区块链第一次实验报告

2013536 汤清云

【实验过程】

1. 使用keygen.py生成三个密钥作为客户。客户为：

|  |  |  |
| --- | --- | --- |
|  | 私钥 | Address |
| 客户一 | cQcwJtZp9sAvtwdBwCbjc57wbsHvJkLkLjq7g7xH8r25VBUHUiAX | mnz38qj3Eq5U4o3iDMfSoGLb5fKRJNsV8U |
| 客户二 | cNwGZD8gBxZvyGYpow8LPmBbn5c91kNVksAcePQhNJwihY3tSRPb | mzitDL44Rtfn1fqwuTqPeWVid4CSt9dMsS |
| 客户三 | cRKnrsyVqK4xjUJVGRUhPBfRs7txVrt5SLJM4yuUk8YrRfXV7XLN | n4KGQSbwDdSvW6nYbEdxbN6RTT2YgfSsap |

银行用户即之前创建的有比特币的用户：

|  |  |
| --- | --- |
| 私钥 | Address |
| cQf8sE9fhMtF6gBCv8Kb5Q7cPgcDvUm4VDGc3TDRKKiEbRekKdap | mz1BD2BUobyRWhMsSnzjkp43bYCJWEVMVf |

1. 将客户的私钥粘贴到ex2a.py对应位置中，并且为了能够正常生成客户对应的地址，我们需要导入包。



1. 由于题目中提到“需要银行与其他任何一个用户的签名才能赎回交易，而不仅仅是银行或者客户”，因此我们重写ex2a\_txout\_scriptPubkey如下：

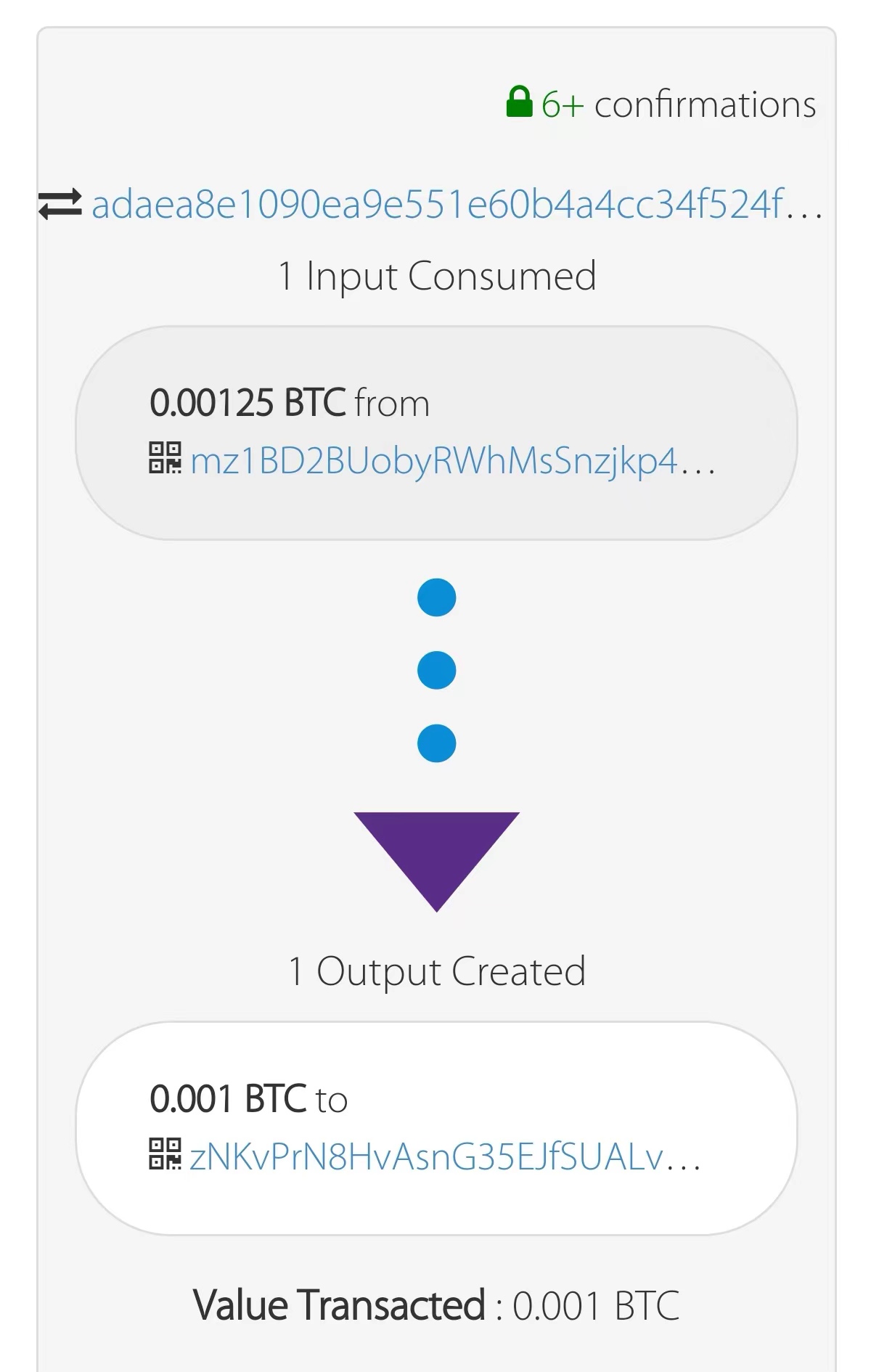
|  |
| --- |
| ex2a\_txout\_scriptPubKey = [my\_public\_key,OP\_CHECKSIGVERIFY,OP\_1,cust1\_public\_key,cust2\_public\_key,cust3\_public\_key,OP\_3,OP\_CHECKMULTISIG] |

