BITCOIN TRANSACTION ASSIGNMENT

QUESTION 1

First 4 bytes:-02 000000 00 01 ,version 2
Next 2 bytes 0001 (0x00 0x01) - it’s a segwit transaction.
Next byte 01 indicates the number of input - 1

Input #0
Previous txid -c1368b8e3daedf15612b0185f79f4e82df90f6bcd93714e0e057c355d31c8131
Previous output index (vout) - 1
scriptSig: empty (length 0) - P2WPKH inputs because the signature and public key appear in the witness field
Sequence: 0xfffffffd - 4294967293 in decimal

Number of outputs 02 - 2

Output #0
Value: 500000 sats = 0.00500000 BTC
scriptPubKey - 001485d78eb795bd9c8a21afefc8b6fdaedf71836809
This has the structure 00 14 <20-byte-hash> meaning it’s a P2WPKH (SegWit v0) output
PubKeyHash: 85d78eb795bd9c8a21afefc8b6fdaedf71836809

Output #1
Value: 1,050,700 sats = 0.01050700 BTC
scriptPubKey (raw): 0014840ab165c9c2555d4a31b9208ad806f89d2535e2
Also follows 00 14 <20-byte-hash> structure which means it’s a P2WPKH (SegWit v0)
PubKeyHash: 840ab165c9c2555d4a31b9208ad806f89d2535e2

Witness data (for input 0)
Witness stack item count: 2

1. Signature (DER + sighash byte)

   304402207bce86d430b58bb6b79e8c1bbecdf67a530eff3bc61581a1399e0b28a741c0ee
   0220303d5ce926c60bf15577f2e407f28a2ef8fe8453abd4048b716e97dbb1e3a85c01
   This is a DER-encoded signature ending with 01 which represents SIGHASH_ALL.

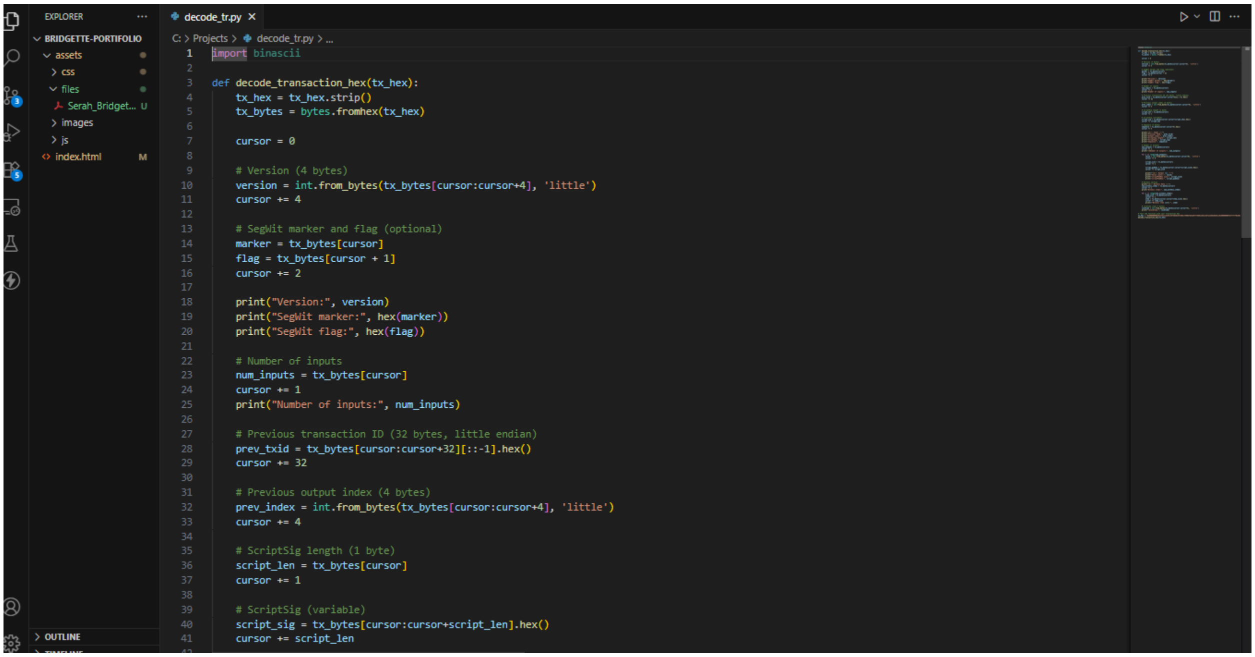
2. Public key (compressed)
   0260828bc77486a55e3bc6032ccbeda915d9494eda17b4a54dbe3b24506d40e4ff
   It starts with 02 which means it’s a compressed public key.

