Team Members: Aditya Naskar (230002005)

Aniket Goyal (230002009)

Armaanjot Singh (230041005)

Bitcoin Scripting - Legacy (P2PKH) and SegWit (P2SH-P2WPKH) Transactions

Part 1: Legacy Address Transactions (P2PKH)

Workflow Overview

1. Transaction from Address A to Address B:
    - A legacy address (A) was funded using the `sendtoaddress` command.
    - A raw transaction was created to transfer coins from Address A to Address B.
    - The transaction was signed using the private key of Address A.
    - The signed transaction was broadcast to the Bitcoin network.
2. Key Details:

    - Transaction ID (`txid`) for this transaction: [6b5e3cbc0bdcb110131dc2ce0ad709f647e21594ce38f8af240de37b84863e64].
    - Address A:[mnSyucWVcS2BnwQyvgG3TgFbGxnBPK33QA]
    - Address B: [mzAdAGTZLPsicxW8pjHu9YKWuCMV8GxTW6].

3. Transaction from Address B to Address C:
    - The `listunspent` command was used to identify unspent transaction outputs (UTXOs) for Address B.
    - A raw transaction was created to transfer coins from Address B to Address C using the UTXO from the previous transaction.
    - The transaction was signed using the private key of Address B.
    - The signed transaction was broadcast, and its details were decoded.
4. Key Details:
    - Transaction ID (`txid`) for this transaction: [e58f4369898c4d8594327329aa4e85bc764f2f99676a2ddb5f3b299b830f4cb1].
    - Address C:[mn4D1VanKQwYAHZttBB3tTKt2JD5yQvudz]

Analysis of Scripts

- Challenge Script (ScriptPubKey):

  The locking script defines conditions that must be met to spend funds. For Address B, it included the public key hash and OP_CHECKSIG operation.

- Response Script (ScriptSig):

  The unlocking script included the signature and public key required to satisfy the locking script.

- Validation:

  Using the Bitcoin Debugger, it was confirmed that the response script matched the challenge script, validating both transactions.

Part 2: SegWit Transactions (P2SH-P2WPKH)

Workflow Overview

1. Transaction from Address A' to Address B':
   - A P2SH-SegWit address (A') was funded using the `sendtoaddress` command.
   - A raw transaction was created to send coins from Address A' to Address B'.
   - The transaction was signed using the private key of Address A' and broadcast.
2. Key Details:
   - Transaction ID (`txid`) for this transaction: [33f8b74eb5a5375406c447db3e78ea474b59e871358166edd228e01beec3576c].
   - Address A: [2N1uiBgu1ysw1BgvmNFnCK8XCW1itt6KDUq]
   - Address B: [2NGAPxG9ftfNvZvy7sK6saPdQNxcsDPq49f]

3. Transaction from Address B' to Address C':
    - UTXOs for Address B' were identified using `listunspent`.
    - A raw transaction was created to transfer coins from Address B' to Address C'.
    - The transaction was signed with the private key of Address B' and broadcast.
4. Key Details:
    - Transaction ID (`txid`) for this transaction: [677e3867a0110436409932f966eb7c6f71e904e649bd56b071ce0b9f7cadd134].
    - Address C: [2N7UNJPP8Eiz5MV6a4Jd9uh56LqKLwvWHSU]

Analysis of Scripts

- Challenge Script (ScriptPubKey):

  For SegWit transactions, the locking script is smaller due to segregated witness data being stored outside the main blockchain structure.
- Response Script (Witness Data):

  The unlocking mechanism uses witness data instead of traditional ScriptSig, reducing size and improving efficiency.
- Validation:

  The Bitcoin Debugger confirmed that witness data satisfied challenge scripts in both transactions

Part 3: Analysis and Explanation

1. Transaction Size:

   Legacy transactions (P2PKH) are larger in size compared to SegWit transactions (P2SH-P2WPKH). This is because the unlocking script (ScriptSig) in legacy transactions contains the signature and public key directly, which adds significant data to the transaction. In contrast, SegWit transactions store witness data separately from the main transaction structure, reducing the size of the transaction in terms of virtual bytes (vbytes).
2. SegWit transactions achieve this reduction by segregating the witness data, which includes the unlocking information, outside the main block structure. As a result, SegWit transactions consume fewer weight units, making them more efficient.
3. Script Structure:
   - Legacy Transactions (P2PKH):

     The challenge script (ScriptPubKey) contains a public key hash and an OP_CHECKSIG operation. The response script (ScriptSig) includes the signature and public key required to satisfy the locking conditions.
   - SegWit Transactions (P2SH-P2WPKH):

