

Alice

Private key: cNmVHb4PKqQYfcSqn2fYXT24eYVorpEuE8P74DPmUAZMw7F5jGuJ
Address: mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP

Bob

Private key: cUaHgy7dvDm3b3shFPU6VBXd6Jv6q176FHBP1u2sXWA1dePp09p3
Address: mmjoy4sU72BmkgF9QTVuA9Q4A2uMgRTbVn

BTC

为Alice在BTC上领取测试币

<https://live.blockcypher.com/btc-testnet/tx/8c4f295adb8955df01cabd6d4b2bd17b14584f13ecf506359b3e2fbe2d44559a/>

领币成功

Bitcoin testnet faucet

Donate?

We sent **0.00026917** bitcoins to address
mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP

tx:
8c4f295adb8955df01cabd6d4b2bd17b14584f13ecf506359b3e2fbe2d44559a

Send coins back, when you don't need them anymore to the address
tb1qerzrlxcfu24davlur5sqmgzzgsal6wusda40er

Back

Bitcoin Talk Thread

↔

Bitcoin Testnet Transaction

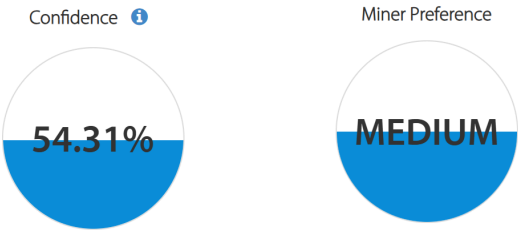
8c4f295adb8955df01cabd6d4b2bd17b14584f13ecf506359b3e2fbe2d444559a

AMOUNT TRANSACTED
1.20992126 BTC

FEES
0.00011862 BTC

RECEIVED
⌚ 3 minutes ago

CONFIRMATIONS ⓘ
🔒 0/6



Size	187 bytes
Virtual Size	136 vbytes
Lock Time	3487788
Version	2
Relayed By:	1.228.21.110:18333

</> API Call

🔗 API Docs

分币为10笔交易

201 Created

```
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "90097821d25dfab51e56fdc62735381d644acdeb3f9a765a3a21f5c3cba72ef",
    "addresses": [
      "mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP"
    ],
    "total": 300,
    "fees": 26617,
    "size": 497,
    "vsize": 497,
    "preference": "low",
    "relayed_by": "111.33.78.6",
    "received": "2024-11-23T17:13:34.60994977Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 10,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "8c4f295adb8955df01cabd6d4b2bd17b14584f13ecf506359b3e2fbe2d44559a",
        "output_index": 1,
        "script": "473044022006e960a18b03a378424e82049975a549b797d721521ac09c2e8e15974ddae8cf022074ad6bcac17e7385f256afa301b86177",
        "output_value": 26917,
        "sequence": 4294967295,
        "addresses": [
          "mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 0
      }
    ],
    "outputs": [
      {
        "value": 30,
        "script": "76a9147b1dd63903518a5db143091465036a343f74bf2788ac",
        "addresses": [
          "mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP"
        ],
        "script_type": "pay-to-pubkey-hash"
      },
      {
        "value": 30,
        "script": "76a9147b1dd63903518a5db143091465036a343f74bf2788ac",
        "addresses": [
          "mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP"
        ],
        "script_type": "pay-to-pubkey-hash"
      },
      {
        "value": 30,
        "script": "76a9147b1dd63903518a5db143091465036a343f74bf2788ac",
        "addresses": [
          "mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}
```

```

    "addresses": [
      "mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP"
    ],
    "script_type": "pay-to-pubkey-hash"
  },
  {
    "value": 30,
    "script": "76a9147b1dd63903518a5db143091465036a343f74bf2788ac",
    "addresses": [
      "mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP"
    ],
    "script_type": "pay-to-pubkey-hash"
  },
  {
    "value": 30,
    "script": "76a9147b1dd63903518a5db143091465036a343f74bf2788ac",
    "addresses": [
      "mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP"
    ],
    "script_type": "pay-to-pubkey-hash"
  },
  {
    "value": 30,
    "script": "76a9147b1dd63903518a5db143091465036a343f74bf2788ac",
    "addresses": [
      "mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP"
    ],
    "script_type": "pay-to-pubkey-hash"
  },
  {
    "value": 30,
    "script": "76a9147b1dd63903518a5db143091465036a343f74bf2788ac",
    "addresses": [
      "mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP"
    ],
    "script_type": "pay-to-pubkey-hash"
  }
]
}