Locktime
Raw (little-endian): 43 03 0e 00

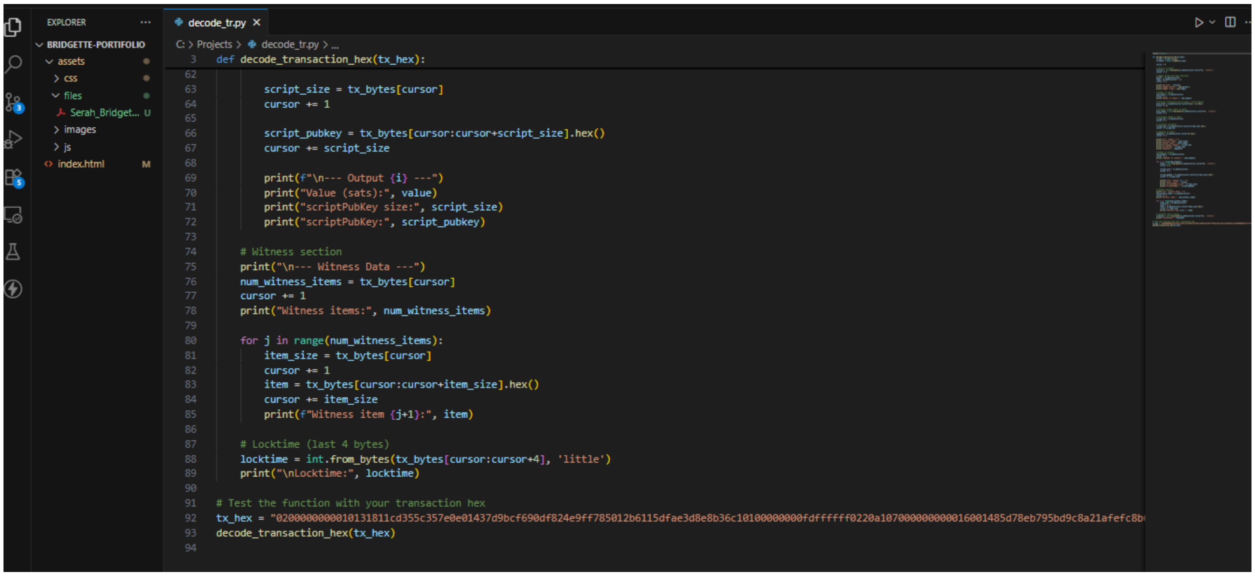
Converted hex (normal order): 0x000e0343
Decimal: 918339

