CRYPTOSPHERE

Bitcoin Transaction Report: Legacy (P2PKH) and SegWit

Legacy (P2PKH) Transactions

Transaction Workflow:

1. **Transaction A to B:**
    a. A transaction is created where A sends Bitcoin to B.
    b. This transaction generates a unique transaction ID (txid).
    c. The output of this transaction becomes an input for the next transaction.

EXECUTION TX A->B

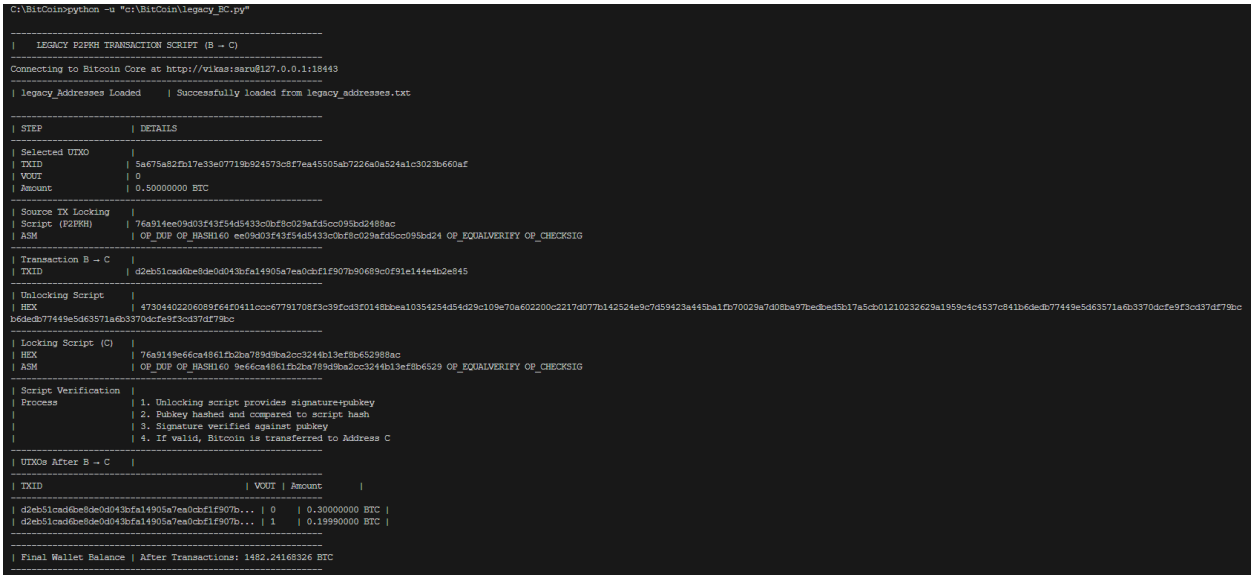
```
C:\BitCoin>python -u "c:\BitCoin\legacy_AB.py"

------------------------------------------------------------
|    LEGACY P2PKH TRANSACTION SCRIPT
------------------------------------------------------------
Connecting to Bitcoin Core at http://vikas:saru@127.0.0.1:18443
------------------------------------------------------------

------------------------------------------------------------
| STEP                 | DETAILS
------------------------------------------------------------
| Wallet Balance       | Before: 1482.24196456 BTC
------------------------------------------------------------
| legacy_Addresses Generated  |
| Address A (Sender)   | mpRMsFj2wdvvc79pPHzPXjhQamafK19RYR
| Address B (Receiver) | n3DasZW642bZkzNNzxj5FrUfAY7Bbjrq15
| Address C (Receiver) | muxWCMD5oUun7ajTFpW6AnJ6TKFaqURrcj
------------------------------------------------------------
| UTXOs Before         | [No UTXOs Found]
------------------------------------------------------------
| Transaction Funded   |
| Sent 1 BTC to A      | TXID: c6657fa5750090df265a98f55a895598d70462a26f977150ddc15d7b16bf3960
------------------------------------------------------------
| Wallet Balance       | After Funding A: 1482.24188326 BTC
------------------------------------------------------------
| Transaction A → B    |
| TXID                 | 5a675a82fb17e33e07719b924573c8f7ea45505ab7226a0a524a1c3023b660af
------------------------------------------------------------
| P2PKH Locking Script |
| HEX                  | 76a914ee09d03f43f54d5433c0bf8c029afd5cc095bd2488ac
| ASM                  | OP_DUP OP_HASH160 ee09d03f43f54d5433c0bf8c029afd5cc095bd24 OP_EQUALVERIFY OP_CHECKSIG
------------------------------------------------------------
| UTXOs After A → B    |
                         TXID: 5a675a82fb17e33e07719b924573c8f7ea45505ab7226a0a524a1c3023b660af | VOUT: 0 | Amount: 0.50000000 BTC
                         TXID: 5a675a82fb17e33e07719b924573c8f7ea45505ab7226a0a524a1c3023b660af | VOUT: 1 | Amount: 0.49990000 BTC
------------------------------------------------------------
| Final Wallet Balance | After Transactions: 1482.24178326 BTC
------------------------------------------------------------
| legacy_Addresses Saved      | Saved to legacy_addresses.txt for the next script
------------------------------------------------------------
```

2. **Transaction B to C:**
    a. B initiates a new transaction sending Bitcoin to C.
    b. The input references the txid from A to B.
    c. The unlocking script provides B's signature and public key to authorize spending.

EXECUTION TX B->C



Decoded Scripts:

Transaction A to B

- **Locking Script (scriptPubKey):** `OP_DUP OP_HASH160 <B's Public Key Hash> OP_EQUALVERIFY OP_CHECKSIG`

- **Unlocking Script (scriptSig):** `<B's Signature> <B's Public Key>`

- **Python Script Execution (legacy_AB.py):**
    - Uses the `bitcoin.core.script` module to construct and validate the transaction script.
    - Simulates the execution of the locking and unlocking scripts.

DECODE TX A->B

```
C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" gettransaction "5a675a82fb17e33e07719b924573c8f7ea45505ab7226a0a524a1c3023b660af"
{
  "amount": 0.00000000,
  "fee": -0.00010000,
  "confirmations": 5,
  "blockhash": "29aa87241a043886a46cde8a2efa19bcead5463cd364b90d2f66dc91eabf9803",
  "blockheight": 7152,
  "blockindex": 1,
  "blocktime": 1742733297,
  "txid": "5a675a82fb17e33e07719b924573c8f7ea45505ab7226a0a524a1c3023b660af",
  "wtxid": "5a675a82fb17e33e07719b924573c8f7ea45505ab7226a0a524a1c3023b660af",
  "walletconflicts": [
  ],
  "mempoolconflicts": [
  ],
  "time": 1742733297,
  "timereceived": 1742733297,
  "bip125-replaceable": "no",
  "details": [
    {
      "address": "n3DasZW642bZkzNNzxj5FrUfAY7Bbjrq15",
      "category": "send",
      "amount": -0.50000000,
      "label": "addr_b",
      "vout": 0,
      "fee": -0.00010000,
      "abandoned": false
    },
    {
      "address": "mpRMsFj2wdvvc79pPHzPXjhQamafK19RYR",
      "category": "send",
      "amount": -0.49990000,
      "label": "addr_a",
      "vout": 1,
      "fee": -0.00010000,
      "abandoned": false
    },
    {
      "address": "n3DasZW642bZkzNNzxj5FrUfAY7Bbjrq15",
      "parent_descs": [
        "pkh(tpubD6NzVbkrYhZ4YjCXirwutAHrkpLm352ND6RyBiFKuZgUF69kS4SPyyBTndgqbN34rC7oXqnVCRLrw9HtPfgLLxa1fxctuWPXuRoXyodcQSc/44h/1h/0h/0/*)#tq6gzlql"
      ],
      "category": "receive",
      "amount": 0.50000000,
      "label": "addr_b",
      "vout": 0,
      "abandoned": false
    },
    {
      "address": "mpRMsFj2wdvvc79pPHzPXjhQamafK19RYR",
      "parent_descs": [
        "pkh(tpubD6NzVbkrYhZ4YjCXirwutAHrkpLm352ND6RyBiFKuZgUF69kS4SPyyBTndgqbN34rC7oXqnVCRLrw9HtPfgLLxa1fxctuWPXuRoXyodcQSc/44h/1h/0h/0/*)#tq6gzlql"
      ],
      "category": "receive",
      "amount": 0.49990000,
      "label": "addr_a",
      "vout": 1,
      "abandoned": false
    }
  ],
  "hex": "02000000016039bf167b5dc1dd5071976fa26204d79855895af5985a26df900075a57f65c6000000006a473044022043841a72fafd98db5f4f050b3fe4fd1ddeb1cb24102135e34886119c52c8c9e3022074 0ec1b32c5826e832f9141ed307fd77ad2417169684e604bda9ce414c3baad5012102dff4b1f2f4d5c0e48042e76da5e90b659efd823d30864ec2dbcee058119c7042ffdfffff0280f0fa0200000000 1976a9146 1aa5045026c85d1646e83486c1895ee1a6faf8288ac00000000",
  "lastprocessedblock": {
    "hash": "559e0c2aceac66b31a2c5ac1f867cb6a629b5e1c67fc090de930060daa3ffd9e",
    "height": 7156
  }
}
```

```
C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" decoderawtransaction "02000000016039bf167b5dc1dd5071976fa26204d79855895af5985a26df900075a57f65c6000000006a473044022043841a72fafd98db5f4f050b3fe4fd1dd
eb1cb24102135e34886119c52c8c9e3022074 0ec1b32c5826e832f9141ed307fd77ad2417169684e604bda9ce414c3baad5012102dff4b1f2f4d5c0e48042e76da5e90b659efd823d30864ec2dbcee058119c7042ffdfffff0280f0fa0200000000 1976a9146ee09d
03f43f54d5433c0bf8c029afd5cc095bd2488ac70c9fa0200000001976a91461aa5045026c85d1646e83486c1895ee1a6faf8288ac00000000"
{
  "txid": "5a675a82fb17e33e07719b924573c8f7ea45505ab7226a0a524a1c3023b660af",
  "hash": "5a675a82fb17e33e07719b924573c8f7ea45505ab7226a0a524a1c3023b660af",
  "version": 2,
  "size": 225,
  "vsize": 225,
  "weight": 900,
  "locktime": 0,
  "vin": [
    {
      "txid": "c6657fa5750090df265a98f55a895598d70462a26f977150ddc15d7b16bf3960",
      "vout": 0,
      "scriptSig": {
        "asm": "304402204 3841a72fafd98db5f4f050b3fe4fd1ddeb1cb24102135e34886119c52c8c9e3022074 0ec1b32c5826e832f9141ed307fd77ad2417169684e604bda9ce414c3baad5[ALL] 02dff4b1f2f4d5c0e48042e76da5e90b659efd823d3086
4ec2dbcee058119c7042",
        "hex": "473044022043841a72fafd98db5f4f050b3fe4fd1ddeb1cb24102135e34886119c52c8c9e3022074 0ec1b32c5826e832f9141ed307fd77ad2417169684e604bda9ce414c3baad5012102dff4b1f2f4d5c0e48042e76da5e90b659efd823d3086
4ec2dbcee058119c7042"
      },
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 0.50000000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 ee09d03f43f54d5433c0bf8c029afd5cc095bd24 OP_EQUALVERIFY OP_CHECKSIG",
        "desc": "addr(n3DasZW642bZkzNNzxj5FrUfAY7Bbjrq15)#x05knqma",
        "hex": "76a914ee09d03f43f54d5433c0bf8c029afd5cc095bd2488ac",
        "address": "n3DasZW642bZkzNNzxj5FrUfAY7Bbjrq15",
        "type": "pubkeyhash"
      }
    },
    {
      "value": 0.49990000,
      "n": 1,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 61aa5045026c85d1646e83486c1895ee1a6faf82 OP_EQUALVERIFY OP_CHECKSIG",
        "desc": "addr(mpRMsFj2wdvvc79pPHzPXjhQamafK19RYR)#2qjtpau0",
        "hex": "76a91461aa5045026c85d1646e83486c1895ee1a6faf8288ac",
        "address": "mpRMsFj2wdvvc79pPHzPXjhQamafK19RYR",
        "type": "pubkeyhash"
      }
    }
  ]
}
```

