ASSIGNMENT - 2

INTRODUCTION TO BLOCKCHAIN

E.Lathika Priya - 230001026
Shaik Soha Sultana - 230001071
G.Harshitha - 230001027

P2PKH TRANSACTIONS

Step 1: Generate Legacy address

```
C:\Users\Dell\OneDrive\SmartCookies_Blockchain_Assignment2>python generate_legacy_addresses.py
Address A: mfcvYJWpesCurDa4Sxe6RZL5PbwPCHasa9
Address B: n1pme2NhAkytVRog7c5FFhQ5mb9ihPnxzx
Address C: mzCaBPF6B755DJfSAGgSWQX2GWWrqa6vzp
```

Step 2: Fund to A

Funding to address A is done directly by using sendtoaddress command

Checking if A consists of the above transaction in UTXO

```
C:\Users\Dell\OneDrive\SmartCookies_Blockchain_Assignment2>bitcoin-cli -regtest listunspent 0 9999999 "[\"mfcvYJWpesCurDa4Sxe6RZL5Pbw
PCHasa9\"]"
[
  {
    "txid": "86631b90de8035f0fc96b2b43b6c2932ce02dd583a5bea5cde8c9d40d1b12250",
    "vout": 0,
    "address": "mfcvYJWpesCurDa4Sxe6RZL5PbwPCHasa9",
    "label": "",
    "scriptPubKey": "76a9140121080523a5cf69019920333a10b9d66f103aa088ac",
    "amount": 10.00000000,
    "confirmations": 0,
    "ancestorcount": 1,
    "ancestorsize": 282,
    "ancestorfees": 2820,
    "spendable": true,
    "solvable": true,
    "desc": "pkh([39b351d7/44h/1h/0h/0/10]02f1fe14ce8a76f5a67531f4776e1690da9cea110b483774e6e5f10e2b7fb9b0a3)#s3vjqa3v",
    "parent_descs": [
      "pkh(tpubD6NzVbkrYhZ4YWV5wSpepS12Jkk1xgBe4uXYaejNDfYtgw6UWsWdPa2zYeCsVTsJ8JiNJ22NnQDHKH7rcQMMz9ebbZfmVyoYm831hkSzRTx/44h/1h/0h/
0/*)#xunwm2dx"
    ],
    "safe": true
  },
```

Step 3: A to B transaction

The previously unspent transaction in the A is used for the above transaction.

```
C:\Users\Dell\OneDrive\SmartCookies_Blockchain_Assignment2>python send_A_to_B.py
🔧 Raw Transaction (Unsigned): 02000000015022b1d1409d8cde5cea5b3a58dd02ce32296c3bb4b296fcf03580de901b63860000000000fdffffff01f0a29a3b
000000001976a914dec11baaab82e6c0d26ee2fd551cd9a9bc448f2688ac00000000
 Transaction successfully sent! TXID: f18cf928ec9669218bdf4f8c24e011d43010007a00db486667587595cc1a7021
```

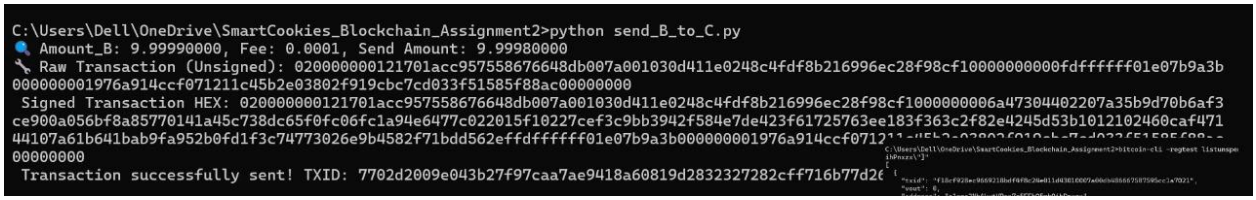
TX_id: f18cf928ec9669218bdf4f8c24e011d43010007a00db486667587595cc1a7021