首先必须要有银行公钥，故放在第一个，之后使用签名确认，OP\_1表明至少要有一个客户的签名，OP\_3表明一共的客户人数，之后使用多重签名确认。

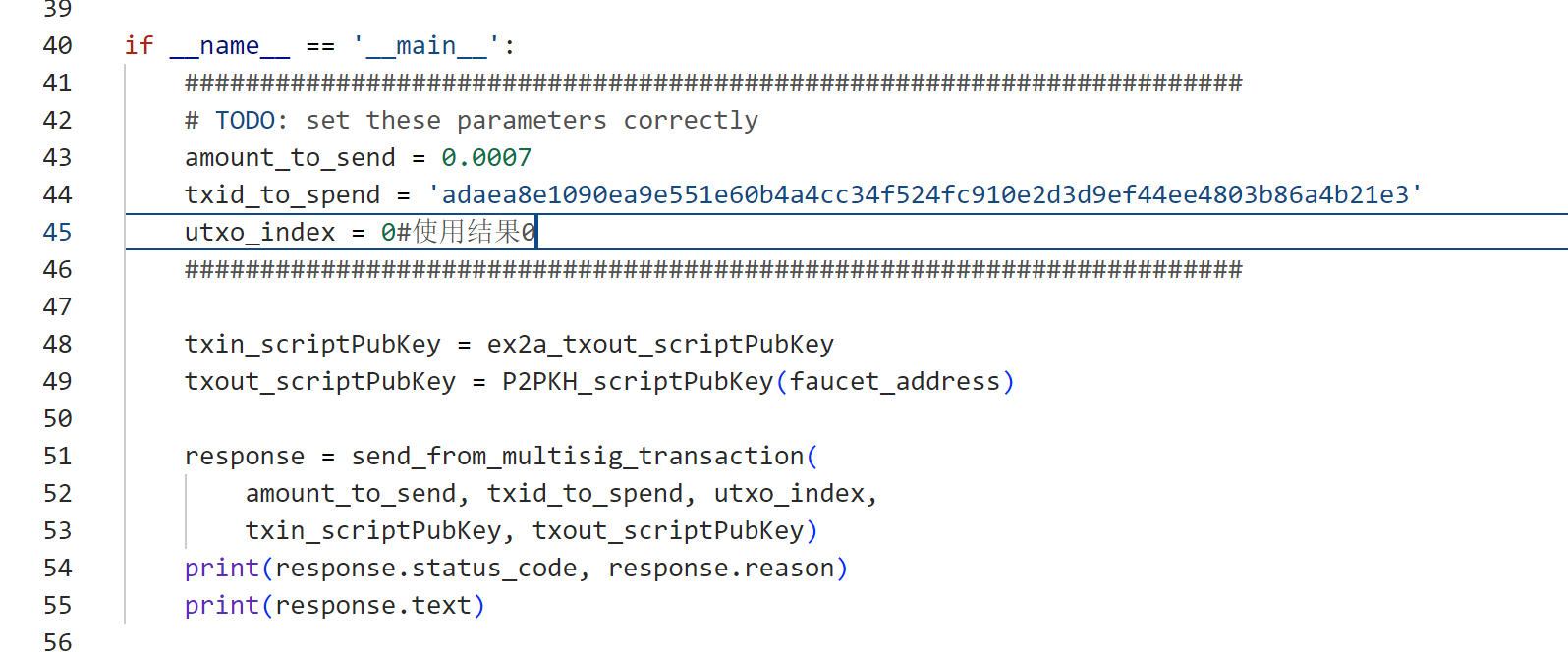
1. 使用之前作业的第五次分发作为此次加锁结果，运行后如下：

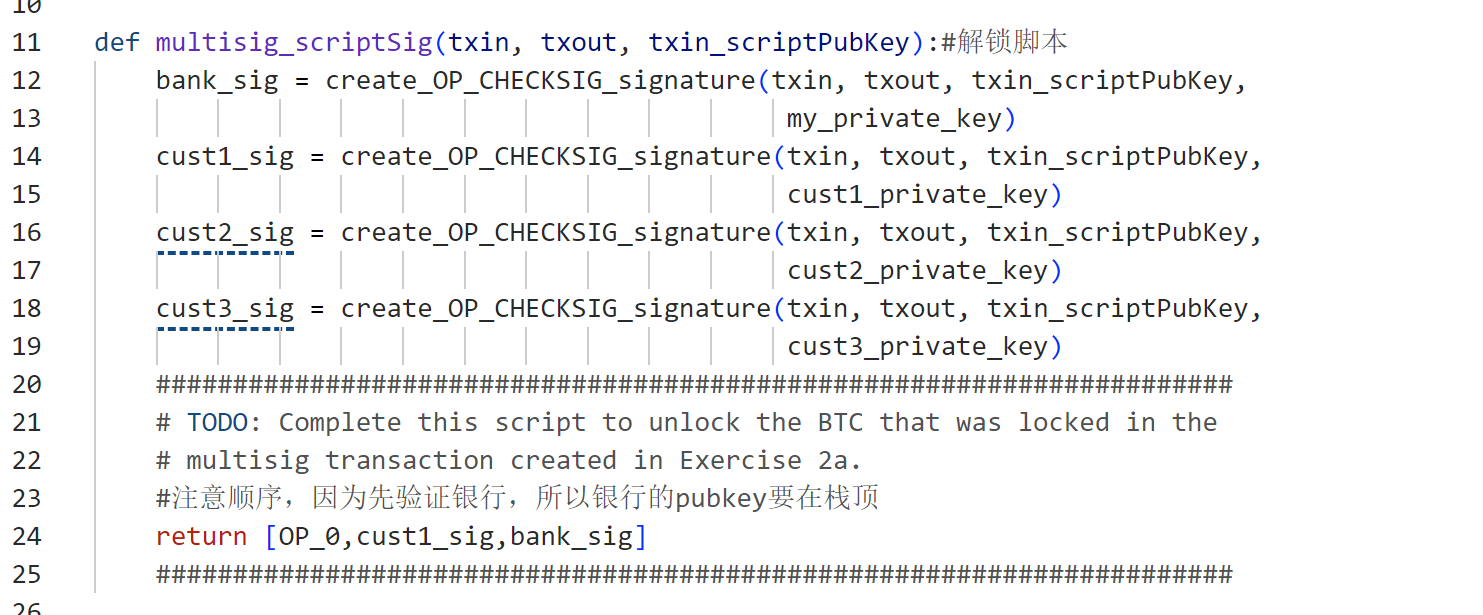
|  |
| --- |
| 201 Created  {  "tx": {  "block\_height": -1,  "block\_index": -1,  "hash": "adaea8e1090ea9e551e60b4a4cc34f524fc910e2d3d9ef44ee4803b86a4b21e3",  "addresses": [  "zNKvPrN8HvAsnG35EJfSUALvWrrWvghuj4",  "mz1BD2BUobyRWhMsSnzjkp43bYCJWEVMVf"  ],  "total": 100000,  "fees": 25000,  "size": 307,  "vsize": 307,  "preference": "medium",  "relayed\_by": "2001:250:401:6576:5d9a:fc62:357e:9356",  "received": "2022-10-25T02:09:22.702983239Z",  "ver": 1,  "double\_spend": false,  "vin\_sz": 1,  "vout\_sz": 1,  "confirmations": 0,  "inputs": [  {  "prev\_hash": "a93e884b671e0bcaf6ec605905616db063d2a37140bb6eff0dcfc86b17d90cf8",  "output\_index": 4,  "script": "483045022100d99bd697a22b5bd47a490290a180c7779d8272032e7b94ff09bfc4d14ed332cc0220440094c66f4c1d3542635e4f0517b92acfe837ddab2951a43647b3733376f091012103040cd5870921a2afa090af6db9638676b33c05c43d98596a6f4a2e203f53a778",  "output\_value": 125000,  {  "value": 100000,  "script": "2103040cd5870921a2afa090af6db9638676b33c05c43d98596a6f4a2e203f53a778ad512103ce6e4afc6f58e1727a1535b8d48d81ec20057fb01b4bc0380c29aa46b32183512102bb4b4b8912be0861bb05f3d5a610d1d31bcbbf13ea82c67d9e37698c3a78cf9521028745a869b8d152a71201ad30b439df17ee4f040fe427614e3a10ecadef4a480353ae",  "addresses": [  "zNKvPrN8HvAsnG35EJfSUALvWrrWvghuj4"  ],  "script\_type": "pay-to-multi-pubkey-hash"  }  ]  }} |

