**Bitcoin Scripting Assignment**

# Bitcoin Scripting

## Introduction

This report presents an in-depth analysis of Bitcoin transaction scripts, comparing the traditional Legacy (P2PKH) format with the newer Segregated Witness (SegWit) format. Bitcoin's scripting system is a stack-based language that determines transaction validity through cryptographic challenges and responses.

## Key Scripting Components

The scripting system consists of two primary components:

- **ScriptPubKey (Locking Script)**: Placed on outputs, defining conditions required to spend bitcoins.
- **ScriptSig (Unlocking Script)**: Provided by the spender to satisfy the conditions in the ScriptPubKey.

The objectives of this assignment are to:

- Create and analyze Legacy (P2PKH) transactions in a controlled regtest environment.
- Create and analyze SegWit transactions in the same environment.
- Compare transaction structures, sizes, and scripts.
- Understand the benefits and implications of the SegWit upgrade.

All transactions were created in Bitcoin Core’s regtest mode, which provides a controlled environment for testing without requiring real bitcoins.

---

# 1. Bitcoin Configuration and Fee Settings

To ensure appropriate transaction fees and confirmation times, the following settings were added/updated in the `bitcoin.conf` file:

## 1.1 Bitcoin Core Configuration (`bitcoin.conf`)

```
paytxfee=0.0001
fallbackfee=0.0002
mintxfee=0.00001
txconfirmtarget=6
```

To automate the configuration, a Python script was used to dynamically update these settings:

```
import os
BITCOIN_CONF_PATH = os.path.expandvars(r"%APPDATA%\Bitcoin\bitcoin.conf")
config_updates = {
    "paytxfee": "0.0001",
    "fallbackfee": "0.0002",
    "mintxfee": "0.00001",
    "txconfirmtarget": "6"
}

def update_bitcoin_conf():
    if os.path.exists(BITCOIN_CONF_PATH):
        with open(BITCOIN_CONF_PATH, "r") as file:
            config_lines = file.readlines()
    else:
        config_lines = []

    config_dict = {line.split("=")[0].strip(): line.split("=")[1].strip()
for line in config_lines if "=" in line and not line.startswith("#")}
    config_dict.update(config_updates)

    with open(BITCOIN_CONF_PATH, "w") as file:
        file.writelines([f"{key}={value}\n" for key, value in
config_dict.items()])
```

This script ensures that the necessary fee parameters are correctly set before transaction execution.

---

# 2. Legacy (P2PKH) Transactions

## 2.1 Transaction Flow Overview

Legacy transactions use the Pay-to-Public-Key-Hash (P2PKH) format, which is the traditional Bitcoin address format. The transaction flow follows:

- **Address A → Address B**
- **Address B → Address C**

**Transaction IDs:**

- **Funding TX**: 9ce50f8a9a03142c793641a3e5f586f898aab7958541c19e5fbeb363e4c85126
- **A to B TX**: 5d814a8d9fab5990c5ef4809d0aff0df1b48ec19f99b7ea9aa794b24613cc6d3

