命令行版本多签交易生成用户手册

Release Table

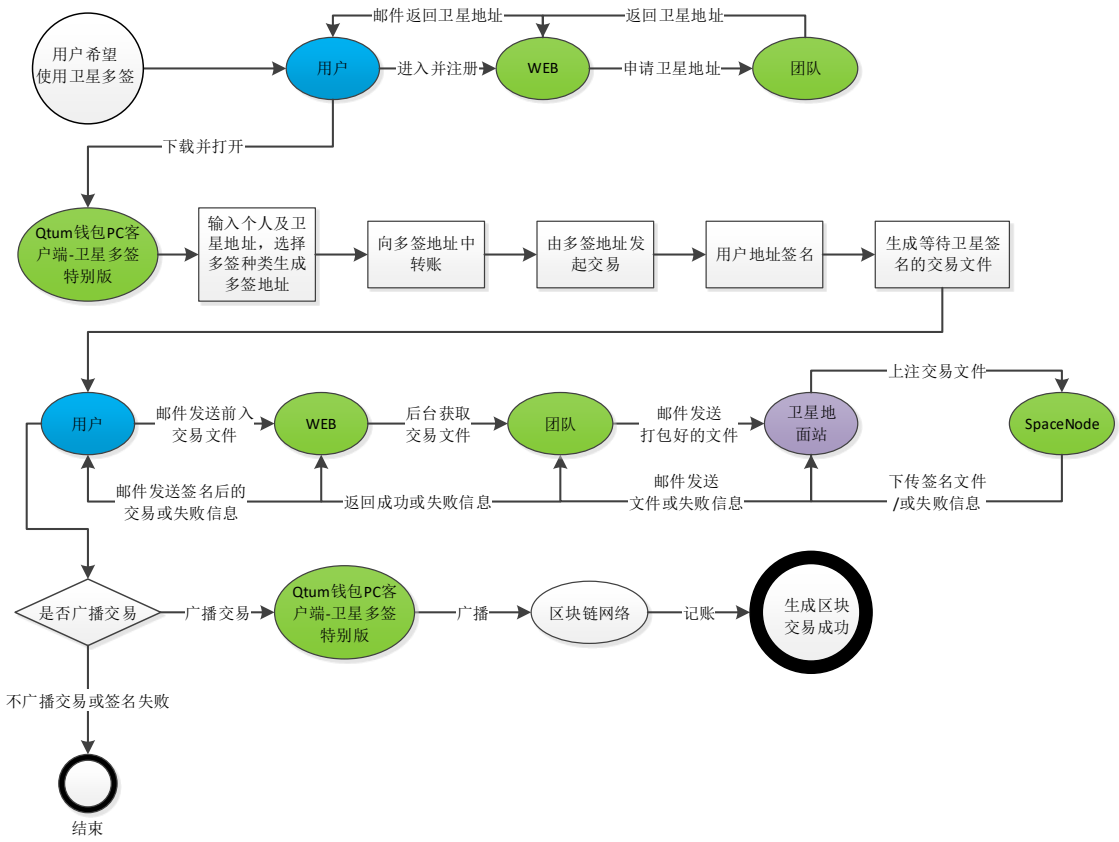
Version	Date	Changes
V0.0	Oct 06, 2018	初始版本;
V1.0	Oct 22, 2018	正式版本;

