Bitcoin Scripting Report

CS 216: Introduction to Blockchain
Assignment 2

Team Members->

Arihant Jain - 230001009

Bhuva Vasudha - 230002017

Tanishq Godha - 230001074

Vedant Jain - 230008038

---

1. Introduction

The purpose of this assignment is to understand Bitcoin transactions using Legacy (P2PKH) and SegWit (P2SH-P2WPKH) address formats. We implement scripts to create, sign, and analyze transactions in both formats and compare their efficiency.

---

2. Legacy (P2PKH) Transactions

Overview:

- **Funding Address A:**
    - **Address:** `mh2m5vTZaX9T9AGHYtBCAPqRuXLnNvLV4X`
    - **Funded Amount:** 0.01 BTC
- **Transaction from A to B:**
    - **TXID:** `509e43e60972daa74dedb17108251dd9055fbaeb79d8d230c8ef17db8344b448`
    - **B's Address:** `mwbtAq1kFJdieQFh4bHJQQW4mofu4HLBjA`

- **Transaction from B to C:**
    - **TXID:** `f3b6e3e25b8c16100f41eb954803aad202cabb3b52d463456090f93d5defc088`
    - **C's Address:** `mn5RDGXhXrgyLEjMaaKscm9Y3tQa8DNwYf`

Scripts:

Transaction A → B:


```
{
 "txid": "509e43e60972daa74dedb17108251dd9055fbaeb79d8d230c8ef17db8344b448",
 "vin": [
  {
   "txid": "cacb74def842f8836d3e8da5720078883dfa71f1b0064d037711a5b3895cc738",
   "scriptSig": {
    "asm": "30440220477dcedea84384116bfaadc7b14fb84ad217bdb3de4fa9bc19cd5c81653da8fc0220742bf35997704df6d3f07a677521f10be4891e122b37277937c647e45d747aaa[ALL] 0323a6194fe7638fddcd961444a3f84643df9a2f101791c000e96e0cdd83af8cf0"
   }
  }
 ],
 "vout": [
  {
   "scriptPubKey": {
    "asm": "OP_DUP OP_HASH160 b070a63a49a02fa788ae540294531967b97b6273 OP_EQUALVERIFY OP_CHECKSIG",
    "address": "mwbtAq1kFJdieQFh4bHJQQW4mofu4HLBjA"
```

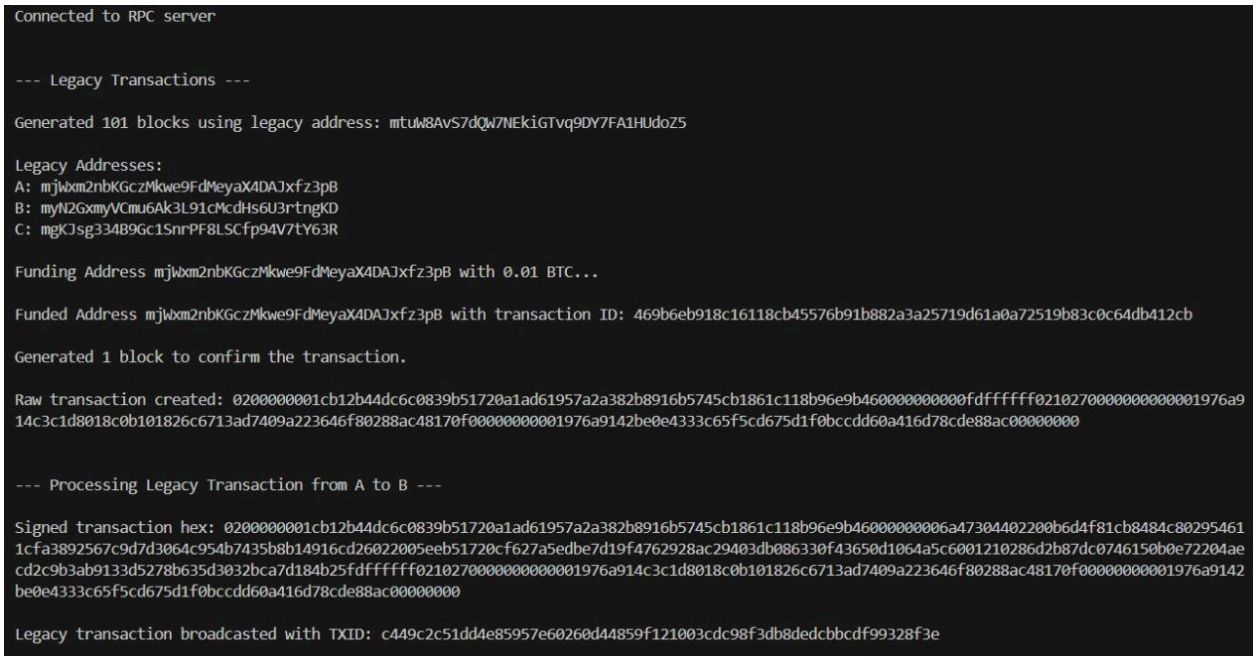
```
    }
   }
  ]
}
```


Transaction B → C:


```
 {
  "txid": "f3b6e3e25b8c16100f41eb954803aad202cabb3b52d463456090f93d5defc088",
  "vin": [
   {
    "txid": "509e43e60972daa74dedb17108251dd9055fbaeb79d8d230c8ef17db8344b448",
    "scriptSig": {
     "asm":
"304402203cbfc9e4ef49b8355ef38554e98ab1b4297ca767c965db58b8139bb1efb226da02207b
18f85fdf7524af4d116409bad23bd0c8e3f211d8154da0fef45e389ac45d18[ALL]
034aca719626c4e7816a5c31fb0f2bd5277a0997daa439d8253185a554298a5fe7"
    }
   }
  ],
  "vout": [
   {
    "scriptPubKey": {
     "asm": "OP_DUP OP_HASH160 47f488fa65e16c20b11b6eb73d11d53fbb620212
OP_EQUALVERIFY OP_CHECKSIG",
     "address": "mn5RDGXhXrgyLEjMaaKscm9Y3tQa8DNwYf"
    }
   }
```

```
]
}
```