## 2.2 Script Analysis

### 2.2.1 Locking Script (ScriptPubKey) for Address B

**P2PKH Locking Script:**

```
OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
```

### 2.2.2 Unlocking Script (ScriptSig) in B to C Transaction

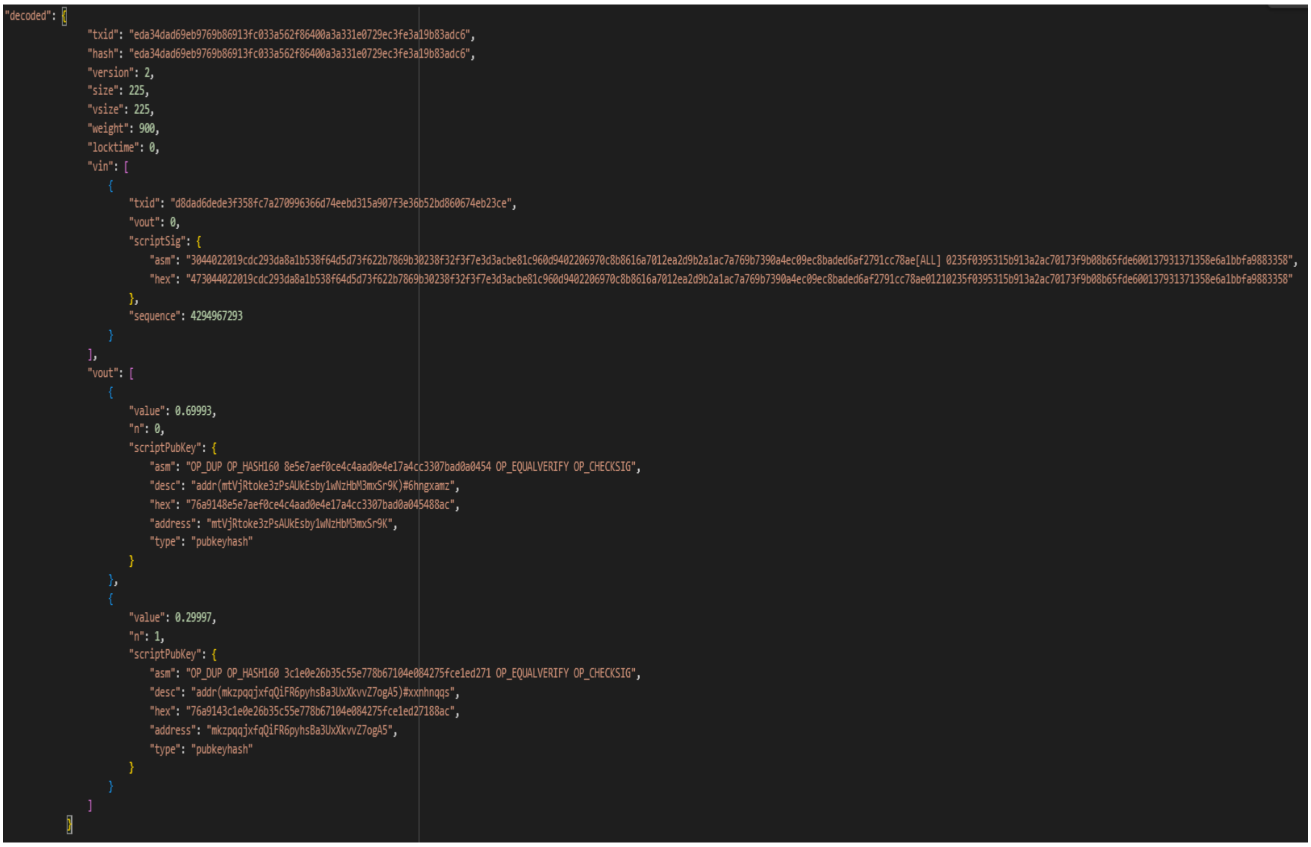
**P2PKH Unlocking Script:**

```
<Signature> <PublicKey>
```

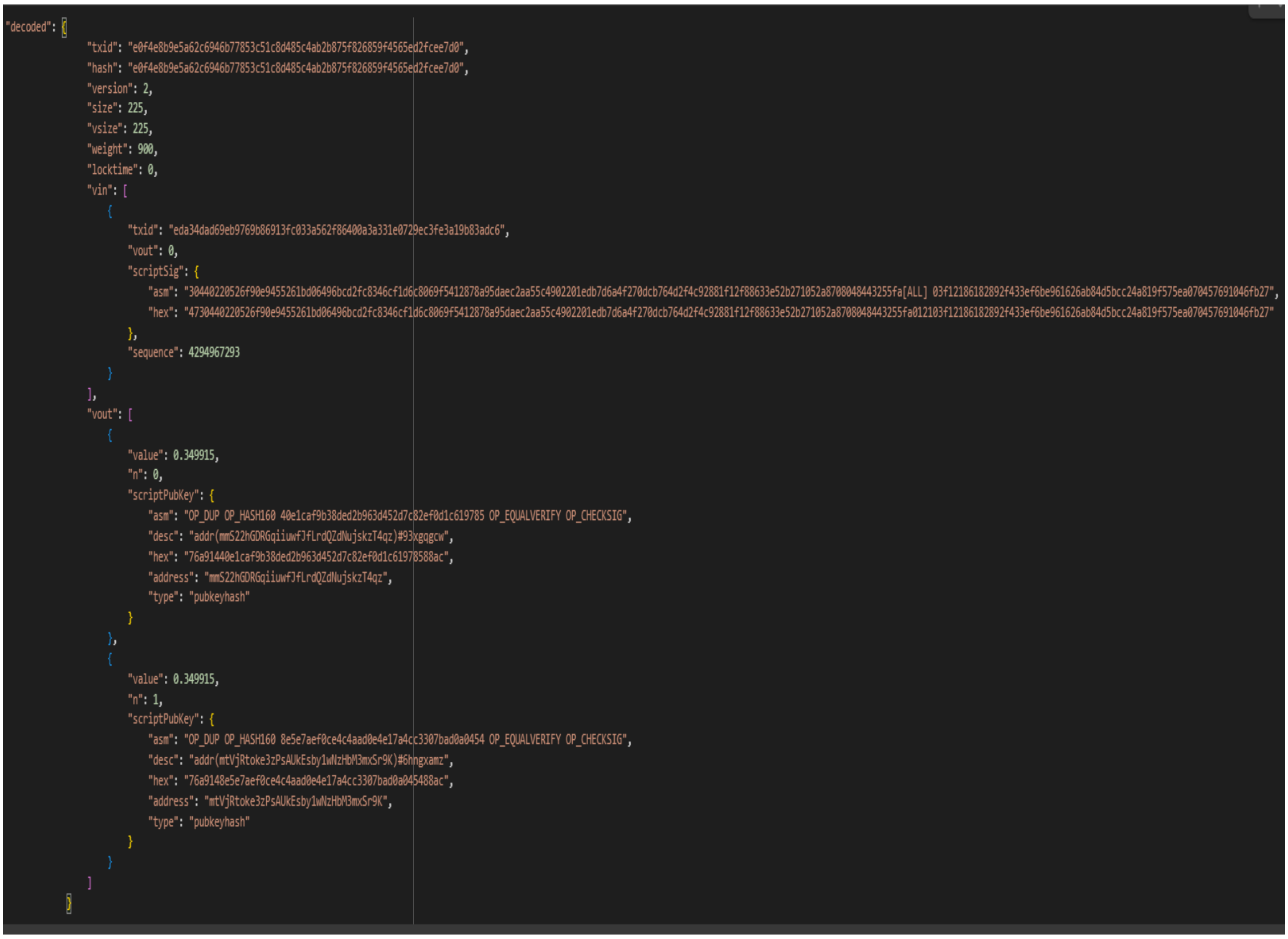
This script provides two critical pieces of data:

- The digital signature, which proves ownership of the private key.
- The public key, which when hashed should match the hash in the locking script.

### Decoded scripts A to B && B to C

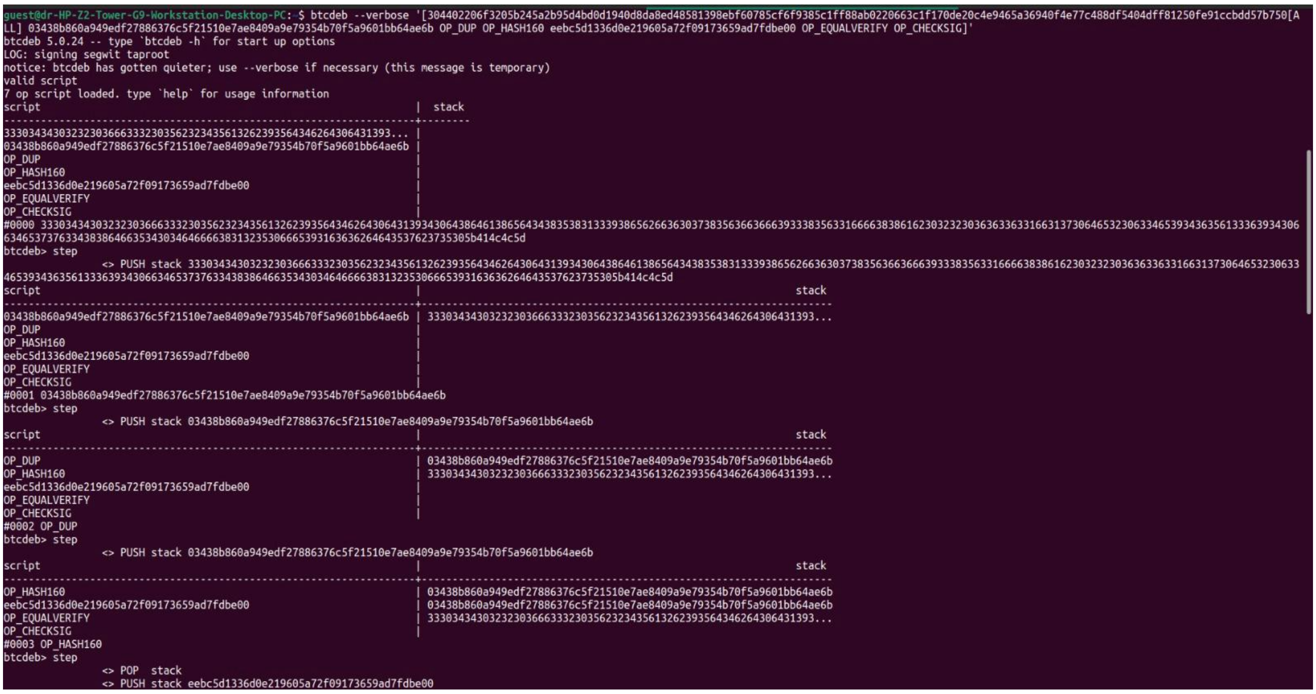


```
"decoded": {
                "txid": "eda34dad69eb9769b86913fc033a562f86400a3a331e0729ec3fe3a19b83adc6",
                "hash": "eda34dad69eb9769b86913fc033a562f86400a3a331e0729ec3fe3a19b83adc6",
                "version": 2,
                "size": 225,
                "vsize": 225,
                "weight": 900,
                "locktime": 0,
                "vin": [
                    {
                        "txid": "d8dad6dede3f358fc7a270996366d74eebd315a907f3e36b52bd860674eb23ce",
                        "vout": 0,
                        "scriptSig": {
                            "asm": "3044022019cdc293da8a1b538f64d5d73f622b7869b30238f32f3f7e3d3acbe81c960d9402206970c8b8616a7012ea2d9b2a1ac7a769b7390a4ec09ec8baded6af2791cc78ae[ALL] 0235f0395315b913a2ac70173f9b08b65fde600137931371358e6a1bbfa9883358",
                            "hex": "473044022019cdc293da8a1b538f64d5d73f622b7869b30238f32f3f7e3d3acbe81c960d9402206970c8b8616a7012ea2d9b2a1ac7a769b7390a4ec09ec8baded6af2791cc78ae01210235f0395315b913a2ac70173f9b08b65fde600137931371358e6a1bbfa9883358"
                        },
                        "sequence": 4294967293
                    }
                ],
                "vout": [
                    {
                        "value": 0.69993,
                        "n": 0,
                        "scriptPubKey": {
                            "asm": "OP_DUP OP_HASH160 8e5e7aef0ce4c4aad0e4e17a4cc3307bad0a0454 OP_EQUALVERIFY OP_CHECKSIG",
                            "desc": "addr(mtVjRtoke3zPsAUkEsby1wNzHbM3mxSr9K)#6hngxamz",
                            "hex": "76a9148e5e7aef0ce4c4aad0e4e17a4cc3307bad0a045488ac",
                            "address": "mtVjRtoke3zPsAUkEsby1wNzHbM3mxSr9K",
                            "type": "pubkeyhash"
                        }
                    },
                    {
                        "value": 0.29997,
                        "n": 1,
                        "scriptPubKey": {
                            "asm": "OP_DUP OP_HASH160 3c1e0e26b35c55e778b67104e084275fce1ed271 OP_EQUALVERIFY OP_CHECKSIG",
                            "desc": "addr(mkzpqqjxfqQiFR6pyhsBa3UxXkvvZ7ogA5)#xxnhnqqs",
                            "hex": "76a9143c1e0e26b35c55e778b67104e084275fce1ed27188ac",
                            "address": "mkzpqqjxfqQiFR6pyhsBa3UxXkvvZ7ogA5",
                            "type": "pubkeyhash"
                        }
                    }
                ]
            }
```

