

# keygen.py

---

Alice

- 1 Private key: cupCNaMwCphDA1NRoeFiSNQhQghDAHCiKnAHjsAYhtC7brHWxSLu
- 2 Address: mjctYGeicFgM3q81mjsPW6YSX28ZLVHYQ2

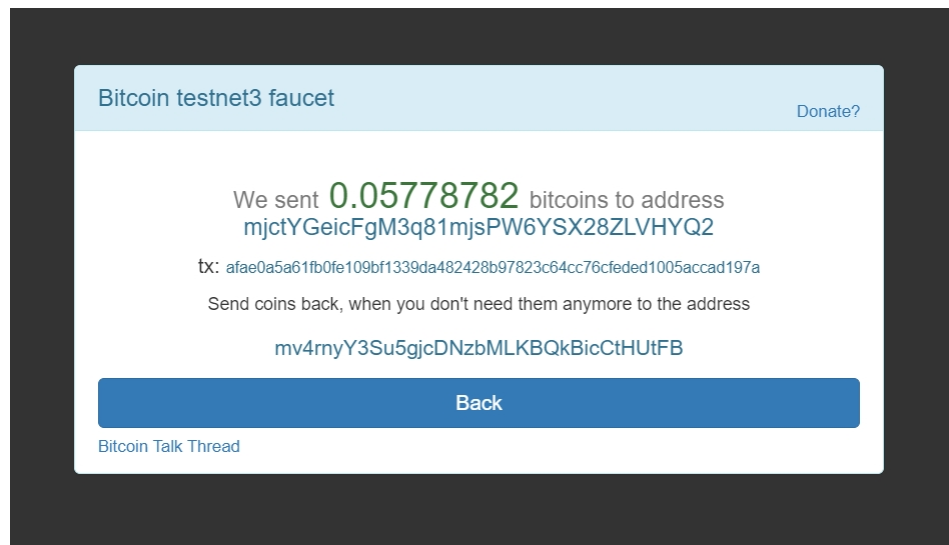
Bob

- 1 Private key: cve2gjMb76HjG8Wr5bu3CUruccBLxPLxE7uDmt5rneDRRCPaXcTZ
- 2 Address: mtYR9tdnmDjDgLtAqEDNL6EfA11TASheha

为Alice在BTC上领取测试币

<https://live.blockcypher.com/btc-testnet/tx/afae0a5a61fb0fe109bf1339da482428b97823c64cc76cfed1005accad197a/>