结果：



1. ex2b用于解锁之前的脚本，发回给faucet\_address，这里我们设定还给其的金额为0.0007，哈希值为第四步中交易得到的哈希值，index=0；而对于签名组合，我们使用cust1+bank：

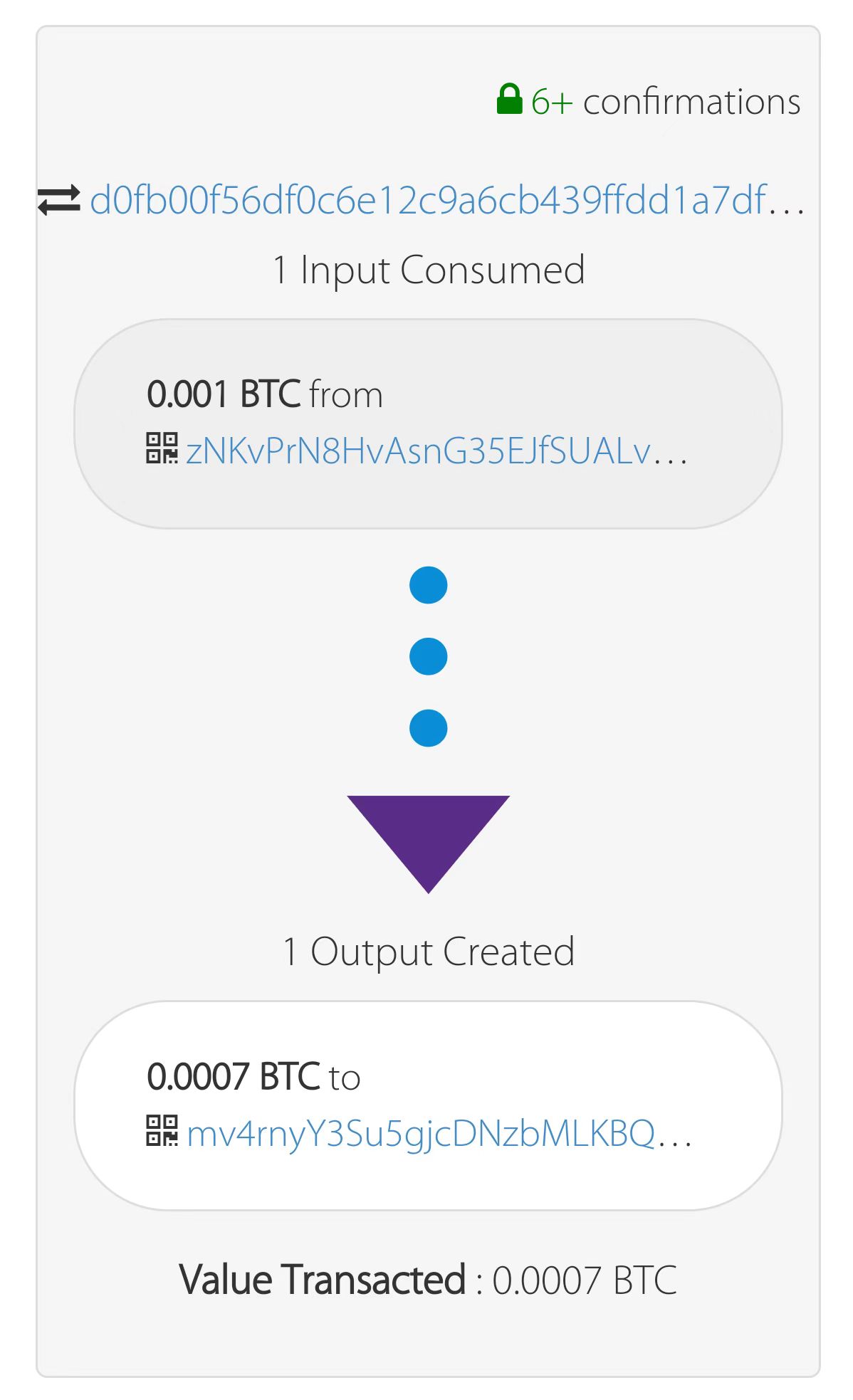




运行ex2b解锁结果：

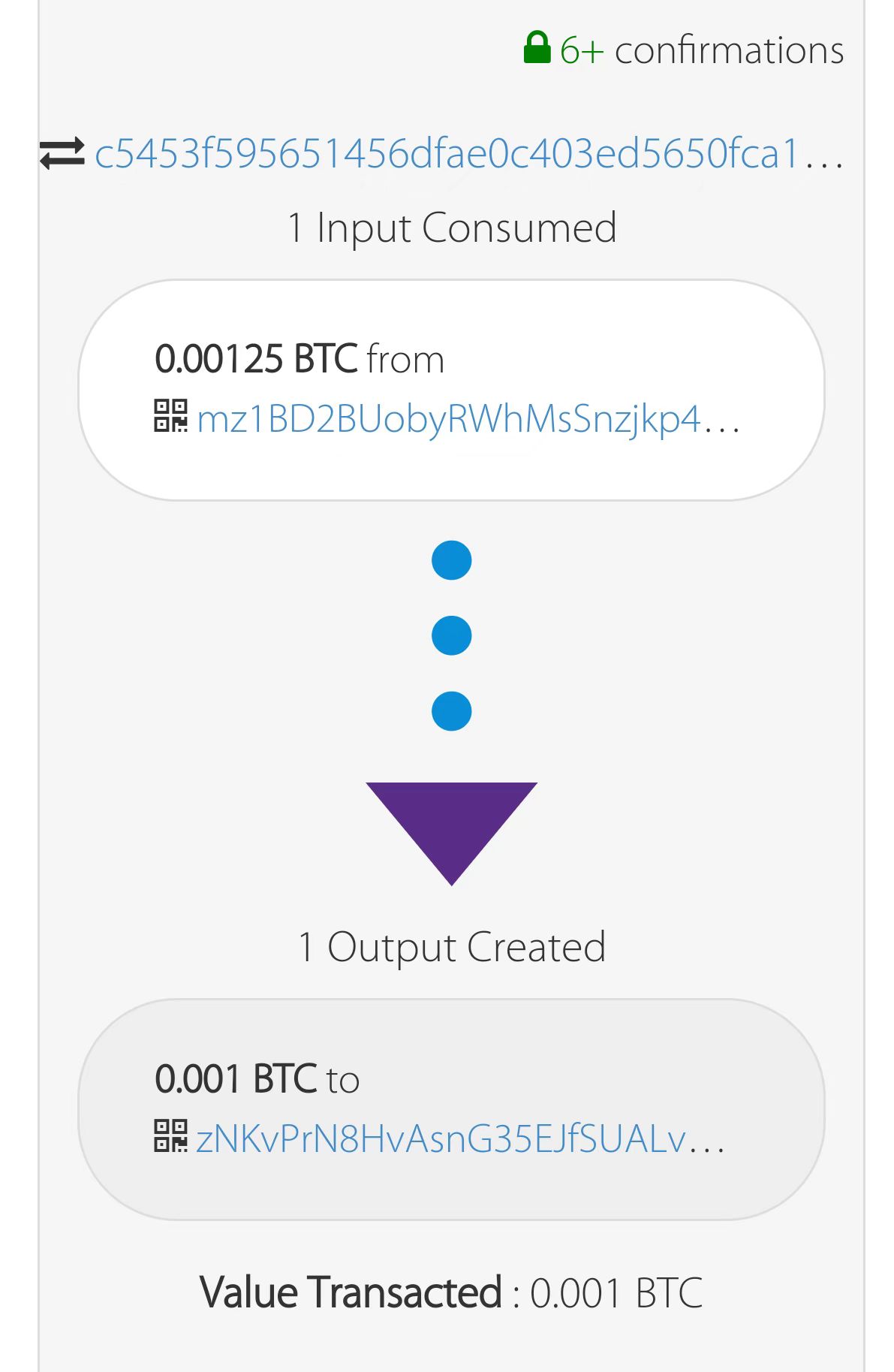
|  |
| --- |
| 201 Created  {  "tx": {  "block\_height": -1,  "block\_index": -1,  "hash": "d0fb00f56df0c6e12c9a6cb439ffdd1a7dfd2028c061cd3e8fe3ce359db435e8",  "addresses": [  "zNKvPrN8HvAsnG35EJfSUALvWrrWvghuj4",  "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"  ],  "total": 70000,  "fees": 30000,  "size": 