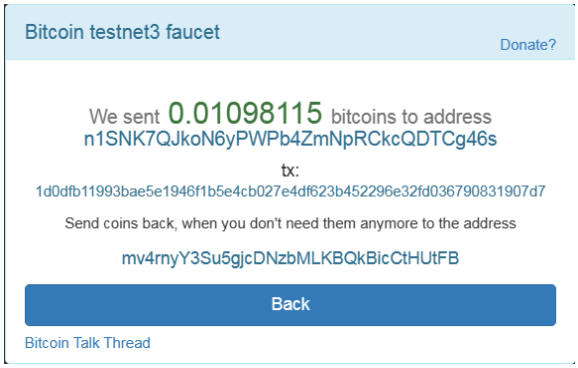
区块链实验一报告

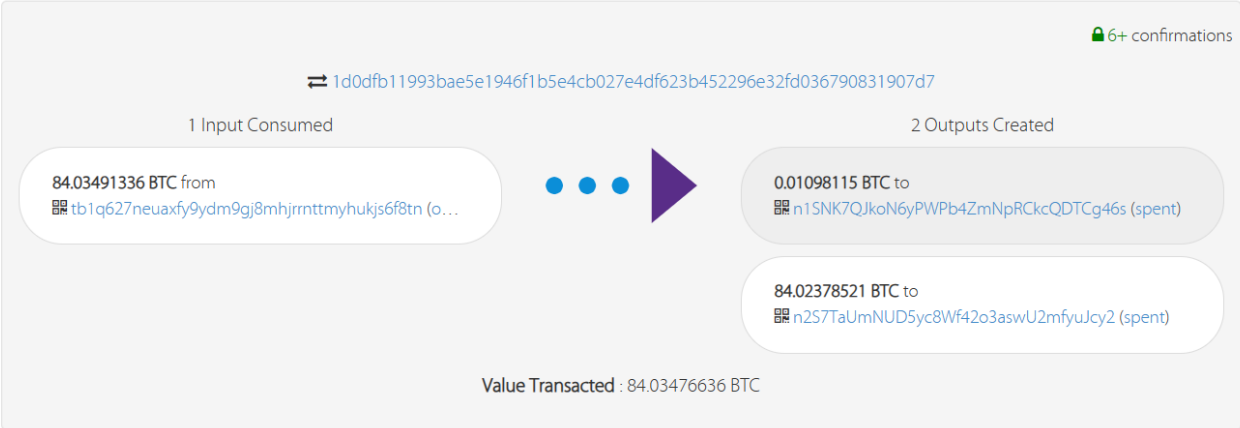
姓名：齐明杰　学号：2113997 班级：信安2班

1　领取比特币

登录网站https://coinfaucet.eu/en/btctestnet，输入地址领取测试币：



查看交易记录：



2　分币操作

faucet 将给我们一个可消费的输出，但我们希望有多个可花费的输出（至少为 3）来完成后面的多个练习，因此需要将其拆分。以防我们意外锁定一些无效的 scripts。编辑 split_test_coins.py.py，如下所示：

```
if __name__ == '__main__':
    ##############################################################################
    # TODO: set these parameters correctly
    amount_to_send = 0.003 # amount of BTC in the output you're splitting minus f
    txid_to_spend = (
        '1d0dfb11993bae5e1946f1b5e4cb027e4df623b452296e32fd036790831907d7')
    utxo_index = 0
    n=3 # number of outputs to split the input into
    ##############################################################################

    split_coins(amount_to_send, txid_to_spend, utxo_index, n)
```

其中txid就是我领取测试币时的交易hash，我将领取的币分为了3个输出。

分币结果:


```
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "0f9e86805172a59753705e6d520485f3f3cc0f8e1996d34a0abfad76dde94df5",
    "addresses": [
      "n1SNK7QJkoN6yPWPb4ZmNpRCkcQDTCg46s"
    ],
    "total": 300000,
    "fees": 798115,
    "size": 259,
    "vsize": 259,
    "preference": "high",
    "relayed_by": "172.105.223.27",
    "received": "2023-09-18T00:06:34.585744909Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 3,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"1d0dfb11993bae5e1946f1b5e4cb027e4df623b452296e32fd036790831907d7",
        "output_index": 0,
        "script":
"473044022069fc8474fc2cee01cfa9492d9bd88218ae03cd1bd250ae9e9238897c3b90b4b00220
76d3f02ee6608f889b02dacb3d77d9a194315058387eb0118f1ea99644a0b712012103389c39b16
35b32119096ce8020862ae2d98bde073572af3201de77ce3ab90553",
        "output_value": 1098115,
        "sequence": 4294967295,
        "addresses": [
          "n1SNK7QJkoN6yPWPb4ZmNpRCkcQDTCg46s"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 0
      }
    ],
    "outputs": [
      {
        "value": 100000,
```

```
        "script": "76a914da847c3ad8729e8ab3d6ca12f9097b9f8c0e141a88ac",
        "addresses": [
          "n1SNK7QJkoN6yPWPb4ZmNpRCkcQDTCg46s"
        ],
        "script_type": "pay-to-pubkey-hash"
      },
      {
        "value": 100000,
        "script": "76a914da847c3ad8729e8ab3d6ca12f9097b9f8c0e141a88ac",
        "addresses": [
          "n1SNK7QJkoN6yPWPb4ZmNpRCkcQDTCg46s"
        ],
        "script_type": "pay-to-pubkey-hash"
      },
      {
        "value": 100000,
        "script": "76a914da847c3ad8729e8ab3d6ca12f9097b9f8c0e141a88ac",
        "addresses": [
          "n1SNK7QJkoN6yPWPb4ZmNpRCkcQDTCg46s"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}
```