- 1 txid: afae0a5a61fb0fe109bf1339da482428b97823c64cc76cfed1005accad197a

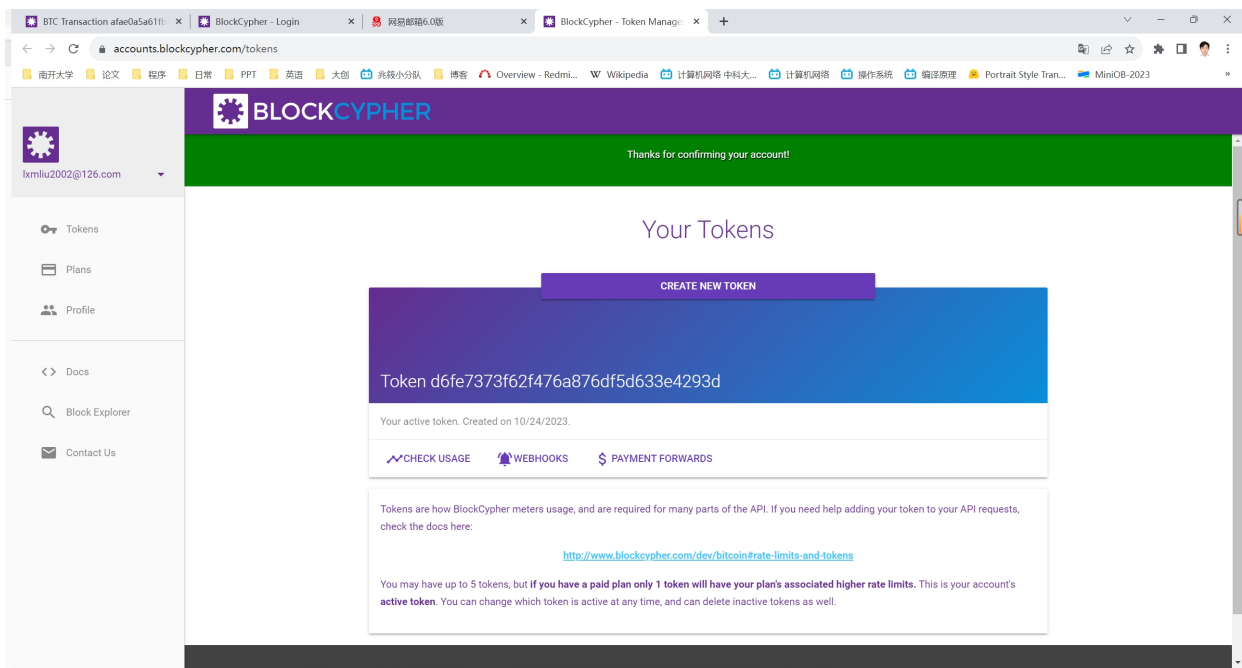


## BCY

---

注册账户获取API token

- 1 Token d6fe7373f62f476a876df5d633e4293d



## 创建密钥

Alice

```
1 C:\Users\lxmli>curl -X POST https://api.blockcypher.com/v1/bcy/test/addr?  
token=d6fe7373f62f476a876df5d633e4293d  
2 {  
3   "private": "3991895a89e87b2b8284eddfa29d25317a694f6a3dd82596581eefc9b101da5b",  
4   "public": "031cafc11a94e1089f952d82852dab31c18965018da5af451b225baed5ec5741d1",  
5   "address": "CFCn7K7hs63cv2sXEMupexF5MA64F2qLYj",  
6   "wif": "BqFWGNameEhPL4Du68pqBktFCwHNJevvn3Hzfd59ykxiEcvIUQS2a"  
7 }
```

Bob

```
1 C:\Users\lxmli>curl -X POST https://api.blockcypher.com/v1/bcy/test/addr?  
token=d6fe7373f62f476a876df5d633e4293d  
2 {  
3   "private": "221d9a49929481c2c2a253dd08f3a1046e66df654bd1e65809b1b75624cee0a4",  
4   "public": "03d0475a17721d708eecd7277f1b8eb38f2480a85fee478b0fae83cffd84d29c88",  
5   "address": "C1UhLgQa51AuDhob8NdjQxYrzeVN8jqNKP",  
6   "wif": "BpUM5wX4hYROWRRypiccACvLRnHwBkb2uEqkaMsLd7Use4XR5qyQ"  
7 }
```

为Bob的BCY地址领取测试币

<https://live.blockcypher.com/bcy/tx/647208d0059a49fe73ea679f8642efcae095cad66269d75c8765503a778afb75/>

```
1 C:\Users\lxmli>curl -d "{\"address\": \"C1UhLgQa51AuDhoB8NdjQxYrzeVN8jqNKP\",
  \"amount\": 1000000}" https://api.blockcypher.com/v1/bcy/test/faucet?
  token=d6fe7373f62f476a876df5d633e4293d
2 {
3   "tx_ref": "647208d0059a49fe73ea679f8642efcae095cad66269d75c8765503a778afb75"
4 }
```