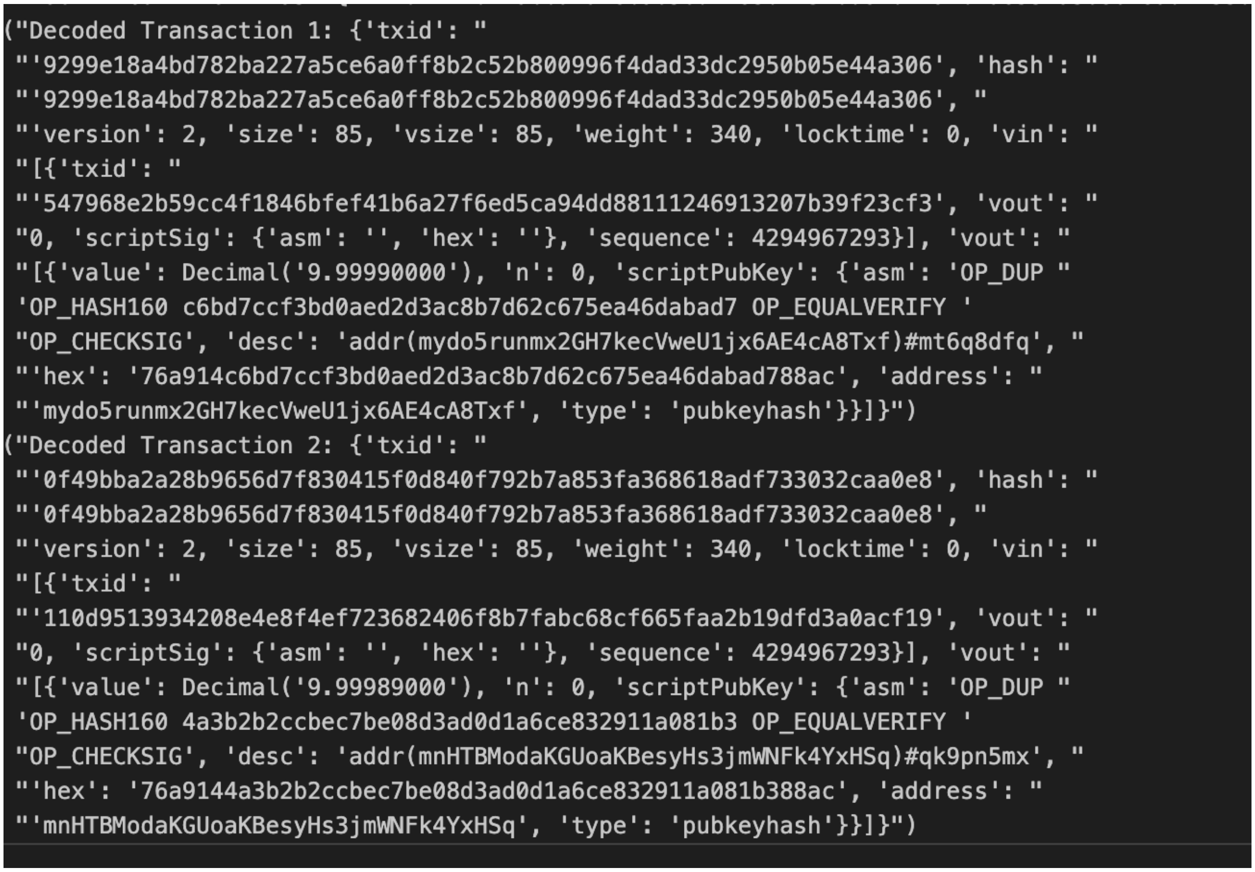
     The challenge script consists of a redeem script that points to a witness program. The witness program contains a public key hash and OP_CHECKSIG operation. The response mechanism uses witness data instead of ScriptSig, which is stored separately from the main transaction data.

4. This difference in script structure contributes to the smaller size and improved efficiency of SegWit transactions.
5. Efficiency and Benefits of SegWit Transactions:
    - Reduced Transaction Size: By storing witness data outside the main block structure, SegWit transactions reduce their size, allowing more transactions to fit into a single block.
    - Lower Fees: Smaller transaction sizes translate into lower fees for users, as fees are calculated based on transaction size in bytes.
    - Increased Network Throughput: With reduced transaction sizes, more transactions can be processed within each block, increasing overall network throughput.
    - Fix for Transaction Malleability: SegWit addresses fix transaction malleability issues by isolating signature data from the transaction hash calculation. This prevents unauthorized modifications to transaction IDs after they are broadcast.
6. Why SegWit Transactions Are Smaller:

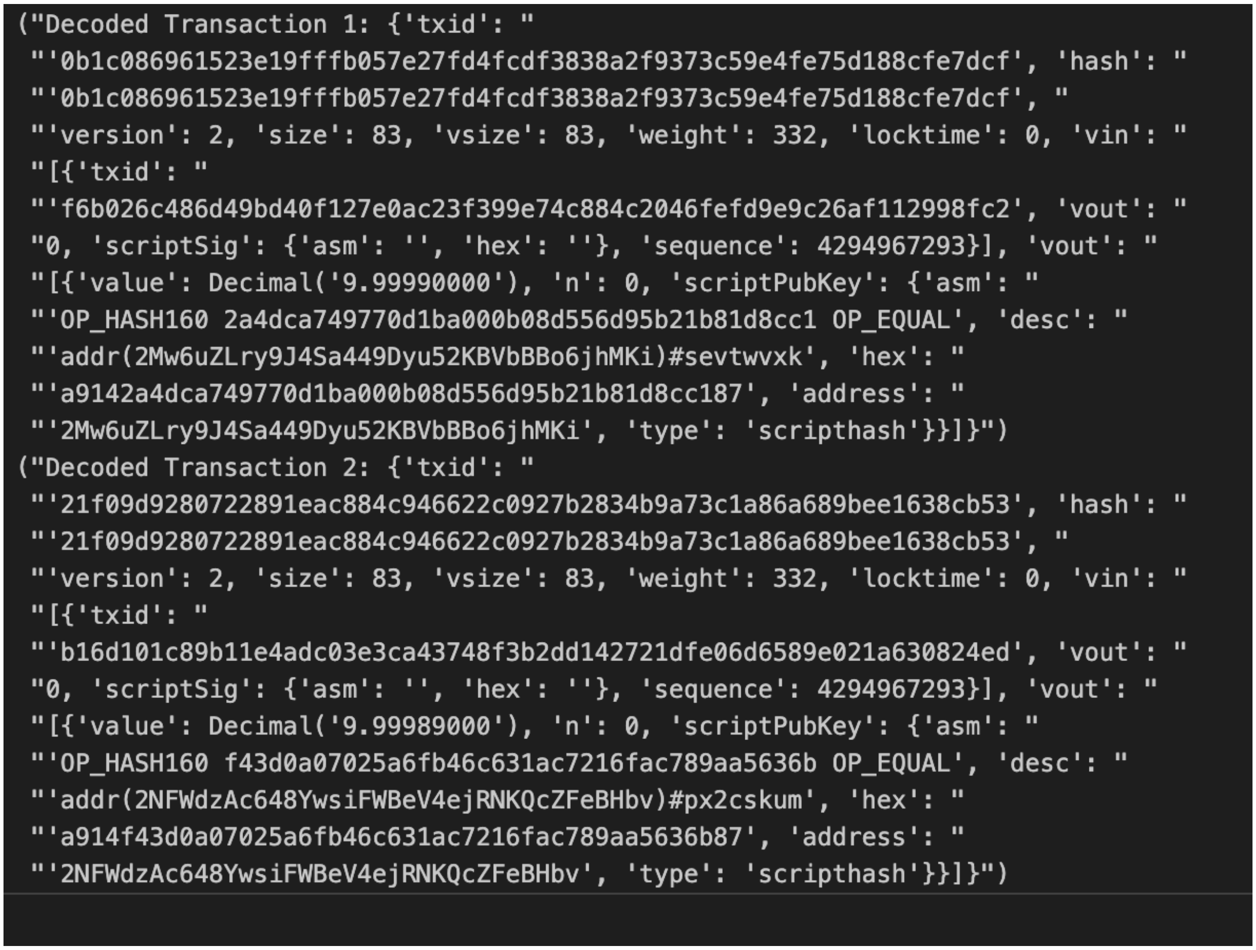
   The primary reason for the reduced size of SegWit transactions lies in how they handle unlocking scripts. Instead of including the signature and public key directly within the ScriptSig, SegWit separates this information into witness data stored outside the main block structure. This segregation reduces the amount of data that needs to be processed and included in blocks, making SegWit transactions more compact.