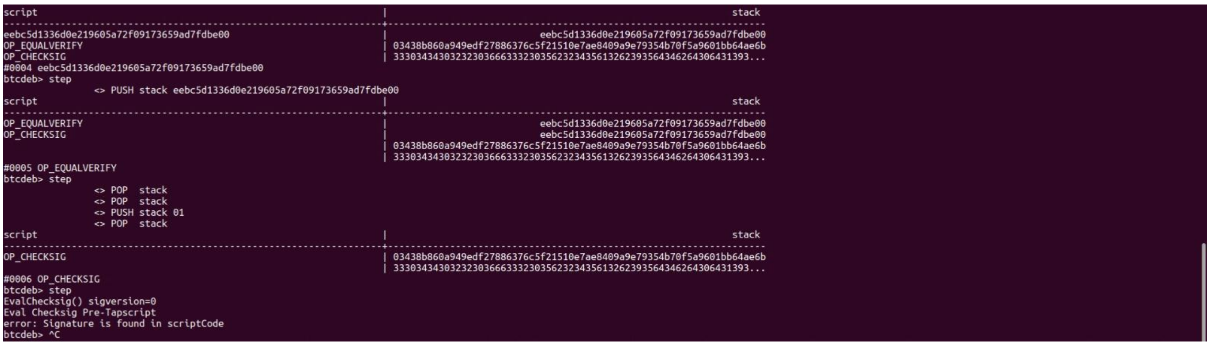


```
"decoded": {
        "txid": "e0f4e8b9e5a62c6946b77853c51c8d485c4ab2b875f826859f4565ed2fcee7d0",
        "hash": "e0f4e8b9e5a62c6946b77853c51c8d485c4ab2b875f826859f4565ed2fcee7d0",
        "version": 2,
        "size": 225,
        "vsize": 225,
        "weight": 900,
        "locktime": 0,
        "vin": [
            {
                "txid": "eda34dad69eb9769b86913fc033a562f86400a3a331e0729ec3fe3a19b83adc6",
                "vout": 0,
                "scriptSig": {
                    "asm": "30440220526f90e9455261bd06496bcd2fc8346cf1d6c8069f5412878a95daec2aa55c4902201edb7d6a4f270dcb764d2f4c92881f12f88633e52b271052a8708048443255fa[ALL] 03f12186182892f433ef6be961626ab84d5bcc24a819f575ea070457691046fb27",
                    "hex": "4730440220526f90e9455261bd06496bcd2fc8346cf1d6c8069f5412878a95daec2aa55c4902201edb7d6a4f270dcb764d2f4c92881f12f88633e52b271052a8708048443255fa012103f12186182892f433ef6be961626ab84d5bcc24a819f575ea070457691046fb27"
                },
                "sequence": 4294967293
            }
        ],
        "vout": [
            {
                "value": 0.349915,
                "n": 0,
                "scriptPubKey": {
                    "asm": "OP_DUP OP_HASH160 40e1caf9b38ded2b963d452d7c82ef0d1c619785 OP_EQUALVERIFY OP_CHECKSIG",
                    "desc": "addr(mmS22hGDRGqiiuwfJfLrdQZdNujskzT4qz)#93xgqgcw",
                    "hex": "76a91440e1caf9b38ded2b963d452d7c82ef0d1c61978588ac",
                    "address": "mmS22hGDRGqiiuwfJfLrdQZdNujskzT4qz",
                    "type": "pubkeyhash"
                }
            },
            {
                "value": 0.349915,
                "n": 1,
                "scriptPubKey": {
                    "asm": "OP_DUP OP_HASH160 8e5e7aef0ce4c4aad0e4e17a4cc3307bad0a0454 OP_EQUALVERIFY OP_CHECKSIG",
                    "desc": "addr(mtVjRtoke3zPsAUkEsby1wNzHbM3mxSr9K)#6hngxamz",
                    "hex": "76a9148e5e7aef0ce4c4aad0e4e17a4cc3307bad0a045488ac",
                    "address": "mtVjRtoke3zPsAUkEsby1wNzHbM3mxSr9K",
                    "type": "pubkeyhash"
                }
            }
        ]
    }
```