## 划分领取的币

BTC\_output

<https://live.blockcypher.com/btc-testnet/tx/26ef803d4a07e1b48dc8c1e7bf7bd9a630ac2e979dcc2c6a3638c0ad1877aae3/>

```
1 201 Created
2 {
3   "tx": {
4     "block_height": -1,
5     "block_index": -1,
6     "hash":
7       "26ef803d4a07e1b48dc8c1e7bf7bd9a630ac2e979dcc2c6a3638c0ad1877aae3",
8     "addresses": [
9       "mjctYGeicFgm3q81mjsPW6YSX28ZLVHYQ2"
10    ],
11    "total": 5500000,
12    "fees": 278782,
13    "size": 498,
14    "vsize": 498,
15    "preference": "high",
16    "relayed_by": "103.20.198.139",
17    "received": "2023-10-24T02:58:16.975827433z",
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          "a5ae0a5a61fb0fe109bf1339da482428b97823c64cc76cfeded1005accad197a",
27        "output_index": 0,
28        "script":
29          "483045022100e5b8a183bedf22676852349b89b14f9dc4b76c1fbbcb414ad3ba3d0de372a75e0
30          2200861985a8c13eab3dfe0d341740e53022367299d4c04dcce09d62d0eed32f29012103887f6
31          bf8f22cac34e6b2c52deca82adb1558c2a49b066c6024e56c61db8f11f",
32        "output_value": 5778782,
33        "sequence": 4294967295,
34        "addresses": [
35          "mjctYGeicFgm3q81mjsPW6YSX28ZLVHYQ2"
36        ],
37        "script_type": "pay-to-pubkey-hash",
38      }
39    ]
40  }
```

```
33     "age": 2534917
34   }
35 ],
36 "outputs": [
37   {
38     "value": 550000,
39     "script": "76a9142cffdd4ee53545362f755a5589ae58b7157fe4b788ac",
40     "addresses": [
41       "mjctYGeicFgm3q81mjsPW6YSX28ZLVHYQ2"
42     ],
43     "script_type": "pay-to-pubkey-hash"
44   },
45   {
46     "value": 550000,
47     "script": "76a9142cffdd4ee53545362f755a5589ae58b7157fe4b788ac",
48     "addresses": [
49       "mjctYGeicFgm3q81mjsPW6YSX28ZLVHYQ2"
50     ],
51     "script_type": "pay-to-pubkey-hash"
52   },
53   {
54     "value": 550000,
55     "script": "76a9142cffdd4ee53545362f755a5589ae58b7157fe4b788ac",
56     "addresses": [
57       "mjctYGeicFgm3q81mjsPW6YSX28ZLVHYQ2"
58     ],
59     "script_type": "pay-to-pubkey-hash"
60   },
61   {
62     "value": 550000,
63     "script": "76a9142cffdd4ee53545362f755a5589ae58b7157fe4b788ac",
64     "addresses": [
65       "mjctYGeicFgm3q81mjsPW6YSX28ZLVHYQ2"
66     ],
67     "script_type": "pay-to-pubkey-hash"
68   },
69   {
70     "value": 550000,
71     "script": "76a9142cffdd4ee53545362f755a5589ae58b7157fe4b788ac",
72     "addresses": [
73       "mjctYGeicFgm3q81mjsPW6YSX28ZLVHYQ2"
74     ],
75     "script_type": "pay-to-pubkey-hash"
76   },
77   {
78     "value": 550000,
79     "script": "76a9142cffdd4ee53545362f755a5589ae58b7157fe4b788ac",
80     "addresses": [
81       "mjctYGeicFgm3q81mjsPW6YSX28ZLVHYQ2"
82     ],
83     "script_type": "pay-to-pubkey-hash"
84   },
85 ]
```

```

85     {
86         "value": 550000,
87         "script": "76a9142cffdd4ee53545362f755a5589ae58b7157fe4b788ac",
88         "addresses": [
89             "mjctYGeicFgM3q81mjsPW6YSX28ZLVHYQ2"
90         ],
91         "script_type": "pay-to-pubkey-hash"
92     },
93     {
94         "value": 550000,
95         "script": "76a9142cffdd4ee53545362f755a5589ae58b7157fe4b788ac",
96         "addresses": [
97             "mjctYGeicFgM3q81mjsPW6YSX28ZLVHYQ2"
98         ],
99         "script_type": "pay-to-pubkey-hash"
100     },
101     {
102         "value": 550000,
103         "script": "76a9142cffdd4ee53545362f755a5589ae58b7157fe4b788ac",
104         "addresses": [
105             "mjctYGeicFgM3q81mjsPW6YSX28ZLVHYQ2"
106         ],
107         "script_type": "pay-to-pubkey-hash"
108     },
109     {
110         "value": 550000,
111         "script": "76a9142cffdd4ee53545362f755a5589ae58b7157fe4b788ac",
112         "addresses": [
113             "mjctYGeicFgM3q81mjsPW6YSX28ZLVHYQ2"
114         ],
115         "script_type": "pay-to-pubkey-hash"
116     }
117 ]
118 }
119 }

```

## 练习

### A

```

1  def coinExchangeScript(public_key_sender, public_key_recipient,
    hash_of_secret):
2      return [
3          # fill this in!
4          public_key_sender,
5          OP_CHECKSIG,
6          OP_IF,
7          public_key_recipient,
8          OP_CHECKSIG,
9          OP_IF,

