CS 216 Bitcoin Scripting Report

Part 1: Legacy (P2PKH) Transactions

1.1 Workflow Overview

- **Address Generation:**
  Three legacy addresses are created:
    - **Address A (Sender), Address B (Receiver), Address C (Extra)**
- **Transaction A → B:**
    - **Funding:** Address A is funded with 1 BTC (by mining 101 blocks).
    - **Transaction Creation:** A transaction is created to send 0.5 BTC from Address A to Address B.
    - **Confirmation:** A block is mined to confirm the transaction.
    - **Key Output:**
        - **TXID (A → B):**

```
(env) C:\Users\sathw\OneDrive\Desktop\CS216\scripting>python legacy_A_to_B.py
============================================================
Legacy P2PKH Transaction (A -> B)
============================================================
Connecting to Bitcoin Core at http://sathwik:btc18@127.0.0.1:18443
Initial Wallet Balance: 14942.84654392 BTC
------------------------------------------------------------
Generated Legacy Addresses:
  Address A (Sender):   n4dFZRcqH71rT6Mwh7kYJh4u9UXZ27rhn9
  Address B (Receiver): n2v9nGvdyuisHKbYjY8aQRec9tTtBggYNo
  Address C (Extra):      n4n9v8PkffUj8LdkXdc3ajSNP1zTQwvPAG
------------------------------------------------------------
Generating 101 blocks for funding...
Funding Transaction: Sent 1.0 BTC to Address A | TXID: 08a1e3047f007e1adb42b332e047f60f36a2cbf5ce08d766
------------------------------------------------------------

Raw Transaction Hex (A -> B):
0200000001d2222c44c6c9aed666d708cef5cba2360ff647e032b342db1a7e007f04e3a1080100000000fdffffff0280f0fa020

Transaction A -> B broadcasted. TXID: 972384ce87d54cb1ee27c89887114ea952b3393ef05af64d6f24abaed06a8930
------------------------------------------------------------
```

        - **Locking Script for Address B:**

```
Locking Script for Address B:
76a914eabdcc0e20c5123bd57168dbfa67de348761854988ac
============================================================
```

- **Transaction B → C:**
    - **Input:** Uses the UTXO from the A → B transaction.
    - **Transaction Creation:** A transaction sends approximately 0.3 BTC from Address B to Address C. The remaining change (after deducting a small fee) returns to Address B.
    - **Confirmation:** A block is mined for transaction confirmation.
    - **Key Output:**
        - **TXID (B → C):**

```
(env) C:\Users\sathw\OneDrive\Desktop\CS216\scripting>python legacy_B_to_C.py
============================================================
Legacy P2PKH Transaction (B -> C)
============================================================
Connecting to Bitcoin Core at http://sathwik:btc18@127.0.0.1:18443
Enter the actual legacy Address B (sender from A->B transaction):
n2v9nGvdyuisHKbYjY8aQRec9tTtBggYNo
Enter the legacy Address C (receiver):
n4n9v8PkffUj8LdkXdc3ajSNP1zTQwvPAG
------------------------------------------------------------
Selected UTXO:
  TXID: 972384ce87d54cb1ee27c89887114ea952b3393ef05af64d6f24abaed06a8930
  VOUT: 0
  Amount: 0.50000000 BTC
------------------------------------------------------------

Raw Transaction Hex (B -> C):
020000000130896ad0aeab246f4df65af03e39b352a94e118798c827eeb14cd587ce84239700000000000fdffffff0280c3c90100(

Transaction B -> C broadcasted. TXID: 6b8373acb3b0722ff07bb7df812cd5cb5091a8fa40005335a0de0f256e0221b4
------------------------------------------------------------
```

