ASSIGNMENT 3 - BITCOIN SCRIPTING

CS 216 - INTRODUCTION TO BLOCKCHAIN

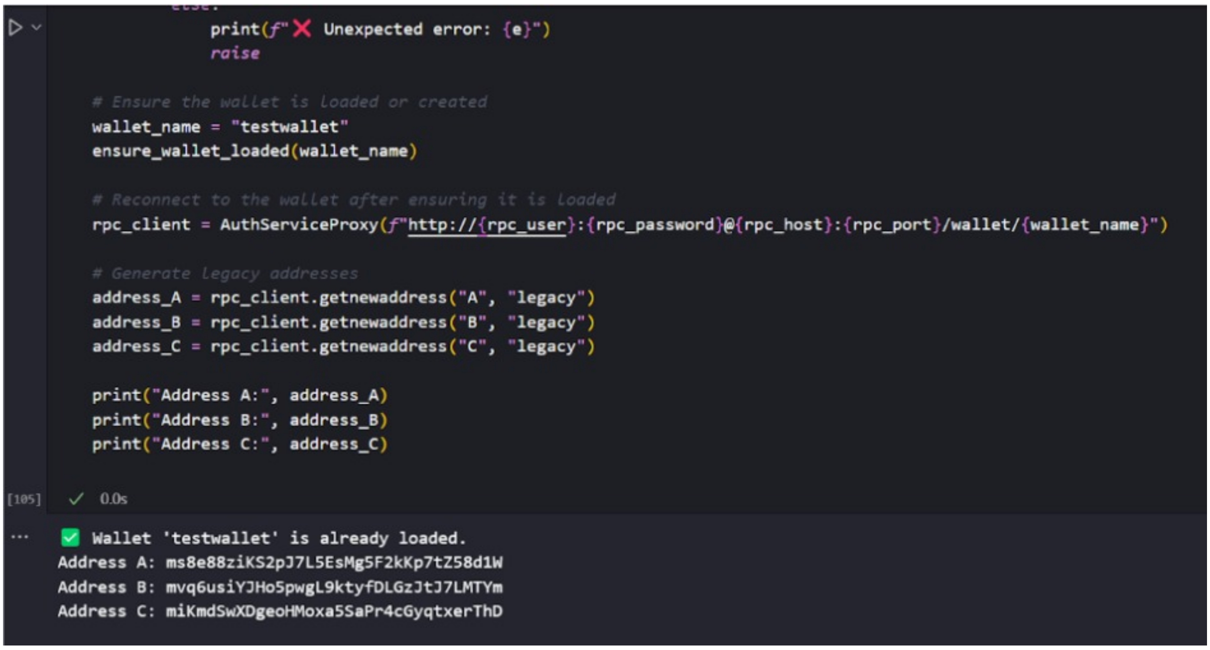
Team
Nidarsana M (230004031)
Nandini Kumari (230001056)
Tripti Anand (230001078)

1 Legacy (P2PKH) Transactions

1.1 Workflow Description

Address Generation: Three legacy addresses A, B, and C were generated using `bitcoind`.

```
Address A: ms8e8zikKS2p7JL5EsMg5Fz8Tk7pZ58d1W
Address B: mvq6usiYJHo5pwgL9ktyfDLGzJtJ7LMTYm
Address C: miKmdSwXDgeoHMoxa5SaPr4cGyqtxerThD
```

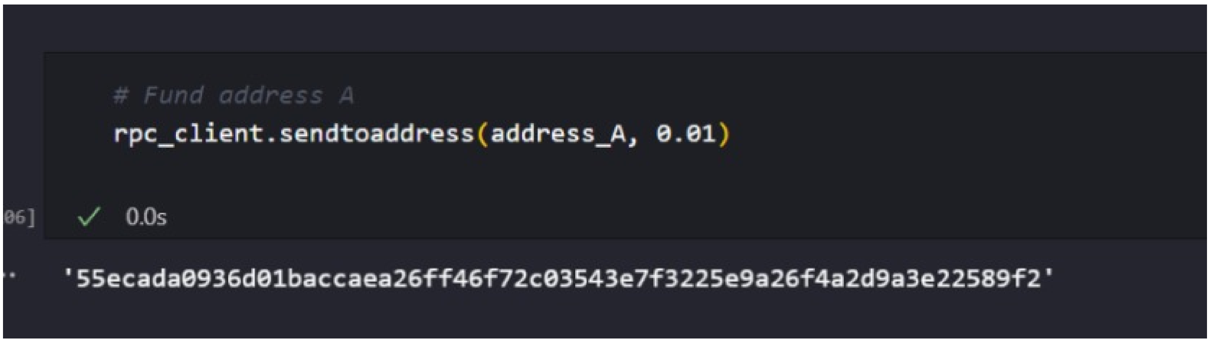


```
        else:
            print(f"❌ Unexpected error: {e}")
            raise

# Ensure the wallet is loaded or created
wallet_name = "testwallet"
ensure_wallet_loaded(wallet_name)

# Reconnect to the wallet after ensuring it is loaded
rpc_client = AuthServiceProxy(f"http://{rpc_user}:{rpc_password}@{rpc_host}:{rpc_port}/wallet/{wallet_name}")

# Generate legacy addresses
address_A = rpc_client.getnewaddress("A", "legacy")
address_B = rpc_client.getnewaddress("B", "legacy")
address_C = rpc_client.getnewaddress("C", "legacy")

print("Address A:", address_A)
print("Address B:", address_B)
print("Address C:", address_C)
```

[105] ✓ 0.0s

```
✅ Wallet 'testwallet' is already loaded.
Address A: ms8e88ziKS2pJ7L5EsMg5F2kKp7tZ58d1W
Address B: mvq6usiYJHo5pwgL9ktyfDLGzJtJ7LMTYm
Address C: miKmdSwXDgeoHMoxa5SaPr4cGyqtxerThD
```

Funding Address A: Address A was funded using the `sendtoaddress` command.



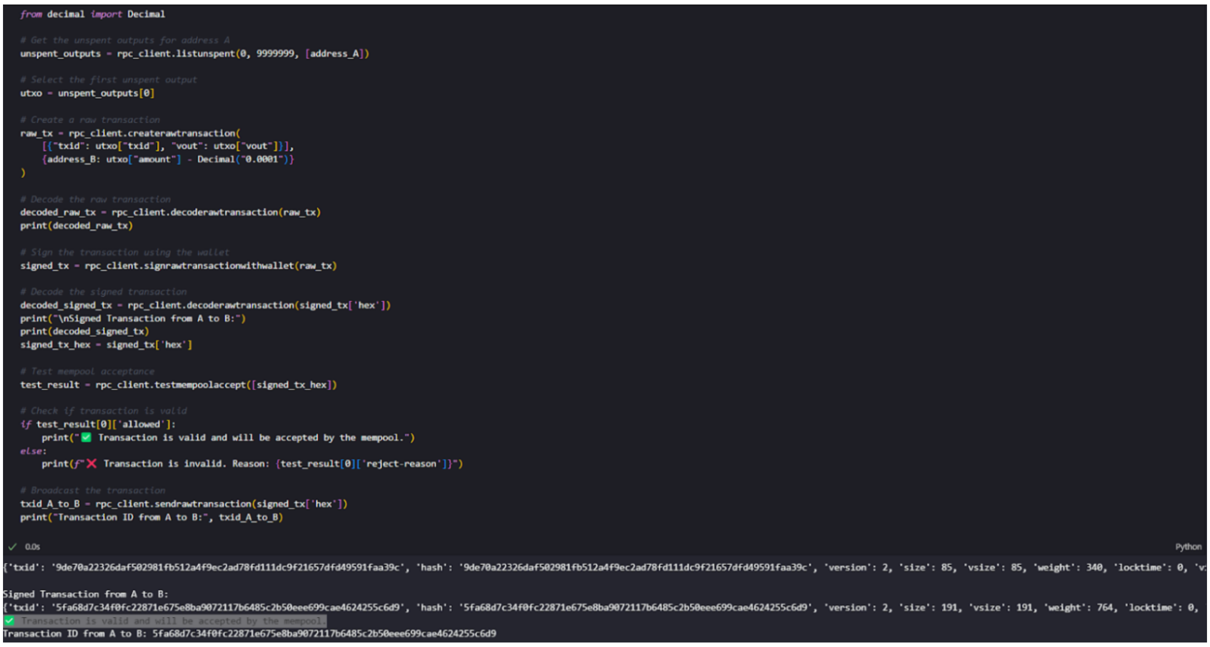
```
# Fund address A
rpc_client.sendtoaddress(address_A, 0.01)
```