```

```

10         OP_1,
11     OP_ELSE,
12         OP_DUP,
13         OP_HASH160,
14         hash_of_secret,
15         OP_EQUAL,
16         OP_IF,
17             OP_1,
18         OP_ELSE,
19             OP_DUP,
20             OP_2,
21             public_key_sender,
22             public_key_recipient,
23             OP_CHECKMULTISIG,
24         OP_ENDIF,
25     OP_ENDIF,
26 OP_ENDIF
27 ]

```

## B

### a

```

1 def coinExchangeScriptSig1(sig_recipient, secret):
2     return [
3         # fill this in!
4         secret,
5         sig_recipient
6     ]

```

### b

```

1 def coinExchangeScriptSig2(sig_sender, sig_recipient):
2     return [
3         # fill this in!
4         sig_recipient,
5         sig_sender
6     ]

```

## C

运行swap.py

```

1 broadcast_transactions = False
2 alice_redeems = False

```

```
● PS E:\刘修铭\南开大学\个人材料\课程\2023-2024 第1学期\区块链基础及应用 苏明\Blockchain_Fundamentals_and_Applications\Ex4\codes\swap.py"
Alice swap tx (BTC) created successfully!
Bob swap tx (BCY) created successfully!
Bob return coins (BCY) tx created successfully!
Alice return coins tx (BTC) created successfully!
```

```
1 broadcast_transactions = False
2 alice_redeems = True
```

```
● PS E:\刘修铭\南开大学\个人材料\课程\2023-2024 第1学期\区块链基础及应用 苏明\Blockchain_Fundamentals_and_Applications\Ex4\codes\swap.py"
Alice swap tx (BTC) created successfully!
Bob swap tx (BCY) created successfully!
Alice redeem from swap tx (BCY) created successfully!
Bob redeem from swap tx (BTC) created successfully!
```

```
1 broadcast_transactions = True
2 alice_redeems = False
```

output

```
1 Alice swap tx (BTC) created successfully!
2 201 Created
3 {
4   "tx": {
5     "block_height": -1,
6     "block_index": -1,
7     "hash":
8       "c7d43a5c1adc6b9af16ca5677d89a2880655ee2fbd3cc651a31597606f10b6df",
9     "addresses": [
10      "mjctYGeicFgm3q81mjsPW6YSX28ZLVHYQ2"
11    ],
12    "total": 400000,
13    "fees": 150000,
14    "size": 342,
15    "vsize": 342,
16    "preference": "high",
17    "relayed_by": "103.20.198.139",
18    "received": "2023-10-24T10:18:25.200874767Z",
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          "26ef803d4a07e1b48dc8c1e7bf7bd9a630ac2e979dcc2c6a3638c0ad1877aae3",
28        "output_index": 1,
```

```

27     "script":
    "483045022100de38a5748a1c8757855c86037b2095c1d13b059f104e03e7e27208d5929ab7b10
    2201d73dcba77e9910cc6fd8704764a9a8eec06ba7e93a520e695b56a8e33e2ddb4012103887f6
    bf8f22cac34e6b2c52deca82adbf1558c2a49b066c6024e56c61db8f11f",
28     "output_value": 550000,
29     "sequence": 4294967295,
30     "addresses": [
31         "mjctYGeicFgm3q81mjsPW6YSX28ZLVHYQ2"
32     ],
33     "script_type": "pay-to-pubkey-hash",
34     "age": 2534921
35 }
36 ],
37 "outputs": [
38     {
39         "value": 400000,
40         "script":
    "2103887f6bf8f22cac34e6b2c52deca82adbf1558c2a49b066c6024e56c61db8f11fac6321039
    f886ecc863bc71cb1b358f12ae19df33457749abe766990120d8027804ed953ac63516776a9148
    53b775079232503df966e626618e1d388a957208763516776522103887f6bf8f22cac34e6b2c52
    deca82adbf1558c2a49b066c6024e56c61db8f11f21039f886ecc863bc71cb1b358f12ae19df33
    457749abe766990120d8027804ed953ae686868",
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":
    "a3bee6e140a3070ddde6dd5f745cdf00edf1f16dcf8f143fd54462a3c94db830",
54         "addresses": [
55             "C1UhLgQa51AuDhoB8NdjQxYrzeVN8jqNKP"
56         ],
57         "total": 900000,
58         "fees": 100000,
59         "size": 342,
60         "vsize": 342,
61         "preference": "high",
62         "relayed_by": "103.20.198.139",
63         "received": "2023-10-24T10:18:26.128916581Z",
64         "ver": 1,
65         "double_spend": false,
66         "vin_sz": 1,
67         "vout_sz": 1,
68         "confirmations": 0,
69         "inputs": [

