区块链练习4

朱浩泽 1911530　王润泽 1811432

一、实验内容

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

swap_scripts.py中的脚本代码内容

```
def coinExchangeScript(public_key_sender, public_key_recipient, hash_of_secret):
    return [
        # fill this in!
        #首先匹配是否包含接收的签名
        public_key_recipient,
        OP_CHECKSIGVERIFY,
        #复制栈顶的元素，因为要进行两种判断
        OP_DUP,
        #检查是不是发送者的签名
        public_key_sender,
        OP_CHECKSIG,
        #如果是
        OP_IF,
        OP_DROP,
        OP_1,
        #如果不是
        OP_ELSE,
        OP_HASH160,
        hash_of_secret,
        OP_EQUAL,
        OP_ENDIF
    ]

# This is the ScriptSig that the receiver will use to redeem coins
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
    ]
```

alice.py和bob.py调用swap_scripts.py文件，swap.py调用alice.py和bob.py完成交换。

两种验证通过的方式

- 提供接收方签名，提供秘密x验证hash(x)的正确性（用于交换交易）
- 提供发送方和接收方的签名（用于取回）

代码解释

- public_key_recipient, OP_CHECKSIGVERIFY

  首先我们验证是否包含接收者的签名，如果不包含直接不符合要求，栈顶压入FALSE拒绝，如果包含进行下一步

- OP_DUP

  因为要进行两种判断，所以要复制栈顶的元素

- public_key_sender, OP_CHECKSIG

  检查是不是发送者的姓名

- OP_IF, OP_DROP, OP_1

  如果是，清空站内元素，压入TRUE

- OP_ELSE, OP_HASH160, hash_of_secret, OP_EQUAL,OP_ENDIF

  如果不是， 判断该元素是不是秘密，如果是，压入TRUE，如果不是，压入FALSE

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将把交换钱的操作写在了TX1中，该交易可以通过双方的签名或Bob的签名和秘密将钱取出，如果Bob不在TX2上签名，则该区块不会广播到网络上，交易没有生效，钱还在Alice手中。如果Bob将其签名了，Alice变获得了Bob的签名，如果Bob没有提供Alice交换钱钱的tx则不能得到秘密，无法将这笔钱赎回，在时间超过48小时后可以通过自己的签名和Bob提供的签名将钱赎回。

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，可以利用任何一个人的签名将钱赎回，可能会发生赎回连续赎回自己发出的钱和对方发送的钱的问题

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选择一个随机数，并利用哈希函数进行加密
2. Alice创建TX1，将钱发给Bob；此时未广播，并没有实质的自己流转，钱仍然在Alice手中
3. Alice创建TX2，为自己可以将钱赎回的交易，将该交易广播到网络上；该交易含有48小时的锁定时间，为了让Bob有足够的时间去兑换TX1中的钱
4. Bob对TX2进行签名，Alice通过TX2获得了Bob的签名，便将TX1广播到网络上
5. Bob创建TX3，将钱发给Alice；此时未广播，并没有实质的自己流转，钱仍然在Bob手中
6. Bob创建TX4，为自己可以将钱赎回的交易，将该交易广播到网络上；该交易含有48小时的锁定时间，为了让Alice有足够的时间去兑换TX3中的钱
7. Alice对TX4进行签名，Bob通过TX4获得了Alice的签名，便将TX3广播到网络上

8. Alice利用自己的签名和秘密对TX3中的钱进行赎回，一旦赎回，秘密便公布在了网络上
9. Bob利用拿到了秘密，利用自己的签名和秘密将TX1中的钱赎回，原子交换完成
10. 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

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?

在上一个问题中，第四步Alice将TX1公布到了网络上，发生了资金流转，此时钱不属于任何人；第七步Bob将TX3公布到了网络上，发生了资金流转，此时钱不属于任何人；第八步Alice利用秘密和自己的签名将TX3中的钱赎回到自己的地址中，发生了自己流动，Bob的钱到了Alice手中；第九步Bob利用秘密和自己的签名将TX1中的钱赎回到自己的地址中，发生了自己流动，Alice的钱到了Bob手中，至此一个成功的跨链原子交易完成。

