Legacy (P2PKH) Transaction Analysis

1. Introduction

This report documents the creation and execution of Bitcoin transactions using the legacy P2PKH (Pay-to-PubKey-Hash) format in a Bitcoin Regtest environment. We explore how an initial transaction from Address A to Address B is used as an input for a second transaction from B to C, detailing the scripts involved and their validation process.

2. Workflow Overview

The following steps were performed in the Bitcoin Regtest environment using Bitcoin Core RPC:

1. Generated three legacy addresses: A, B, and C.

2. Mined 101 blocks to unlock Coinbase rewards.

3. Sent BTC from mining rewards to Address A

4. Created and signed a transaction sending from A to B.

5. Mined a block to confirm the transaction.

6.Signed and broadcasted the transaction A to B.

7. Used the UTXO from A to B to create a second transaction from B to C.

8. Signed and broadcasted the transaction B to C.

9. Decoded both transactions and analyzed the scripts.

3. Transaction Details

Transaction A → B

Transaction ID: 8dccfd129901bf04551ad05b8f56d702eee8356f87108a357a0fa4ce6db954dc

Sender (A): msNsKEFgJJxMpB5wuu7REP2PfZWkpKYJ23

Recipient (B): myGWbh8Qco2ruabgtd5gwPiGhHamVUMeAt

Transaction B → C

Transaction ID: 0f154b6ec784027a70a5633e483019ac3e57e46cc50c7f5e1b3c4c5db65dd551

Sender (B): myGWbh8Qco2ruabgtd5gwPiGhHamVUMeAt

Recipient (C): mm1RcZhqpVPV6GeBEfj9jUTzirpA3vncMj

4. Decoded Scripts and Script Execution

Each Bitcoin transaction consists of two main script components:

1. Locking Script (ScriptPubKey)- Placed by the sender to define spending conditions.

2. Unlocking Script (ScriptSig) - Provided by the recipient to satisfy spending conditions.

Decoded transaction for A → B

```
Decoded Transaction:
{'txid': '8dccfd129901bf04551ad05b8f56d702eee8356f87108a357a0fa4ce6db954dc', 'hash': '8dccfd129901bf04551ad05b8f56d702eee8356f87108a357a0fa4ce6db954
dc', 'version': 2, 'size': 259, 'vsize': 259, 'weight': 1036, 'locktime': 0, 'vin': [{'txid': 'eec19ba257c5a07348535d52923d1a4f6f9b7a1ff520d9572b6eb
8c352ad402e', 'vout': 0, 'scriptSig': {'asm': '30440220480f49c455af8a3a6433299f9d3aa4a6a71d19028a10be731e8989ef4285ee1c02207cd366da0e0fa45c7f4f1c630
b91df28f4e4d4e91e742c89feb36eabc4fe1118[ALL] 03f1d4c796b2c53cf348715f1a0aca3959592477f5a85c0e69ed3cbbeace7dc714', 'hex': '4730440220480f49c455af8a3a
6433299f9d3aa4a6a71d19028a10be731e8989ef4285ee1c02207cd366da0e0fa45c7f4f1c630b91df28f4e4d4e91e742c89feb36eabc4fe1118012103f1d4c796b2c53cf348715f1a0a
ca3959592477f5a85c0e69ed3cbbeace7dc714'}, 'sequence': 4294967293}], 'vout': [{'value': Decimal('5.00000000'), 'n': 0, 'scriptPubKey': {'asm': 'OP_DU
P OP_HASH160 c2b6fda4f1daa676f4416529a08b44725601254b OP_EQUALVERIFY OP_CHECKSIG', 'desc': 'addr(myGWbh8Qco2ruabgtd5gwPiGhHamVUMeAt)#fsaa5mw6', 'hex
': '76a914c2b6fda4f1daa676f4416529a08b44725601254b88ac', 'address': 'myGWbh8Qco2ruabgtd5gwPiGhHamVUMeAt', 'type': 'pubkeyhash'}}, {'value': Decimal(
'4.99990000'), 'n': 1, 'scriptPubKey': {'asm': 'OP_DUP OP_HASH160 821a065bafb5552b7c8f02c2ceee0761990cf899 OP_EQUALVERIFY OP_CHECKSIG', 'desc': 'add
r(msNsKEFgJJxMpB5wuu7REP2PfZWkpKYJ23)#8pgf9utt', 'hex': '76a914821a065bafb5552b7c8f02c2ceee0761990cf89988ac', 'address': 'msNsKEFgJJxMpB5wuu7REP2PfZ
WkpKYJ23', 'type': 'pubkeyhash'}}, {'value': Decimal('0.00007410'), 'n': 2, 'scriptPubKey': {'asm': 'OP_DUP OP_HASH160 65a33d9cf41023bc31d9cc598dbde
5db4cf9c790 OP_EQUALVERIFY OP_CHECKSIG', 'desc': 'addr(mpnN6bAjAMjktu7miEp5tdD8wSpx7Haabj)#90vkrvj3', 'hex': '76a91465a33d9cf41023bc31d9cc598dbde5db
4cf9c79088ac', 'address': 'mpnN6bAjAMjktu7miEp5tdD8wSpx7Haabj', 'type': 'pubkeyhash'}}]}
```


