

# 实验二报告

## 实验要求

1. 生成一个涉及四方的多签名交易，这样交易可以由第一方（银行）与另外三方（客户）中的任何一方（客户）共同赎回，而不仅仅只是客户或银行。对于这个问题，你可以假设是银行的角色，这样银行的私钥就是你的私钥，而银行的公钥就是你的公钥。使用 keygen.py 生成客户密钥并将它们粘贴到 ex2a.py 中。
2. 赎回事务并确保 scriptPubKey 尽可能小。可以使用任何合法的签名组合来赎回交易至 faucet 地址，但要确保所有组合都有效。

## 脚本的设计

P2SH (Pay to Script Hash) 是最复杂的一种形式，这种形式下输出脚本给出的不是收款人的公钥的哈希，而是收款人提供的赎回脚本 (Redeem Script) 的哈希。将来要花这个输出脚本的比特币的时候，相应交易的输入脚本要给出赎回脚本的具体内容，同时还要给出让赎回脚本能正确运行所需要的签名

一般多重签名的脚本设计如下：

input script:

**x**

```
PUSHDATA (Sig_1)
PUSHDATA (Sig_2)
...
PUSHDATA (Sig_M)
```

M个签名

outputScript:

**M** 阈值M

```
PUSHDATA (pubkey_1)
PUSHDATA (pubkey_2)
...
PUSHDATA (pubkey_N)
```

N个公钥

N

CHECKMULTISIG

CSDN @通通的流浪

1. 在ex2a.py中我们必须需要银行的签名才能取出比特币，所以输出脚本中必须包含银行的公钥即“我的公钥”，然后OP\_CHECKSIGVERIFY对签名进行验证
2. 然后给出多重签名，该功能通过CHECKMULTISIG来实现，输入脚本提供M个签名，输出脚本给出N个公钥和阈值M ( $N \geq M$ )，输入脚本只需要提供N个公钥中M个合法签名就能通过验证，且给出的M个签名顺序要和N个公钥中相对顺序一致

3. 输入脚本的第一行有一个红色的X，是因为比特币中CHECKMULTISIG的实现存在一个bug，执行时会从堆栈上多弹出一个元素。这个bug现在已经无法修改，因为去中心化系统中软件升级代价极大，需要硬分叉修改。所以，实际中采用的方案是在输入脚本往栈中多压入一个无用元素OP\_0

## 关键代码

输出脚本：

```
1  ex2a_txout_scriptPubKey =  
    [CBitcoinSecret('cQdaUpxdPJodjP6z5C3iJjx35bxqv4LqexAbyv1DYtfPK48f6VeV').pub,  
     # 我即银行公钥  
2      OP_CHECKSIGVERIFY, #对银行签名的验证  
3      OP_1,              #如果银行公钥验证通过，提供一个客  
                           #户的签名验证通过即可  
4      cust1_private_key.pub,  
5      cust2_private_key.pub,  
6      cust3_private_key.pub, #三个客户的公钥  
7      OP_3,                #共三个客户  
8      OP_CHECKMULTISIG    #验证多重签名  
9  ]
```

给输出脚本的比特币数目及比特币的来源：

```
1  amount_to_send = 0.0006 #减去小费的金额  
2  txid_to_spend = (  
3      'e4b9408d2c84da043882888759fc26d10279566c652929a21bb42fcfc9018fe2') #  
    交易的哈希值  
4  utxo_index = 1
```

输入脚本：

```
1  def multisig_scriptSig(txin, txout, txin_scriptPubKey):  
2      bank_sig = create_OP_CHECKSIG_signature(txin, txout, txin_scriptPubKey,  
3                                              my_private_key)  
4      cust1_sig = create_OP_CHECKSIG_signature(txin, txout, txin_scriptPubKey,  
5                                              cust1_private_key)  
6      cust2_sig = create_OP_CHECKSIG_signature(txin, txout, txin_scriptPubKey,  
7                                              cust2_private_key)  
8      cust3_sig = create_OP_CHECKSIG_signature(txin, txout, txin_scriptPubKey,  
9                                              cust3_private_key)  
10     return [OP_0, #比特币设计的BUG，需要填入一个无效信息  
11             cust1_sig, #任意一个客户即可 因为OP_1...OP_3  
12             bank_sig #这里必须为银行签名，因为输出脚本首先填入的银行公钥  
13             ]
```

给 faucet\_address 的比特币数目及来源：

```
1  amount_to_send = 0.0001 # 减去小费的金额  
2  txid_to_spend =  
    '48e1b7c90864b11a23124f34412111344277fb7369ad7e330adee7c8cad1c10d' # 交易的哈希  
    值  
3  utxo_index = 0
```

