

Bitcoin Scripting Assignment Report

CS 216: Introduction to Blockchain

Bitcoin Scripting

Team Name: HASHPA

Team Members:

- Lawadya Yashwanth Chowhan (230001046)
- M. Mohan Prudhvi Sai (230001047)
- M. Rishik Preetham (230001048)

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. This report details the workflow, transaction details, and comparison of both transaction types using Python and Bitcoin Core RPC.

Part 1: Legacy Address Transactions (P2PKH)

Workflow and Transactions

1. Setup and Wallet Configuration

- Connected to Bitcoin Core using RPC authentication with:
 - RPC User: StandUp
 - RPC Host: 127.0.0.1
 - RPC Port: 18332
- Ensured the wallet "MyNewWallet" exists, loading or creating it if necessary.
- Generated 101 blocks using the `generatetoaddress` command to gain initial balance in regtest mode.

2. Transaction Process

- Generated three legacy addresses:

- i. **Address A:** `rpc_client.getnewaddress("", "legacy")`
- ii. **Address B:** `rpc_client.getnewaddress("", "legacy")`
- iii. **Address C:** `rpc_client.getnewaddress("", "legacy")`
- b. Sent 1 BTC from Address A to Address B: `txid1 = rpc_client.sendtoaddress(address_B, 1.0)`
- c. Sent 0.5 BTC from Address B to Address C: `txid2 = rpc_client.sendtoaddress(address_C, 0.5)`
- d. Decoded the transaction and extracted the locking script (ScriptPubKey) for Address B: `raw_tx = rpc_client.gettransaction(txid1, True)`
`decoded_tx = rpc_client.decoderawtransaction(raw_tx['hex'])`
- e. **ScriptPubKey for Address B:** `mi7ax98TXnsC8mFRgiHTtz12AxFgFEWVSA`.

Decoded Scripts

- Transaction 1 (A → B) Decoded Script:

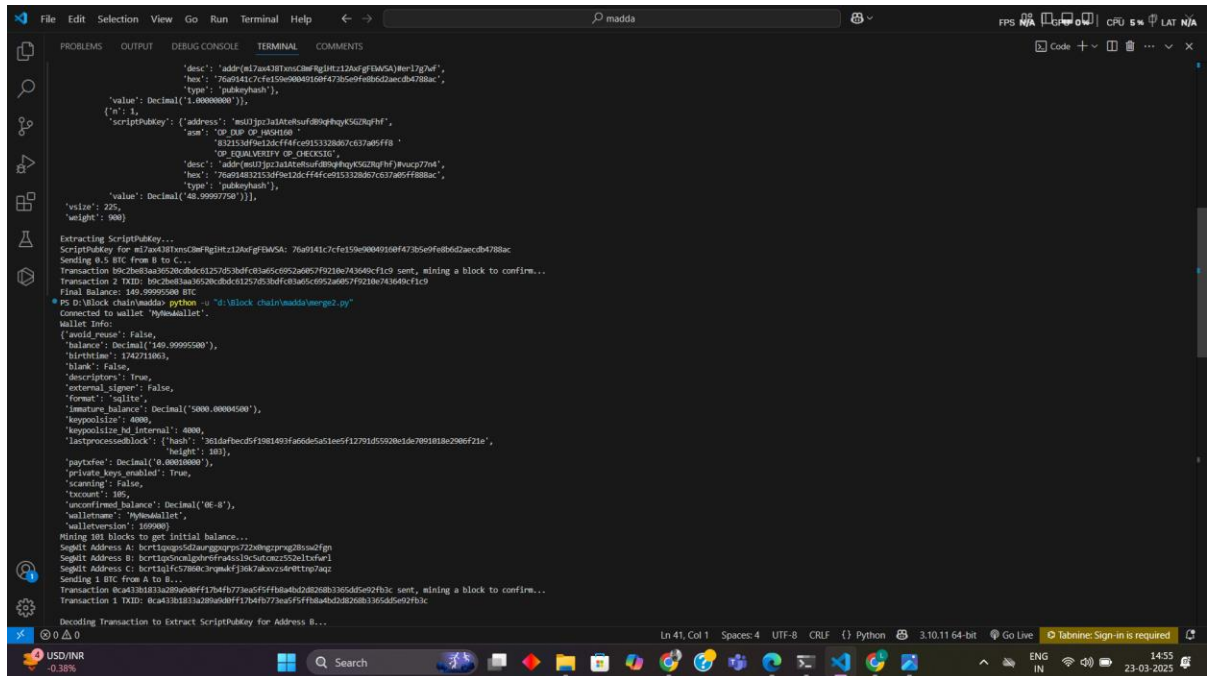
```

PS D:\Block chain\bitcoin> python -u "D:\Block chain\wallet\merge.py"
Wallet "MyNodeWallet" is not loaded. Trying to load it...
Wallet "MyNodeWallet" does not exist. Creating a new one...
Wallet "MyNodeWallet" created successfully.
Connected to wallet "MyNodeWallet".
Wallet Info:
{
  'avoid_reuse': False,
  'balance': Decimal('0.0'),
  'birthtime': 174271863,
  'blake': False,
  'descriptors': True,
  'external_signer': False,
  'format': 'sqlite',
  'immature_balance': Decimal('0.0'),
  'keypoolsize': 4000,
  'keypoolsize_hd_internal': 4000,
  'last_tx_rechash': {'hash': '0f9188f13b70c71f2a335e3af328f52eb436812afca9981a1466e2206',
    'height': 0},
  'paytoeer': Decimal('0.00000000'),
  'private_keys_enabled': True,
  'scanning': False,
  'txoutroot': 0,
  'unconfirmed_balance': Decimal('0.0'),
  'walletname': 'MyNodeWallet',
  'walletversion': 109900
}
Mining 999 blocks to get initial balance...
Legacy Address A: mzaA5oQpQg123ah011ig2vry6GCCR
Legacy Address B: m17ax98TXnsC8mFRgiHTtz12AxFgFEWVSA
Legacy Address C: muf5w6cKX0F4Kac226w0j70scripA
Sending 1 BTC from A to B...
Transaction 06e7a938cf112b0c3895ceb8375514a32399dc19337a4789c3ef935635a2 sent, mining a block to confirm...
Transaction 1 TXID: 06e7a938cf112b0c3895ceb8375514a32399dc19337a4789c3ef935635a2

Decoding Transaction to Extract ScriptPubKey for Address B...

Decoded Transaction:
{
  'hash': '06e7a938cf112b0c3895ceb8375514a32399dc19337a4789c3ef935635a2',
  'locktime': 0,
  'size': 225,
  'txid': '06e7a938cf112b0c3895ceb8375514a32399dc19337a4789c3ef935635a2',
  'version': 2,
  'vin': [
    {
      'scriptSig': [
        'asm: [304402202419321b72b7276ccf7abcc1f8dc7981f4c3914958aaaf47681586e2264af80220090eebd234bf8187c0f4aaac9f7ed28b1b1809837613513128172df2e907c[ALL] '
        '02529180f495d1c540bc1f4e9b40f4018d2d8d105c7a0b084020eb3574',
        'hex: 47304402202419321b72b7276ccf7abcc1f8dc7981f4c3914958aaaf47681586e2264af80220090eebd234bf8187c0f4aaac9f7ed28b1b1809837613513128172df2e907c012182529786f495d1c5f69c1f4e9b40f4018d2d8d105c7a0b084020eb3574'
      ],
      'sequence': 4294967293,
      'txid': '8bf0a49770a5945e8843d59e798f53ed0444243f98293813807f9dc3f694',
      'vout': 0
    }
  ],
  'vout': [
    {
      'address': 'mi7ax98TXnsC8mFRgiHTtz12AxFgFEWVSA',
      'scriptPubKey': [
        'asm: OP_DUP OP_HASH160 '
        '1c7cfe1599004910f47365e9feb6d2accdb47 '
        'OP_EQUALVERIFY OP_CHECKSIG',
        'desc: addr[mi7ax98TXnsC8mFRgiHTtz12AxFgFEWVSA]#013gaf'
      ]
    }
  ]
}
  