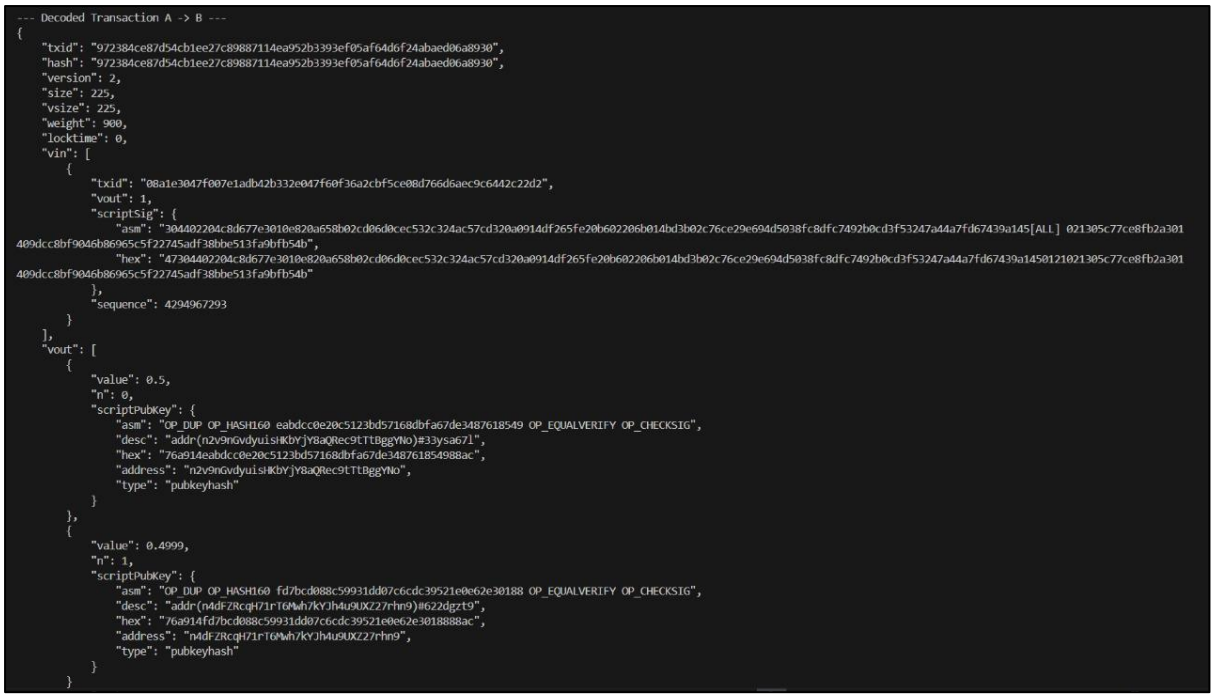
        - **Unlocking Script:**

```
Unlocking Script for Input:
{'asm': '304402204323cd1008a87fa5216e435f4338bde39b8030635d43305005857e28ee1335a7022060f22d4e4131e8ca40651023574864ccbcef51bad1e6984a6d77f5ec74341d7d[ALL] 03d4b061b57db37a49b8278014ca974b61
75c7f345b803481f0727b0c1d8cb448f', 'hex': '473044022043323cd1008a87fa5216e435f4338bde39b8030635d43305005857e28ee1335a7022060f22d4e4131e8ca40651023574864ccbcef51bad1e6984a6d77f5ec74341d7d0121
03d4b061b57db37a49b8278014ca974b6175c7f345b803481f0727b0c1d8cb448f'}
============================================================
```

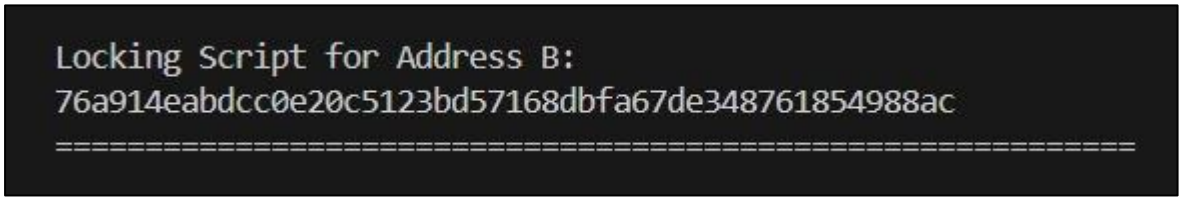
1.2 Decoded Scripts and Script Analysis

- **Transaction A → B:**
    - **Decoded Output:**
        - **Inputs:** Derived from a funding transaction to Address A.
        - **Outputs:**

- 0.5 BTC sent to Address B using a standard locking script.
- Change (≈0.4999 BTC) returned to Address A.



