Part 1Bitcoin Legacy (P2PKH) Transaction Report

1. Transaction Workflow

Step 1: Transaction from A to B

- Sender (Address A): mwBeyD4Td1qEtsUTvrNzypbd6GkV4U9NR9
- Receiver (Address B): mgUdzLweTc8DCW2ouVfCkVQmWLnZyYRMdK
- Transaction ID (TXID): 8fac6031c9d90a1881dac20cf19b2b4d607a825571524e117c080207b27737f6
- Blockhash: 441f87e79c696a2897d287a09cffed3dbb6262c86c901d07c8414426860115d9
- Block Confirmation: The transaction was mined and confirmed.

Step 2: Transaction from B to C

- Sender (Address B): mgUdzLweTc8DCW2ouVfCkVQmWLnZyYRMdK
- Receiver (Address C): mnu6FiX4wx97YzJpVPG9Moj46NcViXNtLP
- Transaction ID (TXID): 03b3ea81f3aa1a41c93546494cdc0ab8415b5f0e419dcd0a26c1fa3846807cb0
- UTXO Used: Output from transaction 8fac6031... was used as input.
- Blockhash: 6463dab24e25b51556f8d5ee22ce1d2bd26fc0842155792b77498fcbf426c992
- Block Confirmation: The transaction was mined and confirmed.

---

2. Decoded Scripts

Transaction A → B

ScriptPubKey (Locking Script - UTXO for B)