ScriptPubKey: 76a914c2b6fda4f1daa676f4416529a08b44725601254b88ac

ScriptSig:
4730440220480f49c455af8a3a6433299f9d3aa4a6a71d19028a10be731e8989ef4285ee1c02207cd366da0e0fa45c7f4f1c630b91df28f4e4d4e91e742c89feb36eabc4fe1118012103f1d4c796b2c53cf348715f1a0aca3959592477f5a85c0e69ed3cbbeace7dc714

Decoded transaction for B → C

```
Decoded Transaction: {"txid":"0f154b6ec784027a70a5633e483019ac3e57e46cc50c7f5e1b3c4c5db65dd551","hash":"0f154b6ec784027a70a5633e483019ac3e57e46cc50
c7f5e1b3c4c5db65dd551","version":2,"size":191,"vsize":191,"weight":764,"locktime":0,"vin":[{"txid":"8dccfd129901bf04551ad05b8f56d702eee8356f87108a35
7a0fa4ce6db954dc","vout":0,"scriptSig":{"asm":"304402207f15d5a5067686885f4e6777de6f87e611158b52ed42ba8d5a7d40daae239d3a02200dda6cf705127452cad3eb0b3
1c3fc9e226ba44207cfeece4dc940a1d9c3bb1c[ALL] 03f208640cbe2c6d6aa486d9e53e4712f382b3bbc7b5f9beea3a50b8028a84b138","hex":"47304402207f15d5a5067686885f
4e6777de6f87e611158b52ed42ba8d5a7d40daae239d3a02200dda6cf705127452cad3eb0b31c3fc9e226ba44207cfeece4dc940a1d9c3bb1c012103f208640cbe2c6d6aa486d9e53e47
12f382b3bbc7b5f9beea3a50b8028a84b138"},"sequence":4294967293}],"vout":[{"value":4.9999,"n":0,"scriptPubKey":{"asm":"OP_DUP OP_HASH160 cf4c14fb232cd9
26e2cd2fb8239b61ca6ffea9b9 OP_EQUALVERIFY OP_CHECKSIG","desc":"addr(mzR3K2h4rXzAuRhzJE8fhyLVQaqRG3m9nQ)#tgtanw0j","hex":"76a914cf4c14fb232cd926e2cd2
fb8239b61ca6ffea9b988ac","address":"mzR3K2h4rXzAuRhzJE8fhyLVQaqRG3m9nQ","type":"pubkeyhash"}}]}
```


ScriptPubKey: 76a914cf4c14fb232cd926e2cd2fb8239b61ca6ffea9b988ac

ScriptSig:
47304402207f15d5a5067686885f4e6777de6f87e611158b52ed42ba8d5a7d40daae239d3a02200dda6cf705127452cad3eb0b31c3fc9e226ba44207cfeece4dc940a1d9c3bb1c012103f208640cbe2c6d6aa486d9e53e4712f382b3bbc7b5f9beea3a50b8028a84b138

5. Script Execution & Debugging

To verify the validity of transactions, we executed the script in Bitcoin Debugger:

1. The unlocking script (ScriptSig) is placed on the stack.

2. The locking script (ScriptPubKey) is executed, checking if conditions are met.

3. The script returns true if the signature matches the expected public key hash.

```
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb '[4730440220480f49c455af8a3a6433299f9d3aa4a6a71d19028a10be731e8989ef4285ee1c02207cd366da0e0
fa45c7f4f1c630b91df28f4e4d4e91e742c89feb36eabc4fe1118012103f1d4c796b2c53cf348715f1a0aca3959592477f5a85c0e69ed3cbbeace7dc714] [76a914c2b6fda4f1daa676
f4416529a08b44725601254b88ac]'
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)
2 op script loaded. type `help` for usage information
script                                                          |  stack
----------------------------------------------------------------+--------
4730440220480f49c455af8a3a6433299f9d3aa4a6a71d19028a10be731e898... |
1976a914c2b6fda4f1daa676f4416529a08b44725601254b88ac              |
#0000 4730440220480f49c455af8a3a6433299f9d3aa4a6a71d19028a10be731e8989ef4285ee1c02207cd366da0e0fa45c7f4f1c630b91df28f4e4d4e91e742c89feb36eabc4fe1118
012103f1d4c796b2c53cf348715f1a0aca3959592477f5a85c0e69ed3cbbeace7dc714
btcdeb> step
             <> PUSH stack 4730440220480f49c455af8a3a6433299f9d3aa4a6a71d19028a10be731e8989ef4285ee1c02207cd366da0e0fa45c7f4f1c630b91df28f4e4d4e9
1e742c89feb36eabc4fe1118012103f1d4c796b2c53cf348715f1a0aca3959592477f5a85c0e69ed3cbbeace7dc714
script                                                          |                                                                  stack
----------------------------------------------------------------+------------------------------------------------------------------------
1976a914c2b6fda4f1daa676f4416529a08b44725601254b88ac              | 4730440220480f49c455af8a3a6433299f9d3aa4a6a71d19028a10be731e898...
#0001 1976a914c2b6fda4f1daa676f4416529a08b44725601254b88ac
btcdeb> step
             <> PUSH stack 1976a914c2b6fda4f1daa676f4416529a08b44725601254b88ac
script                                                          |                                                                  stack
----------------------------------------------------------------+------------------------------------------------------------------------
                                                                |              1976a914c2b6fda4f1daa676f4416529a08b44725601254b88ac
                                                                | 4730440220480f49c455af8a3a6433299f9d3aa4a6a71d19028a10be731e898...
btcdeb> step
script                                                          |                                                                  stack
----------------------------------------------------------------+------------------------------------------------------------------------
                                                                |              1976a914c2b6fda4f1daa676f4416529a08b44725601254b88ac
                                                                | 4730440220480f49c455af8a3a6433299f9d3aa4a6a71d19028a10be731e898...
btcdeb> step
at end of script
btcdeb>
at end of script
btcdeb>
at end of script
```

