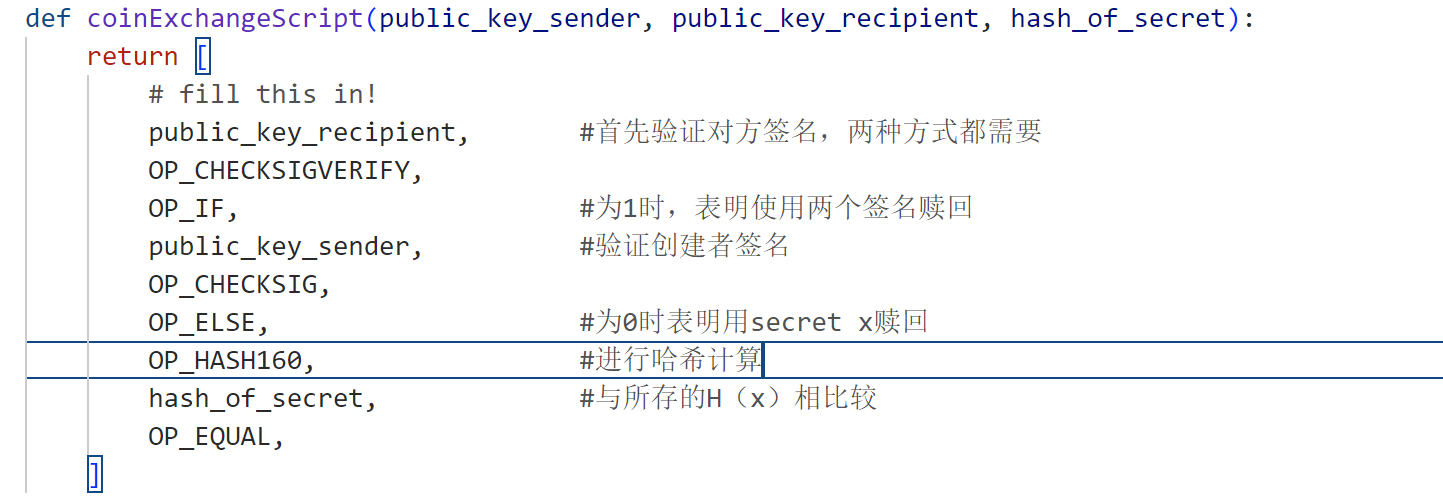
区块链Exercise4实验报告

2010535赵健坤 2013536汤清云

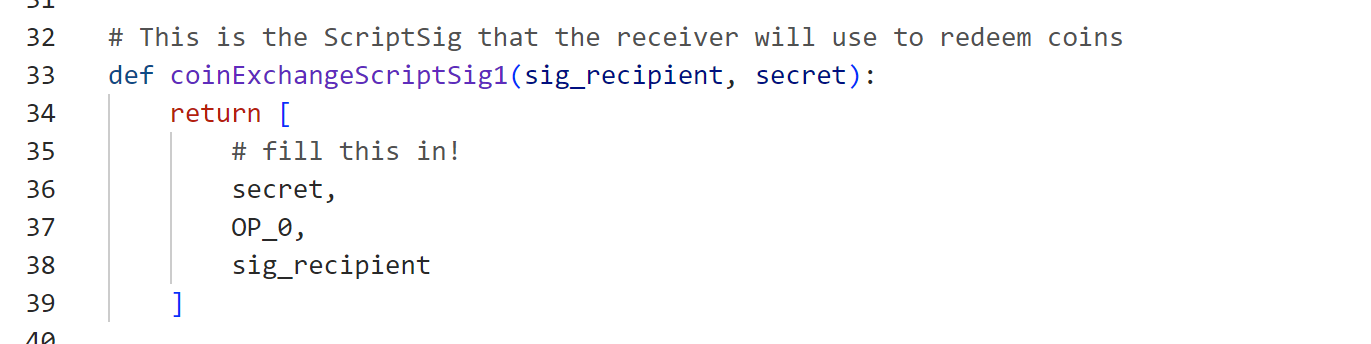
# **实验设计**

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

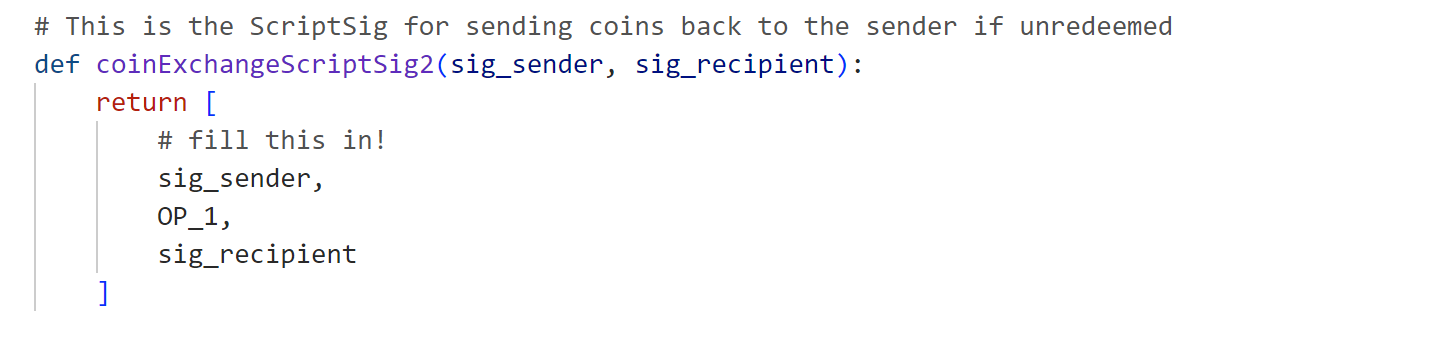


这一函数用于生成存储交易的ScriptPubKey脚本，在跨站原子交易开始阶段被调用。Alice方传入参数为自己和Bob两者的BTC账户公钥以及秘密x的哈希值；在Bob方传入参数为自己和Alice两者的BCY账户公钥以及秘密x的哈希值。该笔交易的赎回条件为：输入脚本ScriptSig中同时提供双方签名（交易未达成，由本人取回存款），或同时提供收款方签名和秘密x的值（交易达成，由对方赎回存款）。该脚本将首先验证对方签名，然后根据传入的0/1值判定输入脚本类型：若为1则输入脚本使用两个签名赎回，于是验证创建者签名；若为0则使用秘密x赎回，于是验证秘密x的哈希值是否正确。

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：



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。



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。

## **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。

## **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。

## **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：

1. Alice创建一个秘密x，并将其进行哈希计算。
2. 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。
3. 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。
4. Alice让Bob在交易B上签名。
5. 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。
6. 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。
7. 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。
8. Bob让Alice在交易D上进行签名。
9. 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。
10. 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。
11. 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。
12. 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。

