区块链基础及应用 LAB3

- 姓名：卢麒萱
- 学号：2010519

代码重点

`ex3a.py`中:

解锁脚本:

```
ex3a_txout_scriptPubKey = [OP_2DUP,OP_ADD,2010,OP_EQUALVERIFY,OP_SUB,520,OP_EQUAL]
```

将栈中两个元素复制相加后与`2010`比较，相减后与`520`比较，若相等则解锁成功。

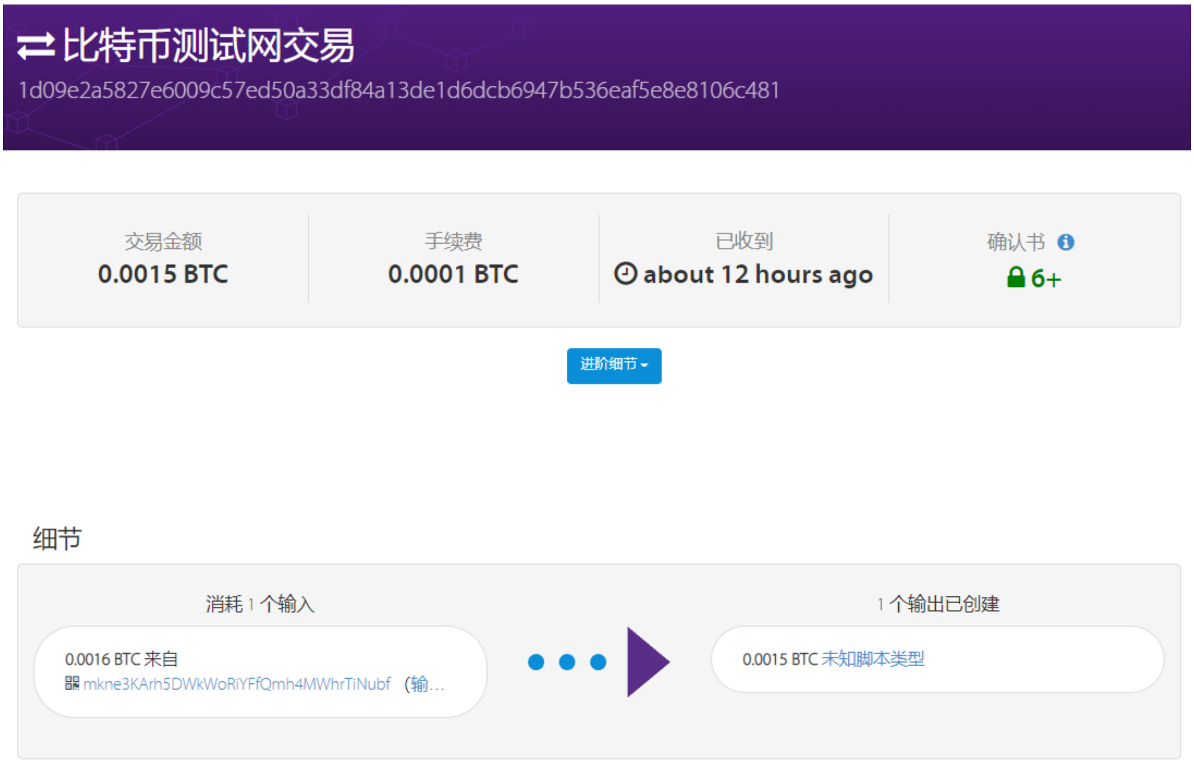
设置要花费 bitcoin 的区块:

```
amount_to_send = 0.0015
txid_to_spend = (
    '16cdf1751652cd0c099ea31a6bc016043b27e159a83e6ad19e1a86b2f39a9449')
utxo_index = 2
```