1 文档说明

1.1 文档功能说明

本文档旨在帮助用户生成多重签名交易。

1.2 卫星签名服务整体流程介绍



2 操作流程

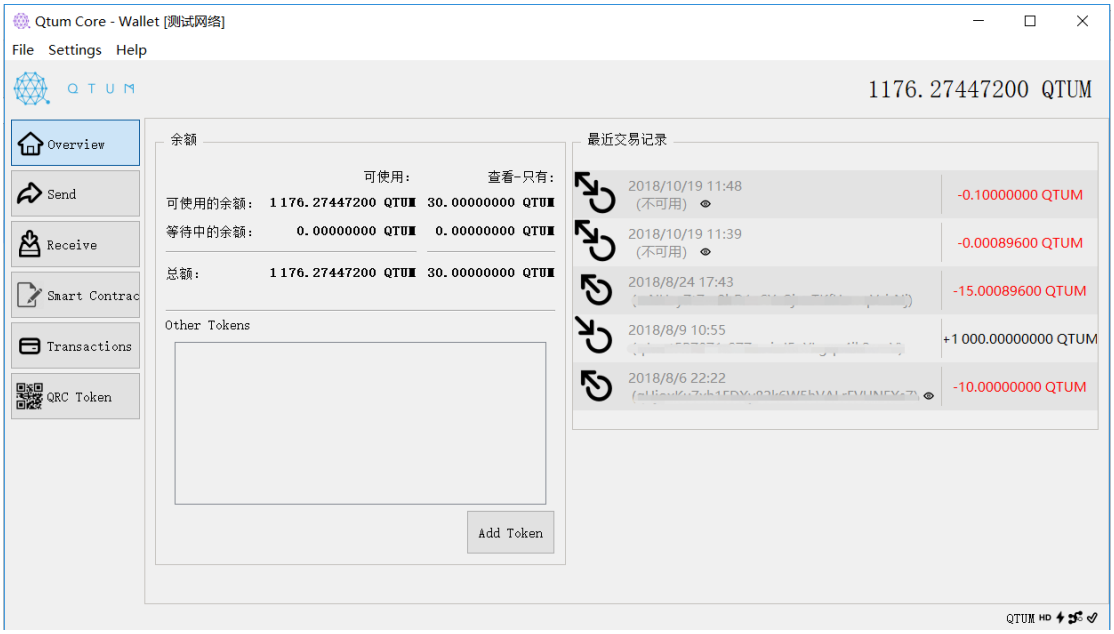
2.1 生成多签钱包地址

获得卫星签名节点地址

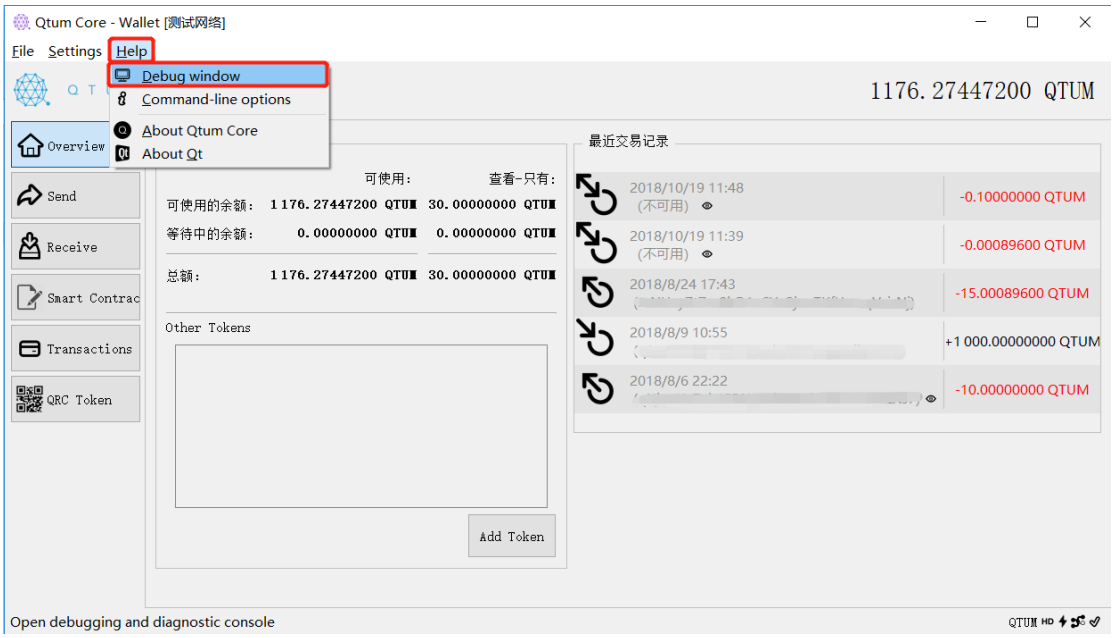
