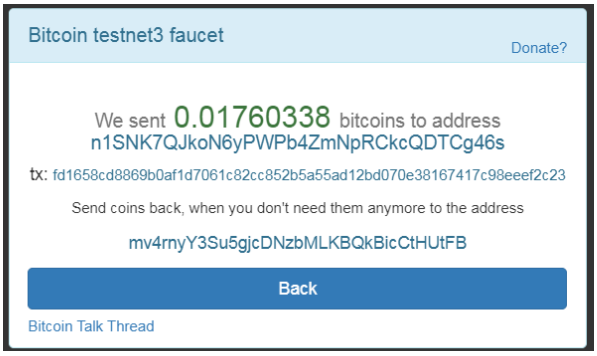
区块链实验二报告

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：



Bitcoin testnet3 faucet

We sent 0.01760338 bitcoins to address n1SNK7QJkoN6yPWPb4ZmNpRCkcQDTCg46s

tx: fd1658cd8869b0af1d7061c82cc852b5a55ad12bd070e38167417c98eeef2c23

Send coins back, when you don't need them anymore to the address

mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB

2　生成客户私钥

运行`keygen.py`三次，生成三个客户的**私钥**：

```
Private key: cTPX3uER5NCBuaSa7uGmmiTkwmaaNoxUsb7Jqmeypgh1vgWRJSYB
Address: mwYrtavjVHTeFCPcCb3nyS8xBbYamhoTsw

Private key: cVMmWt9SHKs7AK2RX4Zkh3kcUDM5vZ5Rbw1V4gTrKTA8yY8vhZQ8
Address: mfaknPc16CqXqZiGXhyTUAmXxRsXfDHtu5

Private key: cSw8pzk5EXxLh7q4FRborXnfaAJPqrLQv99b9G8LxqjRvP25VDHr
Address: n36uuqtyA1ty9zVEYBakFFvhNGy4RYL8jY
```

并分别填入`ex2a.py`的private_key中：

```
cust1_private_key = CBitcoinSecret(
    'cTPX3uER5NCBuaSa7uGmmiTkwmaaNoxUsb7Jqmeypgh1vgWRJSYB')
cust1_public_key = cust1_private_key.pub
cust2_private_key = CBitcoinSecret(
    'cVMmWt9SHKs7AK2RX4Zkh3kcUDM5vZ5Rbw1V4gTrKTA8yY8vhZQ8')
cust2_public_key = cust2_private_key.pub
cust3_private_key = CBitcoinSecret(
    'cSw8pzk5EXxLh7q4FRborXnfaAJPqrLQv99b9G8LxqjRvP25VDHr')
cust3_public_key = cust3_private_key.pub
```

3 生成一个涉及四方的多签名交易

对于一个M-N的多重签名交易锁定脚本，其格式如下：

```
OP_M
<public_key_1>
<public_key_2>
...
<public_key_N>
OP_N
OP_CHECKMULTISIG
```

其中：

- `OP_M` 是一个操作码，表示至少需要 M 个签名才能解锁交易。
- `<public_key_1>`, `<public_key_2>`, ..., `<public_key_N>` 是参与多重签名的公钥，通常是 N 个公钥中的一部分。
- `OP_N` 是一个操作码，表示总共有 N 个公钥。
- `OP_CHECKMULTISIG` 是多重签名检查的操作码，用于验证签名是否有效。

我们不妨令只需要三人中一**个人**的签名即可锁定交易，补充ex2a.py:

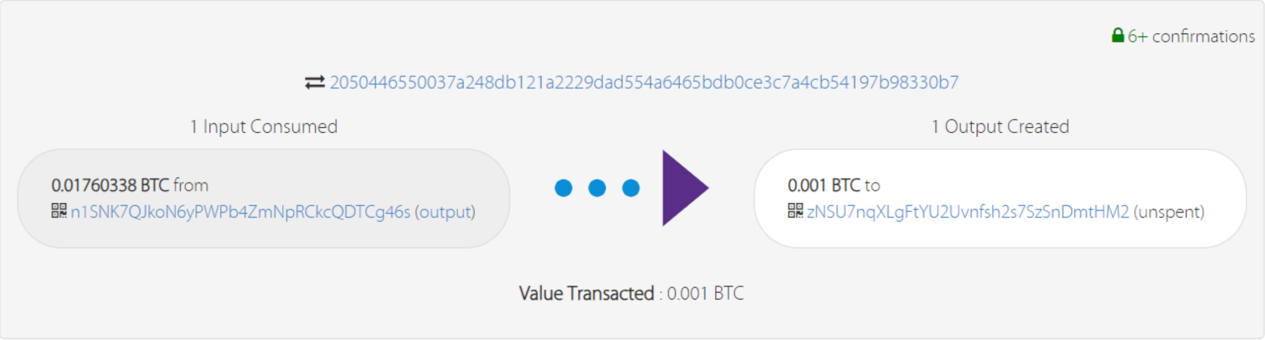
```
ex2a_txout_scriptPubKey = [
    my_public_key,  # 银行的公钥
    OP_CHECKSIGVERIFY,
    OP_1,  # 数字1
    cust1_public_key,  # 第一个客户的公钥
    cust2_public_key,  # 第二个客户的公钥
    cust3_public_key,  # 第三个客户的公钥
    OP_3,  # 数字3
    OP_CHECKMULTISIG  # 多重签名检查
]
...
amount_to_send = 0.001
txid_to_spend = (
   'fd1658cd8869b0af1d7061c82cc852b5a55ad12bd070e38167417c98eeef2c23'
)
utxo_index = 1
```

运行`ex2a.py`，返回结果如下：

```
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "2050446550037a248db121a2229dad554a6465bdb0ce3c7a4cb54197b98330b7",
    "addresses": [
      "n1SNK7QJkoN6yPWPb4ZmNpRCkcQDTCg46s",
      "zNSU7nqXLgFtYU2Uvnfsh2s7SzSnDmtHM2"
    ],
    "total": 100000,
    "fees": 1660338,
    "size": 306,
    "vsize": 306,
    "preference": "high",
    "relayed_by": "172.104.103.203",
    "received": "2023-10-07T00:54:03.134722495Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "fd1658cd8869b0af1d7061c82cc852b5a55ad12bd070e38167417c98eeef2c23",
        "output_index": 1,
        "script": "473044022068581 75e92af34ae6e58bfe8fb5585e0ae7b5472f6474827a931e547555ece1802202247ef1ee89d936ae4fefae2d529a7954ca372269e04d2b38f6e58397e0026c3012103389c39b1635b32119096ce8020862ae2d98bde073572af3201de77ce3ab90553",
        "output_value": 1760338,
        "sequence": 4294967295,
        "addresses": [
          "n1SNK7QJkoN6yPWPb4ZmNpRCkcQDTCg46s"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2530772
      }
    ],
    "outputs": [
      {
        "value": 100000,
        "script": "2103389c39b1635b32119096ce8020862ae2d98bde073572af3201de77ce3ab90553ad51210375d247242cd16dba7845abd1074dcb13b0ed20744a03e8c9b4db4ed11ec727f22102b1519ff9ef12251dbaec8411c78dd9f3cb547bd93545d98e8325fff7c99ea8ff2102c6f664e49b7b0bb27435a50b57bd85e2e859c40aec3cfbaec63134cd680831b153ae",
        "addresses": [
          "zNSU7nqXLgFtYU2Uvnfsh2s7SzSnDmtHM2"
        ],
        "script_type": "pay-to-multi-pubkey-hash"
      }
    ]
  }
}
```