```



```

70     {
71         "prev_hash":
72         "647208d0059a49fe73ea679f8642efcae095cad66269d75c8765503a778afb75",
73         "output_index": 0,
74         "script":
75         "483045022100ab3b7cad03cb0e98d7242744ad7a4e18c91af2194adfb13517ababaa3836e33f0
76         22022a81dce6fe7f8747972b8074be2c48cc126548dbe6215bd0c3650d31551b2d6012103d0475
77         a17721d708eecd7277f1b8eb38f2480a85fee478b0fae83cffd84d29c88",
78         "output_value": 1000000,
79         "sequence": 4294967295,
80         "addresses": [
81             "C1UhLgQa51AudhoB8NdjQxYrzeVN8jqNKP"
82         ],
83         "script_type": "pay-to-pubkey-hash",
84         "age": 1036994
85     }
86 ],
87 "outputs": [
88     "outputs": [
89         {
90             "value": 900000,
91             "script":
92             "2103d0475a17721d708eecd7277f1b8eb38f2480a85fee478b0fae83cffd84d29c88ac6321031
93             cafc11a94e1089f952d82852dab31c18965018da5af451b225baed5ec5741d1ac63516776a9148
94             53b775079232503df966e626618e1d388a957208763516776522103d0475a17721d708eecd7277
95             f1b8eb38f2480a85fee478b0fae83cffd84d29c8821031cafc11a94e1089f952d82852dab31c18
96             965018da5af451b225baed5ec5741d1ae686868",
97             "addresses": null,
98             "script_type": "unknown"
99         }
100     ]
101 }
102 }
103 }
104 Sleeping for 20 minutes to let transactions confirm...
105 Bob return coins (BCY) tx created successfully!
106 Alice return coins tx (BTC) created successfully!
107 Sleeping for bob_locktime blocks to pass locktime...
108 400 Bad Request
109 {"error": "Error validating transaction: Transaction
110 a09f539e5a722f31f045c86fe1298dcd5ca6e749a1ca4fa40b2b3f2552f77dd7 orphaned,
111 missing reference
112 30b84dc9a36244d53f148fcf6df1f1ed00df5c745fdde6dd0d07a340e1e6bea3."}
113 Sleeping for alice_locktime blocks to pass locktime...
114 400 Bad Request
115 {"error": "Error validating transaction: Transaction
116 0961d3af066c3057edf5dcc0ee6b64b51e90d04d83ea4824c4894f62deffa14a orphaned,
117 missing reference
118 dfb6106f609715a351c63cbd2fee550688a2897d67a56cf19a6bdc1a5c3ad4c7."}

```

```

1 broadcast_transactions = True
2 alice_redeems = True

```

由于前面交易已经将Bob的比特币取走，现重新领取

- 生成密钥

```
1 C:\Users\lxmli>curl -X POST https://api.blockcypher.com/v1/bcy/test/addrs?  
token=d6fe7373f62f476a876df5d633e4293d  
2 {  
3   "private":  
   "7bcd57926e60e6aa751d8057ac06adc1065095ad0085edac0bad3eaae60c7d0",  
4   "public":  
   "021505af54164eee76ba6d9731e16082768ad4a4ff2175b0fdf1f4effc23672dcb",  
5   "address": "BzFDzDVkqe7jkwpVZudGXB2Fgx7qtq4BLq",  
6   "wif": "BsUgu39T6ww8HWyJt2hQhzFSnKMZheHosb7ZEV91cpJFXGnhkEg9"  
7 }
```

- 领取比特币

```
1 C:\Users\lxmli>curl -d "{\"address\":  
  \"BzFDzDVkqe7jkwpVZudGXB2Fgx7qtq4BLq\", \"amount\": 1000000}"  
https://api.blockcypher.com/v1/bcy/test/faucet?  
token=d6fe7373f62f476a876df5d633e4293d  
2 {  
3   "tx_ref":  
   "a0a7e88e704df710352eef2543de91ac8ce66d8b6e63a205271f22395e03d2ef"  
4 }
```