## **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。

## **实验过程**

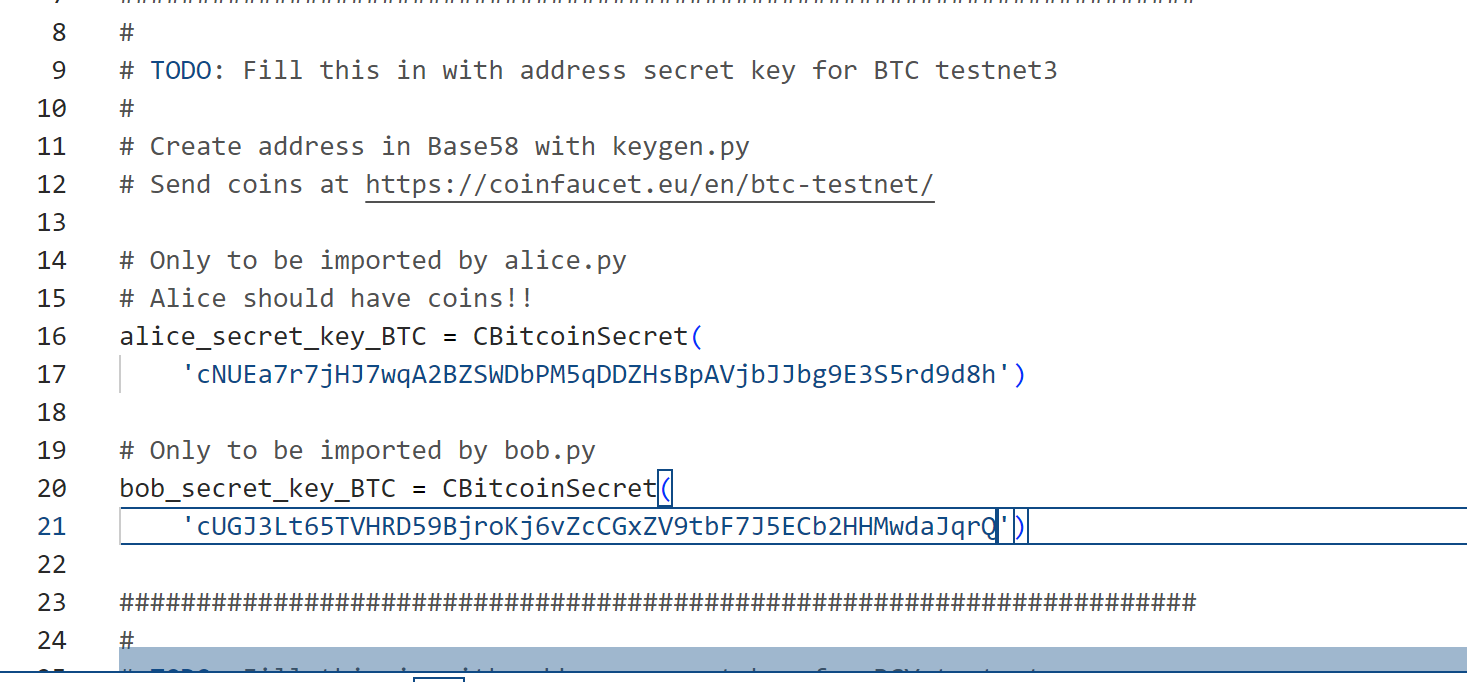
## 使用keygen.py生成Alice的BTC testnet信息如下：

|  |  |
| --- | --- |
| Private key | cNUEa7r7jHJ7wqA2BZSWDbPM5qDDZHsBpAVjbJJbg9E3S5rd9d8h |
| Address | mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD |

## 使用keygen.py生成Bob的BTC testnet信息如下：

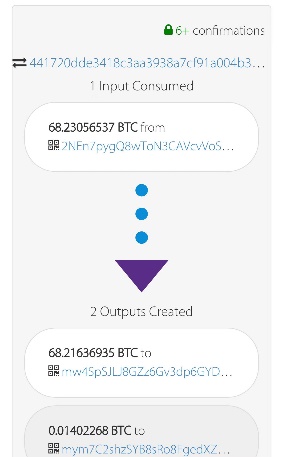
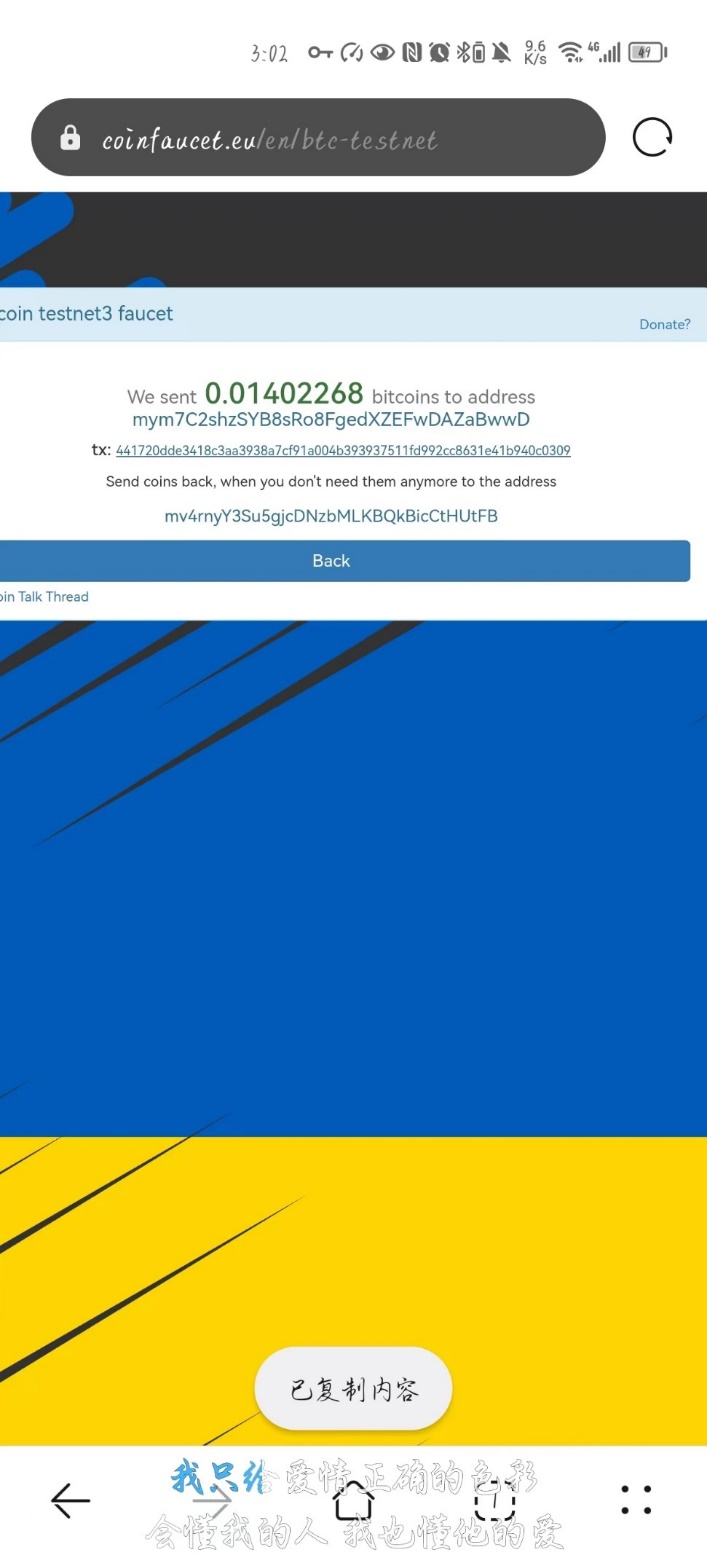
|  |  |
| --- | --- |
| Private key | cUGJ3Lt65TVHRD59BjroKj6vZcCGxZV9tbF7J5ECb2HHMwdaJqrQ |
| Address | mqKpH1cMUq95KM4zLDEVjud9PLEscVekug |

