区块链第四次作业

> 2111460 张洋 2111617 尚然

前期准备

原子跨链交换如何工作?

参考比特币 wiki 页面中的原子跨链交易:

```
 A picks a random number x
 A creates TX1: "Pay w BTC to <B's public key> if (x for H(x) known and signed by B) or (signed by A & B)"
 A creates TX2: "Pay w BTC from TX1 to <A's public key>, locked 48 hours in the future, signed by A"
 A sends TX2 to B
 B signs TX2 and returns to A
 1) A submits TX1 to the network
 B creates TX3: "Pay v alt-coins to <A-public-key> if (x for H(x) known and signed by A) or (signed by A & B)"
 B creates TX4: "Pay v alt-coins from TX3 to <B's public key>, locked 24 hours in the future, signed by B"
 B sends TX4 to A
 A signs TX4 and sends back to B
 2) B submits TX3 to the network
 3) A spends TX3, revealing x
 4) B spends TX1 using x
```

BTC testnet密钥

- Alice

  ```
  Private key: cP9oLiDuhM6vqCjAv2Rdqsqp4poGgfcqeXL4CvkJDZxY2Eq5v77o
  Address: mowj6ZPEFf6pyai5rSESMXwzjFuqBVtui2
  ```

- Bob

  ```
  Private key: cUD4avJR6rgFaekSdaUQx8xFVknmkWjq3eox9zv1EDbaQNsJdnec
  Address: mhPUcfJPXaaqiFu9mXbDxBoPZ3zdwP53th
  ```

BCY testnet密钥

- Alice

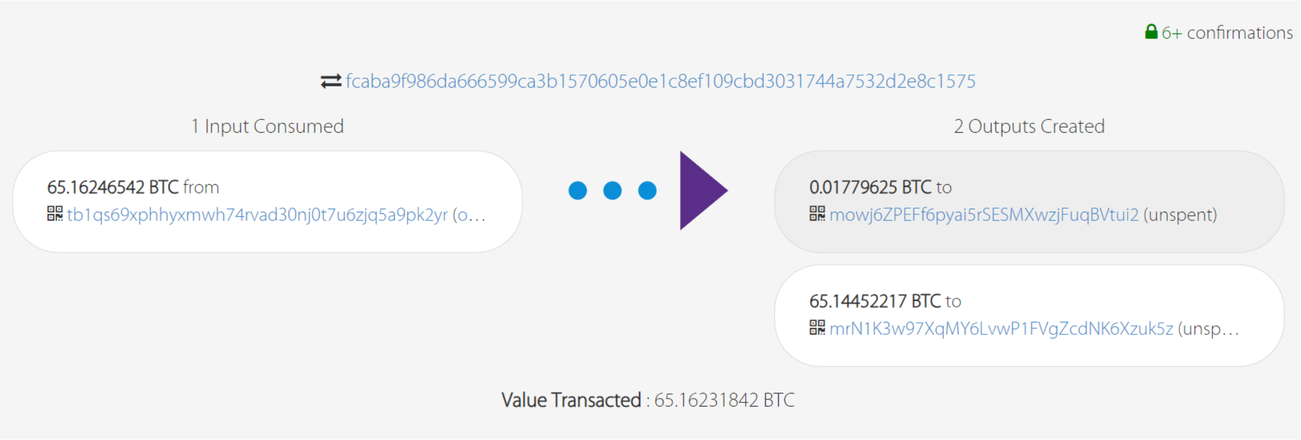
```
curl -X POST https://api.blockcypher.com/v1/bcy/test/addrs?
token=c3c87eaa46dd4fa7a511a3dc3bb6f6ca
{
"private": "1e108886ca36f64562252304a1e99ed62068923eda9dadf5d67e1826136cda9c",
"public": "038ecfcc7682eed146a22730cd22960736b95cf62be67c93c1344c13be8095ae25",
"address": "C56cegme2fHraiK8m7izL87FCM7KSF8XCh",
"wif": "BpLUMPtR8ZoFGQWa6y6mFVraxD3GK3irNaasE7m34LaxeYCEVaWr"
}
```

- Bob

```
curl -X POST https://api.blockcypher.com/v1/bcy/test/addrs?
token=c3c87eaa46dd4fa7a511a3dc3bb6f6ca
{
  "private": "42efd6093c9fa066b437b17afb61a3b988f7cd8dbf57c3771026a847ad203d6d",
  "public": "0322f835d86cb9c501d7dcd0d5612643015aac1bac46c5cb1c9384452be30c0a33",
  "address": "C1VcGk74gGBqDhrAShUAkEUwuAYAy1fcaJ",
  "wif": "Bqa9ViUJkYor1C6H7h48F1bjWiBWEpoPwF7k7tsMHCvFRGEDWJKY"
}
```