QUESTION 2

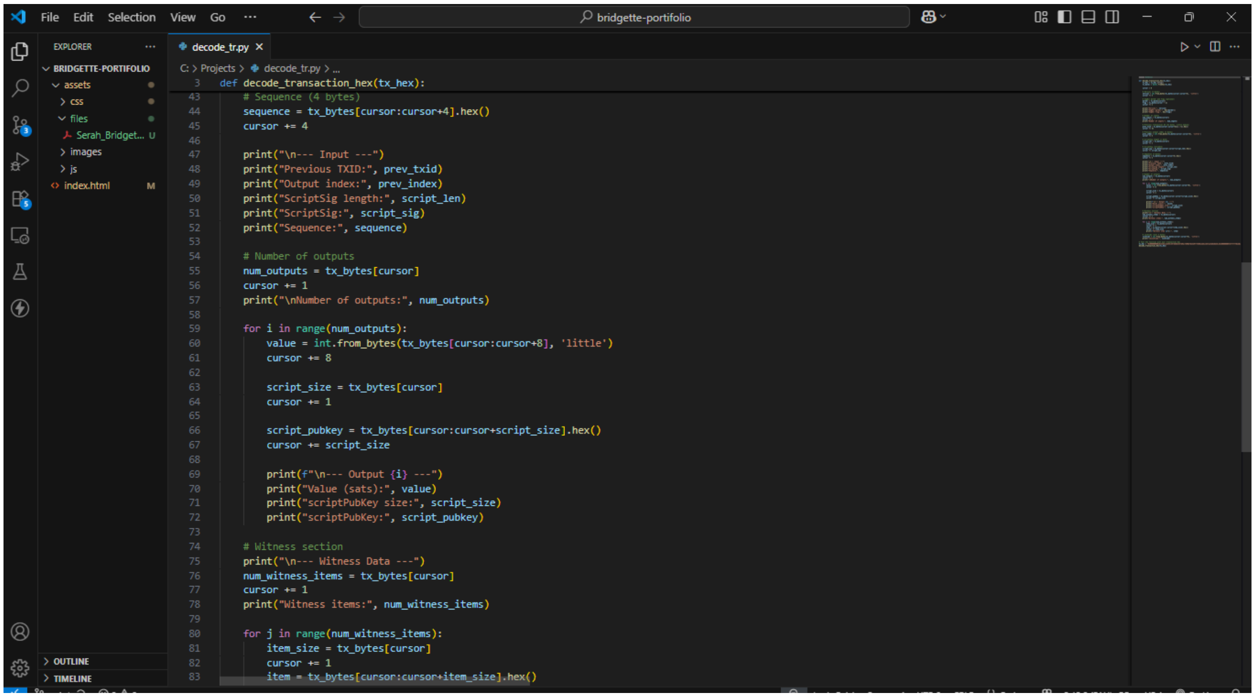
Screenshots :Code



```python
import binascii

def decode_transaction_hex(tx_hex):
    tx_hex = tx_hex.strip()
    tx_bytes = bytes.fromhex(tx_hex)

    cursor = 0

    # Version (4 bytes)
    version = int.from_bytes(tx_bytes[cursor:cursor+4], 'little')
    cursor += 4

    # SegWit marker and flag (optional)
    marker = tx_bytes[cursor]
    flag = tx_bytes[cursor + 1]
    cursor += 2

    print("Version:", version)
    print("SegWit marker:", hex(marker))
    print("SegWit flag:", hex(flag))

    # Number of inputs
    num_inputs = tx_bytes[cursor]
    cursor += 1
    print("Number of inputs:", num_inputs)

    # Previous transaction ID (32 bytes, little endian)
    prev_txid = tx_bytes[cursor:cursor+32][::-1].hex()
    cursor += 32

    # Previous output index (4 bytes)
    prev_index = int.from_bytes(tx_bytes[cursor:cursor+4], 'little')
    cursor += 4

    # ScriptSig length (1 byte)
    script_len = tx_bytes[cursor]
    cursor += 1

    # ScriptSig (variable)
    script_sig = tx_bytes[cursor:cursor+script_len].hex()
    cursor += script_len
```

