Floyce Shitandi

Assignment 3: Transactions

Let's manually decode this hex:

"02000000000101 0131811cd355c357e0e01437d9bcf690df824e9ff785012b6115dfae3d8e8b36c1 01000000 00fdffffff0220a1070000000000160014 85d78eb795bd9c8a21afefc8b6fdaedf718368094c0810000000000001 60014840ab165c9c2555d4a31b9208ad806f89d2535e202 47304402207bce86d430b58bb6b79e8c1bbecdf67a530eff3bc61581a1399e0b28a741c0ee0220303d5ce926c60bf15577f2e407f28a2ef8fe8453abd4048b716e97dbb1e3a85c01 210260828bc77486a55e3bc6032ccbeda915d9494eda17b4a54dbe3b24506d40e4ff43 030e00"

i.) Version – 4 bytes
ii.) Input count – varint
iii.) Inputs – each input includes; Previous txid (32bytes), Previous output index (4 bytes), ScriptSig length(varint), ScriptSig, Sequence (4 bytes)
iv.) Output count – varint
v.) Outputs – each output includes: Value (8 bytes), ScriptPubKey length (varint), ScriptPubKey
vi.) Locktime – 4 bytes

SO;
Version(first 4 bytes)=2bits is 0200000000

Input count 01 = 1 01

Input details: Previous txid:
0131811cd355c357e0e01437d9bcf690df824e9ff785012b6115dfae3d8e8b36c1
Outout index : 01000000

Witness/script(for segwit):
a) Signature 1:
47304402207bce86d430b58bb6b79e8c1bbecdf67a530eff3bc61581a1399e0b28a741c0ee0220303d5ce926c60bf15577f2e407f28a2ef8fe8453abd4048b716e97dbb1e3a85c01
b) Public key:
210260828bc77486a55e3bc6032ccbeda915d9494eda17b4a54dbe3b24506d40e4ff43

Locktime: 030e00"

Output Count: Output count: 02 → 2 outputs

First output:

- Value: 20a1070000000000 → 500,000 satoshis

- ScriptPubKey length: 16 → 22 bytes
- ScriptPubKey: 001485d78eb795bd9c8a21afefc8b6fdaedf71836809 → P2WPKH

Second output:

- Value: 4c08100000000000 → 1,200,000 satoshis
- ScriptPubKey length: 16 → 22 bytes
- ScriptPubKey: 0014840ab165c9c2555d4a31b9208ad806f89d2535e → P2WPKH