南开大学
Nankai University

南　　开　　大　　学

计　算　机　学　院

区块链课程实验报告

Ex2

年级：2022 级

专业：信息安全

姓名：李佳璐

2024 年 10 月 8 日

目录

一、 实验过程

(一) ex2a.py

1. 创建账户

运行 keygen.py 创建 3 个账户（客户）

```
lijialu@lijialu-virtual-machine:/mnt/hgfs/winshare/bc$ python3 keygen.py
Private key: cNLN1CDofkHjsARUMrWJ3pDYMH3cqxh2FQrfoX5qthzYRwVShQCS
Address: n4P5XYCHqRq633LwX71AN78wVPg3rjX987
lijialu@lijialu-virtual-machine:/mnt/hgfs/winshare/bc$ python3 keygen.py
Private key: cTkfDWqLkiws7aMuqdw1stUroLeEK2fDTuSTcLW6ztSDsDJjYQtB
Address: n1cwud8uy7kTEa8SjeyF4nDkNT1826FfJJ
lijialu@lijialu-virtual-machine:/mnt/hgfs/winshare/bc$ python3 keygen.py
Private key: cTu15Tzd5VmtkqUkF1yavUJhGPzAboADMSnqpuTTiBHTsYZiKLw6
Address: mg9gwdtB9dxk94NMSidTMA56F9eZtXngKz
```

图 1: 账户创建

将以上 3 个用户私钥补充进 ex2a.py

ex2a.py （private key）

```
cust1_private_key = CBitcoinSecret('
    cNLN1CDofkHjsARUMrWJ3pDYMH3cqxh2FQrfoX5qthzYRwVShQCS')
cust1_public_key = cust1_private_key.pub
cust2_private_key = CBitcoinSecret('
    cTkfDWqLkiws7aMuqdw1stUroLeEK2fDTuSTcLW6ztSDsDJjYQtB')
cust2_public_key = cust2_private_key.pub
cust3_private_key = CBitcoinSecret('
    cTu15Tzd5VmtkqUkF1yavUJhGPzAboADMSnqpuTTiBHTsYZiKLw6')
cust3_public_key = cust3_private_key.pub
```

2. 生成 scriptPubKey

根据要求设置 scriptPubKey 以及交易的参数，确保它正确地使用 my_public_key 来创建一个锁定脚本，这个脚本将要求提供正确的签名来解锁资金。作为“银行”，需要使用银行的公钥来生成 scriptPubKey。

本次实验使用的是 P2PKH（Pay-to-Pubkey-Hash）脚本，使用银行的公钥哈希来创建这个脚本，补充代码如下

ex2a.py（TODO 部分 scriptPubKey implementation）

```

pubkeys = [my_public_key, cust1_public_key, cust2_public_key,
    cust3_public_key]
m = 2   # 公钥的总数
n = len(pubkeys)
ex2a_txout_scriptPubKey = [
    m,  # 必需的签名数（2）
    *pubkeys,  # 所有参与者的公钥
    n,  # 公钥的总数（4）
```

```
    OP_CHECKMULTISIG  # 多签名验证操作码
]
```

3. 交易主函数

设置交易金额，txid，交易序号

ex2a.py（TODO 部分 set parameters）

```

amount_to_send = 0.000012
    txid_to_spend = (
        '01bdaf2c81d20e746a0884dec791b232189651ea530e663c65e14c8c127b2a2a')
    utxo_index = 2
```

4. 执行结果

执行 ex2a.py，输出信息:

执行 ex2a.py 输出信息

```

201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "303dff7bd8785331c1efb4596268c21733afea83caf9f7c93053cfa8a515ad97
        ",
    "addresses": [
      "miTB9DLzeZ525qcpR1qRGJAHwuKLNKFfeg",
      "zYGzbtuHWT8KxxncVtVpGRFXWJ2XSbVq2U"
    ],
    "total": 1200,
    "fees": 0,
    "size": 305,
    "vsize": 305,
    "preference": "low",
    "relayed_by": "221.238.245.19",
    "received": "2024-10-08T08:20:05.321284447Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "01
            bdaf2c81d20e746a0884dec791b232189651ea530e663c65e14c8c127b2a2a",
        "output_index": 2,
```

```
        "script": "473044022015
            ef92290b304e4b254af4106c120c2f31fdedf159bbeadbac4d43cd95acc18a022031c61ef855cd573b
            ",
        "output_value": 1200,
        "sequence": 4294967295,
        "addresses": [
          "miTB9DLzeZ525qcpR1qRGJAHwuKLNKFfeg"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2994299
      }
    ],
    "outputs": [
      {
        "value": 1200,
        "script": "52210247326
            f7ae63654235e6cb4f5d10e13fb1bc7a610dec99cb76c7be6bd9278a1fd210374d0a9468d9154b4f75
            ",
        "addresses": [
          "zYGzbtuHWT8KxxncVtVpGRFXWJ2XSbVq2U"
        ],
        "script_type": "pay-to-multi-pubkey-hash"
      }
    ]
  }
}
```


