

Lab4 跨链原子交易

郭坤昌 2012522 计算机科学与技术

前期准备

1. 为 Alice 和 Bob 创建 BTC testnet 密钥。你可以用 keygen.py 生成密钥，把它填入 keys.py 中合适的地方。

Alice BTC testnet 私钥和地址：

```
1 Private key: cSX3H7ZTGKSgBmWsuUSFtKobUDaKzMMXqzhzHeD98qpi1qM4rtUf
2 Address: mf1qoZPUQTrNpSHCCMW5K7tRpZ6QDEsLe
```

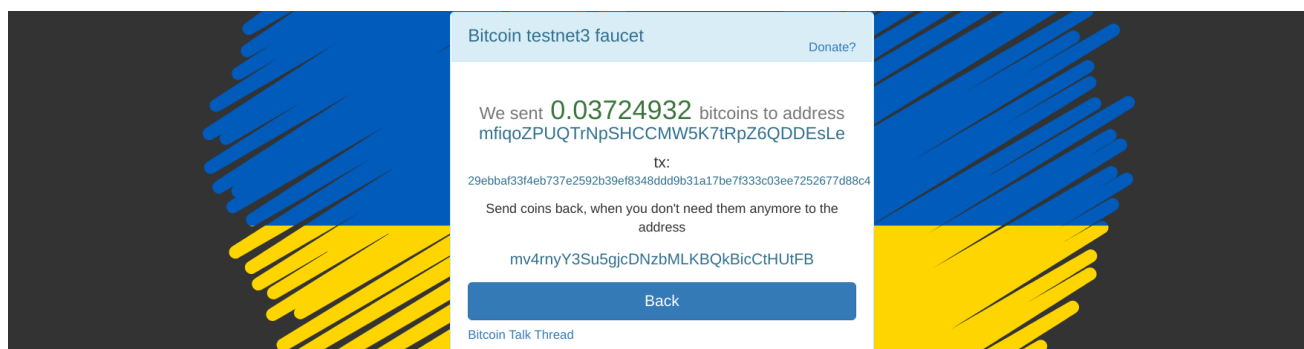
Bob BTC testnet 私钥和地址：

```
1 Private key: cSoUGtb4DFNCZ5BRg3m4BWuv4U8tc19nW8V8Kwy73SWXnfjsR4Nc
2 Address: miQKwKQ1TwJ7uxaRj7U1aB9hrruTNQzD4F
```

2. 2 在Project1 中相同的 coinfaucet 上，<https://coinfaucet.eu/en/btc-testnet/>，为 Alice 的 BTC 地址领取测试币。

为 Alice 的 BTC 地址领取测试币：

```
1 tx: 29ebbf33f4eb737e2592b39ef8348ddd9b31a17be7f333c03ee7252677d88c4
2 bitcoin: 0.03724932
```



确认的结果：

Bitcoin Testnet Transaction

29ebbf33f4eb737e2592b39ef8348ddd9b31a17be7f333c03ee7252677d88c4

AMOUNT TRANACTED
61.64575526 BTC

FEES
0.00014997 BTC

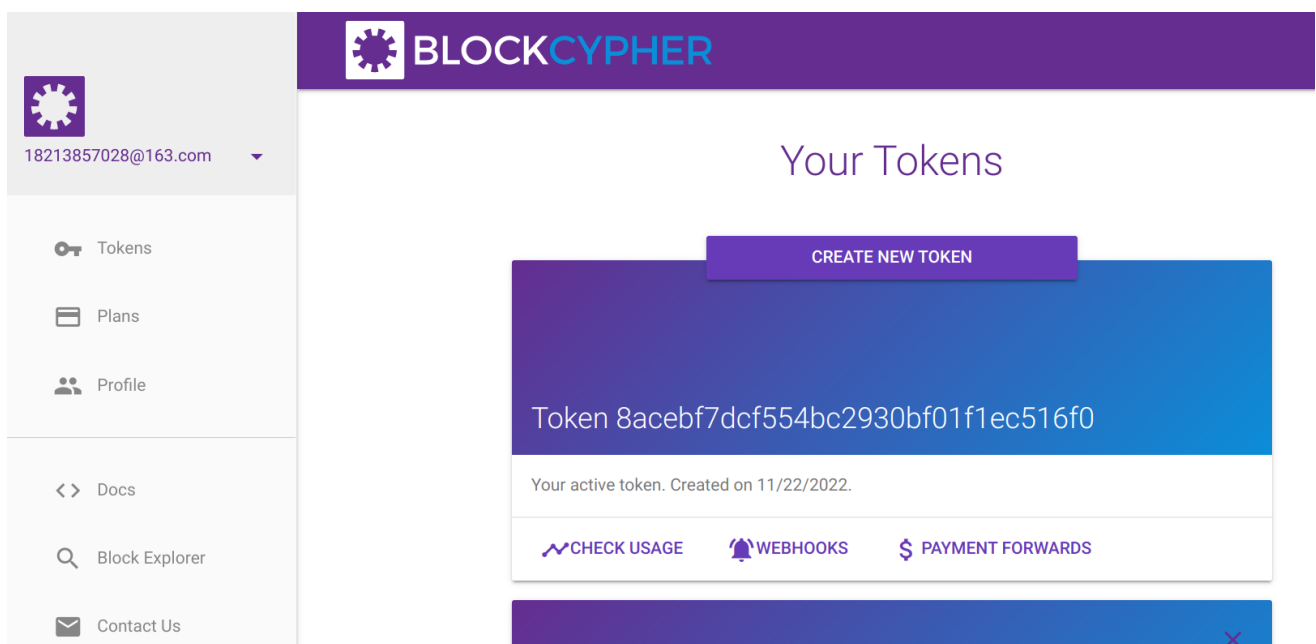
RECEIVED
🕒 about 5 hours ago

CONFIRMATIONS ⓘ
🔒 6+

3. 1 在 Blockcypher 注册帐户以获取 API token:
<https://accounts.blockcypher.com/>。

在 Blockcypher 领取 API token:

```
1 token: 8acebf7dcf554bc2930bf01f1ec516f0
```



3. 2为 Alice 和 Bob 创建 BCY testnet 密钥并填入 keys.py.

