

ASSIGNMENT - 2

INTRODUCTION TO BLOCKCHAIN

Team Members:

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 99999999 "[\"mfcvYJWpesCurDa4Sxe6RZL5PbwPChasa9\"]"
[ {
    "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(tpubD6NzVbkrYhZ4YWV5wSrepS12Jkk1xgBe4uXYaejNDFYtgw6UWsldPa2zYeCsVTsJ8JiNj22NnQDHKH7rcQMMz9ebbZfmVyoYm831hkSzRTx/44h/1h/0h/0/*#xunwm2dx"
    ],
    "safe": true
},
```

```
C:\Users\DELL\OneDrive\SmartCookies_Blockchain_Assignment2>python send_B_to_C.py
Amount_B: 9.99990000, Fee: 0.0001, Send Amount: 9.99980000
Raw Transaction (Unsigned): 020000000121701acc957558676648db007a001030d411e0248c4fdf8b216996ec28f98cf10000000000fdfffff01e07b9a3b000000001976a914ccf071211c45b2e03802f919cbc7cd033f51585f88ac00000000
Signed Transaction HEX: 020000000121701acc957558676648db007a001030d411e0248c4fdf8b216996ec28f98cf1000000000a4f7304402207a35b9d70b6af3ce900a056bf8a85770141a45c738dc65f0fc06fc1a94e6477c022015f10227cef3c9bb3942f584e7de423f61725763ee183f363c2f82e4245d53b1012102460caf47144107a61b641bab9fa952b0fd1f3c74773026e9b4582f71bdd562effdfffff01e07b9a3b00000001976a914ccf07121^-----rE7a-02800010-L-r-02222E5150E5000-00000000
Transaction successfully sent! TXID: 7702d2009e043b27f97caa7ae9418a60819d2832327282cff716b77d2C:\Users\DELL\OneDrive\SmartCookies_Blockchain_Assignment2>bitcoin-cli -regtest listunspent
[ ]
```

P2SH TRANSACTIONS

Step 1: Generate Segwit address

```
[root@DELL ~]# update, ran: pip install -U pip
(virtual) harshitha@Harshithas-MacBook-Pro bc % python generate_legacy_address.py
✓ Address A': 2MzwTXeTFxokmKapzhUqtHqaXDuwS85mBVP
✓ Address B': 2N7cMLw3VppE3MuAwZVRrtiKJjpQzJGhHnz
✓ Address C': 2N6sAQwvv4V8c1BJ6juirCSZAmvgMomPw5q
```

Step 2: Fund to A

```

✓ Address C : 2N05AQWVv4v8CIBJ8jdi1C3ZAmvgM0m-w3q
[(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)
[
  "3ec9c03eb09cab7a1dc833a2ba2d247f1a2026d671fe046cd2811483355fb72"
]
[(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

```

Balance for 2MzwTXeTFxokmKapzhUqtHqaXDuwS85mBVP: 21.0 BTC
[(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 2N7cMLw3VppE3MuAwZVRrtiKJjpQzJGhHz: 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**.

```

6
1
2 # Sign transaction
3 signed_tx = rpc_connection.signrawtransactionwithwallet(raw_tx)
4 signed_hex = signed_tx['hex']
5     (variable) rpc_connection: Any
6 # Broadcast transaction
7 txid_B = rpc_connection.sendrawtransaction(signed_hex)
8 print(f"Transaction A' → B' broadcasted with txid: {txid_B}")
9
0
1

```

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 2N7cMlw3VppE3MuAw2VRrtiKJjpQzJGhHz: 0 BTC
|(venv) harshitha@Harshithas-MacBook-Pro bc % python3 balance.py
Balance for 2N6sQwvv4V8c1BJ6juirCSZAmvgMomPw5q: 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": "e812b99641bc309f35655f8b387bd6dcff0238b066cc3dbd7055c2fbe5464d4be",  
    "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(tpubD6NzVbkzYhZ4YhQqdolH9k1Sv4wgCw6pYYRRMKy5VTDC1j3hG4bNmvreFJpV82wjghiFpkZsuBRhjk95iw4tgbH54ZuhZrENhHaPabgMzBW/49h/1h/0h/0/*))#3w4508vg"  
    ],  
    "safe": true  
  }  
]
```