  - **Locking Script for Address B:**



- **Transaction B → C:**
  - **Decoded Output:**
    - **Inputs:** UTXO from transaction A → B.
    - **Outputs:**
      - Approximately 0.3 BTC to Address C.
      - Change (≈0.1999 BTC) to Address B.

```
--- Decoded Transaction B -> C ---
{
    "txid": "6b8373acb3b0722ff07bb7df812cd5cb5091a8fa40005335a0de0f256e0221b4",
    "hash": "6b8373acb3b0722ff07bb7df812cd5cb5091a8fa40005335a0de0f256e0221b4",
    "version": 2,
    "size": 225,
    "vsize": 225,
    "weight": 900,
    "locktime": 0,
    "vin": [
        {
            "txid": "972384ce87d54cb1ee27c89887114ea952b3393ef05af64d6f24abaed06a8930",
            "vout": 0,
            "scriptSig": {
                "asm": "304402204323cd1008a87fa5216e435f4338bde39b8030635d43305005857e28ee1335a7022060f22d4e4131e8ca40651023574864ccbcef51bad1e6984a6d77f5ec74341d7d[ALL] 03d4b061b57db37a49b
8278014ca974b6175c7f345b803481f0727b0c1d8cb448f",
            },
            "sequence": 4294967293
        }
    ],
    "vout": [
        {
            "value": 0.3,
            "n": 0,
            "scriptPubKey": {
                "asm": "OP_DUP OP_HASH160 ff2ad58013cc99568f25efbf5c134a8e4232293b OP_EQUALVERIFY OP_CHECKSIG",
                "desc": "addr(n4n9v8PkffUj8LdkXdc3ajSNP1zTQwvPAG)#axcrn7md",
                "hex": "76a914ff2ad58013cc99568f25efbf5c134a8e4232293b88ac",
                "address": "n4n9v8PkffUj8LdkXdc3ajSNP1zTQwvPAG",
                "type": "pubkeyhash"
            }
        },
        {
            "value": 0.1999,
            "n": 1,
            "scriptPubKey": {
                "asm": "OP_DUP OP_HASH160 eabdcc0e20c5123bd57168dbfa67de3487618549 OP_EQUALVERIFY OP_CHECKSIG",
                "desc": "addr(n2v9nGvdyuisHKbYjY8aQRec9tTtBggYNo)#33ysa67l",
                "hex": "76a914eabdcc0e20c5123bd57168dbfa67de348761854988ac",
                "address": "n2v9nGvdyuisHKbYjY8aQRec9tTtBggYNo",
                "type": "pubkeyhash"
            }
        }
    ]
```


- **Unlocking Script:**


```
Unlocking Script for Input:
{'asm': '304402204323cd1008a87fa5216e435f4338bde39b8030635d43305005857e28ee1335a7022060f22d4e4131e8ca40651023574864ccbcef51bad1e6984a6d77f5ec74341d7d[ALL] 03d4b061b57db37a49b8278014ca974b61
75c7f345b803481f0727b0c1d8cb448f', 'hex': '47304402204323cd1008a87fa5216e435f4338bde39b8030635d43305005857e28ee1335a7022060f22d4e4131e8ca40651023574864ccbcef51bad1e6984a6d77f5ec74341d7d0121
03d4b061b57db37a49b8278014ca974b6175c7f345b803481f0727b0c1d8cb448f'}
============================================================
```


- **Challenge–Response Mechanism:**
    - The **challenge** (locking) script ensures funds can only be spent by providing a valid signature matching the hashed public key.
    - The **response** (unlocking) script supplies the signature and public key. When executed with the challenge script in a Bitcoin debugger, these prove the spending authority.

1.3 Verification of Legacy Transaction Scripts:

- We verified our A→B transaction by first using :
  bitcoin-cli -regtest gettransaction to confirm the transaction's presence on the blockchain with TXID 972384ce87d54cb1ee27c89887114ea952b3393ef05af64d6f24abaed06a8930. The output confirmed a valid transaction, showing a send of 0.5 BTC from Address A and a corresponding receive at Address B.