`curl -X POST https://api.blockcypher.com/v1/bcy/test/addr?token=8acebf7dcf554bc2930bf01f1ec516f0`

为Alice创建 BCY testnet 密钥:

```
1 {  
2   "private":  
3     "30d71b25d368dbe532c30063cc38d59e7f1f10fcdfbc8c263e414072877d62b2",  
4   "public":  
5     "027eceaaf3478800216099ad300b79f1e0da56f0669760e105b43a9b7a9952b5ea",  
6   "address": "C2RT1LaD9EH1xdaJqtaoRoAMvxKYJQVNKD",  
7   "wif": "BpxyCqxbr1ixqDkjMpeRuqn5diHP1Kai9bMYMXEDabcb7fCSx6rK"  
8 }
```

```
(blockchain) bill@bill-Lenovo-V15-IWL:~/Desktop/blockchain/lab4/program$ curl -X POST https://api.blockcypher.com/v1/bcy/test/addrs?token=8acebf7dcf554bc2930bf01f1ec516f0
{
  "private": "30d71b25d368dbe532c30063cc38d59e7f1f10fcafbcb8c263e414072877d62b2",
  "public": "027eceaaf3478800216099ad300b79f1e0da56f0669760e105b43a9b7a9952b5ea",
  "address": "C2RT1LaD9EH1xdaJqtaoRoAMvxKYJQVVKD",
  "wif": "BpxyCqxbrlixqDKjMpeRuqn5diHP1Kai9bMYMXEDabcb7fCSx6rK"
}(blockchain) bill@bill-Lenovo-V15-IWL:~/Desktop/blockchain/lab4/program$
```

为 Bob 创建 BCY testnet 密钥:

```
1 {
2   "private":
3     "6be882f8746c8ea3bbe9dc15d2c694fd8b75d433c6265dd70558e165849a7200",
4   "public":
5     "0303a04978f9c2d45754c7b9fe7e68f8de8d0636327c62e083ff4edab89e529e2b",
6   "address": "C3Te5ctMDdNAbDyVUCDxWyNPqhrRKnoPJ3",
7   "wif": "BrwnnrXuAX1uFwJTgYUfsKKJ6g2trrBahAHmkNoH8d2Gp4URtPSF"
8 }
```

```
(blockchain) bill@bill-Lenovo-V15-IWL:~/Desktop/blockchain/lab4/program$ curl -X POST https://api.blockcypher.com/v1/bcy/test/addrs?token=8acebf7dcf554bc2930bf01f1ec516f0
{
  "private": "6be882f8746c8ea3bbe9dc15d2c694fd8b75d433c6265dd70558e165849a7200",
  "public": "0303a04978f9c2d45754c7b9fe7e68f8de8d0636327c62e083ff4edab89e529e2b",
  "address": "C3Te5ctMDdNAbDyVUCDxWyNPqhrRKnoPJ3",
  "wif": "BrwnnrXuAX1uFwJTgYUfsKKJ6g2trrBahAHmkNoH8d2Gp4URtPSF"
}(blockchain) bill@bill-Lenovo-V15-IWL:~/Desktop/blockchain/lab4/program$
```


3. 3在 Blockcypher 测试网 (BCY) 上为 Bob 的 BCY 地址领取测试币。

```
curl -d '{"address": "C3Te5ctMDdNAbDyVUCDxWyNPqhrRKnoPJ3", "amount": 1000000}'
https://api.blockcypher.com/v1/bcy/test/faucet?token=8acebf7dcf554bc2930bf01f1ec516f0
```

```
1 {
2   "tx_ref":
3     "3bfd0066036316bb2c88ff4c9346acd236f4254d70d43b574406422fcc4e0efd"
4 }
```




```
V15-IWL:~/Desktop/blockchain/lab4/program$ curl -d '{"address": "C3Te5ctMDdNAbDyVUCDxWyNPqhrRKnoPJ3", "amount": 1000000}' https://api.blockcypher.com/v1/bcy/test/faucet?token=8acebf7dcf554bc2930bf01f1ec516f0
{
  "tx_ref": "3bfd0066036316bb2c88ff4c9346acd236f4254d70d43b574406422fcc4e0efd"
}(blockchain) bill@bill-Lenovo-V15-IWL:~/Desktop/blockchain/lab4/program$
```

查询得到确认结果:



BlockCypher Testnet Transaction

3bfd0066036316bb2c88ff4c9346acd236f4254d70d43b574406422fcc4e0efd

AMOUNT TRANSACTED	FEES	RECEIVED	CONFIRMATIONS 
12.4999 BCY	0.0001 BCY	 4 days ago	 6+

4. 使用 split_test_coins.py (填写文件中的相关字段) 划分领取的币。

划分Alice 在 BTC 地址领取到的币

```
my_private_key = CBitcoinSecret('cSX3H7ZTGKSgBmWsuUSFtKobUDaKzMMXqzhzHeD98qpi1qM4rtUf')

my_public_key = my_private_key.pub
my_address = P2PKHBitcoinAddress.from_pubkey(my_public_key)

amount_to_send = 0.035 # amount of BTC in the output you're splitting minus fee
txid_to_spend = (
    '29ebbafe33f4eb737e2592b39ef8348ddd9b31a17be7f333c03ee7252677d88c4')
utxo_index = 0
n = 10 # number of outputs to split the input into
network = 'btc-test3' # either 'btc-test3' or 'bcy-test'
```

输出为

```
1 201 Created
2 {
3   "tx": {
4     "block_height": -1,
5     "block_index": -1,
6     "hash":
7       "783f4016bee7afdd479902e15b031a02077eb7a772293d731352e0bc4d5197e1",
8     "addresses": [
9       "mfiqozPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
10    ],
11    "total": 3500000,
12    "fees": 224932,
13    "size": 498,
14    "vsize": 498,
15    "preference": "high",
16    "relayed_by": "2001:250:401:6561:64cc:4fde:81b0:5543",
17    "received": "2022-11-26T09:36:26.477039933Z",
18    "ver": 1,
19    "double_spend": false,
20    "vin_sz": 1,
21    "vout_sz": 10,
22    "confirmations": 0,
23    "inputs": [
24      {
25        "prev_hash":
26          "29ebbafe33f4eb737e2592b39ef8348ddd9b31a17be7f333c03ee7252677d88c4",
27        "output_index": 0,
28        "script":
29          "483045022100811925859b1a7955e46337136ce5d0766a10e4749dc2a7b55ef5d44
30          f7735e9a502204ab47566dfb19f47f9f1df2e82d65eabe052c8ee54e5a3c281c6688
31          5f5bc8a4e0121033c562727bb2136198d74e25b13c0966a8b109c8dd42dcf9d150dd
32          66b34140e3a",
33        "output_value": 3724932,
34        "sequence": 4294967295,
```

```

29     "addresses": [
30         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
31     ],
32     "script_type": "pay-to-pubkey-hash",
33     "age": 2408351
34 }
35 ],
36 "outputs": [
37     {
38         "value": 350000,
39         "script":
40 "76a914023f92a8a3f687e082b5e6c8e072fdbe0411620b88ac",
41         "addresses": [
42             "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
43         ],
44         "script_type": "pay-to-pubkey-hash"
45     },
46     {
47         "value": 350000,
48         "script":
49 "76a914023f92a8a3f687e082b5e6c8e072fdbe0411620b88ac",
50         "addresses": [
51             "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
52         ],
53         "script_type": "pay-to-pubkey-hash"
54     },
55     {
56         "value": 350000,
57         "script":
58 "76a914023f92a8a3f687e082b5e6c8e072fdbe0411620b88ac",
59         "addresses": [
60             "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
61         ],
62         "script_type": "pay-to-pubkey-hash"
63     },
64     {
65         "value": 350000,
66         "script":
67 "76a914023f92a8a3f687e082b5e6c8e072fdbe0411620b88ac",
68         "addresses": [
69             "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
70         ],
71         "script_type": "pay-to-pubkey-hash"
72     },
73     {
74         "value": 350000,
75         "script":
76 "76a914023f92a8a3f687e082b5e6c8e072fdbe0411620b88ac",
77         "addresses": [