06] ✓ 0.0s

```
'55ecada0936d01baccaea26ff46f72c03543e7f3225e9a26f4a2d9a3e22589f2'
```

Transaction from A to B: A raw transaction was created from A to B, signed, and broadcasted.

```
Transaction ID from A to B:
    5fa68d7c34f0fc22871e675e8ba9072117b6485c2b50eee699cae4624255c6d9
```

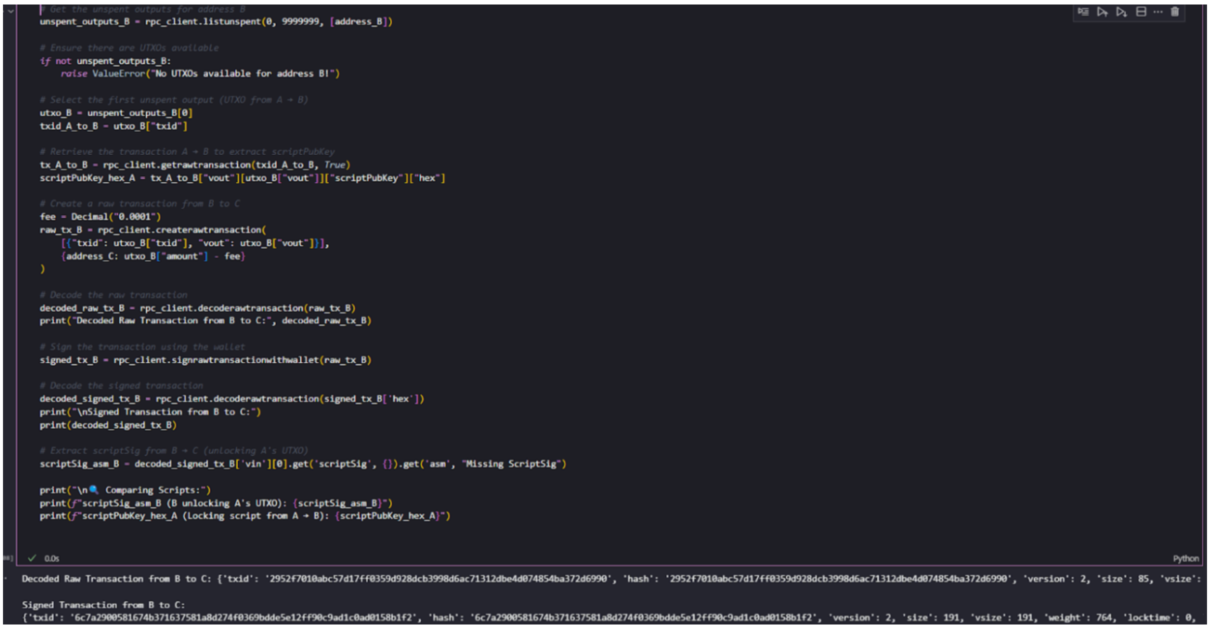


```
from decimal import Decimal

# Get the unspent outputs for address A
unspent_outputs = rpc_client.listunspent(0, 9999999, [address_A])

# Select the first unspent output
utxo = unspent_outputs[0]

# Create a raw transaction
raw_tx = rpc_client.createrawtransaction(
    [{"txid": utxo["txid"], "vout": utxo["vout"]}],
    {address_B: utxo["amount"] - Decimal("0.0001")}
)

# Decode the raw transaction
decoded_raw_tx = rpc_client.decoderawtransaction(raw_tx)
print(decoded_raw_tx)

# Sign the transaction using the wallet
signed_tx = rpc_client.signrawtransactionwithwallet(raw_tx)

# Decode the signed transaction
decoded_signed_tx = rpc_client.decoderawtransaction(signed_tx['hex'])
print("\nSigned Transaction from A to B:")
print(decoded_signed_tx)
signed_tx_hex = signed_tx['hex']

# Test mempool acceptance
test_result = rpc_client.testmempoolaccept([signed_tx_hex])

# Check if transaction is valid
if test_result[0]['allowed']:
    print("✅ Transaction is valid and will be accepted by the mempool.")
else:
    print(f"❌ Transaction is invalid. Reason: {test_result[0]['reject-reason']}")

# Broadcast the transaction
txid_A_to_B = rpc_client.sendrawtransaction(signed_tx['hex'])
print("Transaction ID from A to B:", txid_A_to_B)
```

```
{'txid': '9de70a22326daf502981fb512a4f9ec2ad78fd111dc9f21657dfd49591faa39c', 'hash': '9de70a22326daf502981fb512a4f9ec2ad78fd111dc9f21657dfd49591faa39c', 'version': 2, 'size': 85, 'vsize': 85, 'weight': 340, 'locktime': 0, 'v

Signed Transaction from A to B:
{'txid': '5fa68d7c34f0fc22871e675e8ba9072117b6485c2b50eee699cae4624255c6d9', 'hash': '5fa68d7c34f0fc22871e675e8ba9072117b6485c2b50eee699cae4624255c6d9', 'version': 2, 'size': 191, 'vsize': 191, 'weight': 764, 'locktime': 0,
✅ Transaction is valid and will be accepted by the mempool.
Transaction ID from A to B: 5fa68d7c34f0fc22871e675e8ba9072117b6485c2b50eee699cae4624255c6d9
```

Transaction from B to C: The UTXO from the previous transaction was used to create a transaction from B to C.

```
Transaction ID from B to C:
    6c7a2908581674b37163758f1a80274f06369bdde5e12ff09c9a1cd0ad01581f2
```



```
# Get the unspent outputs for address B
unspent_outputs_B = rpc_client.listunspent(0, 9999999, [address_B])

# Ensure there are UTXOs available
if not unspent_outputs_B:
    raise ValueError("No UTXOs available for address B!")

# Select the first unspent output (UTXO from A → B)
utxo_B = unspent_outputs_B[0]
txid_A_to_B = utxo_B["txid"]

# Retrieve the transaction A → B to extract scriptPubKey
tx_A_to_B = rpc_client.getrawtransaction(txid_A_to_B, True)
scriptPubKey_hex_A = tx_A_to_B["vout"][utxo_B["vout"]]["scriptPubKey"]["hex"]

# Create a raw transaction from B to C
fee = Decimal("0.0001")
raw_tx_B = rpc_client.createrawtransaction(
    [{"txid": utxo_B["txid"], "vout": utxo_B["vout"]}],
    {address_C: utxo_B["amount"] - fee}
)

# Decode the raw transaction
decoded_raw_tx_B = rpc_client.decoderawtransaction(raw_tx_B)
print("Decoded Raw Transaction from B to C:", decoded_raw_tx_B)

# Sign the transaction using the wallet
signed_tx_B = rpc_client.signrawtransactionwithwallet(raw_tx_B)

# Decode the signed transaction
decoded_signed_tx_B = rpc_client.decoderawtransaction(signed_tx_B['hex'])
print("\nSigned Transaction from B to C:")
print(decoded_signed_tx_B)

# Extract scriptSig from B → C (unlocking A's UTXO)
scriptSig_asm_B = decoded_signed_tx_B['vin'][0].get('scriptSig', {}).get('asm', "Missing ScriptSig")

print("\n🔍 Comparing Scripts:")
print(f"scriptSig_asm_B (B unlocking A's UTXO): {scriptSig_asm_B}")
print(f"scriptPubKey_hex_A (Locking script from A → B): {scriptPubKey_hex_A}")
```

```
Decoded Raw Transaction from B to C: {'txid': '2952f7010abc57d17ff0359d928dcb3998d6ac71312dbe4d074854ba372d6990', 'hash': '2952f7010abc57d17ff0359d928dcb3998d6ac71312dbe4d074854ba372d6990', 'version': 2, 'size': 85, 'vsize':

Signed Transaction from B to C:
{'txid': '6c7a2900581674b371637581a8d274f0369bdde5e12ff90c9ad1c0ad0158b1f2', 'hash': '6c7a2900581674b371637581a8d274f0369bdde5e12ff90c9ad1c0ad0158b1f2', 'version': 2, 'size': 191, 'vsize': 191, 'weight': 764, 'locktime': 0,
```