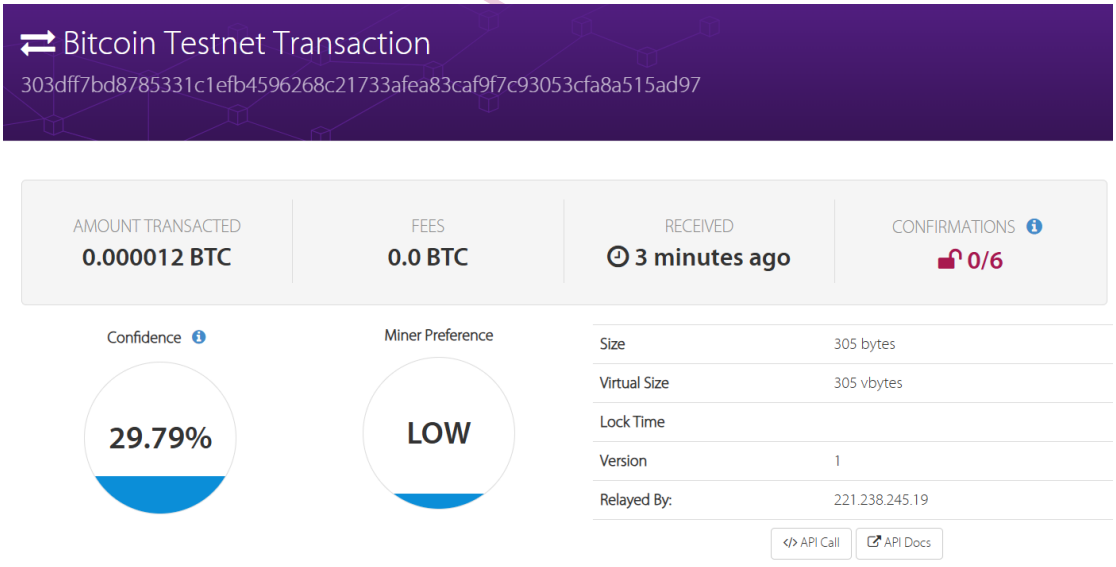

图 2: 网页交易截图

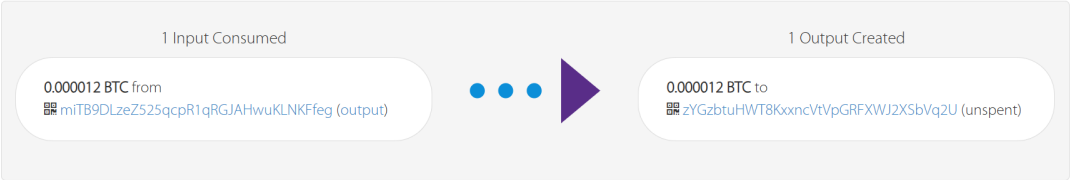

图 3: 网页交易截图

(二) ex2b.py

ex2n.py 的代码功能是发送一个从多签名（multisig）地址到普通公钥哈希（P2PKH）地址的比特币交易。

1. 实现函数

ex2n.py 的代码功能是发送一个从多签名（multisig）地址到普通公钥哈希（P2PKH）地址的比特币交易。

multisig_scriptSig 函数负责为多签交易的输入创建脚本签名（scriptSig）。它使用银行私钥和三个客户的私钥来生成对应的签名。

ex2b.py（TODO 部分）

```
1
2     # TODO: Complete this script to unlock the BTC that was locked in the
3     # multisig transaction created in Exercise 2a.
4     return [OP_0,
5             bank_sig,
6             cust1_sig]
```

2. 交易主函数

在主函数中设置参数

ex2b.py（set parameters）

```
1
2     amount_to_send = 0.000009
3     txid_to_spend =
4     '303dff7bd8785331c1efb4596268c21733afea83caf9f7c93053cfa8a515ad97'
5     utxo_index = 0
```