Output Screenshots containing decoded scripts:



```
Connected to RPC server


--- Legacy Transactions ---

Generated 101 blocks using legacy address: mtuW8AvS7dQW7NEkiGTvq9DY7FA1HUdoZ5

Legacy Addresses:
A: mjWxm2nbKGczMkwe9FdMeyaX4DAJxfz3pB
B: myN2GxmyVCmu6Ak3L91cMcdHs6U3rtngKD
C: mgKJsg334B9Gc1SnrPF8LSCfp94V7tY63R

Funding Address mjWxm2nbKGczMkwe9FdMeyaX4DAJxfz3pB with 0.01 BTC...

Funded Address mjWxm2nbKGczMkwe9FdMeyaX4DAJxfz3pB with transaction ID: 469b6eb918c16118cb45576b91b882a3a25719d61a0a72519b83c0c64db412cb

Generated 1 block to confirm the transaction.

Raw transaction created: 0200000001cb12b44dc6c0839b51720a1ad61957a2a382b8916b5745cb1861c118b96e9b460000000000fdffffff021027000000000000001976a9
14c3c1d8018c0b101826c6713ad7409a223646f80288ac48170f00000000001976a9142be0e4333c65f5cd675d1f0bccdd60a416d78cde88ac00000000


--- Processing Legacy Transaction from A to B ---

Signed transaction hex: 0200000001cb12b44dc6c0839b51720a1ad61957a2a382b8916b5745cb1861c118b96e9b4600000000064730440220 0b6d4f81cb8484c802954611
cfa3892567c9d7d3064c954b7435b8b14916cd26022005eeb51720cf627a5edbe7d19f4762928ac29403db086330f43650d1064a5c6001210286d2b87dc0746150b0e72204ae
cd2c9b3ab9133d5278b635d3032bca7d184b25fdffffff021027000000000000001976a914c3c1d8018c0b101826c6713ad7409a223646f80288ac48170f00000000001976a9142
be0e4333c65f5cd675d1f0bccdd60a416d78cde88ac00000000

Legacy transaction broadcasted with TXID: c449c2c51dd4e85957e60260d44859f121003cdc98f3db8dedcbbcdf99328f3e
```

```
Decoded Transaction: {'txid': 'c449c2c51dd4e85957e60260d44859f121003cdc98f3db8dedcbbcdf99328f3e', 'hash': 'c449c2c51dd4e85957e60260d44859f121
003cdc98f3db8dedcbbcdf99328f3e', 'version': 2, 'size': 225, 'vsize': 225, 'weight': 900, 'locktime': 0, 'vin': [{'txid': '469b6eb918c16118cb4
5576b91b882a3a25719d61a0a72519b83c0c64db412cb', 'vout': 0, 'scriptSig': {'asm': '304402200b6d4f81cb8484c802954611cfa3892567c9d7d3064c954b7435
b8b14916cd26022005eeb51720cf627a5edbe7d19f4762928ac29403db086330f43650d1064a5c60[ALL] 0286d2b87dc0746150b0e72204aecd2c9b3ab9133d5278b635d3032
bca7d184b25', 'hex': '47304402200b6d4f81cb8484c802954611cfa3892567c9d7d3064c954b7435b8b14916cd26022005eeb51720cf627a5edbe7d19f4762928ac29403d
b086330f43650d1064a5c6001210286d2b87dc0746150b0e72204aecd2c9b3ab9133d5278b635d3032bca7d184b25'}, 'sequence': 4294967293}], 'vout': [{'value':
 Decimal('0.00010000'), 'n': 0, 'scriptPubKey': {'asm': 'OP_DUP OP_HASH160 c3c1d8018c0b101826c6713ad7409a223646f802 OP_EQUALVERIFY OP_CHECKSI
G', 'desc': 'addr(myN2GxmyVCmu6Ak3L91cMcdHs6U3rtngKD)#4p7nepmw', 'hex': '76a914c3c1d8018c0b101826c6713ad7409a223646f80288ac', 'address': 'myN
2GxmyVCmu6Ak3L91cMcdHs6U3rtngKD', 'type': 'pubkeyhash'}}, {'value': Decimal('0.00989000'), 'n': 1, 'scriptPubKey': {'asm': 'OP_DUP OP_HASH160
 2be0e4333c65f5cd675d1f0bccdd60a416d78cde OP_EQUALVERIFY OP_CHECKSIG', 'desc': 'addr(mjWxm2nbKGczMkwe9FdMeyaX4DAJxfz3pB)#45svwnnj', 'hex': '7
6a9142be0e4333c65f5cd675d1f0bccdd60a416d78cde88ac', 'address': 'mjWxm2nbKGczMkwe9FdMeyaX4DAJxfz3pB', 'type': 'pubkeyhash'}}]}


--- Listing UTXOs for Legacy Address B ---

UTXO txid: c449c2c51dd4e85957e60260d44859f121003cdc98f3db8dedcbbcdf99328f3e vout: 0 amount: 0.00010000

Raw transaction created: 02000000013e8f3299dfbccbed8ddbf398dc3c0021f15948d46002e65759e8d41dc5c249c4000000000fdffffff028813000000000000001976a9
1408c4503281447ae7f51b84b9f83b51197186978488aca00f000000000000001976a914c3c1d8018c0b101826c6713ad7409a223646f80288ac00000000


--- Processing Legacy Transaction from B to C ---

Signed transaction hex: 02000000013e8f3299dfbccbed8ddbf398dc3c0021f15948d46002e65759e8d41dc5c249c4000000006a47304402206f8ce2f24295cb6d0830fe0
2d0dc655eb5673cce56acc31b635940868f9443a102205d3376422e51b1ceb448bc695581e96db5e3140d90f202f0dffb9d262f411bfb012103fa87cc58d21f58921409d96d1a
b0bbe967be4f7bc59adeefcfddffd074d9c73afdfffffff028813000000000000001976a91408c4503281447ae7f51b84b9f83b51197186978488aca00f000000000000001976a914c
3c1d8018c0b101826c6713ad7409a223646f80288ac00000000

Legacy transaction broadcasted with TXID: a33ee6cf8015a0f1c5a15a157116962b4f0803cc10c18b8790c05c5a26b5b0b1
```

Challenge and Response Scripts:

They are of this format:

- **Locking Script (Challenge):**
  `OP_DUP OP_HASH160 <Public Key Hash> OP_EQUALVERIFY OP_CHECKSIG`
- **Unlocking Script (Response):**
  `<Signature> <Public Key>`

Validation Process:

The unlocking script generates a HASH160 from the provided public key. This computed HASH160 must match the public key hash specified in the locking script. For example, in the transaction from B to C, the expected and computed HASH160 values are identical, validating the transaction.