```

- Transaction 2 (B → C) Decoded Script:



Challenge and Response Script Analysis

- **Challenge Script (ScriptPubKey):** This script locks the output using the recipient's public key hash.
- **Response Script (ScriptSig):** This script contains the unlocking signature and public key, proving ownership.
- **Bitcoin Debugger Validation:** The script execution confirmed that the provided signatures correctly matched the locking conditions.

Part 2: SegWit Address Transactions (P2SH-P2WPKH)

Workflow and Transactions

1. **Wallet Setup and Balance Initialization**
 - a. Used the same wallet as in Part 1.
 - b. Generated 101 blocks to maintain balance.
2. **Transaction Process**
 - a. Generated three SegWit addresses:
 - i. **Address A:** `rpc_client.getnewaddress("", "bech32")`

- ii. **Address B'**: `rpc_client.getnewaddress("", "bech32")`
- iii. **Address C'**: `rpc_client.getnewaddress("", "bech32")`
- b. Sent 1 BTC from Address A' to Address B':

`txid1 = rpc_client.sendtoaddress(address_B, 1.0)`

- c. Decoded the transaction and extracted the locking script (ScriptPubKey) for Address B'.
- d. Sent 0.5 BTC from Address B' to Address C':

`txid2 = rpc_client.sendtoaddress(address_C, 0.5)`

- e. Decoded and validated the transaction scripts.

Decoded Scripts

- **Transaction 1 (A' → B') Decoded Script:**

```

{
  "desc": "addr(m17ea38Tmc3WfRgHt12bafgF4M5A)w1z7w4",
  "hex": "76a914c7cf159e000910f4735e9f0b6d2aecd478bac",
  "type": "pubkeyhash",
  "value": Decimal("1.00000000")
},
{
  "n": 1,
  "scriptPubKey": {
    "address": "m17ea38Tmc3WfRgHt12bafgF4M5A",
    "asm": "OP_DUP OP_HASH160",
    "hex": "812153ff9c12dcff4fce91532867c637a05ff8",
    "op": "OP_EQUALVERIFY OP_CHECKSIG",
    "desc": "addr(m17ea38Tmc3WfRgHt12bafgF4M5A)w1z7w4",
    "hex": "76a914812153ff9c12dcff4fce91532867c637a05ff8bac",
    "type": "pubkeyhash",
    "value": Decimal("0.50000000")
  },
  "vsize": 225,
  "weight": 900
}

```

Extracting ScriptPubKey...

ScriptPubKey for m17ea38Tmc3WfRgHt12bafgF4M5A: 76a914c7cf159e000910f4735e9f0b6d2aecd478bac

Sending 0.5 BTC from B to C...

Transaction 1 TXID: b9c2b8ba3052bdc61257d53bfc83a65c6952a0579210e743649cf1c9

Final balance: 149.99999999 BTC

PS D:\Block chain\maddas python -u "D:\Block chain\maddas\vergo2.py"

Connected to wallet 'Hydrallet'.

Wallet Info:

```

{
  'avoid_reuse': False,
  'balance': Decimal('149.99999999'),
  'blktime': 1742711063,
  'blank': False,
  'descriptors': True,
  'external_signer': False,
  'format': 'sqlite',
  'immature_balance': Decimal('5000.00000000'),
  'keypoolsize': 4000,
  'keypoolsize_hd_internal': 4000,
  'lastprocessedblock': {
    'hash': '381d8f8cd5f1081403fa6d6a5c1e5f12791d55920e1de7095818e200ef21e',
    'weight': 180
  },
  'paytxfee': Decimal('0.00010000'),
  'private_keys_enabled': True,
  'scanning': False,
  'txcount': 105,
  'unconfirmed_balance': Decimal('0E-8'),
  'walletname': 'Hydrallet',
  'walletversion': 169900
}

```

Mining 101 blocks to get initial balance...

