Bitcoin Scripting Assignment Report

CS 216: Introduction to Blockchain

Submission date: 23rd March 2025

Part 1: Legacy Address Transactions (P2PKH)

Workflow of Transactions

1. **Transaction from A to B:**
    - **Generated Bitcoin legacy addresses A and B.**
    - **Funded address A using the `sendtoaddress` command.**
    - **TxID for this transaction is `4c719b9fcd832ae1ec9e794366059c26ea3147961a79cd4d1afc996f96928941`**
    - **Created a raw transaction to transfer funds from A to B.**
    - **Decoded the transaction to extract the locking script (`scriptPubKey`).**
    - **Signed the transaction using the private key of A.**
    - **Broadcasted the transaction to the Bitcoin network.**
    - **TxID of transaction from A to B: `380e43c8dff5ca3358c86ace630ae8b77eff64e93a7e31aa73387f8761f2582a`**
2. **Transaction from B to C:**
    - **Retrieved the UTXO for address B using `listunspent`.**
    - **Created a new transaction using `380e43c8dff5ca3358c86ace630ae8b77eff64e93a7e31aa73387f8761f2582a` as input.**
    - **Funded address C using the output from the previous transaction.**
    - **Decoded the transaction and verified the response script (`scriptSig`).**
    - **Signed and broadcasted the transaction.**
    - **TxID of transaction from B to C: `c2f45d7f5e9346ac67f3460be2e79cabd2c1d03517fec9f10caed0f0fd997fab`**

Decoded Scripts

Transaction from A to B (scriptPubKey):
OP_DUP OP_HASH160 e0699f95e6f18e1aacb368055f19daa8445620db OP_EQUALVERIFY OP_CHECKSIG

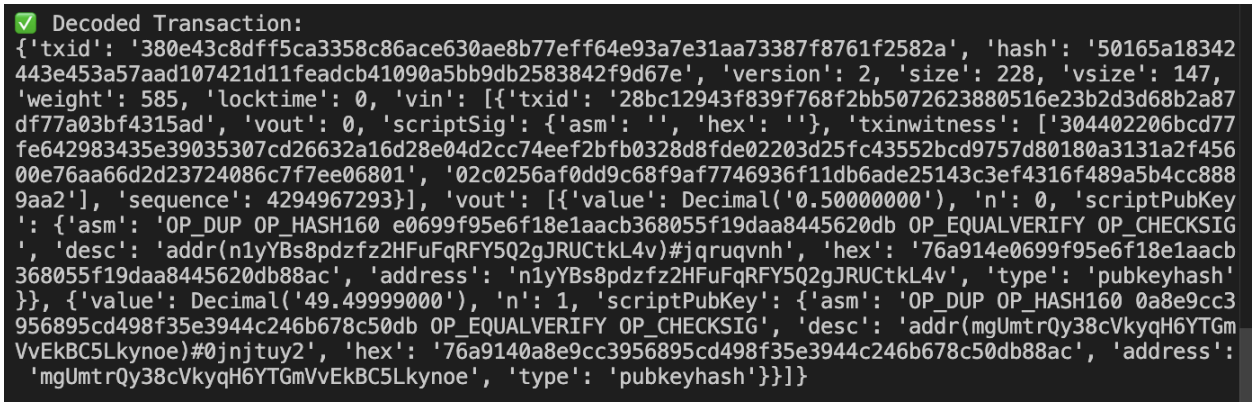
Transaction from B to C (scriptSig):
304402207db4da575f1caf6d2d33df377aafd7be2d5c8e1697870738279b915ee098d1ed022023ec2f2dd37b213fd98aaa48f1e6d266259dbd8df25b1482a49858779c7dc4dc[ALL] 030758180c64321ae222cb9de0be2eb01bf98db8809bfe9475b9928969f6b182e8

Challenge and Response Script Structure

- **Challenge Script (scriptPubKey from A to B): Ensures only B can spend the output by requiring a valid signature matching B's public key.**
- **Response Script (scriptSig in B to C transaction): Provides B's public key and a valid signature proving ownership.**