填入keys.py中：



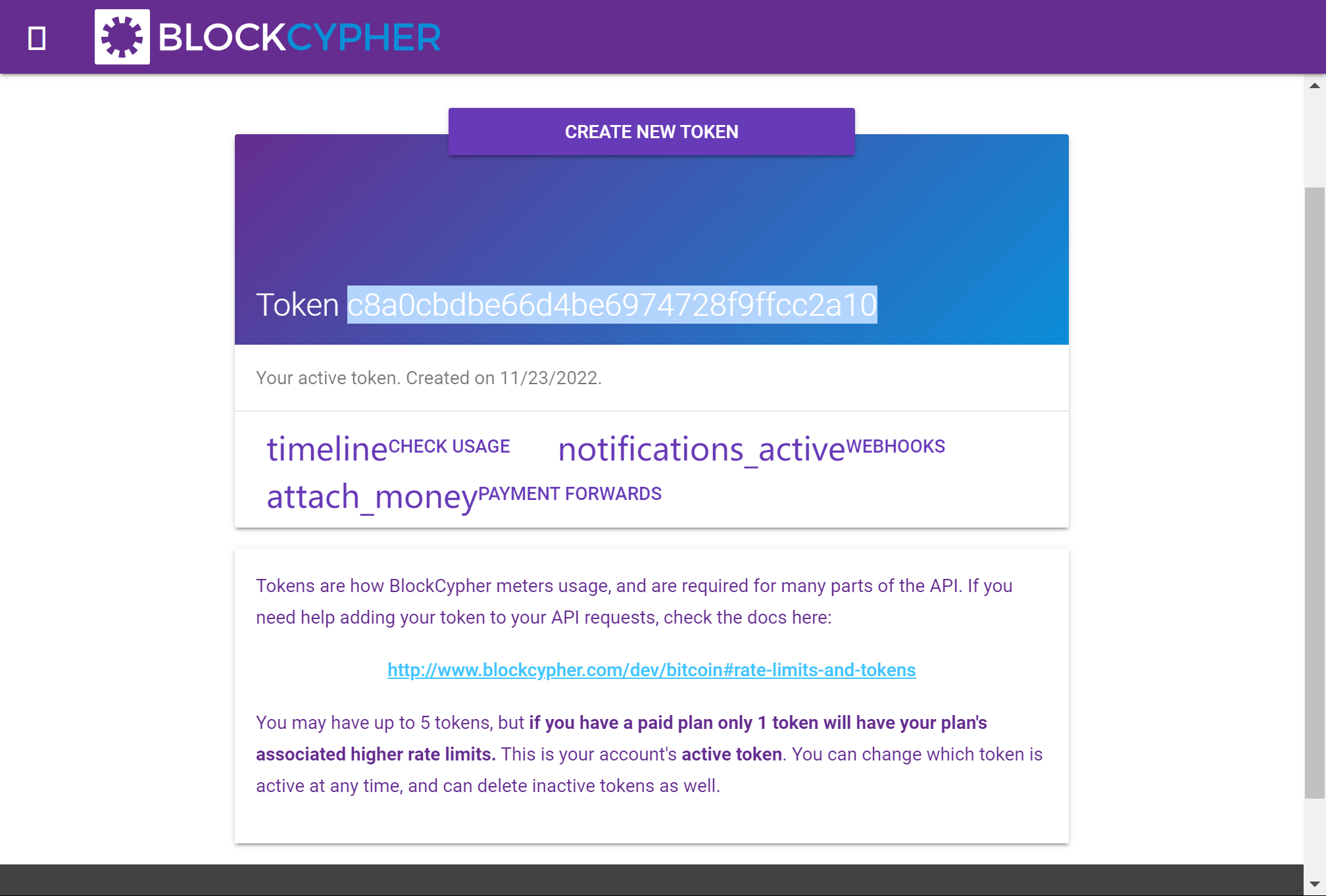
## 为Alice获取测试币：

|  |  |
| --- | --- |
| Hash | 441720dde3418c3aa3938a7cf91a004b393937511fd992cc8631e41b940c0309 |



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

|  |  |
| --- | --- |
| Token | c8a0cbdbe66d4be6974728f9ffcc2a10 |



## 为Alice生成BCY testnet结果：

|  |
| --- |
| {  "private": "2e8da577813ffcfd5e7c5dd54dbc5150347167560e45ce32c4d279d99bdd9494",  "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：