领币

- Alice



6+ confirmations

⇄ fcaba9f986da666599ca3b1570605e0e1c8ef109cbd3031744a7532d2e8c1575

1 Input Consumed

65.16246542 BTC from
tb1qs69xphhyxmwh74rvad30nj0t7u6zjq5a9pk2yr (o…

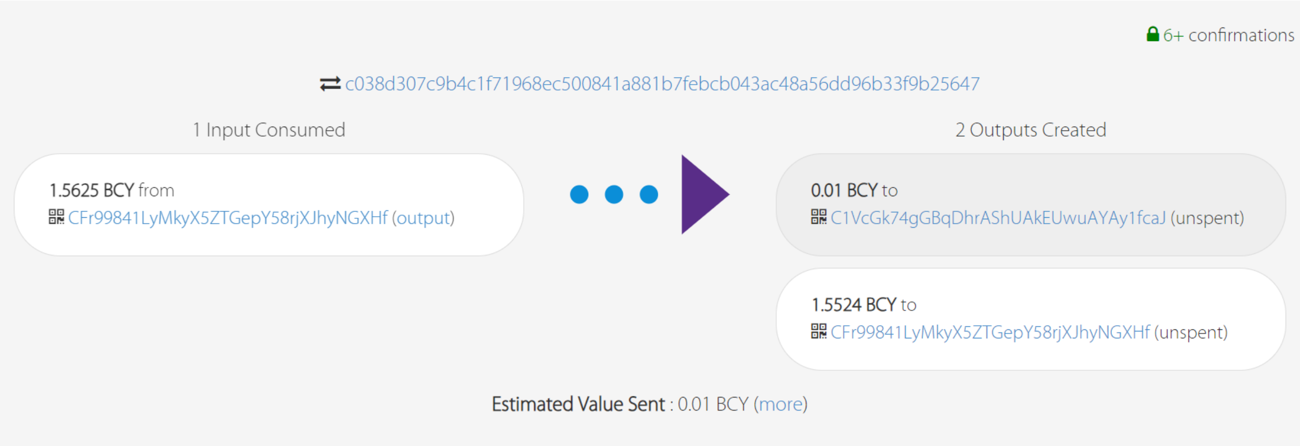
2 Outputs Created

0.01779625 BTC to
mowj6ZPEFf6pyai5rSESMXwzjFuqBVtui2 (unspent)

65.14452217 BTC to
mrN1K3w97XqMY6LvwP1FVgZcdNK6Xzuk5z (unsp…

Value Transacted : 65.16231842 BTC

- Bob


6+ confirmations

⇄ c038d307c9b4c1f71968ec500841a881b7febcb043ac48a56dd96b33f9b25647

1 Input Consumed

1.5625 BCY from
CFr99841LyMkyX5ZTGepY58rjXJhyNGXHf (output)

2 Outputs Created

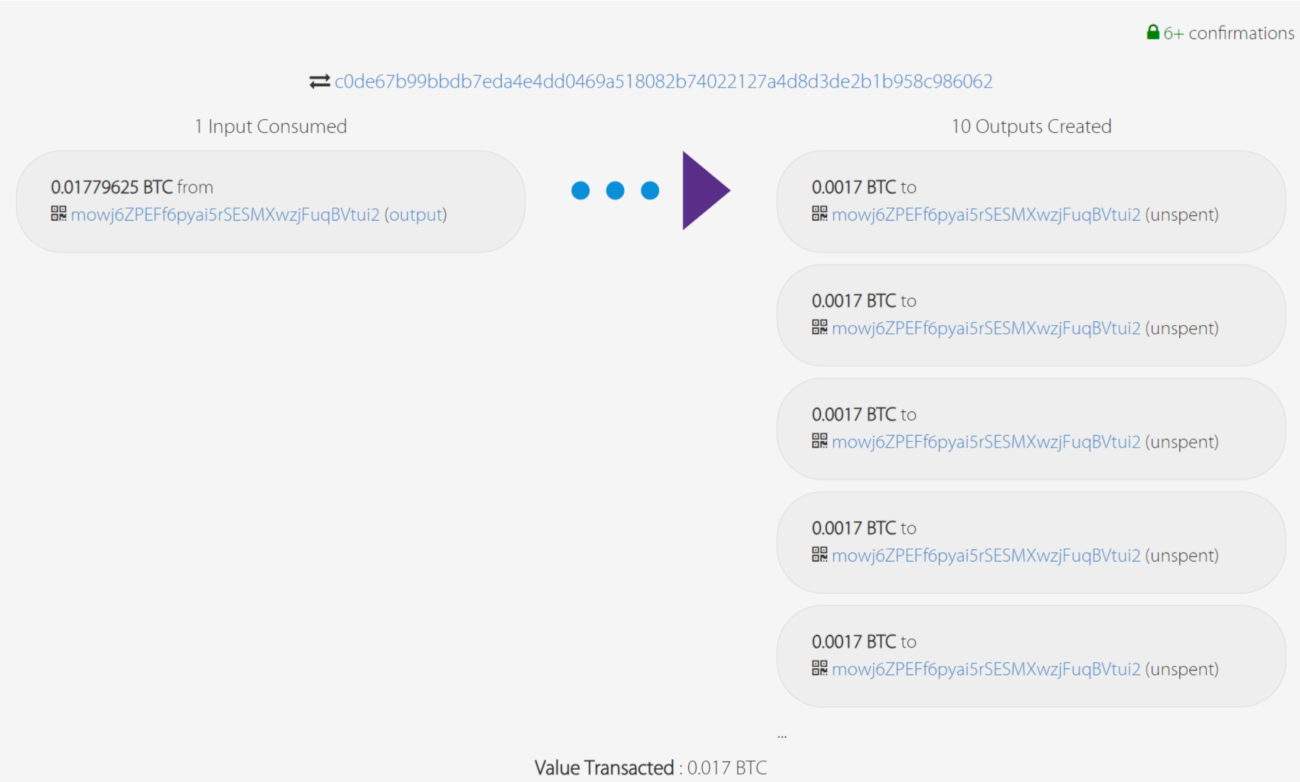
0.01 BCY to
C1VcGk74gGBqDhrAShUAkEUwuAYAy1fcaJ (unspent)

1.5524 BCY to
CFr99841LyMkyX5ZTGepY58rjXJhyNGXHf (unspent)

Estimated Value Sent : 0.01 BCY (more)

分币

- Alice


6+ confirmations

⇄ c0de67b99bbdb7eda4e4dd0469a518082b74022127a4d8d3de2b1b958c986062

1 Input Consumed

0.01779625 BTC from
mowj6ZPEFf6pyai5rSESMXwzjFuqBVtui2 (output)

10 Outputs Created

0.0017 BTC to
mowj6ZPEFf6pyai5rSESMXwzjFuqBVtui2 (unspent)

0.0017 BTC to
mowj6ZPEFf6pyai5rSESMXwzjFuqBVtui2 (unspent)

0.0017 BTC to
mowj6ZPEFf6pyai5rSESMXwzjFuqBVtui2 (unspent)

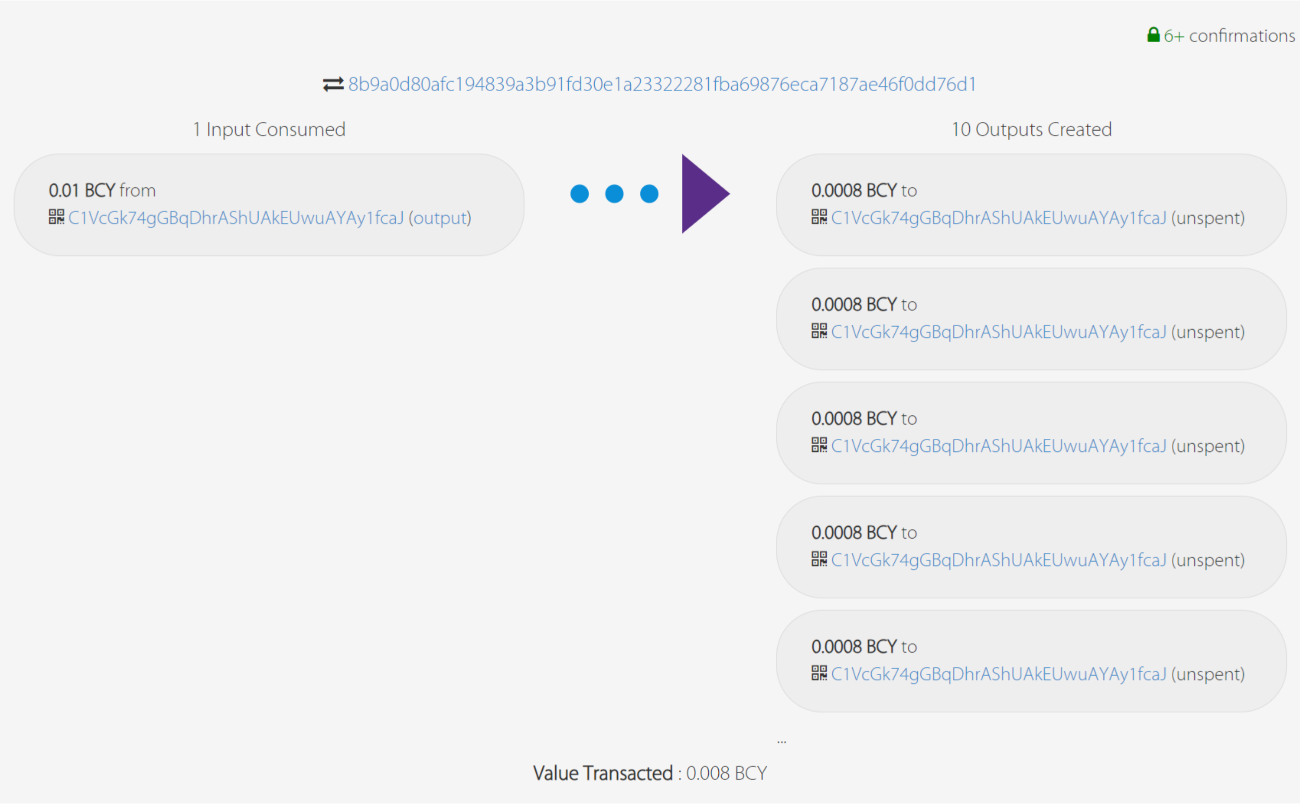
0.0017 BTC to
mowj6ZPEFf6pyai5rSESMXwzjFuqBVtui2 (unspent)