登录 Spacechain 官网，根据官网提示步骤申请卫星签名节点地址。

获取自己的钱包地址

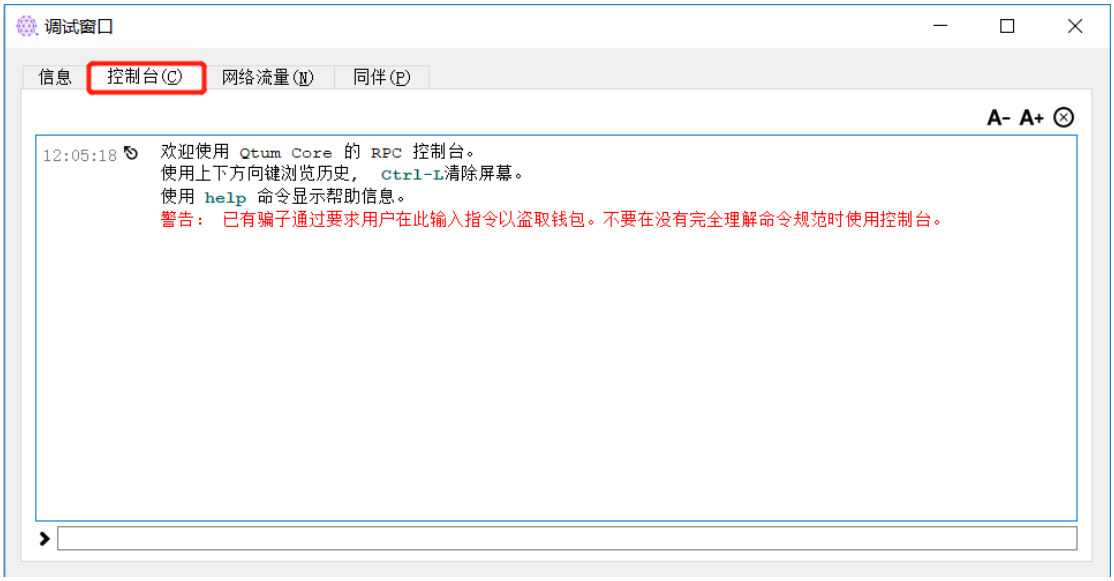
双击图标打开 QTUM 全节点客户端;



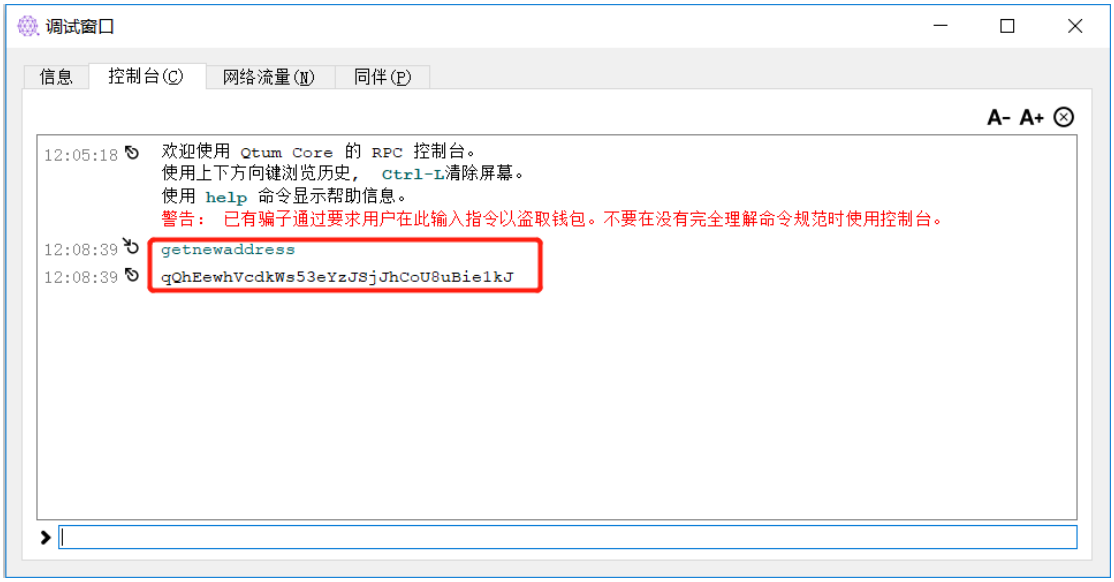
点击上方的**“Help”**标签，点击**“Debug window”**，进入调试窗口；