在网站查看分币结果如下图所示：

3 收币回faucet

完成含有TODO部分的代码，如下所示：

```
def P2PKH_scriptPubKey(address):
    ###############################################################################
    # TODO: Complete the standard scriptPubKey implementation for a
    # PayToPublicKeyHash transaction
    # 使用 OP_DUP、OP_HASH160 和 OP_EQUALVERIFY 来创建 PayToPublicKeyHash 脚本
    # 将地址的哈希值添加到脚本中
    return [OP_DUP, OP_HASH160, address, OP_EQUALVERIFY, OP_CHECKSIG]
    ###############################################################################


def P2PKH_scriptSig(txin, txout, txin_scriptPubKey):
    signature = create_OP_CHECKSIG_signature(txin, txout, txin_scriptPubKey,
                                             my_private_key)
    ###############################################################################
    # TODO: Complete this script to unlock the BTC that was sent to you
    # in the PayToPublicKeyHash transaction. You may need to use variables
    # that are globally defined.
    # 返回包含签名和公钥的脚本
    return [signature, my_public_key]
    ###############################################################################
```

同时，修改config.py中的地址，修改为一开始领取测试币时得到的退回币的地址(mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB)，并将分币得到的hash填入ex1.py中：

```
44  if __name__ == '__main__':
45      ###############################################################################
46      # TODO: set these parameters correctly
47      amount_to_send = 0.0005
48      txid_to_spend = (
49          '0f9e86805172a59753705e6d520485f3f3cc0f8e1996d34a0abfad76dde94df5')
50      utxo_index = 1
51      ###############################################################################
52
53      txout_scriptPubKey = P2PKH_scriptPubKey(faucet_address)
54      response = send_from_P2PKH_transaction(
55          amount_to_send, txid_to_spend, utxo_index, txout_scriptPubKey)
56      print(response.status_code, response.reason)
57      print(response.text)
```

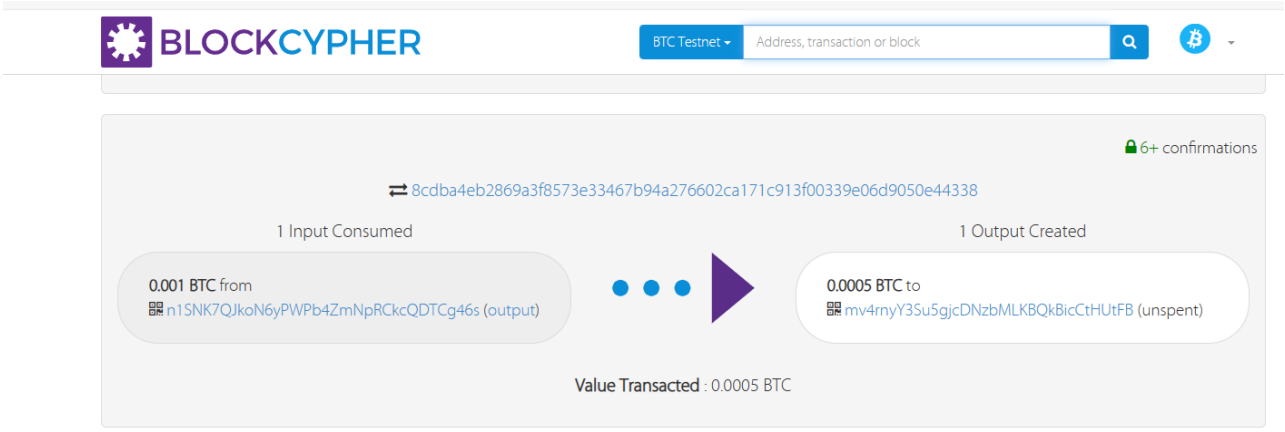
收币结果:

```
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
```

```
    "hash": "8cdba4eb2869a3f8573e33467b94a276602ca171c913f00339e06d9050e44338",
    "addresses": [
      "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB",
      "n1SNK7QJkoN6yPWPb4ZmNpRCkcQDTCg46s"
    ],
    "total": 50000,
    "fees": 50000,
    "size": 192,
    "vsize": 192,
    "preference": "high",
    "relayed_by": "139.162.108.57",
    "received": "2023-09-18T11:30:08.55639076Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"0f9e86805172a59753705e6d520485f3f3cc0f8e1996d34a0abfad76dde94df5",
        "output_index": 1,
        "script":
"483045022100c97998ac1e72f88aa851ba5f8f449826da2ac364425bc1780fb81094c9ce1c4b02
205391142cb1434a5837108adf138814507ff93dab05aa2759c12a85cdecb02948012103389c39b
1635b32119096ce8020862ae2d98bde073572af3201de77ce3ab90553",
        "output_value": 100000,
        "sequence": 4294967295,
        "addresses": [
          "n1SNK7QJkoN6yPWPb4ZmNpRCkcQDTCg46s"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2503320
      }
    ],
    "outputs": [
      {
        "value": 50000,
        "script": "76a9149f9a7abd600c0caa03983a77c8c3df8e062cb2fa88ac",
        "addresses": [
          "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
```

```
}
```

网站记录如下图所示：


BLOCKCYPHER
BTC Testnet
Address, transaction or block
6+ confirmations
8cdba4eb2869a3f8573e33467b94a276602ca171c913f00339e06d9050e44338
1 Input Consumed
1 Output Created
0.001 BTC from
n1SNK7QJkoN6yPWPb4ZmNpRCkcQDTCg46s (output)
0.0005 BTC to
mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB (unspent)
Value Transacted : 0.0005 BTC