Ex4 区块链基础及应用实验4报告

姓名：梁婧涵 于泽林

学号：2112155 2111698

实验要求

在本次任务中，你需要创建一个称为跨链原子交换的交易，允许两个实体在不同的区块链上安全地交换加密货币的所有权。同样将使用 python bitcoinlib 提供启动代码。

请写一个简短的关于这个项目的设计文档文档。需要包括以下内容：

（a） 解释你写的代码内容，以及coinExchangeScript 是如何工作的。

（b） 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？

（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。

（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？

准备阶段

Alice

- **账户信息**

  BTC

private:cQpQEx2gqrHqFxaaDDbUvSMRtGA6MiKtcgaA3cLEZK9qujEXTiLD

address:micZntWbKnfYhit3MPH4h1SZK8eeUxkATX

BCY

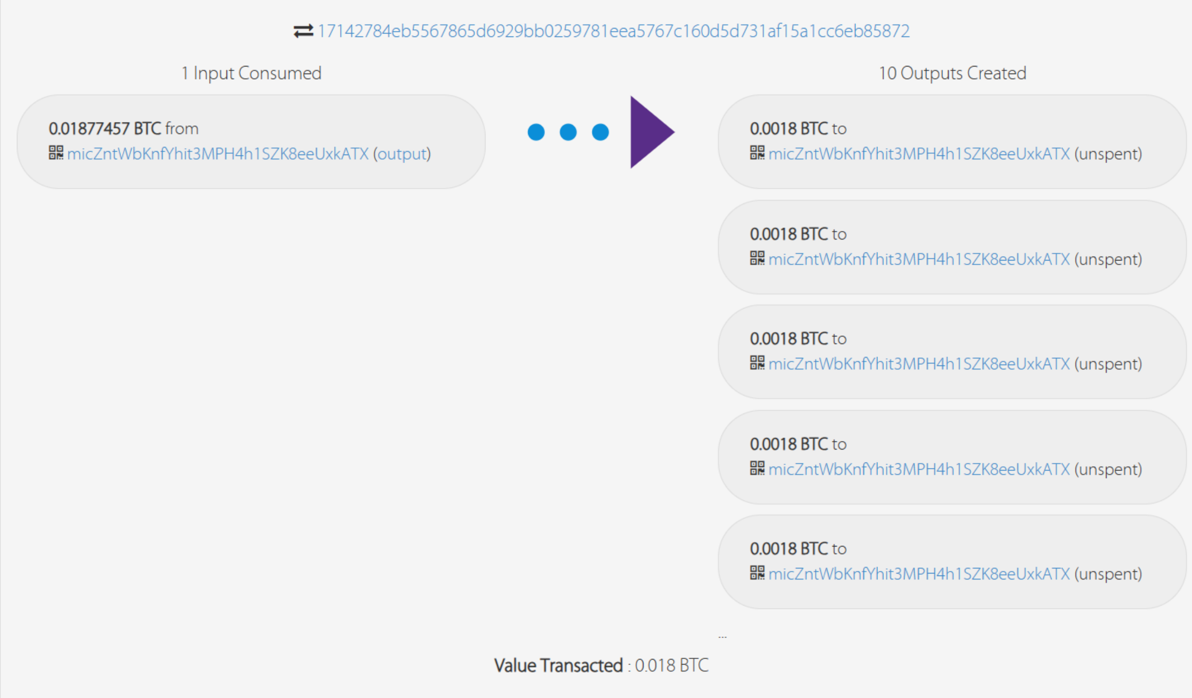
private: dd60be2add5f1f95faf899c9a51bab71b4094c6c1336f4d119a9de7e84158dea
public: 03b70f56022e0e85266ce74541b22d2bd89ba7d89669166b14f6b57f8237fe95cb
address:C4b9kD18NL5Q5sCruRz7XMi65u1YByMicp
wif:BvkMrwBSEXvAb9VQQV2uZ6EXosHxuapqoua2UatbCuXo6zA8bZhL

- **领取测试币**

交易hash：54ea5d61f87eb58fa660633dc973eef6c5716f855fc9a737be036cefbd3ba3ea

- **分币**

将0.018分成了十份，每份0.0018



⇄ 17142784eb5567865d6929bb0259781eea5767c160d5d731af15a1cc6eb85872

1 Input Consumed

0.01877457 BTC from
micZntWbKnfYhit3MPH4h1SZK8eeUxkATX (output)

10 Outputs Created

0.0018 BTC to
micZntWbKnfYhit3MPH4h1SZK8eeUxkATX (unspent)

0.0018 BTC to
micZntWbKnfYhit3MPH4h1SZK8eeUxkATX (unspent)

0.0018 BTC to
micZntWbKnfYhit3MPH4h1SZK8eeUxkATX (unspent)

0.0018 BTC to
micZntWbKnfYhit3MPH4h1SZK8eeUxkATX (unspent)

0.0018 BTC to
micZntWbKnfYhit3MPH4h1SZK8eeUxkATX (unspent)

...