```

```




73         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
74     ],
75     "script_type": "pay-to-pubkey-hash"
76 },
77 {
78     "value": 350000,
79     "script":
80     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
81     "addresses": [
82         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
83     ],
84     "script_type": "pay-to-pubkey-hash"
85 },
86 {
87     "value": 350000,
88     "script":
89     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
90     "addresses": [
91         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
92     ],
93     "script_type": "pay-to-pubkey-hash"
94 },
95 {
96     "value": 350000,
97     "script":
98     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
99     "addresses": [
100         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
101     ],
102     "script_type": "pay-to-pubkey-hash"
103 },
104 {
105     "value": 350000,
106     "script":
107     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
108     "addresses": [
109         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
110     ],
111     "script_type": "pay-to-pubkey-hash"
112 },
113 {
114     "value": 350000,
115     "script":
116     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
117     "addresses": [
118         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
119     ],
120     "script_type": "pay-to-pubkey-hash"
121 },
122 {
123     "value": 350000,
124     "script":
125     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
126     "addresses": [
127         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
128     ],
129     "script_type": "pay-to-pubkey-hash"
130 },
131 {
132     "value": 350000,
133     "script":
134     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
135     "addresses": [
136         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
137     ],
138     "script_type": "pay-to-pubkey-hash"
139 },
140 {
141     "value": 350000,
142     "script":
143     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
144     "addresses": [
145         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
146     ],
147     "script_type": "pay-to-pubkey-hash"
148 },
149 {
150     "value": 350000,
151     "script":
152     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
153     "addresses": [
154         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
155     ],
156     "script_type": "pay-to-pubkey-hash"
157 },
158 {
159     "value": 350000,
160     "script":
161     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
162     "addresses": [
163         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
164     ],
165     "script_type": "pay-to-pubkey-hash"
166 },
167 {
168     "value": 350000,
169     "script":
170     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
171     "addresses": [
172         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
173     ],
174     "script_type": "pay-to-pubkey-hash"
175 },
176 {
177     "value": 350000,
178     "script":
179     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
180     "addresses": [
181         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
182     ],
183     "script_type": "pay-to-pubkey-hash"
184 },
185 {
186     "value": 350000,
187     "script":
188     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
189     "addresses": [
190         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
191     ],
192     "script_type": "pay-to-pubkey-hash"
193 },
194 {
195     "value": 350000,
196     "script":
197     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
198     "addresses": [
199         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
200     ],
201     "script_type": "pay-to-pubkey-hash"
202 },
203 {
204     "value": 350000,
205     "script":
206     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
207     "addresses": [
208         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
209     ],
210     "script_type": "pay-to-pubkey-hash"
211 },
212 {
213     "value": 350000,
214     "script":
215     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
216     "addresses": [
217         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
218     ],
219     "script_type": "pay-to-pubkey-hash"
220 },
221 {
222     "value": 350000,
223     "script":
224     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
225     "addresses": [
226         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
227     ],
228     "script_type": "pay-to-pubkey-hash"
229 },
230 {
231     "value": 350000,
232     "script":
233     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
234     "addresses": [
235         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
236     ],
237     "script_type": "pay-to-pubkey-hash"
238 },
239 {
240     "value": 350000,
241     "script":
242     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
243     "addresses": [
244         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
245     ],
246     "script_type": "pay-to-pubkey-hash"
247 },
248 {
249     "value": 350000,
250     "script":
251     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
252     "addresses": [
253         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
254     ],
255     "script_type": "pay-to-pubkey-hash"
256 },
257 {
258     "value": 350000,
259     "script":
260     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
261     "addresses": [
262         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
263     ],
264     "script_type": "pay-to-pubkey-hash"
265 },
266 {
267     "value": 350000,
268     "script":
269     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
270     "addresses": [
271         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
272     ],
273     "script_type": "pay-to-pubkey-hash"
274 },
275 {
276     "value": 350000,
277     "script":
278     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
279     "addresses": [
280         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
281     ],
282     "script_type": "pay-to-pubkey-hash"
283 },
284 {
285     "value": 350000,
286     "script":
287     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
288     "addresses": [
289         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
290     ],
291     "script_type": "pay-to-pubkey-hash"
292 },
293 {
294     "value": 350000,
295     "script":
296     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
297     "addresses": [
298         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
299     ],
300     "script_type": "pay-to-pubkey-hash"
301 },
302 {
303     "value": 350000,
304     "script":
305     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
306     "addresses": [
307         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
308     ],
309     "script_type": "pay-to-pubkey-hash"
310 },
311 {
312     "value": 350000,
313     "script":
314     "76a914023f92a8a3f687e082b5e6c8e072fdb0411620b88ac",
315     "addresses": [
316         "mfifoZPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
317     ],
318     "script_type": "pay-to-pubkey-hash"
319 },
320 {
321     "value": 350000,
322     "script":
323     "76a91
```

```
117     ]
118   }
119 }
```

确认结果

 Bitcoin Testnet Transaction

783f4016bee7afdd479902e15b031a02077eb7a772293d731352e0bc4d5197e1

AMOUNT TRANSACTED	FEES	RECEIVED	CONFIRMATIONS 
0.035 BTC	0.00224932 BTC	 about 2 hours ago	 6+