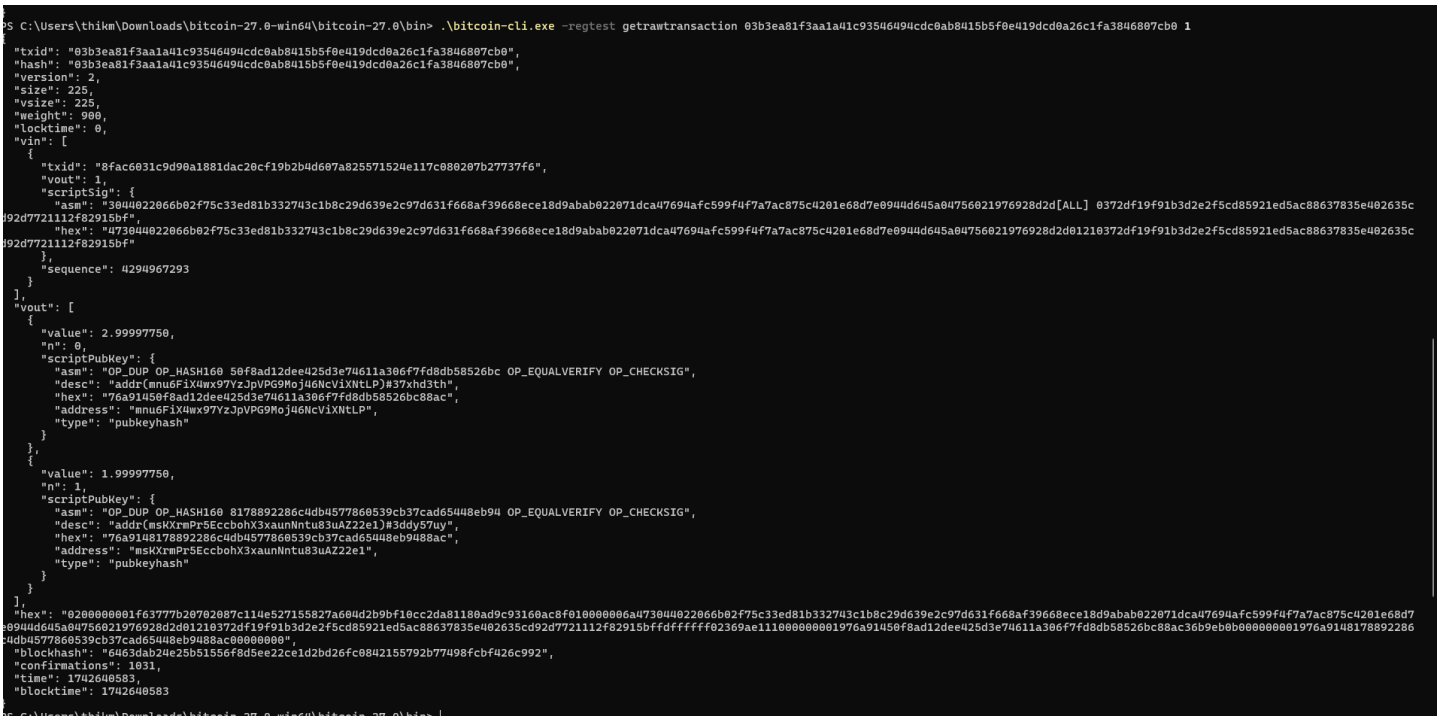

```
PS C:\Users\thikm> cd "C:\Users\thikm\Downloads\bitcoin-27.0-win64\bitcoin-27.0\bin"
PS C:\Users\thikm\Downloads\bitcoin-27.0-win64\bitcoin-27.0\bin> .\bitcoin-cli.exe -regtest getrawtransaction 8fac6031c9d90a1881dac20cf19b2b4d607a825571524e117c080207b27737f6 1
{
  "txid": "8fac6031c9d90a1881dac20cf19b2b4d607a825571524e117c080207b27737f6",
  "hash": "8fac6031c9d90a1881dac20cf19b2b4d607a825571524e117c080207b27737f6",
  "version": 2,
  "size": 225,
  "vsize": 225,
  "weight": 900,
  "locktime": 0,
  "vin": [
    {
      "txid": "4225914dccadabfbc4b54fcb19e5eddbcca04a02ceb231806c3b7da7973dda7a",
      "vout": 0,
      "scriptSig": {
        "asm": "30440220731 3d5938896499f6bd330f032d2ebc30ac1e1c9a838e91af0d29c6255f3029e02205b8c8835b4a4ad0d8b6ae6a0d8ccaac43cae2a275a8121633c7ac15901b47569[ALL] 036998df0cb71cee76e1c0397ddf0659ca8e136458db9895890b00715fd3741d44",
        "hex": "473044022073 13d5938896499f6bd330f032d2ebc30ac1e1c9a838e91af0d29c6255f3029e02205b8c8835b4a4ad0d8b6ae6a0d8ccaac43cae2a275a8121633c7ac15901b475690121036998df0cb71cee76e1c0397ddf0659ca8e136458db9895890b00715fd3741d44"
      },
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 5.00000000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 abdba5abcc890e2bcff41bff486609175d4abc3d OP_EQUALVERIFY OP_CHECKSIG",
        "desc": "addr(mwBeyD4Td1qEtsUTvrNzypbd6GkV4U9NR9)#zn72qxaa",
        "hex": "76a914abdba5abcc890e2bcff41bff486609175d4abc3d88ac",
        "address": "mwBeyD4Td1qEtsUTvrNzypbd6GkV4U9NR9",
        "type": "pubkeyhash"
      }
    },
    {
      "value": 4.99997750,
      "n": 1,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 0a88036a0b905cc324e5933465e60d1f8b7b10d9 OP_EQUALVERIFY OP_CHECKSIG",
        "desc": "addr(mgUdzLweTc8DCW2ouVfCkVQmWLnZyYRMdK)#z72d2e4x",
        "hex": "76a9140a88036a0b905cc324e5933465e60d1f8b7b10d988ac",
        "address": "mgUdzLweTc8DCW2ouVfCkVQmWLnZyYRMdK",
        "type": "pubkeyhash"
      }
    }
  ],
  "hex": "02000000017ada3d97a77d3b6c8031b2ce024aa0ccdbede519cb4fb5c4fbabadcc4d91254200000006a473044022073 13d5938896499f6bd330f032d2ebc30ac1e1c9a838e91af0d29c6255f3029e02205b8c8835b4a4ad0d8b6ae6a0d8ccaac43cae2a275a8121633c7ac15901b475690121036998df0cb71cee76e1c0397ddf0659ca8e136458db9895890b00715fd3741d44fdffffff020065cd1d000000001976a914abdba5abcc890e2bcff41bff486609175d4abc3d88ac365ccd1d000000001976a9140a88036a0b905cc324e5933465e60d1f8b7b10d988ac00000000",
  "blockhash": "441f87e79c696a2897d287a09cffed3dbb6262c86c901d07c8414426860115d9",
  "confirmations": 1032,
  "time": 1742640583,
  "blocktime": 1742640583
}
PS C:\Users\thikm\Downloads\bitcoin-27.0-win64\bitcoin-27.0\bin> .\bitcoin-cli.exe -regtest getrawtransaction 03b3ea81f3aa1a41c93546494cdc0ab8415b5f0e419dcd0a26c1fa3846807cb0 1
{
```


- Locks the output to address mgUdzLweTc8DCW2ouVfCkVQmWLnZyYRMdK.

