

第三次实验报告

2111460 张洋

一、练习 (a)

1. 补全代码

```
from sys import exit
from bitcoin.core.script import *

from utils import *
from config import my_private_key, my_public_key, my_address,
faucet_address
from ex1 import send_from_P2PKH_transaction

#####
# TODO: Complete the scriptPubKey implementation for Exercise 3
ex3a_txout_scriptPubKey = [OP_2DUP, OP_ADD, 211, OP_EQUALVERIFY, OP_SUB,
1459 ,OP_EQUAL]
#####

if __name__ == '__main__':

#####
    # TODO: set these parameters correctly
    amount_to_send = 0.0004
    txid_to_spend =
('c26d91f819ba03038c8936c56830a3996448cfd7dad7a67243ea8e5b95b799eb')
    utxo_index = 3

#####

    response = send_from_P2PKH_transaction(
        amount_to_send, txid_to_spend, utxo_index,
        ex3a_txout_scriptPubKey)
    print(response.status_code, response.reason)
    print(response.text)
```

2. 代码解释

(1) 构建一个交易输出锁定脚本，完成交易要求。

```
ex3a_txout_scriptPubKey = [OP_2DUP, OP_ADD, 211, OP_EQUALVERIFY, OP_SUB,
1459 ,OP_EQUAL]
```

- OP_2DUP: 一个比特币脚本操作码,复制堆栈顶部的两个元素到堆栈的顶部。
- OP_ADD:: 将堆栈顶部的两个元素相加,并将结果推送到堆栈中。
- 211: Student ID 的前 3 位,用于设定 x+y 的值。
- OP_EQUALVERIFY: 比较堆栈顶部的两个元素是否相等,如果相等,则继续执行下一步操作,否则终止交易。
- OP_SUB: 从堆栈顶部弹出两个元素,并计算它们的差,然后将结果推送到堆栈中。
- 1459 = 1460 - 1: Student ID 的后 4 位减 1,用于设定 x-y 的值。
- OP_EQUAL: 比较堆栈顶部的两个元素是否相等,如果相等,则返回 True,否则返回 False。

(2) 填写交易信息

```
amount_to_send = 0.0004
txid_to_spend =
('c26d91f819ba03038c8936c56830a3996448cfd7dad7a67243ea8e5b95b799eb')
utxo_index = 3
```

3. 输出信息


```
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
"84d4f10a8283c3013135dcb1d4c30a89feb98ba18e8e9a0905b63fe714217b72",
    "addresses": [
      "mszn3AE9xncT1QVvJVwFPQEf4ayRR6zFaV"
    ],
    "total": 40000,
    "fees": 45829,
    "size": 177,
    "vsize": 177,
    "preference": "high",
    "relayed_by": "117.131.219.28",
    "received": "2023-10-15T06:09:04.98121661Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
```

```

      "prev_hash":
      "c26d91f819ba03038c8936c56830a3996448cfd7dad7a67243ea8e5b95b799eb",
      "output_index": 3,
      "script":
      "4730440220355faffb77667e5d1f037d003502a2ca76778d60cf286964864dd3230e3b8
      ae1022008e6beb607fc0dac8040e2cfff180f2df16d43f74e5bb503c87d714b18041e10
      12103890bcd555dc24ebd465daf9c024e062123632b6fc9651f3cf98ef06deaeb4544",
      "output_value": 85829,
      "sequence": 4294967295,
      "addresses": [
        "mszn3AE9xncT1QVvJVwFPQEf4ayRR6zFaV"
      ],
      "script_type": "pay-to-pubkey-hash",
      "age": 2477601
    }
  ],
  "outputs": [
    {
      "value": 40000,
      "script": "6e9302d300889402b30587",
      "addresses": null,
      "script_type": "unknown"
    }
  ]
}

```

4. 截图

 Bitcoin Testnet Transaction

84d4f10a8283c3013135dcb1d4c30a89feb98ba18e8e9a0905b63fe714217b72

AMOUNT TRANSACTED

0.0004 BTC

FEES

0.00045829 BTC

RECEIVED

🕒 37 minutes ago

CONFIRMATIONS ⓘ

🔒 6+

Advanced Details ▾

Details

1 Input Consumed

0.00085829 BTC from

mszn3AE9xncT1QVvJVwFPQEf4ayRR6zFaV (output)

