
区块链 Exercise4 实验报告

2010535 赵健坤 2013536 汤清云

实验设计

一. 解释你写的代码内容，以及 coinExchangeScript 是如何工作的

```
def coinExchangeScript(public_key_sender, public_key_recipient, hash_of_secret):  
    return [  
        # fill this in!  
        public_key_recipient,      #首先验证对方签名，两种方式都需要  
        OP_CHECKSIGVERIFY,  
        OP_IF,                      #为1时，表明使用两个签名赎回  
        public_key_sender,         #验证创建者签名  
        OP_CHECKSIG,  
        OP_ELSE,                   #为0时表明用secret x赎回  
        OP_HASH160,                #进行哈希计算  
        hash_of_secret,            #与所存的H(x)相比较  
        OP_EQUAL,  
    ]
```

这一函数用于生成存储交易的 ScriptPubKey 脚本，在跨站原子交易开始阶段被调用。Alice 方传入参数为自己和 Bob 两者的 BTC 账户公钥以及秘密 x 的哈希值；在 Bob 方传入参数为自己和 Alice 两者的 BCY 账户公钥以及秘密 x 的哈希值。该笔交易的赎回条件为：输入脚本 ScriptSig 中同时提供双方签名（交易未达成，由本人取回存款），或同时提供收款方签名和秘密 x 的值（交易达成，由对方赎回存款）。该脚本将首先验证对方签名，然后根据传入的 0/1 值判定输入脚本类型：若为 1 则输入脚本使用两个签名赎回，于是验证创建者签名；若为 0 则使用秘密 x 赎回，于是验证秘密 x 的哈希值是否正确。

因此，该输出脚本规定：由本人取回存款的输入脚本必须首先提供对方签名，然后压入 1，最后提供本人签名；由对方赎回存款的输入脚本必须首先提供秘密 x 的值，然后压入 0，最后提供赎回方签名。根据这种逻辑写出的两种赎回脚本 ScriptSig 如下：

```

32 # This is the ScriptSig that the receiver will use to redeem coins
33 def coinExchangeScriptSig1(sig_recipient, secret):
34     return [
35         # fill this in!
36         secret,
37         OP_0,
38         sig_recipient
39     ]

```

这一函数用于在秘密 x 被揭露（交易达成）的情况下让双方赎回对方发送的币，在 Alice 的 `redeem_swap` 函数中调用此函数，传入参数为 Alice BCY 账户的签名和她设置的秘密 x ；在 Bob 的 `redeem_swap` 函数中调用此函数，传入参数为 BobBTC 账户的签名和 Alice 设置的秘密 x 。

```

# This is the ScriptSig for sending coins back to the sender if unredeemed
def coinExchangeScriptSig2(sig_sender, sig_recipient):
    return [
        # fill this in!
        sig_sender,
        OP_1,
        sig_recipient
    ]

```

这一函数用于发送方在不揭露秘密 x （超时交易未达成）情况下取回自己的币；在 Alice 的 `complete_return_tx` 函数中被调用，传入参数为 Alice 和 Bob 两方 BTC 账户的签名；在 Bob 的 `complete_return_tx` 函数中被调用，传入参数为 Bob 和 Alice 两方 BCY 账户的签名。

下面以 Alice 方为例，介绍脚本验证过程。首先，ScriptSig 将秘密 x 、0、Bob 签名或 Alice 签名、秘密 x 、Bob 签名依次压栈。然后逐条压入 ScriptPubKey 指令。第一步：压栈 Bob 的公钥，弹出 Bob 的公钥及签名，并验证 Bob 的签名，如果验证失败则直接压入 FALSE 拒绝，否则继续验证。第二步：判断脚本类型。弹栈。如果栈顶为 1，表明使用两个签名赎回，这时验证 Alice 签名，若验证通过则压入 TRUE；否则栈顶为 0，表明需要判断传入的元素是不是秘密 x 。弹出秘密 x ，计算哈希并与 ScriptSig 中的值比较，如相等则压入 TRUE，不是则压入 FALSE。分支结束后，若验证通过，栈中将只留下一个 TRUE，此时交易可以赎回。

二. 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？

因为 Alice 首先创建存储交易 A 以支付 BTC 币（但还未广播出去，所以钱仍然在 Alice 手中），此交易记录在 `alice_swap_tx` 中，这一笔交易可以通过双方的 BTC 签名或者 Bob 的 BTC 签名+秘密 `x` 被取走。

之后 Alice 根据交易 A 的哈希值，创建超时赎回交易 A 的交易 B，使得当一定时间后如果 Bob 都不取走这笔钱的话，则钱会返回 Alice 手中。

以上事情完成后，Alice 会邀请 Bob 在交易 B 上签名，如果 Bob 不签名，则交易 A 永远无法广播，Alice 始终持有这笔钱；如果 Bob 签名了，那么 Alice 就拥有了自己和 Bob 双方的签名，交易 A 被广播出去，此时钱不在 Alice 或者 Bob 的手中。

倘若 Bob 没有提供跟 Alice 交换的 BCY 币的 tx，或 Alice 没有赎回 Bob 存储在 BCY 链上的存款，那么交易就没有达成，Bob 就得不到 Alice 的秘密 `x`，所以不能取走交易 A 中的币，在一定时间后交易 B 生效，Alice 将其广播，钱就能回到 Alice 手中。