ScriptSig (Unlocking Script - B spends A’s output)

Transaction B → C

ScriptPubKey (Locking Script - UTXO for C)



ScriptSig (Unlocking Script - C spends B's output)

- Signature and public key to unlock funds from B → C.

Structure of Challenge and Response Scripts & Transaction Validation

In Bitcoin's **Pay-to-PubKey-Hash (P2PKH)** transactions, the transaction validation process relies on **locking (challenge) scripts** and **unlocking (response) scripts**. These scripts ensure that only the rightful owner of a Bitcoin address can spend the funds.

1. Challenge Script (Locking Script) – ScriptPubKey

The **locking script** is embedded in the output (vout) of a transaction. It defines the conditions that must be met to spend the output.

OP_DUP OP_HASH160 <Public Key Hash> OP_EQUALVERIFY OP_CHECKSIG

- OP_DUP: Duplicates the public key.
- OP_HASH160: Hashes the public key.
- OP_EQUALVERIFY: Compares it to the locked address.
- OP_CHECKSIG: Verifies the transaction signature.

2. Response Script (Unlocking Script) – ScriptSig

- The **unlocking script** is included in the input (`vin`) of a transaction when a user wants to spend an output from a previous transaction.

Structure of ScriptSig (Unlocking Script)

<SIGNATURE> <PUBLIC_KEY>

- Signature (SIG): Proves ownership using the sender's private key.

- Public Key (PUBKEY): Provides the necessary key for validation.

3. Validation Process

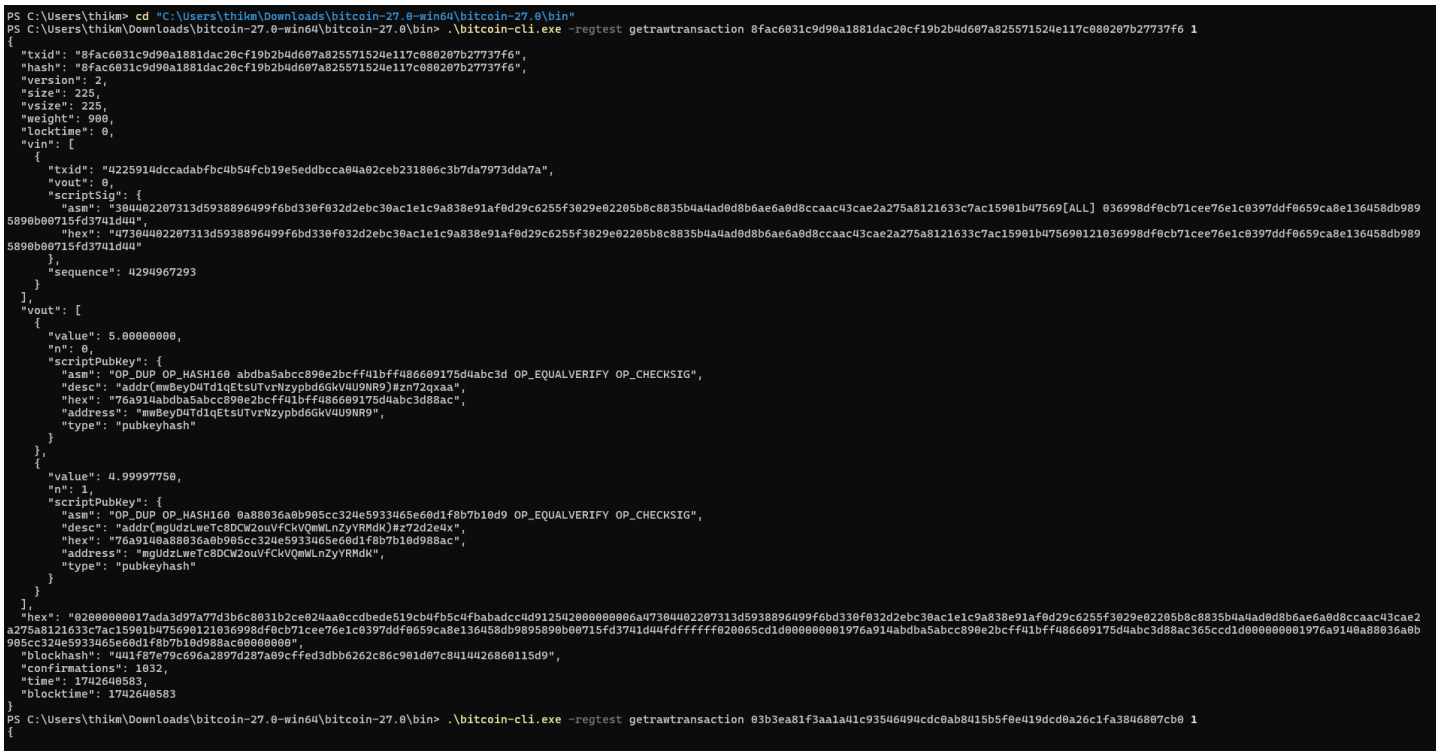
When a node verifies a transaction, it executes **ScriptSig + ScriptPubKey together** as a single script.

