Bitcoin testnet

发送一个交易后得到了一个 16 进制字符串：

010000000196c472ac5cbc3cf6acae1493d4d32f119f39ec9e440176b2fb7de6e6024b9f21010000006a473044022034519a85fb5299e180865dda936c5d53edabaaf6d15cd1740aac9878b76238e002207345fcb5a62deeeb8d9d80e5b412bd24d09151c2008b7fef10eb5f13e484d1e0d01210207c9ece04a9b5ef3ff441f3aad6bb63e323c05047a820ab45ebbe61385aa7446ffffffff0140420f00000000001976a914053496c1ea3d54d649ed54de490fda342522244088ac00000000

对于这个字符串分析可以发现：

01000000 是版本号的小端格式；

01 是输入未花费的交易数量；

96c472ac5cbc3cf6acae1493d4d32f119f39ec9e440176b2fb7de6e6024b9f21 是上一笔交易的 hash，以小端格式表示；

01000000 该笔输入交易在上一笔交易输出所在的位置 output_no，小端格式；

6a 后面解锁脚本的字节数，16 进制编码；

47 PUSHDATA 47，将 47 个字节的数据压入栈中；

044022034519a85fb5299e180865dda936c5d53edabaaf6d15cd1740aac9878b76238e002207345fcb5a62deeb8d9d80e5b412bd24d09151c2008b7fef10eb5f13e484d1e0d 解锁脚本的签名部分；

01 SIGHASH_ALL 指令，为了保护签名部分不被篡改；

21 PUSHDATA 21，将 21 个字节的数据压入栈中；

0207c9ece04a9b5ef3ff441f3aad6bb63e323c05047a820ab45ebbe61385aa7446 大端格式的公钥，解锁脚本的第二部分；

Ffffffff 顺序编号，在该笔交易中为不可用。如果 locktime 为非零，则至少一笔输入交易的顺序编号必须小于 0xffffffff；

01 输出交易的数量；

40420f0000000000 交易的数额，小端格式；

19 上锁脚本（P2PKH）的大小。后面为该脚本的内容；

76 OP_DUP，上锁脚本 scriptPubKey 的一部分；

a9 OP_HASH160，上锁脚本 scriptPubKey 的一部分

14 PUSHDATA 14,将 14 个字节压入栈中，上锁脚本 scriptPubKey 的一部分；

053496c1ea3d54d649ed54de490fda3425222440 接收方公钥的哈希，其结果为 RIPEMD160(SHA256(pubkey))；

88 OP_EQUALVERIFY，上锁脚本 scriptPubKey 的一部分；

ac OP_CHECKSIG，上锁脚本 scriptPubKey 的一部分；

00000000 nLockTime，可以为 UNIX 时间戳或者区块高度。在达到这个数值之前，该笔交易不可被添加进区块。若 nLockTime 为 0 则表示该交易可以被立刻执行。