The previous unspent transaction in A is now used for sending the funds into B.
Now, there wil be no unspent transactions left in A, whereas B consists the transaction A to B.

```
C:\Users\Dell\OneDrive\SmartCookies_Blockchain_Assignment2>bitcoin-cli -regtest listunspent 0 9999999 "[\"n1pme2NhAkytVRog7c5FFhQ5mb9
ihPnxzx\"]"
[
  {
    "txid": "f18cf928ec9669218bdf4f8c24e011d43010007a00db486667587595cc1a7021",
    "vout": 0,
    "address": "n1pme2NhAkytVRog7c5FFhQ5mb9ihPnxzx",
    "label": "",
    "scriptPubKey": "76a914dec11baaab82e6c0d26ee2fd551cd9a9bc448f2688ac",
    "amount": 9.99990000,
    "confirmations": 1,
    "spendable": true,
    "solvable": true,
    "desc": "pkh([39b351d7/44h/1h/0h/0/11]02460caf47144107a61b641bab9fa952b0fd1f3c74773026e9b4582f71bdd562ef)#nezlveqn",
    "parent_descs": [
      "pkh(tpubD6NzVbkrYhZ4YWV5wSpepS12Jkk1xgBe4uXYaejNDfYtgw6UWsWdPa2zYeCsVTsJ8JiNJ22NnQDHKH7rcQMMz9ebbZfmVyoYm831hkSzRTx/44h/1h/0h/
0/*)#xunwm2dx"
    ],
    "safe": true
  }
]
```

Step 4: B to C transaction:

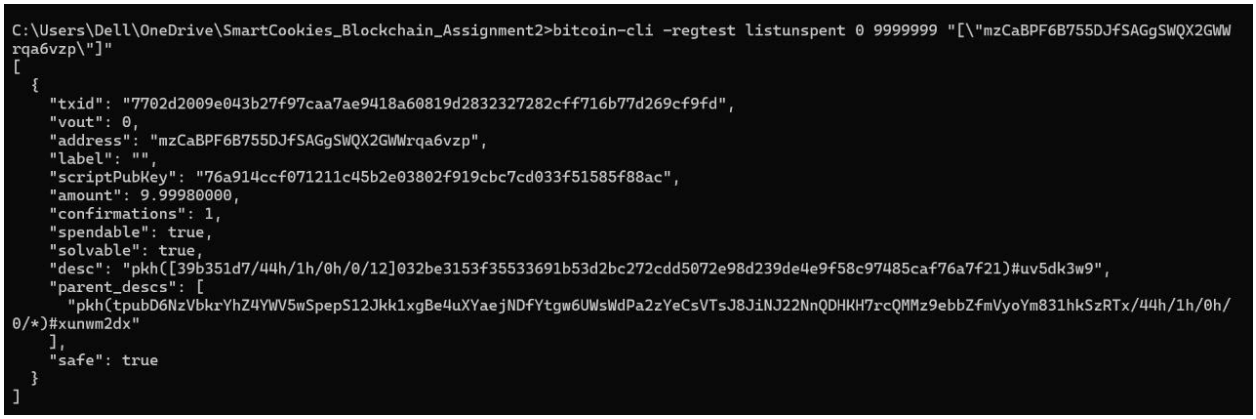
Similarly, the unspent transaction in B is now used for the transaction from B to C.



TX_id: 7702d2009e043b27f97caa7ae9418a60819d283232782cff716b77d26f17e6e7

The above unspent transaction in B is now used to send to C.

This leads to no unspent transactions left in B and C consists of the recently made transaction into its UTXO.