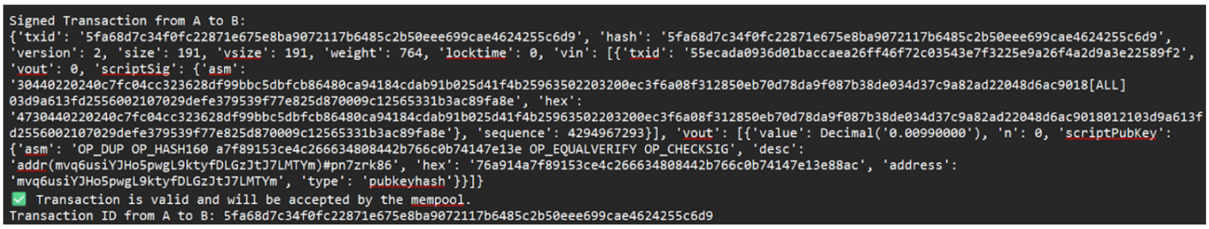
2 Decoded Scripts

2.1 ScriptPubKey for Address B

The locking script for address B was decoded to understand how it locks the output.

2.2 Signed Transaction from A to B

```
{
  "txid": "5fa68d7c34f0fc22871e675e8ba9072117b6485c2b50eee699cae4624255c6d9",
  "version": 2,
  "size": 191,
  "vsize": 191,
  "weight": 764,
  "locktime": 0,
  "vin": [
    {
      "txid": "55ecada0936d01baccaea26ff46f72c03543e7f3225e9a26f4a2d9a3e22589f2",
      "vout": 0,
      "scriptSig": {
        "asm": "3044... [ALL] 03d9...",
        "hex": "4730..."
      },
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 0.00990000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 a7f8... OP_CHECKSIG",
        "hex": "76a9...",
        "address": "mvq6usiYJHo5pwgL9ktyfDLGzJtJ7LMTYm",
        "type": "pubkeyhash"
      }
    }
  ]
}
```



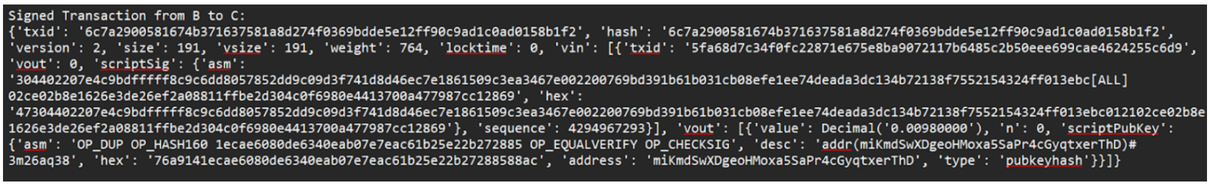
```
Signed Transaction from A to B:
{'txid': '5fa68d7c34f0fc22871e675e8ba9072117b6485c2b50eee699cae4624255c6d9', 'hash': '5fa68d7c34f0fc22871e675e8ba9072117b6485c2b50eee699cae4624255c6d9',
'version': 2, 'size': 191, 'vsize': 191, 'weight': 764, 'locktime': 0, 'vin': [{'txid': '55ecada0936d01baccaea26ff46f72c03543e7f3225e9a26f4a2d9a3e22589f2',
'vout': 0, 'scriptSig': {'asm':
'30440220240c7fc04cc323628df99bbc5dbfcb86480ca94184cdab91b025d41f4b25963502203200ec3f6a08f312850eb70d78da9f087b38de034d37c9a82ad22048d6ac9018[ALL]
03d9a613fd2556002107029defe379539f77e825d870009c12565331b3ac89fa8e', 'hex':
'4730440220240c7fc04cc323628df99bbc5dbfcb86480ca94184cdab91b025d41f4b25963502203200ec3f6a08f312850eb70d78da9f087b38de034d37c9a82ad22048d6ac9018012103d9a613f
d2556002107029defe379539f77e825d870009c12565331b3ac89fa8e'}, 'sequence': 4294967293}], 'vout': [{'value': Decimal('0.00990000'), 'n': 0, 'scriptPubKey':
{'asm': 'OP_DUP OP_HASH160 a7f89153ce4c266634808442b766c0b74147e13e OP_EQUALVERIFY OP_CHECKSIG', 'desc':
'addr(mvq6usiYJHo5pwgL9ktyfDLGzJtJ7LMTYm)#pn7zrk86', 'hex': '76a914a7f89153ce4c266634808442b766c0b74147e13e88ac', 'address':
'mvq6usiYJHo5pwgL9ktyfDLGzJtJ7LMTYm', 'type': 'pubkeyhash'}}]}
✅ Transaction is valid and will be accepted by the mempool.
Transaction ID from A to B: 5fa68d7c34f0fc22871e675e8ba9072117b6485c2b50eee699cae4624255c6d9
```

2.3 ScriptSig for Transaction from B to C

The unlocking script was decoded to see how it unlocks the output.

2.4 Signed Transaction from B to C

```
{
  "txid": "6c7a2900581674b371637581a8d274f0369bdde5e12ff90c9ad1c0ad0158b1f2",
  "version": 2,
  "size": 191,
  "vsize": 191,
  "weight": 764,
  "locktime": 0,
  "vin": [
    {
      "txid": "5fa68d7c34f0fc22871e675e8ba9072117b6485c2b50eee699cae4624255c6d9",
      "vout": 0,
      "scriptSig": {
        "asm": "3044... [ALL] 02ce...",
        "hex": "4730..."
      },
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 0.00980000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 1eca... OP_CHECKSIG",
        "hex": "76a9...",
        "address": "miKmdSwXDgeoHMoxa5SaPr4cGyqtxerThD",
        "type": "pubkeyhash"
      }
    }
  ]
}
```



```
Signed Transaction from B to C:
{'txid': '6c7a2900581674b371637581a8d274f0369bdde5e12ff90c9ad1c0ad0158b1f2', 'hash': '6c7a2900581674b371637581a8d274f0369bdde5e12ff90c9ad1c0ad0158b1f2',
'version': 2, 'size': 191, 'vsize': 191, 'weight': 764, 'locktime': 0, 'vin': [{'txid': '5fa68d7c34f0fc22871e675e8ba9072117b6485c2b50eee699cae4624255c6d9',
'vout': 0, 'scriptSig': {'asm':
'304402207e4c9bdfffff8c9c6dd8057852dd9c09d3f741d8d46ec7e1861509c3ea3467e002200769bd391b61b031cb08efe1ee74deada3dc134b72138f7552154324ff013ebc[ALL]
02ce02b8e1626e3de26ef2a08811ffbe2d304c0f6980e4413700a477987cc12869', 'hex':
'47304402207e4c9bdfffff8c9c6dd8057852dd9c09d3f741d8d46ec7e1861509c3ea3467e002200769bd391b61b031cb08efe1ee74deada3dc134b72138f7552154324ff013ebc012102ce02b8e
1626e3de26ef2a08811ffbe2d304c0f6980e4413700a477987cc12869'}, 'sequence': 4294967293}], 'vout': [{'value': Decimal('0.00980000'), 'n': 0, 'scriptPubKey':
{'asm': 'OP_DUP OP_HASH160 1ecae6080de6340eab07e7eac61b25e22b272885 OP_EQUALVERIFY OP_CHECKSIG', 'desc': 'addr(miKmdSwXDgeoHMoxa5SaPr4cGyqtxerThD)#
3m26aq38', 'hex': '76a9141ecae6080de6340eab07e7eac61b25e22b27288588ac', 'address': 'miKmdSwXDgeoHMoxa5SaPr4cGyqtxerThD', 'type': 'pubkeyhash'}}]}
```

3 Script Analysis

3.1 Challenge and Response Scripts

To validate the transaction, Bitcoin uses a combination of two scripts: the Challenge Script (scriptPubKey) and the Response Script (scriptSig). The validation process ensures that only the rightful owner of the UTXO can spend it.