232,  "vsize": 232,  "preference": "high",  "relayed\_by": "2001:250:401:6576:5d9a:fc62:357e:9356",  "received": "2022-10-25T02:12:51.578251567Z",  "ver": 1,  "double\_spend": false,  "vin\_sz": 1,  "vout\_sz": 1,  "confirmations": 0,  "inputs": [  {  "prev\_hash": "adaea8e1090ea9e551e60b4a4cc34f524fc910e2d3d9ef44ee4803b86a4b21e3",  "output\_index": 0,  "script": "00483045022100bb48e2a9612100ec5fcd8663679160735bc62382e7c239a7e1fe8d9cf38338850220058812d66fd6ca407b1563830d75775fa79f2c48bc5656c548fbbc662fb3108f01483045022100cf48b7e4f0b35d3d9637a2b64e2905cf48af557b3d1b7ff0e3bad7bd7f3821870220470f438037fec439cecd8036825b5614f7a8dd9a7404196817ea5ae73fb7e02401",  "output\_value": 100000,  "sequence": 4294967295,  "addresses": [  "zNKvPrN8HvAsnG35EJfSUALvWrrWvghuj4"  ],  "script\_type": "pay-to-multi-pubkey-hash",  "age": 0  }  ],  "outputs": [  {  "value": 70000,  "script": "76a9149f9a7abd600c0caa03983a77c8c3df8e062cb2fa88ac",  "addresses": [  "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"  ],  "script\_type": "pay-to-pubkey-hash"  }  ]  }  } |