Segwit Address A: bct1p9a5d2uagup9n72zabgrrpg280sdzfn

Segwit Address B: bct1p9c0nagahvfrak5l9c5utcz552eltafw1

Segwit Address C: bct1p9fc57808c3rpkafj3k7akvzsd4rtttrp7aiz

Sending 1 BTC from A to B...

Transaction 0ca4381813a208a0d8ff17b4f773a6f5f8a4bd2d8268b3365dd5e02fb3c sent, mining a block to confirm...

Transaction 1 TXID: 0ca4381813a208a0d8ff17b4f773a6f5f8a4bd2d8268b3365dd5e02fb3c

Decoding Transaction to Extract ScriptPubKey for Address B...

- **Transaction 2 (B' → C') Decoded Script:**

```
Decoded Transaction to Extract ScriptPubKey for Address B...

Decoded Transaction:
{
  'hash': '0ca13813a289a9df12704b773eaf5f4b04b2d8268b3365d5e91b3c',
  'locktime': 204,
  'size': 219,
  'txid': '0ca13813a289a9df12704b773eaf5f4b04b2d8268b3365d5e91b3c',
  'version': 2,
  'vin': [
    {
      'scriptSig': {
        'asm': '384802807caba188fb2476eade18ce27e81014ed277a223940e8006584c62aer9b2002200c3aeba1b238747449cc9a9f78f2be56833483ba47c0df8c5e4fbc4db499[ALL]'
      },
      'hex': '47384802807caba188fb2476eade18ce27e81014ed277a223940e8006584c62aer9b2002200c3aeba1b238747449cc9a9f78f2be56833483ba47c0df8c5e4fbc4db499012103b36c267d43678a12cbb1e67efc1bc8771d53cf9a05897a2f778fa36c20d6',
      'sequence': 4294867293,
      'txid': '0ca13813a289a9df12704b773eaf5f4b04b2d8268b3365d5e91b3c',
      'vout': 1,
      'scriptPubKey': {
        'address': 'bcrt1q5ncmlgphr6fradss19c5utcmz552oltxfw1',
        'asm': '0 35278af4a0d4f491f6b87cb8a71788854a2b3f',
        'desc': 'addr(bcrt1q5ncmlgphr6fradss19c5utcmz552oltxfw1)#0e9ef6w',
        'hex': '001435278af4a0d4f491f6b87cb8a71788854a2b3f',
        'type': 'witness_v0_keyhash',
        'value': Decimal('1.00000000')
      }
    },
    {
      'scriptPubKey': {
        'address': 'bcrt1qypa2651h66t4dz57gchuyayxpfms8ugerk',
        'asm': '0 1183d56e9fbeb4b454f0918bfb0c4e9c3ba770',
        'desc': 'addr(bcrt1qypa2651h66t4dz57gchuyayxpfms8ugerk)#G2p8t4dm',
        'hex': '00141183d56e9fbeb4b454f0918bfb0c4e9c3ba770',
        'type': 'witness_v0_keyhash',
        'value': Decimal('47.9999560')
      }
    }
  ],
  'vsize': 219,
  'weight': 876,
  'vin': [
    {
      'scriptPubKey': {
        'address': 'bcrt1qypa2651h66t4dz57gchuyayxpfms8ugerk',
        'asm': '0 1183d56e9fbeb4b454f0918bfb0c4e9c3ba770',
        'desc': 'addr(bcrt1qypa2651h66t4dz57gchuyayxpfms8ugerk)#G2p8t4dm',
        'hex': '00141183d56e9fbeb4b454f0918bfb0c4e9c3ba770',
        'type': 'witness_v0_keyhash',