Step-by-Step Execution

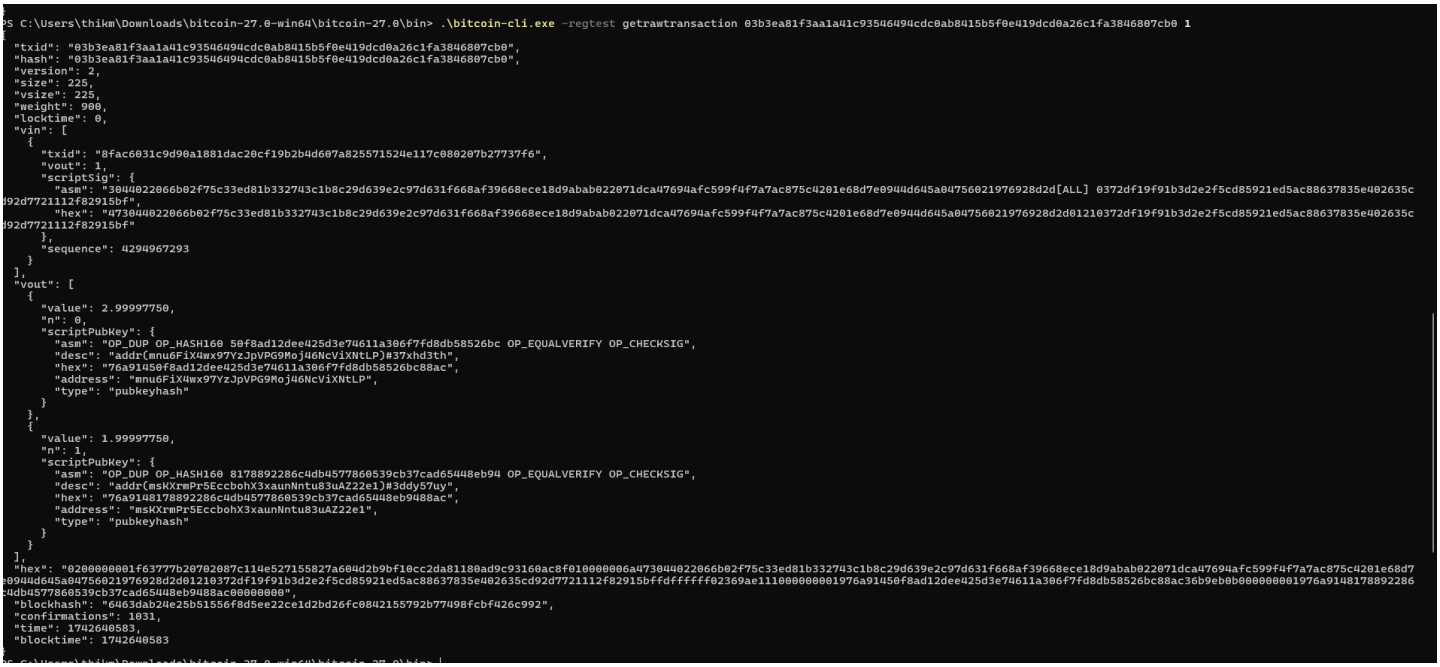
1. **Stack Initialization**
    - The unlocking script (ScriptSig) pushes the **signature** and **public key** onto the stack.
2. **ScriptPubKey Execution**
    - OP_DUP: Duplicates the public key.
    - OP_HASH160: Computes the hash of the public key.
    - OP_EQUALVERIFY: Compares the computed hash with the stored public key hash.
    - OP_CHECKSIG: Uses the public key to verify the provided signature.