Screenshots & Debugging:

Here are the outputs from the btcdeb debugger we ran on windows: (It finally shows a 1(True)) in the stack which indicates that the transaction was properly validated.

```
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb --tx=02000000018712beb51a051de78f2f8d55a172852a5aa6cb241f9fd5ab1ce7c9ec91c3d966000000006a47
3044022074e63637308a68a03e7dab791dbf1fad4ee11fd8c0760f7fbb4384fd2c36861c02206192b3e30f35a13212a3bf7f24d6b261fbef07d393e7f034211293984750956d012102c5
87564ad5ebd8192aa45100e4664855dab85cde87e1cdfa33af56867f5cdd41fdffffff028813000000000001976a9148ad0d691e2807fbe22b243d932b189f4ccfa6af788aca00f0000
000000001976a914bc73d04dd6007f6149ec289b67596c572b57aeed88ac00000000 --txin=0200000001e00c823ecf2ffbadcf91734fe7d3c07df15d42a79894e1cd3ffca67f0e940d
99000000006a473044022002baa94f82fce35953c2902151d1b111126db89a96a7494d29bcd1a467156be2022066cfcd8d457ba4520f8218e5195ec40ffbfb415a087da7f2f4687f7183
9ba2e5012103cfec52c4c7d4ea438275571e77dda4edf9aa42ef2815c63d18dffd1958e941ecfdffffff021027000000000001976a914bc73d04dd6007f6149ec289b67596c572b57ae
ed88ac48170f00000000001976a914ad90198a5fd139c1399e56b7ea67041aa1d7d23e88ac00000000
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)
input tx index = 0; tx input vout = 0; value = 10000
got witness stack of size 0
8 op script loaded. type `help` for usage information
script                                                              |  stack
--------------------------------------------------------------------+--------
3044022074e63637308a68a03e7dab791dbf1fad4ee11fd8c0760f7fbb4384f... |
02c587564ad5ebd8192aa45100e4664855dab85cde87e1cdfa33af56867f5cdd41 |
<<< scriptPubKey >>>                                                |
OP_DUP                                                              |
OP_HASH160                                                          |
bc73d04dd6007f6149ec289b67596c572b57aeed                            |
OP_EQUALVERIFY                                                      |
OP_CHECKSIG                                                         |
#0000 3044022074e63637308a68a03e7dab791dbf1fad4ee11fd8c0760f7fbb4384fd2c36861c02206192b3e30f35a13212a3bf7f24d6b261fbef07d393e7f034211293984750956d01
btcdeb> step
                <> PUSH stack 3044022074e63637308a68a03e7dab791dbf1fad4ee11fd8c0760f7fbb4384fd2c36861c02206192b3e30f35a13212a3bf7f24d6b261fbef07d393
e7f034211293984750956d01
script                                                              |
        stack
--------------------------------------------------------------------+-----------------------------------------------------------------------
02c587564ad5ebd8192aa45100e4664855dab85cde87e1cdfa33af56867f5cdd41 | 3044022074e63637308a68a03e7dab791dbf1fad4ee11fd8c0760f7fbb4384f...
<<< scriptPubKey >>>                                                |
OP_DUP                                                              |
OP_HASH160                                                          |
bc73d04dd6007f6149ec289b67596c572b57aeed                            |
OP_EQUALVERIFY                                                      |
OP_CHECKSIG                                                         |
#0001 02c587564ad5ebd8192aa45100e4664855dab85cde87e1cdfa33af56867f5cdd41
btcdeb> step
                <> PUSH stack 02c587564ad5ebd8192aa45100e4664855dab85cde87e1cdfa33af56867f5cdd41
script                                                              |
        stack
--------------------------------------------------------------------+-----------------------------------------------------------------------
<<< scriptPubKey >>>                                                | 02c587564ad5ebd8192aa45100e4664855dab85cde87e1cdfa33af56867f5cdd41
OP_DUP                                                              | 3044022074e63637308a68a03e7dab791dbf1fad4ee11fd8c0760f7fbb4384f...
OP_HASH160                                                          |
bc73d04dd6007f6149ec289b67596c572b57aeed                            |
OP_EQUALVERIFY                                                      |
OP_CHECKSIG                                                         |
<<< scriptPubKey >>>
btcdeb> step
script                                                              |
        stack
--------------------------------------------------------------------+-----------------------------------------------------------------------
OP_DUP                                                              | 02c587564ad5ebd8192aa45100e4664855dab85cde87e1cdfa33af56867f5cdd41
OP_HASH160                                                          | 3044022074e63637308a68a03e7dab791dbf1fad4ee11fd8c0760f7fbb4384f...
bc73d04dd6007f6149ec289b67596c572b57aeed                            |
OP_EQUALVERIFY                                                      |
OP_CHECKSIG                                                         |
#0003 OP_DUP
btcdeb> step
                <> PUSH stack 02c587564ad5ebd8192aa45100e4664855dab85cde87e1cdfa33af56867f5cdd41
script                                                              |
        stack
--------------------------------------------------------------------+-----------------------------------------------------------------------
OP_HASH160                                                          | 02c587564ad5ebd8192aa45100e4664855dab85cde87e1cdfa33af56867f5cdd41