三. 为什么不能用简单的 1/2 multisig 来解决这个问题？

如果使用了 1/2 multisig 则代表可以利用任何一个人的签名将钱赎回，那么 Bob 就可以在 Alice 创建交易后用自己的签名赎回 Alice 发送的币和自己想交换的币，违反规定。

四. 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。

交易次序如下：

- a. Alice 创建一个秘密 `x`，并将其进行哈希计算。
- b. Alice 创建交易 A 用于将自己的 BTC 币转发给 Bob，但并未广播出去。

为了防止 Alice 单方面赎回交易 A，交易 A 需要 Bob 签名的脚本才能赎

-
- 回。为了保证 Alice 在交易未达成时能够赎回自己的 BTC，Alice 必须得到 Bob 签名的延迟赎回脚本 B 才能将交易 A 广播。但创建交易 B 必须使用交易 A 的哈希值，因此需要先创建交易 A。
- c. Alice 创建交易 B 用于在一定时间后，若 Bob 没有取走这笔钱，将之前发出的 BTC 币返回给自己的账户。
 - d. Alice 让 Bob 在交易 B 上签名。
 - e. Alice 将交易 A 广播到区块链上，此时 Alice 的 BTC 币不在 Alice 或者 Bob 任何一人的手中。
 - f. Bob 创建交易 C 用于将自己的 BCY 币转给 Alice，其中包括交易 A 中包含的秘密 x 的哈希，但是并不广播。
 - g. Bob 创建交易 D 用于在一定时间（这段时间小于交易 B 设置的时间）后，若 Alice 没有取走这笔钱，将之前发出的 BCY 币返回给自己的账户。
 - h. Bob 让 Alice 在交易 D 上进行签名。
 - i. Bob 将交易 C 广播到区块链上，此时 Bob 的 BCY 币不在自己手中也不在 Alice 手中。
 - j. Alice 使用自己签名的带有秘密 x 的交易在规定时间内取走交易 C 中的钱（视为交易 E），同时秘密 x 被揭露。
 - k. Bob 使用自己签名的包含秘密 x 的交易将交易 A 中的钱拿走，至此一次跨链原子交易完成。
 - l. 如果 j 中 Alice 选择不取走交易 C 中币的话，超过规定时间，Bob 和 Alice 依次将交易 B、D 广播到区块链上，使用双方的签名取回自己的币。

五. 本次作业中，一次成功的跨链原子交换中，资金是如何流转的？

在步骤 a~d 中，双方的币均在各自手中，没有进行流转；在步骤 e 中，Alice 的 BTC 币不在 Alice 或者 Bob 任何一方手中；
在步骤 f~h 中，Bob 的 BCY 币仍然在自己手中；

在步骤 i 中, Bob 的 BCY 币不在 Alice 或者 Bob 任何一方手中;

步骤 j 中 Alice 获取 Bob 的 BCY 币;

步骤 k 中 Bob 获取 Alice 的 BTC 币。

六. 实验过程

使用 keygen.py 生成 Alice 的 BTC testnet 信息如下:

Private key	cNUEa7r7jHJ7wqA2BZSWDbPM5qDDZHsBpAVjbJJbg9E3S5rd9d8h
Address	mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD

使用 keygen.py 生成 Bob 的 BTC testnet 信息如下:

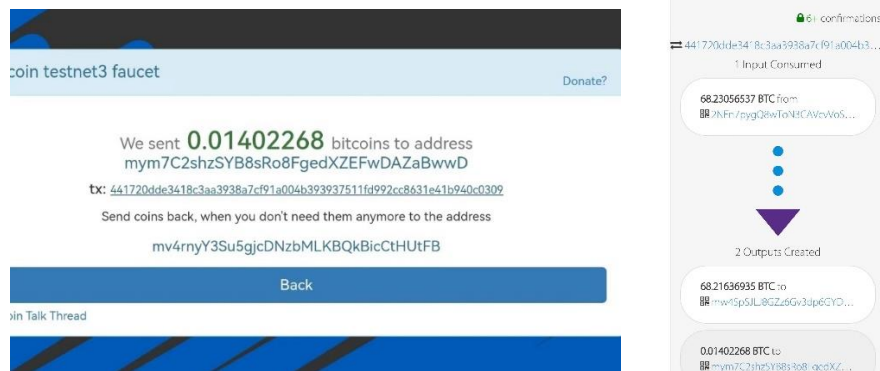
Private key	cUGJ3Lt65TVHRD59BjroKj6vZcCGxZV9tbF7J5ECb2HHMwdaJqrQ
Address	mqKpH1cMUq95KM4zLDEVjud9PLEscVekug

填入 keys.py 中:

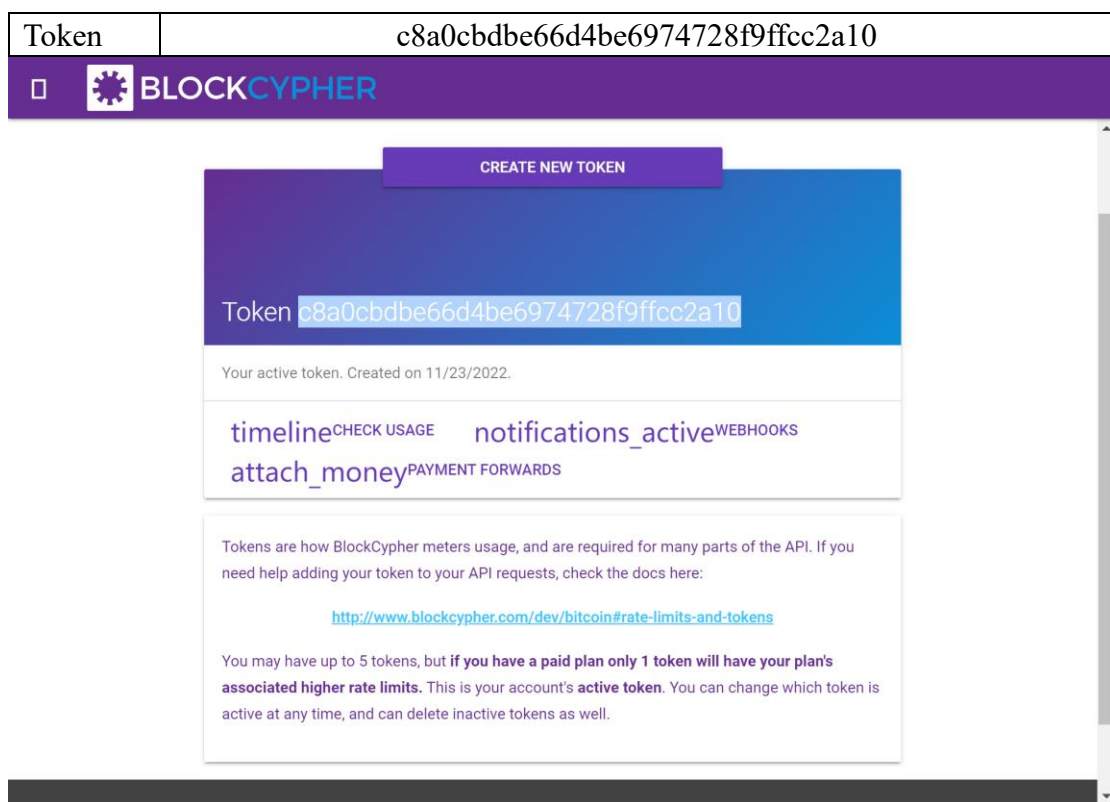
```
8 #
9 # TODO: Fill this in with address secret key for BTC testnet3
10 #
11 # Create address in Base58 with keygen.py
12 # Send coins at https://coinfaucet.eu/en/btc-testnet/
13
14 # Only to be imported by alice.py
15 # Alice should have coins!!
16 alice_secret_key_BTC = CBitcoinSecret(
17     'cNUEa7r7jHJ7wqA2BZSWDbPM5qDDZHsBpAVjbJJbg9E3S5rd9d8h')
18
19 # Only to be imported by bob.py
20 bob_secret_key_BTC = CBitcoinSecret(
21     'cUGJ3Lt65TVHRD59BjroKj6vZcCGxZV9tbF7J5ECb2HHMwdaJqrQ')
22
23 #####
24 #
```

为 Alice 获取测试币:

Hash	441720dde3418c3aa3938a7cf91a004b393937511fd992cc8631e41b940c0309
------	--



在 <https://accounts.blockcypher.com/>注册账户得到 token 为:



为 Alice 生成 BCY testnet 结果:

```
{
  "private":
    "2e8da577813ffcf5e7c5dd54dbc5150347167560e45ce32c4d279d99bdd9494",
  "public":
    "02c3b0944b8787de28c2afb77989cc3c319426276c7a341a3c62cad854a540890f",
  "address": "C42KJ7wavgTpCtK9ob2fuYNWV9ciFnhV24",
  "wif": "BptXN4bpFA3ogxy2a5qu2EF55Dxj33oNPYpLru1CKzjNz163UjP7"
}
```

为 Bob 生成 BCY testnet 结果:

```
{
  "private":
"f4a0081d6a0464a0e1eeb6588489ebc74e868368a7e9e0df2bc99a7c62e999a1",
  "public":
"024d93827557d47cee4e5fe988d452ab05648010b182c1f37a0b968a3ce33c701d",
  "address": "C4CRBV1SjhXmy4DMazNpQDcgYpJiA6yBWG",
  "wif": "BwXYrczS3RKuSMzeJ6pjJtTzdcuJo3LeBb1zvgcFcCmeLXdTYVvR"
}
```

填入代码中:

```
29 # curl -X POST https://api.blockcypher.com/v1/bcy/test/addr?token=c8a0cbdbe66d4be6974728f9f-
30 # curl -X POST https://api.blockcypher.com/v1/bcy/test/addr?token=$YOURTOKEN
31 #
32 # Send coins with
33 # curl -d '{"address": "BCY_ADDRESS", "amount": 1000000}' https://api.blockcypher.com/v1/bcy,
34 # 为bob领取测试币:
35 # curl -d '{"address": "C4CRBV1SjhXmy4DMazNpQDcgYpJiA6yBWG", "amount": 1000000}' https://api
36 # Only to be imported by alice.py
37 alice_secret_key_BCY = CBitcoinSecret.from_secret_bytes(
38 | x('2e8da577813ffcf5e7c5dd54dbc5150347167560e45ce32c4d279d99bdd9494'))
39
40 # Only to be imported by bob.py
41 # Bob should have coins!!
42 bob_secret_key_BCY = CBitcoinSecret.from_secret_bytes(
43 | x('f4a0081d6a0464a0e1eeb6588489ebc74e868368a7e9e0df2bc99a7c62e999a1'))
44
```