划分Bob 在 BCY 地址领取到的币

```
# my_private_key = CBitcoinSecret('cSX3H7ZTGKSgBmWsuUSFtKobUDaKzMMXqzhzHeD98qpi1qM4rtUf')
my_private_key = CBitcoinSecret.from_secret_bytes(x('6be882f8746c8ea3bbe9dc15d2c694fd8b75d433c6265dd70558e165849a7200'))

my_public_key = my_private_key.pub
my_address = P2PKHBitcoinAddress.from_pubkey(my_public_key)

# amount_to_send = 0.035 # amount of BTC in the output you're splitting minus fee
amount_to_send = 0.01
# txid_to_spend = (
#     '29ebbaf33f4eb737e2592b39ef8348ddd9b31a17be7f333c03ee7252677d88c4')
txid_to_spend = (
    '3bfd0066036316bb2c88ff4c9346acd236f4254d70d43b574406422fcc4e0efd')
utxo_index = 0
n = 10 # number of outputs to split the input into
# network = 'btc-test3' # either 'btc-test3' or 'bcy-test'
network = 'bcy-test'
```

在填写Bob私钥时需要使用字节形式的。BCY给出的私钥不是64位编码，因此使用函数 `x()` 将其私钥转为字节，通过 `from_secret_bytes()` 导入

输出为

```
1 201 Created
2 {
3   "tx": {
4     "block_height": -1,
5     "block_index": -1,
6     "hash":
7     "8d8c4595ffc35e468541f6b4233eaf340cdd3574b8fa2bbaa71ed70ac542bc0a",
8     "addresses": [
9       "C3Te5ctMDdNAbDyVUCDxWyNPqhrRKnoPJ3"
10    ],
11    "total": 1000000,
12    "fees": 0,
13    "size": 498,
14    "vsize": 498,
```

```
14     "preference": "low",
15     "relayed_by": "2001:250:401:6561:64cc:4fde:81b0:5543",
16     "received": "2022-11-26T11:21:38.227295006Z",
17     "ver": 1,
18     "double_spend": false,
19     "vin_sz": 1,
20     "vout_sz": 10,
21     "confirmations": 0,
22     "inputs": [
23         {
24             "prev_hash":
25             "3bfd0066036316bb2c88ff4c9346acd236f4254d70d43b574406422fcc4e0efd",
26             "output_index": 0,
27             "script":
28             "483045022100c7aafe3148106bbc8170c3de8e2fbf506c5f866bd8ad52e4e6f0810
29             f8e04c1aa02202d1d7cecc09d7351ee5384aa5ac2f73e73832d20c3a45455349f5a5
30             543211e4f01210303a04978f9c2d45754c7b9fe7e68f8de8d0636327c62e083ff4ed
31             ab89e529e2b",
32             "output_value": 1000000,
33             "sequence": 4294967295,
34             "addresses": [
35                 "C3Te5ctMDdNABDyVUCDxWyNPqhrRKnoPJ3"
36             ],
37             "script_type": "pay-to-pubkey-hash",
38             "age": 556013
39         }
40     ],
41     "outputs": [
42         {
43             "value": 100000,
44             "script":
45             "76a914715a44e68effa79eb6e25d0b0d06f12bfdc67a9788ac",
46             "addresses": [
47                 "C3Te5ctMDdNABDyVUCDxWyNPqhrRKnoPJ3"
48             ],
49             "script_type": "pay-to-pubkey-hash"
50         },
51         {
52             "value": 100000,
53             "script":
54             "76a914715a44e68effa79eb6e25d0b0d06f12bfdc67a9788ac",
55             "addresses": [
56                 "C3Te5ctMDdNABDyVUCDxWyNPqhrRKnoPJ3"
57             ],
58             "script_type": "pay-to-pubkey-hash"
59         },
60         {
61             "value": 100000,
```




```
55     "script":
    "76a914715a44e68effa79eb6e25d0b0d06f12bfdc67a9788ac",
56     "addresses": [
57         "C3Te5ctMDdNAbDyVUCDxWyNPqhrRKnoPJ3"
58     ],
59     "script_type": "pay-to-pubkey-hash"
60 },
61 {
62     "value": 100000,
63     "script":
    "76a914715a44e68effa79eb6e25d0b0d06f12bfdc67a9788ac",
64     "addresses": [
65         "C3Te5ctMDdNAbDyVUCDxWyNPqhrRKnoPJ3"
66     ],
67     "script_type": "pay-to-pubkey-hash"
68 },
69 {
70     "value": 100000,
71     "script":
    "76a914715a44e68effa79eb6e25d0b0d06f12bfdc67a9788ac",
72     "addresses": [
73         "C3Te5ctMDdNAbDyVUCDxWyNPqhrRKnoPJ3"
74     ],
75     "script_type": "pay-to-pubkey-hash"
76 },
77 {
78     "value": 100000,
79     "script":
    "76a914715a44e68effa79eb6e25d0b0d06f12bfdc67a9788ac",
80     "addresses": [
81         "C3Te5ctMDdNAbDyVUCDxWyNPqhrRKnoPJ3"
82     ],
83     "script_type": "pay-to-pubkey-hash"
84 },000
85 {
86     "value": 100000,
87     "script":
    "76a914715a44e68effa79eb6e25d0b0d06f12bfdc67a9788ac",
88     "addresses": [
89         "C3Te5ctMDdNAbDyVUCDxWyNPqhrRKnoPJ3"
90     ],
91     "script_type": "pay-to-pubkey-hash"
92 },
93 {
94     "value": 100000,
95     "script":
    "76a914715a44e68effa79eb6e25d0b0d06f12bfdc67a9788ac",
96     "addresses": [
97         "C3Te5ctMDdNAbDyVUCDxWyNPqhrRKnoPJ3"
```

```

98     ],
99     "script_type": "pay-to-pubkey-hash"
100 },
101 {
102     "value": 100000,
103     "script":
"76a914715a44e68effa79eb6e25d0b0d06f12bfdc67a9788ac",
104     "addresses": [
105         "C3Te5ctMDdNAbDyVUCDxWyNPqhrRKnoPJ3"
106     ],
107     "script_type": "pay-to-pubkey-hash"
108 },
109 {
110     "value": 100000,
111     "script":
"76a914715a44e68effa79eb6e25d0b0d06f12bfdc67a9788ac",
112     "addresses": [
113         "C3Te5ctMDdNAbDyVUCDxWyNPqhrRKnoPJ3"
114     ],
115     "script_type": "pay-to-pubkey-hash"
116 }
117 ]
118 }
119 }




```

验证结果



BlockCypher Testnet Transaction

8d8c4595ffc35e468541f6b4233eaf340cdd3574b8fa2bbaa71ed70ac542bc0a


AMOUNT TRANSACTED	FEES	RECEIVED	CONFIRMATIONS 
0.01 BCY	0.0 BCY	 6 minutes ago	 6+

5. 填写 swap.py.