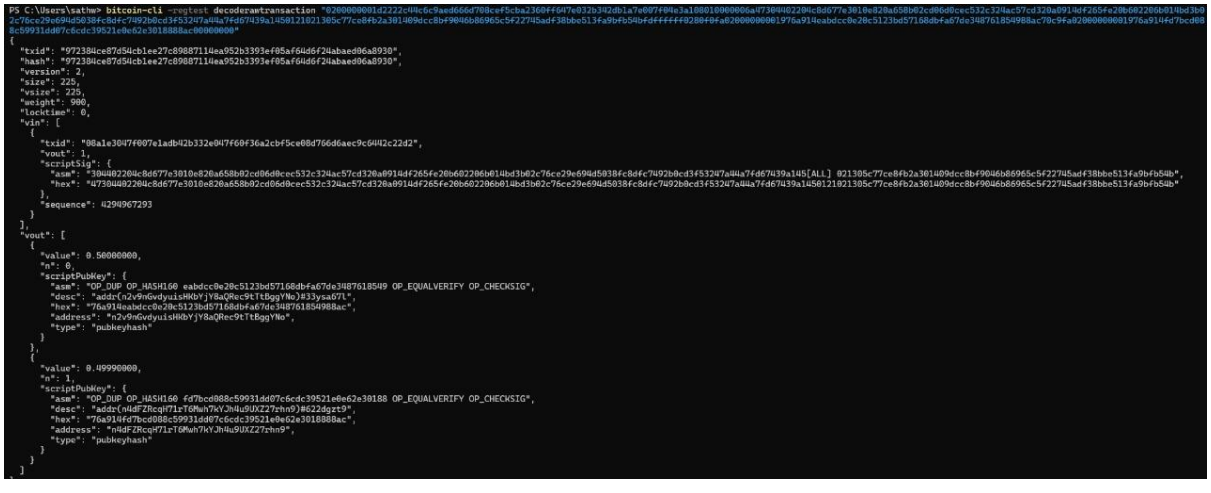
- We then decoded the raw transaction using :
  bitcoin-cli -regtest decoderawtransaction "<raw_tx>"

- The decoded JSON output displayed the locking script for Address B as:
  76a914eabdcc0e20c5123bd57168dbfa67de348761854988ac

- which follows the standard P2PKH pattern (OP_DUP, OP_HASH160, [pubKey hash], OP_EQUALVERIFY, OP_CHECKSIG).

- Additionally, we used btcdeb on the provided server by running: btcdeb -v '76a914eabdcc0e20c5123bd57168dbfa67de348761854988ac'

```
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb -v '76a914eabdcc0e20c5123bd57168dbfa67de348761854988ac'
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                                  |
OP_HASH160                              |
eabdcc0e20c5123bd57168dbfa67de3487618549 |
OP_EQUALVERIFY                          |
OP_CHECKSIG                             |
#0000 OP_DUP
btcdeb>
```



Part 2: SegWit (P2SH-P2WPKH) Transactions

2.1 Workflow Overview

- **Address Generation:**
  Three P2SH-SegWit addresses are generated:
    - **Address A' (Sender)**
    - **Address B' (Receiver)**
    - **Address C' (Extra)**

- **Transaction A' → B':**
    - **Funding:** Address A' is funded with 1 BTC using the sendtoaddress command and 101 blocks are mined.
    - **Transaction Creation:** A raw transaction is created to send 0.5 BTC from Address A' to Address B'. It is signed and broadcast.
    - **Confirmation:** A block is mined.
    - **Key Output:**
        - **TXID (A' → B'):**

```
(env) C:\Users\sathw\OneDrive\Desktop\CS216\scripting>python segwit_A_to_B.py
============================================================
P2SH-SegWit Transaction (A' -> B')
============================================================
Connecting to Bitcoin Core at http://sathwik:btc18@127.0.0.1:18443
Initial Wallet Balance: 14945.38550616 BTC
------------------------------------------------------------
Generated P2SH-SegWit Addresses:
  Address A' (Sender):   2NFCxDRkM2thRo5GZUfhfVST4ei59AGK3J7
  Address B' (Receiver): 2N8dkCTkL3qRZAytdiagHAA7bjmMvusjYUj
  Address C' (Extra):      2MxZicM9xfpP9a5PeTfut5K8wpRikGssFiP
------------------------------------------------------------
Generating 101 blocks to fund coins...
Funding Transaction: Sent 1.0 BTC to Address A' | TXID: 852545191b47491dd343ca3fcae2397efac477ad793af7f5fa
------------------------------------------------------------

Raw Transaction Hex (A' -> B'):
0200000001f4ecdca4a73f39faf5f73a79ad77c4fa7e39e2ca3fca43d31d49471b19452585000000000fdffffff0280f0fa020000

Transaction A' -> B' broadcasted. TXID: 080a9517c24b0d2f245f57e29c9a853ec1ee2fa6360927c2c3ea1a67533582f6
------------------------------------------------------------
```