为 Bob 领取 BCY 测试币:

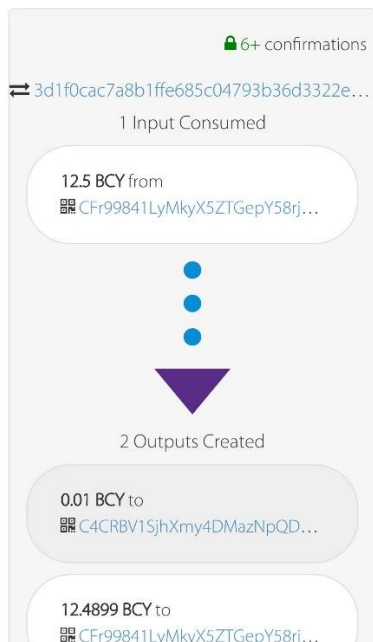
命令为:

```
curl -d '{"address": "C4CRBV1SjhXmy4DMazNpQDcgYpJiA6yBWG", "amount":
1000000}'
https://api.blockcypher.com/v1/bcy/test/faucet?token=c8a0cbdbe66d4be6
974728f9ffcc2a10
```

运行结果为:

```
{
  "tx_ref":
"3d1f0cac7a8b1ffe685c04793b36d3322e465456ce5e042bffd9a922b5a77449"
}
```

1 Transaction



划分 Alice 的 BTC 币:

```
alice.py | bob.py | keygen.py | keys.py | p2pkh.py 1 | split_test_coins.py X | swap

blockchain > split_test_coins.py > ...

28 if __name__ == '__main__':
29     SelectParams('testnet')
30
31     #####
32     # TODO: set these parameters correctly
33     # Alice's private key: cNUEa7r7jHJ7wqA2BZSWDbPM5qDDZHsBpAVjbJJbg9E3S5rd9d8h BTC
34     my_private_key = CBitcoinSecret('cNUEa7r7jHJ7wqA2BZSWDbPM5qDDZHsBpAVjbJJbg9E3S5rd9d8h')
35
36     my_public_key = my_private_key.pub
37     my_address = P2PKHBitcoinAddress.from_pubkey(my_public_key)
38
39     amount_to_send = 0.01 # amount of BTC in the output you're splitting minus fee
40     txid_to_spend = (
41         '441720dde3418c3aa3938a7cf91a004b393937511fd992cc8631e41b940c0309')
42     utxo_index = 1
43     n = 10 # number of outputs to split the input into
44     network = 'btc-test3' # either 'btc-test3' or 'bcy-test'
45
```

201 Created

```
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
    "107b9f2504262bc4d5da731dd3578b1bebf1227be33fd16832d23015f21a181b",
    "addresses": [
      "mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD"
    ],
  },
}
```



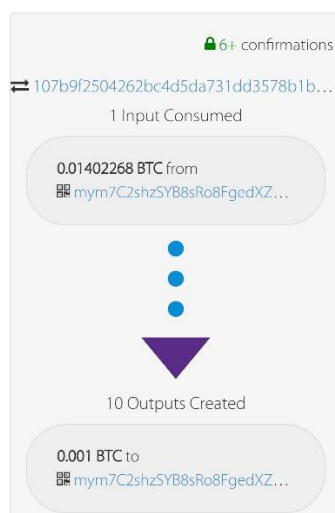
```
"total": 1000000,
"fees": 402268,
"size": 497,
"vsize": 497,
"preference": "high",
"relayed_by": "221.238.245.29",
"received": "2022-11-23T07:58:38.107965463Z",
"ver": 1,
"double_spend": false,
"vin_sz": 1,
"vout_sz": 10,
"confirmations": 0,
"inputs": [
  {
    "prev_hash":
"441720dde3418c3aa3938a7cf91a004b393937511fd992cc8631e41b940c0309",
    "output_index": 1,
    "script":
"47304402204fccb76d7a3efdd77f5b6c7c52f52c5875ad88cfd3acf1d39248fc2cf014
74ba02204962e712f60e33b96417e7015719a0de3c63e656dc7e6ab463315e92bae94
b3f012102e3583865e1e09a67b80b1065a6dc340d8ee6c8bc5712e3e6e38ac514bf25
337e",
    "output_value": 1402268,
    "sequence": 4294967295,
    "addresses": [
      "mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD"
    ],
    "script_type": "pay-to-pubkey-hash",
    "age": 2407835
  }
],
"outputs": [
  {
    "value": 100000,
    "script": "76a914c81f83847342e5e0931faf5412efa656eaf26e4c88ac",
    "addresses": [
      "mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD"
    ],
    "script_type": "pay-to-pubkey-hash"
  },
  {
    "value": 100000,
    "script": "76a914c81f83847342e5e0931faf5412efa656eaf26e4c88ac",
    "addresses": [
```

```
[
  {
    "value": 100000,
    "script": "76a914c81f83847342e5e0931faf5412efa656eaf26e4c88ac",
    "addresses": [
      "mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD"
    ],
    "script_type": "pay-to-pubkey-hash"
  },
  {
    "value": 100000,
    "script": "76a914c81f83847342e5e0931faf5412efa656eaf26e4c88ac",
    "addresses": [
      "mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD"
    ],
    "script_type": "pay-to-pubkey-hash"
  },
  {
    "value": 100000,
    "script": "76a914c81f83847342e5e0931faf5412efa656eaf26e4c88ac",
    "addresses": [
      "mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD"
    ],
    "script_type": "pay-to-pubkey-hash"
  }
]
```

```

{
  "value": 100000,
  "script": "76a914c81f83847342e5e0931faf5412efa656eaf26e4c88ac",
  "addresses": [
    "mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD"
  ],
  "script_type": "pay-to-pubkey-hash"
},
{
  "value": 100000,
  "script": "76a914c81f83847342e5e0931faf5412efa656eaf26e4c88ac",
  "addresses": [
    "mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD"
  ],
  "script_type": "pay-to-pubkey-hash"
},
{
  "value": 100000,
  "script": "76a914c81f83847342e5e0931faf5412efa656eaf26e4c88ac",
  "addresses": [
    "mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD"
  ],
  "script_type": "pay-to-pubkey-hash"
}
]
}

