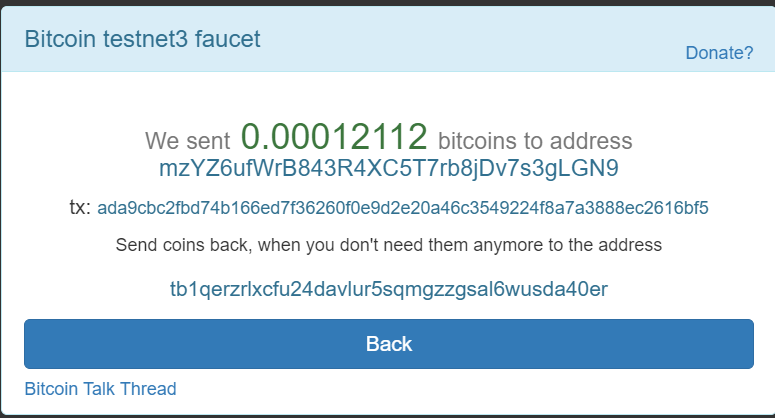
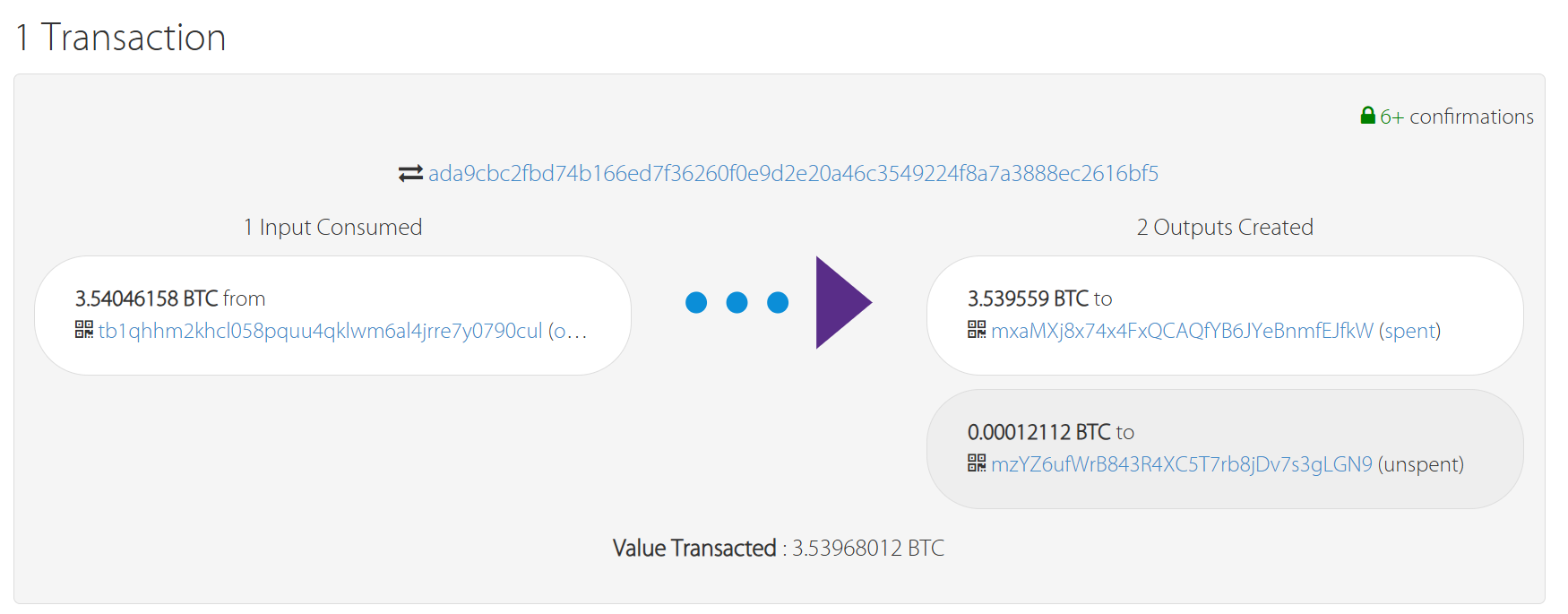
区块链实验一报告