点击上方的**“控制台”**标签，进入控制台；



在下方的输入栏中输入:
getnewaddress
点击**“enter”**执行命令，获取自己的钱包地址;
客户端会自动返回一个新的钱包地址;

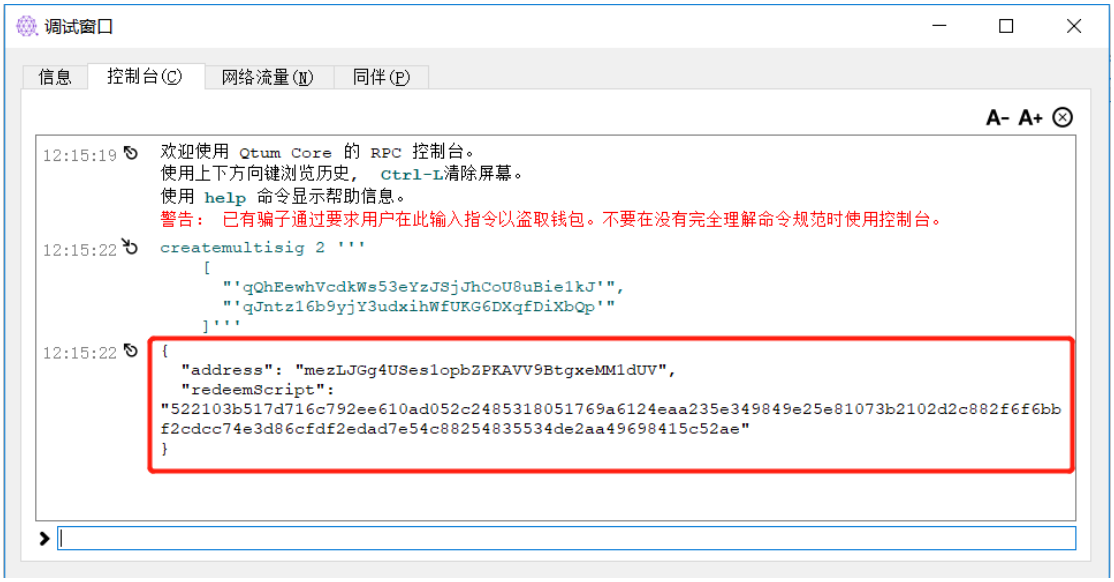


生成多签钱包地址
按照如下格式，拼接多签钱包地址生成命令:
createmultisig 2 '''
[
"'自己的钱包地址'",
"'申请的卫星签名节点地址'"
]'''

拼接后的命令如下:
createmultisig 2 '''

```
[
  "'qQhEewhVcdkWs53eYzJSjJhCoU8uBie1kJ'",
  "'qJntz16b9yjY3udxihWfUKG6DXqfDiXbQp'"
]'''
```