        - **Locking Script for Address B':**

```
Locking Script for Address B':
a914a8cc4184567537ecb3cdb916589fc08ae59e219687
============================================================
```

- **Transaction B’ → C’:**
    - **Input:** The UTXO from transaction A’ → B’ is selected.
    - **Transaction Creation:** A transaction is created to send ~0.3 BTC from Address B’ to Address C’, with change (after a small fee) returned to Address B’.
    - **Confirmation:** A block is mined.
    - **Key Output:**
        - **TXID (B’ → C’):**

```
(env) C:\Users\sathw\OneDrive\Desktop\CS216\scripting>python segwit_B_to_C.py
============================================================
P2SH-SegWit Transaction (B' -> C')
============================================================
Connecting to Bitcoin Core at http://sathwik:btc18@127.0.0.1:18443
Enter the actual P2SH-SegWit Address B' (sender from A'->B transaction):
2N8dkCTkL3qRZAytdiagHAA7bjmMvusjYUj
Enter the P2SH-SegWit Address C' (receiver):
2MxZicM9xfpP9a5PeTfut5K8wpRikGssFiP
------------------------------------------------------------
Selected UTXO:
  TXID: 080a9517c24b0d2f245f57e29c9a853ec1ee2fa6360927c2c3ea1a67533582f6
  VOUT: 0
  Amount: 0.50000000 BTC
------------------------------------------------------------

Raw Transaction Hex (B' -> C'):
0200000001f6823553671aeac3c2270936a62feec13e859a9ce2575f242f0d4bc217950a080000000000fdffffff0280c3c901000

Transaction B' -> C' broadcasted. TXID: 300ede76c0f55c5fe25110dc64c843113b18da95cd947f441e4a95e35d8d59ea
------------------------------------------------------------
```

        - **Unlocking Script:**

```
Unlocking Script for Input:
{'asm': '0014f22c83fac79afd95cef3bfbf91f7fda824860d9a', 'hex': '160014f22c83fac79afd95cef3bfbf91f7fda824860d9a'}
============================================================
```

2.2 Decoded Scripts and Script Analysis

- **Transaction A' → B':**
    - **Decoded Output:**
        - **Inputs:** Derived from a funding transaction to Address A'.
        - **Outputs:**
            - 0.5 BTC is sent to Address B' using a P2SH wrapper.
            - Change (≈0.4999 BTC) returns to Address A'.

```
Transaction A' -> B' broadcasted. TXID: 080a9517c24b0d2f245f57e29c9a853ec1ee2fa6360927c2c3e
------------------------------------------------------------

--- Decoded Transaction A' -> B' ---
{
    "txid": "080a9517c24b0d2f245f57e29c9a853ec1ee2fa6360927c2c3ea1a67533582f6",
    "hash": "b3ab826f6df176725f2ae4bfdeb8d88e1decb8b082f912e3a0d9706558c8eefa",
    "version": 2,
    "size": 247,
    "vsize": 166,
    "weight": 661,
    "locktime": 0,
    "vin": [
        {
            "txid": "852545191b47491dd343ca3fcae2397efac477ad793af7f5fa393fa7a4dcecf4",
            "vout": 0,
            "scriptSig": {
                "asm": "00148a890443635f7f0fa5d94e49300ff97ec0a9ff08",
                "hex": "1600148a890443635f7f0fa5d94e49300ff97ec0a9ff08"
            },
            "txinwitness": [
                "30440220326a45857e008df9becee061befa61b154a134ca0f24d00e1afab70b2bfcad2a02
                "03e60c6042705d5c03691c9bd6397a1ffb05d4b071edd8e7ebeb4ea252f7597e1f"
            ],
            "sequence": 4294967293
        }
    ],
    "vout": [
        {
            "value": 0.5,
            "n": 0,
            "scriptPubKey": {
                "asm": "OP_HASH160 a8cc4184567537ecb3cdb916589fc08ae59e2196 OP_EQUAL",
                "desc": "addr(2N8dkCTkL3qRZAytdiagHAA7bjmMvusjYUj)#xqvv6xqv",
                "hex": "a914a8cc4184567537ecb3cdb916589fc08ae59e219687",
                "address": "2N8dkCTkL3qRZAytdiagHAA7bjmMvusjYUj",
                "type": "scripthash"
            }
        },
        {
            "value": 0.4999,
            "n": 1,
            "scriptPubKey": {
                "asm": "OP_HASH160 f0e4c4b32c927dc9369923750444842eae681ca8 OP_EQUAL",
                "desc": "addr(2NFCxDRkM2thRo5GZUfhfVST4ei59AGK3J7)#p5pqtcsg",
                "hex": "a914f0e4c4b32c927dc9369923750444842eae681ca887",
                "address": "2NFCxDRkM2thRo5GZUfhfVST4ei59AGK3J7",
                "type": "scripthash"
            }
        }
    ]
}
```