查询BTC区块链高度

BTC 高度查询地址: <https://live.blockcypher.com/btc-testnet/>



**Hedera**

What are smart contracts?
Why are smart contracts useful? Hedera

Learn More

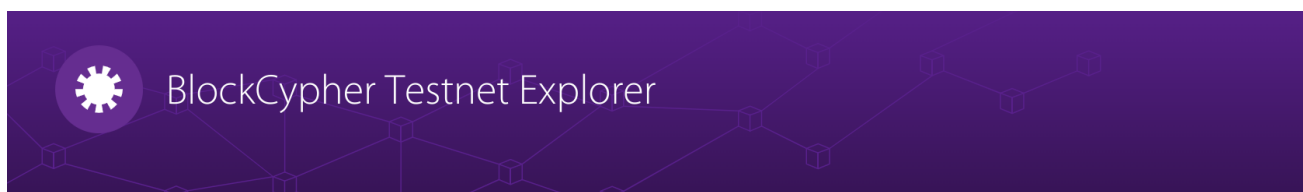
广告 X

Recent Blocks

Height	Age	Transactions	Total Sent	Total Fees	Block Size (in bytes)
2408975	2022-11-29T12:47:16.846Z	32	315.001 BTC	0.002 BTC	8,185
2408974	2022-11-29T12:45:47.558Z	64	131.625 BTC	0.002 BTC	21,588
2408973	2022-11-29T12:42:01.174Z	111	829.786 BTC	0.003 BTC	35,334
2408972	2022-11-29T12:34:56.436Z	9	225.298 BTC	0.001 BTC	2,212

查询BCY区块链高度

BCY 区块高度查询地址: <https://live.blockcypher.com/bcy/>



Recent Blocks

Height	Age	Transactions	Total Sent	Total Fees	Block Size (in bytes)
566549	2022-11-29T13:13:24.577Z	1	0.0 BCY	0.0 BCY	282
566548	2022-11-29T13:12:24.521Z	1	0.0 BCY	0.0 BCY	282
566547	2022-11-29T13:11:24.635Z	2	12.5 BCY	0.0 BCY	473
566546	2022-11-29T13:10:24.531Z	1	0.0 BCY	0.0 BCY	282
566545	2022-11-29T13:09:24.553Z	1	0.0 BCY	0.0 BCY	282

5. 阅读 swap.py, alice.py 和 bob.py, 以及 https://en.bitcoin.it/wiki/Atomic_cross-chain_trading 中的伪代码, 完善 swap_scripts.py 中的脚本。

设计文档

coinExchangeScript工作原理

coinExchangeScript是对交换交易还是返还交易的确认, 对应如下两种情况:

1. 对交换交易的确认: 设计为需要收款方的签名和秘密可赎回, 对应于 coinExchangeScriptSig1。Bob对Alice交换交易的赎回需要秘密和自己的签名, 而Alice赎回Bob的交换交易时只需要自己的签名, 因此为了简便, 这里在赎回交换交易时, 均对自己(收款方)的签名和秘密进行确认。

```

1 def coinExchangeScriptSig1(sig_recipient, secret):
2     return [
3         sig_recipient,
4         secret
5     ]

```

2. 对返还交易的确认：设计为需要付款方的签名，对应于coinExchangeScriptSig2。

```

1 def coinExchangeScriptSig2(sig_sender, sig_recipient):
2     return [
3         sig_sender
4     ]

```

因此，在确认时，首先将栈顶元素与 $H(x)$ 进行比较，若相等，则为秘密，进入第一种情况的进一步确认；否则进一步确认是否为第二种情况。这样，coinExchangeScript实现如下：

```

1 def coinExchangeScript(public_key_sender, public_key_recipient,
2     hash_of_secret):
3     return [
4         OP_DUP,                # 复制栈顶元素
5         OP_HASH160,            # 对栈顶元素进行hash160
6         hash_of_secret,        # 将秘密的哈希压入栈顶
7         OP_EQUAL,              # 比较是与秘密相等
8         OP_IF,                 # 如果为秘密
9         OP_DROP,               # 弹出栈顶多余的元素
10        public_key_recipient,   # 接将收款方公钥压栈，验证收款方的签名
11        OP_ELSE,               # 否则，验证是否为返还交易
12        public_key_sender,      # 将付款方的公钥压入栈顶
13        OP_ENDIF,              # 结束分支判断
14        OP_CHECKSIG             # 验证签名
15    ]

```

步骤	操作	解释
1	OP_DUP	复制栈顶元素
2	OP_HASH160	对栈顶元素执行Hash160计算，结果记为 $H(top)$
3	hash_of_secret	将 $H(x)$ 压栈
4	OP_EQUAL	比较 $H(top)$ 与 $H(x)$ 是否相等。若相等则原栈顶元素为 x ，OP_EQUAL返回1，对应于对交换交易的解锁，接下来执行OP_DROP弹出多余 x ，将收款方公钥压栈，验证收款方签名；否则OP_EQUAL返回0，对应于对返还交易的解锁，将付款方公钥压栈，验证付款方签名。

步骤	操作	解释
5	OP_IF	当栈顶元素不为OP_FALSE时，执行接下来的语句；否则执行OP_ELSE后的语句
6	OP_DROP	弹出多余的 x
7	public_key_recipient	将收款方公钥压栈
8	OP_ELSE	OP_EQUAL返回0，执行接下来的语句
9	public_key_sender	将付款方公钥压栈
10	OP_ENDIF	必须应用此OP_CODE，以结束IF语句
11	OP_CHECKSIG	验证压栈的公钥是否符合签名。若验证收款方成功，则交换交易成功；若验证付款方成功，则收款交易成功；否则，签名错误，交易不成功。

以 Alice 用 coinExchangeScript 向 Bob 发送硬币为例：如果 Bob 不把钱赎回来，Alice 为什么总能拿回她的钱？为什么不能用简单的 1/2 multisig 来解决这个问题？

若Bob没有在Alice创建的自动返还比特币交易上签名，则Alice不能获得Bob的签名，并在解锁Bob的交换交易后告知秘密，这样Bob就不能赎回Alice创建的交换交易，当超过48小时后，Alice将会自动拿回她的钱。