学号：2213603 姓名：李娅琦 专业：计科

1. BTC的领取与记录

通过前一次实验，在linux中运行keygen.py以生成私钥和地址并登录网站领取并查看比特币，领取结果以及交易记录如下图：





1. 拆分BTC

由于faucet只给一个可消费的输出，但想要有多个可花费的输出（至少为 3），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，其中只需正确设置一些参数，设置要发送的BTC数量为0.0001；测试硬币平均分割成的输出数设置为10；txid设置为上一步中事务哈希值；因为我的输出是faucet 事务中的第二个输出值，则 utxo\_id为1。

代码如下：

if \_\_name\_\_ == '\_\_main\_\_':

    ######################################################################

    # TODO: set these parameters correctly

    amount\_to\_send = 0.0001 # amount of BTC in the output you're splitting minus fee

    txid\_to\_spend = (

        'ada9cbc2fbd74b166ed7f36260f0e9d2e20a46c3549224f8a7a3888ec2616bf5')

    utxo\_index = 1  #TXO（未花费的交易输出）的索引

    n=10 # 分割输入的输出数量number of outputs to split the input into

    ######################################################################

    split\_coins(amount\_to\_send, txid\_to\_spend, utxo\_index, n)

分币结果如下：

201 Created

{

"tx": {

"block\_height": -1,

"block\_index": -1,

"hash": "06708fd716c95cd7e2e33afc658efb9bd6d8c4cac558f96748e14d7494792e5c",

"addresses": [

"mzYZ6ufWrB843R4XC5T7rb8jDv7s3gLGN9"

],

"total": 10000,

"fees": 2112,

"size": 497,

"vsize": 497,

"preference": "low",

"relayed\_by": "111.33.78.6",

"received": "2024-09-25T08:38:09.043284509Z",

"ver": 1,

"double\_spend": false,

"vin\_sz": 1,

"vout\_sz": 10,

"confirmations": 0,

"inputs": [

{

"prev\_hash": "ada9cbc2fbd74b166ed7f36260f0e9d2e20a46c3549224f8a7a3888ec2616bf5",

"output\_index": 1,

"script": "47304402203cf21ce0ee31d709ff71948971ac251e1c0faf00b558cbaa99304214f0336b35022061a79cbd70f7316b8eb12d548427d30bf20a040b1300b60d13486ee94388f0fc012102205937ebab4a636973a6495b4a29531273bf726ba3f066d16f365b75bfd85962",

"output\_value": 12112,

"sequence": 4294967295,

"addresses": [

"mzYZ6ufWrB843R4XC5T7rb8jDv7s3gLGN9"

],

"script\_type": "pay-to-pubkey-hash",

"age": 2904231

}

],

"outputs": [

{

"value": 1000,

"script": "76a914d0b7dcaa798f8ee58105a455f72279e8d3fcb69b88ac",

"addresses": [

"mzYZ6ufWrB843R4XC5T7rb8jDv7s3gLGN9"

],

"script\_type": "pay-to-pubkey-hash"

},

{

"value": 1000,

"script": "76a914d0b7dcaa798f8ee58105a455f72279e8d3fcb69b88ac",

"addresses": [

"mzYZ6ufWrB843R4XC5T7rb8jDv7s3gLGN9"

],

"script\_type": "pay-to-pubkey-hash"

},

{

"value": 1000,

"script": "76a914d0b7dcaa798f8ee58105a455f72279e8d3fcb69b88ac",

"addresses": [

"mzYZ6ufWrB843R4XC5T7rb8jDv7s3gLGN9"

],

"script\_type": "pay-to-pubkey-hash"

},

{

"value": 1000,

"script": "76a914d0b7dcaa798f8ee58105a455f72279e8d3fcb69b88ac",

"addresses": [

"mzYZ6ufWrB843R4XC5T7rb8jDv7s3gLGN9"

],

"script\_type": "pay-to-pubkey-hash"