```



划分 Bob 的 BCY 币:

```
34 # my_private_key = CBitcoinSecret('CNuEa/r/JHJ/WQAZBzWUDPMbQUZHSBPAVJ0JJ0gYt333rQ9Q8n')
35 # Bob's private key: f4a081d6a0464a0e1eeb6588489ebc74e868368a7e9e0df2bc99a7c62e999a1 BYC
36 my_private_key = CBitcoinSecret.from_secret_bytes(x('f4a081d6a0464a0e1eeb6588489ebc74e868368a7e9e0df2bc99a7c6
37
38 my_public_key = my_private_key.pub
39 my_address = P2PKHBitcoinAddress.from_pubkey(my_public_key)
40
41 amount_to_send = 0.009 # amount of BTC in the output you're splitting minus fee
42 txid_to_spend = (
43     '3d1f0cac7a8b1ffe685c04793b36d3322e465456ce5e042bffd9a922b5a77449')
44 utxo_index = 0
45 n = 10 # number of outputs to split the input into
46 network = 'bcy-test' # either 'btc-test3' or 'bcy-test'
47
48 #
49 #
50 #####
```



201 Created

```
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
    "929eca26ffdd7a53ca87f22c3830c2c4f30e0c259654775ad944a3ba9782812d",
    "addresses": [
      "C4CRBV1SjhXmy4DMazNpQDcgYpJiA6yBWG"
    ],
    "total": 900000,
    "fees": 100000,
    "size": 497,
    "vsize": 497,
    "preference": "high",
    "relayed_by": "221.238.245.29",
    "received": "2022-11-23T08:08:02.541430608Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 10,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
        "3d1f0cac7a8b1ffe685c04793b36d3322e465456ce5e042bffd9a922b5a77449",
        "output_index": 0,
        "script":
        "47304402204e7055c045297d28306d2e3f273beaf8b15507dd380ea98f726a71b682
        a5e822022038bf5885ba1cf0724e47f11093b83facf15e320c45ff1f38da7e35d4499cb
        3ff0121024d93827557d47cee4e5fe988d452ab05648010b182c1f37a0b968a3ce33c7
        01d",
        "output_value": 1000000,
```

```

"sequence": 4294967295,
"addresses": [
  "C4CRBV1SjhXmy4DMazNpQDcgYpJiA6yBWG"
],
"script_type": "pay-to-pubkey-hash",
"age": 557658
}
],
"outputs": [
  {
    "value": 90000,
    "script": "76a91479716356fabbc31e93b0ae7b94c6a3b8da9b19c988ac",
    "addresses": [
      "C4CRBV1SjhXmy4DMazNpQDcgYpJiA6yBWG"
    ],
    "script_type": "pay-to-pubkey-hash"
  },
  {
    "value": 90000,
    "script": "76a91479716356fabbc31e93b0ae7b94c6a3b8da9b19c988ac",
    "addresses": [
      "C4CRBV1SjhXmy4DMazNpQDcgYpJiA6yBWG"
    ],
    "script_type": "pay-to-pubkey-hash"
  },
  {
    "value": 90000,
    "script": "76a91479716356fabbc31e93b0ae7b94c6a3b8da9b19c988ac",
    "addresses": [
      "C4CRBV1SjhXmy4DMazNpQDcgYpJiA6yBWG"
    ],
    "script_type": "pay-to-pubkey-hash"
  }
]

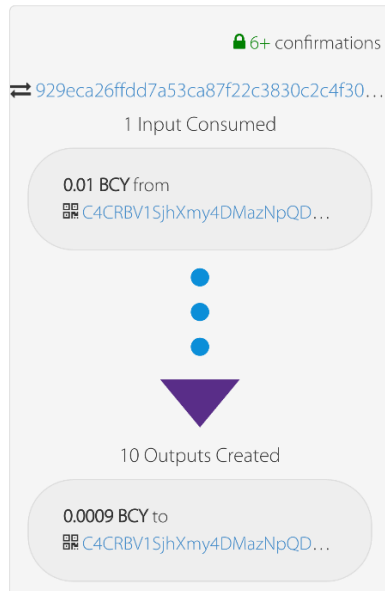
```

```
"addresses": [
  "C4CRBV1SjhXmy4DMazNpQDcgYpJiA6yBWG"
],
"script_type": "pay-to-pubkey-hash"
},
{
  "value": 90000,
  "script": "76a91479716356fabbc31e93b0ae7b94c6a3b8da9b19c988ac",
  "addresses": [
    "C4CRBV1SjhXmy4DMazNpQDcgYpJiA6yBWG"
  ],
  "script_type": "pay-to-pubkey-hash"
},
{
  "value": 90000,
  "script": "76a91479716356fabbc31e93b0ae7b94c6a3b8da9b19c988ac",
  "addresses": [
    "C4CRBV1SjhXmy4DMazNpQDcgYpJiA6yBWG"
  ],
  "script_type": "pay-to-pubkey-hash"
},
{
  "value": 90000,
  "script": "76a91479716356fabbc31e93b0ae7b94c6a3b8da9b19c988ac",
  "addresses": [
    "C4CRBV1SjhXmy4DMazNpQDcgYpJiA6yBWG"
  ],
  "script_type": "pay-to-pubkey-hash"
},
{
  "value": 90000,
  "script": "76a91479716356fabbc31e93b0ae7b94c6a3b8da9b19c988ac",
  "addresses": [
    "C4CRBV1SjhXmy4DMazNpQDcgYpJiA6yBWG"
  ],
  "script_type": "pay-to-pubkey-hash"
}
```

```

    }
  ]
}
}