        'value': Decimal('47.9999560')
      }
    },
    {
      'scriptPubKey': {
        'address': 'bcrt1qypa2651h66t4dz57gchuyayxpfms8ugerk',
        'asm': '0 1183d56e9fbeb4b454f0918bfb0c4e9c3ba770',
        'desc': 'addr(bcrt1qypa2651h66t4dz57gchuyayxpfms8ugerk)#G2p8t4dm',
        'hex': '00141183d56e9fbeb4b454f0918bfb0c4e9c3ba770',
        'type': 'witness_v0_keyhash',
        'value': Decimal('47.9999560')
      }
    },
    {
      'scriptPubKey': {
        'address': 'bcrt1qypa2651h66t4dz57gchuyayxpfms8ugerk',
        'asm': '0 1183d56e9fbeb4b454f0918bfb0c4e9c3ba770',
        'desc': 'addr(bcrt1qypa2651h66t4dz57gchuyayxpfms8ugerk)#G2p8t4dm',
        'hex': '00141183d56e9fbeb4b454f0918bfb0c4e9c3ba770',
        'type': 'witness_v0_keyhash',
        'value': Decimal('47.9999560')
      }
    },
    {
      'scriptPubKey': {
        'address': 'bcrt1qypa2651h66t4dz57gchuyayxpfms8ugerk',
        'asm': '0 1183d56e9fbeb4b454f0918bfb0c4e9c3ba770',
        'desc': 'addr(bcrt1qypa2651h66t4dz57gchuyayxpfms8ugerk)#G2p8t4dm',
        'hex': '00141183d56e9fbeb4b454f0918bfb0c4e9c3ba770',
        'type': 'witness_v0_keyhash',
        'value': Decimal('47.9999560')
      }
    }
  ],
  'vsize': 219,
  'weight': 876
}
```

```

{
  'asm': '0 1183d56e9fbeb4b454f0918bfb0c4e9c3ba770',
  'scriptPubKey': {
    'address': 'bcrt1qypa2651h66t4dz57gchuyayxpfms8ugerk',
    'asm': '0 1183d56e9fbeb4b454f0918bfb0c4e9c3ba770',
    'desc': 'addr(bcrt1qypa2651h66t4dz57gchuyayxpfms8ugerk)#G2p8t4dm',
    'hex': '00141183d56e9fbeb4b454f0918bfb0c4e9c3ba770',
    'type': 'witness_v0_keyhash',
    'value': Decimal('47.9999560')
  }
},
{
  'vsize': 219,
  'weight': 876
}

Extracting ScriptPubKey...
ScriptPubKey for bcrt1q5ncmlgphr6fradss19c5utcmz552oltxfw1: 001435278af4a0d4f491f6b87cb8a71788854a2b3f
Sending 0.5 BTC from B to C...
Transaction 5837ceb08ebc22d807a7f0f383d566a609a6b6f1e70ceac7ab66ad05f9a09b3 sent, mining a block to confirm...
Transaction 2 TXID: 5837ceb08ebc22d807a7f0f383d566a609a6b6f1e70ceac7ab66ad05f9a09b3
Final Balance: 5229.999991529 BTC
PS D:\block chain\maddas
```

Challenge and Response Script Analysis

- **Challenge Script (Witness Program):** The locking mechanism uses a SegWit script that relies on a separate witness stack.

- **Response Script (Witness Stack):** The witness data contains the public key and signature for validation.
- **Bitcoin Debugger Validation:** Verified that the witness data correctly satisfies the spending conditions.