若使用 1/2 multisig，则可以使用任意一方的签名将交易赎回，可能出现一方将两份UTXO均赎回，不能保证在没有互信和第三方的情况下交换一定成功。

Alice和Bob创建的交易内容和先后次序，以及背后设计的原理

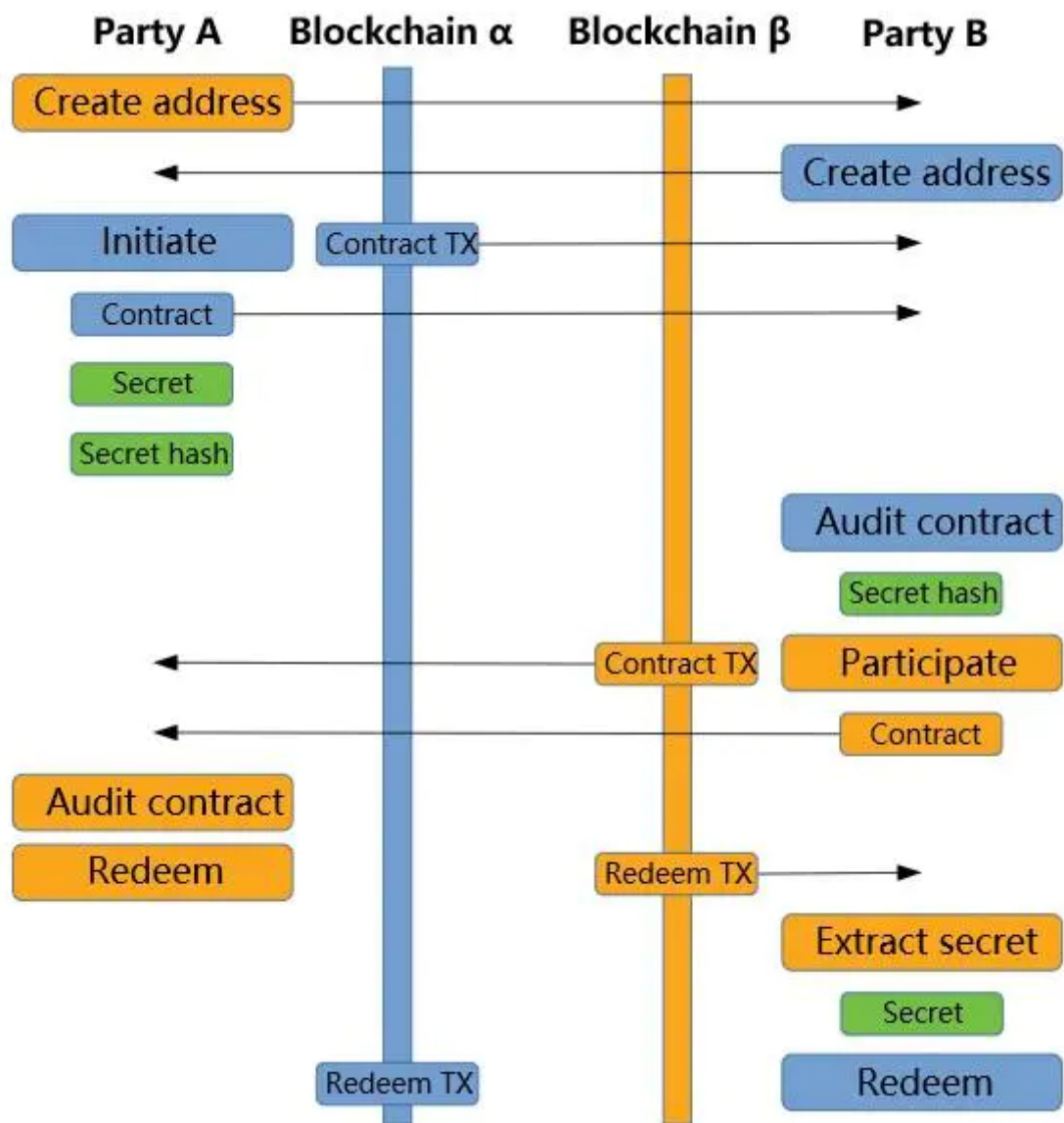
该实验中原子交换的原理简述：围绕只有Alice知道的秘密 x 进行，只广播 $H(x)$ 。如果 x 被透露，那么他们都能赎回对方发送来的货币；如果 x 没有被透露，那么他们都能赎回自己发送的货币，而不需要对方的帮助。

交易过程为：

步骤	详细
1	Alice根据秘密，使用哈希加密，生成tx1：支付 w 比特币（BTC-test）给Bob的公钥，如果 x 已知并由Bob签名，或Alice和Bob共同签名
2	Alice创建tx2，：从tx1支付 w 比特币到Alice的公钥，并在未来48小时内锁定，由Alice签名。若Bob不赎回tx1，这是Alice可以自动将比特币发回的交易

步骤	详细
3	Alice发送tx2给Bob
4	Bob对tx2进行签名并返回给Alice
5	Alice获得Bob的签名，向网络广播tx1
6	Bob创建tx3：若 $H(x)$ 的 x 已知并由Alice签名，或由Alice和Bob共同签名，则将 v 比特币（BCY）支付给Alice的公钥
7	Bob创建tx4：从tx3支付 v 比特币到Bob的公钥，并在未来24小时内锁定，由Bob签名。若Alice不赎回tx3，这是Bob可以自动将比特币发回的交易
8	Bob发送tx4给Alice
9	Alice对tx4签名并返回给Bob
10	Bob获得Alice的签名，向网络广播tx3
11	Alice赎回tx3，同时将该赎回交易广播， x 被Bob得知
12	Bob使用 x 和自己的签名赎回tx1，该赎回交易被广播

交易过程图示如下：（图源：[区块链世界的圣杯----原子互换（Atomic Swaps）技术](#)）



成功跨链原子交换中，资金的流转

这里通过详细步骤进行说明

步骤	详细	资金流转
1	Alice根据秘密，使用哈希加密，生成tx1：支付 w 比特币（BTC-test）给Bob的公钥，如果 x 已知并由Bob签名，或Alice和Bob共同签名	tx1含有的 w 个比特币属于Alice
2	Alice创建tx2，：从tx1支付 w 比特币到Alice的公钥，并在未来48小时内锁定，由Alice签名。若Bob不赎回tx1，这是Alice可以自动将比特币发回的交易	
3	Alice发送tx2给Bob	
4	Bob对tx2进行签名并返回给Alice	

步骤	详细	资金流转
5	Alice获得Bob的签名，向网络广播tx1	
6	Bob创建tx3：若 $H(x)$ 的 x 已知并由Alice签名，或由Alice和Bob共同签名，则将 v 比特币（BCY）支付给Alice的公钥	tx3含有的 v 个比特币属于Bob
7	Bob创建tx4：从tx3支付 v 比特币到Bob的公钥，并在未来24小时内锁定，由Bob签名。若Alice不赎回tx3，这是Bob可以自动将比特币发回的交易	
8	Bob发送tx4给Alice	
9	Alice对tx4签名并返回给Bob	
10	Bob获得Alice的签名，向网络广播tx3	
11	Alice赎回tx3，同时将该赎回交易广播， x 被Bob得知	Alice赎回tx3中的比特币，此时其中 v 个比特币属于Alice
12	Bob使用 x 和自己的签名赎回tx1，该赎回交易被广播	Bob赎回tx1中的比特币，此时其中 w 个比特币属于Bob