If All Conditions Are Met, the Transaction is Valid! ✅

- If any step fails, the transaction is **invalid** and will be rejected by the Bitcoin network



```
PS C:\Users\thikm> cd "C:\Users\thikm\Downloads\bitcoin-27.0-win64\bitcoin-27.0\bin"
PS C:\Users\thikm\Downloads\bitcoin-27.0-win64\bitcoin-27.0\bin> .\bitcoin-cli.exe -regtest getrawtransaction 8fac6031c9d90a1881dac20cf19b2b4d607a825571524e117c080207b27737f6 1
{
  "txid": "8fac6031c9d90a1881dac20cf19b2b4d607a825571524e117c080207b27737f6",
  "hash": "8fac6031c9d90a1881dac20cf19b2b4d607a825571524e117c080207b27737f6",
  "version": 2,
  "size": 225,
  "vsize": 225,
  "weight": 900,
  "locktime": 0,
  "vin": [
    {
      "txid": "4225914dccadabfbc4b54fcb19e5eddbcca04a02ceb231806c3b7da7973dda7a",
      "vout": 0,
      "scriptSig": {
        "asm": "304402207313d5938896499f6bd330f032d2ebc30ac1e1c9a838e91af0d29c6255f3029e02205b8c8835b4a4ad0d8b6ae6a0d8ccaac43cae2a275a8121633c7ac15901b47569[ALL] 036998df0cb71cee76e1c0397ddf0659ca8e136458db9895890b00715fd3741d44",
        "hex": "47304402207313d5938896499f6bd330f032d2ebc30ac1e1c9a838e91af0d29c6255f3029e02205b8c8835b4a4ad0d8b6ae6a0d8ccaac43cae2a275a8121633c7ac15901b4756901210369 98df0cb71cee76e1c0397ddf0659ca8e136458db9895890b00715fd3741d44"
      },
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 5.00000000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 abdba5abcc890e2bcff41bff486609175d4abc3d OP_EQUALVERIFY OP_CHECKSIG",
        "desc": "addr(mwBeyD4Td1qEtsUTvrNzypbd6GkV4U9NR9)#zn72qxaa",
        "hex": "76a914abdba5abcc890e2bcff41bff486609175d4abc3d88ac",
        "address": "mwBeyD4Td1qEtsUTvrNzypbd6GkV4U9NR9",
        "type": "pubkeyhash"
      }
    },
    {
      "value": 4.99997750,
      "n": 1,
      "scriptPubKey": {
        "asm": "OP_DUP OP_HASH160 0a88036a0b905cc324e5933465e60d1f8b7b10d9 OP_EQUALVERIFY OP_CHECKSIG",
        "desc": "addr(mgUdzLweTc8DCW2ouVfCkVQmWLnZyYRMdK)#z72d2e4x",
        "hex": "76a9140a88036a0b905cc324e5933465e60d1f8b7b10d988ac",
        "address": "mgUdzLweTc8DCW2ouVfCkVQmWLnZyYRMdK",
        "type": "pubkeyhash"
      }
    }
  ],
  "hex": "02000000017ada3d97a77d3b6c8031b2ce024aa0ccdbede519cb4fb5c4fbabadcc4d912542000000006a47304402207313d5938896499f6bd330f032d2ebc30ac1e1c9a838e91af0d29c6255f3029e02205b8c8835b4a4ad0d8b6ae6a0d8ccaac43cae2a275a8121633c7ac15901b4756901210369 98df0cb71cee76e1c0397ddf0659ca8e136458db9895890b00715fd3741d44fdffffff020065cd1d000000001976a914abdba5abcc890e2bcff41bff486609175d4abc3d88ac365ccd1d000000001976a9140a88036a0b905cc324e5933465e60d1f8b7b10d988ac00000000",
  "blockhash": "441f87e79c696a2897d287a09cffed3dbb6262c86c901d07c8414426860115d9",
  "confirmations": 1032,
  "time": 1742640583,
  "blocktime": 1742640583
}
PS C:\Users\thikm\Downloads\bitcoin-27.0-win64\bitcoin-27.0\bin> .\bitcoin-cli.exe -regtest getrawtransaction 03b3ea81f3aa1a41c93546494cdc0ab8415b5f0e419dcd0a26c1fa3846807cb0 1
{
```



Part 2: Bitcoin Legacy (P2PKH) Transaction Report

1. Transaction Workflow

Step 1: Transaction from A to B

- Sender (Address A): mx4Su2Fbw1mULJkn2PU2Yi4MjhGxe9emng
- Receiver (Address B): mzt87PAYLB9cCRDCjxkhtBavg6EjzZRgBH
- Transaction ID (txid): 8fac6031c9d90a1881dac20cf19b2b4d607a825571524e117c080207b27737f6
- Block Confirmation: Mined and confirmed.