Screenshots

Decoded Transaction A to B:



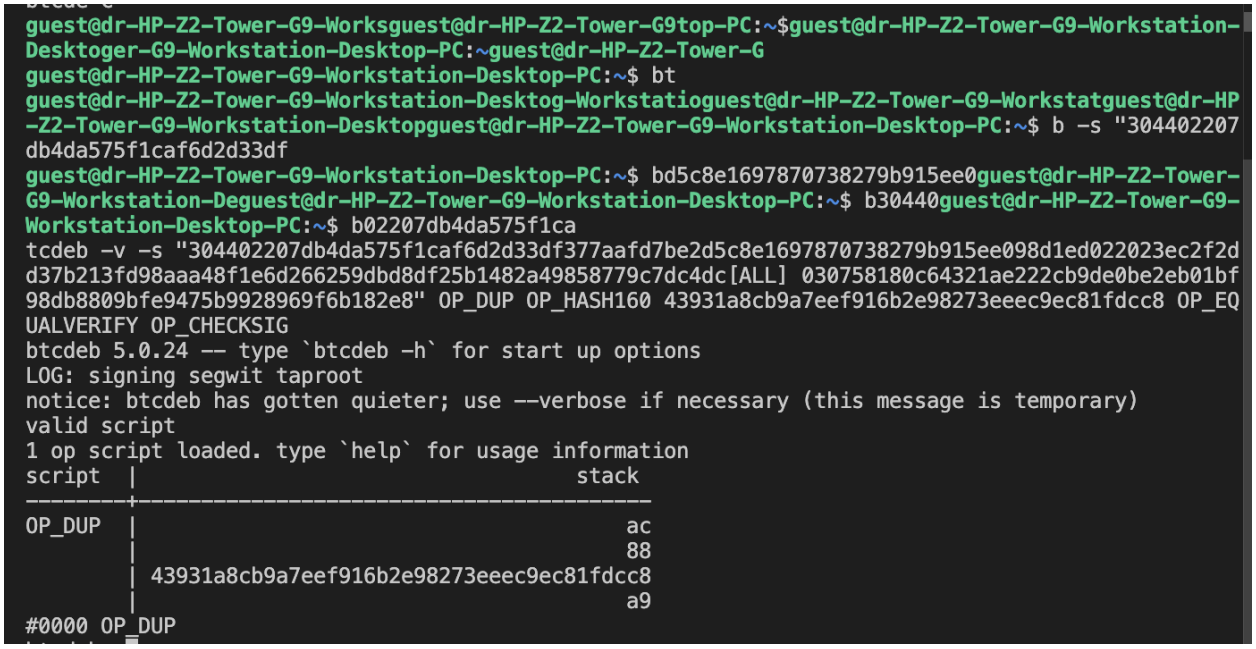
Decoded Transaction B to C:

```
✅ Decoded Transaction: {'txid': 'c2f45d7f5e9346ac67f3460be2e79cabd2c1d03517fec9f10caed0f0fd997fa
b', 'hash': 'c2f45d7f5e9346ac67f3460be2e79cabd2c1d03517fec9f10caed0f0fd997fab', 'version': 2, 'si
ze': 225, 'vsize': 225, 'weight': 900, 'locktime': 0, 'vin': [{'txid': '380e43c8dff5ca3358c86ace6
30ae8b77eff64e93a7e31aa73387f8761f2582a', 'vout': 0, 'scriptSig': {'asm': '304402207db4da575f1caf
6d2d33df377aafd7be2d5c8e1697870738279b915ee098d1ed022023ec2f2dd37b213fd98aaa48f1e6d266259dbd8df25
b1482a49858779c7dc4dc[ALL] 030758180c64321ae222cb9de0be2eb01bf98db8809bfe9475b9928969f6b182e8', '
hex': '47304402207db4da575f1caf6d2d33df377aafd7be2d5c8e1697870738279b915ee098d1ed022023ec2f2dd37b
213fd98aaa48f1e6d266259dbd8df25b1482a49858779c7dc4dc0121030758180c64321ae222cb9de0be2eb01bf98db88
09bfe9475b9928969f6b182e8'}, 'sequence': 4294967293}], 'vout': [{'value': Decimal('0.05000000'),
'n': 0, 'scriptPubKey': {'asm': 'OP_DUP OP_HASH160 43931a8cb9a7eef916b2e98273eeec9ec81fdcc8 OP_EQ
UALVERIFY OP_CHECKSIG', 'desc': 'addr(mmgFnrM3EbcJXGP1FWj1pBZm55xXcYak4E)#vmv2e7zm', 'hex': '76a9
1443931a8cb9a7eef916b2e98273eeec9ec81fdcc888ac', 'address': 'mmgFnrM3EbcJXGP1FWj1pBZm55xXcYak4E',
 'type': 'pubkeyhash'}}, {'value': Decimal('0.44999000'), 'n': 1, 'scriptPubKey': {'asm': 'OP_DUP
 OP_HASH160 e0699f95e6f18e1aacb368055f19daa8445620db OP_EQUALVERIFY OP_CHECKSIG', 'desc': 'addr(n
1yYBs8pdzfz2HFuFqRFY5Q2gJRUCtkL4v)#jqruqvnh', 'hex': '76a914e0699f95e6f18e1aacb368055f19daa844562
0db88ac', 'address': 'n1yYBs8pdzfz2HFuFqRFY5Q2gJRUCtkL4v', 'type': 'pubkeyhash'}}]}
```