实验结果

不赎回不广播

Alice没有对Bob的交换交易进行赎回，因此Bob的返还交易在锁定时间结束后将比特币退回，之后因为Bob没有赎回Alice的交换交易，Alice的返还交易在锁定时间之后将比特币退回。如下为该情况的输出结果，符合流程

```

1 Alice swap tx (BTC) created successfully!
2 Bob swap tx (BCY) created successfully!
3 Bob return coins (BCY) tx created successfully!
4 Alice return coins tx (BTC) created successfully!
```

赎回但不广播

Alice对Bob的交换交易进行赎回，并广播秘密，这样Bob也使用秘密和自己的签名将Alice的交换交易赎回，原子交换成功。如下输出符合流程。


```
1 Alice swap tx (BTC) created successfully!
2 Bob swap tx (BCY) created successfully!
3 Alice redeem from swap tx (BCY) created successfully!
4 Bob redeem from swap tx (BTC) created successfully!
```

赎回且广播

- 完整输出结果

```
1 Alice swap tx (BTC) created successfully!
2 201 Created
3 {
4   "tx": {
5     "block_height": -1,
6     "block_index": -1,
7     "hash":
8       "2c1fa728e7632722fcc55acfc6689683ba0a0b761ddccf4e2f43accce0ee202",
9     "addresses": [
10      "mf1qozPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
11    ],
12    "total": 340000,
13    "fees": 10000,
14    "size": 264,
15    "vsize": 264,
16    "preference": "low",
17    "relayed_by": "2001:250:401:6561:76a7:112f:20a4:dbd1",
18    "received": "2022-12-03T19:06:23.178389124Z",
19    "ver": 1,
20    "double_spend": false,
21    "vin_sz": 1,
22    "vout_sz": 1,
23    "confirmations": 0,
24    "inputs": [
25      {
26        "prev_hash":
27          "783f4016bee7afdd479902e15b031a02077eb7a772293d731352e0bc4d5197e1",
28        "output_index": 7,
29        "script":
30          "483045022100ca22d7114d3d39956849a1f136ed3b3392a5fdc43c3aa458afff294
31          ca2902dbc02207630a6e05ba28ac121aeb44e4e82e896136c34ebe4a6ecba30ecb2e
32          9e94f51820121033c562727bb2136198d74e25b13c0966a8b109c8dd42dcf9d150dd
33          66b34140e3a",
34        "output_value": 350000,
35        "sequence": 4294967295,
36        "addresses": [
37          "mf1qozPUQTrNpSHCCMW5K7tRpZ6QDDEsLe"
38        ],
39        "script_type": "pay-to-pubkey-hash",
40        "age": 2408390
41      }
42    ]
43  }
44 }
```

```

35     }
36 ],
37 "outputs": [
38     {
39         "value": 340000,
40         "script":
"76a914853b775079232503df966e626618e1d388a9572087637521038526a58b829
4738325a59824a38936b5dfdda760b301c6161cba81ed5bc701786721033c562727b
b2136198d74e25b13c0966a8b109c8dd42dcf9d150dd66b34140e3a68ac",
41         "addresses": null,
42         "script_type": "unknown"
43     }
44 ]
45 }
46 }
47 Bob swap tx (BCY) created successfully!
48 201 Created
49 {
50     "tx": {
51         "block_height": -1,
52         "block_index": -1,
53         "hash":
"66150903a0b8d178b43c872517794e3fe8cb9b8046b04e3bc7a4e856cac686b1",
54         "addresses": [
55             "C3Te5ctMDdNABDyVUCDxWyNPqhrRKnoPJ3"
56         ],
57         "total": 90000,
58         "fees": 10000,
59         "size": 263,
60         "vsize": 263,
61         "preference": "low",
62         "relayed_by": "2001:250:401:6561:76a7:112f:20a4:dbd1",
63         "received": "2022-12-03T19:06:24.592342785Z",
64         "ver": 1,
65         "double_spend": false,
66         "vin_sz": 1,
67         "vout_sz": 1,
68         "confirmations": 0,
69         "inputs": [
70             {
71                 "prev_hash":
"8d8c4595ffc35e468541f6b4233eaf340cdd3574b8fa2bbaa71ed70ac542bc0a",
72                 "output_index": 7,
73                 "script":
"4730440220776107903e5820f99ccb107f03cf08be04ff3996698051e201a4a66d8
af2b898022058c4d1a4861862ec190848a2916b8a704ff166e69d1bc89ef1672222c
5a998b901210303a04978f9c2d45754c7b9fe7e68f8de8d0636327c62e083ff4edab
89e529e2b",
74                 "output_value": 100000,

```

```

75     "sequence": 4294967295,
76     "addresses": [
77         "C3Te5ctMDdNAbDyVUCDxWyNPqhrRKnoPJ3"
78     ],
79     "script_type": "pay-to-pubkey-hash",
80     "age": 562168
81 }
82 ],
83 "outputs": [
84     {
85         "value": 90000,
86         "script":
87         "76a914853b775079232503df966e626618e1d388a9572087637521027eceaaf3478
88         800216099ad300b79f1e0da56f0669760e105b43a9b7a9952b5ea67210303a04978f
89         9c2d45754c7b9fe7e68f8de8d0636327c62e083ff4edab89e529e2b68ac",
90         "addresses": null,
91         "script_type": "unknown"
92     }
93 ]
94 }
95 Sleeping for 60 minutes to let transactions confirm...
96 Alice redeem from swap tx (BCY) created successfully!
97 201 Created
98 {
99     "tx": {
100         "block_height": -1,
101         "block_index": -1,
102         "hash":
103         "8bd26b5f75ef67e5fe51dfec8b2079be1d72d6fccce15c7f591be7e9b1dc863b",
104         "addresses": [
105             "C2RT1LaD9EH1xdaJqtaoRoAMvxKYJQVNKD"
106         ],
107         "total": 80000,
108         "fees": 10000,
109         "size": 182,
110         "vsize": 182,
111         "preference": "low",
112         "relayed_by": "2001:250:401:6561:76a7:112f:20a4:dbd1",
113         "received": "2022-12-03T22:06:25.247080971Z",
114         "ver": 1,
115         "double_spend": false,
116         "vin_sz": 1,
117         "vout_sz": 1,
118         "confirmations": 0,
119         "inputs": [
120             {
121                 "prev_hash":
122                 "66150903a0b8d178b43c872517794e3fe8cb9b8046b04e3bc7a4e856cac686b1",

