第二次实验报告

2111460 张洋

一、练习（a）

1. 打开 keygen.py 文件，创建三个新账户。

```
用户 1：
Private key: cPbgYuEDMmnRgqXB3YH1qYmhUttXBqoiyKTg7C2WQDv6tTCkNr55
Address: mwY6s2Xgu5LRuvbpqpPeBJT4B7g6Ttg63F
用户 2：
Private key: cTdj36ujHi1JofzsXqxybuWjMqfXNdwzwkdVfZmz9aQ2vcbZpJzG
Address: mzZbS7HZQnFWhYUknBjKEeEC49RXWSZudA
用户 3：
Private key: cUWJj9wL85ewVbynWSKFoxv2d7Ym7cUG2ghsNzTdheduno5tNiF9
Address: n3ktDn8yvhYzKDnsqibrDzzVQJ1Gh9UUZo
```

2. 将三个账户的私钥填写到 ex2a.py 文件中。

```
cust1_private_key = CBitcoinSecret(
    'cPbgYuEDMmnRgqXB3YH1qYmhUttXBqoiyKTg7C2WQDv6tTCkNr55')
cust1_public_key = cust1_private_key.pub
cust2_private_key = CBitcoinSecret(
    'cTdj36ujHi1JofzsXqxybuWjMqfXNdwzwkdVfZmz9aQ2vcbZpJzG')
cust2_public_key = cust2_private_key.pub
cust3_private_key = CBitcoinSecret(
    'cUWJj9wL85ewVbynWSKFoxv2d7Ym7cUG2ghsNzTdheduno5tNiF9')
cust3_public_key = cust3_private_key.pub
```

3. 补全代码，创建多重签名脚本，完成多签名交易的要求。

```
# 定义所需的签名数量
required_signatures = 3
# 创建包含cust1、cust2和cust3公钥的列表
pubkeys = [cust1_public_key, cust2_public_key, cust3_public_key]
# 创建多重签名脚本
ex2a_txout_scriptPubKey = CScript([required_signatures] + pubkeys + [len(pubkeys), OP_CHECKMULTISIG])
```

4. 填写交易信息。

```
amount_to_send = 0.0008
txid_to_spend = (
    'c26d91f819ba03038c8936c56830a3996448cfd7dad7a67243ea8e5b95b799eb')
utxo_index = 2
```

