南开大学
Nankai University

南　　开　　大　　学

计　算　机　学　院

区块链课程实验报告

Ex3

年级：2022 级

专业：信息安全

姓名：李佳璐

2024 年 10 月 29 日

目录

一、 实验过程

(一) ex3a.py

1. 定义输出脚本

定义了一个输出脚本(scriptPubKey),用于验证一个特定的交易输出。这些操作码(opcodes)定义了在脚本执行时应进行的特定操作。

ex3a.py （Complete the scriptPubKey implementation for Exercise 3）

```
ex3a_txout_scriptPubKey = [OP_2DUP, OP_ADD, 2211, OP_EQUALVERIFY, OP_SUB,
    985, OP_EQUAL]
```

- OP_2DUP：将栈顶的两个值复制到栈顶。也就是说，如果栈顶的两个值是 a 和 b，执行后栈顶的状态将是 a, b, a, b。
- OP_ADD：将栈顶的两个项相加。栈顶两个值（比如 x 和 y）将被相加，结果会保留在栈顶。
- 2211：常量值 2211 被压入栈中。
- OP_EQUALVERIFY：比较栈顶的两个元素，如果它们相等，则移除它们并继续；如果不相等，则导致脚本失败。该操作主要用于验证。
- OP_SUB：将栈顶的两个项相减。也就是说，如果栈顶的是 x 和 y，将会计算 y - x，并把结果放回栈顶。
- 985：又一个常量值 985 被压入栈中。
- OP_EQUAL：比较栈顶的两个元素，如果相等则返回真（1），否则返回假（0）

2. 完善交易信息

ex3a.py （set these parameters correctly）

```
    amount_to_send = 0.00001
    txid_to_spend = (
        '01bdaf2c81d20e746a0884dec791b232189651ea530e663c65e14c8c127b2a2a')
    utxo_index = 3
```

3. 执行结果

ex3a.py 执行输出结果

```
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "f8be0b587d818343b189be8c63f73b958f0a3dd6f9134a71a2dde28733be00a6
        ",
```

```
    "addresses": [
      "miTB9DLzeZ525qcpR1qRGJAHwuKLNKFfeg"
    ],
    "total": 1000,
    "fees": 200,
    "size": 177,
    "vsize": 177,
    "preference": "low",
    "relayed_by": "117.131.219.51",
    "received": "2024-10-23T10:52:44.737283578Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "01
            bdaf2c81d20e746a0884dec791b232189651ea530e663c65e14c8c127b2a2a",
        "output_index": 3,
        "script": "4730440220160
            ffa7712bc8f0cd993fcc8531e01da4d9cfbad7d35e82c3771f45a99d2edab022007fcd45b62b565c33
            ",
        "output_value": 1200,
        "sequence": 4294967295,
        "addresses": [
          "miTB9DLzeZ525qcpR1qRGJAHwuKLNKFfeg"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2994299
      }
    ],
    "outputs": [
      {
        "value": 1000,
        "script": "6e9302a308889402d90387",
        "addresses": null,
        "script_type": "unknown"
      }
    ]
  }
}
```