Value Transacted : 0.018 BTC

Bob

- **账户信息**

BTC

private:cSZRoKXDa9Fdw9BDpBF14FJfcbBwZxapK7AQ5Ks8VLWEZWStMN9o

address:mzbwQ8H1k7kbLviw631gAuKz6aqe5hr6Ji

BCY

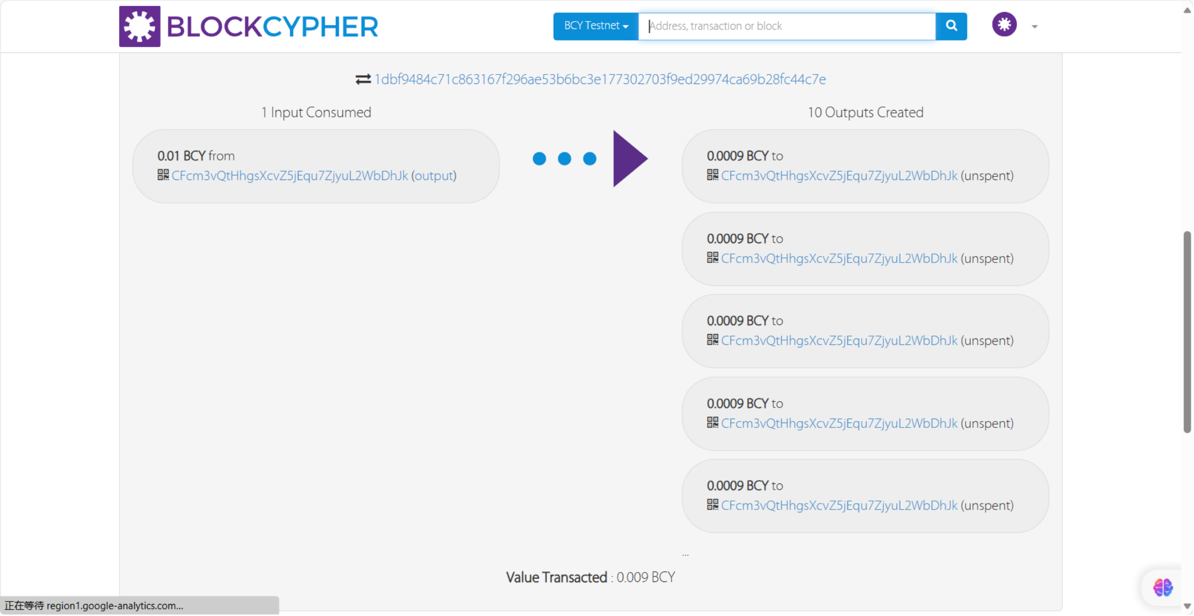
private:22f9033e01b5190af3cd8718bd002dfea09d438a468ab09e91f648d66b6a7a82
public:031d4ddca11daa54643bc7523b45e5b824df55c84156b66f3e0c0fc19d3ebf37e6
address:CFcm3vQtHhgsXcvZ5jEqu7ZjyuL2WbDhJk
wif:BpW1iUTbwocKoNya9RZVzXE6WkhkTnBZ61iXrMnHzpuQFFNvULes

- **领取测试币**

交易hash：b3779226ebbd7f91a1b9faec17d518f3a60f233725200115d4ff37a0f74793cf

- **分币**

将0.009分成10份，每份0.0009



⇄ 1dbf9484c71c863167f296ae53b6bc3e177302703f9ed29974ca69b28fc44c7e

1 Input Consumed

0.01 BCY from
CFcm3vQtHhgsXcvZ5jEqu7ZjyuL2WbDhJk (output)

10 Outputs Created

0.0009 BCY to
CFcm3vQtHhgsXcvZ5jEqu7ZjyuL2WbDhJk (unspent)

0.0009 BCY to
CFcm3vQtHhgsXcvZ5jEqu7ZjyuL2WbDhJk (unspent)

0.0009 BCY to
CFcm3vQtHhgsXcvZ5jEqu7ZjyuL2WbDhJk (unspent)

0.0009 BCY to
CFcm3vQtHhgsXcvZ5jEqu7ZjyuL2WbDhJk (unspent)

0.0009 BCY to
CFcm3vQtHhgsXcvZ5jEqu7ZjyuL2WbDhJk (unspent)

...

Value Transacted : 0.009 BCY

正在等待 region1.google-analytics.com...