},

{

"value": 1000,

"script": "76a914d0b7dcaa798f8ee58105a455f72279e8d3fcb69b88ac",

"addresses": [

"mzYZ6ufWrB843R4XC5T7rb8jDv7s3gLGN9"

],

"script\_type": "pay-to-pubkey-hash"

},

{

"value": 1000,

"script": "76a914d0b7dcaa798f8ee58105a455f72279e8d3fcb69b88ac",

"addresses": [

"mzYZ6ufWrB843R4XC5T7rb8jDv7s3gLGN9"

],

"script\_type": "pay-to-pubkey-hash"

},

{

"value": 1000,

"script": "76a914d0b7dcaa798f8ee58105a455f72279e8d3fcb69b88ac",

"addresses": [

"mzYZ6ufWrB843R4XC5T7rb8jDv7s3gLGN9"

],

"script\_type": "pay-to-pubkey-hash"

},

{

"value": 1000,

"script": "76a914d0b7dcaa798f8ee58105a455f72279e8d3fcb69b88ac",

"addresses": [

"mzYZ6ufWrB843R4XC5T7rb8jDv7s3gLGN9"

],

"script\_type": "pay-to-pubkey-hash"

},

{

"value": 1000,

"script": "76a914d0b7dcaa798f8ee58105a455f72279e8d3fcb69b88ac",

"addresses": [

"mzYZ6ufWrB843R4XC5T7rb8jDv7s3gLGN9"

],

"script\_type": "pay-to-pubkey-hash"

},

{

"value": 1000,

"script": "76a914d0b7dcaa798f8ee58105a455f72279e8d3fcb69b88ac",

"addresses": [

"mzYZ6ufWrB843R4XC5T7rb8jDv7s3gLGN9"

],

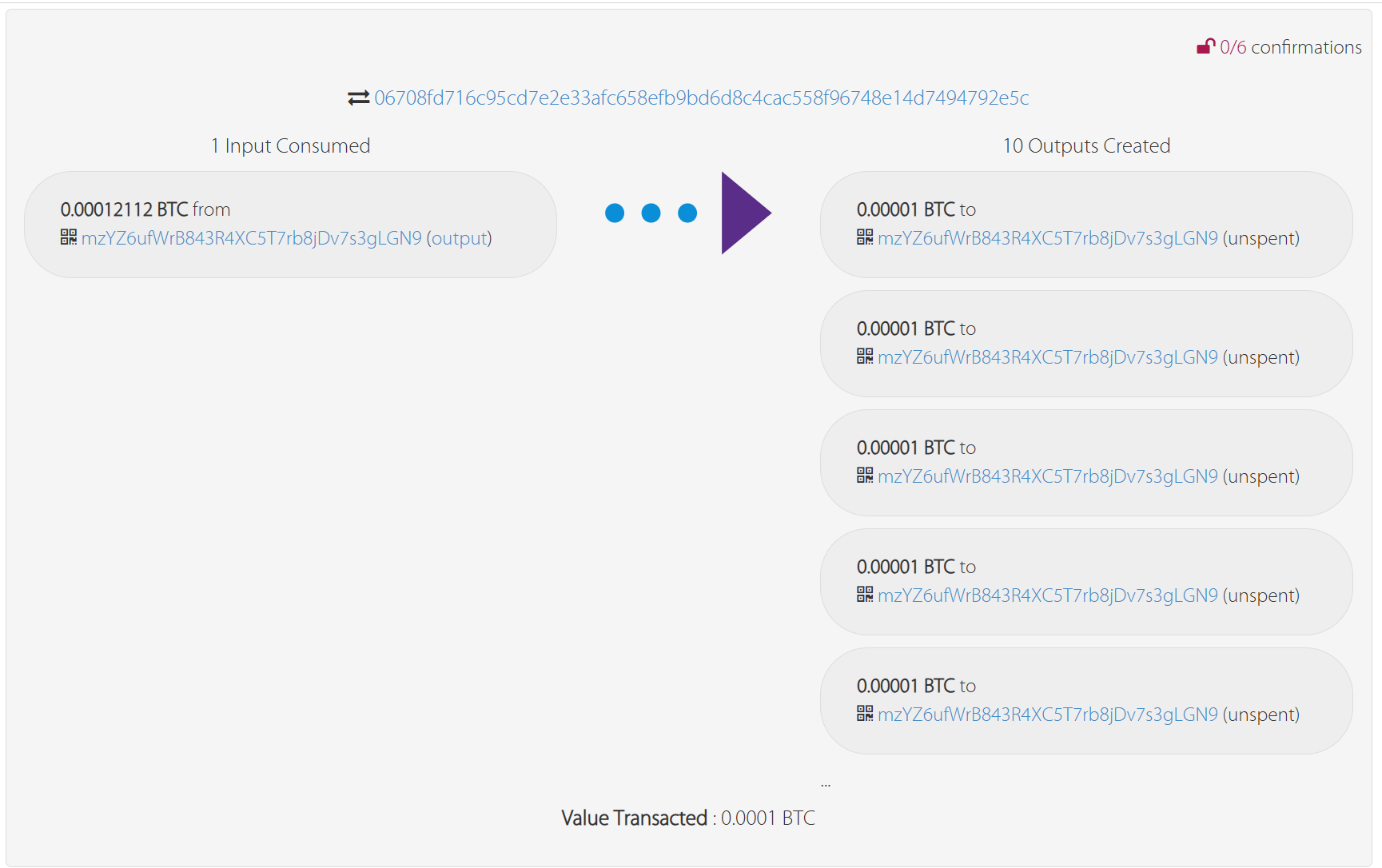
"script\_type": "pay-to-pubkey-hash"