0.0017 BTC to
mowj6ZPEFf6pyai5rSESMXwzjFuqBVtui2 (unspent)

...

Value Transacted : 0.017 BTC

- Bob



6+ confirmations

⇄ 8b9a0d80afc194839a3b91fd30e1a23322281fba69876eca7187ae46f0dd76d1

1 Input Consumed

0.01 BCY from
C1VcGk74gGBqDhrAShUAkEUwuAYAy1fcaJ (output)

10 Outputs Created

0.0008 BCY to
C1VcGk74gGBqDhrAShUAkEUwuAYAy1fcaJ (unspent)

0.0008 BCY to
C1VcGk74gGBqDhrAShUAkEUwuAYAy1fcaJ (unspent)

0.0008 BCY to
C1VcGk74gGBqDhrAShUAkEUwuAYAy1fcaJ (unspent)

0.0008 BCY to
C1VcGk74gGBqDhrAShUAkEUwuAYAy1fcaJ (unspent)

0.0008 BCY to
C1VcGk74gGBqDhrAShUAkEUwuAYAy1fcaJ (unspent)

...

Value Transacted : 0.008 BCY

问题

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 [
        # 推送接收方的公钥到栈上
        public_key_recipient,
        # 验证接收方的签名，并标记为验证结果（不移除）
        OP_CHECKSIGVERIFY,
        # 复制栈顶元素以备双重验证
        OP_DUP,
        # 检查密钥的哈希是否与提供的哈希匹配
        OP_HASH160,
        hash_of_secret,
        OP_EQUAL,
        # 如果条件满足，执行以下操作
        OP_IF,
            # 从栈中移除顶部元素
            OP_DROP,
            # 推送 '1' 到栈上，表示成功
            OP_1,
        # 如果条件不满足，执行以下操作
        OP_ELSE,
            # 检查是否为发送方的签名
            public_key_sender,
            OP_CHECKSIG,
        # 结束条件块
        OP_ENDIF
    ]
```

```
# 这是在接收者知道秘密 x 的情况下，赎回交易所需的 ScriptSig
def coinExchangeScriptSig1(sig_recipient, secret):
    return [
        # 推送密钥到栈上
        secret,
        # 推送接收方的签名到栈上
        sig_recipient
    ]
```