实验原理与过程

场景：*Alice 用 1BTC 与 Bob 交换 3ETH*。

Alice

1. 生成随机数 a 并计算 hash(a)
2. 生成 1BTC 的比特币交易 tx1，但不先广播。tx1 的输出是分支输出：当解锁脚本满足下面某个分支时，可以花费 tx1 里的 1BTC
    1. Alice 和 Bob 的签名
    2. hash(a) 的原像和 Bob 的签名
3. 生成交易 tx11，该交易把 1BTC 从 tx1 转到 Alice 自己的地址里，有 48h locktime，即要前一笔交易上链后过 48h，本交易才能上链。这笔交易是为了保证在整个交换过程失败时，Alice 可以取回她的钱。
4. 请求 Bob 对 tx11 的签名。此后，Alice 再附上自己的签名，tx11 就同时有 Alice 和 Bob 的签名。但 Alice 不能上链该交易，她需要等到 48h 的 locktime。
5. 广播 tx1，该交易上链。

Bob

1. **确认 tx1 上链后**，生成 3ETH 的以太坊交易 tx2，但先不广播。tx2 的输出也是分支输出：当解锁脚本满足下面某个分支时，可以花费 tx2 里的 3ETH
    1. Alice 和 Bob 的签名
    2. hash(a) 的原像和 Alice 的签名
2. 生成交易 tx21，该交易可以在 24h locktime（一定要比 tx11 的 48h locktime 短）之后，把 3ETH 从 tx2 转回 Bob 的以太坊地址里。
3. 请求 Alice 对 tx21 的签名
4. 广播 tx2，该交易上链。

成功的情况

1. Alice 确认 tx2 上链后，在 24h 内构造并广播交易 tx22：将 3ETH 从 tx2 里转到 Alice 的以太坊地址里（满足 tx2 的解锁条件2：揭露 a 和 Alice 的签名）。tx22 上链以太坊网络。

2. Bob 从广播的 tx22 里得到 a 后，构造交易并广播 tx12：将 1BTC 从 tx1 里转到 Bob 的比特币地址里（满足 tx1 的解锁条件2：揭露 a 和 Bob 的签名）。tx12 上链比特币网络。
3. 交易完成

失败的情况

1. 若 24h 内，Alice 没有构造并广播交易 tx22。
2. 则 24h 后，Bob 签名并广播 tx21（超过 locktime，且同时有 Alice 和 Bob 的签名），把 3ETH 转回给自己。tx21 上链以太坊网络。
3. 48h 后，Alice 同理广播 tx11，把 1BTC 转回给自己。tx11 上链比特币网络。
4. 交易失败，但双方都不会损失钱。

前一个交易应该等到后一个交易完全上链，才能保证整个过程的绝对安全，双方都不会损失钱。

> tx11 表示满足 tx1 解锁条件 1 的交易，tx12 表示满足 tx1 解锁条件 2 的交易；tx21 和 tx22 同理

代码分析

```
def coinExchangeScript(public_key_sender, public_key_recipient, hash_of_secret):
    return [
        # fill this in!
        # 先判断栈顶是否是接收方签名
        public_key_recipient,
        OP_CHECKSIGVERIFY,
        #然后判断栈顶的发送方签名或者秘密
        OP_DUP,
        public_key_sender,
        OP_CHECKSIG,
        #如果是发送方签名则直接通过
        OP_IF,
        OP_DROP,
        OP_1,
        #如果不是发送方签名还要检验是否是秘密
        OP_ELSE,
        OP_HASH160,
        hash_of_secret,
        OP_EQUAL,
        OP_ENDIF
    ]
```

主要思想是这个交易的两个解锁条件都包含了接收方的签名，那么首先验证它。若接收方签名有效则继续验证接下来验证发送方签名或者是secret

```
def coinExchangeScriptSig1(sig_recipient, secret):
    return [
        # fill this in!
        secret,
        sig_recipient
    ]

# 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,
        sig_recipient
    ]
```

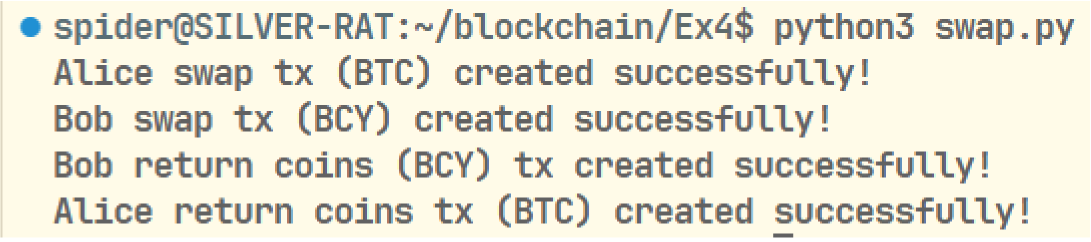
交易成功时需要提供自己的签名（自己作为接收方）和秘密的原像a，失败时要提供接收方签名和自己的签名（自己作为发送方）