## Bitcoin Debugging



```
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb --verbose '[304402206f3205b245a2b95d4bd0d1940d8da8ed48581398ebf60785cf6f9385c1ff88ab0220663c1f170de20c4e9465a36940f4e77c488df5404dff81250fe91ccbdd57b750[A
LL] 03438b860a949edf27886376c5f21510e7ae8409a9e79354b70f5a9601bb64ae6b OP_DUP OP_HASH160 eebc5d1336d0e219605a72f09173659ad7fdbe00 OP_EQUALVERIFY 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
7 op script loaded. type `help` for usage information
script                                                             |  stack
-------------------------------------------------------------------+--------
3330343430323230366633323035623234356132623935643462643064313934... |
03438b860a949edf27886376c5f21510e7ae8409a9e79354b70f5a9601bb64ae6b |
OP_DUP                                                             |
OP_HASH160                                                         |
eebc5d1336d0e219605a72f09173659ad7fdbe00                           |
OP_EQUALVERIFY                                                     |
OP_CHECKSIG                                                        |
#0000 33303434303232303666333230356232343561326239356434626430643139343064386461386564343835383133393865626636303738356366366639333835633166663838616230323230363633633166313730646532306334653934363561333639343066
6346537376334383864663534303464666638313235306665393163636264643537623735305b414c4c5d
btcdeb> step
                <> PUSH stack 333034343032323036663332303562323435613262393564346264306431393430643864613865643438353831333938656266363037383563663666393338356331666638386162303232303636336331663137306465323063
4653934363561333639343066346537376334383864663534303464666638313235306665393163636264643537623735305b414c4c5d
script                                                             |                                                              stack
-------------------------------------------------------------------+-------------------------------------------------------------------
03438b860a949edf27886376c5f21510e7ae8409a9e79354b70f5a9601bb64ae6b | 3330343430323230366633323035623234356132623935643462643064313934...
OP_DUP                                                             |
OP_HASH160                                                         |
eebc5d1336d0e219605a72f09173659ad7fdbe00                           |
OP_EQUALVERIFY                                                     |
OP_CHECKSIG                                                        |
#0001 03438b860a949edf27886376c5f21510e7ae8409a9e79354b70f5a9601bb64ae6b
btcdeb> step
                <> PUSH stack 03438b860a949edf27886376c5f21510e7ae8409a9e79354b70f5a9601bb64ae6b
script                                                             |                                                              stack
-------------------------------------------------------------------+-------------------------------------------------------------------
OP_DUP                                                             | 03438b860a949edf27886376c5f21510e7ae8409a9e79354b70f5a9601bb64ae6b
OP_HASH160                                                         | 3330343430323230366633323035623234356132623935643462643064313934...
eebc5d1336d0e219605a72f09173659ad7fdbe00                           |
OP_EQUALVERIFY                                                     |
OP_CHECKSIG                                                        |
#0002 OP_DUP
btcdeb> step
                <> PUSH stack 03438b860a949edf27886376c5f21510e7ae8409a9e79354b70f5a9601bb64ae6b
script                                                             |                                                              stack
-------------------------------------------------------------------+-------------------------------------------------------------------
OP_HASH160                                                         | 03438b860a949edf27886376c5f21510e7ae8409a9e79354b70f5a9601bb64ae6b
eebc5d1336d0e219605a72f09173659ad7fdbe00                           | 03438b860a949edf27886376c5f21510e7ae8409a9e79354b70f5a9601bb64ae6b
OP_EQUALVERIFY                                                     | 3330343430323230366633323035623234356132623935643462643064313934...
OP_CHECKSIG                                                        |
#0003 OP_HASH160
btcdeb> step
                <> POP  stack
                <> PUSH stack eebc5d1336d0e219605a72f09173659ad7fdbe00
```



```
script                                                             |                                                             stack
-------------------------------------------------------------------+-------------------------------------------------------------------
eebc5d1336d0e219605a72f09173659ad7fdbe00                           |                            eebc5d1336d0e219605a72f09173659ad7fdbe00
OP_EQUALVERIFY                                                     | 03438b860a949edf27886376c5f21510e7ae8409a9e79354b70f5a9601bb64ae6b
OP_CHECKSIG                                                        | 333034343032323036663332303562323435613262393564346264306431393...
#0004 eebc5d1336d0e219605a72f09173659ad7fdbe00
btcdeb> step
                <> PUSH stack eebc5d1336d0e219605a72f09173659ad7fdbe00
script                                                             |                                                             stack
-------------------------------------------------------------------+-------------------------------------------------------------------
OP_EQUALVERIFY                                                     |                            eebc5d1336d0e219605a72f09173659ad7fdbe00
OP_CHECKSIG                                                        |                            eebc5d1336d0e219605a72f09173659ad7fdbe00
                                                                   | 03438b860a949edf27886376c5f21510e7ae8409a9e79354b70f5a9601bb64ae6b
                                                                   | 333034343032323036663332303562323435613262393564346264306431393...
#0005 OP_EQUALVERIFY
btcdeb> step
                <> POP  stack
                <> POP  stack
                <> PUSH stack 01
                <> POP  stack
script                                                             |                                                             stack
-------------------------------------------------------------------+-------------------------------------------------------------------
OP_CHECKSIG                                                        | 03438b860a949edf27886376c5f21510e7ae8409a9e79354b70f5a9601bb64ae6b
                                                                   | 333034343032323036663332303562323435613262393564346264306431393...
#0006 OP_CHECKSIG
btcdeb> step
EvalChecksig() sigversion=0
Eval Checksig Pre-Tapscript
error: Signature is found in scriptCode
btcdeb> ^C
```