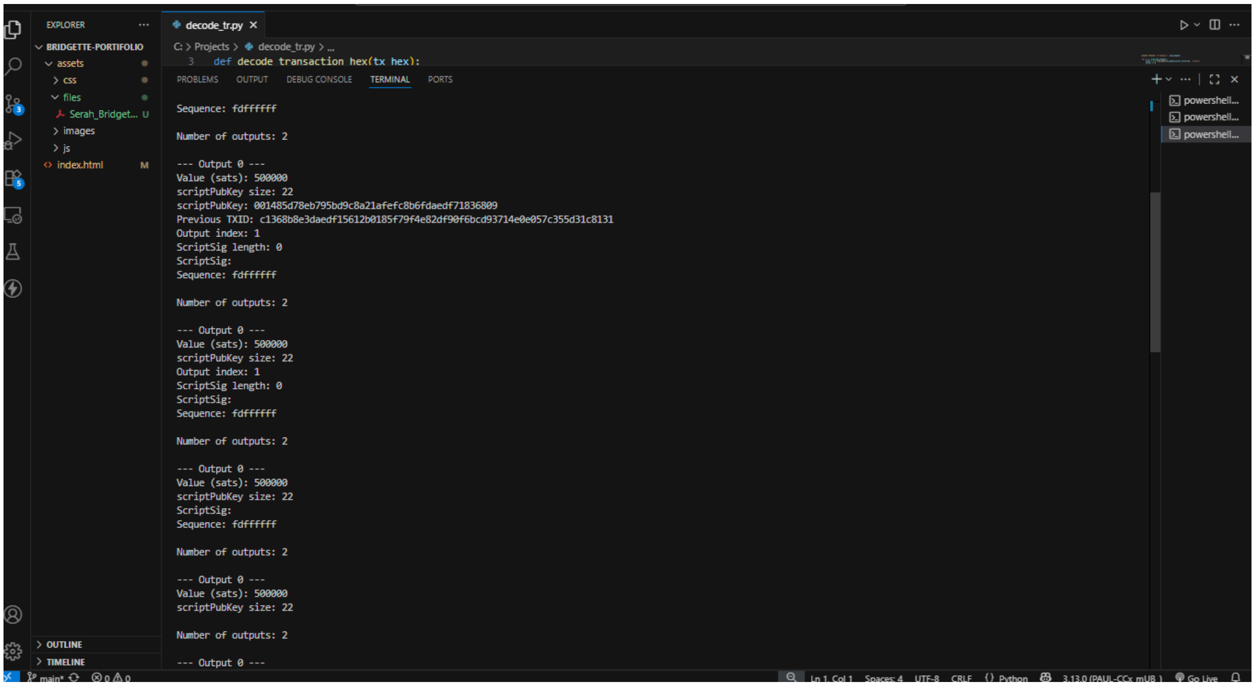


```python
def decode_transaction_hex(tx_hex):

            script_size = tx_bytes[cursor]
            cursor += 1

            script_pubkey = tx_bytes[cursor:cursor+script_size].hex()
            cursor += script_size

            print(f"\n--- Output {i} ---")
            print("Value (sats):", value)
            print("scriptPubKey size:", script_size)
            print("scriptPubKey:", script_pubkey)

        # Witness section
        print("\n--- Witness Data ---")
        num_witness_items = tx_bytes[cursor]
        cursor += 1
        print("Witness items:", num_witness_items)

        for j in range(num_witness_items):
            item_size = tx_bytes[cursor]
            cursor += 1
            item = tx_bytes[cursor:cursor+item_size].hex()
            cursor += item_size
            print(f"Witness item {j+1}:", item)

        # Locktime (last 4 bytes)
        locktime = int.from_bytes(tx_bytes[cursor:cursor+4], 'little')
        print("\nLocktime:", locktime)

# Test the function with your transaction hex
tx_hex = "0200000000010131811cd355c357e0e01437d9bcf690df824e9ff785012b6115dfae3d8e8b36c10100000000fdffffff0220a107000000000016001485d78eb795bd9c8a21afefc8b
decode_transaction_hex(tx_hex)
```