Debugging for transaction A to B.

```
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb '[47304402207f15d5a5067686885f4e6777de6f87e611158b52ed42ba8d5a7d40daae239d3a02200dda6cf7051
27452cad3eb0b31c3fc9e226ba44207cfeece4dc940a1d9c3bb1c012103f208640cbe2c6d6aa486d9e53e4712f382b3bbc7b5f9beea3a50b8028a84b138] [ 76a914cf4c14fb232cd92
6e2cd2fb8239b61ca6ffea9b988ac]'
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)
2 op script loaded. type `help` for usage information
script                                                          |  stack
----------------------------------------------------------------+--------
47304402207f15d5a5067686885f4e6777de6f87e611158b52ed42ba8d5a7d4... |
1976a914cf4c14fb232cd926e2cd2fb8239b61ca6ffea9b988ac              |
#0000 47304402207f15d5a5067686885f4e6777de6f87e611158b52ed42ba8d5a7d40daae239d3a02200dda6cf705127452cad3eb0b31c3fc9e226ba44207cfeece4dc940a1d9c3bb1c
012103f208640cbe2c6d6aa486d9e53e4712f382b3bbc7b5f9beea3a50b8028a84b138
btcdeb> step
             <> PUSH stack 47304402207f15d5a5067686885f4e6777de6f87e611158b52ed42ba8d5a7d40daae239d3a02200dda6cf705127452cad3eb0b31c3fc9e226ba442
07cfeece4dc940a1d9c3bb1c012103f208640cbe2c6d6aa486d9e53e4712f382b3bbc7b5f9beea3a50b8028a84b138
script                                                          |                                                                  stack
----------------------------------------------------------------+------------------------------------------------------------------------
1976a914cf4c14fb232cd926e2cd2fb8239b61ca6ffea9b988ac              | 47304402207f15d5a5067686885f4e6777de6f87e611158b52ed42ba8d5a7d4...
#0001 1976a914cf4c14fb232cd926e2cd2fb8239b61ca6ffea9b988ac
btcdeb> step
             <> PUSH stack 1976a914cf4c14fb232cd926e2cd2fb8239b61ca6ffea9b988ac
script                                                          |                                                                  stack
----------------------------------------------------------------+------------------------------------------------------------------------
                                                                |              1976a914cf4c14fb232cd926e2cd2fb8239b61ca6ffea9b988ac
                                                                | 47304402207f15d5a5067686885f4e6777de6f87e611158b52ed42ba8d5a7d4...
btcdeb> step
script                                                          |                                                                  stack
----------------------------------------------------------------+------------------------------------------------------------------------
                                                                |              1976a914cf4c14fb232cd926e2cd2fb8239b61ca6ffea9b988ac
                                                                | 47304402207f15d5a5067686885f4e6777de6f87e611158b52ed42ba8d5a7d4...
btcdeb> step
at end of script
```

Debugging of transaction B to C.

6. Python Code & Execution Output

The following Python script was used to automate the transaction creation, signing, and broadcasting process:

```
from bitcoinrpc.authproxy import AuthServiceProxy, JSONRPCException
 import requests
 import json
 from decimal import Decimal

# Bitcoin Core RPC Configuration
 RPC_USER = "Cryptocrew"
 RPC_PASSWORD = "abc123"
 RPC_PORT = 18443
 RPC_URL = f"http://{RPC_USER}:{RPC_PASSWORD}@127.0.0.1:{RPC_PORT}"
```

SegWit Transaction Report

1. Workflow Overview

This report describes the step-by-step process of creating and analyzing SegWit transactions in Bitcoin's regtest mode. It includes transaction IDs, decoded scripts, and validation through the Bitcoin Debugger.

The workflow follows these steps:

1. Create a wallet and generate P2SH-SegWit addresses for A, B, and C.
2. Fund A with 10 BTC by mining blocks and sending BTC.
3. Create and broadcast a transaction from A to B.
4. Mine a block to confirm the transaction.
5. Use the output of the A to B transaction as an input for a new transaction from B to C.
6. Decode and analyze both transactions.
7. Extract locking (scriptPubKey) and unlocking (scriptSig) scripts.
8. Validate the scripts using the Bitcoin Debugger.