Bitcoin debugger executing challenge script

```
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btc
guest@dr-HP-Z2-Tower-G9-Workstation-Desktguest@dr-HP-Z2-Tower-G9-Workstation-Dguest@dr-HP-Z2-Towe
r-G9-Workstatiguest@dr-HP-Z2-Tower-G9-Worksguest@dr-HP-Z2-Tower-G9-Wguest@dr-HP-Z2-Tower-guest@dr
-HP-Z2-Tower-G9-Workstation-Desktop-PCguest@dr-HP-Z2-Tower-G9-Workstation-Deguest@dr-HP-Z2-Tower-
G9-Worguest@dr-HP-Z2-Tower-G9-Workguest@dr-HP-Z2-Tower-G9-Workstationguest@dr-HP-Z2-Tower-G9-Work
station-Desktop-PC:~$ b
tcdeb -v -s "304402206bcd77fe642983435e39035307cd26632a16d28e04d2cc74eef2bfb0328d8fde02203d25fc43
552bcd9757d80180a3131a2f45600e76aa66d2d23724086c7f7ee06801 02c0256af0dd9c68f9af7746936f11db6ade25
143c3ef4316f489a5b4cc8889aa2" OP_DUP OP_HASH160 e0699f95e6f18e1aacb368055f19daa8445620db OP_EQUAL
VERIFY 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)
valid script
1 op script loaded. type `help` for usage information
script  |                                  stack
--------+-------------------------------------
OP_DUP  |                                     ac
        |                                     88
        | e0699f95e6f18e1aacb368055f19daa8445620db
        |                                     a9
#0000 OP_DUP
```

Bitcoin debugger executing response script



Part 2: SegWit Transactions (P2SH-P2WPKH)

Workflow of Transactions

1. **Transaction from A' to B':**
    - **Generated SegWit addresses A', B', and C'.**
    - **Funded A' and created a transaction from A' to B'.**
    - **Decoded the transaction to extract the SegWit script.**
    - **Signed and broadcasted the transaction.**
    - **TxID of transaction from A' to B':**