- output

```
1 Alice swap tx (BTC) created successfully!  
2 201 Created  
3 {  
4   "tx": {  
5     "block_height": -1,  
6     "block_index": -1,  
7     "hash":  
8     "12042d39f7c06ba28864786198cbcd3a80fe56b0fcfe182bdd3d51703298be15",  
9     "addresses": [  
10      "mjctYGeicFGm3q81mjsPW6YSX28ZLVHYQ2"  
11    ],  
12    "total": 400000,  
13    "fees": 150000,  
14    "size": 342,  
15    "vsize": 342,  
16    "preference": "high",  
17    "relayed_by": "103.20.198.139",  
18    "received": "2023-10-24T11:29:04.883989263Z",  
19    "ver": 1,  
20    "double_spend": false,  
21    "vin_sz": 1,  
22    "vout_sz": 1,  
    "confirmations": 0,
```

```

23     "inputs": [
24         {
25             "prev_hash":
26             "26ef803d4a07e1b48dc8c1e7bf7bd9a630ac2e979dcc2c6a3638c0ad1877aae3",
27             "output_index": 3,
28             "script":
29             "483045022100f3dbbe0273b053915a9d320d745c9c3055e42f26601202726c18f3573948f
30             9f302203b37c92b363e05f5d9d0f8b7cc7f9f7a66043cd7fcaf1fce09b3ede358f50cac012
31             103887f6bf8f22cac34e6b2c52deca82adbf1558c2a49b066c6024e56c61db8f11f",
32             "output_value": 550000,
33             "sequence": 4294967295,
34             "addresses": [
35                 "mjctYGeicFgm3q81mjsPW6YSX28ZLVHYQ2"
36             ],
37             "script_type": "pay-to-pubkey-hash",
38             "age": 2534921
39         }
40     ],
41     "outputs": [
42         {
43             "value": 400000,
44             "script":
45             "2103887f6bf8f22cac34e6b2c52deca82adbf1558c2a49b066c6024e56c61db8f11fac632
46             1039f886ecc863bc71cb1b358f12ae19df33457749abe766990120d8027804ed953ac63516
47             776a914853b775079232503df966e626618e1d388a957208763516776522103887f6bf8f22
48             cac34e6b2c52deca82adbf1558c2a49b066c6024e56c61db8f11f21039f886ecc863bc71cb
49             1b358f12ae19df33457749abe766990120d8027804ed953ae686868",
50             "addresses": null,
51             "script_type": "unknown"
52         }
53     ]
54 }
55
56 Bob swap tx (BCY) created successfully!
57
58 201 Created
59
60 {
61     "tx": {
62         "block_height": -1,
63         "block_index": -1,
64         "hash":
65         "9a85a6533e7eb33990f4aec2887874f4f75f4e9bc78af361db00fc3df037d9b4",
66         "addresses": [
67             "BzFDzDVKqe7jkwpVZudGXB2Fgx7qtq4BLq"
68         ],
69         "total": 900000,
70         "fees": 100000,
71         "size": 341,
72         "vsize": 341,
73         "preference": "high",
74         "relayed_by": "103.20.198.139",
75         "received": "2023-10-24T11:29:06.583378309Z",
76         "ver": 1,

```

```

65     "double_spend": false,
66     "vin_sz": 1,
67     "vout_sz": 1,
68     "confirmations": 0,
69     "inputs": [
70         {
71             "prev_hash":
72             "a0a7e88e704df710352eef2543de91ac8ce66d8b6e63a205271f22395e03d2ef",
73             "output_index": 0,
74             "script":
75             "473044022012035dffecbe6626b98641e05692c919a59f509e4d8fa55d2d9291e04072c28
76             90220154fbc0dec6479d239bc9fb52ef4e67d95362d7479105d1dd2bd2587ed3b48bf01210
77             21505af54164eee76ba6d9731e16082768ad4a4ff2175b0fdf1f4effc23672dcb",
78             "output_value": 1000000,
79             "sequence": 4294967295,
80             "addresses": [
81                 "BzFDzDVKqe7jkwpVZudGXB2Fgx7qtq4BLq"
82             ],
83             "script_type": "pay-to-pubkey-hash",
84             "age": 1037511
85         }
86     ],
87     "outputs": [
88         {
89             "value": 900000,
90             "script":
91             "21021505af54164eee76ba6d9731e16082768ad4a4ff2175b0fdf1f4effc23672dcbac632
92             1031cafc11a94e1089f952d82852dab31c18965018da5af451b225baed5ec5741d1ac63516
93             776a914853b775079232503df966e626618e1d388a9572087635167765221021505af54164
94             eee76ba6d9731e16082768ad4a4ff2175b0fdf1f4effc23672dcb21031cafc11a94e1089f9
95             52d82852dab31c18965018da5af451b225baed5ec5741d1ae686868",
96             "addresses": null,
97             "script_type": "unknown"
98         }
99     ]
100 }
101 }
102 sleeping for 20 minutes to let transactions confirm...
103 Alice redeem from swap tx (BCY) created successfully!
104 201 Created
105 {
106     "tx": {
107         "block_height": -1,
108         "block_index": -1,
109         "hash":
110         "15326eebf3bd4eeb78898c531da4db5c608891eb3af3f75a4b2213c1102a775e",
111         "addresses": [
112             "CFCn7K7hs63cv2sXEMupexF5MA64F2qLYj"
113         ],
114         "total": 800000,
115         "fees": 100000,
116         "size": 183,

