445d26975977a490780 OP_EQUAL", "desc": "addr(2MxgETHK7EMk1zhMhj8NZbSf6ZMtg7pXQdU)
#8wdzxwgc", "hex": "a9143b936aa1c056f0418b0ce445d26975977a49078087", "address": "2MxgETHK7EMk1zhMhj8NZbSf6ZMtg7pXQdU", "type":
"scripthash"}}, {"value": 0.2499, "n": 1, "scriptPubKey": {"asm": "OP_HASH160 b897b61cb7cdb951b2a61e0fd8b49ea163c4ef67 OP_EQUAL", "desc":
"addr(2NA5G4fvdTpkELh4R75G3GfYNhTG5YHeLS9)#c9zffurh", "hex": "a914b897b61cb7cdb951b2a61e0fd8b49ea163c4ef6787", "address":
"2NA5G4fvdTpkELh4R75G3GfYNhTG5YHeLS9", "type": "scripthash"}}], "hex":
"020000000001018c4c7a18358ced7bf22dac0513b855cd1a4247fddf1a7183aaccab084b00eb6a0000000017160014787 1ee6a2d31b84ffbe6cb96e61f750df20a0ec1fdfffff
ff0240787d010000000017a9143b936aa1c056f0418b0ce445d26975977a4907808730517d010000000017a914b897b61cb7cdb951b2a61e0fd8b49ea163c4ef6787024730440
22063205dff3980bd7caa7294e35ac10e9e845aa9e4e4a97f0e9f7a0f1142f79f2f0220388299919faa1fdca4dcbc3bf94aea23b17532556d05af2523f18bdfd1c315e3012102
20b6848ca7397d91ac5149c294462dbdda4bb9521bc669b319f033718e7af2e200000000", "blockhash":
"0293fe27384a7cd5dcb6c39c8fcab3bd5fe64786dc53840ede5af370c93b7267", "confirmations": 1, "time": 1742725707, "blocktime": 1742725707}
```


Bitcoin Debugger Steps -



```
#0001 OP_HASH160
btcdeb> print
    #0000 OP_DUP
 -> #0001 OP_HASH160
    #0002 7871ee6a2d31b84ffbe6cb96e61f750df20a0ec1
    #0003 OP_EQUALVERIFY
    #0004 OP_CHECKSIG
btcdeb> step
               <> POP  stack
               <> PUSH stack 7871ee6a2d31b84ffbe6cb96e61f750df20a0ec1
script                                 |                                                                stack
---------------------------------------+----------------------------------------------------------------------
7871ee6a2d31b84ffbe6cb96e61f750df20a0ec1 |                          7871ee6a2d31b84ffbe6cb96e61f750df20a0ec1
OP_EQUALVERIFY                         | 0220b6848ca7397d91ac5149c294462dbdda4bb9521bc669b319f033718e7af2e2
OP_CHECKSIG                            | 3044022063205dff3980bd7caa7294e35ac10e9e845aa9e4e4a97f0e9f7a0f1...
#0002 7871ee6a2d31b84ffbe6cb96e61f750df20a0ec1
btcdeb> print
    #0000 OP_DUP
    #0001 OP_HASH160
 -> #0002 7871ee6a2d31b84ffbe6cb96e61f750df20a0ec1
    #0003 OP_EQUALVERIFY
    #0004 OP_CHECKSIG
btcdeb> step
               <> PUSH stack 7871ee6a2d31b84ffbe6cb96e61f750df20a0ec1
script                                 |                                                                stack
---------------------------------------+----------------------------------------------------------------------
OP_EQUALVERIFY                         |                          7871ee6a2d31b84ffbe6cb96e61f750df20a0ec1
OP_CHECKSIG                            |                          7871ee6a2d31b84ffbe6cb96e61f750df20a0ec1
                                       | 0220b6848ca7397d91ac5149c294462dbdda4bb9521bc669b319f033718e7af2e2
                                       | 3044022063205dff3980bd7caa7294e35ac10e9e845aa9e4e4a97f0e9f7a0f1...
#0003 OP_EQUALVERIFY
btcdeb> print
    #0000 OP_DUP
    #0001 OP_HASH160
    #0002 7871ee6a2d31b84ffbe6cb96e61f750df20a0ec1
 -> #0003 OP_EQUALVERIFY
    #0004 OP_CHECKSIG
btcdeb> step
               <> POP  stack
               <> POP  stack
               <> PUSH stack 01
               <> POP  stack
```

```
               <> POP  stack
               <> POP  stack
               <> PUSH stack 01
               <> POP  stack
script                                 |                                                                stack
---------------------------------------+----------------------------------------------------------------------
OP_CHECKSIG                            | 0220b6848ca7397d91ac5149c294462dbdda4bb9521bc669b319f033718e7af2e2
                                       | 3044022063205dff3980bd7caa7294e35ac10e9e845aa9e4e4a97f0e9f7a0f1...