实验结果

不广播（本地测试）

broadcast_transactions = False

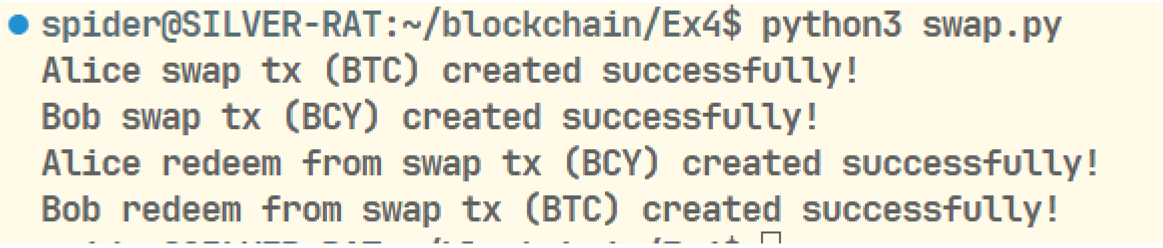
alice_redeems = False



```
● spider@SILVER-RAT:~/blockchain/Ex4$ python3 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!
```

broadcast_transactions = False

alice_redeems = True



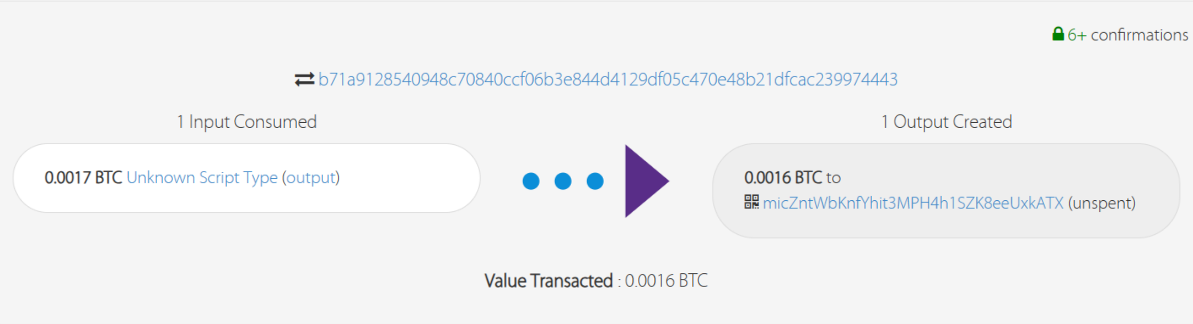
```
● spider@SILVER-RAT:~/blockchain/Ex4$ python3 swap.py
  Alice swap tx (BTC) created successfully!
  Bob swap tx (BCY) created successfully!
  Alice redeem from swap tx (BCY) created successfully!
  Bob redeem from swap tx (BTC) created successfully!
```