7. Impact on Bitcoin Network:

   The adoption of SegWit has had a profound impact on the Bitcoin network by improving scalability and efficiency. By allowing more transactions per block and reducing fees, SegWit enhances user experience while addressing long-standing issues like transaction malleability. Additionally, it paves the way for advanced features like Layer 2 solutions (e.g., Lightning Network), which rely on SegWit for optimal functionality



```
("Decoded Transaction 1: {'txid': "
 "'9299e18a4bd782ba227a5ce6a0ff8b2c52b800996f4dad33dc2950b05e44a306', 'hash': "
 "'9299e18a4bd782ba227a5ce6a0ff8b2c52b800996f4dad33dc2950b05e44a306', "
 "'version': 2, 'size': 85, 'vsize': 85, 'weight': 340, 'locktime': 0, 'vin': "
 "[{'txid': "
 "'547968e2b59cc4f1846bfef41b6a27f6ed5ca94dd88111246913207b39f23cf3', 'vout': "
 "0, 'scriptSig': {'asm': '', 'hex': ''}, 'sequence': 4294967293}], 'vout': "
 "[{'value': Decimal('9.99990000'), 'n': 0, 'scriptPubKey': {'asm': 'OP_DUP "
 'OP_HASH160 c6bd7ccf3bd0aed2d3ac8b7d62c675ea46dabad7 OP_EQUALVERIFY '
 "OP_CHECKSIG', 'desc': 'addr(mydo5runmx2GH7kecVweU1jx6AE4cA8Txf)#mt6q8dfq', "
 "'hex': '76a914c6bd7ccf3bd0aed2d3ac8b7d62c675ea46dabad788ac', 'address': "
 "'mydo5runmx2GH7kecVweU1jx6AE4cA8Txf', 'type': 'pubkeyhash'}}]}")
("Decoded Transaction 2: {'txid': "
 "'0f49bba2a28b9656d7f830415f0d840f792b7a853fa368618adf733032caa0e8', 'hash': "
 "'0f49bba2a28b9656d7f830415f0d840f792b7a853fa368618adf733032caa0e8', "
 "'version': 2, 'size': 85, 'vsize': 85, 'weight': 340, 'locktime': 0, 'vin': "
 "[{'txid': "
 "'110d9513934208e4e8f4ef723682406f8b7fabc68cf665faa2b19dfd3a0acf19', 'vout': "
 "0, 'scriptSig': {'asm': '', 'hex': ''}, 'sequence': 4294967293}], 'vout': "
 "[{'value': Decimal('9.99989000'), 'n': 0, 'scriptPubKey': {'asm': 'OP_DUP "
 'OP_HASH160 4a3b2b2ccbec7be08d3ad0d1a6ce832911a081b3 OP_EQUALVERIFY '
 "OP_CHECKSIG', 'desc': 'addr(mnHTBModaKGUoaKBesyHs3jmWNFk4YxHSq)#qk9pn5mx', "
 "'hex': '76a9144a3b2b2ccbec7be08d3ad0d1a6ce832911a081b388ac', 'address': "
 "'mnHTBModaKGUoaKBesyHs3jmWNFk4YxHSq', 'type': 'pubkeyhash'}}]}")
```



```
("Decoded Transaction 1: {'txid': "
 "'0b1c086961523e19fffb057e27fd4fcdf3838a2f9373c59e4fe75d188cfe7dcf', 'hash': "
 "'0b1c086961523e19fffb057e27fd4fcdf3838a2f9373c59e4fe75d188cfe7dcf', "
 "'version': 2, 'size': 83, 'vsize': 83, 'weight': 332, 'locktime': 0, 'vin': "
 "[{'txid': "
 "'f6b026c486d49bd40f127e0ac23f399e74c884c2046fefd9e9c26af112998fc2', 'vout': "
 "0, 'scriptSig': {'asm': '', 'hex': ''}, 'sequence': 4294967293}], 'vout': "
 "[{'value': Decimal('9.99990000'), 'n': 0, 'scriptPubKey': {'asm': "
 "'OP_HASH160 2a4dca749770d1ba000b08d556d95b21b81d8cc1 OP_EQUAL', 'desc': "
 "'addr(2Mw6uZLry9J4Sa449Dyu52KBVbBBo6jhMKi)#sevtwvxk', 'hex': "
 "'a9142a4dca749770d1ba000b08d556d95b21b81d8cc187', 'address': "
 "'2Mw6uZLry9J4Sa449Dyu52KBVbBBo6jhMKi', 'type': 'scripthash'}}]}")
("Decoded Transaction 2: {'txid': "
 "'21f09d9280722891eac884c946622c0927b2834b9a73c1a86a689bee1638cb53', 'hash': "
 "'21f09d9280722891eac884c946622c0927b2834b9a73c1a86a689bee1638cb53', "
 "'version': 2, 'size': 83, 'vsize': 83, 'weight': 332, 'locktime': 0, 'vin': "
 "[{'txid': "
 "'b16d101c89b11e4adc03e3ca43748f3b2dd142721dfe06d6589e021a630824ed', 'vout': "
 "0, 'scriptSig': {'asm': '', 'hex': ''}, 'sequence': 4294967293}], 'vout': "
 "[{'value': Decimal('9.99989000'), 'n': 0, 'scriptPubKey': {'asm': "
 "'OP_HASH160 f43d0a07025a6fb46c631ac7216fac789aa5636b OP_EQUAL', 'desc': "
 "'addr(2NFWdzAc648YwsiFWBeV4ejRNKQcZFeBHbv)#px2cskum', 'hex': "
 "'a914f43d0a07025a6fb46c631ac7216fac789aa5636b87', 'address': "
 "'2NFWdzAc648YwsiFWBeV4ejRNKQcZFeBHbv', 'type': 'scripthash'}}]}")
```