SCRIPT OF TRANSACTION FROM A TO B

```
,  
  {  
    "txid": "e9e1f127048e5875ca196bcd3559abadc100efcd7a435b0604aad3601a6fa99d",  
    "hash": "6dd6b626eec7179da8d93ee804217853e891a0000766ccb134d5706a3a367aa",  
    "version": 2,  
    "size": 216,  
    "vsize": 134,  
    "weight": 533,  
    "locktime": 0,  
    "vin": [  
      {  
        "txid": "62ba2419b4b3fd65eb79e4ae288244774f169dbc11b929ff1120d219788b3735",  
        "vout": 0,  
        "scriptSig": {  
          "asm": "00141e72b689492e4dbc983e032a49edacac77a80c79",  
          "hex": "1600141e72b689492e4dbc983e032a49edacac77a80c79"},  
        "txinwitness": [  
          "364402202424efc1e207d5de56d0c662531e60af3f419dcfc974f2027d2c71323fb592f6022037fc96b9c55fbbe76c3e0a72affab9f297689b775fe822b80f88c3e510acb01",  
          "36217ef2a094b51048f25dc29261f840fcdb89b25e0bee6ff8575ebb6b1902140b2"  
        ],  
        "sequence": 4294967293  
      },  
      {"vout": [  
        {  
          "value": 19.99990000,  
          "n": 0,  
          "scriptPubKey": {  
            "asm": "OP_DUP OP_HASH160 9d992fc12dfb4f97fdbde35c80732e02314eb OP_EQUAL",  
            "desc": "#addr(2W75MLw3VppE3M AwZRrtikKJp0zJ0hHz) #e6914sgj",  
            "hex": "31919d992fc12dfb4f97fdbde35c80732e02314eb87",  
            "address": "2N7cMLw3VppE3MuAwZRrtikKJp0zJ0hHz",  
            "type": "scripthash"  
          }  
        }  
      ]},  
      {"fee": 0.00010000,  
      "hex": "0200000000010135370b7819d22011ff29b911bc9d164f77448228aee479eb65fdb3b41924ba620000000171600141e72b689492e4dbc983e032a49edacac77a80c79fdffff01f06c35770000000017a9149d90a2fc19dafb4f67fdbde35c80732e02314eb8724738440220242efc1e207d5de56d0c662531860af3f419dcfc974f2027d2c71323fb592f6022037fc96b9c55fbbe76c3e0a72affab9f297689b775fe822b80f88c3e510acb1210217ef2a894b41048f25dc29261f040fcdb89b25e0bee6ff8575ebb6b1902140b20000000"  
      }  
    ]},  
    {"vout": [  
      {  
        "value": 19.99990000,  
        "n": 0,  
        "scriptPubKey": {  
          "asm": "OP_DUP OP_HASH160 9d992fc12dfb4f97fdbde35c80732e02314eb OP_EQUAL",  
          "desc": "#addr(2W75MLw3VppE3M AwZRrtikKJp0zJ0hHz) #e6914sgj",  
          "hex": "31919d992fc12dfb4f97fdbde35c80732e02314eb87",  
          "address": "2N7cMLw3VppE3MuAwZRrtikKJp0zJ0hHz",  
          "type": "scripthash"  
        }  
      }  
    ]},  
    {"fee": 0.00010000,  
    "hex": "0200000000010135370b7819d22011ff29b911bc9d164f77448228aee479eb65fdb3b41924ba620000000171600141e72b689492e4dbc983e032a49edacac77a80c79fdffff01f06c35770000000017a9149d90a2fc19dafb4f67fdbde35c80732e02314eb8724738440220242efc1e207d5de56d0c662531860af3f419dcfc974f2027d2c71323fb592f6022037fc96b9c55fbbe76c3e0a72affab9f297689b775fe822b80f88c3e510acb1210217ef2a894b41048f25dc29261f040fcdb89b25e0bee6ff8575ebb6b1902140b20000000"  
  }  
]
```

SCRIPT OF TRANSACTION FROM B TO C

Debugging of the above transactions:

Format for debugging script

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

For A to B transaction:

```

invalid script
guest@DT-Tower-09-Workstation-Desktop:PC-> $ btcdbe [ '30440220242fc1e207d5de65ddc64253186fb3f419dcf747f28272dc71323fb592f6022037fc9b96b9c55fbbe76c3e9a72a1ffab9f297689b775fe822b80f88c79'
3e510acb01] <--> 30440220242fc1e207d5de65ddc64253186fb3f419dcf747f28272dc71323fb592f6022037fc9b96b9c55fbbe76c3e9a72a1ffab9f297689b775fe822b80f88c79

btcdbe 5.0.24 type 'btcdbe -h' for start up options
LOG: signing segwit taproot
note: btcdbe has gotten quieter; use --verbose if necessary (this message is temporary)
3 op script loaded. type 'help' for usage information
script | stack
-----|-----
30440220242fc1e207d5de65ddc64253186fb3f419dcf747f28272dc71323fb592f6022037fc9b96b9c55fbbe76c3e9a72a1ffab9f297689b775fe822b80f88c79
210217ef2a894b41848f75dc29261f04fcdb89b25e0be6ff8575eb6b1982... | 30440220242fc1e207d5de65ddc64253186fb3f419dcf747f28272dc71323fb592f6022037fc9b96b9c55fbbe76c3e9a72a1ffab9f297689b775fe822b80f88c79
#0008 30440220242fc1e207d5de65ddc64253186fb3f419dcf747f28272dc71323fb592f6022037fc9b96b9c55fbbe76c3e9a72a1ffab9f297689b775fe822b80f88c79
btcdbe step <-> PUSH stack 30440220242fc1e207d5de65ddc64253186fb3f419dcf747f28272dc71323fb592f6022037fc9b96b9c55fbbe76c3e9a72a1ffab9f297689b775fe822b80f88c79
script | stack
-----|-----
210217ef2a894b41848f75dc29261f04fcdb89b25e0be6ff8575eb6b1982... | 30440220242fc1e207d5de65ddc64253186fb3f419dcf747f2827dc713...
1600141e72b689492e4dbc983e832a49edacac77a80c79 | 210217ef2a894b41848f75dc29261f04fcdb89b25e0be6ff8575eb6b1982...
1600141e72b689492e4dbc983e832a49edacac77a80c79 | 30440220242fc1e207d5de65ddc64253186fb3f419dcf747f2827dc713...
btcdbe step <-> PUSH stack 210217ef2a894b41848f75dc29261f04fcdb89b25e0be6ff8575eb6b198210402
script | stack
-----|-----
1600141e72b689492e4dbc983e832a49edacac77a80c79 | 210217ef2a894b41848f75dc29261f04fcdb89b25e0be6ff8575eb6b1982...
1600141e72b689492e4dbc983e832a49edacac77a80c79 | 30440220242fc1e207d5de65ddc64253186fb3f419dcf747f2827dc713...
btcdbe step <-> PUSH stack 1600141e72b689492e4dbc983e832a49edacac77a80c79
script | stack
-----|-----
1600141e72b689492e4dbc983e832a49edacac77a80c79 | 1600141e72b689492e4dbc983e832a49edacac77a80c79
210217ef2a894b41848f75dc29261f04fcdb89b25e0be6ff8575eb6b1982... | 1600141e72b689492e4dbc983e832a49edacac77a80c79
30440220242fc1e207d5de65ddc64253186fb3f419dcf747f2827dc713...
btcdbe step
script | stack
-----|-----
1600141e72b689492e4dbc983e832a49edacac77a80c79 | 1600141e72b689492e4dbc983e832a49edacac77a80c79
210217ef2a894b41848f75dc29261f04fcdb89b25e0be6ff8575eb6b1982... | 210217ef2a894b41848f75dc29261f04fcdb89b25e0be6ff8575eb6b1982...
30440220242fc1e207d5de65ddc64253186fb3f419dcf747f2827dc713...
btcdbe step
at end of script
btcdbe stack
-----|-----
<0> 30440220242fc1e207d5de65ddc64253186fb3f419dcf747f2827dc71323fb592f6022037fc9b96b9c55fbbe76c3e9a72a1ffab9f297689b775fe822b80f88c79
<0> 30440220242fc1e207d5de65ddc64253186fb3f419dcf747f2827dc71323fb592f6022037fc9b96b9c55fbbe76c3e9a72a1ffab9f297689b775fe822b80f88c79
<0> 30440220242fc1e207d5de65ddc64253186fb3f419dcf747f2827dc71323fb592f6022037fc9b96b9c55fbbe76c3e9a72a1ffab9f297689b775fe822b80f88c79
btcdbe