2. Transaction Details

Transaction from A to B

TXID: 020ba4ba581af2bfa4965e83793dae99b1a8863d70e6e357fa8a840af314ea7c

Sender (A): 2Mw9zoaHxFiEjcsQi4qYtK5fjQaxztA1RLo

Recipient (B): 2N7ZZDMn1grNNbMJ3pypyUQptGjtaYtCjDy

Transaction from B to C

TXID: b37fc7621e791fe13983d7fb4af0affd3f21cf6fa2e19da397b23f2a122ca7d6

Sender (B): 2N7ZZDMn1grNNbMJ3pypyUQptGjtaYtCjDy

Recipient (C): 2NATdcftzyrAqJ51UNKRWb9EEJAHKrNecnb

3. Decoded Transactions

Decoded transaction A to B:


```
Decoded A to B Transaction:
{'txid': '020ba4ba581af2bfa4965e83793dae99b1a8863d70e6e357fa8a840af314ea7c', 'hash': '3e28f2736b87dc38f5ae0b934c6d1c574d2808460cf91f522d1dde7fffef492
15', 'version': 2, 'size': 247, 'vsize': 166, 'weight': 661, 'locktime': 0, 'vin': [{'txid': '1207a23156a683f0ef3e6d1443fb51cecda10c901dd79a3f7d860a
cb91b12529', 'vout': 0, 'scriptSig': {'asm': '0014accda5262d66aea63d0965ffd23ac3088ad70178', 'hex': '160014accda5262d66aea63d0965ffd23ac3088ad70178'
}, 'txinwitness': ['304402201a11fb8c73491006d5d7ab0b582091896b82bcc0f98376554l5f0e1ce4a2d9e7022024368e47fa2c3f686492a6a815d8f02ed7fb0360deea8cbd43f2
2fcc078b198001', '03a83cf11b03ae369c0faae56d9d5517e10a4aa56fbd24a33156c33c0988d6bdb8'], 'sequence': 4294967293}], 'vout': [{'value': Decimal('4.8000
0000'), 'n': 0, 'scriptPubKey': {'asm': 'OP_HASH160 9d094bff8691ca4d2c8877ef5bdd37187f2b8358 OP_EQUAL', 'desc': 'addr(2N7ZZDMn1grNNbMJ3pypyUQptGjtaY
tCjDy)#00kh3hs5', 'hex': 'a9149d094bff8691ca4d2c8877ef5bdd37187f2b835887', 'address': '2N7ZZDMn1grNNbMJ3pypyUQptGjtaYtCjDy', 'type': 'scripthash'}},
 {'value': Decimal('5.19990000'), 'n': 1, 'scriptPubKey': {'asm': 'OP_HASH160 2ae36ad6fa3a9654a77575f86bf3b00f97ae9219 OP_EQUAL', 'desc': 'addr(2Mw9
zoaHxFiEjcsQi4qYtK5fjQaxztA1RLo)#p0rcjmx9', 'hex': 'a9142ae36ad6fa3a9654a77575f86bf3b00f97ae921987', 'address': '2Mw9zoaHxFiEjcsQi4qYtK5fjQaxztA1RLo
', 'type': 'scripthash'}}]}
```


Decoded transaction B to C:


```
Decoded B to C Transaction:
{'txid': 'b37fc7621e791fe13983d7fb4af0affd3f21cf6fa2e19da397b23f2a122ca7d6', 'hash': 'c2c8ff4422018e5d1dfff8a341fd160890cdb767834682005581e5f8dd6b89
13', 'version': 2, 'size': 247, 'vsize': 166, 'weight': 661, 'locktime': 0, 'vin': [{'txid': '020ba4ba581af2bfa4965e83793dae99b1a8863d70e6e357fa8a84
0af314ea7c', 'vout': 0, 'scriptSig': {'asm': '0014360ec6b1de87da33fc599c3fab57a9538a7ee0f5', 'hex': '160014360ec6b1de87da33fc599c3fab57a9538a7ee0f5'
}, 'txinwitness': ['3044022073611587d62ddbaaadccdbec9846b2b767545896487O1c0213e7941b1f6c2951022005713a81b02aeff5c65f20df93cc89ff06091fa180fdd8cff0fb
f9a95e8c35eb01', '02edf93a2a25659e1e6d2e5dace52c8d58aab2794e72c280ea1456923fbe2ca8ec'], 'sequence': 4294967293}], 'vout': [{'value': Decimal('4.7000
0000'), 'n': 0, 'scriptPubKey': {'asm': 'OP_HASH160 bcd2da5e4cf26e3adf7206fb55fda5aef5a5a6d5 OP_EQUAL', 'desc': 'addr(2NATdcftzyrAqJ51UNKRWb9EEJAHKr
Necnb)#49qafgnk', 'hex': 'a914bcd2da5e4cf26e3adf7206fb55fda5aef5a5a6d587', 'address': '2NATdcftzyrAqJ51UNKRWb9EEJAHKrNecnb', 'type': 'scripthash'}},
 {'value': Decimal('0.09990000'), 'n': 1, 'scriptPubKey': {'asm': 'OP_HASH160 9d094bff8691ca4d2c8877ef5bdd37187f2b8358 OP_EQUAL', 'desc': 'addr(2N7Z
ZDMn1grNNbMJ3pypyUQptGjtaYtCjDy)#00kh3hs5', 'hex': 'a9149d094bff8691ca4d2c8877ef5bdd37187f2b835887', 'address': '2N7ZZDMn1grNNbMJ3pypyUQptGjtaYtCjDy
', 'type': 'scripthash'}}]}
```

4. Challenge and Response Script Analysis

In Bitcoin transactions, the challenge script (scriptPubKey) is the locking script that defines conditions for spending the output, while the response script (scriptSig or witness) provides the unlocking data.