      3b544b0855be71571df40e749a5abc9bc3bf3339cb3c084d6a4ecaeb8f931903

2. **Transaction from B’ to C’:**

    - **Used 3b544b0855be71571df40e749a5abc9bc3bf3339cb3c084d6a4ecaeb8f931903 as input.**
    - **Funded C’ from B’.**
    - **Signed and broadcasted the transaction.**
    - **TxID of transaction from B’ to C’: 588aa53e94b427374269fd310403b515c54e737c6dc127277d1a20eff4f52003**

Decoded Scripts

Transaction from A’ to B’ (scriptPubKey):

OP_HASH160 66d64bbbe28364786813977274d2f3874c90b435 OP_EQUAL

Transaction from B’ to C’ (scriptSig):
0014bf2fea8a4e9937b21c83b5bd79b00b9949d5c2a8

Challenge and Response Script Structure

- **Challenge Script: Uses SegWit’s native P2WPKH structure to store the public key hash in the witness field.**
- **Response Script: Provides the witness signature and public key to prove ownership.**

Screenshots

Decoded Transaction A to B:

```
✅ Decoded Transaction:
{'txid': '3b544b0855be71571df40e749a5abc9bc3bf3339cb3c084d6a4ecaeb8f931903', 'hash': 'b3a42cf57ea
326da46a0b49b61ec2086cf0d16451c9034147e561c3cf07b89ad', 'version': 2, 'size': 247, 'vsize': 166,
'weight': 661, 'locktime': 0, 'vin': [{'txid': '72c517298e191f0d7ed91857d3b98b3188b3d91ece03f9743
9141e1007c53fd4', 'vout': 0, 'scriptSig': {'asm': '001400de388226ba70348bb5f424163b30764852b913',
 'hex': '16001400de388226ba70348bb5f424163b30764852b913'}, 'txinwitness': ['304402206eb4e3e168634
ef822f738e37c20e3db0290abb73487a732532e5f888eab78a4022005807ce4a731e82253b857c8eb91f2cabdaf00c2ee
a31c0caa8dc3751232061001', '0276d68a6cfd200dfa07b43d1da82c076bf7e74f2c3ff78f5fd8a98f27db356c4f'],
 'sequence': 4294967293}], 'vout': [{'value': Decimal('0.30000000'), 'n': 0, 'scriptPubKey': {'as
m': 'OP_HASH160 66d64bbbe28364786813977274d2f3874c90b435 OP_EQUAL', 'desc': 'addr(2N2cydPMvZHtPAW
AZgd4pfHyZ9KqSoDmn9P)#qevwjh03', 'hex': 'a91466d64bbbe28364786813977274d2f3874c90b43587', 'addres
s': '2N2cydPMvZHtPAWAZgd4pfHyZ9KqSoDmn9P', 'type': 'scripthash'}}, {'value': Decimal('0.19999000'
), 'n': 1, 'scriptPubKey': {'asm': 'OP_HASH160 e6c7aa43c7f65207c9638ce0eef3d3a2c9520044 OP_EQUAL'
, 'desc': 'addr(2NEHUbNwUw6F5ViYi4z79KaNwbM5Z9ay7nN)#a8vvxn6j', 'hex': 'a914e6c7aa43c7f65207c9638
ce0eef3d3a2c952004487', 'address': '2NEHUbNwUw6F5ViYi4z79KaNwbM5Z9ay7nN', 'type': 'scripthash'}}]
}
```