```

```

107     "vsize": 183,
108     "preference": "high",
109     "relayed_by": "103.20.198.139",
110     "received": "2023-10-24T11:49:08.068811206Z",
111     "ver": 1,
112     "double_spend": false,
113     "vin_sz": 1,
114     "vout_sz": 1,
115     "confirmations": 0,
116     "inputs": [
117         {
118             "prev_hash":
119             "9a85a6533e7eb33990f4aec2887874f4f75f4e9bc78af361db00fc3df037d9b4",
120             "output_index": 0,
121             "script":
122             "187468697349734153656372657450617373776f726431323348304502210087d763d15a3
123             b9073506bb85cf425abb7a45ba9764db1f76b7dd08723724ae8f502204486b9e322e76cd8d
124             ddc5c40f06864e4f65a9531056d9d29046c3f9aabd19f6101",
125             "output_value": 900000,
126             "sequence": 4294967295,
127             "script_type": "unknown",
128             "age": 1037516
129         }
130     ],
131     "outputs": [
132         {
133             "value": 800000,
134             "script": "76a914f22c3dd6e8ab9798943b0a57f02af4977ef863f688ac",
135             "addresses": [
136                 "CFCn7K7hs63cv2sXEMupexF5MA64F2qLYj"
137             ],
138             "script_type": "pay-to-pubkey-hash"
139         }
140     ]
141 }
142
143 Bob redeem from swap tx (BTC) created successfully!
144 201 Created
145 {
146     "tx": {
147         "block_height": -1,
148         "block_index": -1,
149         "hash":
150         "22e8b9abfeb44360c5f514c1ec180913031bda5bf0b62895ea1e61ecb17f8149",
151         "addresses": [
152             "mtYR9tdnmDjDgLtAqedNL6EfA11TAsheha"
153         ],
154         "total": 300000,
155         "fees": 100000,
156         "size": 182,
157         "vsize": 182,
158         "preference": "high",

```

```

154     "relayed_by": "103.20.198.139",
155     "received": "2023-10-24T11:49:08.505551691Z",
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             "12042d39f7c06ba28864786198cbcd3a80fe56b0fcfe182bdd3d51703298be15",
165             "output_index": 0,
166             "script":
167             "187468697349734153656372657450617373776f726431323347304402205bced5a3cce5
168             da6e29fc05f7469fdb1a0893f7319690fbef5bf70d3dffcc90402204c487c45b1bea526e31
169             49b235f9371a71fbd7b1553fd9308a3958a628aeca15f01",
170             "output_value": 400000,
171             "sequence": 4294967295,
172             "script_type": "unknown",
173             "age": 2534980
174         }
175     ],
176     "outputs": [
177         {
178             "value": 300000,
179             "script": "76a9148ee078dd9bf2f45188c45d3f50963c85d336b0b588ac",
180             "addresses": [
181                 "mtYR9tdnmDjDgLtAqeDNL6EfA11TAsheha"
182             ],
183             "script_type": "pay-to-pubkey-hash"
184         }
185     ]
186 }

```

## D

### a 解释代码内容，以及coinExchangeScript是如何工作

本次实验中补充的代码主要由两部分组成

- 第一部分是一些密钥等的补充，按照实验指导说明一步步完成即可。
  - 此处遇到的问题是Windows中cmd对单引号的不支持，经过对其进行转义后得以修复。
- 第二部分为交易脚本的编写
  - coinExchangeScript

```

1 def coinExchangeScript(public_key_sender, public_key_recipient,
    hash_of_secret):