# 3. SegWit Transactions

## Transaction Flow Overview

SegWit transactions use the Pay-to-Witness-Public-Key-Hash (P2WPKH) format, which improves scalability by separating the witness data. The transaction flow follows:

- **Address A → Address B**
- **Address B → Address C**

**Transaction IDs:**

- - **Funding TX:** `fb97ed691a4c21257a7d9cf2159435b8ce0b2fa18f80e37cf23ee2a0d27542a8`
- - **A' to B' TX:** `15af3d608d2a3bac51188ea559790c1fe08afe5bf7e7b55620b554cd0ff8e041`
- **B to C TX:** 5d814a8d9fab5990c5ef4809d0aff0df1b48ec19f99b7ea9aa794b24613cc6d3

## Script Analysis

### 2.2.1 Locking Script (ScriptPubKey) for Address B

P2WPKH Locking Script:

```
OP_0 <20-byte PubKeyHash>
```

This script locks the output to a witness program that requires a signature and a public key to spend.

### 2.2.2 Unlocking Script (Witness) in B to C Transaction

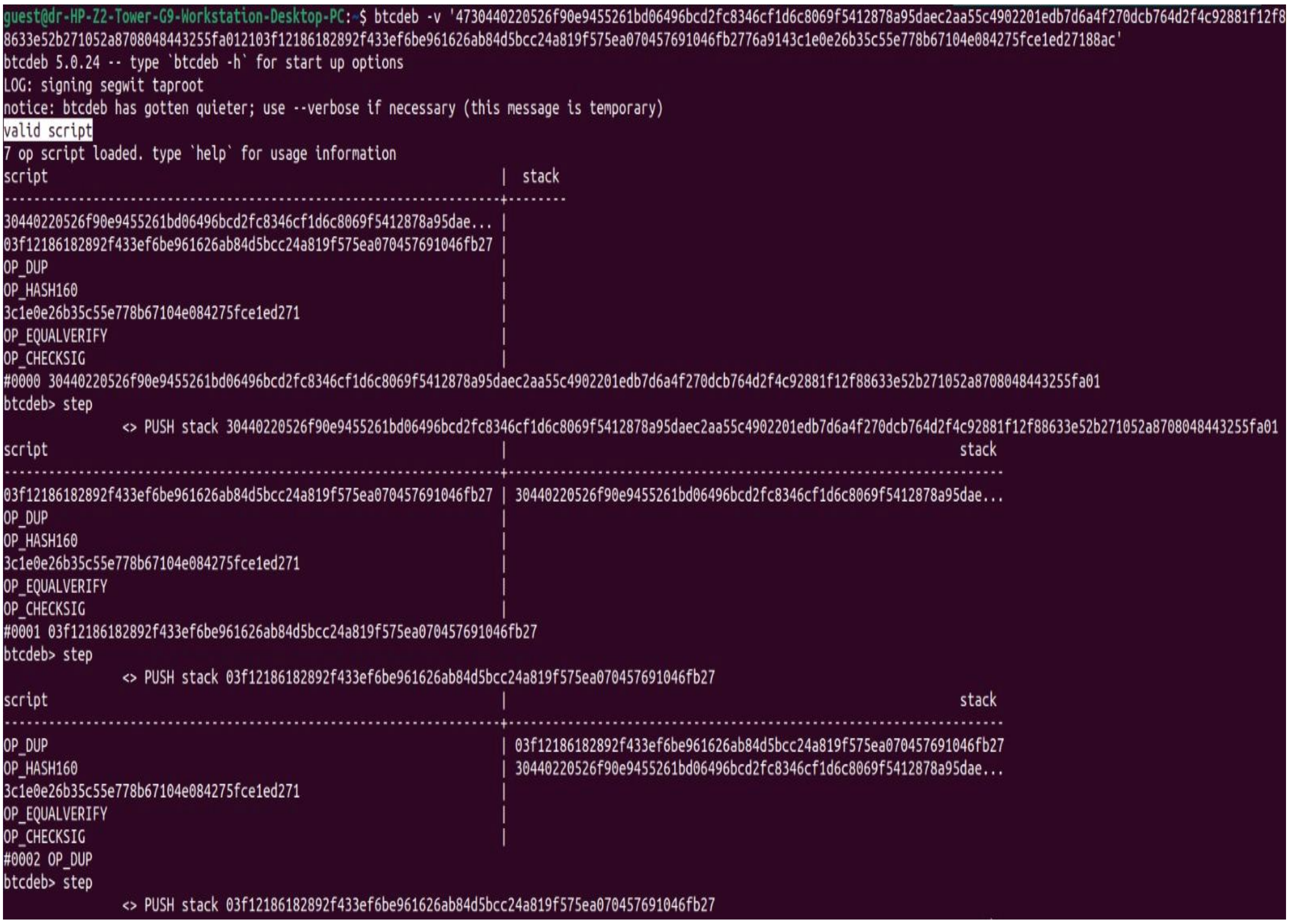
P2WPKH Witness Data:

```
<Signature>
<PublicKey>
```