Step 2: Transaction from B to C

- Sender (Address B): mzt87PAYLB9cCRDCjxkhtBavg6EjzZRgBH
- Receiver (Address C): mrgdFVNReAa2YjUBauNeQMSCVm2rHcbJfa
- Transaction ID (txid): 03b3ea81f3aa1a41c93546494cdc0ab8415b5f0e419dcd0a26c1fa3846807cb0
- UTXO Used: The output from 8fac6031c9d90a1881dac20cf19b2b4d607a825571524e117c080207b27737f6 was used as input.
- Block Confirmation: Mined and confirmed.

2. Decoded Scripts

Transaction A → B

ScriptPubKey (Locking Script - UTXO for B

OP_DUP OP_HASH160 abdba5abcc890e2bcff41bff486609175d4abc3d OP_EQUALVERIFY OP_CHECKSIG

Locks the output to the public key hash of **B**

Decoded ScriptPubKey

{

"asm": "OP_HASH160 5e6a0e1040474ca4c69b87a2e5720258494a1ffc OP_EQUAL",

"desc": "addr(2N1rSZ9CKXDeBTT1QVN11uPwMhs7SFrxQk7)#xzwuzdsp",

"address": "2N1rSZ9CKXDeBTT1QVN11uPwMhs7SFrxQk7",

"type": "scripthash"

}

Transaction B → C

ScriptPubKey (Locking Script - UTXO for C)

OP_DUP OP_HASH160 50f8ad12dee425d3e74611a306f7fd8db58526bc OP_EQUALVERIFY OP_CHECKSIG

Locks the output to the public key hash of **C**

3. Challenge and Response Script Structure

Challenge Script (ScriptPubKey)

OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

Explanation:

1. **OP_DUP**: Duplicates the public key on the stack.
2. **OP_HASH160**: Hashes the public key.
3. **OP_EQUALVERIFY**: Verifies if the provided hash matches the stored hash.
4. **OP_CHECKSIG**: Verifies the digital signature using the public key.

Response Script (ScriptSig)

<SIG> <PUBKEY>

Explanation:

1. **Signature (SIG)**: Generated using the sender's private key.
2. **Public Key (PUBKEY)**: Provided to prove ownership.