# 交易信息

## ex2a.py

```
1  {
2    "tx": {
3      "block_height": -1,
4      "block_index": -1,
5      "hash":
6      "48e1b7c90864b11a23124f34412111344277fb7369ad7e330adee7c8cad1c10d",
7      "addresses": [
8        "mj7pdovSMDVRpze7M15neJdJ9i soHYRLw4",
9        "zA6Z3a3UjRW4bJLLbc1dHJBVEUUDaSMFwu"
10      ],
11      "total": 59999,
12      "fees": 40001,
13      "size": 306,
14      "vsize": 306,
15      "preference": "high",
16      "relayed_by": "2001:250:401:6576:5d9:761f:189b:54de",
17      "received": "2022-10-27T04:30:54.122974912Z",
18      "ver": 1,
19      "double_spend": false,
20      "vin_sz": 1,
21      "vout_sz": 1,
22      "confirmations": 0,
23      "inputs": [
24        {
25          "prev_hash":
26          "e4b9408d2c84da043882888759fc26d10279566c652929a21bb42fcfc9018fe2",
27          "output_index": 1,
28          "script":
29          "47304402200f37e217ae1b2900d836e922d22ba4bda14ebd1d8bc8de7a93cc47b402fe2d140
30          2203ae40f744acdbdc934c3b21abddb7e5cd9a5c25314acb287f53bd276e9b1e701210317d
31          a3c63dd5caad766989c78491c20e490fad03b8675f816895d6b03a9eb47fc",
32          "output_value": 100000,
33          "sequence": 4294967295,
34          "addresses": [
35            "mj7pdovSMDVRpze7M15neJdJ9i soHYRLw4"
36          ],
37          "script_type": "pay-to-pubkey-hash",
38          "age": 2350347
39        }
40      ],
41      "outputs": [
42        {
43          "value": 59999,
44          "script":
45          "210317da3c63dd5caad766989c78491c20e490fad03b8675f816895d6b03a9eb47fcad51210
46          34913464f642c7e677e10cf69422514320c13fed1e7832c2e90f51ceb3d3a324c210337d3cc0
47          dd6f2202e0e2b42934f62c0672e44c55bd05ad60ec21ebad794c07f122103be6aed4392755d
48          a5c7c5e36fb4c6e9140bd036f48cf051ddc27be68d8b5266653ae",
49          "addresses": [
50            "zA6Z3a3UjRW4bJLLbc1dHJBVEUUDaSMFwu"
51          ],
52          "script_type": "pay-to-multi-pubkey-hash"
```

```

44     }
45   ]
46 }
47 }

```

## ex2b.py

```


1  {
2    "tx": {
3      "block_height": -1,
4      "block_index": -1,
5      "hash":
6      "05b208f29b26ed481ed9d354beba9f75ef617855a1dcac1c978472a1c86995b3",
7      "addresses": [
8        "zA6Z3a3UjRW4bJLLbc1dHJBVEUUDaSMFwu",
9        "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUTFB"
10     ],
11     "total": 10000,
12     "fees": 49999,
13     "size": 230,
14     "vsize": 230,
15     "preference": "high",
16     "relayed_by": "2001:250:401:6576:5d9:761f:189b:54de",
17     "received": "2022-10-27T05:00:18.599207763Z",
18     "ver": 1,
19     "double_spend": false,
20     "vin_sz": 1,
21     "vout_sz": 1,
22     "confirmations": 0,
23     "inputs": [
24       {
25         "prev_hash":
26         "48e1b7c90864b11a23124f34412111344277fb7369ad7e330adee7c8cad1c10d",
27         "output_index": 0,
28         "script":
29         "0047304402200218d6ad1f968f3b357a763aaf963d4d141f5a488e0bb985af28d5831e4aaca
30         1022073f20355e9168ee6d2ad0f693731548c82519811ab0341deb21ddbbd50e36b940147304
31         4022071e34da219aa094873fae5f9b4151a639e54314ccc0d4fe2c698d835ae376c5402206b6
32         9832ef435634c73b765f7cb2e7e39a7032fe5702d89da564d8c93b1cbd29f01",
33         "output_value": 59999,
34         "sequence": 4294967295,
35         "addresses": [
36           "zA6Z3a3UjRW4bJLLbc1dHJBVEUUDaSMFwu"
37         ],
38         "script_type": "pay-to-multi-pubkey-hash",
39         "age": 2378320
40       }
41     ],
42     "outputs": [
43       {
44         "value": 10000,
45         "script": "76a9149f9a7abd600c0caa03983a77c8c3df8e062cb2fa88ac",
46         "addresses": [
47           "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUTFB"
48         ],
49         "script_type": "pay-to-pubkey-hash"
50       }
51     ]
52   }
53 }

```

```
45 | ]
46 | }
47 | }
```

## 交易截图

### ex2a.py

 **BLOCKCYPHER**

BTC Testnet Address, transaction or block

48e1b7c90864b11a23124f34412111344277fb7369ad7e330adee7c8cad1c10d

57 confirmations.  
Anything over 6 confirmations is considered completed and irreversible.

AMOUNT TRANSACTED <b>0.00059999 BTC</b>	FEES <b>0.00040001 BTC</b>	RECEIVED <b>about 13 hours ago</b>	CONFIRMATIONS <b>6+</b>
--------------------------------------------	-------------------------------	---------------------------------------	----------------------------

Advanced Details

Details

1 Input Consumed


0.001 BTC from  
mj7pdovSMDVRpze7M15neJdJ9isoHYRLw4 (output)

...

1 Output Created

0.00059999 BTC to  
zA6Z3a3UjRW4bJLLbc1dHJBVEUUDaSMFwu (spent)

### ex2b.py

 **BLOCKCYPHER**

BTC Testnet Address, transaction or block

Bitcoin Testnet Transaction  
05b208f29b26ed481ed9d354beba9f75ef617855a1dcac1c978472a1c86995b3

55 confirmations.  
Anything over 6 confirmations is considered completed and irreversible.

AMOUNT TRANSACTED <b>0.0001 BTC</b>	FEES <b>0.00049999 BTC</b>	RECEIVED <b>about 13 hours ago</b>	CONFIRMATIONS <b>6+</b>
----------------------------------------	-------------------------------	---------------------------------------	----------------------------

Advanced Details

Details

1 Input Consumed

0.00059999 BTC from  
zA6Z3a3UjRW4bJLLbc1dHJBVEUUDaSMFwu (output)

...

1 Output Created

0.0001 BTC to  
mv4rnyY3Su5gjcDNzbMLKBQkBiCtHUtFB (unspent)