```



填写 swap.py

alice.py	bob.py	keygen.py	keys.py	swap.py	swap_scripts.py	utils.py
----------	--------	-----------	---------	---------	-----------------	----------

```

blockchain > swap.py > ...
71 #alice分币hash
72 alice_txid_to_spend = "107b9f2504262bc4d5da731dd3578b1bebf1227be33fd1683d23015f21a181b"
73 alice_utxo_index = 0
74 alice_amount_to_send = 0.0008
75
76 # bob分币hash
77 bob_txid_to_spend = "929eca26ffdd7a53ca87f22c3830c2c4f30e0c259654775ad944a3ba9782812d"
78 bob_utxo_index = 0
79 bob_amount_to_send = 0.0008
80
81 # Get current block height (for locktime) in 'height' parameter for each blockchain (and put it into swap.py):
82 # curl https://api.blockcypher.com/v1/btc/test3
83 btc_test3_chain_height = 2407958
84
85 # curl https://api.blockcypher.com/v1/bcy/test
86 bcy_test_chain_height = 558827
87
88 # Parameter for how long Alice/Bob should have to wait before they can take back their coins
89 ## alice_locktime MUST be > bob_locktime
90 alice_locktime = 5
91 bob_locktime = 3
92
93 tx_fee = 0.001
94
95 # 不需要广播事务
96 broadcast_transactions = False
97 alice_redeems = False

```

使用非广播方式检验代码填写的正确性，Alice 不赎回运行结果：

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!

Alice 赎回运行结果:

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!

因此可以判断代码运行过程基本正确, 进行广播 Alice 赎回:

```
Alice swap tx (BTC) created successfully!
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
"f34c0fcbad10fbc26e436f2a61e76f8b0dd7fedba94f0b9a41b03d6c654d7f11",
    "addresses": [
      "mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD"
    ],
    "total": 70000,
    "fees": 30000,
    "size": 266,
    "vsize": 266,
    "preference": "high",
    "relayed_by": "2001:250:401:6560:e006:5214:9942:2381",
    "received": "2022-11-29T08:15:07.181239321Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"107b9f2504262bc4d5da731dd3578b1bebf1227be33fd16832d23015f21a181b",
        "output_index": 0,
        "script":
"48304502210081400f31427eb8dc81c10aee2ae9d63f9bd031f6e4bbef73d25cf9ce5
928cb14022042d48c5f262d2728bed223b59e02ecc67e44c33a9b0302a87dd47ae892
557337012102e3583865e1e09a67b80b1065a6dc340d8ee6c8bc5712e3e6e38ac514b
f25337e",
        "output_value": 100000,
        "sequence": 4294967295,
```



```

      "addresses": [
        "mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD"
      ],
      "script_type": "pay-to-pubkey-hash",
      "age": 2407844
    }
  ],
  "outputs": [
    {
      "value": 70000,
      "script":
"2103dfd733a1abc0b0b8c16bbb80b48d7ce461250c82a120ea77cb3a298d24f8d3ce
ad762102e3583865e1e09a67b80b1065a6dc340d8ee6c8bc5712e3e6e38ac514bf253
37eac63755167a914853b775079232503df966e626618e1d388a957208768",
      "addresses": null,
      "script_type": "unknown"
    }
  ]
}

```

Bob swap tx (BCY) created successfully!

201 Created

```

{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
"4a9036a0d3d50475d0422bed9f5f57f7838a9ab1d7af5435122283dd04baeac3",
    "addresses": [
      "C4CRBV1SjhXmy4DMazNpQDcgYpJiA6yBWG"
    ],
    "total": 59999,
    "fees": 30001,
    "size": 265,
    "vsize": 265,
    "preference": "high",
    "relayed_by": "2001:250:401:6560:e006:5214:9942:2381",
    "received": "2022-11-29T08:15:08.268786222Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [

```

```

    }
  ],
  "outputs": [
    {
      "value": 59999,
      "script":
"2102c3b0944b8787de28c2afb77989cc3c319426276c7a341a3c62cad854a540890f
ad7621024d93827557d47cee4e5fe988d452ab05648010b182c1f37a0b968a3ce33c7
01dac63755167a914853b775079232503df966e626618e1d388a957208768",
      "addresses": null,
      "script_type": "unknown"
    }
  ]
}
}