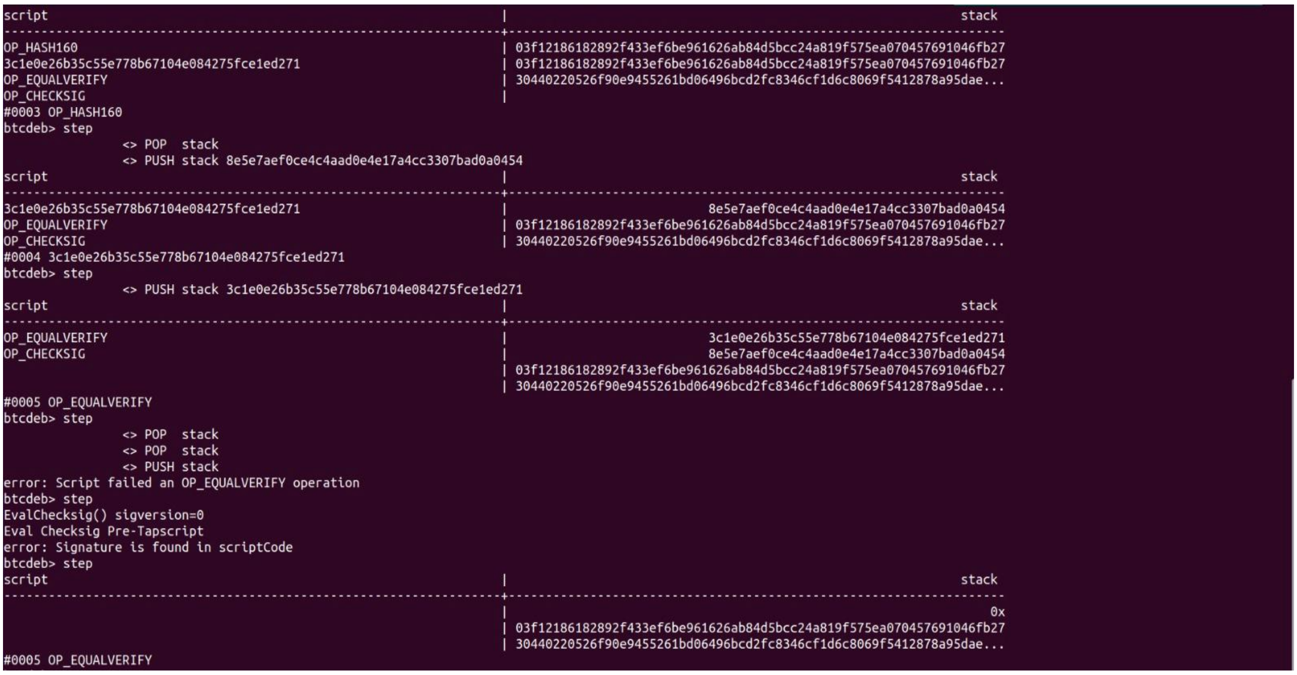
This witness data provides:

- **The digital signature**, proving ownership of the private key.
- **The public key**, which when hashed should match the hash in the locking script.