- **Challenge Script (scriptPubKey):** This script is embedded in the UTXO and specifies the conditions required to spend it.

  ```
  OP_DUP OP_HASH160 <Public Key Hash> OP_EQUALVERIFY OP_CHECKSIG
  ```

  Explanation:

  OP_DUP Duplicates the top item (the public key) on the stack.

  OP_HASH160 Applies the RIPEMD-160(SHA-256(public key)) hash function to the duplicated public key.

  Public Key Hash A 20-byte hash of the public key stored in the UTXO.

  OP_EQUALVERIFY Compares the computed hash with the stored Public Key Hash. If they do not match, the script fails.

  OP_CHECKSIG Verifies that the provided signature is valid for the given public key.

- **Response Script (scriptSig):** This script is included in the spending transaction and provides the necessary data to unlock the UTXO.

  ```
  <Signature> <Public Key>
  ```

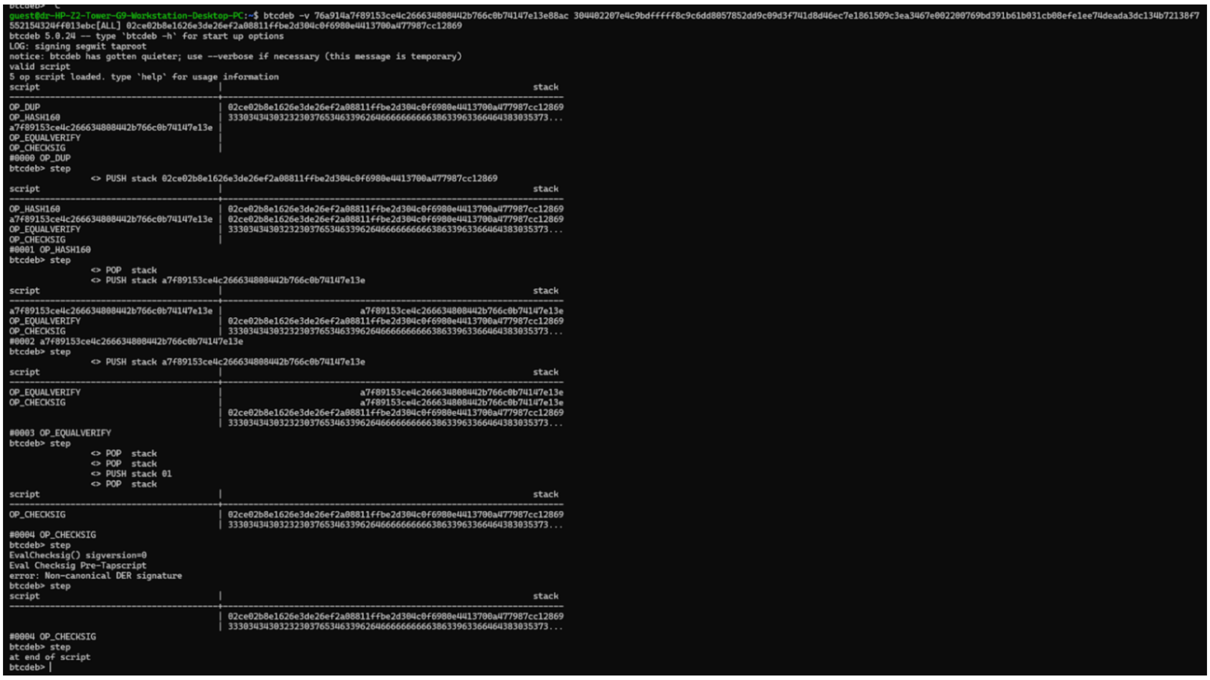
  The public key is pushed onto the stack, and the signature is used to authenticate the transaction.

- **Validation Process:**

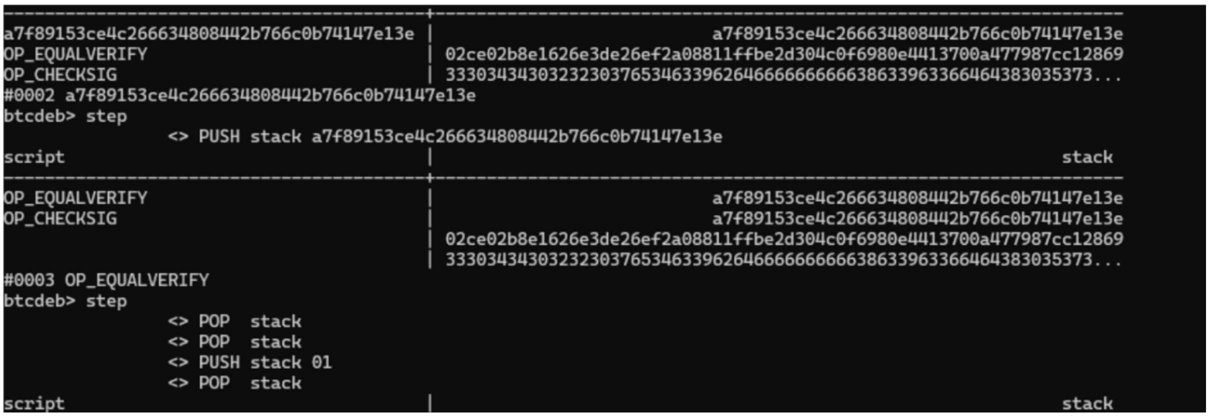
  1. The stack first receives `<Signature>` and `<Public Key>` from `scriptSig`.
  2. The `scriptPubKey` executes:
     (a) `OP_DUP` duplicates the public key.
     (b) `OP_HASH160` hashes the duplicated public key.
     (c) The result is compared to the stored `Public Key Hash` using `OP_EQUALVERIFY`. If they match, execution continues.
     (d) `OP_CHECKSIG` verifies that the provided signature is valid for the given public key and transaction details.
  3. The transaction is valid if all operations complete successfully without errors.

