Transaction Format

01000000018813f79011acb80925dfe69b3def355fe914bd1d96a3f5f71bf8303c6a989c7d100000000 6b483045022100ed81ff192e75a3fd2304004dcadb746fa5e24c5031ccfcf21320b0277457c98f02207a986d955c6e0cb35d446a89d3f56100f4d7f67801c31967743a9c8e10615bed01210349fc4e631e3624a545de3f89f5d8684c7b8138bd94bdd531d2e213bf016b278a ffffffff 02 a135ef0100000000 1976a914bc3b654dca7e56b04dca18f2566cdaf02e8d9ada88ac 99c3980000000000 1976a9141c4bc762dd5423e332166702cb75f40df79fea1288ac 19430600

- 01000000 - version, 4 bytes, LE
- 01 - number of inputs, varint
- 813f...d1 - prev hash, 32 bytes, LE
- 00000000 - prev index, 4 bytes, LE
- 6b48...8a - scriptSig, variable
- ffffffff - sequence, 4 bytes, LE
- 02 - number of outputs, varint
- a135ef0100000000 - value of output, 8 bytes, LE
- 1976a914...88ac - scriptPubKey, variable
- 19430600 - locktime, 4 bytes, LE

Block Format

02000020 8ec39428b17323fa0ddec8e887b4a7c53b8c0a0a220cfd0000000000000000005 b0750fce0a889502d40508d39576821155e9c9e3f5c3157f961db38fd8b25be 1e77a759 e93c0118 a4ffd71d

- 02000020 - version, 4 bytes, LE
- 8ec3...00 - previous block, 32 bytes, LE
- 5b07...be - merkle root, 32 bytes, LE
- 1e77a759 - timestamp, 4 bytes, LE
- e93c0118 - bits, 4 bytes
- a4ffd71d - nonce, 4 bytes

Compressed SEC

0349fc4e631e3624a545de3f89f5d8684c7b8138bd94bdd531d2e213bf016b278a

- 02 if y is even, 03 if odd - Marker
- 49fc...8a - x coordinate - 32 bytes

Uncompressed SEC

047211a824f55b505228e4c3d5194c1fcfaa15a456abdf37f9b9d97a4040afc073dee6c89064984f03385237d92167c13e236446b417ab79a0fcae412ae3316b77

- 04 - Marker
- 7211...73 - x coordinate - 32 bytes
- dee6...77 - y coordinate - 32 bytes

DER Signature Format

3045022100ed81ff192e75a3fd2304004dcadb746fa5e24c5031ccfcf21320b0277457c98f02207a986d955c6e0cb35d446a89d3f56100f4d7f67801c31967743a9c8e10615bed

- 30 - DER Type (always 0x30)
- 45 - Length of rest of signature
- 02 - Marker for r value
- 21 - Length of r value
- 00ed...8f - r value
- 02 - Marker for s value
- 21 - Length of s value
- 7a98...ed - s value

Network Messaging Format

F9beb4d976657273696f6e0000000000 65000000 5f1a69d2 72110100010000000000000bc8f5e54000000001000000000000000000000000000000000000ffffc61b6409208d010000000000000000000000000000000000ffffcb0071c0208d128035cbc97953f80f2f5361746f7368693a302e392e332fcf05050001

- f9beb4d9 - network magic (always 0xf9beb4d9 for mainnet)
- 76657273696f6e0000000000 - command, 12 bytes, human readable (“version”)
- 65000000 - payload length, 4 bytes, little-endian
- 5f1a69d2 - payload checksum, first 4 bytes of double-sha256 of the payload.
- 7211...01 – payload

Programming Blockchain

P2PKH scriptPubKey

76a914bc3b654dca7e56b04dca18f2566cdaf02e8d9ada88ac

- 76 - OP_DUP
- a9 - OP_HASH160
- 14 - Length of <hash>
- bc3b...da - <hash>
- 88 - OP_EQUALVERIFY
- ac - OP_CHECKSIG

P2PKH scriptSig

483045022100ed81ff192e75a3fd2304004dcadb746fa5e24c5031ccfcf21320b0277457c98f02207a986d955c6e0cb35d446a89d3f56100f4d7f67801c31967743a9c8e10615bed01210349fc4e631e3624a545de3f89f5d8684c7b8138bd94bdd531d2e213bf016b278a

- 48 - Length of <signature>
- 30...01 - <signature>
- 21 - Length of <pubkey>
- 0349...8a - <pubkey>

P2SH scriptPubKey

a91474d691da1574e6b3c192ecfb52cc8984ee7b6c5687

- a9 - OP_HASH160
- 14 - Length of <hash>
- 74d6...56 - <hash>
- 87 - OP_EQUAL

P2SH scriptSig

0048304502210 0dc92655fe37036f47756db8102e0d7d5e28b3beb83a8fef4f5dc0559bddfb94e02205a36d4e4e6c7fcd16658c50783e00c341609977aed3ad00937bf4ee942a899370148304502210 0da6bee3c93766232079a01639d07fa869598749729ae323eab8eef53577d611b02207bef15429dcadce2121ea07f233115c6f09034c0be68db99980b9a6c5e75402201475221022626e955ea6ea6d98850c994f9107b036b1334f18ca8830bfff1295d21cfdb702103b287eaf122eea69030a0e9feed096bed8045c8b98bec453e1ffac7fbdbd4bb7152ae

- 00 - OP_0
- 48 - Length of <signaturex>
- 3045...01 - <signaturex>
- 47 - Length of redeemScript
- 5221...ae - <redeemScript>

P2SH RedeemScript

5221022626e955ea6ea6d98850c994f9107b036b1334f18ca8830bfff1295d21cfdb702103b287eaf122eea69030a0e9feed096bed8045c8b98bec453e1ffac7fbdbd4bb7152ae

- 52 - OP_2
- 21 - Length of <pubkeyx>
- 0....01 - <pubkeyx>
- 52 - OP_2
- ae - OP_CHECKMULTISIG

Programming Blockchain