bc73d04dd6007f6149ec289b67596c572b57aeed                            | 02c587564ad5ebd8192aa45100e4664855dab85cde87e1cdfa33af56867f5cdd41
OP_EQUALVERIFY                                                      | 3044022074e63637308a68a03e7dab791dbf1fad4ee11fd8c0760f7fbb4384f...
OP_CHECKSIG                                                         |
#0004 OP_HASH160
```

```
OP_EQUALVERIFY                                                  | 02c587564ad5ebd8192aa45100e4664855dab85cde87e1cdfa33af56867f5cdd41
OP_CHECKSIG                                                     | 3044022074e63637308a68a03e7dab791dbf1fad4ee11fd8c0760f7fbb4384f...
#0005 bc73d04dd6007f6149ec289b67596c572b57aeed
btcdeb> step
               <> PUSH stack bc73d04dd6007f6149ec289b67596c572b57aeed
script                                                          |
        stack
----------------------------------------------------------------+-------------------------------------------------------------------
OP_EQUALVERIFY                                                  |                         bc73d04dd6007f6149ec289b67596c572b57aeed
OP_CHECKSIG                                                     |                         bc73d04dd6007f6149ec289b67596c572b57aeed
                                                                | 02c587564ad5ebd8192aa45100e4664855dab85cde87e1cdfa33af56867f5cdd41
                                                                | 3044022074e63637308a68a03e7dab791dbf1fad4ee11fd8c0760f7fbb4384f...
#0006 OP_EQUALVERIFY
btcdeb> step
               <> POP  stack
               <> POP  stack
               <> PUSH stack 01
               <> POP  stack
script                                                          |
        stack
----------------------------------------------------------------+-------------------------------------------------------------------
OP_CHECKSIG                                                     | 02c587564ad5ebd8192aa45100e4664855dab85cde87e1cdfa33af56867f5cdd41
                                                                | 3044022074e63637308a68a03e7dab791dbf1fad4ee11fd8c0760f7fbb4384f...
#0007 OP_CHECKSIG
btcdeb> step
EvalChecksig() sigversion=0
Eval Checksig Pre-Tapscript
GenericTransactionSignatureChecker::CheckECDSASignature(71 len sig, 33 len pubkey, sigversion=0)
  sig         = 3044022074e63637308a68a03e7dab791dbf1fad4ee11fd8c0760f7fbb4384fd2c36861c02206192b3e30f35a13212a3bf7f24d6b261fbef07d393e7f03421129398
4750956d01
  pub key     = 02c587564ad5ebd8192aa45100e4664855dab85cde87e1cdfa33af56867f5cdd41
  script code = 76a914bc73d04dd6007f6149ec289b67596c572b57aeed88ac
  hash type   = 01 (SIGHASH_ALL)
SignatureHash(nIn=0, nHashType=01, amount=10000)
- sigversion = SIGVERSION_BASE (non-segwit style)
 << txTo.vin[nInput=0].prevout = COutPoint(66d9c391ec, 0)
(SerializeScriptCode)
 << scriptCode.size()=25 - nCodeSeparators=0
 << script:76a914bc73d04dd6007f6149ec289b67596c572b57aeed88ac
 << txTo.vin[nInput].nSequence = 4294967293 [0xfffffffd]
  sighash     = 423eba155ffd3e4e5c61b580a26a309620c163ff4c775da54cbc90cae180ee87
  pubkey.VerifyECDSASignature(sig=3044022074e63637308a68a03e7dab791dbf1fad4ee11fd8c0760f7fbb4384fd2c36861c02206192b3e30f35a13212a3bf7f24d6b261fbef07
d393e7f03421129398 4750956d, sighash=423eba155ffd3e4e5c61b580a26a309620c163ff4c775da54cbc90cae180ee87):
```

```
----------------------------------------------------------------+-------------------------------------------------------------------
OP_CHECKSIG                                                     | 02c587564ad5ebd8192aa45100e4664855dab85cde87e1cdfa33af56867f5cdd41
                                                                | 3044022074e63637308a68a03e7dab791dbf1fad4ee11fd8c0760f7fbb4384f...
#0007 OP_CHECKSIG
btcdeb> step
EvalChecksig() sigversion=0
Eval Checksig Pre-Tapscript
GenericTransactionSignatureChecker::CheckECDSASignature(71 len sig, 33 len pubkey, sigversion=0)
  sig         = 3044022074e63637308a68a03e7dab791dbf1fad4ee11fd8c0760f7fbb4384fd2c36861c02206192b3e30f35a13212a3bf7f24d6b261fbef07d393e7f03421129398
4750956d01
  pub key     = 02c587564ad5ebd8192aa45100e4664855dab85cde87e1cdfa33af56867f5cdd41
  script code = 76a914bc73d04dd6007f6149ec289b67596c572b57aeed88ac
  hash type   = 01 (SIGHASH_ALL)
SignatureHash(nIn=0, nHashType=01, amount=10000)
- sigversion = SIGVERSION_BASE (non-segwit style)
 << txTo.vin[nInput=0].prevout = COutPoint(66d9c391ec, 0)
(SerializeScriptCode)
 << scriptCode.size()=25 - nCodeSeparators=0
 << script:76a914bc73d04dd6007f6149ec289b67596c572b57aeed88ac
 << txTo.vin[nInput].nSequence = 4294967293 [0xfffffffd]
  sighash     = 423eba155ffd3e4e5c61b580a26a309620c163ff4c775da54cbc90cae180ee87
  pubkey.VerifyECDSASignature(sig=3044022074e63637308a68a03e7dab791dbf1fad4ee11fd8c0760f7fbb4384fd2c36861c02206192b3e30f35a13212a3bf7f24d6b261fbef07
d393e7f03421129398 4750956d, sighash=423eba155ffd3e4e5c61b580a26a309620c163ff4c775da54cbc90cae180ee87):
  result: success
               <> POP  stack
               <> POP  stack
               <> PUSH stack 01
script                                                          |
        stack
----------------------------------------------------------------+-------------------------------------------------------------------
                                                                |
            01
btcdeb>
```

