

区块链基础及应用实验报告

Ex3

网络空间安全学院 信息安全专业

2112492 刘修铭 0939

https://github.com/lxmliu2002/Blockchain_Fundamentals_and_Applications

Ex3a

1. 接着补全代码，构建一个交易输出锁定脚本，完成交易要求。

```
1 | ex3a_txout_scriptPubKey = [OP_2DUP, OP_ADD, 211, OP_EQUALVERIFY, OP_SUB,
  | 2491, OP_EQUAL]
```

- `OP_2DUP`：是一个比特币脚本操作码，复制堆栈顶部的两个元素到堆栈的顶部
- `OP_ADD`：将堆栈顶部的两个元素相加，并将结果推送到堆栈中
- `211`：Student ID 的前 3 位，用于设定 $x + y$ 的值
- `OP_EQUALVERIFY`：比较堆栈顶部的两个元素是否相等，如果相等，则继续执行下一步操作，否则终止交易
- `OP_SUB`：从堆栈顶部弹出两个元素，并计算它们的差，然后将结果推送到堆栈中
- `2491`：Student ID 的后 4 位（为了确保存在整数解，此处进行必要调整，将后4位顺序减1），用于设定 $x - y$ 的值
- `OP_EQUAL`：比较堆栈顶部的两个元素是否相等，如果相等，则返回 `True`，否则返回 `False`

2. 填写好交易信息。

```
1 | amount_to_send = 0.0016
2 | txid_to_spend = (
3 |     '8b89b2517a25e6694b17c52b2f37d595578911c928a9434aeb79ecbe7d976d')
4 | utxo_index = 9
```

3. 输出信息

```
1 | 201 Created
2 | {
3 |     "tx": {
4 |         "block_height": -1,
5 |         "block_index": -1,
6 |         "hash":
7 |         "68719817237b46515327783346409064f6ba1e273b8e03e74bed0c4784b783be",
8 |         "addresses": [
9 |             "mm73YFJZTM4wDuAeogx1mxarP1gAday9E5"
```

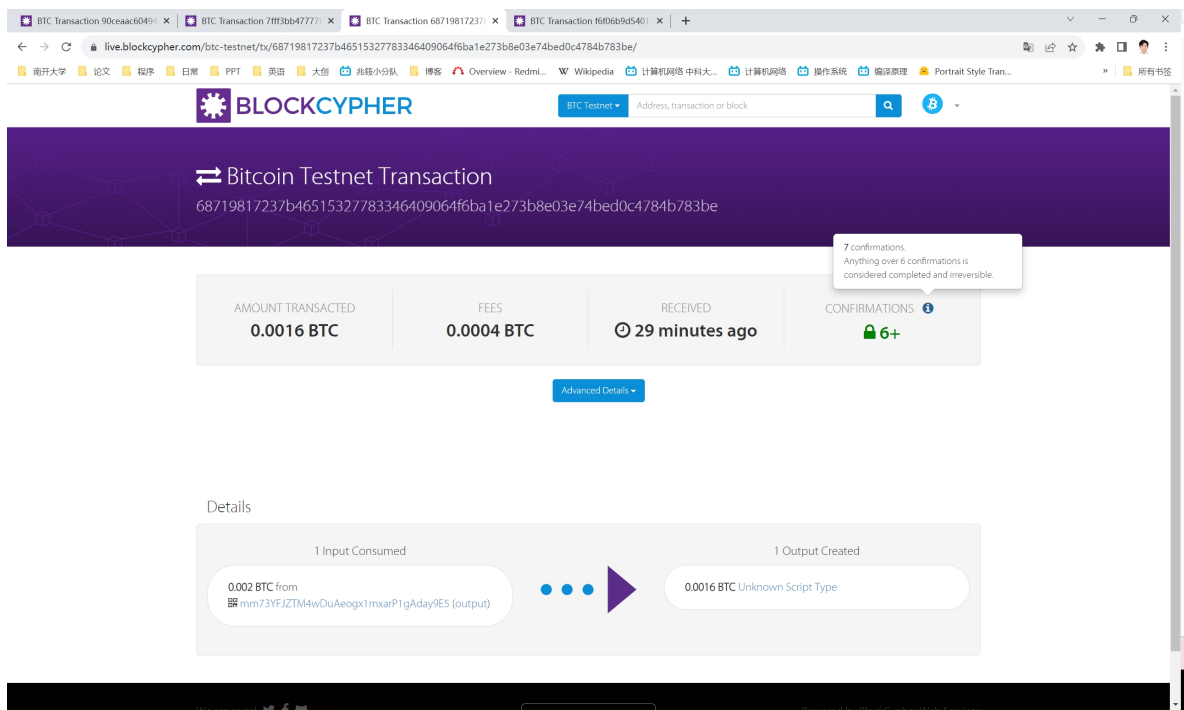
```

9      ],
10     "total": 160000,
11     "fees": 40000,
12     "size": 177,
13     "vsize": 177,
14     "preference": "high",
15     "relayed_by": "103.20.198.138",
16     "received": "2023-10-10T02:21:51.540414988Z",
17     "ver": 1,
18     "double_spend": false,
19     "vin_sz": 1,
20     "vout_sz": 1,
21     "confirmations": 0,
22     "inputs": [
23       {
24         "prev_hash":
25         "8b89b2517a25e6694b17c52b2f37d595578911c928a9434aebea79ecbe7d976d",
26         "output_index": 9,
27         "script":
28         "4730440220048f30578aba19e5f6fc22d97351316826a2b641dc7c3f81ec3c4863aa6947c5
29         022038e290d850795e46c46329a53218fe32d0aa316fe817c0f751b5a3e2856cdbc9012103c
30         85c1570a642c8f4eefac761bd3b62e6eae034290a80eb5b4f78bfbe13bd3502",
31         "output_value": 200000,
32         "sequence": 4294967295,
33         "addresses": [
34           "mm73YFJZTM4wDuAeogx1mxarP1gAday9E5"
35         ],
36         "script_type": "pay-to-pubkey-hash",
37         "age": 2505212
38       }
39     ],
40     "outputs": [
41       {
42         "value": 160000,
43         "script": "6e9302d300889402bb0987",
44         "addresses": null,
45         "script_type": "unknown"
46       }
47     ]
48   }
49 }