Transaction B to C

- **Locking Script (scriptPubKey):** `OP_DUP OP_HASH160 <C's Public Key Hash> OP_EQUALVERIFY OP_CHECKSIG`

- **Unlocking Script (scriptSig):** `<C's Signature> <C's Public Key>`

- **Python Script Execution (legacy_BC.py):**
    - Follows the same structure as legacy_AB.py to validate the transaction.

DECODE TX B->C

```
C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" gettransaction "d2eb51cad6be8de8d043bfa14905a7ea8cbf1f907b90689c0f91e144e4b2e845"
{
  "amount": 0.00000000,
  "fee": -0.00010000,
  "confirmations": 4,
  "blockhash": "2a4133e3981e6762f628e2f585bcca7fec5bb8ad8929097ec86c82c46500e725",
  "blockheight": 7153,
  "blockindex": 1,
  "blocktime": 1742733373,
  "txid": "d2eb51cad6be8de8d043bfa14905a7ea8cbf1f907b90689c0f91e144e4b2e845",
  "wtxid": "d2eb51cad6be8de8d043bfa14905a7ea8cbf1f907b90689c0f91e144e4b2e845",
  "walletconflicts": [
  ],
  "mempoolconflicts": [
  ],
  "time": 1742733373,
  "timereceived": 1742733373,
  "bip125-replaceable": "no",
  "details": [
    {
      "address": "muxWCMD5oUun7ajTFpW6AnJ6TKFaqURrcj",
      "category": "send",
      "amount": -0.30000000,
      "label": "addr_c",
      "vout": 0,
      "fee": -0.00010000,
      "abandoned": false
    },
    {
      "address": "n3DasZW642bZkzNNzxj5FrUfAY7Bbjrq15",
      "category": "send",
      "amount": -0.19990000,
      "label": "addr_b",
      "vout": 1,
      "fee": -0.00010000,
      "abandoned": false
    },
    {
      "address": "muxWCMD5oUun7ajTFpW6AnJ6TKFaqURrcj",
      "parent_descs": [
        "pkh(tpubD6NzVbkrYhZ4YjCXirwutAHrkpLm352ND6RyBiFXuZgUF69kS45PyyBTndgpbN34rCToXqnVCRLrwRHtPfgLixalfectuWPXuRoXyodcQ5c/44h/1h/0h/0/*)#tq6gzlql"
      ],
      "category": "receive",
      "amount": 0.30000000,
      "label": "addr_c",
      "vout": 0,
      "abandoned": false
    },
    {
      "address": "n3DasZW642bZkzNNzxj5FrUfAY7Bbjrq15",
      "parent_descs": [
        "pkh(tpubD6NzVbkrYhZ4YjCXirwutAHrkpLm352ND6RyBiFXuZgUF69kS45PyyBTndgpbN34rCToXqnVCRLrwRHtPfgLixalfectuWPXuRoXyodcQ5c/44h/1h/0h/0/*)#tq6gzlql"
      ],
      "category": "receive",
      "amount": 0.19990000,
      "label": "addr_b",
      "vout": 1,
      "abandoned": false
    }
  ],
  "hex": "0200000001af60b623301c4a520a6a22b75a5045eaf7c87345929b71073ee317fb825a675a000000006a47304402206089f64f0411ccc67791708f3c39fcd3f0148bbea10354254d54d29c109e70a602200c2217d077b142524e9c7d59423a445ba1fb70029a7d08ba97bedbed5b17a5cb0121023262 9a1959c4c4537c841b6dedb77449e5d63571a6b3370dcfe9f3cd37df79bcfdfffff0280c3c90100000001976a9149e66ca4861fb2ba789d9ba2cc3244b13ef8b652988ac00000000",
  "lastprocessedblock": {
    "hash": "559e8c2acaac66b31a2c5ac1f867cb6a629b5e1c07fc890de938060daa3ff6fe",
    "height": 7156
  }
}
```


```
C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" decoderawtransaction "0200000001af60b623301c4a520a6a22b75a5045eaf7c87345929b71073ee317fb825a675a000000006a47304402206089f64f0411ccc67791708f3c39fcd3f0148bbea10354254d54d29c109e70a602200c2217d077b142524e9c7d59423a445ba1fb70029a7d08ba97bedbed5b17a5cb0121023262 9a1959c4c4537c841b6dedb77449e5d63571a6b3370dcfe9f3cd37df79bcfdfffff0280c3c90100000001976a9149e66ca4861fb2ba789d9ba2cc3244b13ef8b652988ac00000000"
{
  "txid": "d2eb51cad6be8de8d043bfa14905a7ea8cbf1f907b90689c0f91e144e4b2e845",
  "hash": "d2eb51cad6be8de8d043bfa14905a7ea8cbf1f907b90689c0f91e144e4b2e845",
  "version": 2,
  "size": 225,
  "vsize": 225,
  "weight": 900,
  "locktime": 0,
  "vin": [
    {
      "txid": "5a675a82fb17e33e07719b924573c8f7ea45505ab7226a0a524a1c3023b660af",
      "vout": 0,
      "scriptSig": {
        "asm": "304402206089f64f0411ccc67791708f3c39fcd3f0148bbea10354254d54d29c109e70a602200c2217d077b142524e9c7d59423a445ba1fb70029a7d08ba97bedbed5b17a5cb[ALL] 0232629a1959c4c4537c841b6dedb77449e5d63571a6b3370dcfe9f3cd37df79bc",
        "hex": "4730440220 6089f64f0411ccc67791708f3c39fcd3f0148bbea10354254d54d29c109e70a602200c2217d077b142524e9c7d59423a445ba1fb70029a7d08ba97bedbed5b17a5cb0121023262 9a1959c4c4537c841b6dedb77449e5d63571a6b3370dcfe9f3cd37df79bc"
      },
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 0.30000000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 9e66ca4861fb2ba789d9ba2cc3244b13ef8b6529 OP_EQUALVERIFY OP_CHECKSIG",
        "desc": "addr(muxWCMD5oUun7ajTFpW6AnJ6TKFaqURrcj)#hs9jra33",
        "hex": "76a9149e66ca4861fb2ba789d9ba2cc3244b13ef8b652988ac",
        "address": "muxWCMD5oUun7ajTFpW6AnJ6TKFaqURrcj",
        "type": "pubkeyhash"
      }
    },
    {
      "value": 0.19990000,
      "n": 1,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 ee09d03f43f54d5433c0bf8c029afd5cc095bd24 OP_EQUALVERIFY OP_CHECKSIG",
        "desc": "addr(n3DasZW642bZkzNNzxj5FrUfAY7Bbjrq15)#x05knqma",
        "hex": "76a914ee09d03f43f54d5433c0bf8c029afd5cc095bd2488ac",
        "address": "n3DasZW642bZkzNNzxj5FrUfAY7Bbjrq15",
        "type": "pubkeyhash"
      }
    }
  ]
}
```

Challenge and Response Script Structure:

Challenge Script = Locking Script (scriptPubKey)

Response Script = Unlocking Script (scriptSig or witness)

- The **challenge script (scriptPubKey)** ensures only the rightful owner can spend the funds.
- The **response script (scriptSig)** must provide a valid signature and public key.
- Validation occurs when the unlocking script correctly satisfies the locking script conditions.