SegWit (P2WPKH) Transactions Report

- **Funding Address A:**
    - **Address:** `bcrt1qjs54g00as9ka3yaqt8eusl8lq494q2qxqc7xfs` is funded with **0.01 BTC**.
- **Transaction from A to B:**
    - **TXID:** `8cb1788a0a00521f2e8e26bf5e6cfc3dba98830c66de2208ece584810b95ea85`
    - **B's Address:** `bcrt1q2d5f8ykj7etdlq6tmn6dvygeghhe33wca498tr`
- **Transaction from B to C:**
    - **TXID:** `2c98e142eb4794c8e98b8520fe34dece0634477a7de8d01f54892be92b3e423c`
    - **C's Address:** `bcrt1q705zyc4eu4er7rdprp9dvz7tvrqkpeyuy5nu7h`

Scripts:

Transaction A → B:


```
{
 "txid": "8cb1788a0a00521f2e8e26bf5e6cfc3dba98830c66de2208ece584810b95ea85",
 "vin": [
  {
   "txid": "9261ed81e951c8371aa138189fbb8ef2afed92860cf48411538480576cca3d33",
   "scriptSig": {
    "asm": "",
    "hex": ""
   },
   "txinwitness": [
```

"304402207c8ec1e577afa01889fdb806f497b166e8f5f060a1e44ee3db74abaa12c86aaa022016e5632646e2397f58fec095a393f2e62f13addc304b2c0acb983088ca7b441401",

"02920ac419838952d92c71d85f1f4abef2727ba3ec0d700e10d0c8f4828f3ae799"

]

}

],

"vout": [

{

"scriptPubKey": {

"asm": "0 53689392d2f656df834bdcf4d6111945ef98c5d8",

"address": "bcrt1q2d5f8ykj7etdlq6tmn6dvygeghhe33wca498tr"

}

},

{

"scriptPubKey": {

"asm": "0 9429543dfd816dd893a059f3c87cff054b502806",

"address": "bcrt1qjs54g00as9ka3yaqt8eusl8lq494q2qxqc7xfs"

}

}

]

}

Transaction B → C:

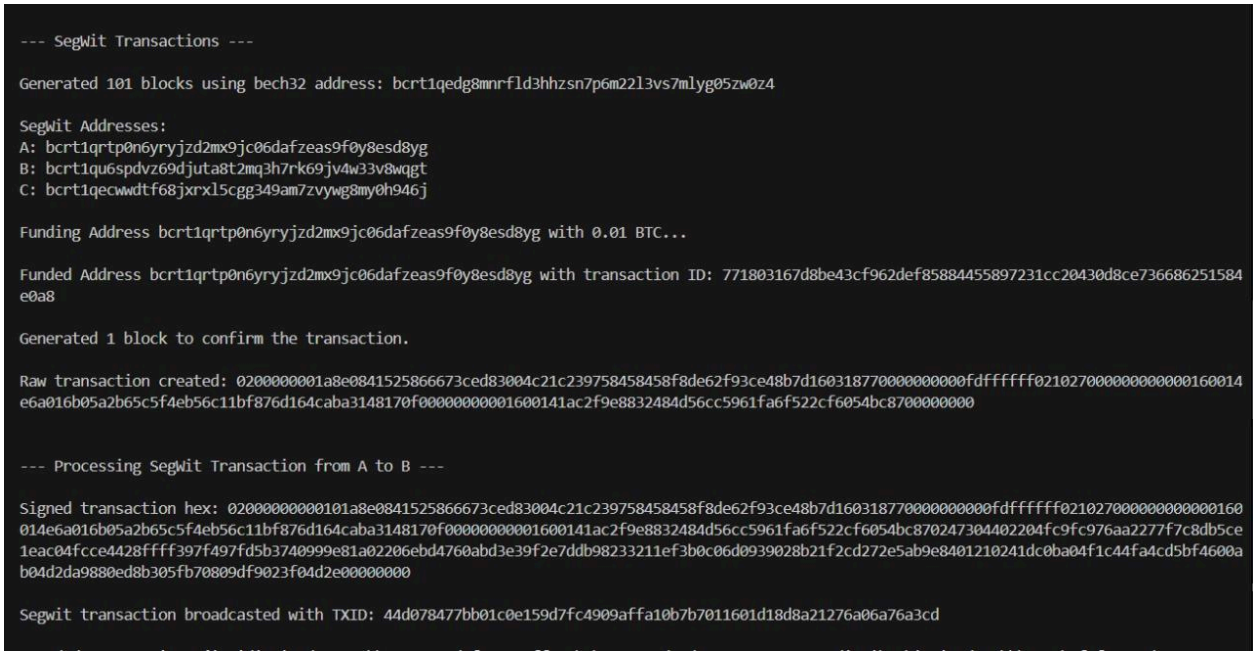
{

"txid": "2c98e142eb4794c8e98b8520fe34dece0634477a7de8d01f54892be92b3e423c",

```
 "vin": [
  {
    "txid": "8cb1788a0a00521f2e8e26bf5e6cfc3dba98830c66de2208ece584810b95ea85",
    "scriptSig": {
      "asm": "",
      "hex": ""
    },
    "txinwitness": [
"3044022055e68bd7aea2859d611d5d712ae8c7acd262a049280374f00a6a45e60651d43f022030ef2b3365a2c45d14434db8d3ee395adbde6798feb5a657137481cb4f4fc57d01",
      "03bf3e78fea1eea07bdf7a6633fa88f38fde8c914065726ba5ad4f5c490b3791b1"
    ]
  }
 ],
 "vout": [
  {
    "scriptPubKey": {
      "asm": "0 f3e82262b9e5723f0da1184ad60bcb60c160e49c",
      "address": "bcrt1q705zyc4eu4er7rdprp9dvz7tvrqkpeyuy5nu7h"
    }
  },
  {
    "scriptPubKey": {
      "asm": "0 53689392d2f656df834bdcf4d6111945ef98c5d8",
```

```
      "address": "bcrt1q2d5f8ykj7etdlq6tmn6dvygeghhe33wca498tr"
    }
  }
 ]
}
```