```

BCY

注册账户获取API token

Alice: 7fd067d5ba3f45dcdb69a9acbdb63d80
Bob: edd09d454064449e9eba503252f1bfc0

创建密钥

Alice

```
>curl -X POST https://api.blockcypher.com/v1/bcy/test/addrs?token=edd09d454064449e9eba503252f1bfc0
{
  "private": "5e5270a7adba1fd5de9f2f108b5c8fee1c700145ab840a37ad89ff77bf985d28",
  "public": "02159a749dbb956217d6f0d4401bbf0e34178f26dc9aa74eb8ce6b96b85df8fdfa",
  "address": "C2LDuH2Jz2LqWFLn5s6UvLk4SaX3ZCjLRG",
  "wif": "BrVP2BhXSXhRidShr2WxUnZgybdKf8Fq2esk62z5HBv6WUoHrz5z"
}
```

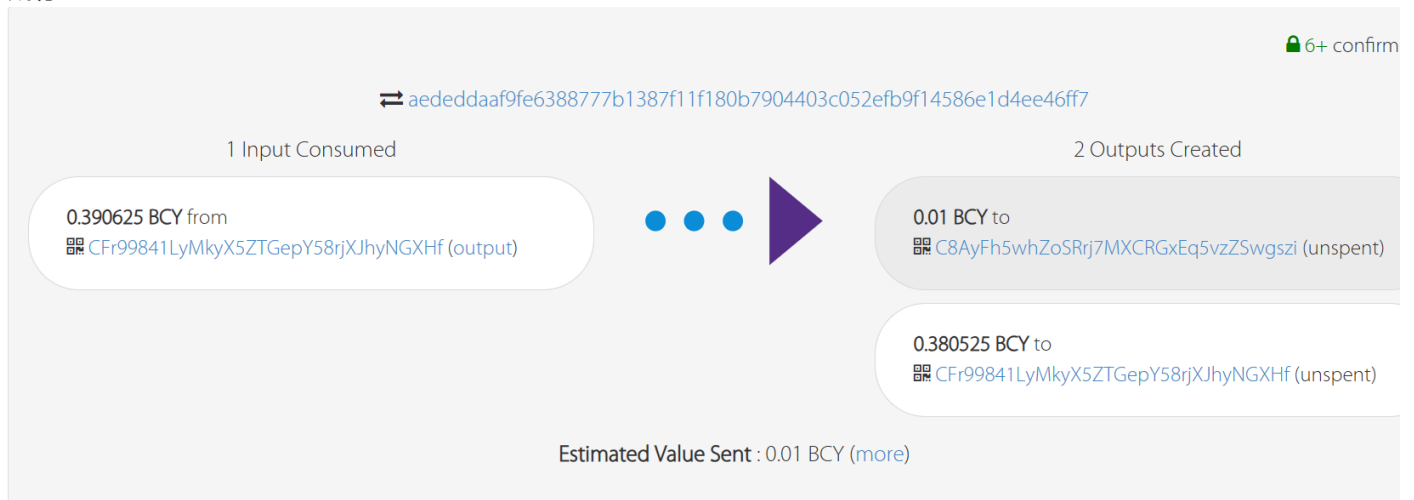
Bob

```
>curl -X POST https://api.blockcypher.com/v1/bcy/test/addrs?token=edd09d454064449e9eba503252f1bfc0
{
  "private": "38e2a9ad1d9faaccefc229765c1598a660a40a9776930843505941cd6b3bf836",
  "public": "03269d53c5eb3452425f8dda43b36cc3b9c85f04ceb451c648de8257895b7ae5bb",
  "address": "C8AyFh5whZoSRrj7MXCRGxEq5vzZSwgszi",
  "wif": "BqEcFTWmD4SGbUetRS6TSGgJVxVCz4ThU83hwCmqGuvFygxwDtk8"
}
```

为Bob的BCY地址领取测试币

```
C:\Users\孙启森>curl -d "{\"address\": \"C8AyFh5whZoSRrj7MXCRGxEq5vzZSwgszi\", \"amount\": 1000000}" https://api.blockcypher.com/v1/bcy/test/addrs?token=edd09d454064449e9eba503252f1bfc0
{
  "tx_ref": "aededdaaf9fe6388777b1387f11f180b7904403c052efb9f14586e1d4ee46ff7"
}
```

领币成功



练习

A

```
def coinExchangeScript(public_key_sender, public_key_recipient, hash_of_secret):  
    return [  
        # fill this in!  
        public_key_recipient,  
        OP_CHECKSIG,  
        OP_IF,  
        OP_DUP,  
        public_key_sender,  
        OP_CHECKSIG,  
        OP_IF,  
        OP_DROP,  
        OP_1,  
        OP_ELSE,  
        OP_HASH160,  
        hash_of_secret,  
        OP_EQUAL,  
        OP_ENDIF,  
        OP_ENDIF  
    ]
```