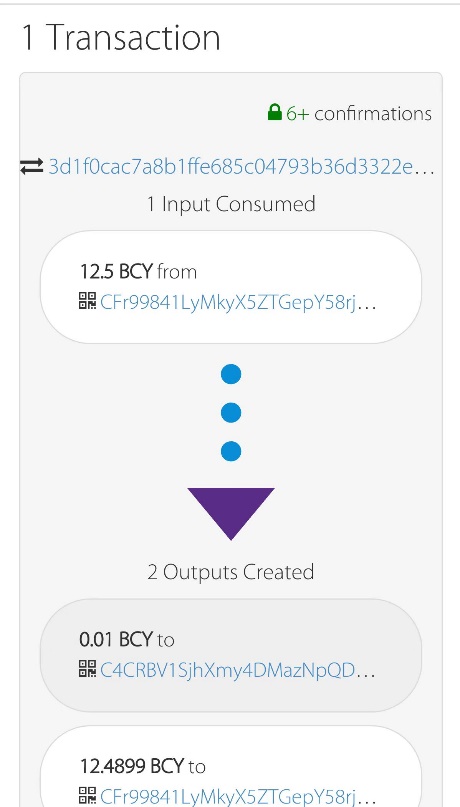
## 为Bob领取BCY测试币：

命令为：

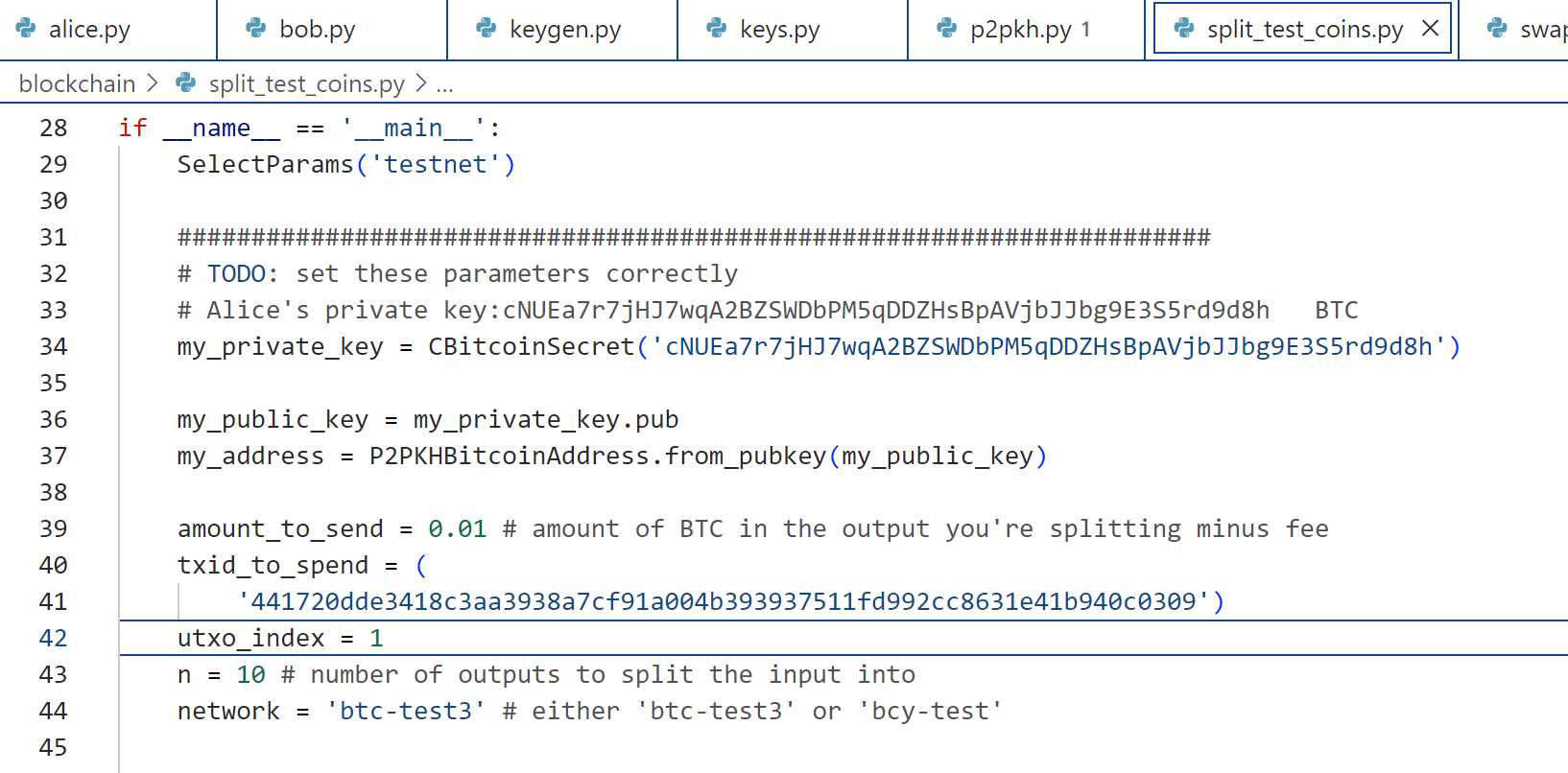
|  |
| --- |
| curl -d '{"address": "C4CRBV1SjhXmy4DMazNpQDcgYpJiA6yBWG", "amount": 1000000}' https://api.blockcypher.com/v1/bcy/test/faucet?token=c8a0cbdbe66d4be6974728f9ffcc2a10 |