SCRIPTS OF ABOVE TRANSACTIONS

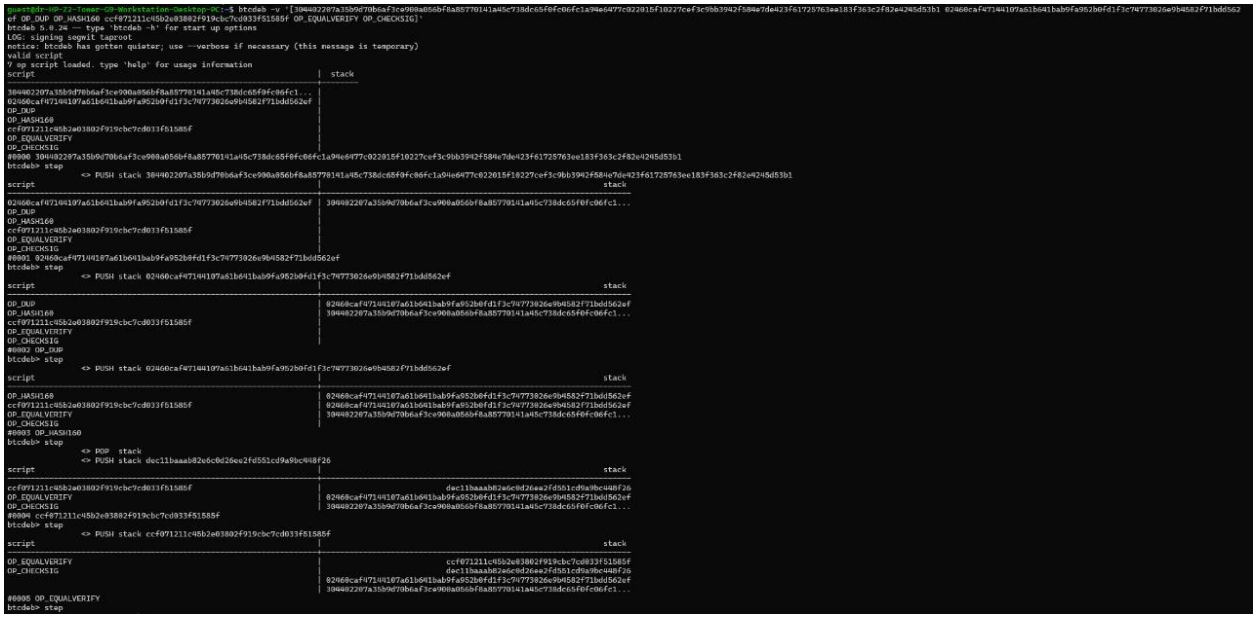
A->B TRANSACTION

B->C TRANSACTION

Debugging of above transactions

A->B transaction debugged

B -> C transaction debugged



Workflow: A → B → C Transaction Flow

The transaction workflow follows these steps:

1. **A → B Transaction (First Transaction)**
    - A sends Bitcoin to B using a P2PKH transaction.
    - The transaction generates a new UTXO (Unspent Transaction Output) assigned to B's address.
    - The transaction ID (txid) of A → B is recorded.
2. **B → C Transaction (Second Transaction)**
    - B uses the received UTXO from the A → B transaction as input.
    - B creates a new transaction sending funds to C, forming a B → C transaction.
    - The second transaction spends the UTXO from the first transaction.

Decoded Scripts for Both Transactions

Here are the decoded scripts for A → B and B → C transactions:

Unlocking Script (scriptSig)

asm

CopyEdit

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

- Signature proves ownership of the private key.
- Public key is used to derive the Bitcoin address.

Locking Script (scriptPubKey)

asm

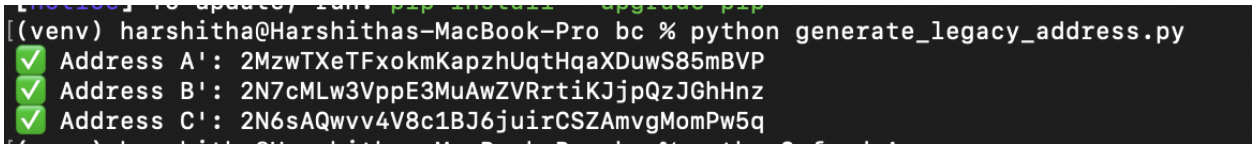
CopyEdit

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

- `OP_DUP`: Duplicates the top stack element (public key).
- `OP_HASH160`: Hashes the public key.
- `OP_EQUALVERIFY`: Verifies the hash matches the recipient's PubKeyHash.
- `OP_CHECKSIG`: Validates the signature.

