BlockChain Ex3

2011269 王楠舟 计算机科学与技术

练习实现步骤

ex3a.py 赎回脚本的实现

```
ex3a_txout_scriptPubKey = [OP_2DUP,
                        OP_ADD,
                        2011,
                        OP_EQUALVERIFY,
                        OP_SUB,
                        269 ,
                        OP_EQUAL]
```

首先`OP_2DUP`命令将栈顶的两个元素分别复制一次，即将栈内的`[x,y]`复制为`[x,y,x,y]`，然后使用`OP_ADD`命令计算`x+y`，验证与我学号的前四位`2011`是否相等，由于不想验证完就退出，所以使用`OP_EQUALVERIFY`；随后用`OP_SUB`命令计算`x-y`的结果，验证和我的学号后三位`269`是否相等，验证完毕就退出，所以使用`OP_EQUAL`.

ex3b.py 解锁脚本的实现

解锁脚本需要做的就是将`x,y`放入栈中，求解`x,y`：

$$x+y=2011, x-y=269$$
$$x=1140, y=871$$

所以解锁脚本为：

```
txin_scriptSig = [1140,871]
```

完整赎回过程

```
NULL        |空栈
<1140> <871>        |x,y入栈
<1140> <871> <1140> <871>       |OP_2DUP执行，复制栈顶两个元素
<1140> <871> <2011>     |OP_ADD执行，1140+871
<1140> <871> <2011> <2011>      |2011入栈
<1140> <871>        |OP_EQUALVERIFY验证成功
<269>       |OP_SUB执行，1140-871
<269> <269>     |269入栈
true        |OP_EQUAL验证成功，返回true
```

交易信息输出

ex3a.py输出：

```
201 Created
```

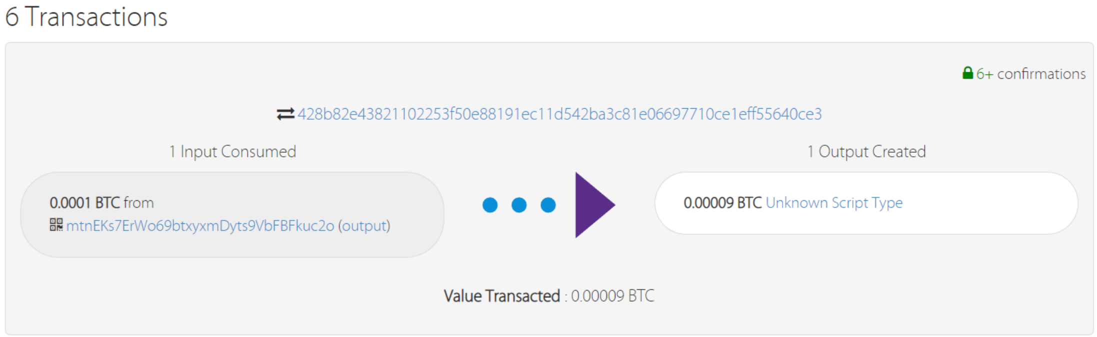
```
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "428b82e43821102253f50e88191ec11d542ba3c81e06697710ce1eff55640ce3",
    "addresses": [
      "mtnEKs7ErWo69btxyxmDyts9VbFBFkuc2o"
    ],
    "total": 9000,
    "fees": 1000,
    "size": 178,
    "vsize": 178,
    "preference": "low",
    "relayed_by": "2001:250:401:6554:f8a1:2d48:f2c7:973e",
    "received": "2022-11-11T15:51:10.003184652Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"0502ee78cda2cb28402348179afc35c4e142cb6bea8e8788e930e25b8e270318",
        "output_index": 3,
        "script":
"483045022100b4196d703aa7fc528d91bcd334aa67dddf276b2fafdc2bde6cfe48ff964588d8022
07e20b35ac11a8643f7015dddc73cab09113bb09752572bbfbdb06bfd81232380012102677de4251
8a760c1a12707a6103d05f4b4c60e5993c7cac98a53594cf7589c4a",
        "output_value": 10000,
        "sequence": 4294967295,
        "addresses": [
          "mtnEKs7ErWo69btxyxmDyts9VbFBFkuc2o"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2360928
      }
    ],
    "outputs": [
      {
        "value": 9000,
        "script": "6e9302db078894020d0187",
        "addresses": null,
        "script_type": "unknown"
      }
    ]
  }
}
```