Legacy AB Transaction:

- *Transaction ID:* 5a675a82fb17e33e07719b924573c8f7ea45505ab7226a0a524a1c3023b660af
- *Hash:* 5a675a82fb17e33e07719b924573c8f7ea45505ab7226a0a524a1c3023b660af
- *Version:* 2
- *Size:* 225 bytes
- *Virtual Size:* 225 vbytes
- *Weight:* 900
- *Locktime:* 0

Input (vin):

- *Previous TX ID:* c6657fa5750090df265a98f55a895598d70462a26f977150ddc15d7b16bf3960
- *Output Index (vout):* 0
- *ScriptSig:*
    - *ASM:*

3044022043841a72fafd98db5f4f050b3fe4fd1ddeb1cb24102135e34886119c52c8c9e30220740ec1b32c5826e832f9141ed307fd77ad2417169684e604bda9ce414c3baad5[ALL]
02dff4b1f2f4d5c0e48042e76da5e90b659efd823d30864ec2dbcee058119c7042

    - *Hex:*

473044022043841a72fafd98db5f4f050b3fe4fd1ddeb1cb24102135e3488611

9c52c8c9e30220740ec1b32c5826e832f9141ed307fd77ad2417169684e604b
da9ce414c3baad5012102dff4b1f2f4d5c0e48042e76da5e90b659efd823d308
64ec2dbcee058119c7042

- *Sequence:* 4294967293

Outputs (vout):

1. *Output 0:*
    a. *Value:* 0.50000000 BTC
    b. *ScriptPubKey ASM:*

OP_DUP OP_HASH160 ee09d03f43f54d5433c0bf8c029afd5cc095bd24
OP_EQUALVERIFY OP_CHECKSIG

    c. *ScriptPubKey Hex:*

76a914ee09d03f43f54d5433c0bf8c029afd5cc095bd2488ac

    d. *Address:* n3DasZW642bZkzNNzxj5FrUfAY7Bbjrq15
    e. *Type:* pubkeyhash
2. *Output 1:*
    a. *Value:* 0.49990000 BTC
    b. *ScriptPubKey ASM:*

OP_DUP OP_HASH160 61aa5045026c85d1646e83486c1895ee1a6faf82
OP_EQUALVERIFY OP_CHECKSIG

    c. *ScriptPubKey Hex:*

76a91461aa5045026c85d1646e83486c1895ee1a6faf8288ac

    d. *Address:* mpRMsFj2wdvvc79pPHzPXjhQamafK19RYR
    e. *Type:* pubkeyhash

Legacy BC Transaction:

- *Transaction ID:* d2eb51cad6be8de0d043bfa14905a7ea0cbf1f907b90689c0f91e144e4b2e845
- *Hash:* d2eb51cad6be8de0d043bfa14905a7ea0cbf1f907b90689c0f91e144e4b2e845
- *Version:* 2
- *Size:* 225 bytes
- *Virtual Size:* 225 vbytes
- *Weight:* 900
- *Locktime:* 0

Input (vin):

- *Previous TX ID:* 5a675a82fb17e33e07719b924573c8f7ea45505ab7226a0a524a1c3023b660af
- *Output Index (vout):* 0
- *ScriptSig:*
    - *ASM:*

304402206089f64f0411ccc67791708f3c39fcd3f0148bbea10354254d54d29c109e70a602200c2217d077b142524e9c7d59423a445ba1fb70029a7d08ba97bedbed5b17a5cb[ALL] 0232629a1959c4c4537c841b6dedb77449e5d63571a6b3370dcfe9f3cd37df79bc

    - *Hex:*

47304402206089f64f0411ccc67791708f3c39fcd3f0148bbea10354254d54d29c109e70a602200c2217d077b142524e9c7d59423a445ba1fb70029a7d08ba97bedbed5b17a5cb01210232629a1959c4c4537c841b6dedb77449e5d63571a6b3370dcfe9f3cd37df79bc

- *Sequence:* 4294967293

Outputs (vout):

1. *Output 0:*
    a. *Value:* 0.30000000 BTC
    b. *ScriptPubKey ASM:*

OP_DUP OP_HASH160 9e66ca4861fb2ba789d9ba2cc3244b13ef8b6529 OP_EQUALVERIFY OP_CHECKSIG

    c. *ScriptPubKey Hex:*

76a9149e66ca4861fb2ba789d9ba2cc3244b13ef8b652988ac

    d. *Address:* muxWCMD5oUun7ajTFpW6AnJ6TKFaqURrcj
    e. *Type:* pubkeyhash
2. *Output 1:*
    a. *Value:* 0.19990000 BTC
    b. *ScriptPubKey ASM:*

OP_DUP OP_HASH160 ee09d03f43f54d5433c0bf8c029afd5cc095bd24 OP_EQUALVERIFY OP_CHECKSIG