```
# 这是在发送方和接收方都签署事务的情况下，未被赎回时将币发送回发送方的 ScriptSig
def coinExchangeScriptSig2(sig_sender, sig_recipient):
    return [
        # 推送发送方的签名到栈上
        sig_sender,
        # 推送接收方的签名到栈上
        sig_recipient
    ]
```

这段代码主要是 `coinExchangeScript` 和两个相关的 `ScriptSig` 函数的实现。

1. `coinExchangeScript` 函数：
    - `public_key_sender` 是发送方的公钥，`public_key_recipient` 是接收方的公钥，`hash_of_secret` 是 `secret` 的哈希值。
    - 该脚本首先将接收方的公钥推送到栈上，并执行 `OP_CHECKSIGVERIFY` 操作来验证接收方的签名，并标记验证结果，但不移除签名。
    - 复制栈顶元素以备双重验证。
    - 执行 `OP_HASH160` 操作来计算栈顶元素的哈希值，通常用于检查密钥的哈希是否与提供的哈希匹配。
    - 如果条件满足，即密钥的哈希匹配，它执行以下操作：
        - `OP_DROP` 操作：从栈中移除顶部元素。
        - `OP_1` 操作：将整数 `1` 推送到栈上，表示成功。
    - 如果条件不满足，即密钥的哈希不匹配，它执行以下操作：
        - 检查是否为发送方的签名。
        - `OP_CHECKSIG` 操作：验证发送方的签名，如果验证成功，则在堆栈上标记为验证结果，但不将其移除。
    - 最后，它使用 `OP_ENDIF` 来结束条件块。
2. `coinExchangeScriptSig1` 函数：
    - 这是接收方用来赎回币的 `ScriptSig`，用于构建签名的部分。
    - `sig_recipient` 是接收方的签名，`secret` 是一个密钥或者密码。
    - 该脚本将密钥（`secret`）推送到栈上，然后将接收方的签名（`sig_recipient`）推送到栈上。这些值将用于验证和完成交易。
3. `coinExchangeScriptSig2` 函数：
    - 这是未被赎回时将币发送回发送方的 `ScriptSig`，用于构建签名的部分。
    - `sig_sender` 是发送方的签名，`sig_recipient` 是接收方的签名。
    - 该脚本将发送方的签名（`sig_sender`）和接收方的签名（`sig_recipient`）推送到栈上，以便进行验证和完成交易。

`coinExchangeScript` 定义了交易的条件和验证步骤，以确保安全的比特币交易。`coinExchangeScriptSig1` 和 `coinExchangeScriptSig2` 则是用来构建签名部分，以满足 `coinExchangeScript` 中定义的条件。这些脚本一起构成了比特币交易的一部分，确保了交易的安全性和有效性。

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?

Alice 创建了 TX2，这笔交易将资金锁定 48 小时。这意味着 Bob 必须在 48 小时内提供他的签名才能赎回资金。

如果 Bob 不在 48 小时内提供签名并广播 TX2，那么 Alice 可以在 48 小时后广播 TX2，将资金赎回到自己的地址。

这种机制允许 Alice 在一定时间内等待 Bob 赎回资金，如果 Bob 不采取行动，Alice 仍然可以获得资金的控制权。这是一个安全保障，确保资金不会永远锁定在 TX1 中。

为什么不能用简单的 1/2 multisig 来解决这个问题?

在双方可信的情况下是有可能达成交易的，但是在双方互不信任的情况下，1/2 multisig存在着公平性和信任问题。每一方都有能力在单方不履行承诺时同时兑换两笔交易，从而导致失去公平性。这种情况下，无法确保一方不会滥用权利。

在之前描述的设计中，使用了一个时间锁定条件和一些复杂的条件来确保在某种情况下，一方可以在另一方未履行时收回资金。这种设计提供了更多的信任和公平性，确保资金只在满足特定条件下才能被提取，从而减少了滥用权利的可能性。这样的设计更适用于双方互不信任的情况，以确保公平和安全的交易。

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 TX1：
   - TX1 中设置了条件，确保只有在提供了 x 和 Bob 的签名或者同时由 Alice 和 Bob 签名时才能完成交易。这确保了资金不会被无授权的人提取。
   - TX1 不会被广播，因为 Alice 尚未获得 Bob 的签名。

2. Alice 创建 TX2：
   - TX2 是 Alice 为了能够在 Bob 未提供签名时将资金回收而创建的交易。
   - TX2 设置了时间锁定条件，确保 Bob 有足够的时间来提供签名。如果 Bob 不赎回 TX1，Alice 可以在 48 小时后执行 TX2。

3. Bob 对 TX2 进行签名并返回给 Alice，Alice 获得 Bob 签名后将 TX1 广播
   - Bob 提供了 TX2 的签名，使得 Alice 可以在需要时广播 TX2 以赎回资金。
   - Alice 把 TX1 广播且不可篡改，Bob兑换后或赎回脚本锁定结束后Alice才能将钱赎回。

4. Bob 创建 TX3：

   - 与 TX1 相同，除了用双方的签名赎回，还可以通过 x 和 Alice 的签名直接兑换，一旦交易广播，Alice可以直接兑换交易，所以暂时不广播。

5. Bob 创建 TX4：

   - 与 TX2 相同，创建 TX4 后 Bob 具备赎回自己交易的能力，如果Alice不签名，Bob不公开TX3。

6. Alice 对 TX4 进行签名并返回给 Bob，Bob 广播 TX3：

   - Alice 对 TX4 进行签名，这允许 Bob 在需要时广播 TX4 以赎回资金。
   - 一旦 TX3 被广播，Alice 就可以随时兑换资金。
   - 当 Alice 兑换资金后，秘密便公布在了网络上，Bob利用自己的签名和秘密将 TX1 中的钱赎回，原子交换完成。

7. 如果双方不赎回，超过48小时后可以将自己的钱通过双方的签名拿回。

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？

成功情况下：

1. Alice 创建 TX1，并设置了条件以确保安全，但不广播。
2. Alice 创建 TX2 以回收资金。
3. Bob签署了 TX2 并返回给 Alice，Alice 将 TX1 广播到网络。
4. Bob 创建 TX3，用以兑换他的 BCY。
5. Bob 创建 TX4 以回收资金。
6. Alice签署了 TX4 并返回给 Bob，Bob广播 TX3。
7. Alice兑换了Bob的 BCY，并公布秘密x。
8. Bob兑换了Alice的 BTC，使用秘密x以及Bob的签名。

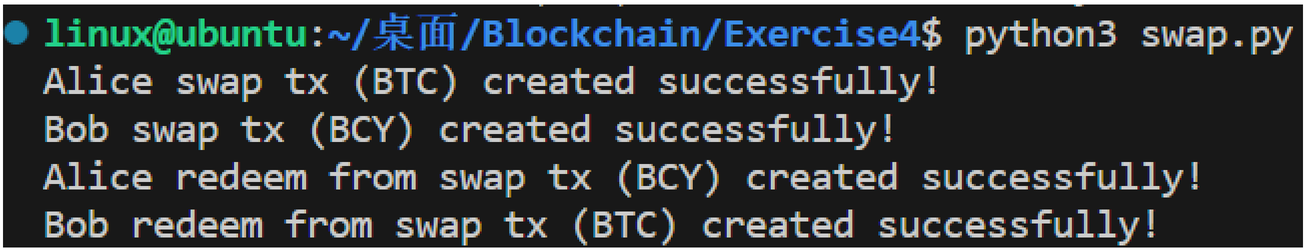
失败情况下：

1. 如果 Bob 不赎回 TX1，则 Alice 会在 48 小时后广播 TX2，以回收她的 BTC。
2. 如果 Alice 不赎回 TX3，则 Bob 会在 24 小时后广播 TX4，以回收他的 BCY。
3. 如果 Alice 和 Bob 都不赎回 TX2 和 TX4，资金将保持在各自的交易中，直到任何一方执行赎回或直到超过48小时为止。

运行结果

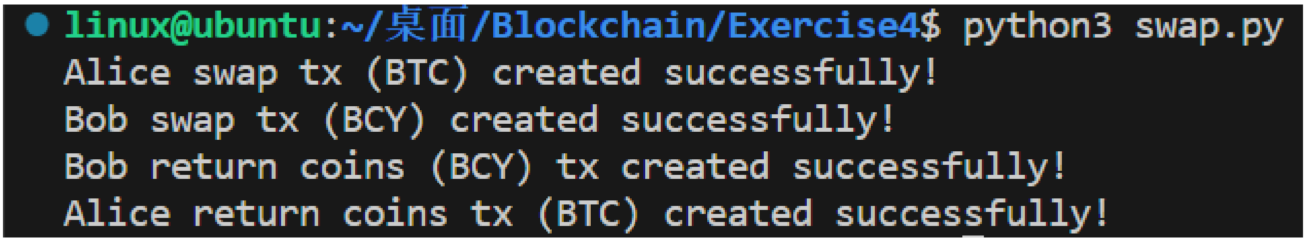
不广播

- Alice赎回



```
linux@ubuntu:~/桌面/Blockchain/Exercise4$ 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!
```

- Alice不赎回

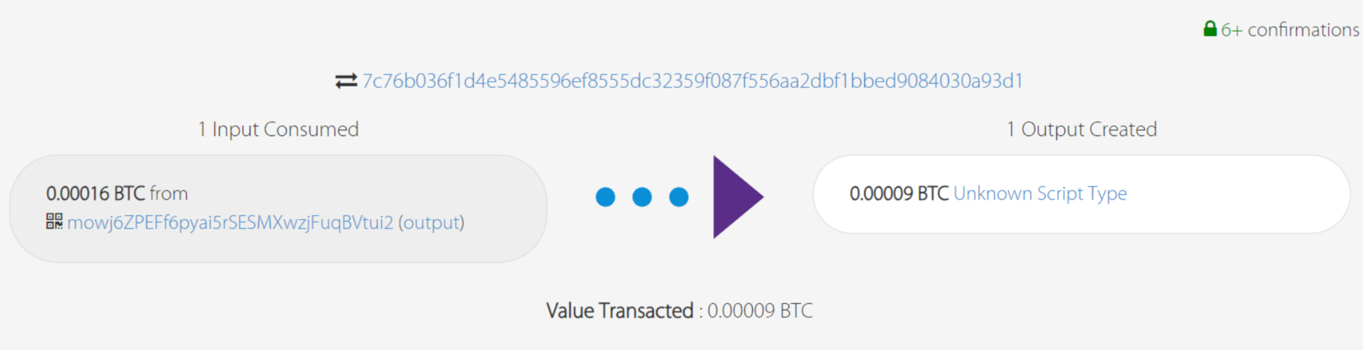