Output Screenshots containing decoded scripts:



```
Decoded Transaction: {'txid': '44d078477bb01c0e159d7fc4909affa10b7b7011601d18d8a21276a06a76a3cd', 'hash': '25d667bbb65c2bcf4fca777d8c98957428
13ad09d8cec6e4c833acbe36850642', 'version': 2, 'size': 222, 'vsize': 141, 'weight': 561, 'locktime': 0, 'vin': [{'txid': '771803167d8be43cf96
2def85884455897231cc20430d8ce736686251584e0a8', 'vout': 0, 'scriptSig': {'asm': '', 'hex': ''}, 'txinwitness': ['304402204fc9fc976aa2277f7c8d
b5ce1eac04fcce4428ffff397f497fd5b3740999e81a02206ebd4760abd3e39f2e7ddb98233211ef3b0c06d0939028b21f2cd272e5ab9e8401', '0241dc0ba04f1c44fa4cd5b
f4600ab04d2da9880ed8b305fb70809df9023f04d2e'], 'sequence': 4294967293}], 'vout': [{'value': Decimal('0.00010000'), 'n': 0, 'scriptPubKey': {'
asm': '0 e6a016b05a2b65c5f4eb56c11bf876d164caba31', 'desc': 'addr(bcrt1qu6spdvz69djuta8t2mq3h7rk69jv4w33v8wqgt)#4gnk8had', 'hex': '0014e6a016
b05a2b65c5f4eb56c11bf876d164caba31', 'address': 'bcrt1qu6spdvz69djuta8t2mq3h7rk69jv4w33v8wqgt', 'type': 'witness_v0_keyhash'}}, {'value': Dec
imal('0.00989000'), 'n': 1, 'scriptPubKey': {'asm': '0 1ac2f9e8832484d56cc5961fa6f522cf6054bc87', 'desc': 'addr(bcrt1qrtp0n6yryjzd2mx9jc06daf
zeas9f0y8esd8yg)#u58n0fw9', 'hex': '00141ac2f9e8832484d56cc5961fa6f522cf6054bc87', 'address': 'bcrt1qrtp0n6yryjzd2mx9jc06dafzeas9f0y8esd8yg',
 'type': 'witness_v0_keyhash'}}]}

Raw transaction created: 0200000001cda3766aa07612a2d8181d6011707b0ba1ff9a90c47f9d150e1cb07b4778d0440000000000fdffffff028813000000000000160014
ce1ce6ad3a3c8c337e98422352f77e1308e41f64a00f0000000000000160014e6a016b05a2b65c5f4eb56c11bf876d164caba3100000000


--- Processing SegWit Transaction from B to C ---

Signed transaction hex: 02000000000101cda3766aa07612a2d8181d6011707b0ba1ff9a90c47f9d150e1cb07b4778d0440000000000fdffffff028813000000000000160
014ce1ce6ad3a3c8c337e98422352f77e1308e41f64a00f0000000000000160014e6a016b05a2b65c5f4eb56c11bf876d164caba3102473040220 4fbf7b1529ebc4925832db6a
f76ef38513d1d920e88a25b7f6747148750fbe4002203972bd613c126ba55911c440d31af90a0abab37e0dbe5f3baf8b537c01e87c9301210274034602c30ed2ae5abaecc3334
01849624135f7c783645987bb4f079b94cb5b00000000

Segwit transaction broadcasted with TXID: 1fb95d6ec374f99fecc309941aead271e2c176121b720a9bf202dc554f80ca98


Decoded Transaction: {'txid': '1fb95d6ec374f99fecc309941aead271e2c176121b720a9bf202dc554f80ca98', 'hash': '5c7aac94ec8e390cd56a14c12890ff0f35
a1b17b140fa7ac6b11731720e39a7f', 'version': 2, 'size': 222, 'vsize': 141, 'weight': 561, 'locktime': 0, 'vin': [{'txid': '44d078477bb01c0e159
a1b17b140fa7ac6b11731720e39a7f', 'version': 2, 'size': 222, 'vsize': 141, 'weight': 561, 'locktime': 0, 'vin': [{'txid': '44d078477bb01c0e159
d7fc4909affa10b7b7011601d18d8a21276a06a76a3cd', 'vout': 0, 'scriptSig': {'asm': '', 'hex': ''}, 'txinwitness': ['304402204fbf7b1529ebc4925832
d7fc4909affa10b7b7011601d18d8a21276a06a76a3cd', 'vout': 0, 'scriptSig': {'asm': '', 'hex': ''}, 'txinwitness': ['304402204fbf7b1529ebc4925832
db6af76ef38513d1d920e88a25b7f6747148750fbe4002203972bd613c126ba55911c440d31af90a0abab37e0dbe5f3baf8b537c01e87c9301', '0274034602c30ed2ae5abae
cc333401849624135f7c783645987bb4f079b94cb5b'], 'sequence': 4294967293}], 'vout': [{'value': Decimal('0.00005000'), 'n': 0, 'scriptPubKey': {'
asm': '0 ce1ce6ad3a3c8c337e98422352f77e1308e41f64', 'desc': 'addr(bcrt1qecwwdtf68jxrxl5cgg349am7zvywg8my0h946j)#8gs0ggx4', 'hex': '0014ce1ce6
ad3a3c8c337e98422352f77e1308e41f64', 'address': 'bcrt1qecwwdtf68jxrxl5cgg349am7zvywg8my0h946j', 'type': 'witness_v0_keyhash'}}, {'value': Dec