B

a

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

b

```
def coinExchangeScriptSig2(sig_sender, sig_recipient):  
    return [  
        # fill this in!  
        sig_sender,  
        sig_recipient  
    ]
```

C

获取区块高度

```
# Get current block height (for locktime) in 'height' parameter for each blockchain (and put it into swap.py):
# curl https://api.blockcypher.com/v1/btc/test3
btc_test3_chain_height = 3487947#都要获取实时的

# curl https://api.blockcypher.com/v1/bcy/test
bcy_test_chain_height = 1604101
```

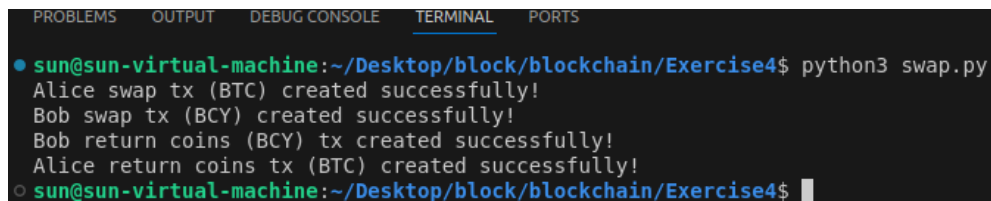
设置lock_time

```
alice_locktime = 5
bob_locktime = 3
```

这里设置alice的锁定时间为5个区块，Bob的为3个区块，这里BOb的锁定时间少于Alice。可以让Alice尽快提供secret。从而确保交易的原子性、防止恶意行为、确保交易的顺利进行、防止网络延迟以及确保资金安全。

运行swap.py

```
这里首先设置为不进行广播，并且回退交易
broadcast_transactions = False
alice_redeems = False
```



```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
● sun@sun-virtual-machine:~/Desktop/block/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!
○ sun@sun-virtual-machine:~/Desktop/block/blockchain/Exercise4$
```

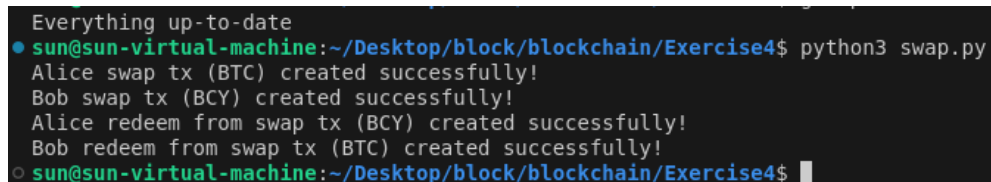
可以看到，二者的钱都发生了回退。

output

```
sun@sun-virtual-machine:~/Desktop/block/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!
```

接下来设置为进行交易

```
broadcast_transactions = False
alice_redeems = True
```



```
Everything up-to-date
● sun@sun-virtual-machine:~/Desktop/block/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!
○ sun@sun-virtual-machine:~/Desktop/block/blockchain/Exercise4$
```

这里看到两者都完成了交易

output

```
sun@sun-virtual-machine:~/Desktop/block/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!
```

```
broadcast_transactions = True  
alice_redeems = False
```

output

ython3 swap.py

Alice swap tx (BTC) created successfully!

201 Created

```
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "c36484240b9420b44f451fdb5d614b4272da77e0fcdf6b4c7b342c488b83dbb5",
    "addresses": [
      "mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP"
    ],
    "total": 1900,
    "fees": 1099,
    "size": 341,
    "vsize": 341,
    "preference": "low",
    "relayed_by": "221.238.245.58",
    "received": "2024-11-24T02:28:02.505759503Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "ee7f7fd527ed2473aaec0ce380c027db4ad171a14ea11fdaea150aff50221151",
        "output_index": 5,
        "script": "4730440220068d81b50c078002d85ebcae2653c130c3d7a80209434c666a4ea8a8c74c250802203d3bd4f76bd0086b0750d6ab6e285793",
        "output_value": 2999,
        "sequence": 4294967295,
        "addresses": [
          "mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2983394
      }
    ],
    "outputs": [
      {
        "value": 1900,
        "script": "2103c064596880c1aff1e77c8875cf507f92aecd2a7a8e865f6edda10f9242e3659cac632103fb43c50a150e6c643959142043ea769a19",
        "addresses": null,
        "script_type": "unknown"
      }
    ]
  }
}
```

Bob swap tx (BCY) created successfully!