```

```

119         "output_index": 0,
120         "script":
"47304402204fa38c32dccc1ae9afbc7c95d534f83ff0be305a28079cb2c05522af9
90f7f2402205d02ed87c069086cea063eda090ae64214c441fc79ae9cbf5012563a5
2a8378b01187468697349734153656372657450617373776f7264313233",
121         "output_value": 90000,
122         "sequence": 4294967295,
123         "script_type": "unknown",
124         "age": 572650
125     }
126 ],
127     "outputs": [
128     {
129         "value": 80000,
130         "script":
"76a91465f8114669e05d98b6320a04677ed2e19eba81bb88ac",
131         "addresses": [
132             "C2RT1LaD9EH1xdaJqtaoRoAMvxKYJQVNKD"
133         ],
134         "script_type": "pay-to-pubkey-hash"
135     }
136 ]
137 }
138 }
139 Bob redeem from swap tx (BTC) created successfully!
140 201 Created
141 {
142     "tx": {
143         "block_height": -1,
144         "block_index": -1,
145         "hash":
"6bc76bfd1796e62953057f1eabbc21ba445f81696d1187eb6602f410af3a5c55",
146         "addresses": [
147             "miQKwKQ1TwJ7uxaRj7U1aB9hrruTNQzD4F"
148         ],
149         "total": 330000,
150         "fees": 10000,
151         "size": 183,
152         "vsize": 183,
153         "preference": "low",
154         "relayed_by": "2001:250:401:6561:76a7:112f:20a4:dbd1",
155         "received": "2022-12-03T22:06:25.797106409Z",
156         "ver": 1,
157         "double_spend": false,
158         "vin_sz": 1,
159         "vout_sz": 1,
160         "confirmations": 0,
161         "inputs": [
162         {

```


```

163     "prev_hash":
164     "2c1fa728e7632722fcca55acfc6689683ba0a0b761ddccf4e2f43accce0ee202",
165     "output_index": 0,
166     "script":
167     "483045022100c623e3792b73ff9fad4511a958b79c119b497a2019b7d5c767421f8
168     42ca87be702201ee77769d010f3d95722afb00bfd8910c43eca91f643a3c74be4638
169     af46598b701187468697349734153656372657450617373776f7264313233",
170     "output_value": 340000,
171     "sequence": 4294967295,
172     "script_type": "unknown",
173     "age": 2409652
174 }
175 ],
176 "outputs": [
177 {
178     "value": 330000,
179     "script":
180     "76a9141fa7882789fa7699c326f7c863684673450758f688ac",
181     "addresses": [
182     "miQKwKQ1TwJ7uxaRj7U1aB9hrruTNQzD4F"
183     ],
184     "script_type": "pay-to-pubkey-hash"
185 }
186 ]
187 }
188 }

```




- 截图

Bob对Alice创建的返还交易即tx2进行签名后，Alice广播交换交易即tx1，tx1的确认结果



Bitcoin Testnet Transaction


2c1fa728e7632722fcca55acfc6689683ba0a0b761ddccf4e2f43accce0ee202

AMOUNT TRANSACTED	FEES	RECEIVED	CONFIRMATIONS 
0.0034 BTC	0.0001 BTC	 about 8 hours ago	 6+

[Advanced Details](#)

Details

1 Input Consumed

0.0035 BTC from
 mfiqoZPUQTnNpSHCCMW5K7tRpZ6QDEsLe (output)

1 Output Created

0.0034 BTC Unknown Script Type

创建的交换交易即tx3，Alice对Bob创建的返还交易即tx4进行签名后，Bob广播交换交易即tx3，tx3的确认结果

BlockCypher Testnet Transaction

66150903a0b8d178b43c872517794e3fe8cb9b8046b04e3bc7a4e856cac686b1

AMOUNT TRANSACTED	FEES	RECEIVED	CONFIRMATIONS
0.0009 BCY	0.0001 BCY	about 8 hours ago	6+

Advanced Details

Details

1 Input Consumed

0.001 BCY from
C3Te5ctMDdNAbDyVUCdXWyNPqhrRKnoPJ3 (output)

...

1 Output Created

0.0009 BCY Unknown Script Type

Alice赎回Bob创建的交换交易即tx3，该赎回交易的确认结果

BlockCypher Testnet Transaction

8bd26b5f75ef67e5fe51dfec8b2079be1d72d6fccce15c7f591be7e9b1dc863b

AMOUNT TRANSACTED	FEES	RECEIVED	CONFIRMATIONS
0.0008 BCY	0.0001 BCY	about 5 hours ago	6+

Advanced Details

Details

1 Input Consumed

0.0009 BCY Unknown Script Type (output)

...

1 Output Created

0.0008 BCY to
C2RT1LaD9EH1xdaJqtaoRoAMvxKYJQVNKD (unspent)

Bob赎回Alice创建的交换交易即tx1，该赎回交易的确认结果

Bitcoin Testnet Transaction

6bc76bfd1796e62953057f1eabbc21ba445f81696d1187eb6602f410af3a5c55

AMOUNT TRANSACTED 0.0033 BTC	FEES 0.0001 BTC	RECEIVED 🕒 about 5 hours ago	CONFIRMATIONS ⓘ 🔒 6+
--	---------------------------	--	--------------------------------

Advanced Details ▾

Details



遇到的问题

赎回交易时遇到missing reference

- 问题现象

```
1 # tx3序列号
2 8c755151d9ae31c0d4e1dabe9156207176817d2f2a008268803a724f4c1b28c2
3
4 # 赎回tx3时报错
5 {"error": "Error validating transaction: Transaction
dc8e0dd1d6f96d5a7d117a0c6a0381d88531a53a77c06975e3e98bde84a1ab90
orphcy/test/taned, missing reference
c2281b4c4f723a806882002a2f7d817671205691bedae1d4c031aed95151758c."}
```

- 问题原因

在助教学长的指导下，得知发生该错误的原因是b2x函数得到的是大端序列，因此序列号对不上。注意到missing reference中的txid正是tx3对应序列号

- 问题解决

将获取txid的函数由大端转为小端，即将b2x函数修改为使用b2lx函数

```

1 def b2x(b):
2     """Convert bytes to a hex string"""
3     return binascii.hexlify(b).decode('utf8')
4
5 def b2lx(b):
6     """Convert bytes to a little-endian hex string
7
8     Lets you show uint256's and uint160's the way the Satoshi codebase
9     shows
10    them.
11    """
12    return binascii.hexlify(b[::-1]).decode('utf8')

```

以Alice.py中的函数return_coins_tx为例，依次修改Alice.py和Bob.py中相应的调用位置

```

def return_coins_tx(amount_to_send, last_tx, lock_time):
    txin = create_txin(b2lx(last_tx.GetTxid()), 0) 从b2x修改为b2lx
    txout = create_txout(amount_to_send, P2PKH_scriptPubKey(bob_address_BCY))
    tx = CMutableTransaction([txin], [txout], nLockTime=lock_time)
    return tx

```