3.2 Bitcoin Debugger Execution

- The challenge and response scripts were executed in the Bitcoin Debugger.



```
btcdeb> ^C
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb -v 76a914a7f89153ce4c266634808442b766c0b74147e13e88ac 304402207e4c9bdfffff8c9c6dd8057852dd9c09d3f741d8d46ec7e1861509c3ea3467e002200769bd391b61b031cb08efe1ee74deada3dc134b72138f7
552154324ff013ebc[ALL] 02ce02b8e1626e3de26ef2a08811ffbe2d304c0f6980e4413700a477987cc12869
btcdeb 5.0.24 -- type `btcdeb -h` for start up options
LOG: signing segwit taproot
notice: btcdeb has gotten quieter; use --verbose if necessary (this message is temporary)
valid script
5 op script loaded. type `help` for usage information
script                                    |                                                             stack
------------------------------------------+-------------------------------------------------------------------
OP_DUP                                    | 02ce02b8e1626e3de26ef2a08811ffbe2d304c0f6980e4413700a477987cc12869
OP_HASH160                                | 333034343032323037653463396264666666666663863396336646438303537 3...
a7f89153ce4c266634808442b766c0b74147e13e |
OP_EQUALVERIFY                            |
OP_CHECKSIG                               |
#0000 OP_DUP
btcdeb> step
                <> PUSH stack 02ce02b8e1626e3de26ef2a08811ffbe2d304c0f6980e4413700a477987cc12869
script                                    |                                                             stack
------------------------------------------+-------------------------------------------------------------------
OP_HASH160                                | 02ce02b8e1626e3de26ef2a08811ffbe2d304c0f6980e4413700a477987cc12869
a7f89153ce4c266634808442b766c0b74147e13e | 02ce02b8e1626e3de26ef2a08811ffbe2d304c0f6980e4413700a477987cc12869
OP_EQUALVERIFY                            | 33303434303232303765346339626466666666666386339633664643830353373...
OP_CHECKSIG                               |
#0001 OP_HASH160
btcdeb> step
                <> POP  stack
                <> PUSH stack a7f89153ce4c266634808442b766c0b74147e13e
script                                    |                                                             stack
------------------------------------------+-------------------------------------------------------------------
a7f89153ce4c266634808442b766c0b74147e13e |                         a7f89153ce4c266634808442b766c0b74147e13e
OP_EQUALVERIFY                            | 02ce02b8e1626e3de26ef2a08811ffbe2d304c0f6980e4413700a477987cc12869
OP_CHECKSIG                               | 33303434303232303765346339626466666666666386339633664643830353373...
#0002 a7f89153ce4c266634808442b766c0b74147e13e
btcdeb> step
                <> PUSH stack a7f89153ce4c266634808442b766c0b74147e13e
script                                    |                                                             stack
------------------------------------------+-------------------------------------------------------------------
OP_EQUALVERIFY                            |                         a7f89153ce4c266634808442b766c0b74147e13e
OP_CHECKSIG                               |                         a7f89153ce4c266634808442b766c0b74147e13e
                                          | 02ce02b8e1626e3de26ef2a08811ffbe2d304c0f6980e4413700a477987cc12869
                                          | 33303434303232303765346339626466666666666386339633664643830353373...
#0003 OP_EQUALVERIFY
btcdeb> step
                <> POP  stack
                <> POP  stack
                <> PUSH stack 01
                <> POP  stack
script                                    |                                                             stack
------------------------------------------+-------------------------------------------------------------------
OP_CHECKSIG                               | 02ce02b8e1626e3de26ef2a08811ffbe2d304c0f6980e4413700a477987cc12869
                                          | 33303434303232303765346339626466666666666386339633664643830353373...
#0004 OP_CHECKSIG
btcdeb> step
EvalChecksig() sigversion=0
Eval Checksig Pre-Tapscript
error: Non-canonical DER signature
btcdeb> step
script                                    |                                                             stack
------------------------------------------+-------------------------------------------------------------------
                                          | 02ce02b8e1626e3de26ef2a08811ffbe2d304c0f6980e4413700a477987cc12869
                                          | 33303434303232303765346339626466666666666386339633664643830353373...
#0004 OP_CHECKSIG
btcdeb> step
at end of script
btcdeb> |
```



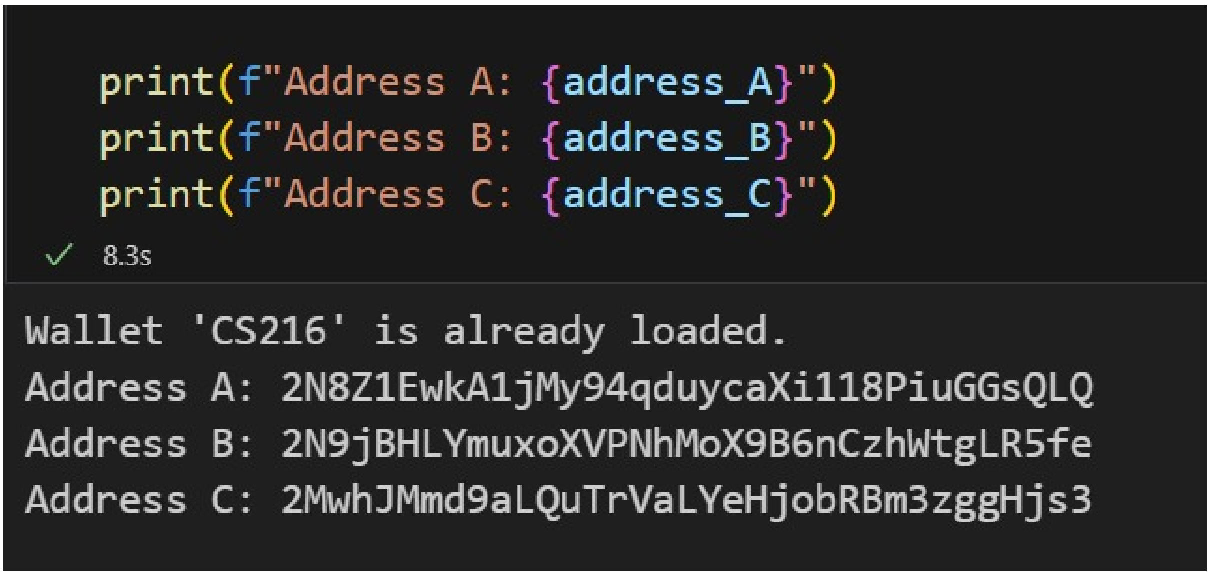
```
------------------------------------------+-------------------------------------------------------------------
a7f89153ce4c266634808442b766c0b74147e13e |                         a7f89153ce4c266634808442b766c0b74147e13e
OP_EQUALVERIFY                            | 02ce02b8e1626e3de26ef2a08811ffbe2d304c0f6980e4413700a477987cc12869
OP_CHECKSIG                               | 33303434303232303765346339626466666666666386339633664643830353373...
#0002 a7f89153ce4c266634808442b766c0b74147e13e
btcdeb> step
                <> PUSH stack a7f89153ce4c266634808442b766c0b74147e13e
script                                    |                                                             stack
------------------------------------------+-------------------------------------------------------------------
OP_EQUALVERIFY                            |                         a7f89153ce4c266634808442b766c0b74147e13e
OP_CHECKSIG                               |                         a7f89153ce4c266634808442b766c0b74147e13e
                                          | 02ce02b8e1626e3de26ef2a08811ffbe2d304c0f6980e4413700a477987cc12869
                                          | 33303434303232303765346339626466666666666386339633664643830353373...

#0003 OP_EQUALVERIFY
btcdeb> step
                <> POP  stack
                <> POP  stack
                <> PUSH stack 01
                <> POP  stack
script                                    |                                                             stack
```

4 SegWit (P2SH-P2WPKH) Transactions

4.1 Workflow Description

Address Generation: Three legacy addresses A, B, and C were generated using `bitcoind`.

```
Address A: 2N8Z1EwkA1jMy94qduycaXi118PiuGGsQLQ
Address B: 2N9jBHLYmuxoXVPNhMoX9B6nCzhWtgLR5fe
Address C: 2MwhJMmd9aLQuTrVaLYeHjobRBm3zggHjs3
```

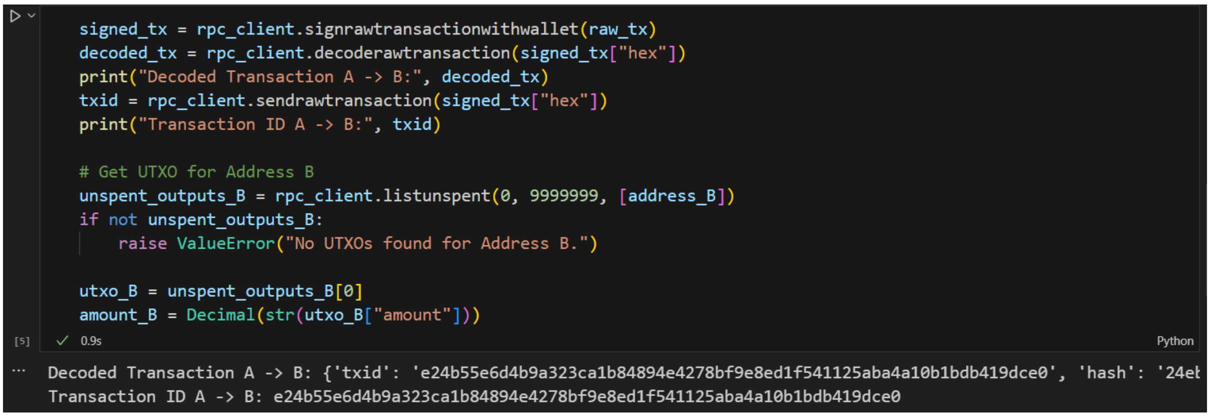


```
print(f"Address A: {address_A}")
print(f"Address B: {address_B}")
print(f"Address C: {address_C}")
```

```
Wallet 'CS216' is already loaded.
Address A: 2N8Z1EwkA1jMy94qduycaXi118PiuGGsQLQ
Address B: 2N9jBHLYmuxoXVPNhMoX9B6nCzhWtgLR5fe
Address C: 2MwhJMmd9aLQuTrVaLYeHjobRBm3zggHjs3
```

Transaction from A to B: The transaction ID for sending Bitcoin from Address A to Address B was obtained and used as an input for the next transaction.