    c. *ScriptPubKey Hex:*

76a914ee09d03f43f54d5433c0bf8c029afd5cc095bd2488ac

    d. *Address:* n3DasZW642bZkzNNzxj5FrUfAY7Bbjrq15
    e. *Type:* pubkeyhash

CHALLENGE AND RESPONSE SCRIPTS

```
| Transaction B → C    |
| TXID                 | d2eb51cad6be8de0d043bfa14905a7ea0cbf1f907b90689c0f91e144e4b2e845
| Unlocking Script     |
| HEX                  | 473044022060089f64f0411ccc67791708f3c39fcd3f0148bbea10354254d54d29c109e70a602200c2217d077b142524e9c7d59423a445ba1fb70029a7d08ba97bedbed5b17a5cb01210232629a1959c4c4537c841b6dedb77449e5d63571a6b3370dcfe9f3cd37df79bc
b6dedb77449e5d63571a6b3370dcfe9f3cd37df79bc
| Locking Script (C)   |
| HEX                  | 76a9149e66ca4861fb2ba789d9ba2cc3244b13ef8b652988ac
| ASM                  | OP_DUP OP_HASH160 9e66ca4861fb2ba789d9ba2cc3244b13ef8b6529 OP_EQUALVERIFY OP_CHECKSIG
```

```
C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" decodescript "473044022060089f64f0411ccc67791708f3c39fcd3f0148bbea10354254d54d29c109e70a602200c2217d077b142524e9c7d59423a445ba1fb70029a7d08ba97bedbed5
b17a5cb01210232629a1959c4c4537c841b6dedb77449e5d63571a6b3370dcfe9f3cd37df79bc"
{
  "asm": "304402206089f64f0411ccc67791708f3c39fcd3f0148bbea10354254d54d29c109e70a602200c2217d077b142524e9c7d59423a445ba1fb70029a7d08ba97bedbed5b17a5cb01 0232629a1959c4c4537c841b6dedb77449e5d63571a6b3370dcfe9f
3cd37df79bc",
  "desc": "raw(4730440220608 9f64f0411ccc67791708f3c39fcd3f0148bbea10354254d54d29c109e70a602200c2217d077b142524e9c7d59423a445ba1fb70029a7d08ba97bedbed5b17a5cb01210232629a1959c4c4537c841b6dedb77449e5d63571a6b33
70dcfe9f3cd37df79bc)#au04dt8v",
  "type": "nonstandard",
  "p2sh": "2MvFno6n6do5p6tjdUftmQSytHEeXpZpw8o",
  "segwit": {
    "asm": "0 186550dc72c9a5ccd5e4e353dff65abb5e82eab27d037849c2629f0ad1cf82a5",
    "desc": "addr(bcrt1qrpj4phrjexjue40yudfalaj6hd0g964j05phsjwzv20s45w0s2jssgn62r)#aczjk76j",
    "hex": "0020186550dc72c9a5ccd5e4e353dff65abb5e82eab27d037849c2629f0ad1cf82a5",
    "address": "bcrt1qrpj4phrjexjue40yudfalaj6hd0g964j05phsjwzv20s45w0s2jssgn62r",
    "type": "witness_v0_scripthash",
    "p2sh-segwit": "2NF7MSRiEeQHc3VM9t3HE79RUW4cXAuvq2C"
  }
}

C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" decodescript "76a914ee09d03f43f54d5433c0bf8c029afd5cc095bd2488ac"
{
  "asm": "OP_DUP OP_HASH160 ee09d03f43f54d5433c0bf8c029afd5cc095bd24 OP_EQUALVERIFY OP_CHECKSIG",
  "desc": "addr(n3DasZW642bZkzNNzxj5FrUfAY7Bbjrq15)#x05knqma",
  "address": "n3DasZW642bZkzNNzxj5FrUfAY7Bbjrq15",
  "type": "pubkeyhash",
  "p2sh": "2MvQh12UTXsHCR5YzSRFB3DVNjBRkmEYvYB",
  "segwit": {
    "asm": "0 ee09d03f43f54d5433c0bf8c029afd5cc095bd24",
    "desc": "addr(bcrt1qacyaq06r74x4gv7qh7xq9xhatnqft0fyl7vf7u)#uu5ktxt3",
    "hex": "0014ee09d03f43f54d5433c0bf8c029afd5cc095bd24",
    "address": "bcrt1qacyaq06r74x4gv7qh7xq9xhatnqft0fyl7vf7u",
    "type": "witness_v0_keyhash",
    "p2sh-segwit": "2N5jEA3nabMjYVDA2q4U1FJuWHKfAGVQvFs"
  }
}

C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" decodescript "76a91461aa5045026c85d1646e83486c1895ee1a6faf8288ac"
{
  "asm": "OP_DUP OP_HASH160 61aa5045026c85d1646e83486c1895ee1a6faf82 OP_EQUALVERIFY OP_CHECKSIG",
  "desc": "addr(mpRMsFj2wdvvc79pPHzPXjhQamafK19RYR)#2qjtpau0",
  "address": "mpRMsFj2wdvvc79pPHzPXjhQamafK19RYR",
  "type": "pubkeyhash",
  "p2sh": "2NB2fUYRKm9hBtMDZqjSEqnvKfdiBJTX82c",
  "segwit": {
    "asm": "0 61aa5045026c85d1646e83486c1895ee1a6faf82",
    "desc": "addr(bcrt1qvx49q3gzdjzazerwsdyxcxy4acdxltuzp6glyz)#zh2f0dh5",
    "hex": "001461aa5045026c85d1646e83486c1895ee1a6faf82",
    "address": "bcrt1qvx49q3gzdjzazerwsdyxcxy4acdxltuzp6glyz",
    "type": "witness_v0_keyhash",
    "p2sh-segwit": "2NAZvWmSkujTRaTb18q4o5XcMBsa9heootm"
  }
}
```

```
C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" decodescript "473044022060089f64f0411ccc67791708f3c39fcd3f0148bbea10354254d54d29c109e70a602200c2217d077b142524e9c7d59423a445ba1fb70029a7d08ba97bedbed5
b17a5cb01210232629a1959c4c4537c841b6dedb77449e5d63571a6b3370dcfe9f3cd37df79bc"
{
  "asm": "304402206089f64f0411ccc67791708f3c39fcd3f0148bbea10354254d54d29c109e70a602200c2217d077b142524e9c7d59423a445ba1fb70029a7d08ba97bedbed5b17a5cb01 0232629a1959c4c4537c841b6dedb77449e5d63571a6b3370dcfe9f
3cd37df79bc",
  "desc": "raw(4730440220608 9f64f0411ccc67791708f3c39fcd3f0148bbea10354254d54d29c109e70a602200c2217d077b142524e9c7d59423a445ba1fb70029a7d08ba97bedbed5b17a5cb01210232629a1959c4c4537c841b6dedb77449e5d63571a6b33
70dcfe9f3cd37df79bc)#au04dt8v",
  "type": "nonstandard",
  "p2sh": "2MvFno6n6do5p6tjdUftmQSytHEeXpZpw8o",
  "segwit": {
    "asm": "0 186550dc72c9a5ccd5e4e353dff65abb5e82eab27d037849c2629f0ad1cf82a5",
    "desc": "addr(bcrt1qrpj4phrjexjue40yudfalaj6hd0g964j05phsjwzv20s45w0s2jssgn62r)#aczjk76j",
    "hex": "0020186550dc72c9a5ccd5e4e353dff65abb5e82eab27d037849c2629f0ad1cf82a5",
    "address": "bcrt1qrpj4phrjexjue40yudfalaj6hd0g964j05phsjwzv20s45w0s2jssgn62r",
    "type": "witness_v0_scripthash",
    "p2sh-segwit": "2NF7MSRiEeQHc3VM9t3HE79RUW4cXAuvq2C"
  }
}

C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" decodescript "76a9149e66ca4861fb2ba789d9ba2cc3244b13ef8b652988ac"
{
  "asm": "OP_DUP OP_HASH160 9e66ca4861fb2ba789d9ba2cc3244b13ef8b6529 OP_EQUALVERIFY OP_CHECKSIG",
  "desc": "addr(muxWCMD5oUun7ajTFpW6AnJ6TKFaqURrcj)#hs9jra33",
  "address": "muxWCMD5oUun7ajTFpW6AnJ6TKFaqURrcj",
  "type": "pubkeyhash",
  "p2sh": "2MumBvmk2jsM13n1hnrZX9abhwrJdYLh2i7",
  "segwit": {
    "asm": "0 9e66ca4861fb2ba789d9ba2cc3244b13ef8b6529",
    "desc": "addr(bcrt1qnenv5jrplv460zwehgkvxfztz0hckeffgj2jtm)#r2efwf3j",
    "hex": "00149e66ca4861fb2ba789d9ba2cc3244b13ef8b6529",
    "address": "bcrt1qnenv5jrplv460zwehgkvxfztz0hckeffgj2jtm",
    "type": "witness_v0_keyhash",
    "p2sh-segwit": "2NFgdc6d43ZnDHsnQHECH8Wiku7wK62xnSX"
  }
}

C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" decodescript "76a914ee09d03f43f54d5433c0bf8c029afd5cc095bd2488ac"
{
  "asm": "OP_DUP OP_HASH160 ee09d03f43f54d5433c0bf8c029afd5cc095bd24 OP_EQUALVERIFY OP_CHECKSIG",
  "desc": "addr(n3DasZW642bZkzNNzxj5FrUfAY7Bbjrq15)#x05knqma",
  "address": "n3DasZW642bZkzNNzxj5FrUfAY7Bbjrq15",
  "type": "pubkeyhash",
  "p2sh": "2MvQh12UTXsHCR5YzSRFB3DVNjBRkmEYvYB",
  "segwit": {
    "asm": "0 ee09d03f43f54d5433c0bf8c029afd5cc095bd24",
    "desc": "addr(bcrt1qacyaq06r74x4gv7qh7xq9xhatnqft0fyl7vf7u)#uu5ktxt3",
    "hex": "0014ee09d03f43f54d5433c0bf8c029afd5cc095bd24",
    "address": "bcrt1qacyaq06r74x4gv7qh7xq9xhatnqft0fyl7vf7u",
    "type": "witness_v0_keyhash",
    "p2sh-segwit": "2N5jEA3nabMjYVDA2q4U1FJuWHKfAGVQvFs"
  }
}
```

Execution Steps for Legacy (P2PKH) Transaction

1. Running the Transaction from A to B

- Execute the `legacy_AB.py` script to generate and sign the transaction where A sends Bitcoin to B.
- Extract the **transaction ID (txid)** from the output.
- Decode the transaction to view the **locking script (scriptPubKey)** and **unlocking script (scriptSig)**.

Command:

```
python legacy_AB.py
```

Expected Output:

- Displays the transaction details including txid.
- Shows the generated `scriptPubKey` and `scriptSig`.

2. Running the Transaction from B to C

- Use the txid from `legacy_AB.py` as input for the next transaction.
- Execute the `legacy_BC.py` script to generate the transaction where B sends Bitcoin to C.
- Decode and verify the **locking and unlocking scripts**.

Command:

```
python legacy_BC.py
```

Expected Output:

- Shows the new transaction details including updated txid.
- Displays the `scriptPubKey` and `scriptSig`.

3. Debugging and Verifying the Scripts

- Use a Bitcoin script debugger (e.g., `bitcoin-cli`, `bx`, or an online script debugger).
- Run the unlocking script (`scriptSig`) followed by the locking script (`scriptPubKey`) to check if they validate correctly.

Example Validation Using Bitcoin Debugger:

```
bx script-encode "<B's Signature> <B's Public Key> OP_DUP OP_HASH160
<B's Public Key Hash> OP_EQUALVERIFY OP_CHECKSIG"
```

- If valid, the script should return **"True"** or "Script executed successfully."

SegWit Transactions

Transaction Workflow:

1. **Transaction A to B:**
    a. A sends Bitcoin to B using SegWit (separating signatures from transaction data).
    b. A unique txid is generated.
    c. The output of this transaction is used in the next transaction from B to C.