201 Created

```
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "b60e94de0d766c739ffd5516e2e546d00f9ad3637aa2321e043f56e1154e9e38",
    "addresses": [
      "C8AyFh5whZoSRrj7MXCRGxEq5vzZSwgszi"
    ],
    "total": 999900,
    "fees": 100,
    "size": 342,
    "vsize": 342,
    "preference": "low",
    "relayed_by": "111.33.78.6",

```

```

"received": "2024-11-24T02:28:03.73192042Z",
"ver": 1,
"double_spend": false,
"vin_sz": 1,
"vout_sz": 1,
"confirmations": 0,
"inputs": [
  {
    "prev_hash": "4a9f867a1f0a5a06deab4c5187dbd6d7f65085f5840cd5533751842d8044aa9c",
    "output_index": 0,
    "script": "483045022100824f88cd9396558245571f7118e3cabeb3a9d836f4173f2da871db1114d43cb4022079b2fbd33057fc172f65e503ea7c81",
    "output_value": 1000000,
    "sequence": 4294967295,
    "addresses": [
      "C8AyFh5whZoSRrj7MXCRGxEq5vzZSwgszi"
    ],
    "script_type": "pay-to-pubkey-hash",
    "age": 1604133
  }
],
"outputs": [
  {
    "value": 999900,
    "script": "2103269d53c5eb3452425f8dda43b36cc3b9c85f04ceb451c648de8257895b7ae5bbac632102159a749dbb956217d6f0d4401bbf0e3417",
    "addresses": null,
    "script_type": "unknown"
  }
]
}
}
Sleeping for 20 minutes to let transactions confirm...
Bob return coins (BCV) 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": "ce868bf7b2f1a5f643ec54f1d0179a26b9d344de407e2bd9e1fd80d2d4dfe260",
    "addresses": [
      "C8AyFh5whZoSRrj7MXCRGxEq5vzZSwgszi"
    ],
    "total": 999800,
    "fees": 100,
    "size": 230,
    "vsize": 230,
    "preference": "low",
    "relayed_by": "221.238.245.58",
    "received": "2024-11-24T03:18:04.83399429Z",
    "ver": 1,
    "lock_time": 1604142,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "b60e94de0d766c739fffd5516e2e546d00f9ad3637aa2321e043f56e1154e9e38",
        "output_index": 0,
        "script": "483045022100d5c20045a731b131a596d89880f5cd546dabf8eb0753bb8a58bbdf289adc7d022014238db96bbb8b6b96e078265d8bac",
        "output_value": 999900,
        "sequence": 4294967295,

```

```

    "script_type": "unknown",
    "age": 1604165
  }
],
"outputs": [
  {
    "value": 999800,
    "script": "76a914a50bd5031d1a07a59014747cd234e73134944e1288ac",
    "addresses": [
      "C8AyFh5whZoSRnj7MXCRGxEq5vzZSwgszi"
    ],
    "script_type": "pay-to-pubkey-hash"
  }
]
}
}

```

Sleeping for alice_locktime blocks to pass locktime...

201 Created

```

{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "04eb345296b58461f6e0d7399680930b374f51221bff2177a7011ae226e17a44",
    "addresses": [
      "mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP"
    ],
    "total": 1800,
    "fees": 100,
    "size": 229,
    "vsize": 229,
    "preference": "low",
    "relayed_by": "221.238.245.58",
    "received": "2024-11-24T03:38:06.144808504Z",
    "ver": 1,
    "lock_time": 3487969,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "c36484240b9420b44f451fdb5d614b4272da77e0fcd6b4c7b342c488b83dbb5",
        "output_index": 0,
        "script": "473044022049fbc0efcb2f45529fc47b317611afdd564706b4d17cbcd51f8895aa830e58f502206cafedd7989e0c36177e57f7a5a70396",
        "output_value": 1900,
        "sequence": 4294967295,
        "script_type": "unknown",
        "age": 0
      }
    ],
    "outputs": [
      {
        "value": 1800,
        "script": "76a9147b1dd63903518a5db143091465036a343f74bf2788ac",
        "addresses": [
          "mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}

```

可以看到交易进行了回退

10 of 18 Transactions

5/6 confirmations

ce868bf7b2f1a5f643ec54f1d0179a26b9d344de407e2bd9e1fd80d2d4dfe260

1 Input Consumed

0.009999 BCY Unknown Script Type (output)

...

1 Output Created

0.009998 BCY to
C8AyFh5whZoSRj7MXCRGxEq5vzZSwgszi (unspent)

Value Transacted : 0.009998 BCY

0/6 confirmations

04eb345296b58461f6e0d7399680930b374f51221bff2177a7011ae226e17a44

1 Input Consumed

0.000019 BTC Unknown Script Type (output)

...