imal('0.00004000'), 'n': 1, 'scriptPubKey': {'asm': '0 e6a016b05a2b65c5f4eb56c11bf876d164caba31', 'desc': 'addr(bcrt1qu6spdvz69djuta8t2mq3h7r
k69jv4w33v8wqgt)#4gnk8had', 'hex': '0014e6a016b05a2b65c5f4eb56c11bf876d164caba31', 'address': 'bcrt1qu6spdvz69djuta8t2mq3h7rk69jv4w33v8wqgt',
 'type': 'witness_v0_keyhash'}}]}
```

```
Decoded Transaction: {'txid': '1fb95d6ec374f99fecc309941aead271e2c176121b720a9bf202dc554f80ca98', 'hash': '5c7aac94ec8e390cd56a14c12890ff0f35
a1b17b140fa7ac6b11731720e39a7f', 'version': 2, 'size': 222, 'vsize': 141, 'weight': 561, 'locktime': 0, 'vin': [{'txid': '44d078477bb01c0e159
a1b17b140fa7ac6b11731720e39a7f', 'version': 2, 'size': 222, 'vsize': 141, 'weight': 561, 'locktime': 0, 'vin': [{'txid': '44d078477bb01c0e159
d7fc4909affa10b7b7011601d18d8a21276a06a76a3cd', 'vout': 0, 'scriptSig': {'asm': '', 'hex': ''}, 'txinwitness': ['304402204fbf7b1529ebc4925832
d7fc4909affa10b7b7011601d18d8a21276a06a76a3cd', 'vout': 0, 'scriptSig': {'asm': '', 'hex': ''}, 'txinwitness': ['304402204fbf7b1529ebc4925832
db6af76ef38513d1d920e88a25b7f6747148750fbe4002203972bd613c126ba55911c440d31af90a0abab37e0dbe5f3baf8b537c01e87c9301', '0274034602c30ed2ae5abae
cc333401849624135f7c783645987bb4f079b94cb5b'], 'sequence': 4294967293}], 'vout': [{'value': Decimal('0.00005000'), 'n': 0, 'scriptPubKey': {'
asm': '0 ce1ce6ad3a3c8c337e98422352f77e1308e41f64', 'desc': 'addr(bcrt1qecwwdtf68jxrxl5cgg349am7zvywg8my0h946j)#8gs0ggx4', 'hex': '0014ce1ce6
ad3a3c8c337e98422352f77e1308e41f64', 'address': 'bcrt1qecwwdtf68jxrxl5cgg349am7zvywg8my0h946j', 'type': 'witness_v0_keyhash'}}, {'value': Dec
imal('0.00004000'), 'n': 1, 'scriptPubKey': {'asm': '0 e6a016b05a2b65c5f4eb56c11bf876d164caba31', 'desc': 'addr(bcrt1qu6spdvz69djuta8t2mq3h7r
k69jv4w33v8wqgt)#4gnk8had', 'hex': '0014e6a016b05a2b65c5f4eb56c11bf876d164caba31', 'address': 'bcrt1qu6spdvz69djuta8t2mq3h7rk69jv4w33v8wqgt',
 'type': 'witness_v0_keyhash'}}]}

Verifying segwit input spending 44d078477bb01c0e159d7fc4909affa10b7b7011601d18d8a21276a06a76a3cd:0
asm': '0 ce1ce6ad3a3c8c337e98422352f77e1308e41f64', 'desc': 'addr(bcrt1qecwwdtf68jxrxl5cgg349am7zvywg8my0h946j)#8gs0ggx4', 'hex': '0014ce1ce6
ad3a3c8c337e98422352f77e1308e41f64', 'address': 'bcrt1qecwwdtf68jxrxl5cgg349am7zvywg8my0h946j', 'type': 'witness_v0_keyhash'}}, {'value': Dec
imal('0.00004000'), 'n': 1, 'scriptPubKey': {'asm': '0 e6a016b05a2b65c5f4eb56c11bf876d164caba31', 'desc': 'addr(bcrt1qu6spdvz69djuta8t2mq3h7r
k69jv4w33v8wqgt)#4gnk8had', 'hex': '0014e6a016b05a2b65c5f4eb56c11bf876d164caba31', 'address': 'bcrt1qu6spdvz69djuta8t2mq3h7rk69jv4w33v8wqgt',
 'type': 'witness_v0_keyhash'}}]}

Verifying segwit input spending 44d078477bb01c0e159d7fc4909affa10b7b7011601d18d8a21276a06a76a3cd:0

  Expected HASH160 (from locking script): e6a016b05a2b65c5f4eb56c11bf876d164caba31
k69jv4w33v8wqgt)#4gnk8had', 'hex': '0014e6a016b05a2b65c5f4eb56c11bf876d164caba31', 'address': 'bcrt1qu6spdvz69djuta8t2mq3h7rk69jv4w33v8wqgt',
 'type': 'witness_v0_keyhash'}}]}

Verifying segwit input spending 44d078477bb01c0e159d7fc4909affa10b7b7011601d18d8a21276a06a76a3cd:0

  Expected HASH160 (from locking script): e6a016b05a2b65c5f4eb56c11bf876d164caba31

  Expected HASH160 (from locking script): e6a016b05a2b65c5f4eb56c11bf876d164caba31
  Expected HASH160 (from locking script): e6a016b05a2b65c5f4eb56c11bf876d164caba31

  Computed HASH160 (from witness pubkey): e6a016b05a2b65c5f4eb56c11bf876d164caba31

  Verification PASSED for this segwit input.

All transactions completed.
```