将命令复制到输入栏中，点击**“enter”**生成多签钱包地址；



客户端返回的结果有三个字段：

address 为生成的多签钱包地址；

redeemScript 为多签地址的签名脚本；

导入多签地址到钱包

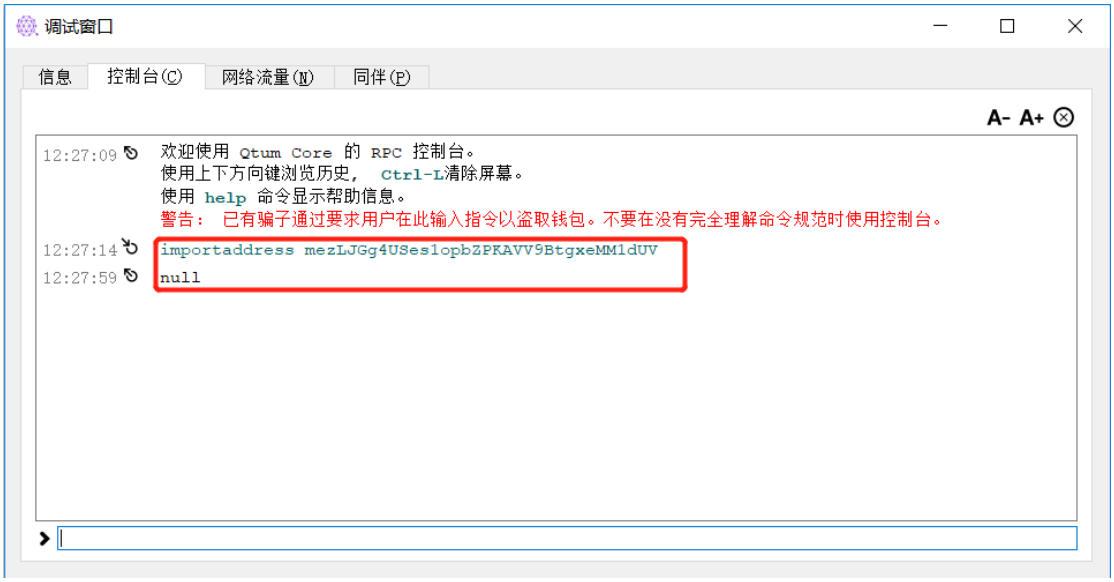
在命令输入

importaddress + 多签钱包地址数

即：

importaddress `mezLJGg4USes1opbZPKAVV9BtgxeMM1dUV`

点击**“enter”**，将多签钱包地址导入客户端中，时间较长，请耐心等待；



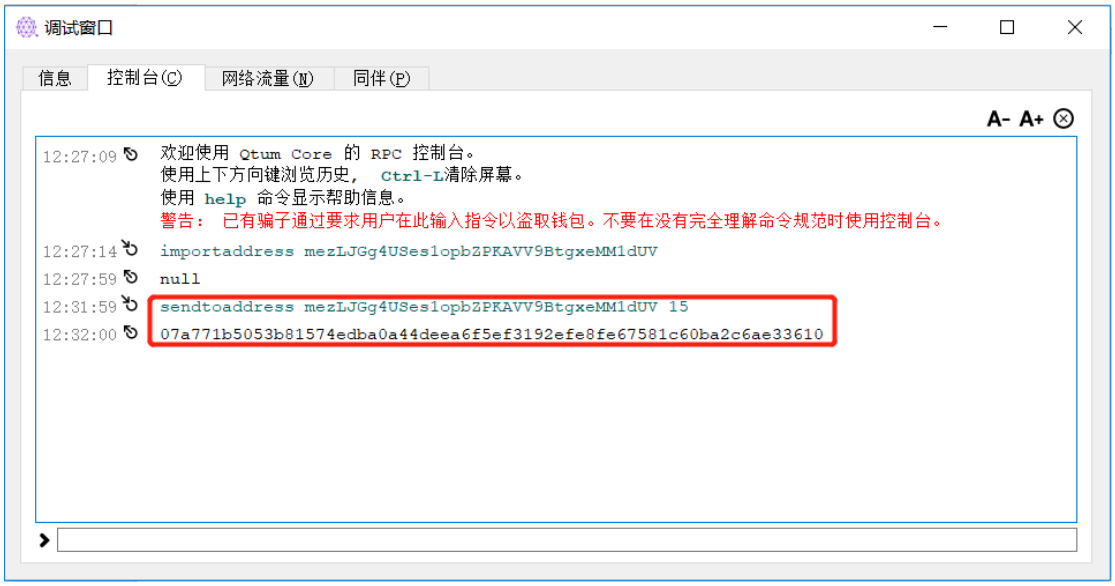
导入成功后，客户端会返回**“null”**。

2.2 多签钱包地址充值

