区块链lab3

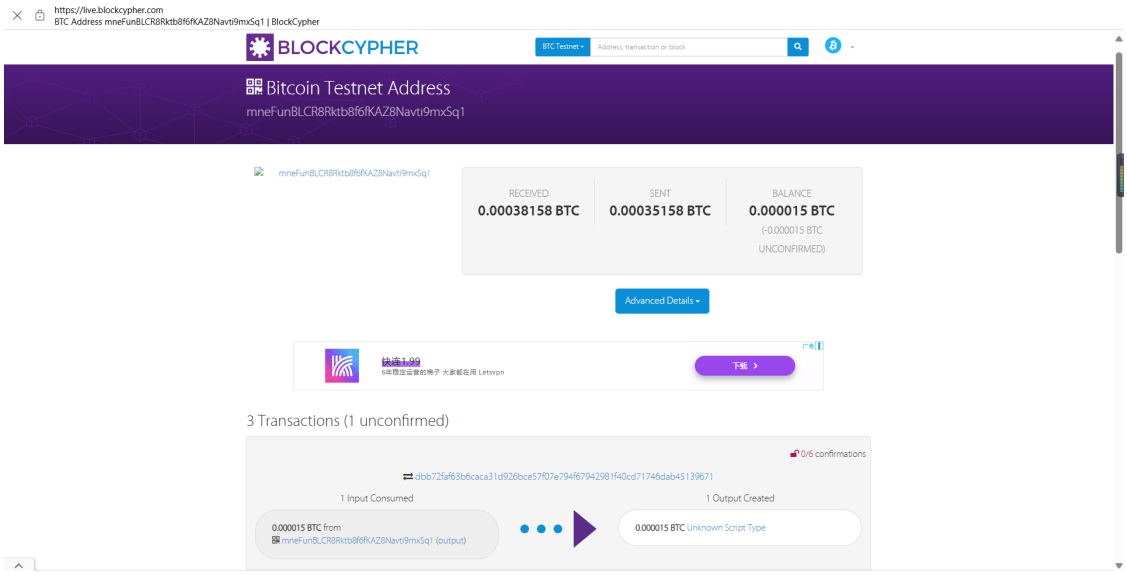
ex3a

补全代码：

`ex3a_txout_scriptPubKey = [OP_2DUP, OP_ADD, 221, OP_EQUALVERIFY, OP_SUB, 0977, OP_EQUAL]`

- `OP_2DUP`：是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
- `221`：`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
- `0977：` Student ID`的后 4 位（为了确保存在整数解，此处进行必要调整，将后4位**顺序减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`

交易截图



ex3b

补全代码

`txin_scriptSig = [1953,617]`

由规定x+y=2210,x-y=976可得x=1953，y=617

BLOCKCYPHER

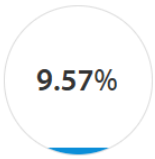
BTC Testnet | Address, transaction or block

Bitcoin Testnet Transaction

8fe942cee535c5be1fd5114eb5fc93e28e27f5fcd5d320e2a20477e0b3f20346

AMOUNT TRANSACTED	FEES	RECEIVED	CONFIRMATIONS
0.00001 BTC	0.000005 BTC	4 minutes ago	0/6

Confidence



Miner Preference

Size	91 bytes
Virtual Size	91 vbytes
Lock Time	
Version	1
Relayed By:	60.29.153.7

</> API Call | API Docs

Details

1 Input Consumed

0.000015 BTC Unknown Script Type (output)

1 Output Created

0.00001 BTC to n1KEfUMArwiKvdzgXbuCfTH3wpgaBmBjTJ (unspent)