Challenge and Response Scripts:

- **Locking Script (Challenge):**
  For SegWit P2WPKH, the locking script is:
  `0 <Public Key Hash>`
- **Unlocking Script (Response) – Witness Data:**
  `[Signature, Public Key]`

Validation Process:

In SegWit transactions, validation is performed by:

1. Extracting the witness data (signature and public key).
2. Computing the HASH160 of the provided public key.
3. Comparing the computed hash with the public key hash in the locking script. For example, in Transaction A → B, the HASH160 computed from the witness public key matches the one in the locking script, thereby validating the transaction.

Screenshots & Debugging:

Here are the outputs from the btcdeb debugger we ran on windows: (It finally shows a 1(True)) in the stack which indicates that the transaction was properly validated.

```
guest@dr-HP-Z2-Tower-G9-Workstation-Desktop-PC:~$ btcdeb --tx=02000000000101cda3766aa07612a2d8181d6011707b0ba1ff9a90c47f9d150e1cb07b4778d044000000000
00fdffffff0288130000000000001600 14ce1ce6ad3a3c8c337e98422352f77e1308e41f64a00f000000000000160014e6a016b05a2b65c5f4eb56c11bf876d164caba3102473044022
04fbf7b1529ebc4925832db6af76ef38513d1d920e88a25b7f6747148750fbe4002203972bd613c126ba55911c440d31af90a0abab37e0dbe5f3baf8b537c01e87c9301210274034602c3
0ed2ae5abaecc333401849624135f7c783645987bb4f079b94cb5b00000000 --txin=02000000000101a8e0841525866673ced83004c21c239758458458f8de62f93ce48b7d160318777
0000000000fdffffff02102700000000000016001 4e6a016b05a2b65c5f4eb56c11bf876d164caba3148170f000000000016001 41ac2f9e8832484d56cc5961fa6f522cf6054bc870247
304402204fc9fc976aa2277f7c8db5ce1eac04fcce4428ffff397f497fd5b3740999e81a02206ebd4760abd3e39f2e7ddb98233211ef3b0c06d0939028b21f2cd272e5ab9e8401210241
dc0ba04f1c44fa4cd5bf4600ab04d2da9880ed8b305fb70809df9023f04d2e00000000
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)
input tx index = 0; tx input vout = 0; value = 10000
got witness stack of size 2
22 bytes (P2WPKH)
valid script
- generating prevout hash from 1 ins
[+] COutPoint(44d078477b, 0)
note: there is a for-clarity preamble (use --verbose for details)
5 op script loaded. type `help` for usage information
script                                  |                                                                  stack
----------------------------------------+------------------------------------------------------------------------
OP_DUP                                  | 0274034602c30ed2ae5abaecc333401849624135f7c783645987bb4f079b94cb5b
OP_HASH160                              | 304402204fbf7b1529ebc4925832db6af76ef38513d1d920e88a25b7f674714...
e6a016b05a2b65c5f4eb56c11bf876d164caba31 |
OP_EQUALVERIFY                          |
OP_CHECKSIG                             |
#0000 OP_DUP
btcdeb> step
                <> PUSH stack 0274034602c30ed2ae5abaecc333401849624135f7c783645987bb4f079b94cb5b
script                                  |                                                                  stack
----------------------------------------+------------------------------------------------------------------------
OP_HASH160                              | 0274034602c30ed2ae5abaecc333401849624135f7c783645987bb4f079b94cb5b
e6a016b05a2b65c5f4eb56c11bf876d164caba31 | 0274034602c30ed2ae5abaecc333401849624135f7c783645987bb4f079b94cb5b
OP_EQUALVERIFY                          | 304402204fbf7b1529ebc4925832db6af76ef38513d1d920e88a25b7f674714...
OP_CHECKSIG                             |
#0001 OP_HASH160
btcdeb> step
                <> POP  stack
                <> PUSH stack e6a016b05a2b65c5f4eb56c11bf876d164caba31
script                                  |                                                                  stack
----------------------------------------+------------------------------------------------------------------------
e6a016b05a2b65c5f4eb56c11bf876d164caba31 |                                 e6a016b05a2b65c5f4eb56c11bf876d164caba31
OP_EQUALVERIFY                          | 0274034602c30ed2ae5abaecc333401849624135f7c783645987bb4f079b94cb5b
OP_CHECKSIG                             | 304402204fbf7b1529ebc4925832db6af76ef38513d1d920e88a25b7f674714...
#0002 e6a016b05a2b65c5f4eb56c11bf876d164caba31
btcdeb> step
                <> PUSH stack e6a016b05a2b65c5f4eb56c11bf876d164caba31
script                                  |                                                                  stack
----------------------------------------+------------------------------------------------------------------------
OP_EQUALVERIFY                          |                                 e6a016b05a2b65c5f4eb56c11bf876d164caba31
OP_CHECKSIG                             |                                 e6a016b05a2b65c5f4eb56c11bf876d164caba31
                                        | 0274034602c30ed2ae5abaecc333401849624135f7c783645987bb4f079b94cb5b
                                        | 304402204fbf7b1529ebc4925832db6af76ef38513d1d920e88a25b7f674714...
#0003 OP_EQUALVERIFY
btcdeb> step
                <> POP  stack
                <> POP  stack
                <> PUSH stack 01
                <> POP  stack
script                                  |                                                                  stack
----------------------------------------+------------------------------------------------------------------------
OP_CHECKSIG                             | 0274034602c30ed2ae5abaecc333401849624135f7c783645987bb4f079b94cb5b
                                        | 304402204fbf7b1529ebc4925832db6af76ef38513d1d920e88a25b7f674714...
#0004 OP_CHECKSIG
btcdeb> step
EvalChecksig() sigversion=1
Eval Checksig Pre-Tapscript
GenericTransactionSignatureChecker::CheckECDSASignature(71 len sig, 33 len pubkey, sigversion=1)
  sig         = 304402204fbf7b1529ebc4925832db6af76ef38513d1d920e88a25b7f6747148750fbe4002203972bd613c126ba55911c440d31af90a0abab37e0dbe5f3baf8b537c
01e87c9301
  pub key     = 0274034602c30ed2ae5abaecc333401849624135f7c783645987bb4f079b94cb5b
  script code = 76a914e6a016b05a2b65c5f4eb56c11bf876d164caba3188ac
  hash type   = 01 (SIGHASH_ALL)
SignatureHash(nIn=0, nHashType=01, amount=10000)
- sigversion == SIGVERSION_WITNESS_V0
  sighash     = 18cd65c6cb0494693490a75d66cb3a9cf96266757f3106e7eaad037fb8f27ffc
  pubkey.VerifyECDSASignature(sig=304402204fbf7b1529ebc4925832db6af76ef38513d1d920e88a25b7f6747148750fbe4002203972bd613c126ba55911c440d31af90a0abab3
7e0dbe5f3baf8b537c01e87c93, sighash=18cd65c6cb0494693490a75d66cb3a9cf96266757f3106e7eaad037fb8f27ffc):
  result: success
                <> POP  stack
                <> POP  stack
                <> PUSH stack 01
script                                  |                                                                   stack
----------------------------------------+-------------------------------------------------------------------------
                                        |                                                                      01
```

---

4. Comparison & Analysis

Feature	P2PKH (Legacy)	P2SH-P2WPKH (SegWit)

Transaction Size	Larger	Smaller
Script Structure	Uses `ScriptSig`	Uses witness field
Security	Vulnerable to malleability	Malleability-resistant
Efficiency	Less efficient	More efficient

4.1 Why SegWit is Better

- **Reduces transaction size**, lowering fees.
- **Eliminates malleability**, improving multi-signature setups.
- **Enables second-layer solutions** like the Lightning Network.

Here is a screenshot of comparison of sizes of the two types of transactions:

```
--- Transaction Virtual Size (vsize) Comparison ---

Legacy transaction (c449c2c51dd4e85957e60260d44859f121003cdc98f3db8dedcbbcdf99328f3e) vsize: 225 bytes

SegWit transaction (44d078477bb01c0e159d7fc4909affa10b7b7011601d18d8a21276a06a76a3cd) vsize: 141 bytes

SegWit transaction is smaller by 84 bytes (vsize).
```