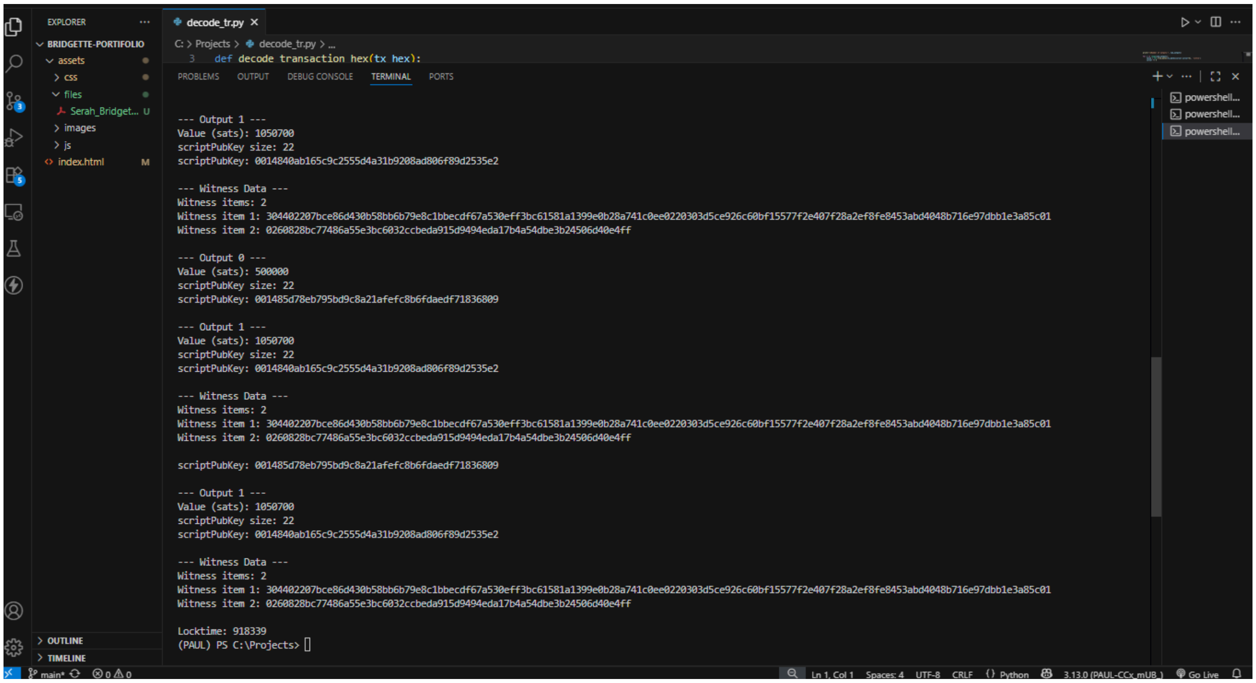
```python
def decode_transaction_hex(tx_hex):
        # Sequence (4 bytes)
        sequence = tx_bytes[cursor:cursor+4].hex()
        cursor += 4

        print("\n--- Input ---")
        print("Previous TXID:", prev_txid)
        print("Output index:", prev_index)
        print("ScriptSig length:", script_len)
        print("ScriptSig:", script_sig)
        print("Sequence:", sequence)

        # Number of outputs
        num_outputs = tx_bytes[cursor]
        cursor += 1
        print("\nNumber of outputs:", num_outputs)

        for i in range(num_outputs):
            value = int.from_bytes(tx_bytes[cursor:cursor+8], 'little')
            cursor += 8

            script_size = tx_bytes[cursor]
            cursor += 1

            script_pubkey = tx_bytes[cursor:cursor+script_size].hex()
            cursor += script_size

            print(f"\n--- Output {i} ---")
            print("Value (sats):", value)
            print("scriptPubKey size:", script_size)
            print("scriptPubKey:", script_pubkey)

        # Witness section
        print("\n--- Witness Data ---")
        num_witness_items = tx_bytes[cursor]
        cursor += 1
        print("Witness items:", num_witness_items)

        for j in range(num_witness_items):
            item_size = tx_bytes[cursor]
            cursor += 1
            item = tx_bytes[cursor:cursor+item_size].hex()
```