是`ex1`中分币出的第三个块。

运行`ex3a`输出:

```
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash": "1d09e2a5827e6009c57ed50a33df84a13de1d6dcb6947b536eaf5e8e8106c481",
    "addresses": [
      "mkne3KArh5DWkWoRiYFfQmh4MWhrTiNubf"
    ],
    "total": 150000,
    "fees": 10000,
    "size": 177,
    "vsize": 177,
    "preference": "low",
    "relayed_by": "2a01:4f8:202:1002:1111:1111:28e0:1",
    "received": "2022-11-12T15:10:32.196609227Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash": "16cdf1751652cd0c099ea31a6bc016043b27e159a83e6ad19e1a86b2f39a9449",
        "output_index": 2,
        "script": "47304402201560aaadcad5b5c75d3f1993c7e435b28237d3e5bba0e686c31f62ae79ec703d0220550f5778eecca6b1a626a3b4bf6b03107da5344c1692888a2f7e123a88dd41350121032dd5771a470b7a3f4428d7c096f63cc41974221aca801c97add36f8ecd51df4a",
        "output_value": 160000,
        "sequence": 4294967295,
        "addresses": [
          "mkne3KArh5DWkWoRiYFfQmh4MWhrTiNubf"
        ],
        "script_type": "pay-to-pubkey-hash",
        "age": 2349446
      }
    ],
    "outputs": [
      {
        "value": 150000,
        "script": "6e9302da07889402080287",
        "addresses": null,
        "script_type": "unknown"
      }
    ]
  }
}
```



⇄ 比特币测试网交易

1d09e2a5827e6009c57ed50a33df84a13de1d6dcb6947b536eaf5e8e8106c481

交易金额	手续费	已收到	确认书
0.0015 BTC	0.0001 BTC	about 12 hours ago	6+

细节

消耗 1 个输入

0.0016 BTC 来自
mkne3KArh5DWkWoRiYFfQmh4MWhrTiNubf （输…

1 个输出已创建

0.0015 BTC 未知脚本类型

`ex2b.py`中，**加锁脚本：**

```
txin_scriptSig = [1265,745]
```

将方程正确解压入栈中。

设置要花费 bitcoin 的区块：

```
amount_to_send = 0.0014
txid_to_spend =
'1d09e2a5827e6009c57ed50a33df84a13de1d6dcb6947b536eaf5e8e8106c481'
utxo_index = 0
```