```

4. faucet截图

<https://live.blockcypher.com/btc-testnet/tx/68719817237b46515327783346409064f6ba1e273b8e03e74bed0c4784b783be/>



Ex3b

1. 补全解锁交易输出的解锁脚本。

- 按照前面设定，这两个数值需要满足

$$\begin{cases} x + y = 211 \\ x - y = 2491 \end{cases}$$

- 经过计算可以得到

$$\begin{cases} x = 1351 \\ y = -1140 \end{cases}$$

- 将上面两个值作为参数传入，用作锁定脚本中的条件的数据

```
1 | txin_scriptsig = [1351, -1140]
```

2. 填写好交易信息。

```
1 | amount_to_send = 0.0013
2 | txid_to_spend =
  | '68719817237b46515327783346409064f6ba1e273b8e03e74bed0c4784b783be'
3 | utxo_index = 0
```

3. 输出信息

```
1 | 201 Created
```

```

2 {
3   "tx": {
4     "block_height": -1,
5     "block_index": -1,
6     "hash":
7     "f6f06b9d54014afe1c127e8653e5bcc728765feb43df2e8f88f9f3953752a681",
8     "addresses": [
9       "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHutFB"
10    ],
11    "total": 130000,
12    "fees": 30000,
13    "size": 91,
14    "vsize": 91,
15    "preference": "high",
16    "relayed_by": "103.20.198.138",
17    "received": "2023-10-10T02:26:12.190162639Z",
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        "68719817237b46515327783346409064f6ba1e273b8e03e74bed0c4784b783be",
27        "output_index": 0,
28        "script": "024705027484",
29        "output_value": 160000,
30        "sequence": 4294967295,
31        "script_type": "unknown",
32        "age": 2531663
33      }
34    ],
35    "outputs": [
36      {
37        "value": 130000,
38        "script": "76a9149f9a7abd600c0caa03983a77c8c3df8e062cb2fa88ac",
39        "addresses": [
40          "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHutFB"
41        ],
42        "script_type": "pay-to-pubkey-hash"
43      }
44    ]
45  }
46 }

```

4. faucet截图

<https://live.blockcypher.com/btc-testnet/tx/f6f06b9d54014afe1c127e8653e5bcc728765feb43df2e8f88f9f3953752a681/>

BTC Transaction 90ceaac6049

BTC Transaction 7ff3bb47777

BTC Transaction 68719817237

BTC Transaction f6f06b9d54014afe1c127e8653e5bcc728765feb43df2e8f88f9f3953752a681

live.blockcypher.com/btc-testnet/bx/f6f06b9d54014afe1c127e8653e5bcc728765feb43df2e8f88f9f3953752a681/

南开大学

论文

程序

日常

PPT

英语

大创

兆级小分队

博客

Overview - Redmi...

Wikipedia

计算机网络 中科大...


计算机网络

操作系统

编译原理


Portrait Style Tran...


所有书签


BLOCKCYPHER

BTC Testnet

Address, transaction or block





Bitcoin Testnet Transaction

f6f06b9d54014afe1c127e8653e5bcc728765feb43df2e8f88f9f3953752a681


AMOUNT TRANSACTED

0.0013 BTC


FEES

0.0003 BTC

RECEIVED

 23 minutes ago

CONFIRMATIONS

 6+


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

Advanced Details


Details

1 Input Consumed




0.0016 BTC Unknown Script Type (output)



1 Output Created

0.0013 BTC to  mv4mryY35u5gjcDNzbMLKBQk8icCtHUF8 (unspent)

We are social

Fork me on GitHub

Powered by [BlockCypher Web Services](#)
© 2023 - BlockCypher