区块链第三次实验报告

2013536 汤清云

【实验目标】

1. 生成一个可以由以下线性方程组的解赎回的交易：

|  |
| --- |
| X+y=2013 |
| x-y=535 |

此处由于我学号的前四位和后三位奇偶性不同，故修改为2013535

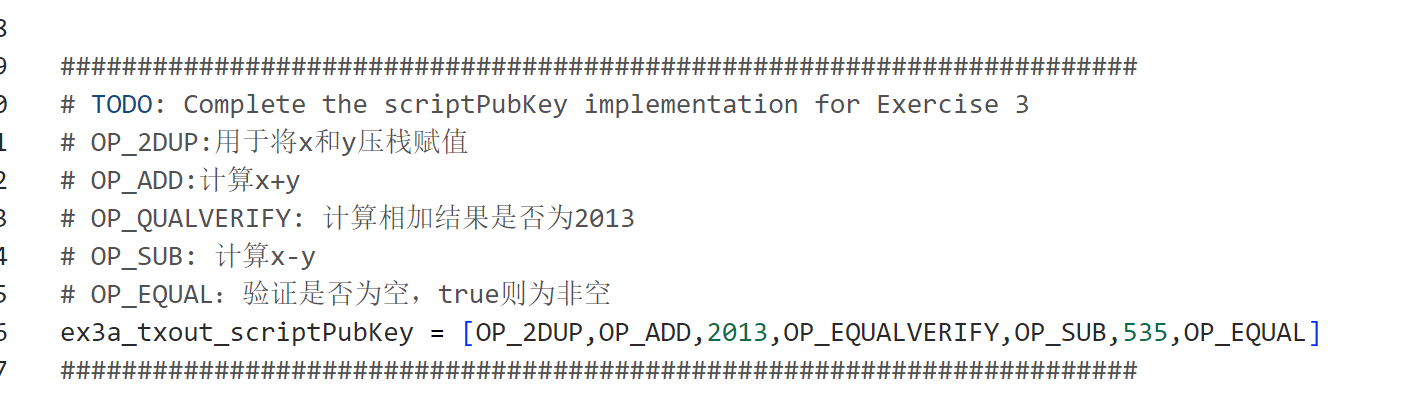
1. 赎回交易。赎回脚本应尽可能小。

【实验过程】

由于之前分发的币已经用完了，所以新申请了一个地址用于本次实验。

|  |
| --- |
| Private key: cVWrNVeTWPG5HKEz2G3AwJV5j9ABuupcREWhBcF1t7seNWbtjucF |
| Address: mnbt1BdPdS2VyMbqo5s2YUqdZfUv8EC4wz |
| 分币hash：  1641fe39ff2bd4873c27eb6710f4d6bd426ab249e6e473660533cf73a300f318 |