#0004 OP_CHECKSIG
btcdeb> print
    #0000 OP_DUP
    #0001 OP_HASH160
    #0002 7871ee6a2d31b84ffbe6cb96e61f750df20a0ec1
    #0003 OP_EQUALVERIFY
 -> #0004 OP_CHECKSIG
btcdeb> step
EvalChecksig() sigversion=1
Eval Checksig Pre-Tapscript
GenericTransactionSignatureChecker::CheckECDSASignature(71 len sig, 33 len pubkey, sigversion=1)
  sig         = 3044022063205dff3980bd7caa7294e35ac10e9e845aa9e4e4a97f0e9f7a0f1142f79f2f0220388299919faa1fdca4dcbc3bf94aea23b17532556d05af2523f18bdfd1c315e301
  pub key     = 0220b6848ca7397d91ac5149c294462dbdda4bb9521bc669b319f033718e7af2e2
  script code = 76a9147871ee6a2d31b84ffbe6cb96e61f750df20a0ec188ac
  hash type   = 01 (SIGHASH_ALL)
SignatureHash(nIn=0, nHashType=01, amount=50000000)
- sigversion == SIGVERSION_WITNESS_V0
  sighash     = 8690f59b77ed31c3e9f8ca17de4225f569222555771589050463a6cf2884eb62
  pubkey.VerifyECDSASignature(sig=3044022063205dff3980bd7caa7294e35ac10e9e845aa9e4e4a97f0e9f7a0f1142f79f2f0220388299919faa1fdca4dcbc3bf94aea23b17532556d05af2523f18bdfd1c315e3, sighash=8690f5
9b77ed31c3e9f8ca17de4225f569222555771589050463a6cf2884eb62):
  result: success
               <> POP  stack
               <> POP  stack
               <> PUSH stack 01
script                                 |                                                                stack
---------------------------------------+----------------------------------------------------------------------
                                       |                                                                   01
btcdeb> print
    #0000 OP_DUP
    #0001 OP_HASH160
    #0002 7871ee6a2d31b84ffbe6cb96e61f750df20a0ec1
    #0003 OP_EQUALVERIFY
    #0004 OP_CHECKSIG
btcdeb>
```

Comparing Legacy and P2SH-SegWit Address Transactions:

1. **Size:**
    a. P2PKH - 119 bytes or 119 vbytes or 476 weight units
    b. P2SH-SegWit - 247 bytes or 166 vbytes or 661 weight unit.

The higher size of P2SH-SegWit transactions compared to P2PKH transactions is primarily due to the following reasons:

1. Extra Redeem Script in P2SH

- P2SH (Pay-to-Script-Hash) transactions include a **redeem script**, which contains the script that unlocks the funds.
- This script is **not present in standard P2PKH transactions**, leading to additional bytes.

2. Segregated Witness Data

- SegWit transactions store signatures (witness data) in a separate **witness field** rather than inside the main transaction structure.
- This adds additional fields, which increase the overall transaction size.

3. Script Complexity

- A P2PKH transaction uses a **simple locking script** (standard public key hash).
- In contrast, **P2SH-SegWit transactions** require both:
    1. The redeem script (which itself contains a script).
    2. The witness data (which holds the actual signatures).

However, if we use Bech32 addresses, then the size would be lower than legacy addresses.

Bech32 (Native SegWit) addresses (P2WPKH, P2WSH) are lighter compared to **P2SH-SegWit** transactions.

Why Are SegWit Transactions Smaller?

1. **Signature Data Moved to Witness Field** → Reduces main transaction size.
2. **Witness Data is Discounted** → 1 byte = 1 weight unit (instead of 4), lowering virtual size.
3. **No Redeem Script in Bech32** → More efficient than P2SH-SegWit.

Benefits of SegWit Transactions

Lower Fees → Uses less virtual space, reducing transaction costs.
Increases Block Capacity → More transactions fit in a block.
Prevents Malleability → Enables secure Layer 2 solutions like **Lightning Network**.
Future Upgrades → Supports **Taproot** & **Schnorr Signatures** for better privacy & efficiency.

💡 **Conclusion:** SegWit makes Bitcoin **cheaper, faster, and more scalable** without increasing block size.

2. **Script Structures:**
   As mentioned above, the structures of P2PKH scripts and P2SH-SegWit scripts are as follows:

   P2PKH -

   Challenge Script: OP_DUP OP_HASH160 <Public Key Hash> OP_EQUALVERIFY OP_CHECKSIG
   Response Script: <Signature> <Public Key>

   P2SH-SegWit -

   Challenge Script: OP_HASH160 <Redeem Script Hash> OP_EQUAL
   Response Script: <Signature> <Public Key> <Redeem Script>