P2SH TRANSACTIONS

Step 1: Generate Segwit address



Step 2: Fund to A

```
(venv) harshitha@Harshithas-MacBook-Pro bc % python3 fund_A.py
⛏ Mining 101 blocks...
Enter Address A': 2MzwTXeTFxokmKapzhUqtHqaXDuwS85mBVP
✅ Funded Address A' with TXID: e812b99641bc309f35655f8b387bd6dcf0238b066cc3dbd7055c2fbe5464d4be
(venv) harshitha@Harshithas-MacBook-Pro bc % python3 balance.py
Balance for 2MzwTXeTFxokmKapzhUqtHqaXDuwS85mBVP: 0 BTC
(venv) harshitha@Harshithas-MacBook-Pro bc % bitcoin-cli generatetoaddress 1 $(bitcoin-cli getnewaddress)
[
  "3ec9c03eb09cabe7a1dc833a2ba2d247f1a2026d671fe046cd2811483355fb72"
]
(venv) harshitha@Harshithas-MacBook-Pro bc % python3 balance.py
Balance for 2MzwTXeTFxokmKapzhUqtHqaXDuwS85mBVP: 1.0 BTC
(venv) harshitha@Harshithas-MacBook-Pro bc % python3 fund_A.py
⛏ Mining 101 blocks...
Enter Address A': 2MzwTXeTFxokmKapzhUqtHqaXDuwS85mBVP
✅ Funded Address A' with TXID: 62ba2419b4b3fd65eb79e4ae288244774f169dbc11b929ff1120d219780b3735
(venv) harshitha@Harshithas-MacBook-Pro bc % bitcoin-cli generatetoaddress 1 $(bitcoin-cli getnewaddress)
[
  "74c3d4f99e5734294f2223ce80d98b7b4cd4223cfe08b8f049525975a3692149"
]
(venv) harshitha@Harshithas-MacBook-Pro bc % python3 balance.py
Balance for 2MzwTXeTFxokmKapzhUqtHqaXDuwS85mBVP: 21.0 BTC
```

1st fund tx_id: e812b99641bc309f35655f8b387bd6dcf0238b066cc3dbd7055c2fbe5464d4be (LEFT UNSPENT)
2nd fund tx_id: 62ba2419b4b3fd65eb79e4ae288244774f169dbc11b929ff1120d219780b3735

Address A is funded twice, first with 1 BTC and then with 20 BTC, resulting in a total balance of 21 BTC.

//In the above transactions the address of A',B',C' are directly given in the code

Step 3: A to B transaction

```
(venv) harshitha@Harshithas-MacBook-Pro bc % python3 send_A_to_B.py
Transaction A' → B' broadcasted with txid: e9e1f127048e5875ca196bcd3559abadc100efcd7a435b0604aad3601a6fa99d
(venv) harshitha@Harshithas-MacBook-Pro bc % bitcoin-cli generatetoaddress 1 $(bitcoin-cli getnewaddress)
[
  "423ba084615bd0b597c7c15c59b33429f153ac25b73294ba3f7c2a803486c94a"
]
(venv) harshitha@Harshithas-MacBook-Pro bc % python3 balance.py
Balance for 2N7cMLw3VppE3MuAwZVRrtiKJjpQzJGhHnz: 19.9999 BTC
(venv) harshitha@Harshithas-MacBook-Pro bc % python3 balance.py
Balance for 2MzwTXeTFxokmKapzhUqtHqaXDuwS85mBVP: 1.0 BTC
```

Tx_id of A to B: e9e1f127048e5875ca196bcd3559abadc100efcd7a435b0604aad3601a6fa99d

For the transaction from A to B, the first unspent transaction output (UTXO) from A is used to send funds to B. Since the last received transaction was 20 BTC, it is utilized for the transfer. After deducting the transaction fee, 19.9999 BTC is sent to B, while the remaining 1 BTC stays in A as an unspent UTXO. This results in a final balance of **19.9999 BTC for B** and **1 BTC for A.**

```
)

# Sign transaction
signed_tx = rpc_connection.signrawtransactionwithwallet(raw_tx)
signed_hex = signed_tx['hex']

# Broadca   (variable) rpc_connection: Any
txid_B = rpc_connection.sendrawtransaction(signed_hex)
print(f"Transaction A' → B' broadcasted with txid: {txid_B}")
```

The signature of transaction is directly given in code for each of transaction.