1. 加锁脚本：

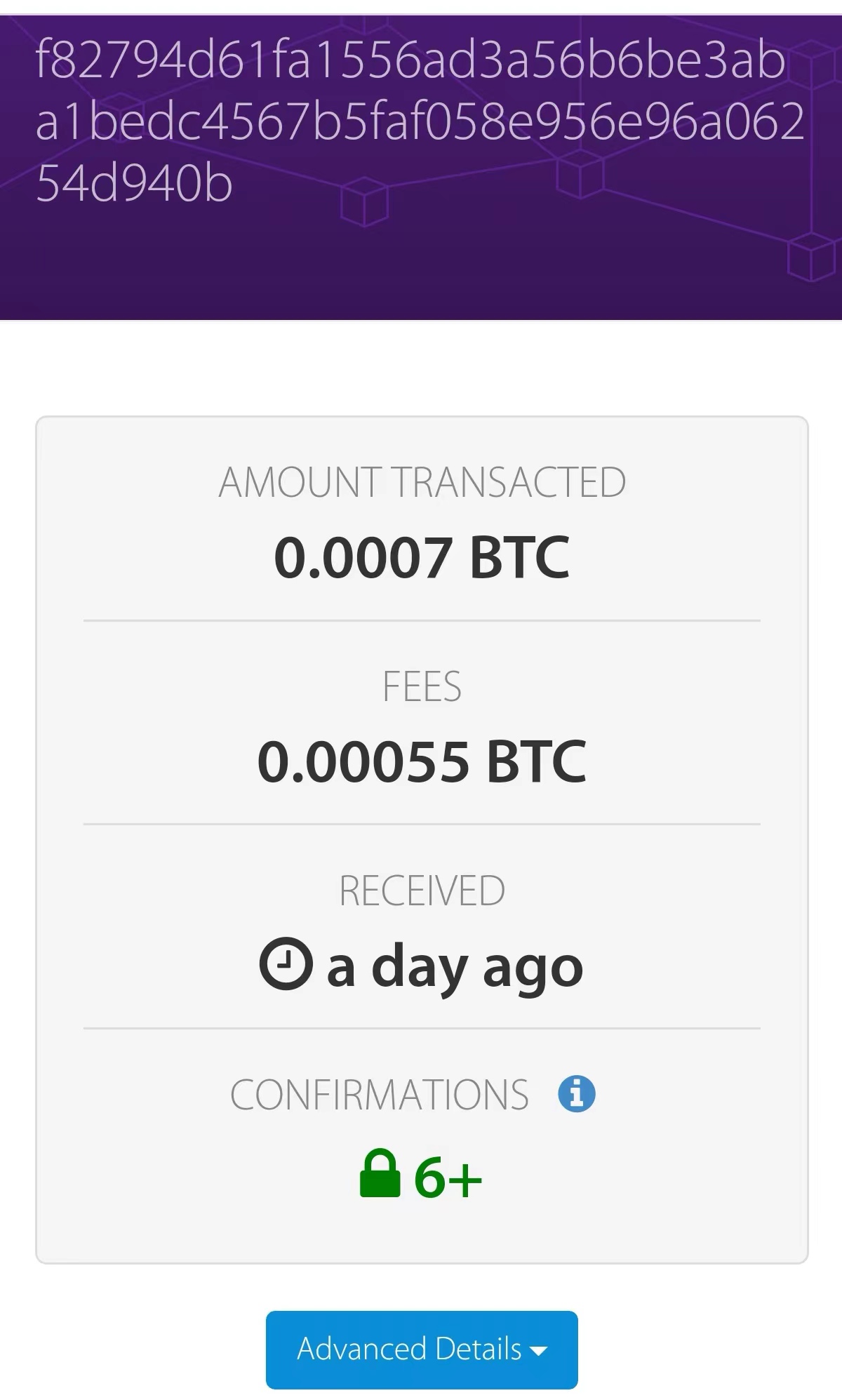




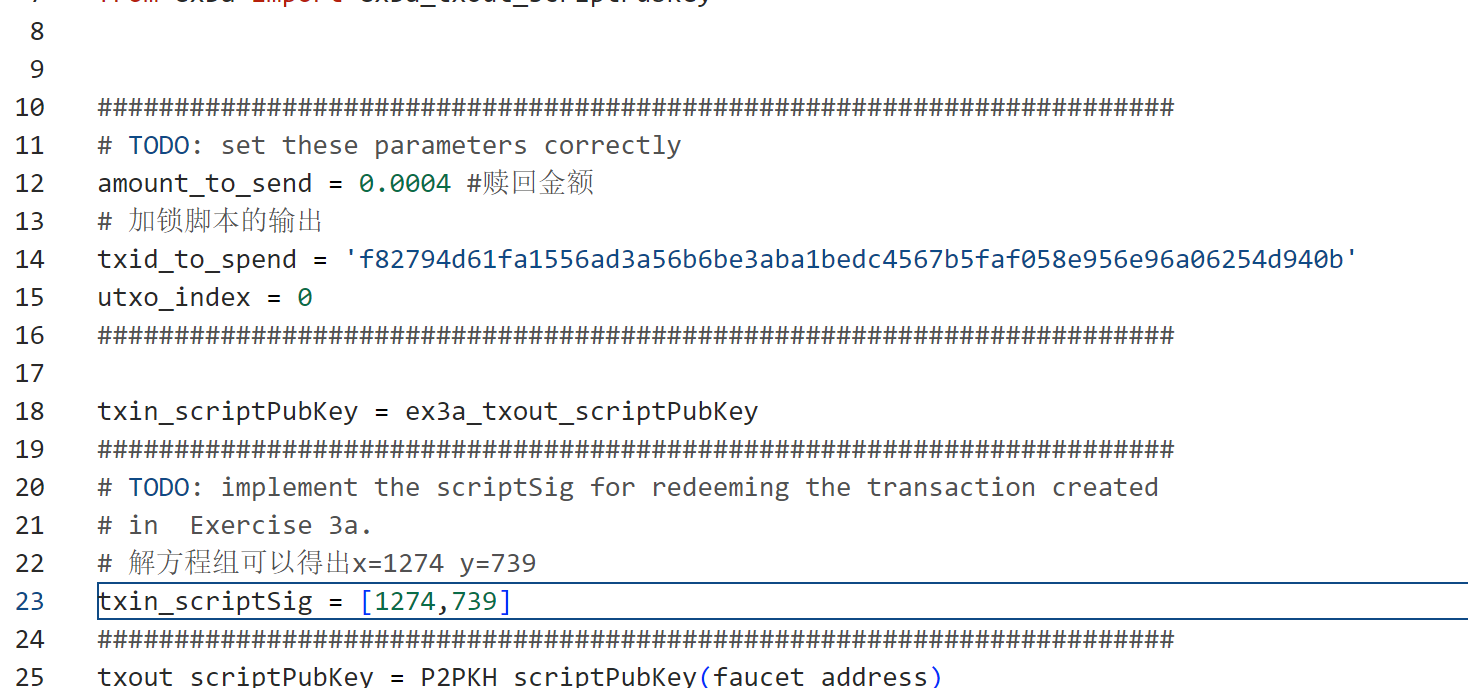
运行结果：

|  |
| --- |
| 201 Created  {  "tx": {  "block\_height": -1,  "block\_index": -1,  "hash": "f82794d61fa1556ad3a56b6be3aba1bedc4567b5faf058e956e96a06254d940b",  "addresses": [  "mnbt1BdPdS2VyMbqo5s2YUqdZfUv8EC4wz"  ],  "total": 70000,  "fees": 55000,  "size": 177,  "vsize": 177,  "preference": "high",  "relayed\_by": "2001:250:401:6560:20c9:315:8525:fc9f",  "received": "2022-11-09T07:18:36.749155664Z",  "ver": 1,  "double\_spend": false,  "vin\_sz": 1,  "vout\_sz": 1,  "confirmations": 0,  "inputs": [  {  "age": 2405348  }  ], "outputs": [  {  "value": 70000,  "script": "6e9302dd07889402170287",  "addresses": null,  "script\_type": "unknown"  }  ]  }  } |

结果为：



1. 解锁脚本



运行结果：

|  |
| --- |
| 201 Created  {  "tx": {  "block\_height": -1,  "block\_index": -1,  "hash": "afb9098d23cc40ad5b340be808e004014c6b3692c3eb08aa3af5b7600cb67f6d",  "addresses": [  "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"  ],  "total": 40000,  "fees": 30000,  "size": 91,  "vsize": 91,  "preference": "high",  "relayed\_by": "2001:250:401:6560:20c9:315:8525:fc9f",  "received": "2022-11-09T08:08:26.690993535Z",  "ver": 1,  "double\_spend": false,  "vin\_sz": 1,  "vout\_sz": 1,  "confirmations": 0,  "inputs": [  {  "prev\_hash": "f82794d61fa1556ad3a56b6be3aba1bedc4567b5faf058e956e96a06254d940b",  "script": "76a9149f9a7abd600c0caa03983a77c8c3df8e062cb2fa88ac",  "addresses": [  "mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB"  ],  "script\_type": "pay-to-pubkey-hash"  }  ]  }  } |

结果为：