Validation Process

- **Bitcoin nodes execute**: ScriptSig + ScriptPubKey
- **The public key is checked**: If it matches the hash stored in the UTXO.
- **The digital signature is verified**: Ensuring only the rightful owner can spend the UTXO.
- **If all conditions are met, the transaction is valid** and gets confirmed.

```
PS C:\Users\thikm\Downloads\bitcoin-27.0-win64\bitcoin-27.0\bin> .\bitcoin-cli.exe -regtest getrawtransaction 00e377d54ff6edcb269ccfdf39e06b0d144895d817eec4068ea596858af93087 1
{
  "txid": "00e377d54ff6edcb269ccfdf39e06b0d144895d817eec4068ea596858af93087",
  "hash": "250551441f8ceac474e386d9cc22a4a781cfd032cabbe5ccd644bbaf6c56ac8c",
  "version": 2,
  "size": 247,
  "vsize": 166,
  "weight": 661,
  "locktime": 0,
  "vin": [
    {
      "txid": "1b6d1c0fda42449e43989cab2a09e2cc7dd2f14f487ac2e20f371839193105e2",
      "vout": 0,
      "scriptSig": {
        "asm": "0014900ae9f5ca02461e975183ed19c1adb9b979490ba6",
        "hex": "1600149ae9f5ca02461e975183ed19c1adb9b979490ba6"
      },
      "txinwitness": [
        "304402204777 8ec461ce256a53241610dfd4581dce44feb219723c07cd6402a11780fb5802207c91009e436cf83b187e4ae9863da33361cce65899fe5774517af6af1009d46c01",
        "02849e6615aad11a77ee0c2445484de1e70ddabcbaa1914fb8c2d6d6b1b6dcbd9d"
      ],
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 5.00000000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_HASH160 53e8dc7c6e7ce42451e67ce03e59c70b087e6ec3 OP_EQUAL",
        "desc": "addr(2Mztu2h2AT2sy5Y4H8u1HWaQrUPiS2t2Qxx)#8nnu8qd9",
        "hex": "a91453e8dc7c6e7ce42451e67ce03e59c70b087e6ec387",
        "address": "2Mztu2h2AT2sy5Y4H8u1HWaQrUPiS2t2Qxx",
        "type": "scripthash"
      }
    },
    {
      "value": 4.99998340,
      "n": 1,
      "scriptPubKey": {
        "asm": "OP_HASH160 5e6a0e1040474ca4c69b87a2e5720258494a1ffc OP_EQUAL",
        "desc": "addr(2N1rSZ9CKXDeBTT1QVN11uPwMhs7SFrxQk7)#xzwuzdsp",
        "hex": "a9145e6a0e1040474ca4c69b87a2e5720258494a1ffc87",
        "address": "2N1rSZ9CKXDeBTT1QVN11uPwMhs7SFrxQk7",
        "type": "scripthash"
      }
    }
  ],
  "hex": "0200000000101e20531193918370fe2c27a484ff1d27dcce2092aab9c98439e4442da0f1c6d1b0000000017160014 9ae9f5ca02461e975183ed19c1adb9b979490ba6fdffffff020065cd1d0000000017a91453e8dc7c6e7ce42451e67ce03e59c70b087e6ec387845ecd1d0000000017a9145e6a0e1040474ca4c69b87a2e5720258494a1ffc8702473044022047778ec461ce256a53241610dfd4581dce44feb219723c07cd6402a11780fb5802207c91009e436cf83b187e4ae9863da33361cce65899fe5774517af6af1009d46c012102849e6615aad11a77ee0c2445484de1e70ddabcbaa1914fb8c2d6d6b1b6dcbd9d00000000",
  "blockhash": "71c091813a289dcc3829463b36b4174e00d05631e388ec5f384547c36d753062",
  "confirmations": 106,
  "time": 1742732059,
  "blocktime": 1742732059
```

```
PS C:\Users\thikm\Downloads\bitcoin-27.0-win64\bitcoin-27.0\bin> .\bitcoin-cli.exe -regtest getrawtransaction 48c6abf2d03ad400dcd7037df86b958a41ad4726d65fdd85db4a88b52d4b6e81 1
{
  "txid": "48c6abf2d03ad400dcd7037df86b958a41ad4726d65fdd85db4a88b52d4b6e81",
  "hash": "fbd914b5d22711287d79dc1274ae2803f2f594505d4d81a3966d3b30c47c6e50",
  "version": 2,
  "size": 247,
  "vsize": 166,
  "weight": 661,
  "locktime": 0,
  "vin": [
    {
      "txid": "00e377d54ff6edcb269ccfdf39e06b0d144895d817eec4068ea596858af93087",
      "vout": 1,
      "scriptSig": {
        "asm": "001467560 4b5b0d197d682ef9284772c8651344e0b88",
        "hex": "160014675604b5b0d197d682ef9284772c8651344e0b88"
      },
      "txinwitness": [
        "304402203f1e2726d218209dbf7835fb3335f68bc01fea40d25cb959873b01ed165054f1022025a429d6fe5f8e43240145a70d08fe3e9e22f785991b56ed78fb2103805243e301",
        "02e57385c570b3bbbcd96015024ed15b15b138ee2b2d1f4573dca71728d830a3fc"
      ],
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 2.99998340,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_HASH160 dd8df43894f0b1ab0fc977cf9123caa7fcb7d060 OP_EQUAL",
        "desc": "addr(2NDShNpCEG1TfLh8xh6eoYr4asrZMJYfanc)#wv98jlhv",
        "hex": "a914dd8df43894f0b1ab0fc977cf9123caa7fcb7d06087",
        "address": "2NDShNpCEG1TfLh8xh6eoYr4asrZMJYfanc",
        "type": "scripthash"
      }
    },
    {
      "value": 1.99998340,
      "n": 1,
      "scriptPubKey": {
        "asm": "OP_HASH160 931ba312f15d2f7489837add12d35a16b55f52b1 OP_EQUAL",
        "desc": "addr(2N6f4Rje87WkNCEdBJtU4nx2XepZSHKywfW)#fvwrf2cp",
        "hex": "a914931ba312f15d2f7489837add12d35a16b55f52b187",
        "address": "2N6f4Rje87WkNCEdBJtU4nx2XepZSHKywfW",
        "type": "scripthash"
      }
    }
  ],
  "hex": "020000000010187 30f98a8596a58e06c4ee17d8954 8140d6be039dfcf9c26cbedf64fd577e3000100000017160014675604b5b0d197d682ef9284772c86513 44e0b88fdffffff02849ce1100000000017a914dd8df43894f0b1ab0fc977cf9123caa7fcb7d0608784bbeb0b0000000017a914931ba312f15d2f7489837add12d35a16b55f52b187024730440220 3f1e2726d218209dbf7835fb3335f68bc01fea40d25cb959873b01ed165054f1022025a429d6fe5f8e43240145a70d08fe3e9e22f785991b56ed78fb2103805243e30121 02e57385c570b3bbbcd96015024ed15b15b138ee2b2d1f4573dca71728d830a3fc00000000",
  "blockhash": "030be47d302ff2c4d3742af72988de98aa00392c012f2860bd8cfad8eef95c87",
  "confirmations": 105,
  "time": 1742732059,
  "blocktime": 1742732059
}
```