```
linux@ubuntu:~/桌面/Blockchain/Exercise4$ python3 swap.py
Alice swap tx (BTC) created successfully!
Bob swap tx (BCY) created successfully!
Bob return coins (BCY) tx created successfully!
Alice return coins tx (BTC) created successfully!
```

广播

- Alice赎回

Alice创建TX1



6+ confirmations

⇄ 7c76b036f1d4e5485596ef8555dc32359f087f556aa2dbf1bbed9084030a93d1

1 Input Consumed

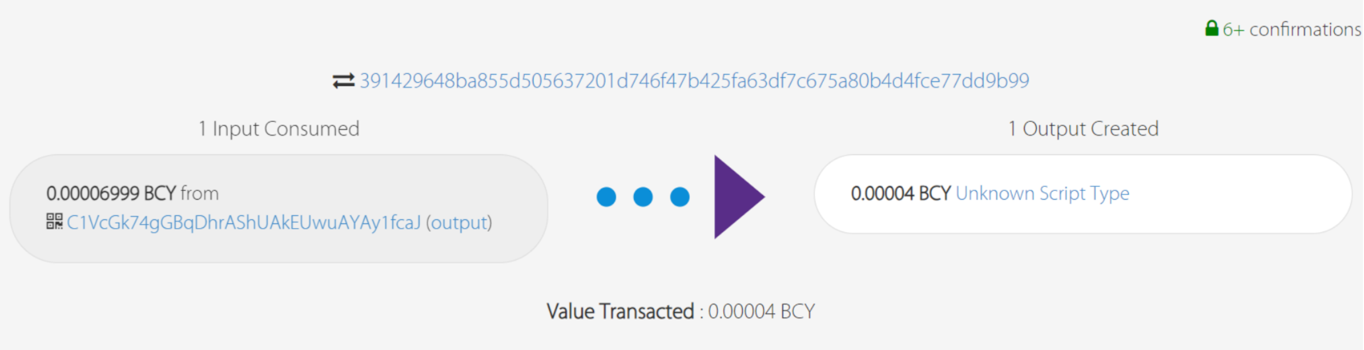
0.00016 BTC from
mowj6ZPEFf6pyai5rSESMXwzjFuqBVtui2 (output)

1 Output Created

0.00009 BTC Unknown Script Type

Value Transacted : 0.00009 BTC

Bob创建TX3



6+ confirmations

⇄ 391429648ba855d505637201d746f47b425fa63df7c675a80b4d4fce77dd9b99

1 Input Consumed

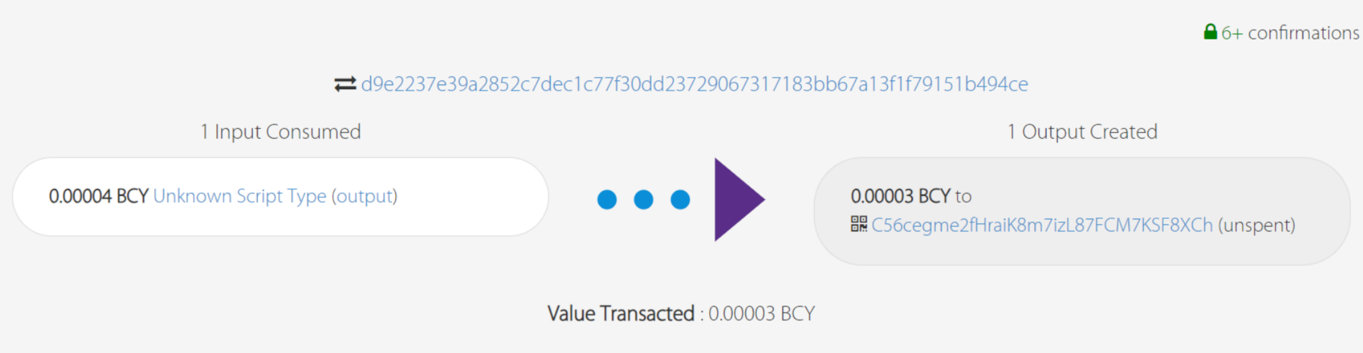
0.00006999 BCY from
C1VcGk74gGBqDhrAShUAkEUwuAYAy1fcaJ (output)

1 Output Created

0.00004 BCY Unknown Script Type

Value Transacted : 0.00004 BCY

Alice赎回，TX3中的钱转移到Alice的BCY账户



6+ confirmations

⇄ d9e2237e39a2852c7dec1c77f30dd23729067317183bb67a13f1f79151b494ce

1 Input Consumed

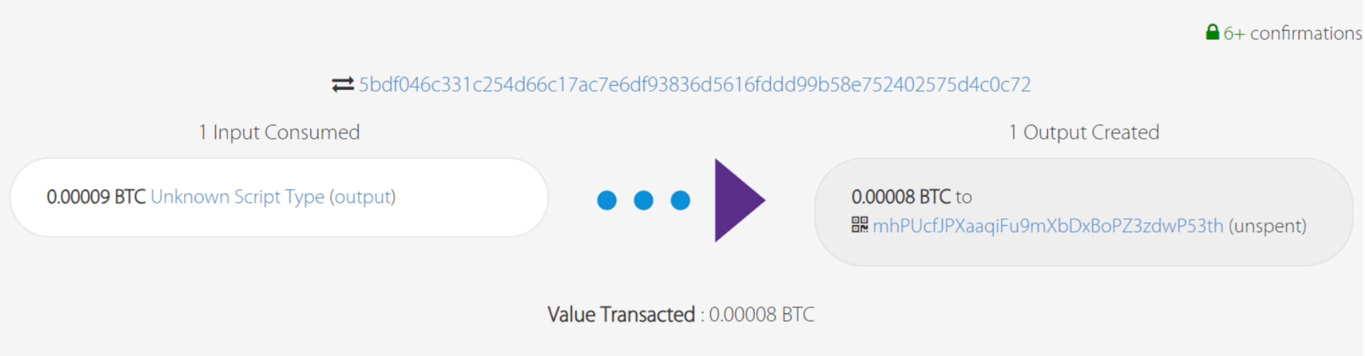
0.00004 BCY Unknown Script Type (output)

1 Output Created

0.00003 BCY to
C56cegme2fHraiK8m7izL87FCM7KSF8XCh (unspent)

Value Transacted : 0.00003 BCY

TX1中的钱转移到Bob的BTC账户



6+ confirmations

⇄ 5bdf046c331c254d66c17ac7e6df93836d5616fddd99b58e752402575d4c0c72

1 Input Consumed

0.00009 BTC Unknown Script Type (output)

1 Output Created

0.00008 BTC to
mhPUcfJPXaaqiFu9mXbDxBoPZ3zdwP53th (unspent)

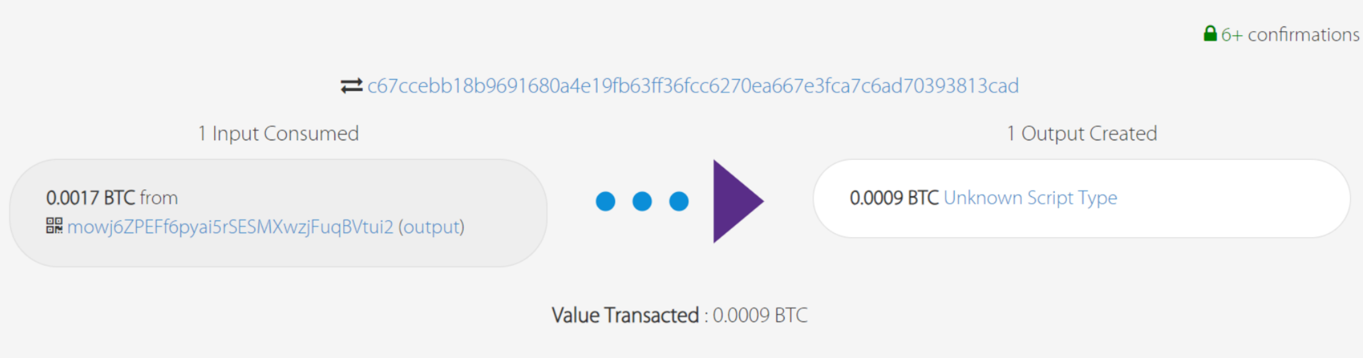
Value Transacted : 0.00008 BTC

输出信息