```

```

2     return [
3         # fill this in!
4         public_key_recipient,
5         OP_CHECKSIG,
6         OP_IF,
7         OP_IF,
8             OP_HASH160,
9             hash_of_secret,
10            OP_EQUAL,
11            OP_IF,
12            OP_1,
13            OP_ENDIF,
14        OP_ELSE,
15            public_key_recipient,
16            OP_CHECKSIG,
17            OP_IF,
18            OP_1,
19            OP_ENDIF,
20        OP_ENDIF,
21    OP_ENDIF
22 ]

```

- 该脚本首先检查接收者的身份，如果能够通过签名认证，则首先检查其是否知晓秘密x，如果知晓，则说明可以赎回；如果不知晓秘密x，但能够拥有发送者的认证签名，则说明可以赎回；否则，无法赎回。

- coinExchangeScriptSig1

```

1 def coinExchangeScriptSig1(sig_recipient, secret):
2     return [
3         # fill this in!
4         secret,
5         sig_recipient
6     ]

```

- 该脚本能够实现接收者知道秘密x的情况下赎回交易

- coinExchangeScriptSig2

```

1 def coinExchangeScriptSig2(sig_sender, sig_recipient):
2     return [
3         # fill this in!
4         sig_recipient,
5         sig_sender
6     ]

```

- 该脚本能够在发送方和接收方都签署事务的情况下赎回事务

## b 以Alice用coinExchangeScript向Bob发送硬币为例

### 1) 如果Bob不把钱赎回来，Alice为什么总能拿回她的钱？

- Alice知道秘密x，因此她可以通过她自己的签名与秘密x赎回脚本
- 且加之locktime机制的存在，如果Bob一段时间后未赎回，Alice将由自己的签名与秘密赎回脚本

### 2) 为什么不能用简单的1/2 multisig来解决这个问题？

- 1/2 multisig要求在赎回资金时需要两个签名，这意味着双方必须合作。如果一方不愿意提供签名，资金将无法赎回，也就是说，存在资金被锁定的情况，除非双方都同意方可解锁。
- 1/2 multisig通常需要在线签署，不适于离线交易

## c 解释Alice (Bob) 创建的一些交易内容和先后次序，以及背后的设计原理。

1. Alice 创建一个随机字符串 x 将其作为秘密，并计算其哈希值H(x)
2. Alice 创建 DepositA，将要交换的钱输入其中但不予以广播，此时这笔钱不属于任何人；
3. Alice 创建 RefundA，向 Bob 索要签名，并将其广播至网络，同时设定 `alice_locktime`：如果 Bob 在该时间内未赎回，Alice 还能拿回自己的钱；
4. 如果 Bob 签署了 RefundA，Alice 会将 DepositA 广播至网络，但 RefundA 仍然保密；
5. Bob 创建 DepositB，将要交换的钱输入其中但不予以广播，此时这笔钱不属于任何人；
6. Bob 创建 RefundB，向 Alice 索要签名，并将其广播至网络，同时设定 `bob_locktime`：如果 Alice 在该时间内未赎回，Bob 还能拿回自己的钱；
7. 如果 Alice 签署了 RefundB，Bob 会将 DepositB 广播至网络，但 RefundB 仍然保密；
8. Alice 使用自己的正确签名与自己的秘密 x 赎回 DepositB，然后将秘密 x 广播至网络；
9. Bob 使用自己的正确签名与 Alice 广播的秘密 x 赎回 DepositA，完成交易。

这个设计的原理是创建一系列的交易，其中每个交易要么等待秘密 x 的哈希值，要么等待正确的签名以解锁。这使得 Alice 和 Bob 可以相互安全地进行资金交换，并确保在需要时能够取回自己的资金。

## d 以该作业为例，一次成功的跨链原子交换中，数字货币是如何流转的？如果失败，数字货币又是如何流转的？

- 成功
  1. 数字货币由交换货币的双方发送至网络，此时二人暂时失去这些数字货币的所有权；
  2. 交易的双方完成需要的签名认证等环节后，凭借自己获得的信息赎回网络上的数字货币，获得所有权，完成跨链原子交换。
- 失败
  1. 数字货币由交换货币的双方发送至网络，此时二人暂时失去这些数字货币的所有权；
  2. 如果交易失败，数字货币会最终由本人赎回，即流转回自己手中；