运行结果为：

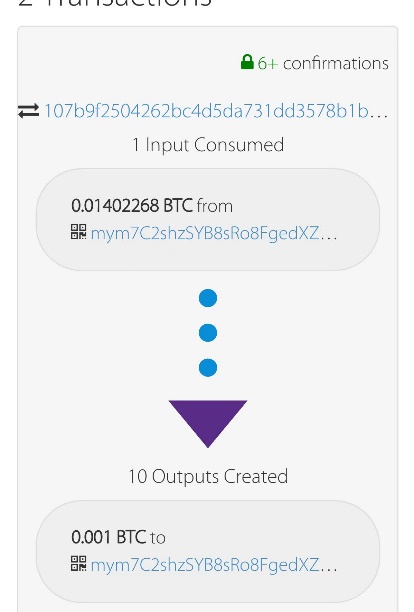
|  |
| --- |
| {  "tx\_ref": "3d1f0cac7a8b1ffe685c04793b36d3322e465456ce5e042bffd9a922b5a77449"  } |



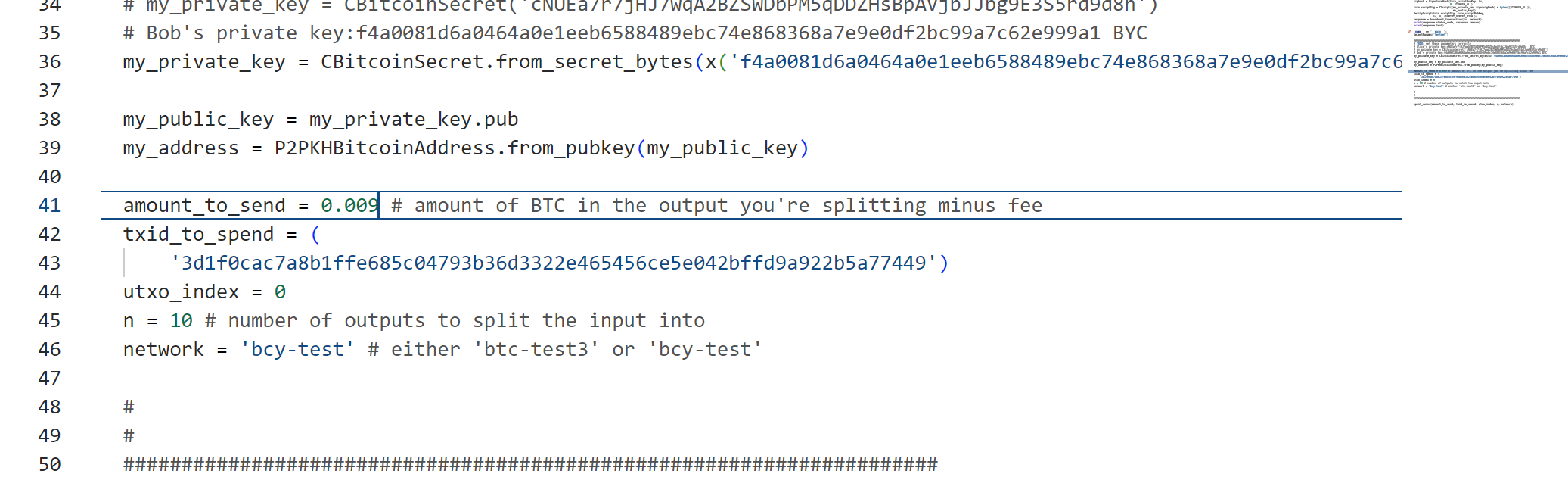
## 划分Alice的BTC币：



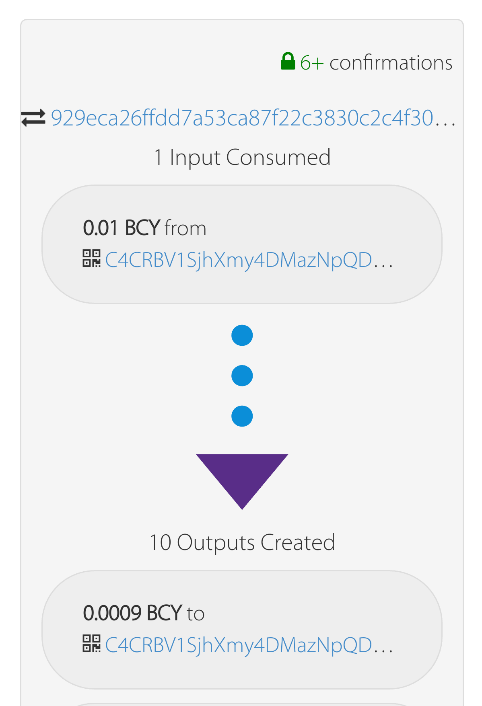
|  |
| --- |
| 201 Created  {  "tx": {  "block\_height": -1,  "block\_index": -1,  "hash": "107b9f2504262bc4d5da731dd3578b1bebf1227be33fd16832d23015f21a181b",  "addresses": [  "mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD"  ],  "total": 1000000,  "fees": 402268,  "size": 497,  "vsize": 497,  "preference": "high",  "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": "47304402204fccb76d7a3efdd77f5b6c7c52f52c5875ad88cfd3acf1d39248fc2cf01474ba02204962e712f60e33b96417e7015719a0de3c63e656dc7e6ab463315e92bae94b3f012102e3583865e1e09a67b80b1065a6dc340d8ee6c8bc5712e3e6e38ac514bf25337e",  "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": [  "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"  },  {  "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：



|  |
| --- |
| 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": "47304402204e7055c045297d28306d2e3f273beaf8b15507dd380ea98f726a71b682a5e822022038bf5885ba1cf0724e47f11093b83facf15e320c45ff1f38da7e35d4499cb3ff0121024d93827557d47cee4e5fe988d452ab05648010b182c1f37a0b968a3ce33c701d",  "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"  },  {  "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"  },  {  "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

## 

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": "48304502210081400f31427eb8dc81c10aee2ae9d63f9bd031f6e4bbef73d25cf9ce5928cb14022042d48c5f262d2728bed223b59e02ecc67e44c33a9b0302a87dd47ae892557337012102e3583865e1e09a67b80b1065a6dc340d8ee6c8bc5712e3e6e38ac514bf25337e",  "output\_value": 100000,  "sequence": 4294967295,  "addresses": [  "mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD"  ],  "script\_type": "pay-to-pubkey-hash",  "age": 2407844  }  ],  "outputs": [  {  "value": 70000,  "script": "2103dfd733a1abc0b0b8c16bbb80b48d7ce461250c82a120ea77cb3a298d24f8d3cead762102e3583865e1e09a67b80b1065a6dc340d8ee6c8bc5712e3e6e38ac514bf25337eac63755167a914853b775079232503df966e626618e1d388a957208768",  "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": "2102c3b0944b8787de28c2afb77989cc3c319426276c7a341a3c62cad854a540890fad7621024d93827557d47cee4e5fe988d452ab05648010b182c1f37a0b968a3ce33c701dac63755167a914853b775079232503df966e626618e1d388a957208768",  "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：

