区块链基础及应用 LAB2

- 姓名：卢麒萱
- 学号：2010519

代码重点

`ex2a.py` 中，首先用 `keygen` 生成三组公私钥对：

```
cust1_private_key = CBitcoinSecret(
    'cTqV2yaBVwNBx5CiV4dqJBiPT2TMW43vThWxwNVXA744Wu9BLwm3')
cust1_public_key = cust1_private_key.pub
cust2_private_key = CBitcoinSecret(
    'cUkL5HBxHHqjeo1TjPCz3EB1yfUEnmrvMKi18HLeVxuDsV7L5NeY')
cust2_public_key = cust2_private_key.pub
cust3_private_key = CBitcoinSecret(
    'cMsRq4v1YfDv7qyZvashTUYJXoyyQrWy9jGDeQJoDvzefCEBEKQd')
cust3_public_key = cust3_private_key.pub
```

解锁脚本：

```
ex2a_txout_scriptPubKey = [my_public_key, OP_CHECKSIGVERIFY, OP_1,
cust1_public_key, cust2_public_key, cust3_public_key, OP_3, OP_CHECKMULTISIG]
```

设置要花费 bitcoin 的区块：

```
amount_to_send = 0.0015
txid_to_spend = (
    '16cdf1751652cd0c099ea31a6bc016043b27e159a83e6ad19e1a86b2f39a9449')
utxo_index = 0
```

是 `ex1` 中分币出的第一个块。

运行 `ex2a` 输出：

```
┌─root at DESKTOP-IKOECBQ in ~/src/blockchain/ex2 22-10-25 - 20:32:35
└─○ /bin/python3 /root/src/blockchain/ex2/ex2a.py
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
"5445dfa34f41b10462e78ff16676f5db3cb3d6dda17026ee31f02b6fa3b57929",
    "addresses": [
      "mkne3KArh5DWkWoRiYFfQmh4MWhrTiNubf",
      "zG4gtCADYH8jHVPJCfdbv5CSQezig1yZoj"
    ],
    "total": 150000,
    "fees": 10000,
    "size": 307,
    "vsize": 307,
```

```
    "preference": "low",
    "relayed_by": "103.172.41.206",
    "received": "2022-10-25T12:33:13.530328767Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"16cdf1751652cd0c099ea31a6bc016043b27e159a83e6ad19e1a86b2f39a9449",
        "output_index": 0,
        "script":
"483045022100a43ddbd2e4f7b99c5e2379e290a5e256466973b6c12040030df506d64e700fe
d02206d099197b0217aa47157946b8e686ab0fd89137b1cd81ee026a64279f43cf8c20121032
dd5771a470b7a3f4428d7c096f63cc41974221aca801c97add36f8ecd51df4a",
        "output_value": 160000,
        "sequence": 4294967295,
        "addresses": [
          "mkne3KArh5DWkWoRiYFfQmh4MWhrTiNubf"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2349446
      }
    ],
    "outputs": [
      {
        "value": 150000,
        "script":
"21032dd5771a470b7a3f4428d7c096f63cc41974221aca801c97add36f8ecd51df4aad51210
27d74835583210521195b9339f7cde09eee18ac1c57602b326f2e1b37564ab8622103e7444ed
761e99d01153b213037eb2c5790f1cee686a20affd923e12c13ff786a2103145e336ac56fbf7
4d77094e204a589320bc017e4d8d6232a33dd739950cfd26b53ae",
        "addresses": [
          "zG4gtCADYH8jHVPJCfdbv5CSQezig1yZoj"
        ],
        "script_type": "pay-to-multi-pubkey-hash"
      }
    ]
  }
}
```


`ex2b.py` 中，**加锁脚本：**

```
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]
```

`ex2b`中的脚本先入栈，`ex2a`的脚本后入栈，总入栈顺序为`[OP_0, cust1_sig, bank_sig, my_public_key, OP_CHECKSIGVERIFY, OP_1, cust1_public_key, cust2_public_key, cust3_public_key, OP_3, OP_CHECKMULTISIG]`。

`OP_CHECKSIGVERIFY`检查`bank_sig`和`my_public_key`以验证银行身份。`cust3_sig`的位置可以是`cust1_sig`、`cust2_sig`、`cust3_sig`中的任意一个，`OP_CHECKMULTISIG`实现了3选1的验证身份。

设置要花费 bitcoin 的区块：

```
amount_to_send = 0.0014
txid_to_spend =
    '5445dfa34f41b10462e78ff16676f5db3cb3d6dda17026ee31f02b6fa3b57929'
utxo_index = 0
```

花费的是`ex2a`输出中新创建的区块。

交易信息：