EXECUTION TX A->B

```
C:\BitCoin>python -u "c:\BitCoin\segwit_AB.py"

------------------------------------------------------------
|    P2SH-SEGWIT TRANSACTION SCRIPT (A' → B')
------------------------------------------------------------
Connecting to Bitcoin Core at http://vikas:saru@127.0.0.1:18443
------------------------------------------------------------

------------------------------------------------------------
| STEP                | DETAILS
------------------------------------------------------------
| Wallet Balance      | Before: 1482.24168326 BTC
------------------------------------------------------------
| Addresses Generated |
| Address A' (Sender) | 2NEtyxkxJeNnzyo6rUDnyHV9nYbN29VJLgs
| Address B' (Receiver)| 2MwuH62PRuN8MUVDYCRqdtfcQBz3XZTJozh
| Address C' (Receiver)| 2NEJAwtzaFenNbhXm5KgjSm86mcT1vMAjaM
------------------------------------------------------------
| UTXOs Before        | [No UTXOs Found]
------------------------------------------------------------
| Transaction Funded  |
| Sent 1 BTC to A'    | TXID: 24578c38f6ae8900eed0d48963165493f6bc6a17babce3b986fec0b9e04c0bea
------------------------------------------------------------
| Wallet Balance      | After Funding A': 1482.24164856 BTC
------------------------------------------------------------
| Transaction A' → B' |
| TXID                | bd0e1018585cc244a781eb4dad6e0e8a19b9c62da7786706c07df3862eacfbb6
------------------------------------------------------------
| P2SH-SegWit Script  |
| HEX                 | a9143312e5864a87bc291b241a3ab647c1f55cd2949087
| ASM                 | OP_HASH160 3312e5864a87bc291b241a3ab647c1f55cd29490 OP_EQUAL
| Type                | scripthash
------------------------------------------------------------
| UTXOs After A' → B' |
                        TXID: bd0e1018585cc244a781eb4dad6e0e8a19b9c62da7786706c07df3862eacfbb6 | VOUT: 0 | Amount: 0.50000000 BTC
                        TXID: bd0e1018585cc244a781eb4dad6e0e8a19b9c62da7786706c07df3862eacfbb6 | VOUT: 1 | Amount: 0.49990000 BTC
------------------------------------------------------------
| Final Wallet Balance | After Transactions: 1482.24154856 BTC
------------------------------------------------------------
| Addresses Saved     | Saved to segwit_addresses.txt for the next script
------------------------------------------------------------
```

2. **Transaction B to C:**
    a. B sends Bitcoin to C.
    b. The input references the previous txid.
    c. The unlocking data (witness data) includes B's signature and public key.

EXECUTION TX B->C

```
C:\BitCoin>python -u "c:\BitCoin\segwit_BC.py"

------------------------------------------------------------
|    P2SH-SEGWIT TRANSACTION SCRIPT (B' → C')
------------------------------------------------------------
Connecting to Bitcoin Core at http://vikas:saru@127.0.0.1:18443
------------------------------------------------------------
| Addresses Loaded     | Successfully loaded from segwit_addresses.txt

------------------------------------------------------------
| STEP                 | DETAILS
------------------------------------------------------------
| Selected UTXO        |
| TXID                 | bd0e1018585cc244a781eb4dad6e0e8a19b9c62da7786706c07df3862eacfbb6
| VOUT                 | 0
| Amount               | 0.50000000 BTC
------------------------------------------------------------
| Source TX Locking    |
| Script (P2SH-SegWit) | a9143312e5864a87bc291b241a3ab647c1f55cd2949087
| ASM                  | OP_HASH160 3312e5864a87bc291b241a3ab647c1f55cd29490 OP_EQUAL
------------------------------------------------------------
| Transaction B' → C'  |
| TXID                 | 72e54dfd8e0d33529fb4d019ecf3093fbd908dba2c5e245a87db325371a59707
------------------------------------------------------------
| Unlocking Script     |
| HEX                  | 160014a8a7f8bd5f3dbe50599efe6510bf202df4d87c9f
| ASM                  | 0014a8a7f8bd5f3dbe50599efe6510bf202df4d87c9f
| Witness Data         |
|   Item 0             | 30440220536d7ca1ac8fd6657b1c8fe2c3f4328b0a19bb7b587fff32e376ec7807095c7c02202af31b5ac5dc01dfd63d30b3b26dff55e68a62e30c13149d4f983c5c60d4aabc01
|   Item 1             | 02ebfebd2aae0ebe8a47fcc1c9d0344991c9cd81d65d832dc1cf412ab28b168e8a
------------------------------------------------------------
| Locking Script (C')  |
| HEX                  | a914e6e959c8cf5b53f25a87459671be58c1f75db2d987
| ASM                  | OP_HASH160 e6e959c8cf5b53f25a87459671be58c1f75db2d9 OP_EQUAL
------------------------------------------------------------
| Script Verification  |
| Process              | 1. P2SH-SegWit unlocking script provides redeemScript
|                      | 2. Witness data contains signature and pubkey
|                      | 3. Script hash is verified against address
|                      | 4. Signature validated with witness program
|                      | 5. If valid, Bitcoin is transferred to Address C'
------------------------------------------------------------
| UTXOs After B' → C'  |
------------------------------------------------------------
| TXID                                  | VOUT | Amount       |
------------------------------------------------------------
| 72e54dfd8e0d33529fb4d019ecf3093fbd908dba2c... | 0    | 0.30000000 BTC |
| 72e54dfd8e0d33529fb4d019ecf3093fbd908dba2c... | 1    | 0.19990000 BTC |
------------------------------------------------------------
------------------------------------------------------------
| Final Wallet Balance | After Transactions: 1482.24144856 BTC
```

Decoded Scripts:

Transaction A to B

- **Locking Script (scriptPubKey):** `OP_0 <B's Public Key Hash>`

- **Witness Data:** `<B's Signature> <B's Public Key>`

- **Python Script Execution (segwit_AB.py):**
    - Implements SegWit transaction structure using the `bitcoin.core.script` module.
    - Separates signature from the main transaction data.

DECODE TX A->B

```
C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" gettransaction "bd0e1018585cc244a781eb4dad6e0e8a19b9c62da7786706c07df3862eacfbb6"
{
  "amount": 0.00000000,
  "fee": -0.00010000,
  "confirmations": 2,
  "blockhash": "202be7c30fb23c538cca3254425df4bbb5e24f851d448cbf49c85532a382d4383",
  "blockheight": 7155,
  "blockindex": 1,
  "blocktime": 1742733586,
  "txid": "bd0e1018585cc244a781eb4dad6e0e8a19b9c62da7786706c07df3862eacfbb6",
  "wtxid": "4b6b44b2e674f0626d952a3679dc2d8528735cd569ad9956e63137fe61a3ef19",
  "walletconflicts": [
  ],
  "mempoolconflicts": [
  ],
  "time": 1742733586,
  "timereceived": 1742733586,
  "bip125-replaceable": "no",
  "details": [
    {
      "address": "2MwuH62PRuN8MUVDYCRqdtfcQBz3XZTJozh",
      "category": "send",
      "amount": -0.50000000,
      "label": "addr_b",
      "vout": 0,
      "fee": -0.00010000,
      "abandoned": false
    },
    {
      "address": "2NEtyxkxJeNnzyo6rUDnyHV9nYbN29VJLgs",
      "category": "send",
      "amount": -0.49990000,
      "label": "addr_a",
      "vout": 1,
      "fee": -0.00010000,
      "abandoned": false
    },
    {
      "address": "2MwuH62PRuN8MUVDYCRqdtfcQBz3XZTJozh",
      "category": "receive",
      "parent_descs": [
        "sh(wpkh(tpubD6NzVbkrYhZ4Y1JCXirwutAHrHpLm352ND6RyBiFXuZgUF69k545PyyBTndqqbN34rC7oXqnVCRLrw9HtPfgLLxalfxctaWPXuRoXyodcQSc/49h/1h/0h/0/*))#3e0ugwlj"
      ],
      "category": "receive",
      "amount": 0.50000000,
      "label": "addr_b",
      "vout": 0,
      "abandoned": false
    },
    {
      "address": "2NEtyxkxJeNnzyo6rUDnyHV9nYbN29VJLgs",
      "parent_descs": [
        "sh(wpkh(tpubD6NzVbkrYhZ4Y1JCXirwutAHrHpLm352ND6RyBiFXuZgUF69k545PyyBTndqqbN34rC7oXqnVCRLrw9HtPfgLLxalfxctaWPXuRoXyodcQSc/49h/1h/0h/0/*))#3e0ugwlj"
      ],
      "category": "receive",
      "amount": 0.49990000,
      "label": "addr_a",
      "vout": 1,
      "abandoned": false
    }
  ],
  "hex": "02000000000101ea0b4ce0b9c0fe86b9e3bcba176abcf69354166389d4d0ee0889aef6388c57240000000001716001423bb377d5fe0c355be6a6cbe964a0fc3d769f38bfdfffffff0280f0fa02000000017a9143312e5864a87bc291b241a3ab647c1f55cd294908770c9fa020000000017a914ed7ebd4c21afe61f20c95321bddf441b2bef3d6d87024730440220053c31f6d18634549569faaadd8bfefc362ede6ee7cc29e894f0f184e566929570220360a58139e6a5cc08d8feded903697e9dcf9fce12955345d40885aeaca194d25b0121026df0a7f06e3a7975db44b9f3b8327be9c89dbcfeb63e9000669f75911175d2e600000000",
  "lastprocessedblock": {
    "hash": "559eb2aac66b31a2c5ac1f887cb6a629b5e1cd7fc090da930860daa3ffd9e",
    "height": 7156
  }
}
```


```
C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" decoderawtransaction "02000000000101ea0b4ce0b9c0fe86b9e3bcba176abcf69354166389d4d0ee0889aef6388c57240000000001716001423bb377d5fe0c355be6a6cbe964a0fc3d
769f38bfdfffffff0280f0fa02000000017a9143312e5864a87bc291b241a3ab647c1f55cd294908770c9fa020000000017a914ed7ebd4c21afe61f20c95321bddf441b2bef3d6d87024730440220053c31f6d18634549569faaadd8bfefc362ede6ee7cc29e894f0
f184e566929570220360a58139e6a5cc08d8feded903697e9dcf9fce12955345d40885aeaca194d25b0121026df0a7f06e3a7975db44b9f3b8327be9c89dbcfeb63e9000669f75911175d2e600000000"
{
  "txid": "bd0e1018585cc244a781eb4dad6e0e8a19b9c62da7786706c07df3862eacfbb6",
  "hash": "4b6b44b2e674f0626d952a3679dc2d8528735cd569ad9956e63137fe61a3ef19",
  "version": 2,
  "size": 247,
  "vsize": 166,
  "weight": 661,
  "locktime": 0,
  "vin": [
    {
      "txid": "24578c38f6ae8900eed0d48963165493f6bc6a17babce3b986fec0b9e04c0bea",
      "vout": 0,
      "scriptSig": {
        "asm": "001423bb377d5fe0c355be6a6cbe964a0fc3d769f38b",
        "hex": "16001423bb377d5fe0c355be6a6cbe964a0fc3d769f38b"
      },
      "txinwitness": [
        "3044022853c31f6d18634549569faaadd8bfefc362ede6ee7cc29e894f0f184e566929570220360a58139e6a5cc08d8feded903697e9dcf9fce12955345d40885aeaca194d25b01",
        "026df0a7f06e3a7975db44b9f3b8327be9c89dbcfeb63e9000669f75911175d2e6"
      ],
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 0.50000000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_HASH160 3312e5864a87bc291b241a3ab647c1f55cd29490 OP_EQUAL",
        "desc": "addr(2MwuH62PRuN8MUVDYCRqdtfcQBz3XZTJozh)#tv52jz8r",
        "hex": "a9143312e5864a87bc291b241a3ab647c1f55cd2949087",
        "address": "2MwuH62PRuN8MUVDYCRqdtfcQBz3XZTJozh",
        "type": "scripthash"
      }
    },
    {
      "value": 0.49990000,
      "n": 1,
      "scriptPubKey": {
        "asm": "OP_HASH160 ed7ebd4c21afe61f20c95321bddf441b2bef3d6d OP_EQUAL",
        "desc": "addr(2NEtyxkxJeNnzyo6rUDnyHV9nYbN29VJLgs)#ugn3t99k",
        "hex": "a914ed7ebd4c21afe61f20c95321bddf441b2bef3d6d87",
        "address": "2NEtyxkxJeNnzyo6rUDnyHV9nYbN29VJLgs",
        "type": "scripthash"
      }
    }
  ]
}
```