For A to B transaction:

Locking Script (scriptPubKey): a9149d094bff8691ca4d2c8877ef5bdd37187f2b835887

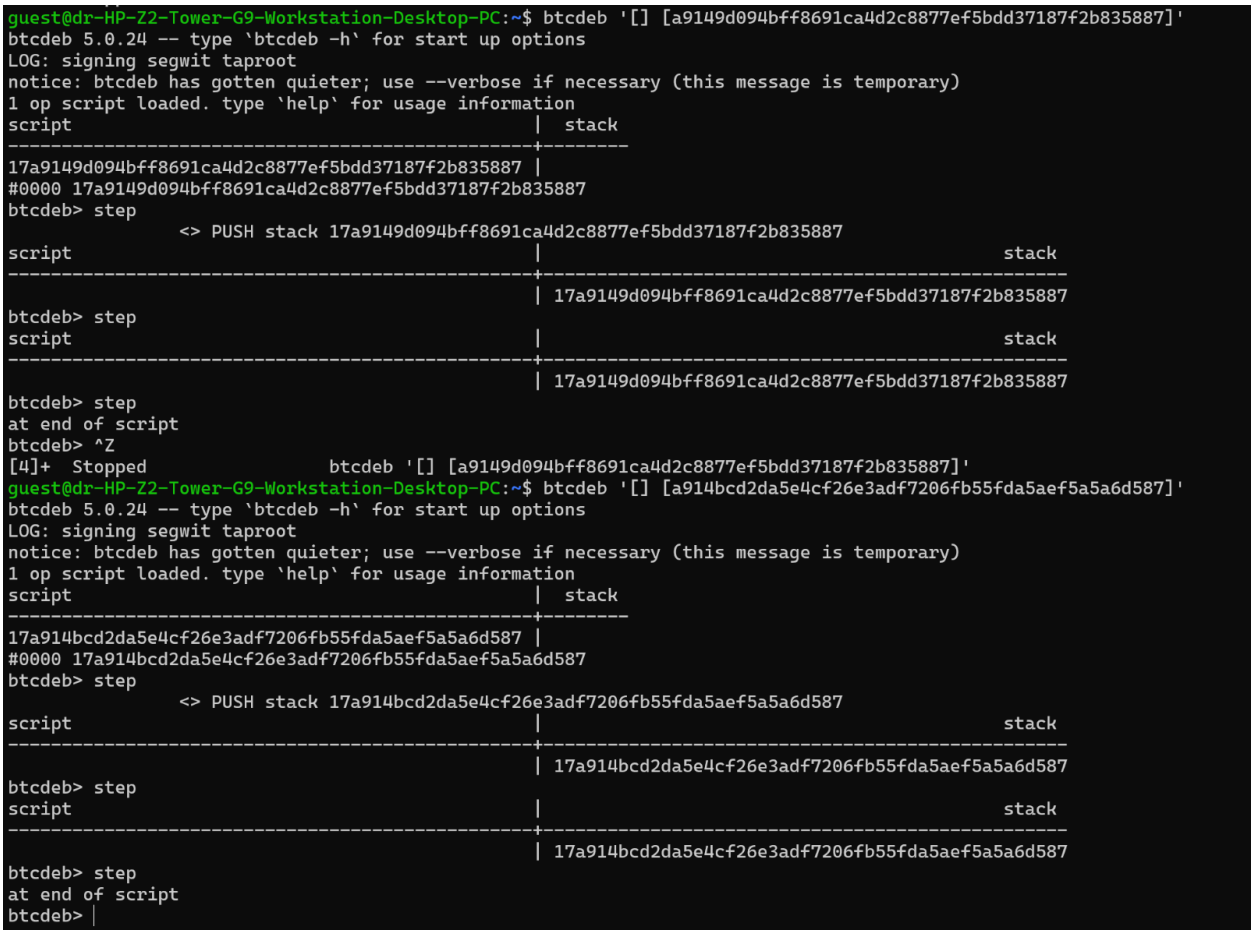
Unlocking Script (scriptSig): 160014accda5262d66aea63d0965ffd23ac3088ad70178