- **Bitcoin debugging**



```
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb -v '4730440220526f90e9455261bd06496bcd2fc8346cf1d6c8069f5412878a95daec2aa55c4902201edb7d6a4f270dcb764d2f4c92881f12f8
8633e52b271052a8708048443255fa012103f12186182892f433ef6be961626ab84d5bcc24a819f575ea070457691046fb2776a9143c1e0e26b35c55e778b67104e084275fce1ed27188ac'
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
-------------------------------------------------------------------+-------
30440220526f90e9455261bd06496bcd2fc8346cf1d6c8069f5412878a95dae... |
03f12186182892f433ef6be961626ab84d5bcc24a819f575ea070457691046fb27 |
OP_DUP                                                             |
OP_HASH160                                                         |
3c1e0e26b35c55e778b67104e084275fce1ed271                           |
OP_EQUALVERIFY                                                     |
OP_CHECKSIG                                                        |
#0000 30440220526f90e9455261bd06496bcd2fc8346cf1d6c8069f5412878a95daec2aa55c4902201edb7d6a4f270dcb764d2f4c92881f12f88633e52b271052a8708048443255fa01
btcdeb> step
                <> PUSH stack 30440220526f90e9455261bd06496bcd2fc8346cf1d6c8069f5412878a95daec2aa55c4902201edb7d6a4f270dcb764d2f4c92881f12f88633e52b271052a8708048443255fa01
script                                                             |                                                             stack
-------------------------------------------------------------------+-------------------------------------------------------------------
03f12186182892f433ef6be961626ab84d5bcc24a819f575ea070457691046fb27 | 30440220526f90e9455261bd06496bcd2fc8346cf1d6c8069f5412878a95dae...
OP_DUP                                                             |
OP_HASH160                                                         |
3c1e0e26b35c55e778b67104e084275fce1ed271                           |
OP_EQUALVERIFY                                                     |
OP_CHECKSIG                                                        |
#0001 03f12186182892f433ef6be961626ab84d5bcc24a819f575ea070457691046fb27
btcdeb> step
                <> PUSH stack 03f12186182892f433ef6be961626ab84d5bcc24a819f575ea070457691046fb27
script                                                             |                                                             stack
-------------------------------------------------------------------+-------------------------------------------------------------------
OP_DUP                                                             | 03f12186182892f433ef6be961626ab84d5bcc24a819f575ea070457691046fb27
OP_HASH160                                                         | 30440220526f90e9455261bd06496bcd2fc8346cf1d6c8069f5412878a95dae...
3c1e0e26b35c55e778b67104e084275fce1ed271                           |
OP_EQUALVERIFY                                                     |
OP_CHECKSIG                                                        |
#0002 OP_DUP
btcdeb> step
                <> PUSH stack 03f12186182892f433ef6be961626ab84d5bcc24a819f575ea070457691046fb27
```



```
script                                                             |                                                             stack
-------------------------------------------------------------------+-------------------------------------------------------------------
OP_HASH160                                                         | 03f12186182892f433ef6be961626ab84d5bcc24a819f575ea070457691046fb27
3c1e0e26b35c55e778b67104e084275fce1ed271                           | 03f12186182892f433ef6be961626ab84d5bcc24a819f575ea070457691046fb27
OP_EQUALVERIFY                                                     | 30440220526f90e9455261bd06496bcd2fc8346cf1d6c8069f5412878a95dae...
OP_CHECKSIG                                                        |
#0003 OP_HASH160
btcdeb> step
                <> POP  stack
                <> PUSH stack 8e5e7aef0ce4c4aad0e4e17a4cc3307bad0a0454
script                                                             |                                                             stack
-------------------------------------------------------------------+-------------------------------------------------------------------
3c1e0e26b35c55e778b67104e084275fce1ed271                           |                           8e5e7aef0ce4c4aad0e4e17a4cc3307bad0a0454
OP_EQUALVERIFY                                                     | 03f12186182892f433ef6be961626ab84d5bcc24a819f575ea070457691046fb27
OP_CHECKSIG                                                        | 30440220526f90e9455261bd06496bcd2fc8346cf1d6c8069f5412878a95dae...
#0004 3c1e0e26b35c55e778b67104e084275fce1ed271
btcdeb> step
                <> PUSH stack 3c1e0e26b35c55e778b67104e084275fce1ed271
script                                                             |                                                             stack
-------------------------------------------------------------------+-------------------------------------------------------------------
OP_EQUALVERIFY                                                     |                           3c1e0e26b35c55e778b67104e084275fce1ed271
OP_CHECKSIG                                                        |                           8e5e7aef0ce4c4aad0e4e17a4cc3307bad0a0454
                                                                   | 03f12186182892f433ef6be961626ab84d5bcc24a819f575ea070457691046fb27
                                                                   | 30440220526f90e9455261bd06496bcd2fc8346cf1d6c8069f5412878a95dae...
#0005 OP_EQUALVERIFY
btcdeb> step
                <> POP  stack
                <> POP  stack
                <> PUSH stack
error: Script failed an OP_EQUALVERIFY operation
btcdeb> step
EvalChecksig() sigversion=0
Eval Checksig Pre-Tapscript
error: Signature is found in scriptCode
btcdeb> step
script                                                             |                                                             stack
-------------------------------------------------------------------+-------------------------------------------------------------------
                                                                   |                                                                 0x
                                                                   | 03f12186182892f433ef6be961626ab84d5bcc24a819f575ea070457691046fb27
                                                                   | 30440220526f90e9455261bd06496bcd2fc8346cf1d6c8069f5412878a95dae...
#0005 OP_EQUALVERIFY
```

## 4. Comparative Analysis

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

| 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 |

## Conclusion

This report analyzed and compared Legacy and SegWit transactions. Key takeaways:

- SegWit reduces transaction size and fees.
- SegWit fixes transaction malleability issues.
- The separation of witness data in SegWit enables future protocol upgrades

**Team Members:**

Chebolu Srikanth (230001018)

Hruday Amrit (230001051)

Jothirmai (230003032)