1 Output Created

0.000018 BTC to
mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP (unspent)

Value Transacted : 0.000018 BTC

```
broadcast_transactions = True
alice_redeems = True
```

这里设置了广播并设置为进行交易，可以看到等待了20分钟进行了确认
output

Alice swap tx (BTC) created successfully!

201 Created

```
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "79953b31e9ccc857d0e16dc85eb4141b95c947bfce088be139037ec7b66c91cd",
    "addresses": [
      "mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP"
    ],
    "total": 1900,
    "fees": 1099,
    "size": 341,
    "vsize": 341,
    "preference": "low",
    "relayed_by": "111.33.78.6",
    "received": "2024-11-24T02:03:13.959078757Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "ee7f7fd527ed2473aaec0ce380c027db4ad171a14ea11fdaea150aff50221151",
        "output_index": 4,
        "script": "47304402204e24f7d8a36ebabb9f6533b5cce0c40ade819e3ba47e665c95717d362701bc7d02207d23a16807897de4f87215dc397c6bd9",
        "output_value": 2999,
        "sequence": 4294967295,
        "addresses": [
          "mrjw9kGnUfcCEAYWXkSB5du1eoSCwsFNPP"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2983394
      }
    ],
    "outputs": [
      {
        "value": 1900,
        "script": "2103c064596880c1aff1e77c8875cf507f92aecd2a7a8e865f6edda10f9242e3659cac632103fb43c50a150e6c643959142043ea769a19",
        "addresses": null,
        "script_type": "unknown"
      }
    ]
  }
}
```

Bob swap tx (BCY) created successfully!

201 Created

```
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "ced9739daab4260322cb2498e5704bba381f658586eedb694aae5be38442d16d",
    "addresses": [
      "C8AyFh5whZoSRrj7MXCRGxEq5vzZSwgszi"
    ],
    "total": 999900,
    "fees": 100,
    "size": 342,
    "vsize": 342,
    "preference": "low",
    "relayed_by": "221.238.245.58",
    "received": "2024-11-24T02:03:14.973848588Z",
```

```

"ver": 1,
"double_spend": false,
"vin_sz": 1,
"vout_sz": 1,
"confirmations": 0,
"inputs": [
  {
    "prev_hash": "3aca8b76de04bf832a11c6e75321ceb4aa0488a3e51f4d3c6e22dfffb841f0882",
    "output_index": 0,
    "script": "483045022100a79d0805dd25dc9f44b47cce04cfb4f8fec9d98b80f3c4b3307ac81f6981950d02205fac205884850591bd7ec283666850",
    "output_value": 1000000,
    "sequence": 4294967295,
    "addresses": [
      "C8AyFh5whZoSRnj7MXCRGxEq5vzZSwgszi"
    ],
    "script_type": "pay-to-pubkey-hash",
    "age": 1604133
  }
],
"outputs": [
  {
    "value": 999900,
    "script": "2103269d53c5eb3452425f8dda43b36cc3b9c85f04ceb451c648de8257895b7ae5bbac632102159a749dbb956217d6f0d4401bbf0e3417",
    "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": "f017d670e6bda746c4ba5c7a6a0edd295e297419a8ebe290e81b2e3829d5f8c8",
    "addresses": [
      "C2LDuH2Jz2LqWFLn5s6UvLk4SaX3ZCjLRG"
    ],
    "total": 999800,
    "fees": 100,
    "size": 183,
    "vsize": 183,
    "preference": "low",
    "relayed_by": "111.33.78.6",
    "received": "2024-11-24T02:23:16.390777528Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "ced9739daab4260322cb2498e5704bba381f658586eedb694aae5be38442d16d",
        "output_index": 0,
        "script": "187468697349734153656372657450617373776f7264313233483045022100834a33a1df823ad2b8d47217a8f0bbaef9d7f36b245417df",
        "output_value": 999900,
        "sequence": 4294967295,
        "script_type": "unknown",
        "age": 1604140
      }
    ],