For B to C transaction:

Locking Script (scriptPubKey): a914bcd2da5e4cf26e3adf7206fb55fda5aef5a5a6d587

Unlocking Script (scriptSig): 160014360ec6b1de87da33fc599c3fab57a9538a7ee0f5

5.Bitcoin Debugger Validation



Debugging of transaction from A to B and B to C.

Comparison of P2PKH (Legacy) and P2SH-P2WPKH (SegWit) Transactions

1. Transaction Size Comparison

In this section, we compare the transaction size, weight units (WU), and virtual size (vBytes) between legacy and SegWit transactions.

- Approximate Size (bytes):

  P2PKH (Legacy)- ~250 bytes

  P2SH-P2WPKH (SegWit)- ~140 bytes

- Weight Units (WU):

  P2PKH (Legacy)- 4x vBytes

  P2SH-P2WPKH (SegWit)- ~360 WU

- Virtual Size (vBytes):

  P2PKH (Legacy)- ~250 vBytes

  P2SH-P2WPKH (SegWit)- ~90 vBytes

- SegWit transactions are significantly smaller than legacy transactions.
- The virtual size (vBytes) of SegWit transactions is lower than the byte size of P2PKH, meaning they require less block space.
- SegWit uses Weight Units (WU), where 1 vByte = 4 WU, allowing better block efficiency.

2. Script Structure Comparison

P2PKH (Legacy) Transaction Script

Locking Script (scriptPubKey)

OP_DUP OP_HASH160 <Receiver's Public Key Hash> OP_EQUALVERIFY OP_CHECKSIG

Unlocking Script (scriptSig)

<Sender's Signature> <Sender's Public Key>

For transaction A to B:

ScriptPubKey: 76a914c2b6fda4f1daa676f4416529a08b44725601254b88ac

ScriptSig:
4730440220480f49c455af8a3a6433299f9d3aa4a6a71d19028a10be731e8989ef4285ee1c02207c
d366da0e0fa45c7f4f1c630b91df28f4e4d4e91e742c89feb36eabc4fe1118012103f1d4c796b2c53cf
348715f1a0aca3959592477f5a85c0e69ed3cbbeace7dc714

P2SH-P2WPKH (SegWit) Transaction Script

Locking Script (scriptPubKey)

OP_HASH160 <Redeem Script Hash> OP_EQUAL

Unlocking Script (scriptSig)

<Sender's Signature> <Sender's Public Key>

For transaction A to B:

scriptPubKey: a9149d094bff8691ca4d2c8877ef5bdd37187f2b835887

scriptSig: 160014accda5262d66aea63d0965ffd23ac3088ad70178

3. Why SegWit Transactions Are Smaller & Their Benefits

Why Are SegWit Transactions Smaller?

1. Signatures Are in Witness Data
 - Instead of storing the public key & signature inside the main transaction (scriptSig), they are moved to the witness structure.
 - This reduces the effective size of the transaction since the witness is discounted when computing block size.

2. Weight-Based Block Calculation
 - SegWit introduced a weight-based system:
  - Legacy transactions take 4 WU per byte.

- Witness data only takes 1 WU per byte.
- This makes SegWit transactions more efficient in terms of block space.

Conclusion

- SegWit transactions (P2SH-P2WPKH) are smaller than legacy transactions (P2PKH) because they move signatures to witness data, reducing the transaction's vByte size.
- Smaller transactions = lower fees and better scalability.
- SegWit eliminates transaction malleability, making Bitcoin more secure and enabling advanced features like the Lightning Network.
- This comparison highlights why SegWit adoption is crucial for Bitcoin's future efficiency and growth.