Decoded Transaction B to C:

```
✅ Decoded Transaction:
{'txid': '588aa53e94b427374269fd310403b515c54e737c6dc127277d1a20eff4f52003', 'hash': '917fcab78e3
70f0af50d0047223790c7dba6c05293ebee497028db5db5fc454d', 'version': 2, 'size': 247, 'vsize': 166,
'weight': 661, 'locktime': 0, 'vin': [{'txid': '3b544b0855be71571df40e749a5abc9bc3bf3339cb3c084d6
a4ecaeb8f931903', 'vout': 0, 'scriptSig': {'asm': '0014bf2fea8a4e9937b21c83b5bd79b00b9949d5c2a8',
 'hex': '160014bf2fea8a4e9937b21c83b5bd79b00b9949d5c2a8'}, 'txinwitness': ['30440220157f59db16f9b
8ad5a316fc9f29ed975fd169c1c10b4b1bb597c07d7d8a3a82f022018c84e09465822a4c739983ae4814f9715f9772401
b723ef97c541378937e00201', '03a0771f8ad3031eba20f72530ff9328964ac2447bb285fa7cec6947b9ab4467bf'],
 'sequence': 4294967293}], 'vout': [{'value': Decimal('0.20000000'), 'n': 0, 'scriptPubKey': {'as
m': 'OP_HASH160 fd79b4a6f63a1ec45ceddbbbbd8b64470de9e822 OP_EQUAL', 'desc': 'addr(2NGMUk5L1DgBqeQ
XNsrsvv4oDEMT7GhFLwY)#df8xskun', 'hex': 'a914fd79b4a6f63a1ec45ceddbbbbd8b64470de9e82287', 'addres
s': '2NGMUk5L1DgBqeQXNsrsvv4oDEMT7GhFLwY', 'type': 'scripthash'}}, {'value': Decimal('0.09999000'
), 'n': 1, 'scriptPubKey': {'asm': 'OP_HASH160 66d64bbbe28364786813977274d2f3874c90b435 OP_EQUAL'
, 'desc': 'addr(2N2cydPMvZHtPAWAZgd4pfHyZ9KqSoDmn9P)#qevwjh03', 'hex': 'a91466d64bbbe283647868139
77274d2f3874c90b43587', 'address': '2N2cydPMvZHtPAWAZgd4pfHyZ9KqSoDmn9P', 'type': 'scripthash'}}]
}
```

Bitcoin debugger executing challenge script

```
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb -v -s "04402206eb4e3e168634ef822f738e37c
20e3db0290abb73487a732532e5f888eab78a4022005807ce4a731e82253b857c8eb91f2cabdaf00c2eea31c0caa8dc37
51232061001 0276d68a6cfd200dfa07b43d1da82c076bf7e74f2c3ff78f5fd8a98f27db356c4f" OP_HASH160 66d64b
bbe28364786813977274d2f3874c90b435 OP_EQUAL
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
1 op script loaded. type `help` for usage information
script     |                                  stack
-----------+---------------------------------------
OP_HASH160 |                                     87
           | 66d64bbbe28364786813977274d2f3874c90b435
#0000 OP_HASH160
```

Bitcoin debugger executing response script

```
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb -v -s "30440220157f59db16f9b8ad5a316fc9f
29ed975fd169c1c10b4b1bb597c07d7d8a3a82f022018c84e09465822a4c739983ae4814f9715f9772401b723ef97c541
378937e00201 03a0771f8ad3031eba20f72530ff9328964ac2447bb285fa7cec6947b9ab4467bf" OP_HASH160 fd79b
4a6f63a1ec45ceddbbbbd8b64470de9e822 OP_EQUAL
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
1 op script loaded. type `help` for usage information
script     |                                   stack
-----------+---------------------------------------
OP_HASH160 |                                      87
           | fd79b4a6f63a1ec45ceddbbbbd8b64470de9e822
#0000 OP_HASH160
```

Part 3: Analysis and Explanation

Comparison of P2PKH and SegWit Transactions

Feature	P2PKH (Legacy)	P2SH-P2WPKH (SegWit)
Transaction Size	Larger	Smaller
Script Structure	Uses scriptSig	Uses witness data
Weight/Vbytes	Higher	Lower
Validation	scriptSig executes the full script	Witness separates signature validation

Why SegWit Transactions Are Smaller

- Removes signatures from the main transaction, reducing the size of the transaction.
- Uses `witness` data, which does not count fully towards the block size limit, improving efficiency.

- **Reduces malleability, preventing changes to transaction IDs.**

Benefits of SegWit Transactions

- **Increased transaction throughput due to reduced size.**
- **Lower fees due to reduced weight.**
- **Enables second-layer solutions like Lightning Network.**