```

```

    "outputs": [
      {
        "value": 999800,
        "script": "76a91464fb0c6ff0369edf0936fac20e3a205d00c4f0bd88ac",
        "addresses": [
          "C2LDuH2Jz2LqWFLn5s6UvLk4SaX3ZCjLRG"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}

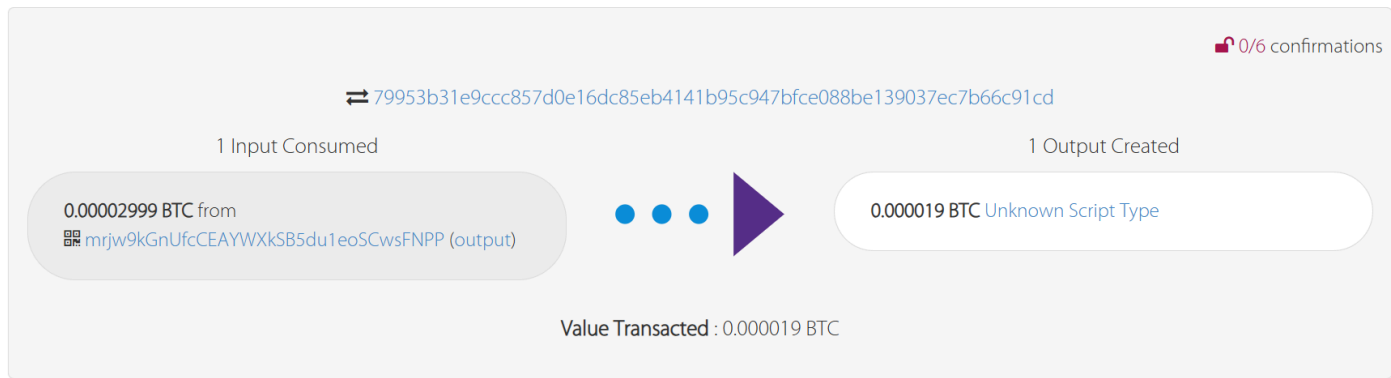
Bob redeem from swap tx (BTC) created successfully!
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "a8f689bc75ae653adfc15f15afae174630ed2af7e26662b7044020efa75ef261",
    "addresses": [
      "mmjoy4sU72BmkgF9QTVuA9Q4A2uMgRTbVn"
    ],
    "total": 1800,
    "fees": 100,
    "size": 182,
    "vsize": 182,
    "preference": "low",
    "relayed_by": "111.33.78.6",
    "received": "2024-11-24T02:23:17.557639139Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "79953b31e9ccc857d0e16dc85eb4141b95c947bfce088be139037ec7b66c91cd",
        "output_index": 0,
        "script": "187468697349734153656372657450617373776f72643132334730440220386502ceef1cfb5954df49c526a94724092a09b2ce81854ec0",
        "output_value": 1900,
        "sequence": 4294967295,
        "script_type": "unknown",
        "age": 0
      }
    ],
    "outputs": [
      {
        "value": 1800,
        "script": "76a914443f35fc56fc804aa900b6d489be08d3da8dee6288ac",
        "addresses": [
          "mmjoy4sU72BmkgF9QTVuA9Q4A2uMgRTbVn"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}