广播

broadcast_transactions = True

alice_redeems = False

Alice并没有赎回交易导致这次跨链原子交换没有成功，两人的转账各自返回各自账户



6+ confirmations

⇄ b71a9128540948c70840ccf06b3e844d4129df05c470e48b21dfcac239974443

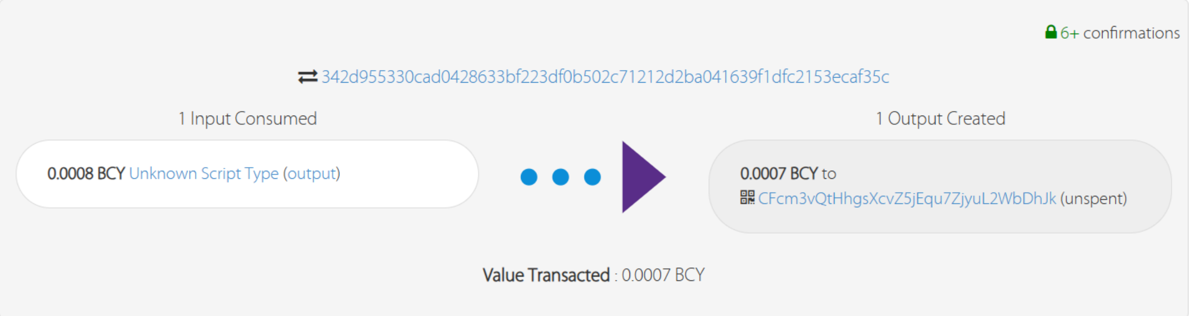
1 Input Consumed

0.0017 BTC Unknown Script Type (output)

1 Output Created

0.0016 BTC to
micZntWbKnfYhit3MPH4h1SZK8eeUxkATX (unspent)

Value Transacted : 0.0016 BTC



6+ confirmations

⇄ 342d955330cad0428633bf223df0b502c71212d2ba041639f1dfc2153ecaf35c

1 Input Consumed

0.0008 BCY Unknown Script Type (output)

1 Output Created

0.0007 BCY to
CFcm3vQtHhgsXcvZ5jEqu7ZjyuL2WbDhJk (unspent)

Value Transacted : 0.0007 BCY

> 注意alice.py和bob.py里面的return_coins_tx函数里的b2x应该改成b2lx

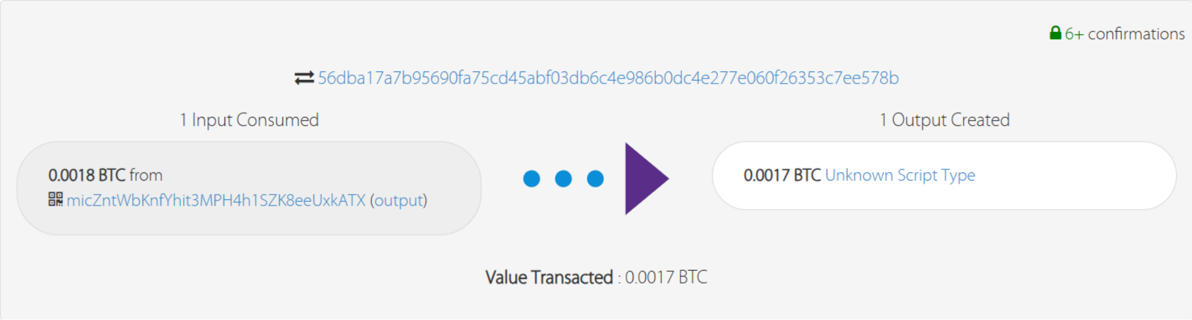
output如下

```
Alice swap tx (BTC) created successfully!
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
"58ba622acc7ee5b597b6893c9f62b3ab476ea5b5170a0395515fcbf69fbdcbeb",
    "addresses": [
      "micZntWbKnfYhit3MPH4h1SZK8eeUxkATX"
    ],
    "total": 170000,
    "fees": 10000,
    "size": 265,
    "vsize": 265,
    "preference": "low",
    "relayed_by": "60.29.153.26",
    "received": "2023-11-09T00:51:16.184908388Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"17142784eb5567865d6929bb0259781eea5767c160d5d731af15a1cc6eb85872",
        "output_index": 8,
        "script":
"47304402202a5d110f3360cdfb8a7d5eb00b3a97bbf6d77f30a8d95629f1bca9caf3f0a291
02202daffaee5a37c6f8d35f0f3f4d5d8fc90e6d298dd3b75a73618dde422e30b1d00121022
f44f6a8373a192a6ad3e294d740ab6638eff247af3de920c2f1caa79934f5fb",
        "output_value": 180000,
        "sequence": 4294967295,
        "addresses": [
          "micZntWbKnfYhit3MPH4h1SZK8eeUxkATX"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2537312
      }
    ],
    "outputs": [
      {
        "value": 170000,
        "script":
"2103ff3807fd635501ff01748832fead2404b48ac851cf442780a41846d7dda5d3a7ad7621
022f44f6a8373a192a6ad3e294d740ab6638eff247af3de920c2f1caa79934f5fbac6375516
7a914853b775079232503df966e626618e1d388a957208768",
        "addresses": null,
        "script_type": "unknown"
      }
    ]
  }
}
Bob swap tx (BCY) created successfully!
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
"82fd925be0a0d571ae9cba75ce71ac9f40c7e0604ee434319e5007cd8069f94c",
    "addresses": [
      "CFcm3vQtHhgsXcvZ5jEqu7ZjyuL2WbDhJk"
    ],
    "total": 80000,
    "fees": 10000,
    "size": 265,
    "vsize": 265,
    "preference": "low",
    "relayed_by": "60.29.153.26",
    "received": "2023-11-09T00:51:17.492028172Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"1dbf9484c71c863167f296ae53b6bc3e177302703f9ed29974ca69b28fc44c7e",
        "output_index": 8,
        "script":
"473044022022216315d1f8e60f8647ebfeb685ef4e981ba13f257669c6dc8f6986c814d6e26
02204a5efa10445775eb8ddb918cd1d70b3c5ff1d5c642bff324958f51e65bd30e060121031
d4ddca11daa54643bc7523b45e5b824df55c84156b66f3e0c0fc19d3ebf37e6",
        "output_value": 90000,
        "sequence": 4294967295,
        "addresses": [
          "CFcm3vQtHhgsXcvZ5jEqu7ZjyuL2WbDhJk"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 1057535
      }
    ],