OUTPUT



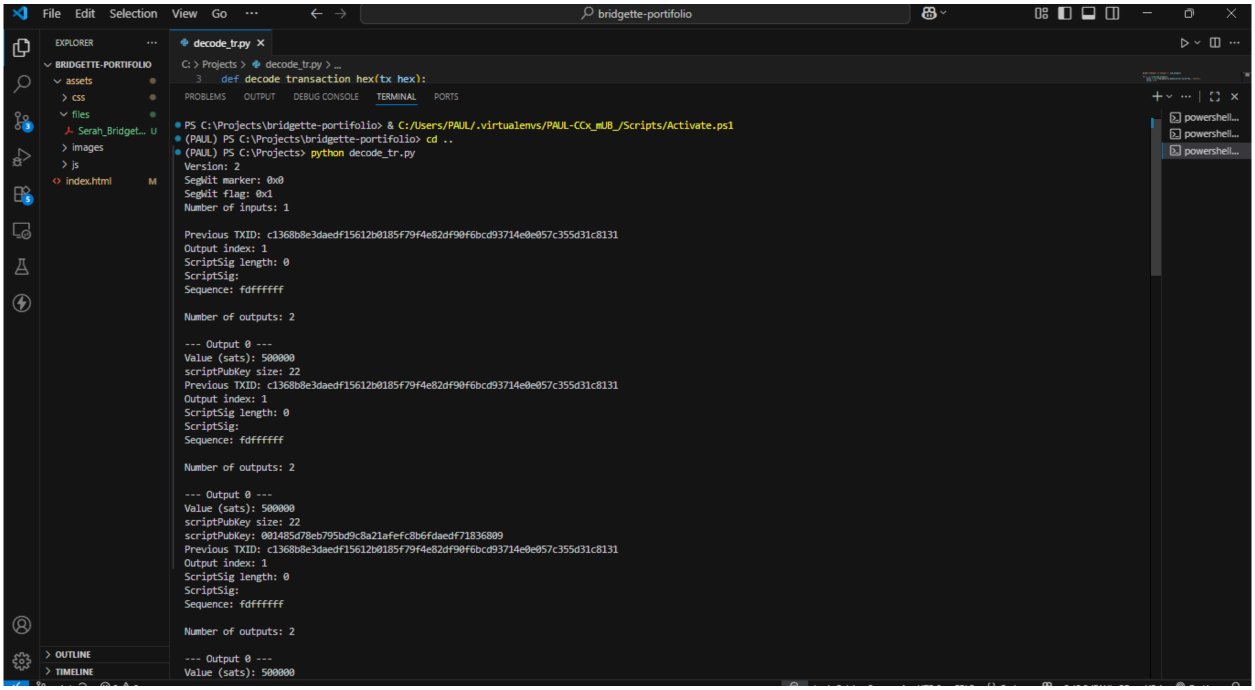
```
3   def decode transaction hex(tx hex):
```

```
Sequence: fdffffff

Number of outputs: 2

--- Output 0 ---
Value (sats): 500000
scriptPubKey size: 22
scriptPubKey: 001485d78eb795bd9c8a21afefc8b6fdaedf71836809
Previous TXID: c1368b8e3daedf15612b0185f79f4e82df90f6bcd93714e0e057c355d31c8131
Output index: 1
ScriptSig length: 0
ScriptSig:
Sequence: fdffffff

Number of outputs: 2

--- Output 0 ---
Value (sats): 500000
scriptPubKey size: 22
Output index: 1
ScriptSig length: 0
ScriptSig:
Sequence: fdffffff

Number of outputs: 2

--- Output 0 ---
Value (sats): 500000
scriptPubKey size: 22
ScriptSig:
Sequence: fdffffff

Number of outputs: 2

--- Output 0 ---
Value (sats): 500000
scriptPubKey size: 22

Number of outputs: 2

--- Output 0 ---
```



```
3   def decode transaction hex(tx hex):
```

```
--- Output 1 ---
Value (sats): 1050700
scriptPubKey size: 22
scriptPubKey: 0014840ab165c9c2555d4a31b9208ad806f89d2535e2

--- Witness Data ---
Witness items: 2
Witness item 1: 304402207bce86d430b58bb6b79e8c1bbecdf67a530eff3bc61581a1399e0b28a741c0ee0220303d5ce926c60bf15577f2e407f28a2ef8fe8453abd4048b716e97dbb1e3a85c01
Witness item 2: 0260828bc77486a55e3bc6032ccbeda915d9494eda17b4a54dbe3b24506d40e4ff

--- Output 0 ---
Value (sats): 500000
scriptPubKey size: 22
scriptPubKey: 001485d78eb795bd9c8a21afefc8b6fdaedf71836809

--- Output 1 ---
Value (sats): 1050700
scriptPubKey size: 22
scriptPubKey: 0014840ab165c9c2555d4a31b9208ad806f89d2535e2

--- Witness Data ---
Witness items: 2
Witness item 1: 304402207bce86d430b58bb6b79e8c1bbecdf67a530eff3bc61581a1399e0b28a741c0ee0220303d5ce926c60bf15577f2e407f28a2ef8fe8453abd4048b716e97dbb1e3a85c01