```
Alice swap tx (BTC) created successfully!
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "7c76b036f1d4e5485596ef8555dc32359f087f556aa2dbf1bbed9084030a93d1",
    "addresses": [
      "mowj6ZPEFf6pyai5rSESMXwzjFuqBVtui2"
    ],
    "total": 9000,
    "fees": 7000,
    "size": 265,
    "vsize": 265,
    "preference": "low",
    "relayed_by": "117.131.219.57",
    "received": "2023-11-13T14:49:32.878938828Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"ff7449e78daa35f8b3407b802c9e8cb6957c315f4c3604bdf5ae1ccbb1ccb90a",
        "output_index": 5,
        "script":
"47304402202b3aec7f2e31f84cc187b6d0318d3cf69b7936de3efea0e0b20059f5a02f27ce0220097be8d
4771f89eeb10c843a343397eb97764f2d9e11cb6fefdf78360b562f02012103b4d36a0ee9e578cb5abcc31
7108db988641aba3be96858d7bc8a1deb896a00e2",
        "output_value": 16000,
        "sequence": 4294967295,
        "addresses": [
          "mowj6ZPEFf6pyai5rSESMXwzjFuqBVtui2"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2538134
      }
    ],
    "outputs": [
      {
        "value": 9000,
        "script":
"2103e5e975a5020b39382bc5d44c39600e96e2ef6a5d2f662ceb58458d40a5c2c83fad76a914853b77507
9232503df966e626618e1d388a9572087637551672103b4d36a0ee9e578cb5abcc317108db988641aba3be
96858d7bc8a1deb896a00e2ac68",
        "addresses": null,
        "script_type": "unknown"
      }
    ]
  }
}
Bob swap tx (BCY) created successfully!
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "391429648ba855d505637201d746f47b425fa63df7c675a80b4d4fce77dd9b99",
    "addresses": [
      "C1VcGk74gGBqDhrAShUAkEUwuAYAy1fcaJ"
    ],
    "total": 4000,
    "fees": 2999,
    "size": 265,
    "vsize": 265,
    "preference": "low",
    "relayed_by": "117.131.219.57",
    "received": "2023-11-13T14:49:34.248806178Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"56af4443664e5540e879153af393eff894a160cfbd98f571dc44d6b2760d25db",
        "output_index": 5,
        "script":
"473044022035dbfef55d95f4d1c35192e31cf93614a4f6c6e019bc15796a821f3fef82a62a02206c21b7d
bc7e59cdb6d1bc2c5444a8213715245fbb6d8dc0bab8ba000ec1fd02301210322f835d86cb9c501d7dcd0d
5612643015aac1bac46c5cb1c9384452be30c0a33",
        "output_value": 6999,
        "sequence": 4294967295,
        "addresses": [
          "C1VcGk74gGBqDhrAShUAkEUwuAYAy1fcaJ"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 1065004
      }
    ],
    "outputs": [
      {
        "value": 4000,
        "script":
"21038ecfcc7682eed146a22730cd22960736b95cf62be67c93c1344c13be8095ae25ad76a914853b77507
9232503df966e626618e1d388a957208763755167210322f835d86cb9c501d7dcd0d5612643015aac1bac4
6c5cb1c9384452be30c0a33ac68",
        "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": "d9e2237e39a2852c7dec1c77f30dd23729067317183bb67a13f1f79151b494ce",
    "addresses": [
      "C56cegme2fHraiK8m7izL87FCM7KSF8XCh"
    ],
    "total": 3000,
    "fees": 1000,
    "size": 182,
    "vsize": 182,
    "preference": "low",
    "relayed_by": "117.131.219.57",
    "received": "2023-11-13T15:09:35.821389945Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"391429648ba855d505637201d746f47b425fa63df7c675a80b4d4fce77dd9b99",