    "outputs": [
      {
        "value": 80000,
        "script": "2103b70f56022e0e85266ce74541b22d2bd89ba7d89669166b14f6b57f8237fe95cbad7621031d4ddca11daa54643bc7523b45e5b824df55c84156b66f3e0c0fc19d3ebf37e6ac63755167a914853b775079232503df966e626618e1d388a957208768",
        "addresses": null,
        "script_type": "unknown"
      }
    ]
  }
}
Sleeping for 20 minutes to let transactions confirm...
Bob return coins (BCY) tx created successfully!
Alice return coins tx (BTC) created successfully!
Sleeping for bob_locktime blocks to pass locktime...
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "342d955330cad0428633bf223df0b502c71212d2ba041639f1dfc2153ecaf35c",
    "addresses": [
      "CFcm3vQtHhgsXcvZ5jEqu7ZjyuL2WbDhJk"
    ],
    "total": 70000,
    "fees": 10000,
    "size": 230,
    "vsize": 230,
    "preference": "low",
    "relayed_by": "111.33.78.4",
    "received": "2023-11-09T01:45:48.173140779Z",
    "ver": 1,
    "lock_time": 1057538,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "82fd925be0a0d571ae9cba75ce71ac9f40c7e0604ee434319e5007cd8069f94c",
        "output_index": 0,
        "script": "473044022076bed9c23a075e16cbce688680be492e755b255de6b5ff2cafc6d22c6c35a670022043c94c214ba3c18f2b576d5a9d118b3bc8cb6124508c976fae8bf70a029e927501483045022100b7fb8b046eddfad5a5196c783db84bef3cf8b0a8c4d9c31de6ed73a6aee5f80f022022b1d62d960ea2f88051d815154b5b349a8cdf3b10654afbd20acb963eb3241d01",
        "output_value": 80000,
        "sequence": 4294967295,
        "script_type": "unknown",
        "age": 1059914
      }
    ],
    "outputs": [
      {
        "value": 70000,
        "script": "76a914f6b55750a9766cb57cd7dd6937003face6a69f8988ac",
        "addresses": [
          "CFcm3vQtHhgsXcvZ5jEqu7ZjyuL2WbDhJk"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}
Sleeping for alice_locktime blocks to pass locktime...
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "b71a9128540948c70840ccf06b3e844d4129df05c470e48b21dfcac239974443",
    "addresses": [
      "micZntWbKnfYhit3MPH4h1SZK8eeUxkATX"
    ],
    "total": 160000,
    "fees": 10000,
    "size": 230,
    "vsize": 230,
    "preference": "low",
    "relayed_by": "111.33.78.4",
    "received": "2023-11-09T02:11:27.221701725Z",
    "ver": 1,
    "lock_time": 2537317,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "58ba622acc7ee5b597b6893c9f62b3ab476ea5b5170a0395515fcbf69fbdcbeb",
        "output_index": 0,
        "script": "483045022100c5c38a97a0dc1b13d8bcfd9bef45273c37b1de7c884554279b3c251c63932ae602206caf68c5ed892712fd09d99e5f69b9acd6eed1a00754633e276ff91a5f0f785c0147304402206a32e9a2de60b38a1752a5153b8709a28f1b9cbad17ed859c0cce215f52ada93022029a409655e3db87ba25e5fb72ec62f6a3e1d6f1a3c5e58b2eca05dc43d1fb70001",
        "output_value": 170000,
        "sequence": 4294967295,
        "script_type": "unknown",
        "age": 2537593
      }
    ],
    "outputs": [
      {
        "value": 160000,
        "script": "76a91421f816b4812d45880c1f64f97c824e5e1f4238ec88ac",
        "addresses": [
          "micZntWbKnfYhit3MPH4h1SZK8eeUxkATX"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}
```