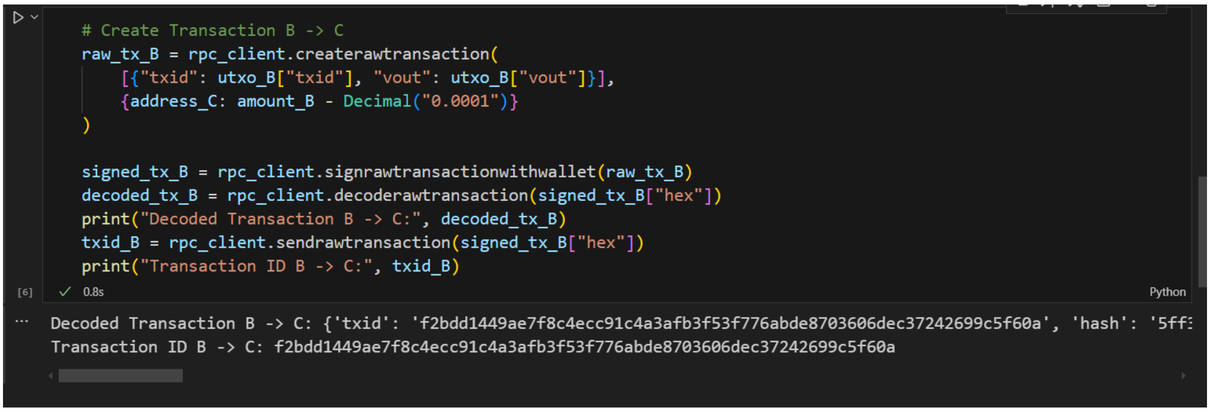
```
Transaction ID from A to B:
    e24b55e6d4b9a323ca1b84894e4278bf9e8ed1f541125aba4a10b1bdb419dce0
```



```
signed_tx = rpc_client.signrawtransactionwithwallet(raw_tx)
decoded_tx = rpc_client.decoderawtransaction(signed_tx["hex"])
print("Decoded Transaction A -> B:", decoded_tx)
txid = rpc_client.sendrawtransaction(signed_tx["hex"])
print("Transaction ID A -> B:", txid)

# Get UTXO for Address B
unspent_outputs_B = rpc_client.listunspent(0, 9999999, [address_B])
if not unspent_outputs_B:
    raise ValueError("No UTXOs found for Address B.")

utxo_B = unspent_outputs_B[0]
amount_B = Decimal(str(utxo_B["amount"]))
```

```
Decoded Transaction A -> B: {'txid': 'e24b55e6d4b9a323ca1b84894e4278bf9e8ed1f541125aba4a10b1bdb419dce0', 'hash': '24eb
Transaction ID A -> B: e24b55e6d4b9a323ca1b84894e4278bf9e8ed1f541125aba4a10b1bdb419dce0
```

Transaction from B to C: The UTXO from the transaction A to B was used as an input for the transaction from B to C.



```
# Create Transaction B -> C
raw_tx_B = rpc_client.createrawtransaction(
    [{"txid": utxo_B["txid"], "vout": utxo_B["vout"]}],
    {address_C: amount_B - Decimal("0.0001")}
)

signed_tx_B = rpc_client.signrawtransactionwithwallet(raw_tx_B)
decoded_tx_B = rpc_client.decoderawtransaction(signed_tx_B["hex"])
print("Decoded Transaction B -> C:", decoded_tx_B)
txid_B = rpc_client.sendrawtransaction(signed_tx_B["hex"])
print("Transaction ID B -> C:", txid_B)
```

```
Decoded Transaction B -> C: {'txid': 'f2bdd1449ae7f8c4ecc91c4a3afb3f53f776abde8703606dec37242699c5f60a', 'hash': '5ff:
Transaction ID B -> C: f2bdd1449ae7f8c4ecc91c4a3afb3f53f776abde8703606dec37242699c5f60a
```

4.2 Decoded Scripts

4.3 Signed Transaction from A to B

```
{
  "txid": "e24b55e6d4b9a323ca1b84894e4278bf9e8ed1f541125aba4a10b1bdb419dce0",
  "hash": "24eb46d849ab4103cb04191e5842bb2ea27ad5cfcb4f0cfba2889a25e0e9a2bc",
  "version": 2,
  "size": 215,
  "vsize": 134,
  "weight": 533,
  "locktime": 0,
  "vin": [
    {
      "txid": "0f062d0ced04d25c2c9d4d726027d1e6313020d5ab2cb72a69263d9557bfb286",
      "vout": 0,
      "scriptSig": {
        "asm": "00143e2000fc3f63e88972392d769b6b1b321d169865",
        "hex": "1600143e2000fc3f63e88972392d769b6b1b321d169865"
      },
      "txinwitness": [
        "3044022068183
            d30e406d7115c6d76bd05bb2dcc44d3c83c3876291610c384fd521739170220552eb211771fdee49b44607a631d
            ",
        "034c032633b9ce1f3f554e0f44da4f7be638182fb7d829d9cdd74fe3ee87ba378e"
      ],
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 0.00990000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_HASH160 b4cb6690868781ea6bd0e36ef42ae205ae458f1d OP_EQUAL",
        "desc": "addr(2N9jBHLYmuxoXVPNhMoX9B6nCzhWtgLR5fe)#acrkg4lh",
        "hex": "a914b4cb6690868781ea6bd0e36ef42ae205ae458f1d87",
        "address": "2N9jBHLYmuxoXVPNhMoX9B6nCzhWtgLR5fe",
        "type": "scripthash"
      }
    }
  ]
}
```

4.4 Signed Transaction from B to C

```
Transaction ID from B to C:
     f2bdd1449ae7f8c4ecc91c4a3afb3f53f776abde8703606dec37242699c5f60a
     \subsection{Decoded Transaction B $
ightarrow$ C}

The following is the decoded transaction from B to C:

\begin{lstlisting}
{
  "txid": "f2bdd1449ae7f8c4ecc91c4a3afb3f53f776abde8703606dec37242699c5f60a",
  "hash": "5ff30609d496aa8dcf6319818966fb51e1c44c80c9b131988bd46bab0772f7e5",
  "version": 2,
  "size": 215,
  "vsize": 134,
  "weight": 533,
  "locktime": 0,
  "vin": [
    {
      "txid": "e24b55e6d4b9a323ca1b84894e4278bf9e8ed1f541125aba4a10b1bdb419dce0",
      "vout": 0,
      "scriptSig": {
        "asm": "0014345d301aed4f75d42447639d275ae80279f8a0f5",
        "hex": "160014345d301aed4f75d42447639d275ae80279f8a0f5"
      },
      "txinwitness": [
        "304402204
            b324a3740e72cb8c015a2b07fac722312b10fd18b948c97ebc97c2ca98a35a40220411769bfb7368a03d0252e59
            ",
        "0379f1b04400212166c1de756142ddafcec54e620b9e5f48fb4d2624e4d0d9e5f0"
      ],
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 0.00980000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_HASH160 30cef766bd8ddd8da28ef91a3744b48b437ccfb0 OP_EQUAL",
        "desc": "addr(2MwhJMmd9aLQuTrVaLYeHjobRBm3zggHjs3)#a9lkj277",
        "hex": "a91430cef766bd8ddd8da28ef91a3744b48b437ccfb087",
        "address": "2MwhJMmd9aLQuTrVaLYeHjobRBm3zggHjs3",
        "type": "scripthash"
      }
    }
  ]
}
```