```

等待 20min 后结果如下：

Alice redeem from swap tx (BCY) created successfully!
 400 Bad Request
 {"error": "Error validating transaction: Transaction
 802b476ec0e66afb74310f3ee076bc2dc4794000b181c2a116d6b8bcd6cad64c
 orphaned, missing reference
 c3eaba04dd8322123554afd7b19a8a83f7575f9fed2b42d07504d5d3a036904a."}

Bob redeem from swap tx (BTC) created successfully!
 201 Created
 {
 "tx": {
 "block_height": -1,
 "block_index": -1,
 "hash":
 "d211ea2eea99bfec73d3324b6d73cc03af7123a7597c6ded3ea84d8831c76994",
 "addresses": [
 "mqKpH1cMUq95KM4zLDEVjud9PLEscVekug"
],
 "total": 60000,
 "fees": 10000,
 "size": 182,
 "vsize": 182,
 "preference": "low",
 "relayed_by": "2001:250:401:6560:e006:5214:9942:2381",
 "received": "2022-11-29T10:15:10.350972118Z",
 "ver": 1,
 "double_spend": false,
 "vin_sz": 1,
 "vout_sz": 1,
 "confirmations": 0,
 "inputs": [

```
}
]
}
}
```

发现问题:

Alice 无法获取币, 报错 `invalid transaction`, 错误情况如下:

在询问助教后得知, 出现这个错误可能是由以下两个原因导致的:

1. 等待时间过少, 20min 后交易还未得到确认, 因此为 `invalid transaction`
2. 观察报错信息发现, `reference` 的区块其 tx 恰好为 Bob 的 swap transaction 哈希值的大端存储方式:

【下图为 Bob swap transaction】

```
Bob swap tx (BCY) created successfully!
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "4a9036a0d3d50475d0422bed9f5f57f7838a9ab1d7af5435122283dd04baec3",
    "addresses": [
      "C4CRBV1SjhXmy4DMazNpQDcgYpJiA6yBWG"
    ],
    "total": 59999,
    "fees": 30001,
    "size": 265,
    "vsize": 265,
    "preference": "high",
    "relayed_by": "2001:250:401:6560:e006:5214:9942:2381",
    "received": "2022-11-29T08:15:08.268786222Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1
  }
}
```

【下图为 Alice redeem transaction 报错】

```
Alice redeem from swap tx (BCY) created successfully!
400 Bad Request
{"error": "Error validating transaction: Transaction 802b476ec0e66afb74310f3ee076bc2dc4794000b181c2a116d6b8bcd6cad64c orphaned, missing reference c3eaba04dd8322123554afd7b19a8a83f7575f9fed2b42d07504d5d3a036904a."}
```

根据助教的提示, 因此重新观察 Alice 与 Bob 两者赎回交易的代码, 发现在赎回交易函数中, Alice 使用的转换方法为 `b2x` (直接将 `byte` 转化为 `string`), 而 Bob 使用的是 `b2lx` (将 `byte` 转化为小尾存储的 `string`)。

【下图为 `byte->string` 转换函数】

```

39
40 def b2x(b):
41     """Convert bytes to a hex string"""
42     return binascii.hexlify(b).decode('utf8')
43
44 def lx(h):
45     """Convert a little-endian hex string to bytes
46
47     Lets you write uint256's and uint160's the way the Satoshi codebase shows
48     them.
49     """
50     return binascii.unhexlify(h.encode('utf8'))[::-1]
51
52 def b2lx(b):
53     """Convert bytes to a little-endian hex string
54
55     Lets you show uint256's and uint160's the way the Satoshi codebase shows
56     them.
57     """
58     return binascii.hexlify(b[::-1]).decode('utf8')
59

```

Alice

Bob

因此修改 Alice 赎回交易代码为 b2lx，重新赎回结果如下：

```

Alice swap tx (BTC) created successfully!
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
    "d996f97fa57a2ba92b52c3210a599efe23da60d8e17c8472e089a349b162bb34",
    "addresses": [
      "mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD"
    ],
    "total": 70000,
    "fees": 30000,
    "size": 265,
    "vsize": 265,
    "preference": "high",
    "relayed_by": "2001:250:401:6560:e006:5214:9942:2381",
    "received": "2022-11-29T12:15:34.388778229Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
        "107b9f2504262bc4d5da731dd3578b1bebf1227be33fd16832d23015f21a181b",
        "output_index": 1,
        "script":
        "47304402203a7a94bd42ff613ab681073f27b6ec7cca6940ddf8317e76606da0da869
        e779302203a3123cfdc5525121b8fc18ad62c544fa7777d8e249847a00b05f296b74e

```

```
72ff012102e3583865e1e09a67b80b1065a6dc340d8ee6c8bc5712e3e6e38ac514bf25
337e",
    "output_value": 100000,
    "sequence": 4294967295,
    "addresses": [
        "mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD"
    ],
    "script_type": "pay-to-pubkey-hash",
    "age": 2407844
}
],
"outputs": [
    {
        "value": 70000,
        "script":
"2103dfd733a1abc0b0b8c16bbb80b48d7ce461250c82a120ea77cb3a298d24f8d3ce
ad762102e3583865e1e09a67b80b1065a6dc340d8ee6c8bc5712e3e6e38ac514bf253
37eac63755167a914853b775079232503df966e626618e1d388a957208768",
        "addresses": null,
        "script_type": "unknown"
    }
]
}
```

Bitcoin Testnet Transaction

d996f97fa57a2ba92b52c3210a599
efe23da60d8e17c8472e089a349b
162bb34

AMOUNT TRANSACTED

0.0007 BTC

FEES

0.0003 BTC

RECEIVED

🕒 2 days ago

CONFIRMATIONS 

🔒 6+

Bob swap tx (BCY) created successfully!

