区块链第三次实验报告

2013536 汤清云

【实验目标】

1. 生成一个可以由以下线性方程组的解赎回的交易：

X+y=2013
x-y=535

此处由于我学号的前四位和后三位奇偶性不同，故修改为 2013535

2. 赎回交易。赎回脚本应尽可能小。

【实验过程】

由于之前分发的币已经用完了，所以新申请了一个地址用于本次实验。

Private key: cVWrNVeTWPG5HKEz2G3AwJV5j9ABuupcREWhBcF1t7seNWbtjucF
Address: mnbt1BdPdS2VyMbqo5s2YUqdZfUv8EC4wz
分币 hash：1641fe39ff2bd4873c27eb6710f4d6bd426ab249e6e473660533cf73a300f318

1. 加锁脚本：

```
3
9   ###########################################################################
9   # TODO: Complete the scriptPubKey implementation for Exercise 3
L   # OP_2DUP:用于将x和y压栈赋值
2   # OP_ADD:计算x+y
3   # OP_QUALVERIFY: 计算相加结果是否为2013
4   # OP_SUB: 计算x-y
5   # OP_EQUAL: 验证是否为空，true则为非空
5   ex3a_txout_scriptPubKey = [OP_2DUP,OP_ADD,2013,OP_EQUALVERIFY,OP_SUB,535,OP_EQUAL]
7   ###########################################################################
```

```
19
20  #学号为2013536，为保证奇偶性，修改为2013535
21  if __name__ == '__main__':
22      ###########################################################################
23      # TODO: set these parameters correctly
24      amount_to_send = 0.0007 #设置分发金额为0.0007
25      txid_to_spend = (
26          '1641fe39ff2bd4873c27eb6710f4d6bd426ab249e6e473660533cf73a300f318')
27      utxo_index = 0 #使用新币的第一份输出
28      ###########################################################################
29
30      response = send_from_P2PKH_transaction(#调用ex1中的函数
31          amount_to_send, txid_to_spend, utxo_index,
32          ex3a_txout_scriptPubKey)
33      print(response.status_code, response.reason)
34      print(response.text)
35
```

运行结果：

```
201 Created
{
   "tx": {
      "block_height": -1,
      "block_index": -1,
      "hash":
"f82794d61fa1556ad3a56b6be3aba1bedc4567b5faf058e956e96a06254d940b",
      "addresses": [
         "mnbt1BdPdS2VyMbqo5s2YUqdZfUv8EC4wz"
      ],
      "total": 70000,
      "fees": 55000,
      "size": 177,
      "vsize": 177,
      "preference": "high",
      "relayed_by": "2001:250:401:6560:20c9:315:8525:fc9f",
      "received": "2022-11-09T07:18:36.749155664Z",
      "ver": 1,
      "double_spend": false,
      "vin_sz": 1,
      "vout_sz": 1,
      "confirmations": 0,
      "inputs": [
         {
            "age": 2405348
         }
      ],       "outputs": [
         {
            "value": 70000,
            "script": "6e9302dd07889402170287",
            "addresses": null,
            "script_type": "unknown"
         }
      ]
   }
}
```


结果为：

f82794d61fa1556ad3a56b6be3aba1bedc4567b5faf058e956e96a06254d940b

AMOUNT TRANSACTED

0.0007 BTC

FEES

0.00055 BTC

RECEIVED

a day ago

CONFIRMATIONS

6+

Advanced Details

2. 解锁脚本

```
8
9
10  ##############################################################################
11  # TODO: set these parameters correctly
12  amount_to_send = 0.0004 #赎回金额
13  # 加锁脚本的输出
14  txid_to_spend = 'f82794d61fa1556ad3a56b6be3aba1bedc4567b5faf058e956e96a06254d940b'
15  utxo_index = 0
16  ##############################################################################
17
18  txin_scriptPubKey = ex3a_txout_scriptPubKey
19  ##############################################################################
20  # TODO: implement the scriptSig for redeeming the transaction created
21  # in  Exercise 3a.
22  # 解方程组可以得出x=1274 y=739
23  txin_scriptSig = [1274,739]
24  ##############################################################################
25  txout scriptPubKey = P2PKH scriptPubKey(faucet address)
```

运行结果：

201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
"afb9098d23cc40ad5b340be808e004014c6b3692c3eb08aa3af5b7600cb67f6d",
    "addresses": [
      "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"
    ],
    "total": 40000,
    "fees": 30000,
    "size": 91,
    "vsize": 91,
    "preference": "high",
    "relayed_by": "2001:250:401:6560:20c9:315:8525:fc9f",
    "received": "2022-11-09T08:08:26.690993535Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"f82794d61fa1556ad3a56b6be3aba1bedc4567b5faf058e956e96a06254d940b",
        "script":
"76a9149f9a7abd600c0caa03983a77c8c3df8e062cb2fa88ac",

```
            "addresses": [
                "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"
            ],
            "script_type": "pay-to-pubkey-hash"
        }
    ]
  }
}
```

结果为：

afb9098d23cc40ad5b340be808e0
04014c6b3692c3eb08aa3af5b760
0cb67f6d

AMOUNT TRANSACTED

0.0004 BTC

FEES

0.0003 BTC

RECEIVED

a day ago

CONFIRMATIONS

6+

Advanced Details