区块链实验三报告

姓名：齐明杰　学号：2113997 班级：信安2班

1　实验目的

- 生成可通过以下两个线性方程组的解（x，y）赎回的交易：

$x + y =$（$StudentID$前3位）和 $x - y =$（$StudentID$后4位）

[为确保存在整数解，请必要时调整（顺序减 1）你的 StudentID 后 4 位，使 StudentID 前 3 位和 StudentID 后 4 位奇偶性相同]。

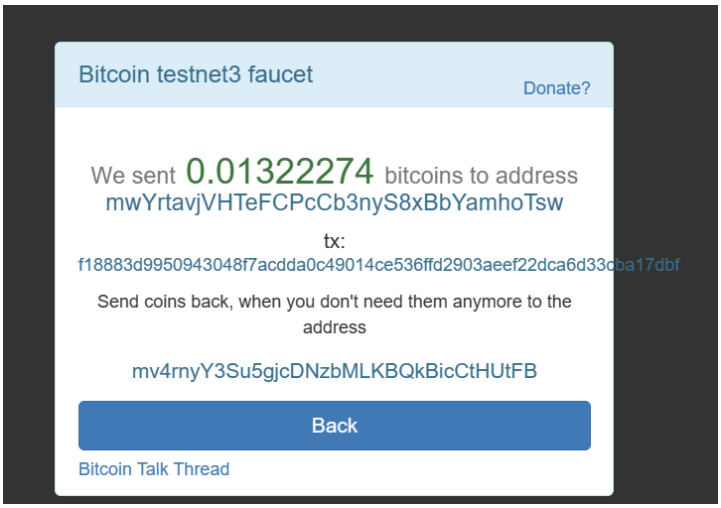
- 赎回交易。赎回脚本应尽可能小。也就是说，一个有效的 `scriptSig` 应该是简单地将两个整

数 x 和 y 发送到堆栈中。确保在 `scriptPubKey` 中使用了 `OP_ADD` 和 `OP_SUB`。

2　实验过程

2.1　领取比特币

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



2.2　生成交易

我们需要编写一个脚本，修改代码如下：

```
ex3a_txout_scriptPubKey = [
    OP_2DUP,
    OP_ADD,
    211,
    OP_EQUALVERIFY,
    OP_SUB,
    3997,
    OP_EQUAL
]

amount_to_send = 0.001
txid_to_spend =
('f18883d9950943048f7acdda0c49014ce536ffd2903aeef22dca6d33cba17dbf')
utxo_index = 1
```

用了以下操作码：

1. `OP_2DUP`：
   - **功能**：复制堆栈的顶部两个值。
2. `OP_ADD`：
   - **功能**：弹出堆栈的顶部两个值，相加，并将结果推入堆栈。
3. `OP_EQUALVERIFY`：
   - **功能**：检查堆栈的顶部两个值是否相等。如果它们相等，它们都会被弹出；如果不等，脚本执行失败。
4. `OP_SUB`：
   - **功能**：弹出堆栈的顶部两个值，并从第二个值中减去第一个值，然后将结果推入堆栈。
5. `OP_EQUAL`：
   - **功能**：检查堆栈的顶部两个值是否相等。如果它们相等，堆栈顶部为 TRUE；否则，为 FALSE。

脚本运行时堆栈的变化如下：

初始堆栈：x, y

1. `OP_2DUP`：复制堆栈的顶部两个值。
   - 堆栈：x, y, x, y
2. `OP_ADD`：弹出堆栈的顶部两个值并将它们相加，然后将结果推到堆栈的顶部。

- 堆栈：$x, y, x + y$

3. 推送数字 211 到堆栈。
   - 堆栈：$x, y, x + y, 211$
4. `OP_EQUALVERIFY`：检查堆栈的顶部两个值是否相等。如果它们相等，它们都会被弹出；如果不等，脚本执行失败。
   - 堆栈：x, y
5. `OP_SUB`：弹出堆栈的顶部两个值并减去它们，然后将结果推到堆栈的顶部。
   - 堆栈：$x - y$
6. 推送数字 3997 到堆栈。
   - 堆栈：$x - y, 3997$
7. `OP_EQUAL`：检查堆栈的顶部两个值是否相等。如果它们相等，堆栈顶部为 TRUE；否则，为 FALSE。
   - 堆栈：$TRUE$ (如果 $x - y$ 等于 3997)

     或
   - 堆栈：$FALSE$ (如果 $x - y$ 不等于 3997)