201 Created

```
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
    "4fcd0d22f88de311e7885a8acb4fc426d3c4bb2710cfc7624cf8692a26f96018",
    "addresses": [
      "C4CRBV1SjhXmy4DMazNpQDcgYpJiA6yBWG"
    ],
    "total": 59999,
    "fees": 30001,
    "size": 266,
    "vsize": 266,
    "preference": "high",
    "relayed_by": "2001:250:401:6560:e006:5214:9942:2381",
    "received": "2022-11-29T12:15:34.827007387Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
```

```

"confirmations": 0,
"inputs": [
],
"outputs": [
  {
    "value": 59999,
    "script":
"2102c3b0944b8787de28c2afb77989cc3c319426276c7a341a3c62cad854a540890f
ad7621024d93827557d47cee4e5fe988d452ab05648010b182c1f37a0b968a3ce33c7
01dac63755167a914853b775079232503df966e626618e1d388a957208768",
    "addresses": null,
    "script_type": "unknown"
  }
]
}
}

```

Testnet Transaction

4fcd0d22f88de311e7885a8acb4fc
426d3c4bb2710cfc7624cf8692a26
f96018

AMOUNT TRANSACTED


0.00059999 BCY

FEES

0.00030001 BCY

RECEIVED

🕒 2 days ago

CONFIRMATIONS 

🔒 6+

等待 60min:

Alice redeem from swap tx (BCY) created successfully!

201 Created

```

{
  "tx": {
    "block_height": -1,
    "block_index": -1,

```

```
"hash":
"f472665e8da3e527914aac2f42525ac3027528cba35b6d631ceb911ce7797ef1",
  "addresses": [
    "C42KJ7wavgTpCtK9ob2fuYNWV9ciFnhV24"
  ],
  "total": 50000,
  "fees": 9999,
  "size": 183,
  "vsize": 183,
  "preference": "low",
  "relayed_by": "2001:250:401:6560:e006:5214:9942:2381",
  "received": "2022-11-29T13:15:35.280097872Z",
  "ver": 1,
  "double_spend": false,
  "vin_sz": 1,
  "vout_sz": 1,
  "confirmations": 0,
  "inputs": [
    {
      "prev_hash":
"4fcd0d22f88de311e7885a8acb4fc426d3c4bb2710cfc7624cf8692a26f96018",
      "output_index": 0,
      "script":
"187468697349734153656372657450617373776f7264313233483045022100bcd4
5b56926175d9ad63dcc8042b0eea1fba42f03a34eed99935f08e27df586c02205a0b91
9d7457112f5fc97ca4dbfa2cc91c7a276ad94ef4114e41b66c29a65ec101",
      "output_value": 59999,
      "sequence": 4294967295,
      "script_type": "unknown",
      "age": 566492
    }
  ],
  "outputs": [
    {
      "value": 50000,
      "script": "76a914778850be03c3d997bf37c8b95766a459a51f231188ac",
      "addresses": [
        "C42KJ7wavgTpCtK9ob2fuYNWV9ciFnhV24"
      ],
      "script_type": "pay-to-pubkey-hash"
    }
  ]
}
```


↔ BlockCypher Testnet Transaction

f472665e8da3e527914aac2f42525
ac3027528cba35b6d631ceb911ce
7797ef1

AMOUNT TRANSACTED

0.0005 BCY

FEES

0.00009999 BCY

RECEIVED

🕒 2 days ago

CONFIRMATIONS ⓘ

🔒 6+

Bob redeem from swap tx (BTC) created successfully!

201 Created

```
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
    "ac51df3c76fbcf80a8cb459bb0d3cba8c6832ffa679ab15c7ae953fc2ab7de3c",
    "addresses": [
      "mqKpH1cMUq95KM4zLDEVjud9PLEscVekug"
    ],
    "total": 60000,
    "fees": 10000,
    "size": 182,
    "vsize": 182,
    "preference": "low",
    "relayed_by": "2001:250:401:6560:e006:5214:9942:2381",
    "received": "2022-11-29T13:15:36.405581346Z",
    "ver": 1,
    "double_spend": false,
```

```
"vin_sz": 1,
"vout_sz": 1,
"confirmations": 0,
"inputs": [
  {
    "prev_hash":
"d996f97fa57a2ba92b52c3210a599efe23da60d8e17c8472e089a349b162bb34",
    "output_index": 0,
    "script":
"187468697349734153656372657450617373776f726431323347304402207ea8963
16ca4875471aefda818c5080cd1acefa32a6557fa4f8a3f685f3e871f022017aa9eaacce
8a2f908830e7f2666457485f2f07e9720a82e5c1c58fa2cde53a801",
    "output_value": 70000,
    "sequence": 4294967295,
    "script_type": "unknown",
    "age": 2408970
  }
],
"outputs": [
  {
    "value": 60000,
    "script": "76a9146b95fd3b64f53c8b2061f521fb31539d242c34fc88ac",
    "addresses": [
      "mqKpH1cMUq95KM4zLDEVjud9PLEscVekug"
    ],
    "script_type": "pay-to-pubkey-hash"
  }
]
}
```

此交易无法查询。