1 Output Created

0.0004 BTC Unknown Script Type

二、练习 (b)

1. 补全代码

```
from sys import exit
from bitcoin.core.script import *

from utils import *
from config import my_private_key, my_public_key, my_address,
faucet_address
from ex1 import P2PKH_scriptPubKey
from ex3a import ex3a_txout_scriptPubKey

#####
# TODO: set these parameters correctly
amount_to_send = 0.0001
txid_to_spend =
'84d4f10a8283c3013135dcb1d4c30a89feb98ba18e8e9a0905b63fe714217b72'
utxo_index = 0
#####

txin_scriptPubKey = ex3a_txout_scriptPubKey
#####
# TODO: implement the scriptSig for redeeming the transaction created
# in Exercise 3a.
#  $x+y=211$  &  $x-y=1459 \Rightarrow x=835$   $y=-624$ 
txin_scriptSig = [835, -624]
#####
txout_scriptPubKey = P2PKH_scriptPubKey(faucet_address)

response = send_from_custom_transaction(
    amount_to_send, txid_to_spend, utxo_index,
    txin_scriptPubKey, txin_scriptSig, txout_scriptPubKey)
print(response.status_code, response.reason)
print(response.text)
```

2. 代码解释

(1) 补全解锁交易输出的解锁脚本。

```
#  $x+y=211$  &  $x-y=1459 \Rightarrow x=835$   $y=-624$ 
txin_scriptSig = [835, -624]
```

x 和 y 需要满足 $x+y=211$ & $x-y=1459$, 经过计算可以得到 $x=835$, $y=-624$ 。

将上面两个值作为参数传入, 用作锁定脚本中的条件的数据。

(2) 填写交易信息


```
amount_to_send = 0.0001
txid_to_spend =
'84d4f10a8283c3013135dcb1d4c30a89feb98ba18e8e9a0905b63fe714217b72'
utxo_index = 0
```

3. 输出信息

```
201 Created
{
  "tx": {
    "block_height": -1,
    "block_index": -1,
    "hash":
"fb23dc3ecfe5af66db4d10e6f1b2980ba5525d7a1b54e835b3932c96b83c9052",
    "addresses": [
      "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"
    ],
    "total": 10000,
    "fees": 30000,
    "size": 91,
    "vsize": 91,
    "preference": "high",
    "relayed_by": "221.238.245.4",
    "received": "2023-10-15T06:51:04.10896553Z",
    "ver": 1,
    "double_spend": false,
    "vin_sz": 1,
    "vout_sz": 1,
    "confirmations": 0,
    "inputs": [
      {
        "prev_hash":
"84d4f10a8283c3013135dcb1d4c30a89feb98ba18e8e9a0905b63fe714217b72",
        "output_index": 0,
        "script": "024303027082",
        "output_value": 40000,
        "sequence": 4294967295,
        "script_type": "unknown",
        "age": 2533073
      }
    ],
    "outputs": [
      {
        "value": 10000,
        "script": "76a9149f9a7abd600c0caa03983a77c8c3df8e062cb2fa88ac",
```

```
    "addresses": [
      "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"
    ],
    "script_type": "pay-to-pubkey-hash"
  }
]
```

4. 截图

 Bitcoin Testnet Transaction
fb23dc3ecfe5af66db4d10e6f1b2980ba5525d7a1b54e835b3932c96b83c9052

AMOUNT TRANSACTED 0.0001 BTC	FEES 0.0003 BTC	RECEIVED 🕒 about 2 hours ago	CONFIRMATIONS ⓘ 🔒 6+
--	---------------------------	---------------------------------	-------------------------

Advanced Details ▾

Details

1 Input Consumed

0.0004 BTC Unknown Script Type (output)

...

▶

1 Output Created

0.0001 BTC to
mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB (unspent)