Transaction B to C

- **Locking Script (scriptPubKey):** `OP_0 <C's Public Key Hash>`

- **Witness Data:** `<C's Signature> <C's Public Key>`

- **Python Script Execution (segwit_BC.py):**
    - Similar to segwit_AB.py, following SegWit transaction validation.

DECODE TX B->C


C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" gettransaction "72e54dfd8e0d33529fb4d019ecf3893fbd908dba2c5e245a87db325371a59707"
{
"amount": 0.00000000,
"fee": -0.00010000,
"confirmations": 1,
"blockhash": "559e0c2aceac66b31a2c5ac1f867cb6a629b5e1c07fc090de930060daa3ffd9e",
"blockheight": 7156,
"blockindex": 1,
"blocktime": 1742733658,
"txid": "72e54dfd8e0d33529fb4d019ecf3893fbd908dba2c5e245a87db325371a59707",
"wtxid": "880fded4feb6bee7e359a1044845339ee0f077f7269e147c62512e3622cd7118",
"walletconflicts": [
],
"mempoolconflicts": [
],
"time": 1742733658,
"timereceived": 1742733658,
"bip125-replaceable": "no",
"details": [
{
"address": "2NEJAwtzaFenNbhXm5KgjSm86mcT1vMAjaM",
"category": "send",
"amount": -0.30000000,
"label": "addr_c",
"vout": 0,
"fee": -0.00010000,
"abandoned": false
},
{
"address": "2MwuH62PRuN8MUVDYCRqdtfcQBz3XZTJozh",
"category": "send",
"amount": -0.19990000,
"label": "addr_b",
"vout": 1,
"fee": -0.00010000,
"abandoned": false
},
{
"address": "2NEJAwtzaFenNbhXm5KgjSm86mcT1vMAjaM",
"parent_descs": [
"sh(wpkh(tpubD6NzVbkrYhZ4YjCXirwutAHrkpLm352RD6RyBiFXuZgUF69h54SPyyBTndgqbW3HzC7oXqnVCRLzw9HtPFgLLxalfxctuWPXuRoXyodcQ5c/49h/1h/0h/0/*))#3e0ugwlj"
],
"category": "receive",
"amount": 0.30000000,
"label": "addr_c",
"vout": 0,
"abandoned": false
},
{
"address": "2MwuH62PRuN8MUVDYCRqdtfcQBz3XZTJozh",
"parent_descs": [
"sh(wpkh(tpubD6NzVbkrYhZ4YjCXirwutAHrkpLm352RD6RyBiFXuZgUF69h54SPyyBTndgqbW3HzC7oXqnVCRLzw9HtPFgLLxalfxctuWPXuRoXyodcQ5c/49h/1h/0h/0/*))#3e0ugwlj"
],
"category": "receive",
"amount": 0.19990000,
"label": "addr_b",
"vout": 1,
"abandoned": false
}
],
"hex": "02000000000101b6fbac2e86f37dc0066778a72dc6b9198a8e6ead4deb81a744c25c5818100ebd0000000017160014a8a7f8bd5f3dbe50599efe6510bf202df4d87c9ffdffffff0288c3c9010000000017a914e6e959c8cf5b53f25a87459671be58c1f75db2d987f0053101000000017a9143312e5864a87bc291b241a3ab647c1f55cd2949087024730440220536d7ca1ac8fd6657b1c8fe2c3f4328b0a19bb7b587fff32e376ec7807095c7c02202af31b5ac5dc01dfd63d30b3b26dff55e68a62e30c13149d4f983c5c60d4aabc012102ebfebd2aae0ebe8a47fcc1c9d0344991c9cd81d65d832dc1cf412ab28b168e8a00000000",
"tx": {
"hash": "559e0c2aceac66b31a2c5ac1f867cb6a629b5e1c07fc090de930060daa3ffd9e",
"height": 7156
}
}


C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" decoderawtransaction "02000000000101b6fbac2e86f37dc0066778a72dc6b9198a8e6ead4deb81a744c25c5818100ebd0000000017160014a8a7f8bd5f3dbe50599efe6510bf202df4d87c9ffdffffff0288c3c9010000000017a914e6e959c8cf5b53f25a87459671be58c1f75db2d987f0053101000000017a9143312e5864a87bc291b241a3ab647c1f55cd2949087024730440220536d7ca1ac8fd6657b1c8fe2c3f4328b0a19bb7b587fff32e376ec7807095c7c02202af31b5ac5dc01dfd63d30b3b26dff55e68a62e30c13149d4f983c5c60d4aabc012102ebfebd2aae0ebe8a47fcc1c9d0344991c9cd81d65d832dc1cf412ab28b168e8a00000000"
{
"txid": "72e54dfd8e0d33529fb4d019ecf3893fbd908dba2c5e245a87db325371a59707",
"hash": "880fded4feb6bee7e359a1044845339ee0f077f7269e147c62512e3622cd7118",
"version": 2,
"size": 247,
"vsize": 166,
"weight": 661,
"locktime": 0,
"vin": [
{
"txid": "bd0e1018585cc244a781eb4dad6e0e8a19b9c62da7786706c07df3862eacfbb6",
"vout": 0,
"scriptSig": {
"asm": "0014a8a7f8bd5f3dbe50599efe6510bf202df4d87c9f",
"hex": "160014a8a7f8bd5f3dbe50599efe6510bf202df4d87c9f"
},
"txinwitness": [
"304402220536d7ca1ac8fd6657b1c8fe2c3f4328b0a19bb7b587fff32e376ec7807095c7c02202af31b5ac5dc01dfd63d30b3b26dff55e68a62e30c13149d4f983c5c60d4aabc01",
"02ebfebd2aae0ebe8a47fcc1c9d0344991c9cd81d65d832dc1cf412ab28b168e8a"
],
"sequence": 4294967293
}
],
"vout": [
{
"value": 0.30000000,
"n": 0,
"scriptPubKey": {
"asm": "OP_HASH160 e6e959c8cf5b53f25a87459671be58c1f75db2d9 OP_EQUAL",
"desc": "addr(2NEJAwtzaFenNbhXm5KgjSm86mcT1vMAjaM)#g8uaq0gu",
"hex": "a914e6e959c8cf5b53f25a87459671be58c1f75db2d987",
"address": "2NEJAwtzaFenNbhXm5KgjSm86mcT1vMAjaM",
"type": "scripthash"
}
},
{
"value": 0.19990000,
"n": 1,
"scriptPubKey": {
"asm": "OP_HASH160 3312e5864a87bc291b241a3ab647c1f55cd29490 OP_EQUAL",
"desc": "addr(2MwuH62PRuN8MUVDYCRqdtfcQBz3XZTJozh)#tv52jz8r",
"hex": "a9143312e5864a87bc291b241a3ab647c1f55cd2949087",
"address": "2MwuH62PRuN8MUVDYCRqdtfcQBz3XZTJozh",
"type": "scripthash"
}
}
]
}

Challenge and Response Script Structure:

Challenge Script = Locking Script (scriptPubKey)

Response Script = Unlocking Script (scriptSig or witness)

- In SegWit, the **locking script** is minimal, with the actual validation occurring in the witness data.
- The **witness field** contains the signature and public key, separate from the transaction structure.
- This approach reduces transaction size and enhances efficiency.