Part 3: Analysis and Comparison

Transaction Size Comparison

Transaction Type	Size (vbytes)	Efficiency
P2PKH (Legacy)	Larger (225)	Less efficient
P2SH-SegWit	Smaller (219)	More efficient

Key Differences in Script Structures

Feature	P2PKH (Legacy)	P2SH-P2WPKH (SegWit)
Challenge Script	ScriptPubKey	Witness Program
Response Script	ScriptSig	Witness Stack
Transaction Size	Larger	Smaller
Fee Efficiency	Higher Fees	Lower Fees

Why SegWit Transactions are Smaller and Their Benefits

- **Smaller Transaction Size:** SegWit removes the signature data from the main transaction structure, significantly reducing size.
- **Lower Fees:** Due to reduced transaction weight, fees are lower compared to legacy transactions.
- **Fix for Transaction Malleability:** The segregated witness structure prevents TXID modifications, enhancing security and enabling features like the Lightning Network.

Bitcoin Debugging

P2PKH (Legacy)

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\lamad> ssh guest@10.206.4.201
guest@10.206.4.201's password:
Permission denied, please try again.
guest@10.206.4.201's password:
Permission denied, please try again.
guest@10.206.4.201's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

12 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sun Mar 23 13:06:11 2025 from 10.15.3.238
guest@10.206.4.201:~$ btcdeb -v '47304402207ca8a188fb24766eade18bce27e081014ed277a8228460e0046b84c62aec9b2002200c3aeba1b23d87474496ce9a9f30f2b
e56833483ba47cbdf86c5e4f8c4db4699012102b306267d43678a12cbb61e67e3fe1bc8771dd53cf50a59d97a2f738fa36c20d676a914832153df9e12dcff4fce9153328d67c637a05ff888ac'
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
7 op script loaded. type 'help' for usage information

script | stack
-----|-----
304402207ca8a188fb24766eade18bce27e081014ed277a8228460e0046b84c... |
02b306267d43678a12cbb61e67e3fe1bc8771dd53cf50a59d97a2f738fa36c20d6 |
OP_DUP |
OP_HASH160 |
832153df9e12dcff4fce9153328d67c637a05ff8 |
OP_EQUALVERIFY |
OP_CHECKSIG |
#0000 304402207ca8a188fb24766eade18bce27e081014ed277a8228460e0046b84c62aec9b2002200c3aeba1b23d87474496ce9a9f30f2be56833483ba47cbdf86c5e4f8c4db469901
btcdeb> client_loop: send disconnect: Connection reset
PS C:\Users\lamad>
```

P2SH-P2WPKH (SegWit)

```
guest@dr-HP-Z2-Tower-G9-V x + v FPS N/A GPU 0% CPU 5% LAT N/A
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\lawad> ssh guest@10.206.4.201
guest@10.206.4.201's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

12 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sun Mar 23 14:55:44 2025 from 10.18.6.29
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb -v '001435278dfd06b8f491f6b087cb8a7178d8854a2b3f47304402207ca8a188fb24766eade18bce27e081014ed277a82
28460e0046b84c62aec9b2002200c3aeb1b23d87474496ce9a9f30f2be56833483ba47cbdf86c5e4f8c4db4699012102b306267d43678a12cbb61e67e3fe1bc8771dd53cf50a59d97a2f738fa36
c20d6'
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
4 op script loaded. type 'help' for usage information
script ----- | stack
0 |
35278dfd06b8f491f6b087cb8a7178d8854a2b3f |
304402207ca8a188fb24766eade18bce27e081014ed277a8228460e0046b84c... |
02b306267d43678a12cbb61e67e3fe1bc8771dd53cf50a59d97a2f738fa36c20d6 |
#0000 0 |
btcdeb> |
```

Conclusion

This assignment successfully demonstrated the creation and analysis of both Legacy (P2PKH) and SegWit (P2SH-P2WPKH) transactions. Through script analysis and transaction comparisons, we observed the efficiency of SegWit transactions over legacy transactions. The use of the Bitcoin Debugger provided deeper insights into the locking and unlocking mechanisms of each transaction type.