broadcast_transactions = True

alice_redeems = True

Alice转0.0017BTC给Bob，同时Bob转0.0008BCY给Alice



6+ confirmations

⇄ 56dba17a7b95690fa75cd45abf03db6c4e986b0dc4e277e060f26353c7ee578b

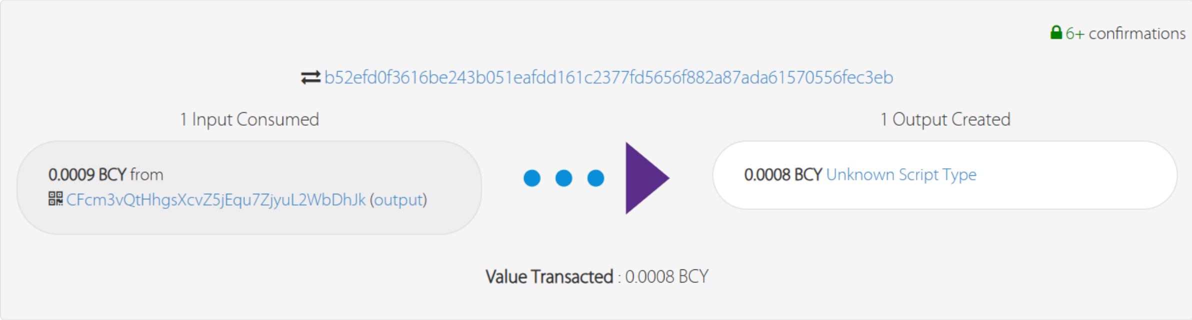
1 Input Consumed

0.0018 BTC from
micZntWbKnfYhit3MPH4h1SZK8eeUxkATX (output)

1 Output Created

0.0017 BTC Unknown Script Type

Value Transacted : 0.0017 BTC



6+ confirmations

⇄ b52efd0f3616be243b051eafdd161c2377fd5656f882a87ada61570556fec3eb

1 Input Consumed

0.0009 BCY from
CFcm3vQtHhgsXcvZ5jEqu7ZjyuL2WbDhJk (output)

1 Output Created

0.0008 BCY Unknown Script Type

Value Transacted : 0.0008 BCY

output如下

```
Alice swap tx (BTC) created successfully!
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
"56dba17a7b95690fa75cd45abf03db6c4e986b0dc4e277e060f26353c7ee578b",
    "addresses": [
      "micZntWbKnfYhit3MPH4h1SZK8eeUxkATX"
    ],
    "total": 170000,
    "fees": 10000,
    "size": 265,
    "vsize": 265,
    "preference": "low",
    "relayed_by": "221.238.245.29",
    "received": "2023-11-08T02:54:48.471690748Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"17142784eb5567865d6929bb0259781eea5767c160d5d731af15a1cc6eb85872",
        "output_index": 2,
        "script":
"4730440220795858b60cc2338b5aa02e759fca742e853ed07adb8261d21fa95bb4bbf00455
022052d4ffcc6c84f973eb6f810e542d2fb669317646ef144e0e0a41d809dfa16f950121022
f44f6a8373a192a6ad3e294d740ab6638eff247af3de920c2f1caa79934f5fb",
        "output_value": 180000,
        "sequence": 4294967295,
        "addresses": [
          "micZntWbKnfYhit3MPH4h1SZK8eeUxkATX"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2537312
      }
    ],
    "outputs": [
      {
        "value": 170000,
        "script":
"2103ff3807fd635501ff01748832fead2404b48ac851cf442780a41846d7dda5d3a7ad7621
022f44f6a8373a192a6ad3e294d740ab6638eff247af3de920c2f1caa79934f5fbac6375516
7a914853b775079232503df966e626618e1d388a957208768",
        "addresses": null,
        "script_type": "unknown"
      }
    ]
  }
}
Bob swap tx (BCY) created successfully!
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
"b52efd0f3616be243b051eafdd161c2377fd5656f882a87ada61570556fec3eb",
    "addresses": [
      "CFcm3vQtHhgsXcvZ5jEqu7ZjyuL2WbDhJk"
    ],
    "total": 80000,
    "fees": 10000,
    "size": 265,
    "vsize": 265,
    "preference": "low",
    "relayed_by": "221.238.245.29",
    "received": "2023-11-08T02:54:49.374538903Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"1dbf9484c71c863167f296ae53b6bc3e177302703f9ed29974ca69b28fc44c7e",
        "output_index": 2,
        "script":
"473044022100982ceb470eab90ed7f394a3fe1237f029692a21442ef4e4530dd4b39708d68
9e021f3398bec3993f2e1ec4938a3d2c42fb98a355dfe39f51d08e38243d9448701a0121031
d4ddca11daa54643bc7523b45e5b824df55c84156b66f3e0c0fc19d3ebf37e6",
        "output_value": 90000,
        "sequence": 4294967295,
        "addresses": [
          "CFcm3vQtHhgsXcvZ5jEqu7ZjyuL2WbDhJk"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 1057535
      }
    ],
    "outputs": [
      {
        "value": 80000,
        "script":
"2103b70f56022e0e85266ce74541b22d2bd89ba7d89669166b14f6b57f8237fe95cbad7621
031d4ddca11daa54643bc7523b45e5b824df55c84156b66f3e0c0fc19d3ebf37e6ac6375516
7a914853b775079232503df966e626618e1d388a957208768",
        "addresses": null,
        "script_type": "unknown"
      }
    ]
  }
}
Sleeping for 20 minutes to let transactions confirm...
Alice redeem from swap tx (BCY) created successfully!
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
"dd3cbda42fbdb8e4bdbc6ff7004ed870ad5b3e93f023358ed7a637ea567ae9e4",
    "addresses": [
      "C4b9kD18NL5Q5sCruRz7XMi65u1YByMicp"
    ],
    "total": 70000,
    "fees": 10000,
    "size": 183,
    "vsize": 183,
    "preference": "low",
    "relayed_by": "60.29.153.22",
    "received": "2023-11-08T03:17:00.528070455Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "b52efd0f3616be243b051eafdd161c2377fd5656f882a87ada61570556fec3eb",
        "output_index": 0,
        "script": "1874686973497341536563726574506173737776f726431323348304502210 0d9853b83059b0d6f89654d6d5706455009ab01a80c6c274a5915960cb36ccc6002202b678ed81c0b2f6c25ffc29274ba9ef52fcef5285175795fb3979e8d71dbc26901",
        "output_value": 80000,
        "sequence": 4294967295,
        "script_type": "unknown",
        "age": 1058599
      }
    ],
    "outputs": [
      {
        "value": 70000,
        "script": "76a9147dbe11ec9aaa90b8779758c3b982b3f10604938388ac",
        "addresses": [
          "C4b9kD18NL5Q5sCruRz7XMi65u1YByMicp"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}
Bob redeem from swap tx (BTC) created successfully!
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "72f288490cce74ab3fda274355fff59e4cd74269b2fee909c3d22f5913850fcb",
    "addresses": [
      "mzbwQ8H1k7kbLviw631gAuKz6aqe5hr6Ji"
    ],
    "total": 160000,
    "fees": 10000,
    "size": 182,
    "vsize": 182,
    "preference": "low",
    "relayed_by": "60.29.153.22",
    "received": "2023-11-08T03:17:01.612959133Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "56dba17a7b95690fa75cd45abf03db6c4e986b0dc4e277e060f26353c7ee578b",
        "output_index": 0,
        "script": "187468697349734153656372657450617373776f72643132334730440220304964e0d176e2dc12cb1ee8275a8db33a79f0a051c181e453517b361b041c8002207c5b3187a900c523e21addd93b3c8ca13c7e2d48e60c0a792fe1d9ac6312176c01",
        "output_value": 170000,
        "sequence": 4294967295,
        "script_type": "unknown",
        "age": 2537445
      }
    ],
    "outputs": [
      {
        "value": 160000,
        "script": "76a914d15bb8eb10be545498d9555555ebd3127f0c3e8988ac",
        "addresses": [
          "mzbwQ8H1k7kbLviw631gAuKz6aqe5hr6Ji"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}
```