    - **Locking Script for Address B':**

```
Locking Script for Address B':
a914a8cc4184567537ecb3cdb916589fc08ae59e219687
================================================================
```

- **Transaction B’ → C’:**
    - **Decoded Output:**
        - **Inputs:** Uses the UTXO from transaction A’ → B’.
        - **Outputs:**
            - Approximately 0.3 BTC is sent to Address C’.
            - Change (≈0.1999 BTC) is sent back to Address B’.


```
--- Decoded Transaction B' -> C' ---
{
    "txid": "300ede76c0f55c5fe25110dc64c843113b18da95cd947f441e4a95e35d8d59ea",
    "hash": "33c11c080fc22d4648615ae9a4410e1a5ac6df207509b4d447186d2d280bdfd3",
    "version": 2,
    "size": 247,
    "vsize": 166,
    "weight": 661,
    "locktime": 0,
    "vin": [
        {
            "txid": "080a9517c24b0d2f245f57e29c9a853ec1ee2fa6360927c2c3ea1a67533582f6",
            "vout": 0,
            "scriptSig": {
                "asm": "0014f22c83fac79afd95cef3bfbf91f7fda824860d9a",
                "hex": "160014f22c83fac79afd95cef3bfbf91f7fda824860d9a"
            },
            "txinwitness": [
                "3044022020c4a3d4c8e68d263452d2e7817d2d3d8f1fd32e34a65172cb65c2fe5dba3285
                "0294cc188bd2e87f5decd71814348ea5bedc24c798bf6df49d9600e4cea1f5899e"
            ],
            "sequence": 4294967293
        }
    ],
    "vout": [
        {
            "value": 0.3,
            "n": 0,
            "scriptPubKey": {
                "asm": "OP_HASH160 3a58022d7117627eb499dfb93269e63e1c8a5051 OP_EQUAL",
                "desc": "addr(2MxZicM9xfpP9a5PeTfut5K8wpRikGssFiP)#49n2gcqv",
                "hex": "a9143a58022d7117627eb499dfb93269e63e1c8a505187",
                "address": "2MxZicM9xfpP9a5PeTfut5K8wpRikGssFiP",
                "type": "scripthash"
            }
        },
        {
            "value": 0.1999,
            "n": 1,
            "scriptPubKey": {
                "asm": "OP_HASH160 a8cc4184567537ecb3cdb916589fc08ae59e2196 OP_EQUAL",
                "desc": "addr(2N8dkCTkL3qRZAytdiagHAA7bjmMvusjYUj)#xqvv6xqv",
                "hex": "a914a8cc4184567537ecb3cdb916589fc08ae59e219687",
                "address": "2N8dkCTkL3qRZAytdiagHAA7bjmMvusjYUj",
                "type": "scripthash"
            }
        }
    ]
}
----------------------------------------------------------------
```


    - **Unlocking Script:**

```
Unlocking Script for Input:
{'asm': '0014f22c83fac79afd95cef3bfbf91f7fda824860d9a', 'hex': '160014f22c83fac79afd95cef3bfbf91f7fda824860d9a'}
============================================================
```

- **Challenge–Response Mechanism:**
    - The **challenge** script (locking script) in a SegWit transaction is a simple P2SH script that wraps a witness program.
    - The **response** is provided in the witness field, which supplies the signature and public key.
    - When the Bitcoin Debugger executes the combined script (witness data plus locking script), it validates the spending condition.