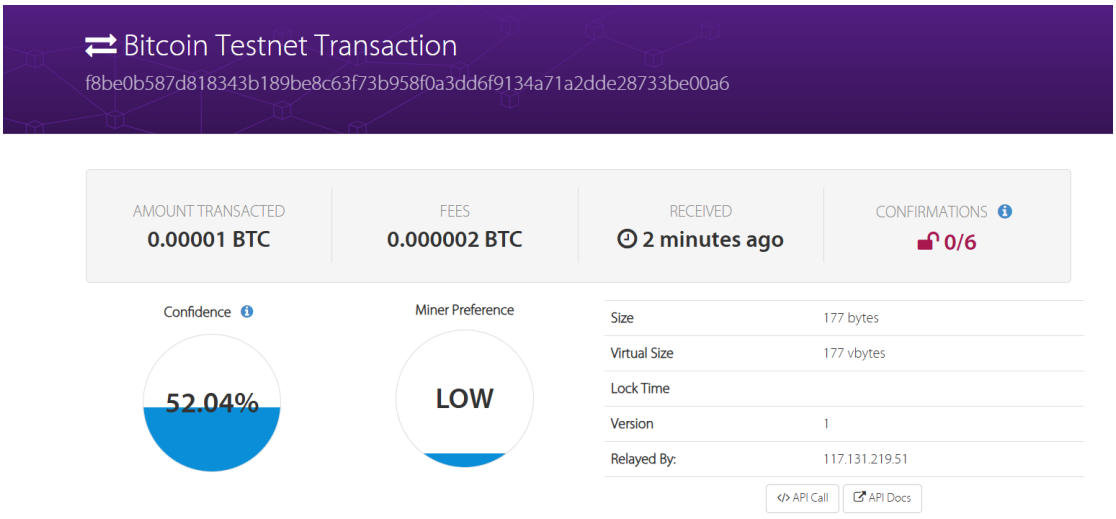

图 1: Ex3a 执行网页截图

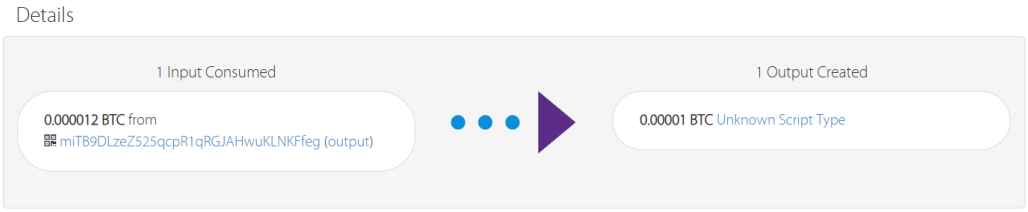

图 2: Ex3a 执行网页截图

将以上 3 个用户私钥补充进 ex2a.py

(二) ex3b.py

用于构建和发送比特币交易。它从一个未花费的交易输出（UTXO）中消费比特币，并创建一个新的交易，包含输入和输出。

1. 完善交易信息

ex3b.py （set these parameters correctly）

```
amount_to_send = 0.000009
txid_to_spend = '
    f8be0b587d818343b189be8c63f73b958f0a3dd6f9134a71a2dde28733be00a6'
utxo_index = 0
```

2. 补充解锁脚本参数

定义输入脚本（txin_scriptSig）以解锁之前的交易，使用的数学解是根据给定的方程得出的。

ex3b.py （implement the scriptSig for redeeming the transaction created）

```
# in  Exercise 3a.
# x+y=2211 & x-y=985 => x=1598,y=613
txin_scriptSig = [1598,613]
```

x 和 y 需要满足 x+y=2211 & x-y=985，经过计算可以得到 x=1598,y=613。将上面两个值作为参数传入，用作锁定脚本中的条件的数据。

3. 执行结果

ex3b.py 输出结果


```
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "eaa50da197d188e3c9b9697b69d0cc9c1d1145094c1efa25b2383d3fce3cc7e8
        ",
    "addresses": [
      "miTB9DLzeZ525qcpR1qRGJAHwuKLNKFfeg"
    ],
    "total": 900,
    "fees": 100,
    "size": 91,
    "vsize": 91,
    "preference": "low",
    "relayed_by": "221.238.245.24",
    "received": "2024-10-23T11:12:36.689410178Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "
            f8be0b587d818343b189be8c63f73b958f0a3dd6f9134a71a2dde28733be00a6"
            ,
        "output_index": 0,
        "script": "023e06026502",
        "output_value": 1000,
        "sequence": 4294967295,
        "script_type": "unknown",
        "age": 0
      }
    ],
    "outputs": [
      {
        "value": 900,
```

```
        "script": "76a91420317028e1c9908463c1b5970f7a7a9e29220cec88ac",
        "addresses": [
          "miTB9DLzeZ525qcpR1qRGJAHwuKLNKFfeg"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}
```

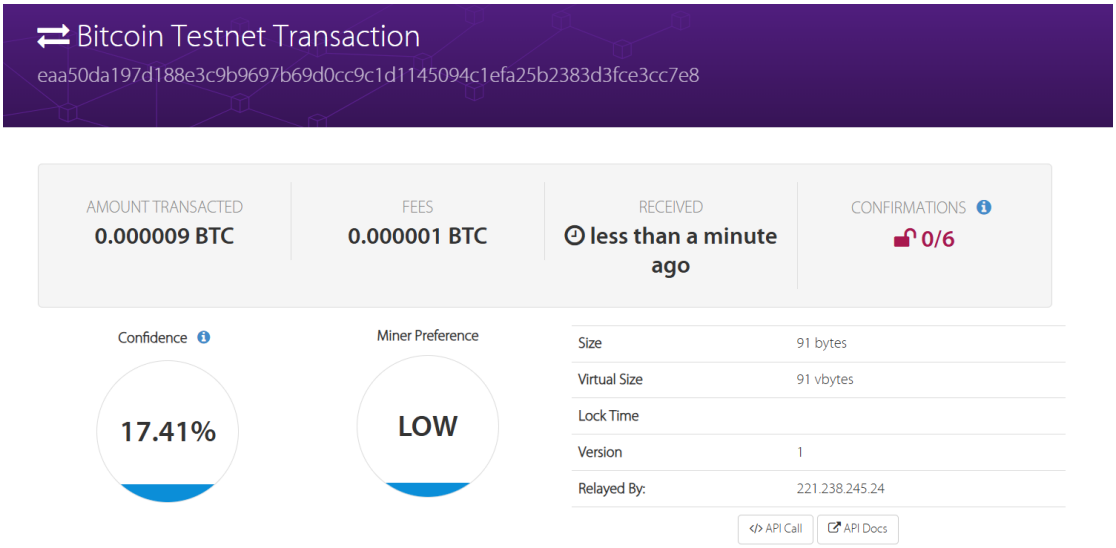

图 3: Ex3b 执行网页截图

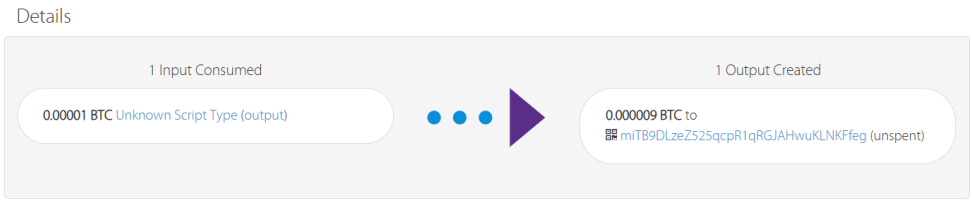

图 4: Ex3b 执行网页截图