Decode script from A->B and B->c

```
PS C:\Users\thikm\Downloads\bitcoin-27.0-win64\bitcoin-27.0\bin> .\bitcoin-cli.exe -regtest decodescript a9145e6a0e1040474ca4c69b87a2e5720258494a1ffc87
{
  "asm": "OP_HASH160 5e6a0e1040474ca4c69b87a2e5720258494a1ffc OP_EQUAL",
  "desc": "addr(2N1rSZ9CKXDeBTT1QVN11uPwMhs7SFrxQk7)#xzwuzdsp",
  "address": "2N1rSZ9CKXDeBTT1QVN11uPwMhs7SFrxQk7",
  "type": "scripthash"
}
PS C:\Users\thikm\Downloads\bitcoin-27.0-win64\bitcoin-27.0\bin> .\bitcoin-cli.exe -regtest decodescript a914dd8df43894f0b1ab0fc977cf9123caa7fcb7d06087
{
  "asm": "OP_HASH160 dd8df43894f0b1ab0fc977cf9123caa7fcb7d060 OP_EQUAL",
  "desc": "addr(2NDShNpCEG1TfLh8xh6eoYr4asrZMJYfanc)#wv98jlhv",
  "address": "2NDShNpCEG1TfLh8xh6eoYr4asrZMJYfanc",
  "type": "scripthash"
}
```

Steps of Bitcoin Debugger Executing Challenge and Response Script

Step 1: Open the Bitcoin Script Debugger

Step 2: Input the Unlocking (ScriptSig) and Locking (ScriptPubKey) Scripts

For P2PKH (Legacy) Transaction

For P2SH-SegWit Transaction

Step 3: Execute the Scripts

Step 4: Validate in Bitcoin Mempool/Block Explorer

Part 3: Analysis and Explanation

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

1.Transaction Size Comparison

Transaction Type	Size (bytes)	vSize (vbytes)	Weight (WU)
P2PKH (Legacy	225 bytes	225 vB	900 WU
P2SH-P2WPKH (SegWit)	247 bytes	166 vB	661 WU

Observations:

- SegWit transactions have a lower vSize and weight compared to Legacy transactions.
- Even though the total byte size of SegWit transactions is slightly larger, their vSize (virtual size) is smaller.
- Weight is reduced in SegWit transactions due to the witness data being separated

Script Structure Comparison

- P2PKH (Legacy) Transaction Structure

ScriptSig (Unlocking Script)

<Signature> <Public Key>

ScriptPubKey (Locking Script)

OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

 Challenge: Public key hash is locked.

 Response: The spender provides a valid public key and a digital signature.

- P2SH-P2WPKH (SegWit) Transaction Structure

ScriptSig (Unlocking Script)

0014 <20-byte Public Key Hash>

Witness (Separate from ScriptSig

<Signature> <Public Key>

ScriptPubKey (Locking Script)

OP_HASH160 <Redeem Script Hash> OP_EQUAL

Challenge**:** Redeem script is stored in scriptPubKey (P2SH wrapper).

Response**:** The spender provides the witness (Signature + Public Key)

Why SegWit Transactions Are Smaller & Their Benefits

- Why are SegWit Transactions Smaller**?**

1. Witness Data is Separated:
    - In SegWit, the signature (witness data) is moved outside the transaction structure, reducing the transaction's effective size.
2. Lower vSize Calculation:
    - The witness data is discounted by a factor of 4, making transactions more compact.
3. No Signature Malleability:
    - SegWit prevents modifications to the signature, making transactions **more secure**.

- Benefits of SegWit Transactions

Lower Transaction Fees: SegWit transactions occupy less block space, reducing the fee per byte.
Increased Block Capacity: More transactions can fit into a block, improving network efficiency.
Fixes Malleability Issues: Since the witness data is separate, it prevents attacks where transaction IDs change due to signature modifications.
Enables Second Layer Solutions (e.g., Lightning Network): Lightning Network relies on SegWit for off-chain transactions.