4.5 Script Analysis

Bitcoin uses two components for script validation:

- **Challenge Script (scriptPubKey)**: This defines the locking condition that must be met to spend the output.

  ```
      OP_HASH160 <Redeem Script Hash> OP_EQUAL
  ```

- **Response Script (scriptSig and Witness)**: This provides the unlocking data required to satisfy the scriptPubKey.

  ```
      Witness: <Signature> <Public Key>
      ScriptSig: <Redeem Script>
  ```

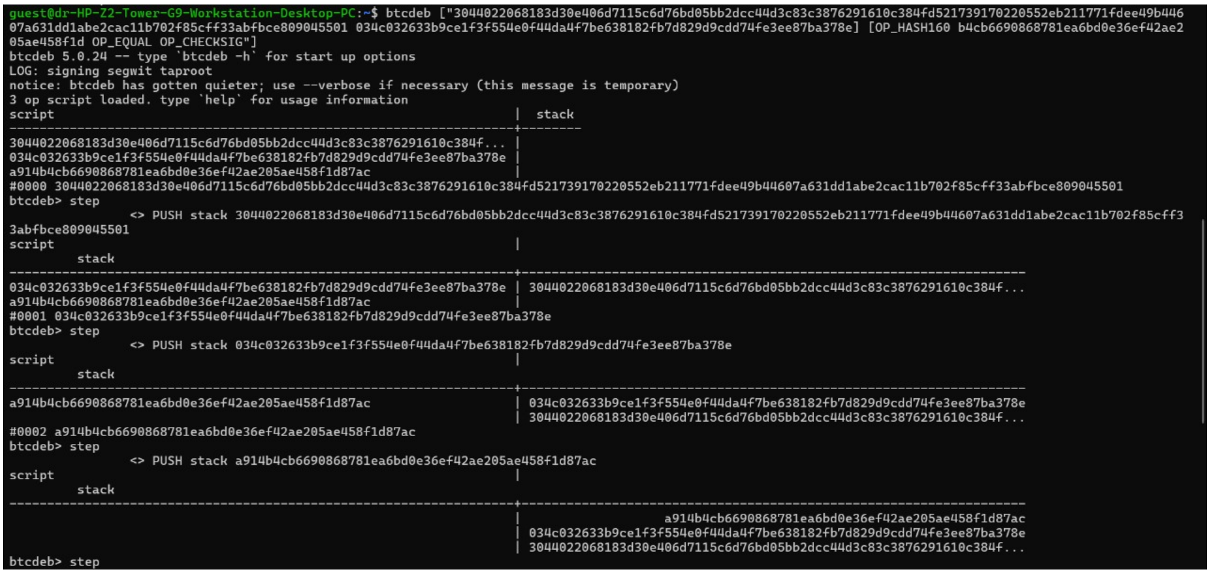
- **Validation Process:**

  1. The scriptSig pushes the Redeem Script onto the stack.
  2. The scriptPubKey verifies that the Redeem Script matches the expected hash.
  3. The SegWit execution process evaluates the Witness stack:
     (a) The public key is pushed onto the stack.
     (b) The signature is verified using OP_CHECKSIG.
  4. If all conditions pass, the transaction is valid.

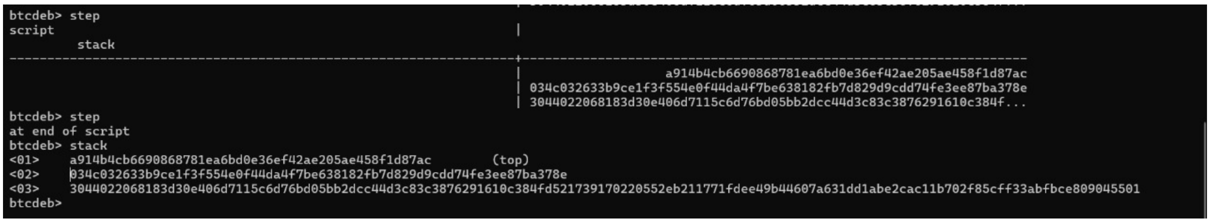
4.6 Bitcoin Debugger Execution

- The challenge and response scripts were executed in the Bitcoin Debugger.
- Screenshots of the execution steps are attached, showing the script validation process.

4.6.1 Transaction from A to B

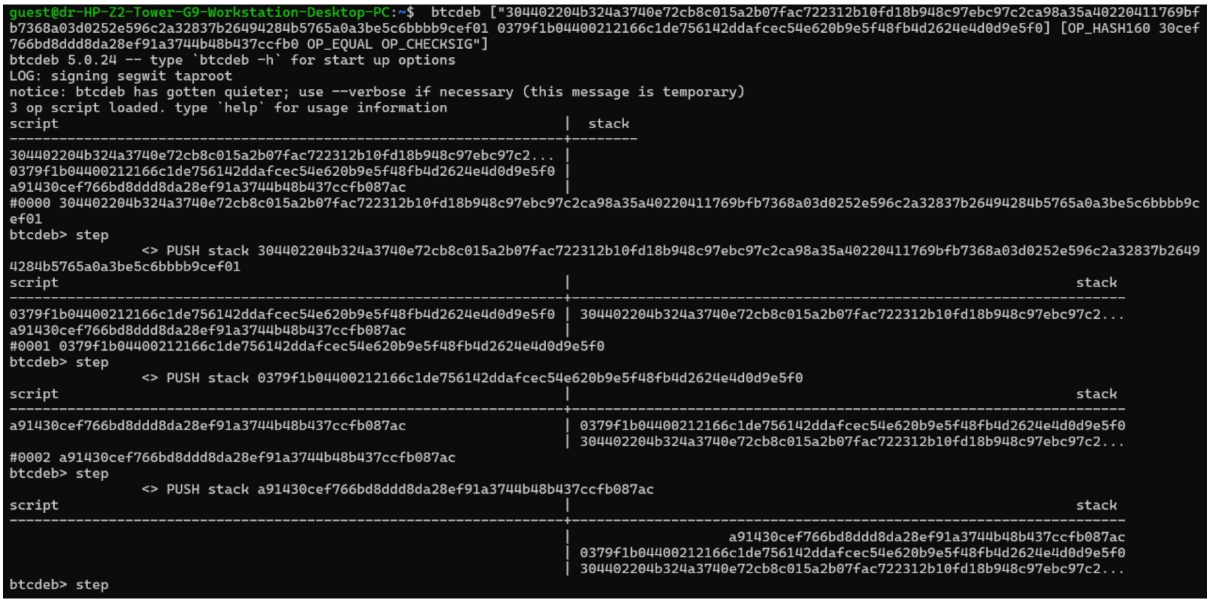


```
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb ["3044022068183d30e406d7115c6d76bd05bb2dcc44d3c83c3876291610c384fd521739170220552eb211771fdee49b446
07a631dd1abe2cac11b702f85cff33abfbce809045501 034c032633b9ce1f3f554e0f44da4f7be638182fb7d829d9cdd74fe3ee87ba378e] [OP_HASH160 b4cb6690868781ea6bd0e36ef42ae2
05ae458f1d OP_EQUAL OP_CHECKSIG"]
btcdeb 5.0.24 -- type `btcdeb -h` for start up options
LOG: signing segwit taproot
notice: btcdeb has gotten quieter; use --verbose if necessary (this message is temporary)
3 op script loaded. type `help` for usage information
script                                                             |  stack
-------------------------------------------------------------------+--------
3044022068183d30e406d7115c6d76bd05bb2dcc44d3c83c3876291610c384f... |
034c032633b9ce1f3f554e0f44da4f7be638182fb7d829d9cdd74fe3ee87ba378e |
a914b4cb6690868781ea6bd0e36ef42ae205ae458f1d87ac                   |
#0000 3044022068183d30e406d7115c6d76bd05bb2dcc44d3c83c3876291610c384fd521739170220552eb211771fdee49b44607a631dd1abe2cac11b702f85cff33abfbce809045501
btcdeb> step
                <> PUSH stack 3044022068183d30e406d7115c6d76bd05bb2dcc44d3c83c3876291610c384fd521739170220552eb211771fdee49b44607a631dd1abe2cac11b702f85cff3
3abfbce809045501
script                                                             |
        stack
-------------------------------------------------------------------+-------------------------------------------------------------------
034c032633b9ce1f3f554e0f44da4f7be638182fb7d829d9cdd74fe3ee87ba378e | 3044022068183d30e406d7115c6d76bd05bb2dcc44d3c83c3876291610c384f...
a914b4cb6690868781ea6bd0e36ef42ae205ae458f1d87ac                   |
#0001 034c032633b9ce1f3f554e0f44da4f7be638182fb7d829d9cdd74fe3ee87ba378e
btcdeb> step
                <> PUSH stack 034c032633b9ce1f3f554e0f44da4f7be638182fb7d829d9cdd74fe3ee87ba378e
script                                                             |
        stack
-------------------------------------------------------------------+-------------------------------------------------------------------
a914b4cb6690868781ea6bd0e36ef42ae205ae458f1d87ac                   | 034c032633b9ce1f3f554e0f44da4f7be638182fb7d829d9cdd74fe3ee87ba378e
                                                                   | 3044022068183d30e406d7115c6d76bd05bb2dcc44d3c83c3876291610c384f...
#0002 a914b4cb6690868781ea6bd0e36ef42ae205ae458f1d87ac
btcdeb> step
                <> PUSH stack a914b4cb6690868781ea6bd0e36ef42ae205ae458f1d87ac
script                                                             |
        stack
-------------------------------------------------------------------+-------------------------------------------------------------------
                                                                   |                   a914b4cb6690868781ea6bd0e36ef42ae205ae458f1d87ac
                                                                   | 034c032633b9ce1f3f554e0f44da4f7be638182fb7d829d9cdd74fe3ee87ba378e
                                                                   | 3044022068183d30e406d7115c6d76bd05bb2dcc44d3c83c3876291610c384f...
btcdeb> step
```