}

]

}

}



1. BTC的回收与记录

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

    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.

    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，并将分币得到的hash填入ex1.py中：

if \_\_name\_\_ == '\_\_main\_\_':

    ######################################################################

    # TODO: set these parameters correctly

    amount\_to\_send = 0.00001

    txid\_to\_spend = (

        '06708fd716c95cd7e2e33afc658efb9bd6d8c4cac558f96748e14d7494792e5c')

    utxo\_index = 1

    ######################################################################

    txout\_scriptPubKey = P2PKH\_scriptPubKey(faucet\_address)

    response = send\_from\_P2PKH\_transaction(

        amount\_to\_send, txid\_to\_spend, utxo\_index, txout\_scriptPubKey)

    print(response.status\_code, response.reason)

    print(response.text)

收币结果：

201 Created

{

"tx": {

"block\_height": -1,

"block\_index": -1,

"hash": "20211e539803c55ed8cee5007a800e778cdaf9cb7a86deec1f211389f15ffccb",

"addresses": [

"mypWY15NQqnrdcpVU14eUGd6ndft4FY2d3",

"mzYZ6ufWrB843R4XC5T7rb8jDv7s3gLGN9"

],

"total": 1000,

"fees": 0,

"size": 191,

"vsize": 191,

"preference": "low",

"relayed\_by": "111.33.78.6",

"received": "2024-09-25T08:59:05.905354772Z",

"ver": 1,

"double\_spend": false,

"vin\_sz": 1,

"vout\_sz": 1,

"confirmations": 0,

"inputs": [

{

"prev\_hash": "06708fd716c95cd7e2e33afc658efb9bd6d8c4cac558f96748e14d7494792e5c",

"output\_index": 1,

"script": "473044022049b7ae14a71c6cc87f01a7131fa72d9105d857b854060cdd59d26d212f6bd4560220022c4da0457a67747326d960ef5f19e50a104b1273d00345f61ecebabe933e36012102205937ebab4a636973a6495b4a29531273bf726ba3f066d16f365b75bfd85962",

"output\_value": 1000,

"sequence": 4294967295,

"addresses": [

"mzYZ6ufWrB843R4XC5T7rb8jDv7s3gLGN9"

],

"script\_type": "pay-to-pubkey-hash",

"age": 0

}

],

"outputs": [

{

"value": 1000,

"script": "76a914c8c43f9b09e2aadeb3fc1d200da042443bfd3b9088ac",

"addresses": [

"mypWY15NQqnrdcpVU14eUGd6ndft4FY2d3"

],

"script\_type": "pay-to-pubkey-hash"

}

]

}

}