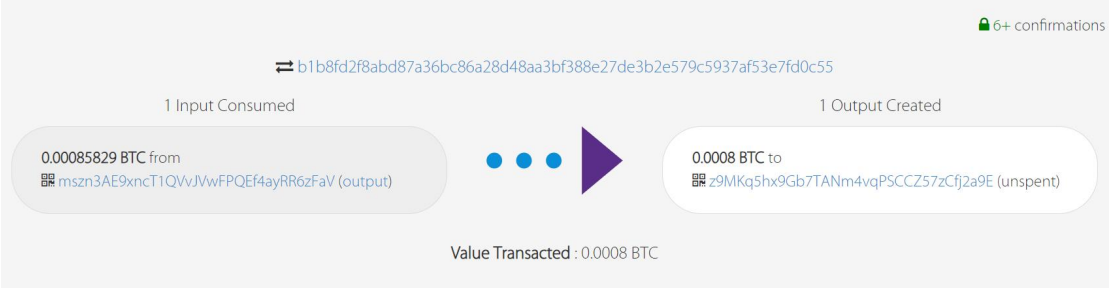
5. 输出信息

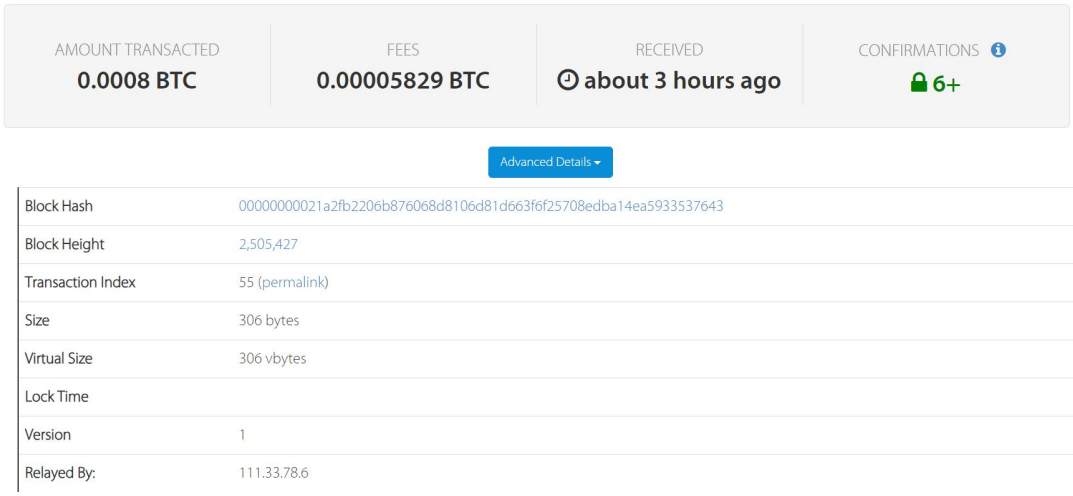
```
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
"b1b8fd2f8abd87a36bc86a28d48aa3bf388e27de3b2e579c5937af53e7fd0c55",
```

```
    "addresses": [
      "mszn3AE9xncT1QVvJVwFPQEf4ayRR6zFaV",
      "z9MKq5hx9Gb7TANm4vqPSCCZ57zCfj2a9E"
    ],
    "total": 80000,
    "fees": 5829,
    "size": 306,
    "vsize": 306,
    "preference": "low",
    "relayed_by": "111.33.78.6",
    "received": "2023-09-27T11:00:04.712096948Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"c26d91f819ba03038c8936c56830a3996448cfd7dad7a67243ea8e5b95b799eb",
        "output_index": 2,
        "script":
"473044022060460 93e84b238f8a1d964060200cadf24c3da77626ad31a013bbff40103d
ff302202a91a80a18a3838a5f31147d3f8147633453ae83050cdb7aebc23173e26cf7e60
12103890bcd555dc24ebd465daf9c024e062123632b6fc9651f3cf98ef06deaeb4544",
        "output_value": 85829,
        "sequence": 4294967295,
        "addresses": [
          "mszn3AE9xncT1QVvJVwFPQEf4ayRR6zFaV"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2477601
      }
    ],
    "outputs": [
      {
        "value": 80000,
        "script":
"2103890bcd555dc24ebd465daf9c024e062123632b6fc9651f3cf98ef06deaeb4544ad5
12102007da8ac9b66d67ff7385abc06b1323356e3a3bb52f95d0a617d374e0cf587d6210
27d3425b5e808ffeadc4228e9f00592e7283bcd1f6a6c57c0cd67090526c451802103dff
6557479ec77c372dae52dcfec1be58907066a5d49d9add4dc034e510904ec53ae",
        "addresses": [
          "z9MKq5hx9Gb7TANm4vqPSCCZ57zCfj2a9E"
```

```
        ],
        "script_type": "pay-to-multi-pubkey-hash"
      }
    ]
  }
}
```

6. 截图





二、练习（b）

1. 补全多重签名脚本的解锁脚本函数。使用银行私钥和三个客户的私钥来生成签名。然后，它将这些签名与操作码 OP_0 一起返回，以构建多重签名的解锁脚本。

```
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.
    return [OP_0,
    cust1_sig,
    bank_sig]
    ##########################################################################
```

2. 填写交易信息

```
amount_to_send = 0.0004
txid_to_spend = 'b1b8fd2f8abd87a36bc86a28d48aa3bf388e27de3b2e579c5937af53e7fd0c55'
utxo_index = 0
```

3. 输出信息


```
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
"e10a6ccf57672c77ba11847572d9ad27a64cd37a7b3be01773b2036faf299317",
    "addresses": [
      "z9MKq5hx9Gb7TANm4vqPSCCZ57zCfj2a9E",
      "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"
    ],
    "total": 40000,
    "fees": 40000,
    "size": 232,
    "vsize": 232,
    "preference": "high",
    "relayed_by": "111.33.78.5",
    "confirmed": "2023-09-27T14:43:17Z",
    "received": "2023-09-27T14:25:53.587Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 3,
    "confidence": 1,
    "inputs": [
        {
        "prev_hash":
"b1b8fd2f8abd87a36bc86a28d48aa3bf388e27de3b2e579c5937af53e7fd0c55",
        "output_index": 0,
        "script":
"00483045022100bf77a8eb82c71b0fd0fb5d84b6d9e32528b3f7ae0d8bc8b3061047559
1147ab90220383ed795d5610a0756d755ab3c072b129fa150bc28e75d30c9a78c36500c5
534014830450221 00b5204a6ceb8aca7c999e7820a10300d6bcb25bab78a66e979cb5105
eb7afbc7d022064e1632369b80a2d6541037c492d171164ccf5b32c7a3c9ffab6664de2c
d471e01",
        "output_value": 80000,
        "sequence": 4294967295,
        "addresses": [
```

```
            "z9MKq5hx9Gb7TANm4vqPSCCZ57zCfj2a9E"
        ],
        "script_type": "pay-to-multi-pubkey-hash",
        "age": 2505427
        }
    ],
    "outputs": [
        {
        "value": 40000,
        "script": "76a9149f9a7abd600c0caa03983a77c8c3df8e062cb2fa88ac",
        "addresses": [
            "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"
        ],
        "script_type": "pay-to-pubkey-hash"
        }
    ]
  }
}
```


4. 截图