ex3b.py输出:

```
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "0b62b24b554d6a8519441a3247aa880a8b45e9d48b0f849ae64c575be4ea520b",
    "addresses": [
      "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"
    ],
    "total": 8000,
    "fees": 1000,
    "size": 91,
    "vsize": 91,
    "preference": "low",
    "relayed_by": "2001:250:401:6554:f8a1:2d48:f2c7:973e",
    "received": "2022-11-11T15:52:49.886360138Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"428b82e43821102253f50e88191ec11d542ba3c81e06697710ce1eff55640ce3",
        "output_index": 0,
        "script": "027404026703",
        "output_value": 9000,
        "sequence": 4294967295,
        "script_type": "unknown",
        "age": 0
      }
    ],
    "outputs": [
      {
        "value": 8000,
        "script": "76a9149f9a7abd600c0caa03983a77c8c3df8e062cb2fa88ac",
        "addresses": [
          "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}
```

交易截图

ex3a.py 交易截图：



6 Transactions

🔒 6+ confirmations

⇄ 428b82e43821102253f50e88191ec11d542ba3c81e06697710ce1eff55640ce3

1 Input Consumed

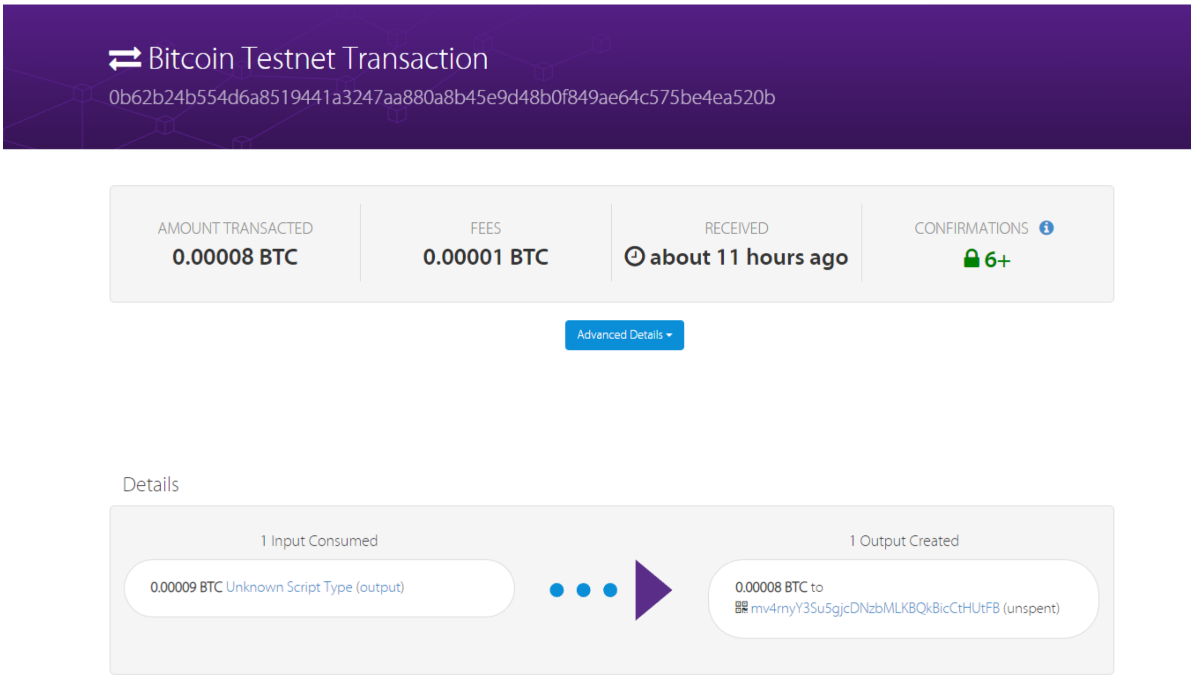
0.0001 BTC from
mtnEKs7ErWo69btxyxmDyts9VbFBFkuc2o (output)

1 Output Created

0.00009 BTC Unknown Script Type

Value Transacted : 0.00009 BTC

ex3b.py 交易截图：



⇄ Bitcoin Testnet Transaction

0b62b24b554d6a8519441a3247aa880a8b45e9d48b0f849ae64c575be4ea520b

AMOUNT TRANSACTED	FEES	RECEIVED	CONFIRMATIONS
0.00008 BTC	0.00001 BTC	about 11 hours ago	🔒 6+

Details

1 Input Consumed

0.00009 BTC Unknown Script Type (output)

1 Output Created

0.00008 BTC to
mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB (unspent)