Witness item 2: 0260828bc77486a55e3bc6032ccbeda915d9494eda17b4a54dbe3b24506d40e4ff

scriptPubKey: 001485d78eb795bd9c8a21afefc8b6fdaedf71836809

--- Output 1 ---
Value (sats): 1050700
scriptPubKey size: 22
scriptPubKey: 0014840ab165c9c2555d4a31b9208ad806f89d2535e2

--- Witness Data ---
Witness items: 2
Witness item 1: 304402207bce86d430b58bb6b79e8c1bbecdf67a530eff3bc61581a1399e0b28a741c0ee0220303d5ce926c60bf15577f2e407f28a2ef8fe8453abd4048b716e97dbb1e3a85c01
Witness item 2: 0260828bc77486a55e3bc6032ccbeda915d9494eda17b4a54dbe3b24506d40e4ff

Locktime: 918339
(PAUL) PS C:\Projects>
```



```
3   def decode transaction hex(tx hex):
```

```
PS C:\Projects\bridgette-portifolio> & C:/Users/PAUL/.virtualenvs/PAUL-CCx_mUB_/Scripts/Activate.ps1
(PAUL) PS C:\Projects\bridgette-portifolio> cd ..
(PAUL) PS C:\Projects> python decode_tr.py
Version: 2
SegWit marker: 0x0
SegWit flag: 0x1
Number of inputs: 1

Previous TXID: c1368b8e3daedf15612b0185f79f4e82df90f6bcd93714e0e057c355d31c8131
Output index: 1
ScriptSig length: 0
ScriptSig:
Sequence: fdffffff

Number of outputs: 2

--- Output 0 ---
Value (sats): 500000
scriptPubKey size: 22
Previous TXID: c1368b8e3daedf15612b0185f79f4e82df90f6bcd93714e0e057c355d31c8131
Output index: 1
ScriptSig length: 0
ScriptSig:
Sequence: fdffffff

Number of outputs: 2

--- Output 0 ---
Value (sats): 500000
scriptPubKey size: 22
scriptPubKey: 001485d78eb795bd9c8a21afefc8b6fdaedf71836809
Previous TXID: c1368b8e3daedf15612b0185f79f4e82df90f6bcd93714e0e057c355d31c8131
Output index: 1
ScriptSig length: 0
ScriptSig:
Sequence: fdffffff

Number of outputs: 2

--- Output 0 ---
Value (sats): 500000
```