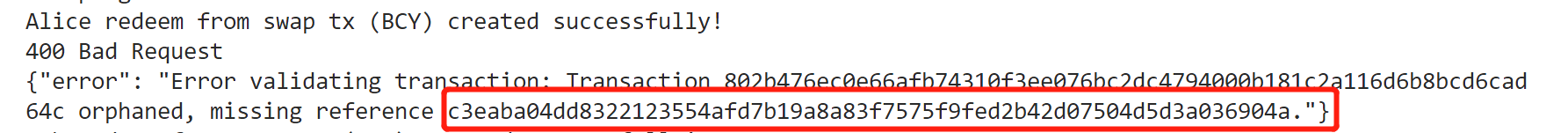
在询问助教后得知，出现这个错误可能是由以下两个原因导致的：

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】

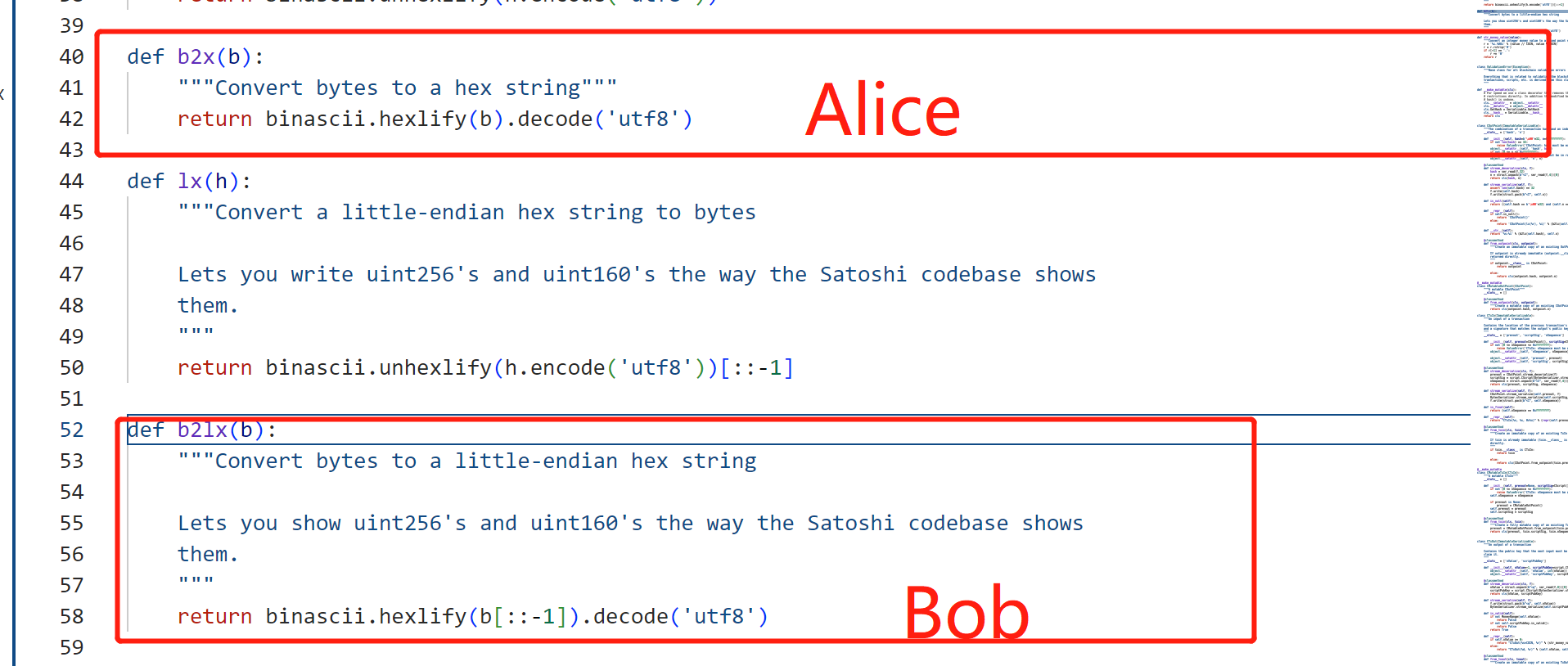


【下图为Alice redeem transaction报错】



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】



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": "47304402203a7a94bd42ff613ab681073f27b6ec7cca6940ddf8317e76606da0da869e779302203a3123cfdc5525121b8fc18ad62c544fa7777d8e249847a00b05f296b74e72ff012102e3583865e1e09a67b80b1065a6dc340d8ee6c8bc5712e3e6e38ac514bf25337e",  "output\_value": 100000,  "sequence": 4294967295,  "addresses": [  "mym7C2shzSYB8sRo8FgedXZEFwDAZaBwwD"  ],  "script\_type": "pay-to-pubkey-hash",  "age": 2407844  }  ],  "outputs": [  {  "value": 70000,  "script": "2103dfd733a1abc0b0b8c16bbb80b48d7ce461250c82a120ea77cb3a298d24f8d3cead762102e3583865e1e09a67b80b1065a6dc340d8ee6c8bc5712e3e6e38ac514bf25337eac63755167a914853b775079232503df966e626618e1d388a957208768",  "addresses": null,  "script\_type": "unknown"  }  ]  }  } |
| 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": "2102c3b0944b8787de28c2afb77989cc3c319426276c7a341a3c62cad854a540890fad7621024d93827557d47cee4e5fe988d452ab05648010b182c1f37a0b968a3ce33c701dac63755167a914853b775079232503df966e626618e1d388a957208768",  "addresses": null,  "script\_type": "unknown"  }  ]  }  } |

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": "187468697349734153656372657450617373776f7264313233483045022100bcd45b56926175d9ad63dcc8042b0eea1fba42f03a34eed99935f08e27df586c02205a0b919d7457112f5fc97ca4dbfa2cc91c7a276ad94ef4114e41b66c29a65ec101",  "output\_value": 59999,  "sequence": 4294967295,  "script\_type": "unknown",  "age": 566492  }  ],  "outputs": [  {  "value": 50000,  "script": "76a914778850be03c3d997bf37c8b95766a459a51f231188ac",  "addresses": [  "C42KJ7wavgTpCtK9ob2fuYNWV9ciFnhV24"  ],  "script\_type": "pay-to-pubkey-hash"  }  ]  }  } |
| 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": "187468697349734153656372657450617373776f726431323347304402207ea896316ca4875471aefda818c5080cd1acefa32a6557fa4f8a3f685f3e871f022017aa9eaacce8a2f908830e7f2666457485f2f07e9720a82e5c1c58fa2cde53a801",  "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。 |