按照以下格式拼接向多签钱包地址转账的命令：
sendtoaddress 多签钱包地址 转账数额

以充值 15 个 token 为例，命令即为：
sendtoaddress mezLJGg4USes1opbZPKAVV9BtgxeMM1dUV 15

点击**“enter”**执行命令，向多签钱包地址转账 15 个 token；



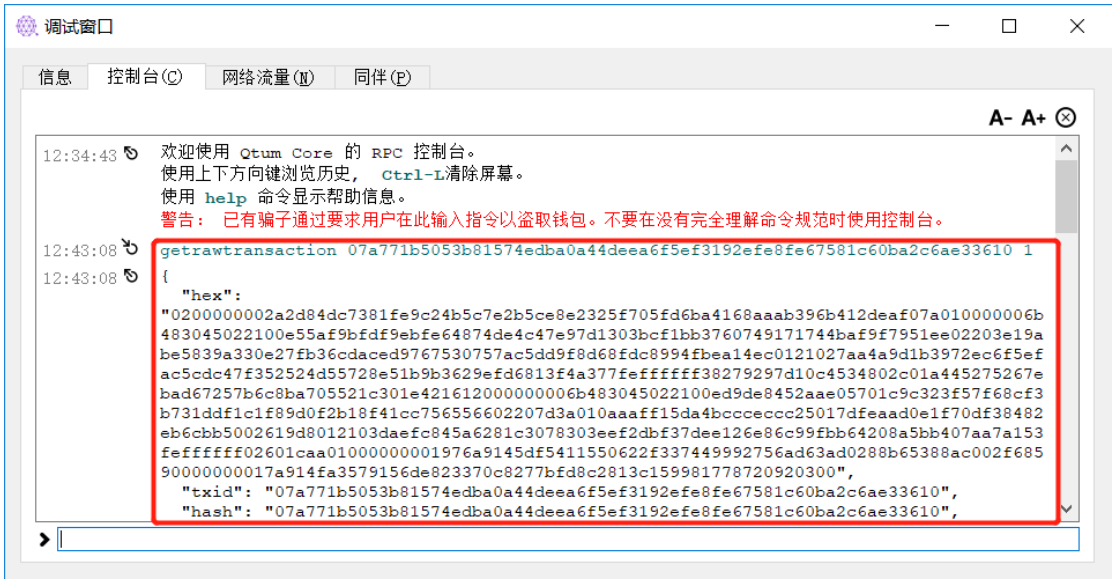
客户端会返回交易的 txid，请将 txid 复制到 txt 文档中保存好，接下来的步骤中会用到。

2.3 创建多签交易

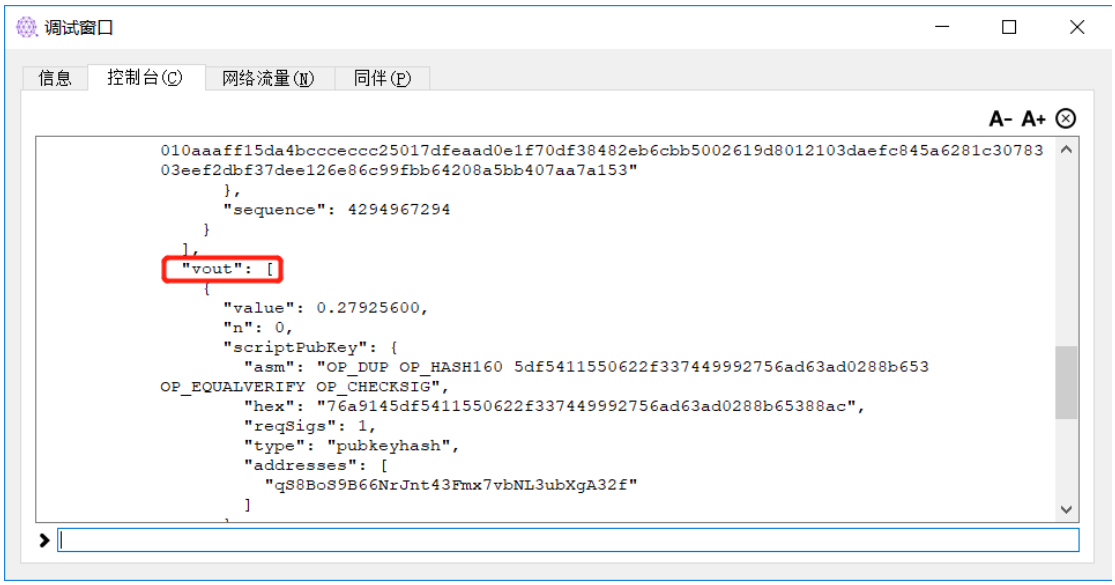
获取地址中的余额信息
在输入栏中输入：
getrawtransaction 返回的 txid 1