可以看到生成了一个新的账户`zNSU7nqXLgFtYU2Uvnfsh2s7SzSnDmtHM2`，供三个账户维护。

网站显示如下：



6+ confirmations

⇄ 2050446550037a248db121a2229dad554a6465bdb0ce3c7a4cb54197b98330b7

1 Input Consumed

0.01760338 BTC from
n1SNK7QJkoN6yPWPb4ZmNpRCkcQDTCg46s (output)

1 Output Created

0.001 BTC to
zNSU7nqXLgFtYU2Uvnfsh2s7SzSnDmtHM2 (unspent)

Value Transacted : 0.001 BTC

4 赎回事务

补充ex2b.py如下：

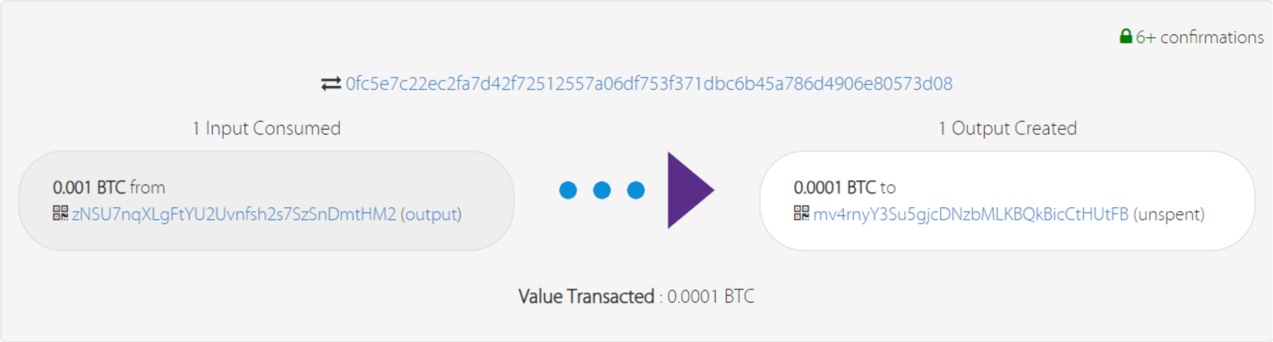
```
def multisig_scriptSig(txin, txout, txin_scriptPubKey):
    bank_sig = create_OP_CHECKSIG_signature(txin, txout, txin_scriptPubKey,
                                             my_private_key)
    cust1_sig = create_OP_CHECKSIG_signature(txin, txout, txin_scriptPubKey,
                                             cust1_private_key)
    cust2_sig = create_OP_CHECKSIG_signature(txin, txout, txin_scriptPubKey,
                                             cust2_private_key)
    cust3_sig = create_OP_CHECKSIG_signature(txin, txout, txin_scriptPubKey,
                                             cust3_private_key)
    ######################################################################
    # TODO: Complete this script to unlock the BTC that was locked in the
    # multisig transaction created in Exercise 2a.
    scriptSig = [OP_0, cust3_sig, bank_sig]
    return scriptSig
    ######################################################################


amount_to_send = 0.0001
```

```
txid_to_spend ='2050446550037a248db121a2229dad554a6465bdb0ce3c7a4cb54197b98330b7'
utxo_index = 0
```

运行结果：

```
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "0fc5e7c22ec2fa7d42f72512557a06df753f371dbc6b45a786d4906e80573d08",
    "addresses": [
      "zNSU7nqXLgFtYU2Uvnfsh2s7SzSnDmtHM2",
      "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"
    ],
    "total": 10000,
    "fees": 90000,
    "size": 231,
    "vsize": 231,
    "preference": "high",
    "relayed_by": "172.104.103.203",
    "received": "2023-10-07T01:11:57.000030986Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "2050446550037a248db121a2229dad554a6465bdb0ce3c7a4cb54197b98330b7",
        "output_index": 0,
        "script": "00483045022100f75dab12c26c5cd800300edb7f59bb01513ca7d08e1d9d2f99d6f34086f6dd5a02205432e43d85038cb854740a8e609e252b373023a6e4e1841be73ed632eb0bf904014730440220681fec1368ef2cb6fcbe70c7835c388ebd65ab8ba5433f6965c7df016f9eb58d0220325478cf35ad4c5c1786133eb6e0df7a21aa939fbc3950454d7b54498e2a0a1b01",
        "output_value": 100000,
        "sequence": 4294967295,
        "addresses": [
          "zNSU7nqXLgFtYU2Uvnfsh2s7SzSnDmtHM2"
        ],
        "script_type": "pay-to-multi-pubkey-hash",
        "age": 2530778
      }
    ],
    "outputs": [
      {
        "value": 10000,
        "script": "76a9149f9a7abd600c0caa03983a77c8c3df8e062cb2fa88ac",
        "addresses": [
          "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}
```

网站结果如下：



🔒 6+ confirmations

⇄ 0fc5e7c22ec2fa7d42f72512557a06df753f371dbc6b45a786d4906e80573d08

1 Input Consumed

0.001 BTC from
zNSU7nqXLgFtYU2Uvnfsh2s7SzSnDmtHM2 (output)

1 Output Created

0.0001 BTC to
mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB (unspent)

Value Transacted : 0.0001 BTC