问题详解

1、 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？

- 以介绍实验原理使用的场景为例，如果Bob不把他自己的3ETH赎回，那么无论Alice是否解锁这3ETH，她都可以在48h之后通过tx11拿回自己的钱
- 实现双方得到，又能自己赎回使用1/2 multisig，在双方可信的状态下可以实现。但由于初始模型建立交换货币的双方不可信，如果使用1/2 multisig，每一方都有同时兑换两笔交易的能力，失去公平性，不能操作。

2、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。

- alice创建tx1，tx1满足只有输入x和bob签名或者alice签名和bob签名才能进行交易

  并没有使该交易广播出去，因为alice没有获得bob的签名，所以一旦广播出去也可能无法赎回。交易的目的就是为了后续能够兑换赎回
- alice创建tx11，可以赎回tx1的钱，将这笔钱锁定是为了alice过一段时间才能执行赎回脚本，给bob足够时间兑换交易
- bob对交易tx11签名，alice获得bob签名后将tx1广播，如果bob不签名，前面的消息没有广播，没有影响。bob签名后alice用自己的签名和bob签名赎回钱。如果赎回脚本解锁bob还没有兑换，alice就可以直接赎回这笔钱。alice把tx1广播，tx1不可篡改，bob兑换后或赎回脚本锁定结束后alice才能将钱赎回
- bob创建tx2，与alice相似，一旦交易广播，alice可以直接兑换交易，所以暂时不广播
- bob创建tx21，具备赎回自己交易的能力，如果alice不签名，bob不上链tx2
- alice对交易签名，bob得到alice签名，bob将tx2广播，广播后，alice得到secret和自己签名，可以兑换钱，当alice兑换完钱后，secret会暴露，bob得到secret后，也能通过上链tx12兑换tx1，双方完成兑换。alice不兑换，超时后双方都可以赎回交易

3、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

以Alice首先发起为例，Bob的钱会流转到该链上的Alice账户里，之后Alice的钱会流转到Bob账户里（此时是另一条链）

- 失败

这种情况下，双方都会解锁自己之前锁定的交易，都没有损失资金