```

For B to C transaction:

```
[guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC: ~]$ btcddeb '[3044022046b3d5a8fabd329a7df9f0e25ec4da9d8577017e89ea3afa28f3d6e538ed2c75022028d6fd7a2d48440e3ffe2868091ca90b69af278c5e3cd7999ac52c3e] fccb51901] [023bb268ae1f9826c1611eb77dd1a39c25b4671ded8abf3000244d3a48fa61eaf] [7edeaa8bb8c53dff08c730f947acb59932f57fc1'
btcddeb 5.0.24 -- type 'btcddeb -h' for start up options
L0: signing segwit taproot
notice: btcddeb has gotten quieter; use --verbose if necessary (this message is temporary)
3 on script loaded. type 'help' for usage information
script | stack
3844022046b3d5a8fabd329a7df9f0e25ec4da9d8577017e89ea3afa28f3d6e538ed2c75022028d6fd7a2d48440e3ffe2868091ca90b69af278c5e3cd7999ac52c3efccba51901
| stack
147edeaa8bb8c53dff08c730f947acb59932f57fc1
#0002 3044022046b3d5a8fabd329a7df9f0e25ec4da9d8577017e89ea3afa28f3d6e538ed2c75022028d6fd7a2d48440e3ffe2868091ca90b69af278c5e3cd7999ac52c3efccba51901
| stack
btcddeb> step <> PUSH stack 3044022046b3d5a8fabd329a7df9f0e25ec4da9d8577017e89ea3afa28f3d6e538ed2c75022028d6fd7a2d48440e3ffe2868091ca90b69af278c5e3cd7999ac52c3efccba51901
script | stack
21023bb268ae1f9826c1611eb77dd1a39c25b4671ded8abf3000244d3a48fa61eaf
147edeaa8bb8c53dff08c730f947acb59932f57fc1
#0002 21023bb268ae1f9826c1611eb77dd1a39c25b4671ded8abf3000244d3a48fa61eaf
| stack
btcddeb> step <> PUSH stack 21023bb268ae1f9826c1611eb77dd1a39c25b4671ded8abf3000244d3a48fa61eaf
script | stack
147edeaa8bb8c53dff08c730f947acb59932f57fc1
| stack
147edeaa8bb8c53dff08c730f947acb59932f57fc1
| 21023bb268ae1f9826c1611eb77dd1a39c25b4671ded8abf3000244d3a48fa6...
| 3044022046b3d5a8fabd329a7df9f0e25ec4da9d8577017e89ea3afa28f3d6e...
| stack
btcddeb> step <> PUSH stack 147edeaa8bb8c53dff08c730f947acb59932f57fc1
script | stack
147edeaa8bb8c53dff08c730f947acb59932f57fc1
| 21023bb268ae1f9826c1611eb77dd1a39c25b4671ded8abf3000244d3a48fa6...
| 3044022046b3d5a8fabd329a7df9f0e25ec4da9d8577017e89ea3afa28f3d6e...
| stack
btcddeb> step
at end of script
btcddeb> stack
<01> 023bb268ae1f9826c1611eb77dd1a39c25b4671ded8abf3000244d3a48fa61eaf (top)
<02> 21023bb268ae1f9826c1611eb77dd1a39c25b4671ded8abf3000244d3a48fa61eaf
<03> 3044022046b3d5a8fabd329a7df9f0e25ec4da9d8577017e89ea3afa28f3d6e538ed2c75022028d6fd7a2d48440e3ffe2868091ca90b69af278c5e3cd7999ac52c3efccba51901
btcddeb>
```

//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:
 - o The **scriptSig** is empty (P2WPKH stores unlocking data in the witness).
 - o The **witness** stack provides:
 - **public key**
 - **signature**
 - o The public key is hashed.
 - o The computed hash must match the public key hash stored in the locking script.
 - o 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:
 - o The actual redeem script.
 - o 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 <code>scriptPubKey</code>
4	TRUE	<code>OP_EQUALVERIFY</code> ensures match
5	TRUE	<code>OP_CHECKSIG</code> 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.