运行结果

不广播

- Alice赎回

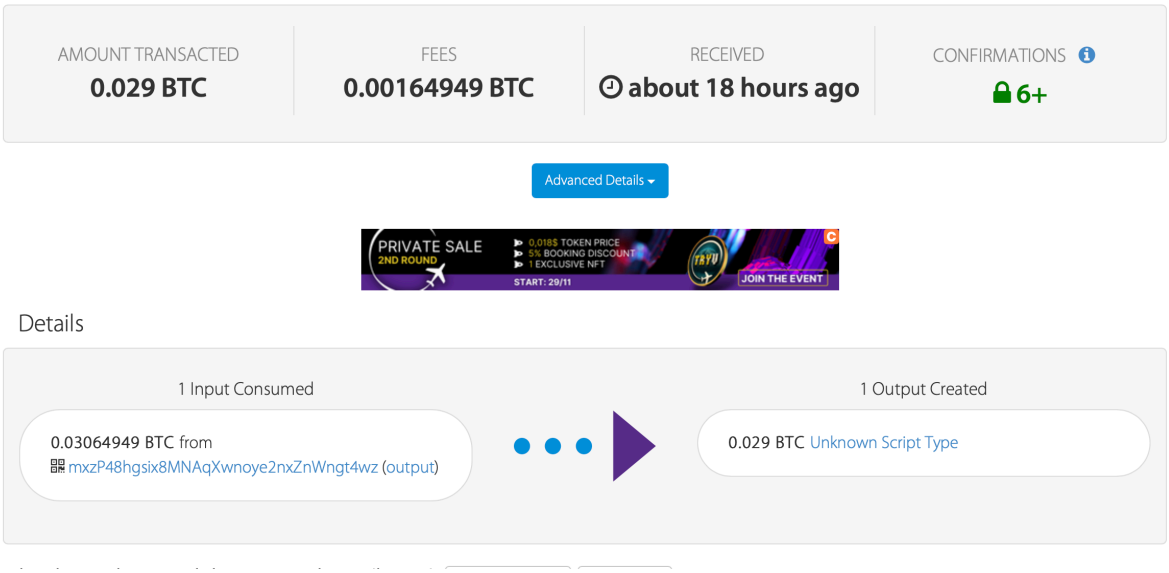
```
Alice swap tx (BTC) created successfully!
Bob swap tx (BCY) created successfully!
Alice redeem from swap tx (BCY) created successfully!
Bob redeem from swap tx (BTC) created successfully!
```

- Alice不赎回

```
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!
```

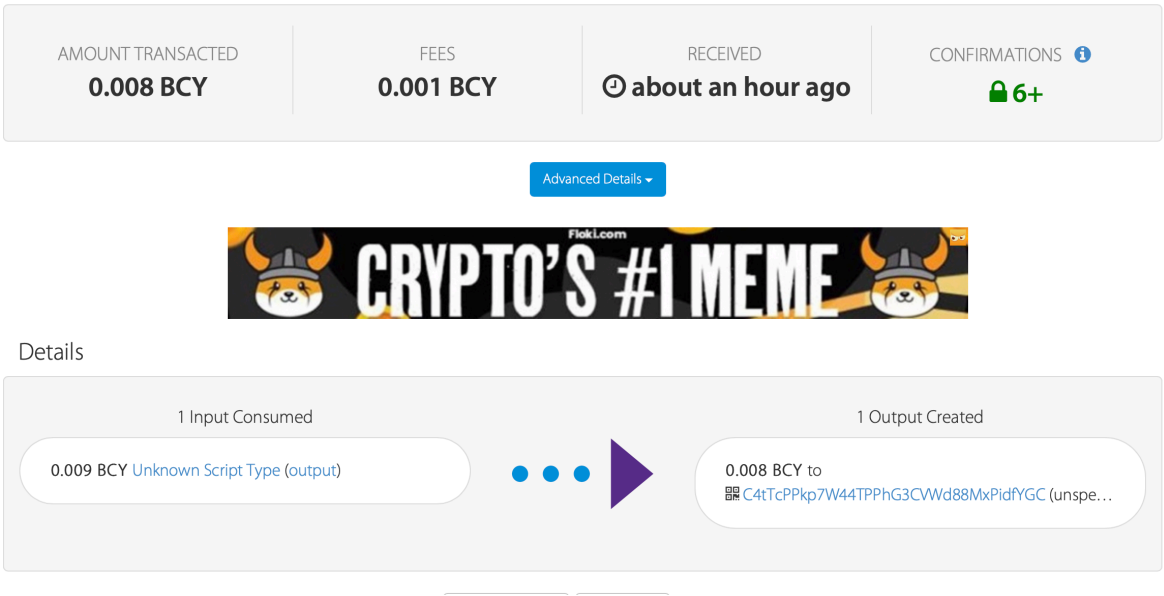
广播

- Alice赎回
  - 将TX1广播02688427fd96e1bfeba4114ac4835227f267e812d237b1ff2651fbf59669df88



- Bob取出TX1中的币a1270545ad0d517dd3924ac447e441666a96046e9be4d2a0fda3ca1b239419ad（该tx查不到，已经跟助教说明）

- 将TX3广播 2a1b2ee753e550302204391edfed6498306d121ef39f8ed9cf1787094dc75983



- Alice取出TX3中的币3e34e88cb53e2415a8f79b8a756253d011ae974b350785cf37fbe99f42e6445b