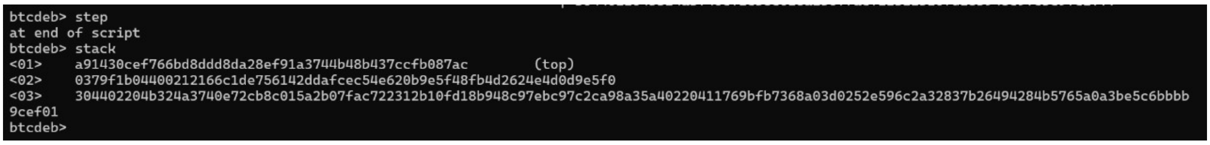


```
btcdeb> step
script                                                             |
        stack
-------------------------------------------------------------------+-------------------------------------------------------------------
                                                                   |                   a914b4cb6690868781ea6bd0e36ef42ae205ae458f1d87ac
                                                                   | 034c032633b9ce1f3f554e0f44da4f7be638182fb7d829d9cdd74fe3ee87ba378e
                                                                   | 3044022068183d30e406d7115c6d76bd05bb2dcc44d3c83c3876291610c384f...
btcdeb> step
at end of script
btcdeb> stack
<01>    a914b4cb6690868781ea6bd0e36ef42ae205ae458f1d87ac        (top)
<02>    034c032633b9ce1f3f554e0f44da4f7be638182fb7d829d9cdd74fe3ee87ba378e
<03>    3044022068183d30e406d7115c6d76bd05bb2dcc44d3c83c3876291610c384fd521739170220552eb211771fdee49b44607a631dd1abe2cac11b702f85cff33abfbce809045501
btcdeb>
```

4.6.2 Transaction from B to C



```
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$  btcdeb ["304402204b324a3740e72cb8c015a2b07fac722312b10fd18b948c97ebc97c2ca98a35a40220411769bf
b7368a03d0252e596c2a32837b26494284b5765a0a3be5c6bbbb9cef01 0379f1b04400212166c1de756142ddafcec54e620b9e5f48fb4d2624e4d0d9e5f0] [OP_HASH160 30cef
766bd8ddd8da28ef91a3744b48b437ccfb0 OP_EQUAL OP_CHECKSIG"]
btcdeb 5.0.24 -- type `btcdeb -h` for start up options
LOG: signing segwit taproot
notice: btcdeb has gotten quieter; use --verbose if necessary (this message is temporary)
3 op script loaded. type `help` for usage information
script                                                             |  stack
-------------------------------------------------------------------+--------
304402204b324a3740e72cb8c015a2b07fac722312b10fd18b948c97ebc97c2... |
0379f1b04400212166c1de756142ddafcec54e620b9e5f48fb4d2624e4d0d9e5f0 |
a91430cef766bd8ddd8da28ef91a3744b48b437ccfb087ac                   |
#0000 304402204b324a3740e72cb8c015a2b07fac722312b10fd18b948c97ebc97c2ca98a35a40220411769bfb7368a03d0252e596c2a32837b26494284b5765a0a3be5c6bbbb9c
ef01
btcdeb> step
                <> PUSH stack 304402204b324a3740e72cb8c015a2b07fac722312b10fd18b948c97ebc97c2ca98a35a40220411769bfb7368a03d0252e596c2a32837b2649
4284b5765a0a3be5c6bbbb9cef01
script                                                             |                                                              stack
-------------------------------------------------------------------+-------------------------------------------------------------------
0379f1b04400212166c1de756142ddafcec54e620b9e5f48fb4d2624e4d0d9e5f0 | 304402204b324a3740e72cb8c015a2b07fac722312b10fd18b948c97ebc97c2...
a91430cef766bd8ddd8da28ef91a3744b48b437ccfb087ac                   |
#0001 0379f1b04400212166c1de756142ddafcec54e620b9e5f48fb4d2624e4d0d9e5f0
btcdeb> step
                <> PUSH stack 0379f1b04400212166c1de756142ddafcec54e620b9e5f48fb4d2624e4d0d9e5f0
script                                                             |                                                              stack
-------------------------------------------------------------------+-------------------------------------------------------------------
a91430cef766bd8ddd8da28ef91a3744b48b437ccfb087ac                   | 0379f1b04400212166c1de756142ddafcec54e620b9e5f48fb4d2624e4d0d9e5f0
                                                                   | 304402204b324a3740e72cb8c015a2b07fac722312b10fd18b948c97ebc97c2...
#0002 a91430cef766bd8ddd8da28ef91a3744b48b437ccfb087ac
btcdeb> step
                <> PUSH stack a91430cef766bd8ddd8da28ef91a3744b48b437ccfb087ac
script                                                             |                                                              stack
-------------------------------------------------------------------+-------------------------------------------------------------------
                                                                   |                   a91430cef766bd8ddd8da28ef91a3744b48b437ccfb087ac
                                                                   | 0379f1b04400212166c1de756142ddafcec54e620b9e5f48fb4d2624e4d0d9e5f0
                                                                   | 304402204b324a3740e72cb8c015a2b07fac722312b10fd18b948c97ebc97c2...
btcdeb> step
```



```
btcdeb> step
at end of script
btcdeb> stack
<01>    a91430cef766bd8ddd8da28ef91a3744b48b437ccfb087ac        (top)
<02>    0379f1b04400212166c1de756142ddafcec54e620b9e5f48fb4d2624e4d0d9e5f0
<03>    304402204b324a3740e72cb8c015a2b07fac722312b10fd18b948c97ebc97c2ca98a35a40220411769bfb7368a03d0252e596c2a32837b26494284b5765a0a3be5c6bbbb
9cef01
btcdeb>
```