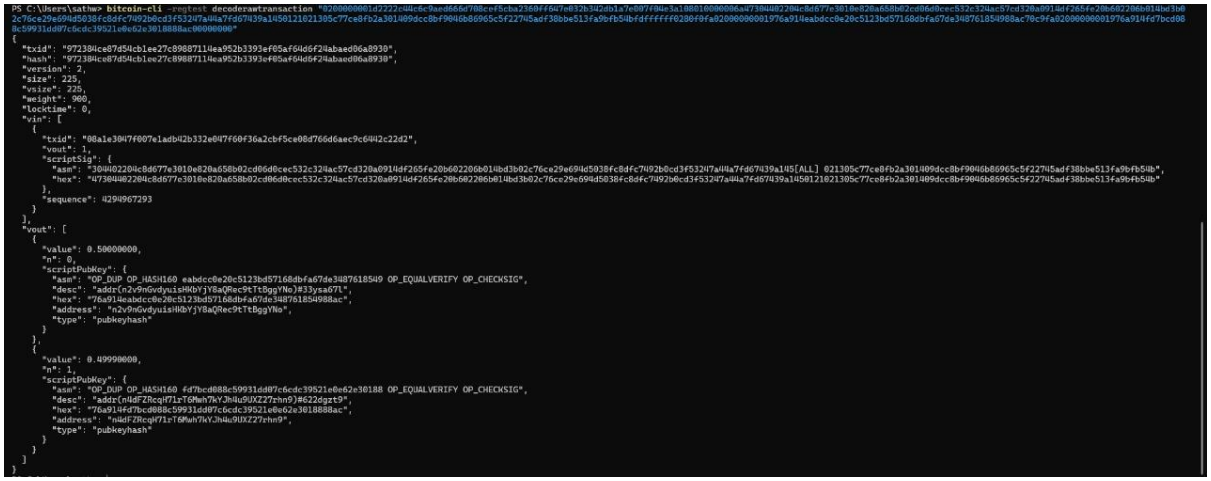
2.3 Verification of Challenge and Response Scripts

- We verified the correctness of our transaction scripts using Bitcoin Core's decoder and btcdeb. For our segqwit transaction, we obtained the following locking script (challenge) from the A→B transaction: 76a914eabdcc0e20c5123bd57168dbfa67de348761854988ac

- Using the command: btcdeb -v'76a914eabdcc0e20c5123bd57168dbfa67de348761854988ac'