交易结果为：



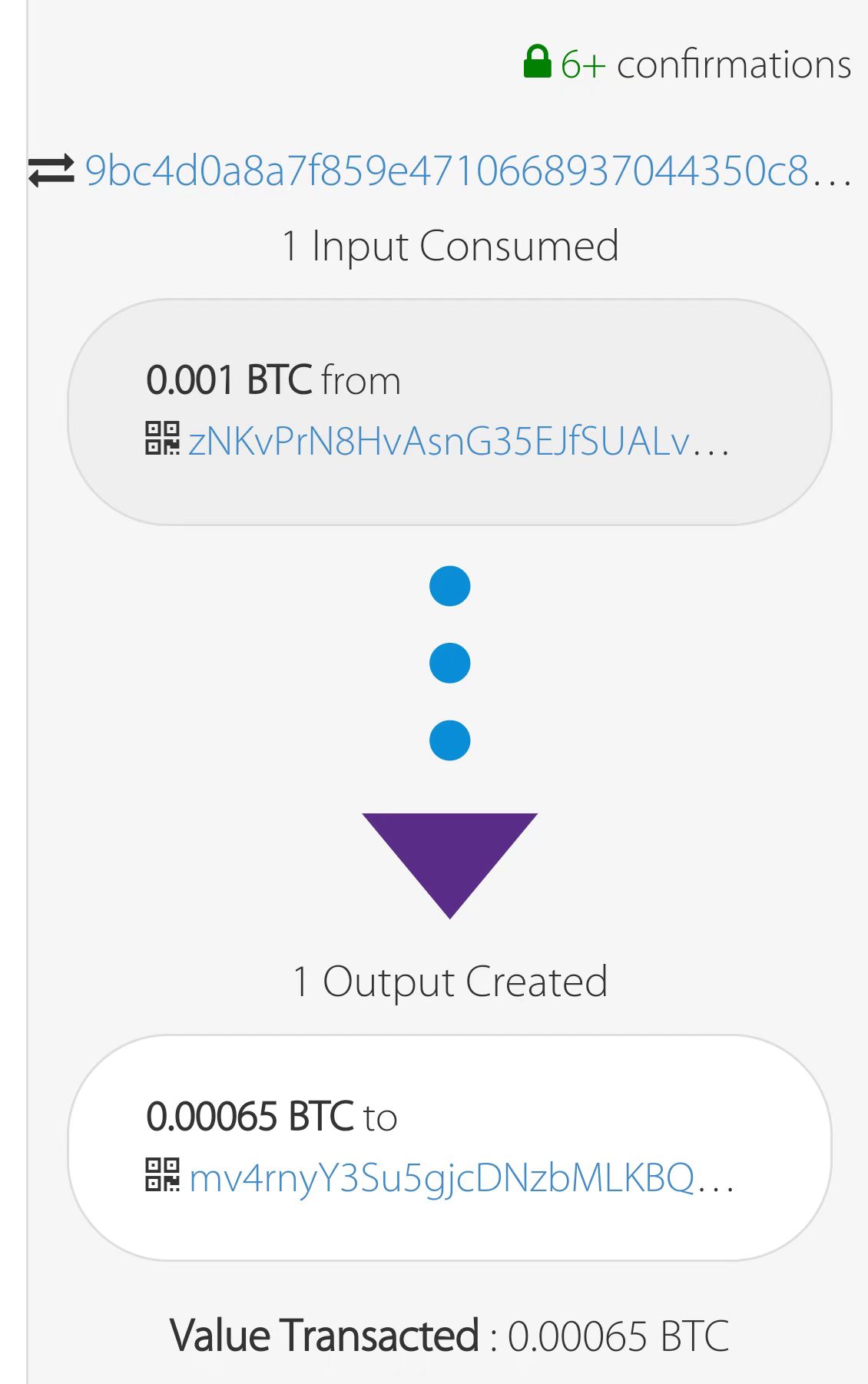
1. 使用之前作业的第七次分发作为另一次加锁结果以验证bank+cus2的结果。取回0.0065