        "output_index": 0,
        "script":
"187468697349734153656372657450617373776f7264313233473044022048fb1c432d8c941d8f70eb872
c432c17682db56412f6de959d27020a1737b9d402207ac34a1960453434afbef3eef75b61fe13a03a4e8ef
96e0d6374566a9adc87a001",
        "output_value": 4000,
        "sequence": 4294967295,
        "script_type": "unknown",
        "age": 1066511
      }
    ],
    "outputs": [
      {
        "value": 3000,
        "script": "76a9148350978760f97e27f4b85a72f5fb321006f4562588ac",
        "addresses": [
          "C56cegme2fHraiK8m7izL87FCM7KSF8XCh"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}
Bob redeem from swap tx (BTC) created successfully!
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "5bdf046c331c254d66c17ac7e6df93836d5616fddd99b58e752402575d4c0c72",
    "addresses": [
      "mhPUcfJPXaaqiFu9mXbDxBoPZ3zdwP53th"
    ],
    "total": 8000,
    "fees": 1000,
    "size": 182,
    "vsize": 182,
    "preference": "low",
    "relayed_by": "60.29.153.8",
    "received": "2023-11-13T15:09:36.62146485Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"7c76b036f1d4e5485596ef8555dc32359f087f556aa2dbf1bbed9084030a93d1",
        "output_index": 0,
        "script":
"18746869734973415365637265745061737377 6f72643132334730440220 43dd1fbf1fedf602a48266b68
0a9fa486a16434222452c94ba57d4fdb33e3f2102200f2655001b5335715b401bcef6b0a00e5f71014b9db
ace31abaae9c712391afb01",
        "output_value": 9000,
        "sequence": 4294967295,
        "script_type": "unknown",
        "age": 2538277
      }
    ],
    "outputs": [
      {
        "value": 8000,
        "script": "76a91414863c027e86a573f4f24ff805811d60e67f5f5688ac",
        "addresses": [
          "mhPUcfJPXaaqiFu9mXbDxBoPZ3zdwP53th"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
    }
}![](/uploads/upload_09b26b274f06b531cac42afdcc649ec9.png)
```

- Alice不赎回

Alice创建TX1



🔒 6+ confirmations

⇄ c67ccebb18b9691680a4e19fb63ff36fcc6270ea667e3fca7c6ad70393813cad

1 Input Consumed

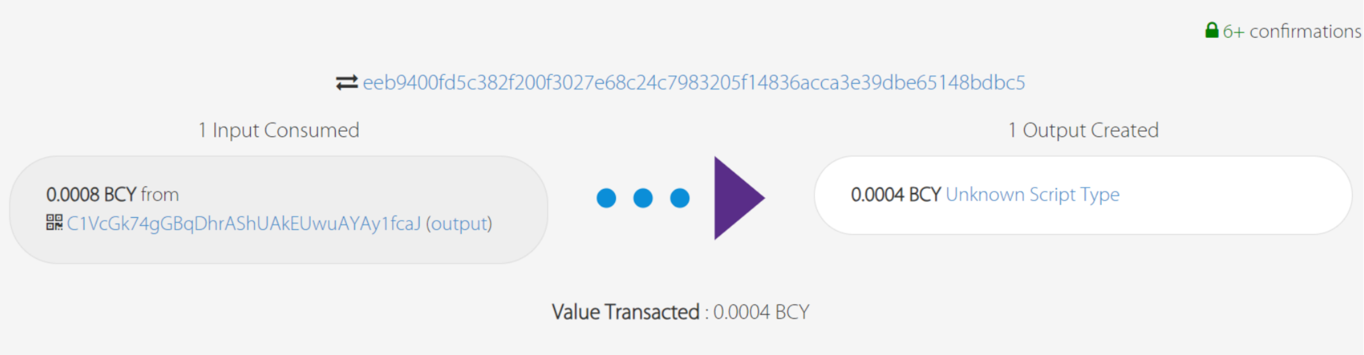
0.0017 BTC from
mowj6ZPEFf6pyai5rSESMXwzjFuqBVtui2 (output)

1 Output Created

0.0009 BTC Unknown Script Type

Value Transacted : 0.0009 BTC

Bob创建TX3



🔒 6+ confirmations

⇄ eeb9400fd5c382f200f3027e68c24c7983205f14836acca3e39dbe65148bdbc5

1 Input Consumed

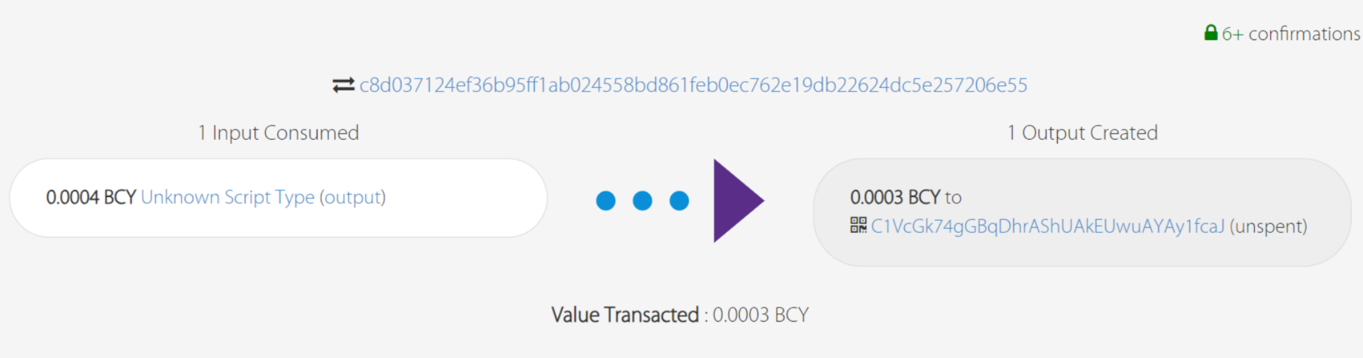
0.0008 BCY from
C1VcGk74gGBqDhrAShUAkEUwuAYAy1fcaJ (output)

1 Output Created

0.0004 BCY Unknown Script Type

Value Transacted : 0.0004 BCY

超过时间后TX3中的钱转回到Bob的BCY账户



🔒 6+ confirmations

⇄ c8d037124ef36b95ff1ab024558bd861feb0ec762e19db22624dc5e257206e55

1 Input Consumed

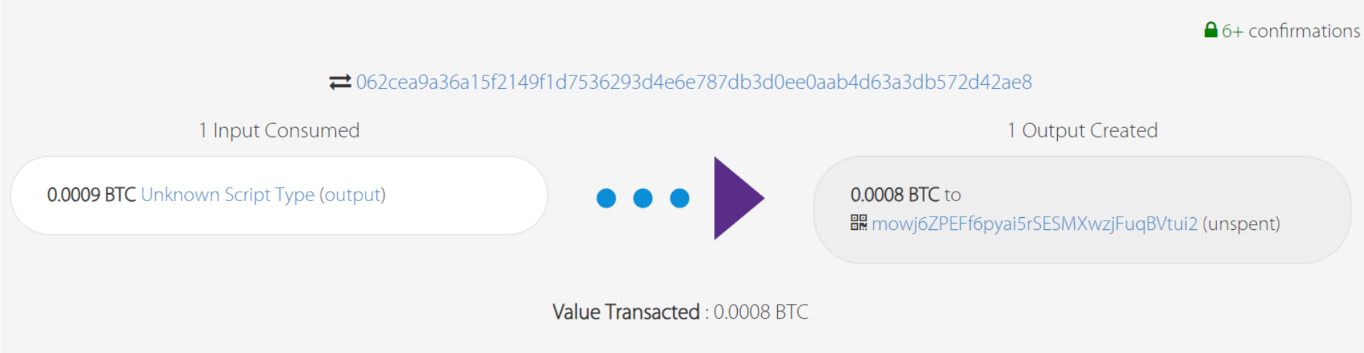
0.0004 BCY Unknown Script Type (output)

1 Output Created

0.0003 BCY to
C1VcGk74gGBqDhrAShUAkEUwuAYAy1fcaJ (unspent)

Value Transacted : 0.0003 BCY

超过时间后TX1中的钱转回到Alice的BTC账户



🔒 6+ confirmations

⇄ 062cea9a36a15f2149f1d7536293d4e6e787db3d0ee0aab4d63a3db572d42ae8

1 Input Consumed

0.0009 BTC Unknown Script Type (output)

1 Output Created

0.0008 BTC to
mowj6ZPEFf6pyai5rSESMXwzjFuqBVtui2 (unspent)

Value Transacted : 0.0008 BTC

输出信息