```

交易截图

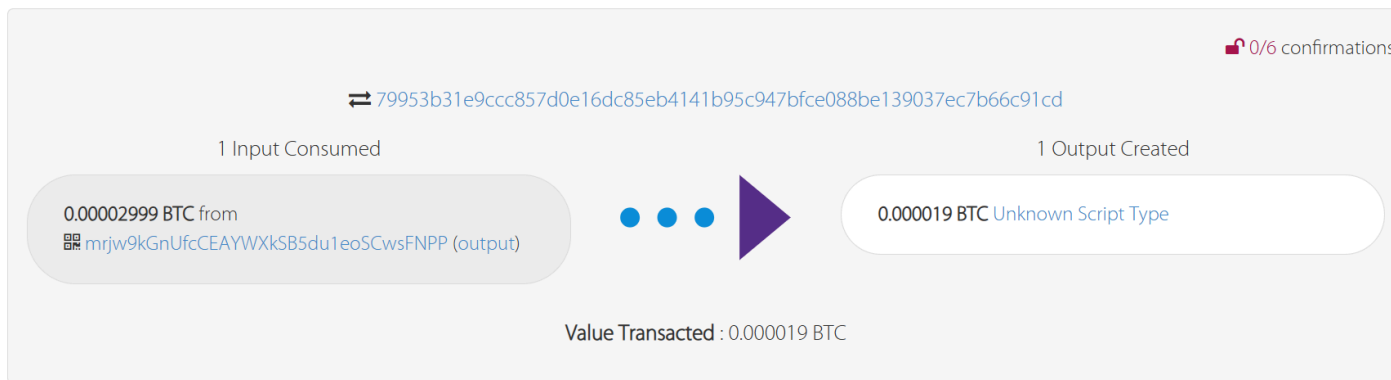
Alice创建TX1

7 Transactions (2 unconfirmed)

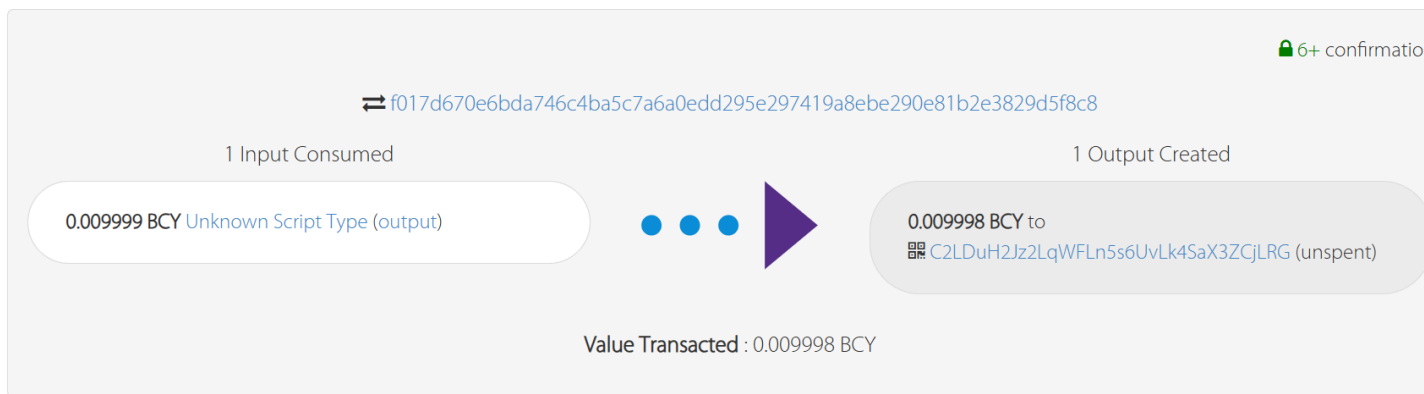


Bob创建交易TX3

7 Transactions (2 unconfirmed)

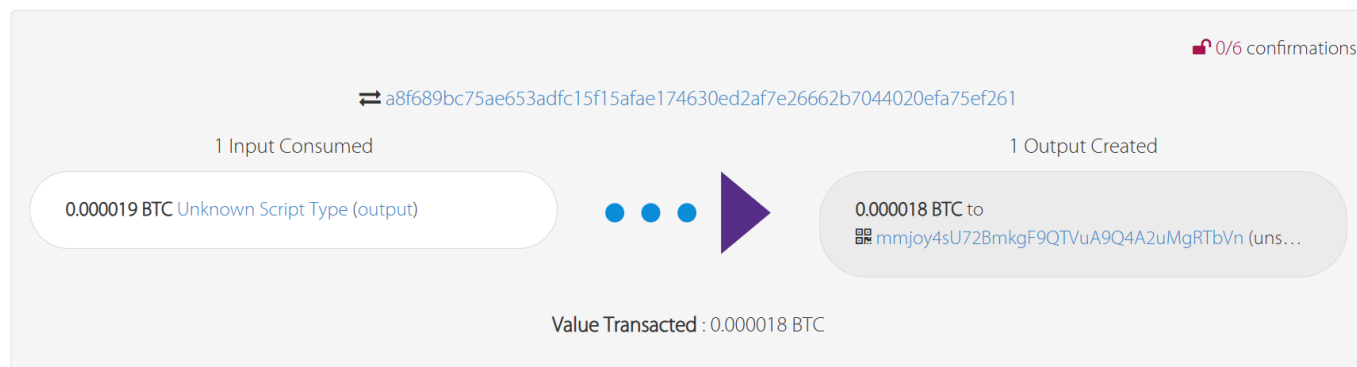


Alice获取Bob的BCY



Bob获取Alice发送的BTC

7 Transactions (1 unconfirmed)



D

a 解释代码内容，以及coinExchangeScript是如何工作

本次实验中补充的代码主要由两部分组成

- 第一部分是一些密钥等的补充，按照实验指导说明一步步完成即可。
 - 此处遇到的问题是Windows中cmd对单引号的不支持，经过对其进行转义后得以修复。
- 第二部分为交易脚本的编写
- coinExchangeScript

```
def coinExchangeScript(public_key_sender, public_key_recipient, hash_of_secret):  
    return [  
        # fill this in!  
        public_key_recipient,  
        OP_CHECKSIG, #首先判断接收者的签名  
        OP_IF, #若为1则继续  
        OP_DUP, #复制栈顶元素，用来接续if, else。不然到else时会发生空的情况  
        public_key_sender, #判断是否是发送者来赎回  
        OP_CHECKSIG, #验证签名  
        OP_IF,  
        OP_DROP,  
        OP_1, ##是的话则清空前面的复制，设置为真  
        OP_ELSE, #为假则继续else  
        OP_HASH160,  
        hash_of_secret, #判断是否为秘密  
        OP_EQUAL, ##验证真假  
        OP_ENDIF,  
        OP_ENDIF  
    ]
```