|  |
| --- |
| 201 Created  {  "tx": {  "block\_height": -1,  "block\_index": -1,  "hash": "c5453f595651456dfae0c403ed5650fca100abb8cfa60579bc0a4ea8786b6cf3",  "addresses": [  "mz1BD2BUobyRWhMsSnzjkp43bYCJWEVMVf",  "zNKvPrN8HvAsnG35EJfSUALvWrrWvghuj4"  ],  "total": 100000,  "fees": 25000,  "size": 306,  "vsize": 306,  "preference": "medium",  "relayed\_by": "2001:250:401:6576:5d9a:fc62:357e:9356",  "received": "2022-10-25T02:37:22.559598132Z",  "ver": 1,  "double\_spend": false,  "vin\_sz": 1,  "vout\_sz": 1,  "confirmations": 0,  "inputs": [  {  "prev\_hash": "a93e884b671e0bcaf6ec605905616db063d2a37140bb6eff0dcfc86b17d90cf8",  "output\_index": 6,  "script": "473044022052c4bab6263b7f9f1ac09eb753faf970eb7e91228d96442bbd8f73c47aa34bbb02206c73ee2d875d34b730f1e96bc7c98ba1356112e1b046b51c58dbfb32350081b9012103040cd5870921a2afa090af6db9638676b33c05c43d98596a6f4a2e203f53a778",  "output\_value": 125000,  "sequence": 4294967295,  "addresses": [  "mz1BD2BUobyRWhMsSnzjkp43bYCJWEVMVf"  ],  "script\_type": "pay-to-pubkey-hash",  "age": 2350569  }  ],  "outputs": [  {  "value": 100000,  "script": "2103040cd5870921a2afa090af6db9638676b33c05c43d98596a6f4a2e203f53a778ad512103ce6e4afc6f58e1727a1535b8d48d81ec20057fb01b4bc0380c29aa46b32183512102bb4b4b8912be0861bb05f3d5a610d1d31bcbbf13ea82c67d9e37698c3a78cf9521028745a869b8d152a71201ad30b439df17ee4f040fe427614e3a10ecadef4a480353ae",  "addresses": [  "zNKvPrN8HvAsnG35EJfSUALvWrrWvghuj4"  ],  "script\_type": "pay-to-multi-pubkey-hash"  }  ]  }  } |



解锁结果为

|  |
| --- |
| 201 Created  {  "tx": {  "block\_height": -1,  "block\_index": -1,  "hash": "9bc4d0a8a7f859e4710668937044350c8e19d8596a5101778b3812de05bcac42",  "addresses": [  "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB",  "zNKvPrN8HvAsnG35EJfSUALvWrrWvghuj4"  ],  "total": 65000,  "fees": 35000,  "size": 231,  "vsize": 231,  "preference": "high",  "relayed\_by": "2001:250:401:6576:5d9a:fc62:357e:9356",  "received": "2022-10-25T02:39:04.572806252Z",  "ver": 1,  "double\_spend": false,  "vin\_sz": 1,  "vout\_sz": 1,  "confirmations": 0,  "inputs": [  {  "prev\_hash": "c5453f595651456dfae0c403ed5650fca100abb8cfa60579bc0a4ea8786b6cf3",  "output\_index": 0,  "script": "00483045022100e627a5c90a936b8e56e6361b43499ea3e3b13383c7a0e1448e967d369b59eb3202204c7af0c54dc88cdce2645ec38bff9695a366a7d04d9a23f8c5d35bef11456be50147304402206bc6b90daa05d49656f8b2c4107403c31a53037019d9a8f0a97221a925af090c02203f8f0abce9aa83f413f84f58917b14be8a8f2114a9d32dfcfec0fe9e2365cced01",  "output\_value": 100000,  "sequence": 4294967295,  "addresses": [  "zNKvPrN8HvAsnG35EJfSUALvWrrWvghuj4"  ],  "script\_type": "pay-to-multi-pubkey-hash",  "age": 0  }  ],  "outputs": [  {  "value": 65000,  "script": "76a9149f9a7abd600c0caa03983a77c8c3df8e062cb2fa88ac",  "addresses": [  "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"  ],  "script\_type": "pay-to-pubkey-hash"  }  ]  }  } |



使用第八份检测是否可以两个cus赎回。

加锁结果：

|  |
| --- |
|  |

解锁结果：

|  |
| --- |
|  |