- We similarly verified the segwit transaction by loading its challenge (locking) script: btcdeb -v 'a914a8cc4184567537ecb3cdb916589fc08ae59e219687'

```
PS C:\Users\sathw> bitcoin-cli -regtest gettransaction 97238ce87d54cb1ee27c89887114ea952b3393ef05af64d6f24abaed06a8930
{
  "amount": 0.00000000,
  "fee": -0.00010000,
  "confirmations": 106,
  "blockhash": "423d1524f8b031c98be35ec0b05a4ddbfe3b959aa26aec3af18d32d3715dc05d",
  "blockheight": 1859,
  "blockindex": 1,
  "blocktime": 1742738167,
  "txid": "97238ce87d54cb1ee27c89887114ea952b3393ef05af64d6f24abaed06a8930",
  "wtxid": "97238ce87d54cb1ee27c89887114ea952b3393ef05af64d6f24abaed06a8930",
  "walletconflicts": [
  ],
  "time": 1742738157,
  "timereceived": 1742738157,
  "bip125-replaceable": "no",
  "details": [
    {
      "address": "n2v9nGwdyuisHKbYjY8aQRec9tTtBggYNo",
      "category": "send",
      "amount": -0.50000000,
      "label": "addr_B",
      "vout": 0,
      "fee": -0.00010000,
      "abandoned": false
    },
    {
      "address": "n4dFZRcqH71rT6Mwh7kYJh4u9UXZ27rhn9",
      "category": "send",
      "amount": -0.49990000,
      "label": "addr_A",
      "vout": 1,
      "fee": -0.00010000,
      "abandoned": false
    },
    {
      "address": "n2v9nGwdyuisHKbYjY8aQRec9tTtBggYNo",
      "parent_descs": [
        "pkh(tpubD6NzVbkrYhZ4WqvHT2K6TFYXhPHNL7JFdJEqNZwnzb8cKgERTzMV1AYbx2WX2L1mbJ9PpMqC1KVdAgfbed3kRfjpSg7HjDHa9so2yYwEsCV/44h/1h/0h/0/*)#x8kkxlkm"
      ],
      "category": "receive",
      "amount": 0.50000000,
      "label": "addr_B",
      "vout": 0,
      "abandoned": false
    },
    {
      "address": "n4dFZRcqH71rT6Mwh7kYJh4u9UXZ27rhn9",
      "parent_descs": [
        "pkh(tpubD6NzVbkrYhZ4WqvHT2K6TFYXhPHNL7JFdJEqNZwnzb8cKgERTzMV1AYbx2WX2L1mbJ9PpMqC1KVdAgfbed3kRfjpSg7HjDHa9so2yYwEsCV/44h/1h/0h/0/*)#x8kkxlkm"
      ],
      "category": "receive",
      "amount": 0.49990000,
      "label": "addr_A",
      "vout": 1,
      "abandoned": false
    }
  ],
  "hex": "0200000001d2222c44c6c9aed666d708cef5cba2360ff6f47e032b342db1a7e007f04e3a108010000006a47304402204c8d677e3010e828a658b02cd06d0cec532c324ac57cd320a0914df2655fe20b602206b014bd3b02c76ce29e694d5038fc8dfc7492b0cd3f532f47a44a7fd67439a145012102130577ce8fb2a301409dcc8bf99f46b86965c5f2774 5adf38bbe513fa9bfb54bfdfffff0280f0fa0200000001976a914eabdcc0e20c5123bd57168dbfa67de348761854988ac70c9fa0200000001976a914fd7bcd088c59931dd07c6cdc39521e0e62e3018888ac00000000",
  "lastprocessedblock": {
    "hash": "729d90e5c4654a114fd3b50a2d3fedb94e9e530e1144a6f335122e217050e132",
    "height": 1964
  }
}
```



Part 3: Comparative Analysis of Legacy vs. SegWit Transactions

3.1 Transaction Size Comparison

Metric	Legacy (P2PKH)	SegWit (P2SH-P2WPKH)
Raw Size (bytes)	225	247
Virtual Size (vbytes)	225	166
Weight (units)	900	661

- **Observation:**
  Although the raw size (total bytes) of the SegWit transactions (247 bytes) is slightly higher than that of the Legacy transactions (225 bytes), the effective cost is measured by virtual size and weight. The SegWit transactions show a significant reduction in both virtual size (166 vbytes) and weight (661 weight units). This is achieved by moving the bulky witness data (signature and public key) outside the main transaction structure.

3.2 Script Structure Comparison

- **Legacy (P2PKH):**
  - **Locking Script:**
    Uses the standard format:
  - **Unlocking Script:**
    Embeds the full digital signature and public key.
- **SegWit (P2SH-P2WPKH):**
  - **Locking Script:**
    A simplified P2SH format:

- **Unlocking Script:**
  Contains minimal data (a 20-byte hash), while the full signature and public key reside in the witness field.

3.3 Benefits of SegWit Transactions

- **Lower Fees:**
  Due to the reduced virtual size and weight, transaction fees (which are fee-per-vbyte or fee-per-weight-unit based) are lower in SegWit transactions.
- **Efficient Block Space Utilization:**
  The segregation of witness data allows for more transactions to be included in a block, enhancing scalability.
- **Faster Verification:**
  With the witness data separated from the main transaction, the Bitcoin network can process and validate transactions more efficiently.