SegWit AB Transaction:

- *Transaction ID:* bd0e1018585cc244a781eb4dad6e0e8a19b9c62da7786706c07df3862eacfbb6
- *Hash:* 4b6b44b2e674f0626d952a3679dc2d8528735cd569ad9956e63137fe61a3ef19
- *Version:* 2
- *Size:* 247 bytes
- *Virtual Size:* 166 vbytes
- *Weight:* 661
- *Locktime:* 0

Input (vin):

- *Previous TX ID:* 24578c38f6ae8900eed0d48963165493f6bc6a17babce3b986fec0b9e04c0bea
- *Output Index (vout):* 0
- *ScriptSig:*
    - *ASM:*

001423bb377d5fe0c355be6a6cbe964a0fc3d769f38b

    - *Hex:* 16001423bb377d5fe0c355be6a6cbe964a0fc3d769f38b
- *Witness:*
    - *Signature:* 3044022053c31f6d18634549569faaadd8bfefc362ede6ee7cc29e894f0f184e56692957022036a58139e6a5cc08d8feded903697e9dcf9fce12955345d40885aeaca194d25b01
    - *Public Key:* 026df0a7f06e3a7975db44b9f3b8327be9c89dbcfeb63e9000669f75911175d2e6
- *Sequence:* 4294967293

Outputs (vout):

1. *Output 0:*
    a. *Value:* 0.50000000 BTC
    b. *ScriptPubKey ASM:* OP_HASH160 3312e5864a87bc291b241a3ab647c1f55cd29490 OP_EQUAL
    c. *Address:* 2MwuH62PRuN8MUVDYCRqdtfcQBz3XZTJozh
    d. *Type:* scripthash
2. *Output 1:*
    a. *Value:* 0.49990000 BTC
    b. *ScriptPubKey ASM:* OP_HASH160 ed7ebd4c21afe61f20c95321bddf441b2bef3d6d OP_EQUAL
    c. *Address:* 2NEtyxkxJeNnzyo6rUDnyHV9nYbN29VJLgs
    d. *Type:* scripthash

SegWit BC Transaction:

- *Transaction ID:* 72e54dfd8e0d33529fb4d019ecf3093fbd908dba2c5e245a87db325371a59707
- *Hash:* 880fded4feb6bee7e359a1044845339ee0f077f7269e147c62512e3622cd7118
- *Version:* 2
- *Size:* 247 bytes
- *Virtual Size:* 166 vbytes
- *Weight:* 661
- *Locktime:* 0

Input (vin):

- *Previous TX ID:* bd0e1018585cc244a781eb4dad6e0e8a19b9c62da7786706c07df3862eacfbb6
- *Output Index (vout):* 0
- *ScriptSig:*
    - *ASM:* 0014a8a7f8bd5f3dbe50599efe6510bf202df4d87c9f
    - *Hex:* 160014a8a7f8bd5f3dbe50599efe6510bf202df4d87c9f
- *Witness:*
    - *Signature:* 30440220536d7ca1ac8fd6657b1c8fe2c3f4328b0a19bb7b587fff32e376ec7807095c7c02202af31b5ac5dc01dfd63d30b3b26dff55e68a62e30c13149d4f983c5c60d4aabc01
    - *Public Key:* 02ebfebd2aae0ebe8a47fcc1c9d0344991c9cd81d65d832dc1cf412ab28b168e8a
- *Sequence:* 4294967293

Outputs (vout):

1. *Output 0:*
    a. *Value:* 0.30000000 BTC
    b. *ScriptPubKey ASM:* OP_HASH160 e6e959c8cf5b53f25a87459671be58c1f75db2d9 OP_EQUAL
    c. *Address:* 2NEJAwtzaFenNbhXm5KgjSm86mcT1vMAjaM
    d. *Type:* scripthash
2. *Output 1:*
    a. *Value:* 0.19990000 BTC
    b. *ScriptPubKey ASM:* OP_HASH160 3312e5864a87bc291b241a3ab647c1f55cd29490 OP_EQUAL
    c. *Address:* 2MwuH62PRuN8MUVDYCRqdtfcQBz3XZTJozh
    d. *Type:* scripthash

CHALLENGE AND RESPONSE SCRIPTS

```
-------------------------------------------------------------------
| Unlocking Script     |
| HEX                  | 160014a8a7f8bd5f3dbe50599efe6510bf202df4d87c9f
| ASM                  | 0014a8a7f8bd5f3dbe50599efe6510bf202df4d87c9f
| Witness Data         |
|   Item 0             | 30440220536d7ca1ac8fd6657b1c8fe2c3f4328b0a19bb7b587fff32e376ec7807095c7c02202af31b5ac5dc01dfd63d30b3b26dff55e68a62e30c13149d4f983c5c60d4aabc01
|   Item 1             | 02ebfebd2aae0ebe8a47fcc1c9d0344991c9cd81d65d832dc1cf412ab28b168e8a
-------------------------------------------------------------------
| Locking Script (C')  |
| HEX                  | a914e6e959c8cf5b53f25a87459671be58c1f75db2d987
| ASM                  | OP_HASH160 e6e959c8cf5b53f25a87459671be58c1f75db2d9 OP_EQUAL
-------------------------------------------------------------------
```

```
C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" decodescript "4730440220689f64f0411ccc67791708f3c39fcd3f0148bbea1035425d54d29c109e70a602200c2217d077b142524e9c7d59423a445ba1fb70029a7d08ba97bedbed5b17a5cb01210232629a1959c4c4537c841b6dedb77449e5d63571a6b3370dcfe9f3cd37df79bc"
{
  "asm": "304402206089f64f0411ccc67791708f3c39fcd3f0148bbea1035425d54d29c109e70a602200c2217d077b142524e9c7d59423a445ba1fb70029a7d08ba97bedbed5b17a5cb01 0232629a1959c4c4537c841b6dedb77449e5d63571a6b3370dcfe9f3cd37df79bc",
  "desc": "raw(4730440220689f64f0411ccc67791708f3c39fcd3f0148bbea1035425d54d29c109e70a602200c2217d077b142524e9c7d59423a445ba1fb70029a7d08ba97bedbed5b17a5cb01210232629a1959c4c4537c841b6dedb77449e5d63571a6b3370dcfe9f3cd37df79bc)#au84dt8v",
  "type": "nonstandard",
  "p2sh": "2MvFno6n6do5p6tjdUftmQSytHEeXpZpw8o",
  "segwit": {
    "asm": "0 186550dc72c9a5ccd5e4e353dff65abb5e82eab27d037849c2629f0ad1cf82a5",
    "desc": "addr(bcrt1qrpj4phrjexjue40yudfalaj6hd0g964j05phsjwzv20s45w0s2jssgn62r)#aczjk76j",
    "hex": "0020186550dc72c9a5ccd5e4e353dff65abb5e82eab27d037849c2629f0ad1cf82a5",
    "address": "bcrt1qrpj4phrjexjue40yudfalaj6hd0g964j05phsjwzv20s45w0s2jssgn62r",
    "type": "witness_v0_scripthash",
    "p2sh-segwit": "2NF7M5RiEeQHc3VM9t3HE79RUW4cXAuvq2C"
  }
}

C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" decodescript "76a914ee09d03f43f54d5433c0bf8c029afd5cc095bd2488ac"
{
  "asm": "OP_DUP OP_HASH160 ee09d03f43f54d5433c0bf8c029afd5cc095bd24 OP_EQUALVERIFY OP_CHECKSIG",
  "desc": "addr(n3DasZW642bZkzNNzxj5FrUfAY7Bbjrq15)#x05knqma",
  "address": "n3DasZW642bZkzNNzxj5FrUfAY7Bbjrq15",
  "type": "pubkeyhash",
  "p2sh": "2MvQh12UTXsHCR5YzSRFB3DVNjBRkmEYvYB",
  "segwit": {
    "asm": "0 ee09d03f43f54d5433c0bf8c029afd5cc095bd24",
    "desc": "addr(bcrt1qacyaq06r74x4gv7qh7xq9xhatnqft0fyl7vf7u)#uu5ktxt3",
    "hex": "0014ee09d03f43f54d5433c0bf8c029afd5cc095bd24",
    "address": "bcrt1qacyaq06r74x4gv7qh7xq9xhatnqft0fyl7vf7u",
    "type": "witness_v0_keyhash",
    "p2sh-segwit": "2N5jEA3nabMjYVDA2q4U1FJuWHKfAGVQvFs"
  }
}

C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" decodescript "76a91461aa5045026c85d1646e83486c1895ee1a6faf8288ac"
{
  "asm": "OP_DUP OP_HASH160 61aa5045026c85d1646e83486c1895ee1a6faf82 OP_EQUALVERIFY OP_CHECKSIG",
  "desc": "addr(mpRMsFj2wdvvc79pPHzPXjhQamafK19RYR)#2qjtpau0",
  "address": "mpRMsFj2wdvvc79pPHzPXjhQamafK19RYR",
  "type": "pubkeyhash",
  "p2sh": "2NB2fUYRkm9hBtMDZqj5EqnvKfdiBJTX82c",
  "segwit": {
    "asm": "0 61aa5045026c85d1646e83486c1895ee1a6faf82",
    "desc": "addr(bcrt1qvx49q3gzdjzazerwsdyxcxy4acdxltuzp6glyz)#zh2f0dh5",
    "hex": "001461aa5045026c85d1646e83486c1895ee1a6faf82",
    "address": "bcrt1qvx49q3gzdjzazerwsdyxcxy4acdxltuzp6glyz",
    "type": "witness_v0_keyhash",
    "p2sh-segwit": "2NAZvWmSkujTRaTb18q4o5XcMBsa9heootm"
  }
}
```

```
C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" decodescript "160014a8a7f8bd5f3dbe50599efe6510bf202df4d87c9f"
{
  "asm": "0014a8a7f8bd5f3dbe50599efe6510bf202df4d87c9f",
  "desc": "raw(160014a8a7f8bd5f3dbe50599efe6510bf202df4d87c9f)#gsvfv6g3",
  "type": "nonstandard",
  "p2sh": "2NC5hA4edheHLVUyS56a3TcX5RkTh9oGNp6",
  "segwit": {
    "asm": "0 1e97edb61ee20d1132d09c2ef77f496925fcbddde0acec77c7fdb992e9daa0b6",
    "desc": "addr(bcrt1qr6t7mds7ugx3zvksnsh0wl6fdyjle0wauzkwca78lkue96w65zmqdz3fkx)#4vlqlwwk",
    "hex": "00201e97edb61ee20d1132d09c2ef77f496925fcbddde0acec77c7fdb992e9daa0b6",
    "address": "bcrt1qr6t7mds7ugx3zvksnsh0wl6fdyjle0wauzkwca78lkue96w65zmqdz3fkx",
    "type": "witness_v0_scripthash",
    "p2sh-segwit": "2N19Xf8zgvUva3ZsSwVSyjWJtjjLquMm1E7"
  }
}

C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" decodescript "a914e6e959c8cf5b53f25a87459671be58c1f75db2d987"
{
  "asm": "OP_HASH160 e6e959c8cf5b53f25a87459671be58c1f75db2d9 OP_EQUAL",
  "desc": "addr(2NEJAwtzaFenNbhXm5KgjSm86mcT1vMAjaM)#g8uaq0gu",
  "address": "2NEJAwtzaFenNbhXm5KgjSm86mcT1vMAjaM",
  "type": "scripthash"
}

C:\Users\Sumathi>bitcoin-cli -regtest -rpcwallet="project" decodescript "a9143312e5864a87bc291b241a3ab647c1f55cd2949087"
{
  "asm": "OP_HASH160 3312e5864a87bc291b241a3ab647c1f55cd29490 OP_EQUAL",
  "desc": "addr(2MwuH62PRuN8MUVDYCRqdtfcQBz3XZTJozh)#tv52jz8r",
  "address": "2MwuH62PRuN8MUVDYCRqdtfcQBz3XZTJozh",
  "type": "scripthash"
}
```