逻辑功能

这个脚本允许通过以下条件之一解锁资金：

1. **发送者和接收者双方签名：**
如果发送者和接收者的签名都有效，则资金可以被花费。
2. **匹配秘密哈希值：**
如果一方提供了秘密 x ，并且其哈希值与预定义的 $H(x)$ 匹配，则允许花费资金。

- coinExchangeScriptSig1

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

- 这种情况实现接收者知道秘密x的情况下赎回交易

- coinExchangeScriptSig2

```
def coinExchangeScriptSig2(sig_sender, sig_recipient):  
    return [  
        # fill this in!  
        sig_recipient,  
        sig_sender  
    ]
```

- 这种情况下可以在双方都同意的情况下赎回交易

b 以Alice用coinExchangeScript向Bob发送硬币为例

1) 如果Bob不把钱赎回来，Alice为什么总能拿回她的钱？

- 采用了时间锁的机制，当在设定的锁定时间内没有完成时，Alice就可以解锁自己的回退交易，从而将自己的钱拿回。

2) 为什么不能用简单的1/2 multisig来解决这个问题？

- 1/2 multisig 无法结合时间锁定和哈希锁定来保证交易的原子性。如果使用了1/2 multisig，可能会发生连续赎回自己发出的钱和对方发送的钱的问题。

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。

交易描述和顺序

1. TX1: Alice 支付给 Bob 的比特币

- 解锁条件：

SigA && SigB 或者 SigB && H(x)

- 说明：

这是 Alice 创建的交易，它将比特币锁定到一个脚本地址。Bob 可以通过以下任意一种方式解锁资金：

- 双方签名 SigA && SigB

- Bob 提供秘密 x 的哈希值 $H(x)$ ，加上他的签名 SigB

这个设计确保资金只有在揭露 x 或双方同意时，才能被 Bob 领取。

2. TX2: 从 TX1 支付给 Alice 的比特币

- 解锁条件：

SigA，锁定 48 小时后可执行。

- 说明：

这是 Alice 的退款交易。它允许 Alice 在 Bob 未能解锁 TX1 的条件下，等待 48 小时后收回比特币。这确保了 Alice 的资金不会永久被锁定。

3. TX3: Bob 支付给 Alice 的 BCY

- 解锁条件：

SigA && SigB 或者 SigA && H(x)

- 说明：

Bob 创建了这个交易，将 BCY 锁定到脚本地址。Alice 可以通过以下任意一种方式解锁：

- 双方签名 SigA && SigB 或者 SigA && H(x)

- Alice 提供秘密 x 的哈希值 $H(x)$ ，加上她的签名 SigA

这个设计确保 Alice 必须提供 x 或双签，才能领取 BCY。

4. TX4: 从 TX3 支付给 Bob 的 BCY

- 解锁条件：

SigB，锁定 24 小时后可执行。

- 说明：

这是 Bob 的退款交易。如果 Alice 未能解锁 TX3 的条件，Bob 可以在等待 24 小时后取回 BCY。这避免了资金永久锁定。

设计原理

1. 双向锁定机制：

- Alice 和 Bob 的资金均被锁定到条件脚本中，确保一方完成操作时，另一方能同步完成。
- 条件基于 $H(x)$ 和时间锁，保障了安全性和公平性。

2. 时间锁设计：

- TX2 的时间锁（48 小时）比 TX4 的时间锁（24 小时）更长。
- 这确保了 Bob 有足够时间根据 Alice 公开的 x 在其链上解锁资金。

3. 秘密揭露机制：

- Alice 赎回 TX3（BCY）时必须提供 x 。这导致 x 被广播到链上，Bob 可利用该 x 赎回 TX1（比特币）。
- 使用 x 作为核心，确保跨链的原子性。

4. 退款保障：

- 如果交易中途失败，双方都能在各自设定的时间锁到期后，取回自己的资金，避免资产永久锁定。

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？

- 成功
 - i. 首先双方在对应的网络创建了交易，Alice的BTC在btc网络，而Bob的BCY在BCY网络。
 - ii. 接着由Alice用secret解锁BOB的交易。这时Bob的BCY就已经到了Alice手中。同时这时Bob获取到了secret，通过secret解锁Alice的交易，从而得到btc。
- 失败
 - i. 同样是双方先创建了交易
 - ii. 当交易失败后，经过了对应的时间锁，Alice的货币就会回到自己的手中，仍旧是btc，交换失败。同样的，Bob的BCY也会回到自己手中，得不到想要的btc。