如果堆栈的顶部值为 TRUE，则脚本成功执行。如果为 FALSE 或脚本在执行过程中失败，则脚本执行失败。

2.3 赎回事务

手动求解以下方程组：

$$x + y = 211$$
$$x - y = 3997$$

得到解：

$$x = 2104$$
$$y = -1893$$

因此解锁脚本为：

```
txin_scriptSig = [2104, -1893]

amount_to_send = 0.0005
txid_to_spend =
'aca1ab96912e4cb3f2bf11131dafeb37a04a64c4bc0dbbcba5ff6a8a1c2a839c'
utxo_index = 0
```

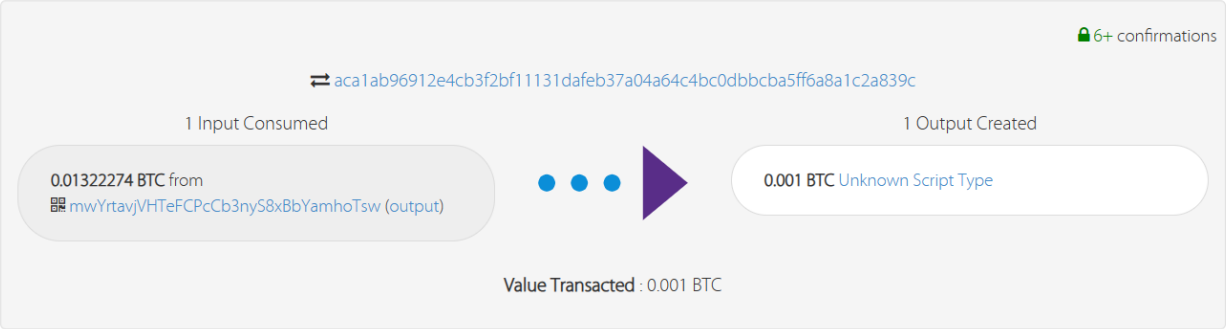
3 实验结果

运行`ex3a.py`，返回结果如下：


```
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
"aca1ab96912e4cb3f2bf11131dafeb37a04a64c4bc0dbbcba5ff6a8a1c2a839c",
    "addresses": [
      "mwYrtavjVHTeFCPcCb3nyS8xBbYamhoTsw"
    ],
    "total": 100000,
    "fees": 1222274,
    "size": 178,
    "vsize": 178,
    "preference": "high",
    "relayed_by": "172.233.65.43",
    "received": "2023-10-16T07:08:52.923318023Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"f18883d9950943048f7acdda0c49014ce536ffd2903aeef22dca6d33cba17dbf",
        "output_index": 1,
        "script":
"483045022100f6a4881af31687e9242c158974302a3126aaab16d5905548847bc77b3d48c
74602203f03eb180e5f0b71db297a98d91b4e73bc75b0ae2bdd09818978bee1550b6106012
10375d247242cd16dba7845abd1074dcb13b0ed20744a03e8c9b4db4ed11ec727f2",
        "output_value": 1322274,
        "sequence": 4294967295,
        "addresses": [
          "mwYrtavjVHTeFCPcCb3nyS8xBbYamhoTsw"
```

```
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2533342
      }
    ],
    "outputs": [
      {
        "value": 100000,
        "script": "6e9302d3008894029d0f87",
        "addresses": null,
        "script_type": "unknown"
      }
    ]
  }
}
```

网站显示如下：



运行`ex3b.py`，返回结果如下：：

```
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
"9efae9939bb4f37b876c728495c925208cc79854037b7acb9a3d5dccacb64a5c",
    "addresses": [
      "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"
    ],
    "total": 50000,
    "fees": 50000,
    "size": 91,
    "vsize": 91,
    "preference": "high",
    "relayed_by": "172.233.65.43",
    "received": "2023-10-16T07:09:29.358582398Z",
    "ver": 1,
```

```
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"aca1ab96912e4cb3f2bf11131dafeb37a04a64c4bc0dbbcba5ff6a8a1c2a839c",
        "output_index": 0,
        "script": "023808026587",
        "output_value": 100000,
        "sequence": 4294967295,
        "script_type": "unknown",
        "age": 0
      }
    ],
    "outputs": [
      {
        "value": 50000,
        "script": "76a9149f9a7abd600c0caa03983a77c8c3df8e062cb2fa88ac",
        "addresses": [
          "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}
```


网站结果如下：