Execution Steps for SegWit Transactions

1. Running the Transaction from A to B

- Execute the `segwit_AB.py` script to create and sign a SegWit transaction from A to B.
- Extract the **transaction ID (txid)**.
- Decode the transaction to view the **locking script (scriptPubKey)** and **witness data**.

Command:

```
python segwit_AB.py
```

Expected Output:

- Displays SegWit transaction details including txid.
- Shows `scriptPubKey` and `witness data`.

2. Running the Transaction from B to C

- Use the txid from `segwit_AB.py` as input for the next transaction.
- Execute the `segwit_BC.py` script to create the transaction from B to C.
- Decode and verify the **locking script and witness data**.

Command: `python segwit_BC.py`

Expected Output:

- Displays updated transaction details with new txid.
- Shows `scriptPubKey` and `witness data`.

3. Debugging and Verifying the Scripts

- Use a SegWit-compatible Bitcoin debugger.
- Run the witness script to validate it against the locking script.

Example Validation Using Bitcoin Debugger:

```
bx script-encode "<B's Signature> <B's Public Key> OP_0 <B's Public Key Hash>"
```

- If valid, the script should return **"True"** or "Script executed successfully."

Part 3: Analysis and Explanation

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

1. Size Comparison:

Transaction Type	Version	Size (bytes)	Virtual Size (vbytes)	Weight
Legacy AB	2	225	225	900
Legacy BC	2	225	225	900
SegWit AB	2	247	166	661
SegWit BC	2	247	166	661

2. Script Structure Comparison:

Type	Script Type	Input Script (Challenge)	Output Script (Response)
Legacy	P2PKH (Pay to PubKey Hash)		OP_DUP OP_HASH160 OP_EQUALVERIFY OP_CHECKSIG
SegWit	P2SH-P2WPKH (Pay to Witness Public Key Hash)	(witness signature and public key are separate)	OP_HASH160 OP_EQUAL
SegWit	Witness Data		-

3. Why SegWit Transactions Are Smaller:

SegWit (Segregated Witness) transactions are smaller in terms of *weight and virtual size* compared to legacy transactions. This reduction in size is primarily because the witness data (signature and public key) is stored separately from the transaction itself. The key factors contributing to the reduced size are:

1. *Witness Data Segregation:*
    a. In SegWit transactions, the signature data is moved to a separate witness structure.

    b. This results in a smaller *vsize* (virtual size) since the witness data has a weight factor of *1* instead of *4* for non-witness data.
2. *Efficiency in Script Execution:*
    a. Legacy transactions contain signatures and public keys directly in the input script (scriptSig), making the transaction size larger.
    b. SegWit moves this data to the witness, resulting in smaller script sizes and therefore less space consumed.
3. *Reduced Malability:*
    a. SegWit transactions help in eliminating transaction malleability by segregating the signature data.
    b. This improves the consistency of the transaction ID (TXID).
4. *Increased Block Capacity:*
    a. By reducing the effective size of transactions, more transactions can fit into a block, effectively increasing the throughput.

4. Benefits of SegWit Transactions:

1. *Higher Transaction Throughput:*
    a. Reduced size and weight allow more transactions to fit in a single block, increasing the transaction throughput and efficiency.
2. *Reduced Transaction Fees:*
    a. Since fees are calculated based on the size of the transaction in *vbytes*, SegWit transactions generally incur lower fees.
3. *Elimination of Malleability:*
    a. Moving signature data to the witness structure significantly reduces transaction malleability.
4. *Backward Compatibility:*
    a. SegWit maintains backward compatibility with legacy transactions, allowing seamless integration into existing infrastructure.
5. *Support for Lightning Network:*

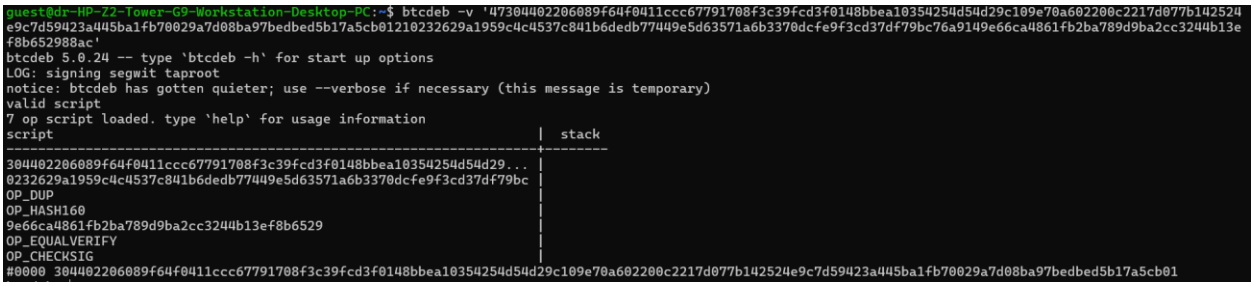
a. SegWit is a fundamental upgrade that supports second-layer solutions like the Lightning Network, enabling faster and cheaper transactions.

Summary:

SegWit transactions are more space-efficient and less prone to malleability compared to legacy transactions. The separation of witness data from the main transaction reduces the weight and virtual size, making them faster and cheaper. These improvements ultimately help in optimizing the network and making it more scalable, while also paving the way for advanced solutions like the Lightning Network.

DEBUGGER

LEGACY TRANSACTION DEBUGGER



SEGWIT TRANSACTION DEBUGGER