Step 4: B to C transaction

```
(venv) harshitha@Harshithas-MacBook-Pro bc % python3 send_B_to_C.py
Transaction B' → C' broadcasted with txid: c49b72cf23d6c5ae6e1ea03f4f873c2315633d2201bbd2940fa8266eae725e6b
(venv) harshitha@Harshithas-MacBook-Pro bc % bitcoin-cli generatetoaddress 1 $(bitcoin-cli getnewaddress)
[
  "322299871739d84a44cbe23572cc2d8f85643b513cad726f4958d89f09468652"
]
(venv) harshitha@Harshithas-MacBook-Pro bc % python3 balance.py
Balance for 2N7cMLw3VppE3MuAwZVRrtiKJjpQzJGhHnz: 0 BTC
(venv) harshitha@Harshithas-MacBook-Pro bc % python3 balance.py
Balance for 2N6sAQwvv4V8c1BJ6juirCSZAmvgMomPw5q: 19.9998 BTC
```

Tx_id of B to C:c49b72cf23d6c5ae6e1ea03f4f873c2315633d2201bbd2940fa8266eae725e6b

For the transaction from B to C, B uses its only unspent UTXO of **19.999 BTC** to send funds to C. After deducting the transaction fee, **C receives 19.998 BTC**, and since B had only one UTXO, its balance becomes **0 BTC.**

```
# Create raw transaction
raw_tx = rpc_connection.createrawtransaction(
    [{"txid": txid, "vout": vout}],
    {address_C: float(amount) - tx_fee}  # Convert Decimal to float
)

# Sign transaction
signed_tx = rpc_connection.signrawtransactionwithwallet(raw_tx)
signed_hex = signed_tx['hex']

# Broadcast transaction
txid_C = rpc_connection.sendrawtransaction(signed_hex)
print(f"Transaction B' → C' broadcasted with txid: {txid_C}")
```

SCRIPT OF UNSPENT TRANSACTION IN FUND A


```
[
  {
    "txid": "e812b99641bc309f35655f8b387bd6dcf0238b066cc3dbd7055c2fbe5464d4be",
    "vout": 0,
    "address": "2MzwTXeTFxokmKapzhUqtHqaXDuwS85mBVP",
    "label": "",
    "redeemScript": "00141e72b689492e4dbc983e032a49edacac77a80c79",
    "scriptPubKey": "a9145464d27b4d72c0afc76836a8d39cb213422147ee87",
    "amount": 1.00000000,
    "confirmations": 105,
    "spendable": true,
    "solvable": true,
    "desc": "sh(wpkh([82b544a9/49h/1h/0h/0/9]0217ef2a894b41048f25dc29261f040fcdb89b25e0bee6ff8575ebb6b1902140b2))#z8pldsn3",
    "parent_descs": [
      "sh(wpkh(tpubD6NzVbkrYhZ4YhQqdoiH9k1Sv4wgCW6pVYRRMkY5VTDC1j3hG4bNmvreFJpV82wjghiFpkZsuBRhjk95iw4tgbH54ZuhZrENhHaPabgMz8W/49h/1h/0h/0/*))#3w4508vg"
    ],
    "safe": true
  }
]
```


SCRIPT OF TRANSACTION FROM A TO B


```
    },
    {
      "txid": "e9e1f127048e5875ca196bcd3559abadc100efcd7a435b0604aad3601a6fa99d",
      "hash": "6d6b626eec7179da8d9d36e804217853e891a00007f66ccb134d5706a3a367aa",
      "version": 2,
      "size": 215,
      "vsize": 134,
      "weight": 533,
      "locktime": 0,
      "vin": [
        {
          "txid": "62ba2419b4b3fd65eb79e4ae288244774f169dbc11b929ff1120d219780b3735",
          "vout": 0,
          "scriptSig": {
            "asm": "00141e72b689492e4dbc983e032a49edacac77a80c79",
            "hex": "1600141e72b689492e4dbc983e032a49edacac77a80c79"
          },
          "txinwitness": [
            "30440220242efc1e207d5de56d0c662531860afb3f419dcfc974f2027d2c71323fb592f6022037fcb96b9c55fbbbe76c3e0a72a1ffab9f297689b775fe822b80f88c3e510acb01",
            "0217ef2a894b41048f25dc29261f040fcdb89b25e0bee6ff8575ebb6b1902140b2"
          ],
          "sequence": 4294967293
        }
      ],
      "vout": [
        {
          "value": 19.99990000,
          "n": 0,
          "scriptPubKey": {
            "asm": "OP_HASH160 9d90a2fc19dafb4f67fdbede35c80732e82314eb OP_EQUAL",
            "desc": "addr(2N7cMLw3VppE3MuAwZVRrtiKJjpQzJGhHnz)#e6914sgj",
            "hex": "a9149d90a2fc19dafb4f67fdbede35c80732e82314eb87",
            "address": "2N7cMLw3VppE3MuAwZVRrtiKJjpQzJGhHnz",
            "type": "scripthash"
          }
        }
      ],
      "fee": 0.00010000,
      "hex": "02000000000101353370b7819d22011ff29b911bc9d164f7744b228aee479eb65fdb3b41924ba62000000001716001 41e72b689492e4dbc983e032a49edacac77a80c79fdffffff01f06c35770000000017a9149d90a2fc19d
afb4f67fdbede35c80732e82314eb8702473044022042efc1e207d5de56d0c662531860afb3f419dcfc974f2027d2c71323fb592f6022037fcb96b9c55fbbbe76c3e0a72a1ffab9f297689b775fe822b80f88c3e510acb01210217ef2a894b
41048f25dc29261f040fcdb89b25e0bee6ff8575ebb6b1902140b200000000"
    }
  ]
}
```