3. 执行结果

执行 ex2b.py 输出信息

```
1
2 201 Created
3 {
4   "tx": {
5     "block_height": -1,
```

```
    "block_index": -1,
    "hash": "00c78877f5b2d35ab260399358b9b5f1014ddce43296f5e421f8ae2adf44fc62
        ",
    "addresses": [
      "zYGzbtuHWT8KxxncVtVpGRFXWJ2XSbVq2U",
      "miTB9DLzeZ525qcpR1qRGJAHwuKLNKFfeg"
    ],
    "total": 900,
    "fees": 300,
    "size": 231,
    "vsize": 231,
    "preference": "low",
    "relayed_by": "221.238.245.19",
    "received": "2024-10-08T08:35:39.974398088Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "303
            dff7bd8785331c1efb4596268c21733afea83caf9f7c93053cfa8a515ad97",
        "output_index": 0,
        "script": "00483045022100881983
            d7f9f910494be2f52fa09616b69a34f18ec3d99115cc39632a282aae60b02203a30218fece5801c062
            ",
        "output_value": 1200,
        "sequence": 4294967295,
        "addresses": [
          "zYGzbtuHWT8KxxncVtVpGRFXWJ2XSbVq2U"
        ],
        "script_type": "pay-to-multi-pubkey-hash",
        "age": 0
      }
    ],
    "outputs": [
      {
        "value": 900,
        "script": "76a91420317028e1c9908463c1b5970f7a7a9e29220cec88ac",
        "addresses": [
          "miTB9DLzeZ525qcpR1qRGJAHwuKLNKFfeg"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}
```

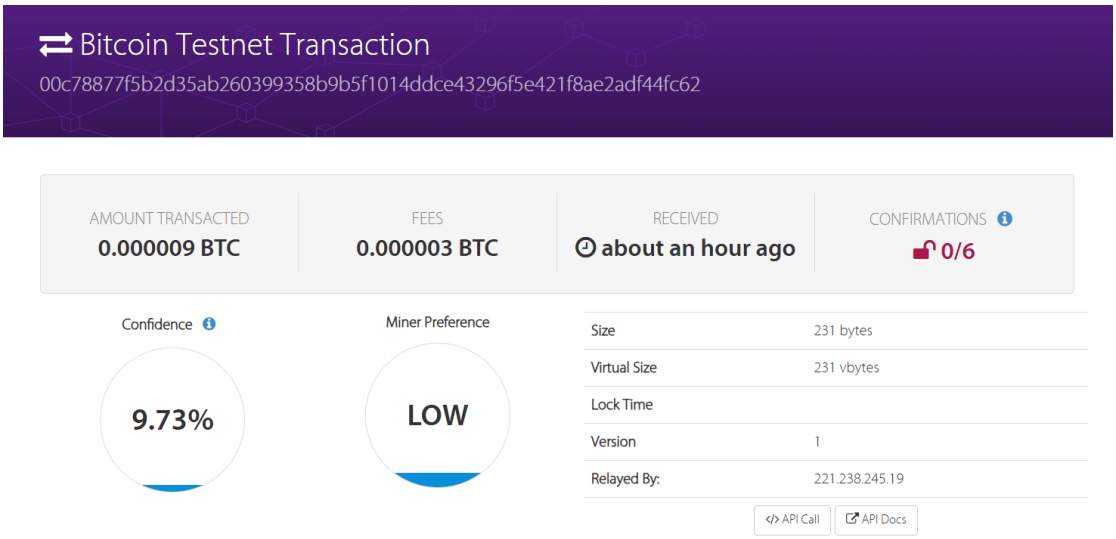

图 4: 网页截图

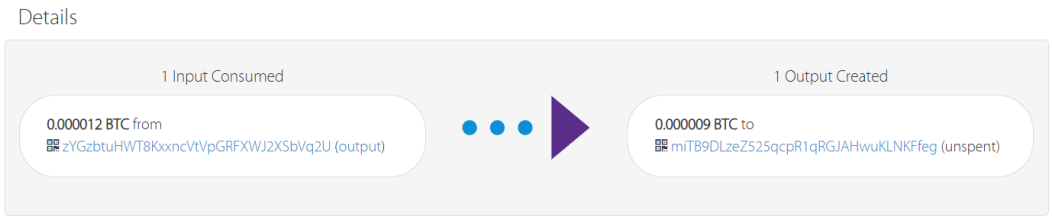

图 5: 网页截图