是`ex3a`中新产生的块。

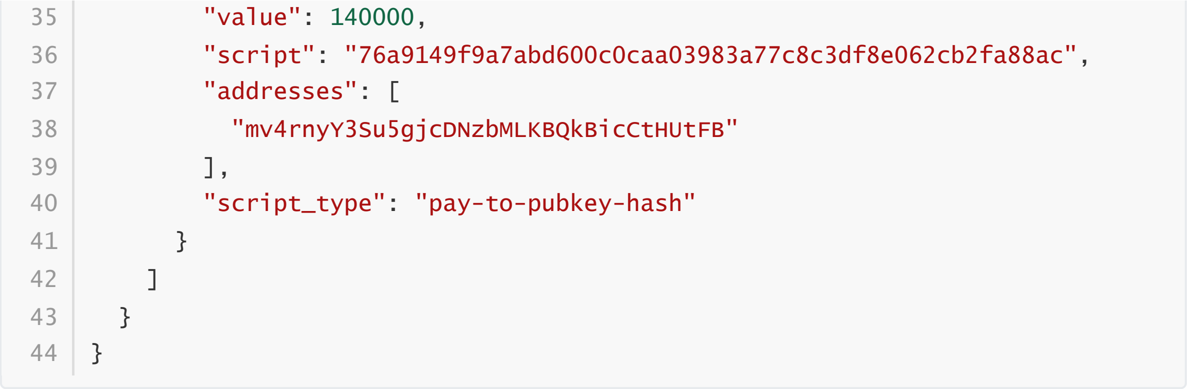
运行`ex3b`输出：

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

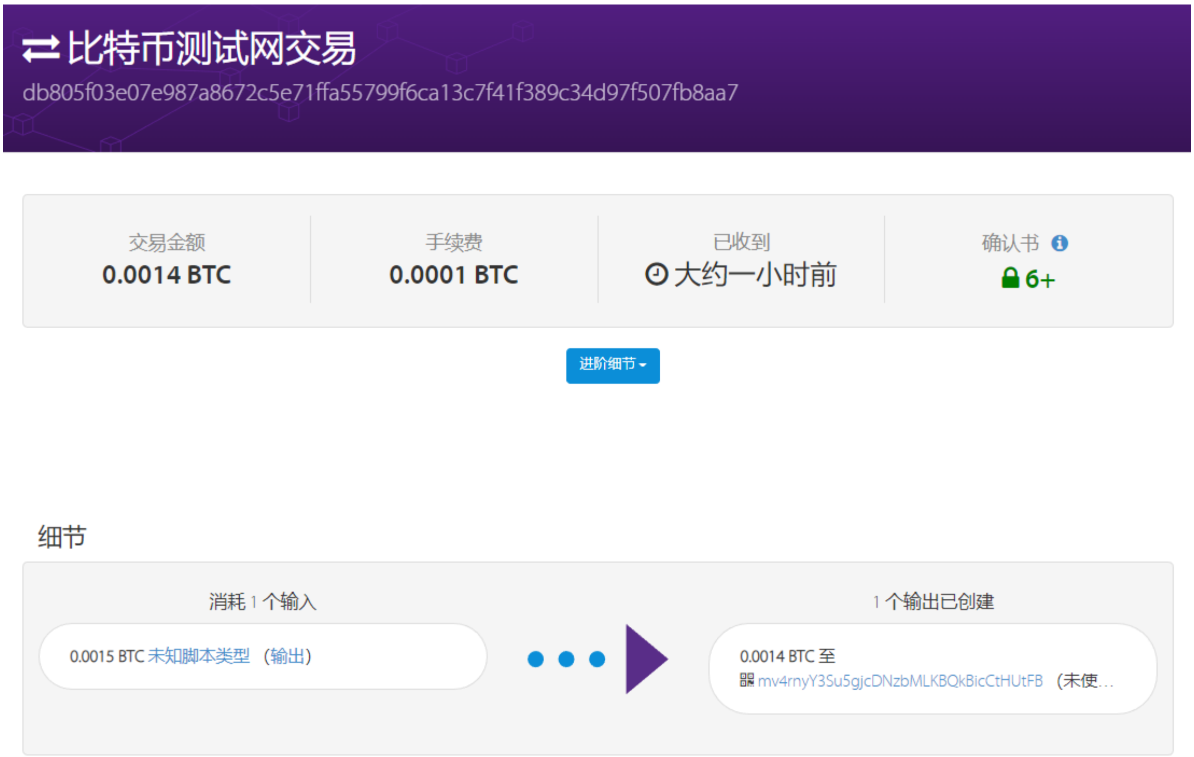
花费的是`ex2a`输出中新创建的区块。

交易信息：

```
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
"db805f03e07e987a8672c5e71ffa55799f6ca13c7f41f389c34d97f507fb8aa7",
    "addresses": [
      "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"
    ],
    "total": 140000,
    "fees": 10000,
    "size": 91,
    "vsize": 91,
    "preference": "high",
    "relayed_by": "2a01:4f8:202:1002:1111:1111:28e0:1",
    "received": "2022-11-13T03:13:42.636198034Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"1d09e2a5827e6009c57ed50a33df84a13de1d6dcb6947b536eaf5e8e8106c481",
        "output_index": 0,
        "script": "02f10402e902",
        "output_value": 150000,
        "sequence": 4294967295,
        "script_type": "unknown",
        "age": 2405947
      }
    ],
    "outputs": [
      {
```



```
        "value": 140000,
        "script": "76a9149f9a7abd600c0caa03983a77c8c3df8e062cb2fa88ac",
        "addresses": [
          "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"
        ],
        "script_type": "pay-to-pubkey-hash"
      }
    ]
  }
}
```



⇄ 比特币测试网交易

db805f03e07e987a8672c5e71ffa55799f6ca13c7f41f389c34d97f507fb8aa7

交易金额	手续费	已收到	确认书
0.0014 BTC	0.0001 BTC	大约一小时前	6+

细节

消耗 1 个输入

0.0015 BTC 未知脚本类型 （输出）

1 个输出已创建

0.0014 BTC 至
mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB （未使…