SCRIPT OF TRANSACTION FROM B TO C

```
    },
    {
      "txid": "c49b72cf23d6c5ae6e1ea03f4f873c2315633d2201bbd2940fa8266eae725e6b",
      "hash": "66c5092c36f428d4af44a1930748c168ce97f7c88418429da5475adf4b507eb5",
      "version": 2,
      "size": 215,
      "vsize": 134,
      "weight": 533,
      "locktime": 0,
      "vin": [
        {
          "txid": "e9e1f127048e5875ca196bcd3559abadc100efcd7a435b0604aad3601a6fa99d",
          "vout": 0,
          "scriptSig": {
            "asm": "00147edea8bb0c53dff08c730fa947acb59932f57fc1",
            "hex": "1600147edea8bb0c53dff08c730fa947acb59932f57fc1"
          },
          "txinwitness": [
            "3044022046b3d5a8fabd329a7df9f0e25ec4da9d8577017e89ea3afa28f3d6e538ed2c75022028d6fd7a2d48440e3ffe2868091ca90b69af278c5e3cd7999ac52c3efccba51901",
            "023bb268ae1f9826c1611eb77dd1a39c25b4671ded8abf3000244d3a48fa61eafa"
          ],
          "sequence": 4294967293
        }
      ],
      "vout": [
        {
          "value": 19.99980000,
          "n": 0,
          "scriptPubKey": {
            "asm": "OP_HASH160 9565a0316df697f77685706bf1c73933e2bfb079 OP_EQUAL",
            "desc": "addr(2N6sAQwvv4V8c1BJ6juirCSZAmvgMomPw5q)#3zwhqlm9",
            "hex": "a9149565a0316df697f77685706bf1c73933e2bfb07987",
            "address": "2N6sAQwvv4V8c1BJ6juirCSZAmvgMomPw5q",
            "type": "scripthash"
          }
        }
      ],
      "fee": 0.00010000,
      "hex": "020000000001019da96f1a60d3aa04065b437acdef00c1adab5935cd6b19ca75588e0427f1e1e90000000017160014 7edea8bb0c53dff08c730fa947acb59932f57fc1fdffffff01e0435770000000017a9149565a0316df697f77685706bf1c73933e2bfb07987024730440220462 046b3d5a8fabd329a7df9f0e25ec4da9d8577017e89ea3afa28f3d6e538ed2c75022028d6fd7a2d48440e3ffe2868091ca90b69af278c5e3cd7999ac52c3efccba5190121023bb268ae1f9826c1611eb77dd1a39c25b4671ded8abf3000244d3a48fa61eafa00000000"
    }
  ]
}
```


Debugging of the above transactions:

Format for debugging script

btcdeb '[<signature>] [<public_key>] <locking_script>'