```
Alice swap tx (BTC) created successfully!
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "c67ccebb18b9691680a4e19fb63ff36fcc6270ea667e3fca7c6ad70393813cad",
    "addresses": [
      "mowj6ZPEFf6pyai5rSESMXwzjFuqBVtui2"
    ],
    "total": 90000,
    "fees": 80000,
    "size": 266,
    "vsize": 266,
    "preference": "high",
    "relayed_by": "221.238.245.63",
    "received": "2023-11-12T07:30:16.418991346Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"c0de67b99bbdb7eda4e4dd0469a518082b74022127a4d8d3de2b1b958c986062",
        "output_index": 6,
        "script":
"483045022100c88560bcfa5d4dac13e7a5ff11a3ade907dfb21b612bfafe4f1fac36d573ed14022020856
9cc9cbe4a93449bcf95b4b29d16f61992c56d3b1ece9d77d21679a444b6012103b4d36a0ee9e578cb5abcc
317108db988641aba3be96858d7bc8a1deb896a00e2",
        "output_value": 170000,
        "sequence": 4294967295,
        "addresses": [
          "mowj6ZPEFf6pyai5rSESMXwzjFuqBVtui2"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2538020
      }
    ],
    "outputs": [
      {
        "value": 90000,
        "script":
"2103e5e975a5020b39382bc5d44c39600e96e2ef6a5d2f662ceb58458d40a5c2c83fad762103b4d36a0ee
9e578cb5abcc317108db988641aba3be96858d7bc8a1deb896a00e2ac63755167a914853b775079232503d
f966e626618e1d388a957208768",
        "addresses": null,
        "script_type": "unknown"
      }
    ]
  }
}
Bob swap tx (BCY) created successfully!
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "eeb9400fd5c382f200f3027e68c24c7983205f14836acca3e39dbe65148bdbc5",
    "addresses": [
      "C1VcGk74gGBqDhrAShUAkEUwuAYAy1fcaJ"
    ],
    "total": 40000,
    "fees": 40000,
    "size": 265,
    "vsize": 265,
    "preference": "high",
    "relayed_by": "117.131.219.9",
    "received": "2023-11-12T07:30:17.65911213Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"8b9a0d80afc194839a3b91fd30e1a23322281fba69876eca7187ae46f0dd76d1",
        "output_index": 6,
        "script":
"47304402206af380748aa04c16a638c82dc8c08aba5beb88caf07978a6ab4ff0ffd1f85f9502205cca0a7
27f684e277fbed5458d42d068866ad20e731b5c3156bdae7bf83af09e01210322f835d86cb9c501d7dcd0d
5612643015aac1bac46c5cb1c9384452be30c0a33",
        "output_value": 80000,
        "sequence": 4294967295,
        "addresses": [
          "C1VcGk74gGBqDhrAShUAkEUwuAYAy1fcaJ"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 1063663
      }
    ],
    "outputs": [
      {
        "value": 40000,
        "script":
"21038ecfcc7682eed146a22730cd22960736b95cf62be67c93c1344c13be8095ae25ad76210322f835d86
cb9c501d7dcd0d5612643015aac1bac46c5cb1c9384452be30c0a33ac63755167a914853b775079232503d
f966e626618e1d388a957208768",
        "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": "c8d037124ef36b95ff1ab024558bd861feb0ec762e19db22624dc5e257206e55",
    "addresses": [
      "C1VcGk74gGBqDhrAShUAkEUwuAYAy1fcaJ"
    ],
    "total": 30000,
    "fees": 10000,
    "size": 230,
    "vsize": 230,
    "preference": "low",
    "relayed_by": "221.238.245.63",
    "received": "2023-11-12T08:28:06.86750143Z",
    "ver": 1,
    "lock_time": 1064570,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"eeb9400fd5c382f200f3027e68c24c7983205f14836acca3e39dbe65148bdbc5",
        "output_index": 0,
        "script":
"47304402205fc709897de4029e17e79949a067a15758a52720c67d8c16250cab0461b619b002205607758
d3f9393025880fb2ce5ee058c16634e9f1e5a724996264e0e701c52f501483045022100bcc5b78d1b1501d
38523d6aa060ffb498eae2a4510ffbbb0dbcaf798567c9132022073caaad9cd49bb7ce0e16ddf694984c61
2746de93339001a05765141b3be7f2601",
        "output_value": 40000,
        "sequence": 4294967295,
        "script_type": "unknown",
        "age": 1064632
      }
    ],
    "outputs": [
      {
        "value": 30000,
        "script": "76a9145bc957102f74e82afc20905d8a29e30fe9ea714588ac",
        "addresses": [
          "C1VcGk74gGBqDhrAShUAkEUwuAYAy1fcaJ"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}
Sleeping for alice_locktime blocks to pass locktime...
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "062cea9a36a15f2149f1d7536293d4e6e787db3d0ee0aab4d63a3db572d42ae8",
    "addresses": [
      "mowj6ZPEFf6pyai5rSESMXwzjFuqBVtui2"
    ],
    "total": 80000,
    "fees": 10000,
    "size": 230,
    "vsize": 230,
    "preference": "low",
    "relayed_by": "117.131.219.9",
    "received": "2023-11-12T08:48:09.891245479Z",
    "ver": 1,
    "lock_time": 2538107,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"c67ccebb18b9691680a4e19fb63ff36fcc6270ea667e3fca7c6ad70393813cad",
        "output_index": 0,
        "script":
"47304402207bbed1d67c9f2f02bab20edc511a719c3504f6299533ad2c8b4f120d9e55352e02206640010
6590048aceb15be67342717cb209f5947beb03dcc62ea13dadfaf690401483045022100c79c1d8313cd0bb
dd9840cb18be39b9823e12864e9fcb0c503ffaab6d05aadcc02200502e5febb695cac04536abf9e9f2ddec
19f7f8ff39d7dae47f01c01b3b2253d01",
        "output_value": 90000,
        "sequence": 4294967295,
        "script_type": "unknown",
        "age": 2538107
      }
    ],
    "outputs": [
      {
        "value": 80000,
        "script": "76a9145c70635577dadeadeafd0e85e0f76413ba11b25188ac",
        "addresses": [
          "mowj6ZPEFf6pyai5rSESMXwzjFuqBVtui2"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}
```

遇到的问题及说明

1. 在广播赎回阶段由于Bob的BTC账户一直不能确认赎回的比特币，因此发现一开始编写的`coinExchangeScript`脚本有错误。一开始编写的脚本在if条件语句判断阶段写的代码为判断是不是发送方的签名，但是这样编写代码后Bob的BTC账户迟迟得不到确认，猜测如果不是发送方的签名就直接使得交易不能正常进行。因此更改了判断条件，再次实验发现Bob的BTC账户得到确认。

2. 由于一开始分币的次数为10次，但是我们并没有再10次内完成实验，故而把分币信息中`utxo_index = 9`的这一条交易中的钱再次分成10份进行试验，因此实验中的截图可能出现钱数不一致的现象。