For A to B transaction:

```
invalid script
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb '[30440220242efc1e207d5de56d0c662531860afb3f419dcfc974f2027d2c71323fb592f6022037fcb96b9c55fbbbe76c3e0a72a1ffab9f297689b775fe822b80f88c
3e510acb01] [0217ef2a894b41048f25dc29261f040fcdb89b25e0bee6ff8575ebb6b1902140b2] [00141e72b689492e4dbc983e032a49edacac77a80c79]'
'
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)
3 op script loaded. type `help` for usage information
script                                                          |  stack
----------------------------------------------------------------+-------
30440220242efc1e207d5de56d0c662531860afb3f419dcfc974f2027d2c713... |
210217ef2a894b41048f25dc29261f040fcdb89b25e0bee6ff8575ebb6b1902... |
1600141e72b689492e4dbc983e032a49edacac77a80c79                  |
#0000 30440220242efc1e207d5de56d0c662531860afb3f419dcfc974f2027d2c71323fb592f6022037fcb96b9c55fbbbe76c3e0a72a1ffab9f297689b775fe822b80f88c3e510acb01
btcdeb> step
                <> PUSH stack 30440220242efc1e207d5de56d0c662531860afb3f419dcfc974f2027d2c71323fb592f6022037fcb96b9c55fbbbe76c3e0a72a1ffab9f297689b775fe822b80f88c3e510acb01
script                                                          |                                                                 stack
----------------------------------------------------------------+-----------------------------------------------------------------------
210217ef2a894b41048f25dc29261f040fcdb89b25e0bee6ff8575ebb6b1902... | 30440220242efc1e207d5de56d0c662531860afb3f419dcfc974f2027d2c713...
1600141e72b689492e4dbc983e032a49edacac77a80c79                  |
#0001 210217ef2a894b41048f25dc29261f040fcdb89b25e0bee6ff8575ebb6b1902140b2
btcdeb> step
                <> PUSH stack 210217ef2a894b41048f25dc29261f040fcdb89b25e0bee6ff8575ebb6b1902140b2
script                                                          |                                                                 stack
----------------------------------------------------------------+-----------------------------------------------------------------------
1600141e72b689492e4dbc983e032a49edacac77a80c79                  | 210217ef2a894b41048f25dc29261f040fcdb89b25e0bee6ff8575ebb6b1902...
                                                                | 30440220242efc1e207d5de56d0c662531860afb3f419dcfc974f2027d2c713...

#0002 1600141e72b689492e4dbc983e032a49edacac77a80c79
btcdeb> step
                <> PUSH stack 1600141e72b689492e4dbc983e032a49edacac77a80c79
script                                                          |                                                                 stack
----------------------------------------------------------------+-----------------------------------------------------------------------
                                                                |                                 1600141e72b689492e4dbc983e032a49edacac77a80c79
                                                                | 210217ef2a894b41048f25dc29261f040fcdb89b25e0bee6ff8575ebb6b1902...
                                                                | 30440220242efc1e207d5de56d0c662531860afb3f419dcfc974f2027d2c713...
btcdeb> step
script                                                          |                                                                 stack
----------------------------------------------------------------+-----------------------------------------------------------------------
                                                                |                                 1600141e72b689492e4dbc983e032a49edacac77a80c79
                                                                | 210217ef2a894b41048f25dc29261f040fcdb89b25e0bee6ff8575ebb6b1902...
                                                                | 30440220242efc1e207d5de56d0c662531860afb3f419dcfc974f2027d2c713...
btcdeb> step
at end of script
btcdeb> stack
<01>    1600141e72b689492e4dbc983e032a49edacac77a80c79  (top)
<02>    210217ef2a894b41048f25dc29261f040fcdb89b25e0bee6ff8575ebb6b1902140b2
<03>    30440220242efc1e207d5de56d0c662531860afb3f419dcfc974f2027d2c71323fb592f6022037fcb96b9c55fbbbe76c3e0a72a1ffab9f297689b775fe822b80f88c3e510acb01
btcdeb>
```

For B to C transaction:

//the values in the above explanation are taken from the A to B transaction and can be modified for B to C transaction, the execution works as same way.

Unlocking Script Execution Steps

1. **The public key (0217ef2a894b...) is pushed onto the stack.**
2. **The signature (3044...acb01) is pushed onto the stack.**
3. **The scriptPubKey (locking script from the previous transaction) executes.**
4. **Validation steps:**
    - **The scriptSig is empty (P2WPKH stores unlocking data in the witness).**
    - **The witness stack provides:**
        - **public key**
        - **signature**
    - **The public key is hashed.**
    - **The computed hash must match the public key hash stored in the locking script.**
    - **The signature is verified using the public key.**

Locking Script Execution

- **This is a Pay-to-Script-Hash (P2SH) script.**
- **The scriptPubKey requires a redeem script that hashes to 9d90a2fc19dafb4f67fdbede35c80732e82314eb.**
- **The next transaction spending this output must provide:**
    - **The actual redeem script.**
    - **Data required by the redeem script.**

Input Script Validation (Witness-based P2WPKH)

Stack Execution

Step	Stack State	Operation
1	<Signature> <Public Key>	Initial witness stack
2	<Public Key Hash>	Compute hash of <Public Key>
3	<Expected Public Key Hash>	From scriptPubKey
4	TRUE	OP_EQUALVERIFY ensures match
5	TRUE	OP_CHECKSIG verifies signature

Output Script (P2SH) Locking Condition

- The locking script requires a redeem script with hash 9d90a2fc19dafb4f67fdbede35c80732e82314eb.
- The next transaction must provide:
    - The correct redeem script.
    - Any required signatures.

Legacy vs Segwit

1. Transaction Size Comparison

To compare transaction sizes, let's look at the estimated sizes of both transaction types:

- P2PKH (Legacy)
    - Input size: ~148 bytes per input
    - Output size: ~34 bytes per output
    - Total transaction size (1 input, 1 output): ~192-226 bytes
- P2SH-P2WPKH (SegWit)
    - Input size (before SegWit discount): ~91 bytes per input
    - SegWit discount applies to witness data, reducing effective size
    - Output size: ~32 bytes per output
    - Total transaction size (1 input, 1 output): ~140 bytes (effective vsize)

Thus, SegWit transactions are smaller due to witness data being stored separately and discounted when calculating fees.

2. Script Structure Comparison

P2PKH (Legacy)

P2PKH (Pay-to-Public-Key-Hash) follows this structure:

Locking Script (ScriptPubKey)

asm

OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

- **Locks the output to the hash of the recipient's public key.**

Unlocking Script (ScriptSig)

asm

CopyEdit

<Signature> <PublicKey>

- **Provides a valid signature and public key that match the PubKeyHash.**

P2SH-P2WPKH (SegWit)

P2SH-P2WPKH (Pay-to-Script-Hash, Wrapped SegWit) involves multiple scripts.

Locking Script (ScriptPubKey)

asm

CopyEdit

OP_HASH160 <RedeemScriptHash> OP_EQUAL

- **The redeem script hash corresponds to a SegWit redeem script.**

Redeem Script

asm

CopyEdit

0 <PubKeyHash>

- **This is the witness script, which defines the conditions for spending.**

Witness Data (txinwitness)

asm
CopyEdit
<Signature> <PublicKey>

- **Similar to P2PKH, but stored separately as witness data.**

3. Why SegWit Transactions Are Smaller

- **Witness Data Separation: The witness (signature) is removed from the main transaction structure and stored separately.**
- **Weight-based Fee Calculation: Bitcoin transactions are measured in weight units (WU) instead of raw bytes.**
    - **Legacy transactions: 1 byte = 4 WU**
    - **SegWit transactions: Witness data gets a 75% discount.**
- **Smaller vsize (virtual size): This results in lower fees because only non-witness data contributes fully to transaction size calculations.**

4. Benefits of SegWit Transactions

- **Lower Transaction Fees: Reduced virtual size means lower fees per transaction.**
- **Increased Block Capacity: More transactions can fit in each block due to the size reduction.**
- **Eliminates Malleability Issues: Fixes transaction malleability by separating witness data, which prevents modifications to signatures affecting transaction IDs.**
- **Lightning Network Compatibility: Enables off-chain transactions via Lightning Network, improving Bitcoin's scalability.**

Conclusion

- **P2PKH transactions are larger because the signature data is included inside the transaction.**
- **P2SH-P2WPKH transactions are smaller and more efficient due to SegWit's witness discount.**
- **SegWit improves Bitcoin's scalability, reduces fees, and enables advanced features like Lightning Network.**