以本次为例，即为：
getrawtransaction
07a771b5053b81574edba0a44deea6f5ef3192efe8fe67581c60ba2c6ae33610 1

点击**“enter”**执行命令，获取余额信息；

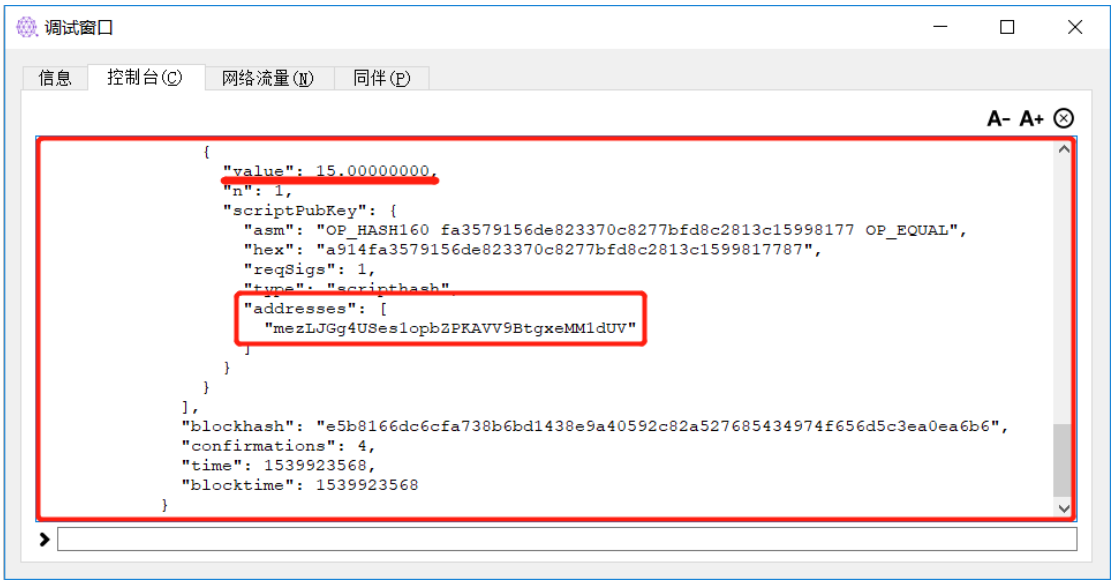


余额的相关信息有很多，我们需要找到需要的部分。
拖动滚动条，找到**“vout”**字段；



在“vout”字段下，找到“value”字段与转账数额匹配且“addresses”字段为多签地址的一组数据；

以本次实验为例，即找到“value”字段为 15，“addresses”字段为 mezLJGg4USes1opbZPKAVV9BtgxeMM1dUV 的数据段；



请将这段数据复制到 txt 文件中保存，之后的操作后用到。

创建裸交易

按照如下格式拼接裸交易生成命令：

```
createrawtransaction '''
    [
      {
        "txid": "'返回的 txid'",
        "vout": '余额信息中的“n”字段内容'
      }
  ]
  ''' '''
  {
    "'收款人地址'": 转账金额
  }'''
```

将之前充值后客户端返回的“txid”填写到裸交易生成命令的“txid”字段。

在之前获取的余额信息有效字段中，将“n”字段的内容填写到裸交易生成命令的“vout”字段；

将收款人地址填写到对应字段；

在转账金额位置输入转账金额；

注意：为了安全起见，强烈建议：用户在体验交易时，输入的转账金额一定为充值金额减去 0.1（即：转账金额 = 充值金额 – 0.1）；

以本次为例，拼接后的命令为：

```
createrawtransaction '''
    [
```

```
        {
          "txid":
"'07a771b5053b81574edba0a44deea6f5ef3192efe8fe67581c60ba2c6ae33610'",
          "vout": '1'
        }
    ]
    ''' '''
    {
      "'qg9nLsvSURtBcNJbWS4TiqrKkMuppUKHv1'": 14.9
    }'''
```

点击“enter”执行命令，创建裸交易；

客户端会返回，交易的 hex 码。

将交易的 hex 码复制到 txt 文档保存，以后的步骤会用到。

2.4 交易签名确认

获取自己的私钥

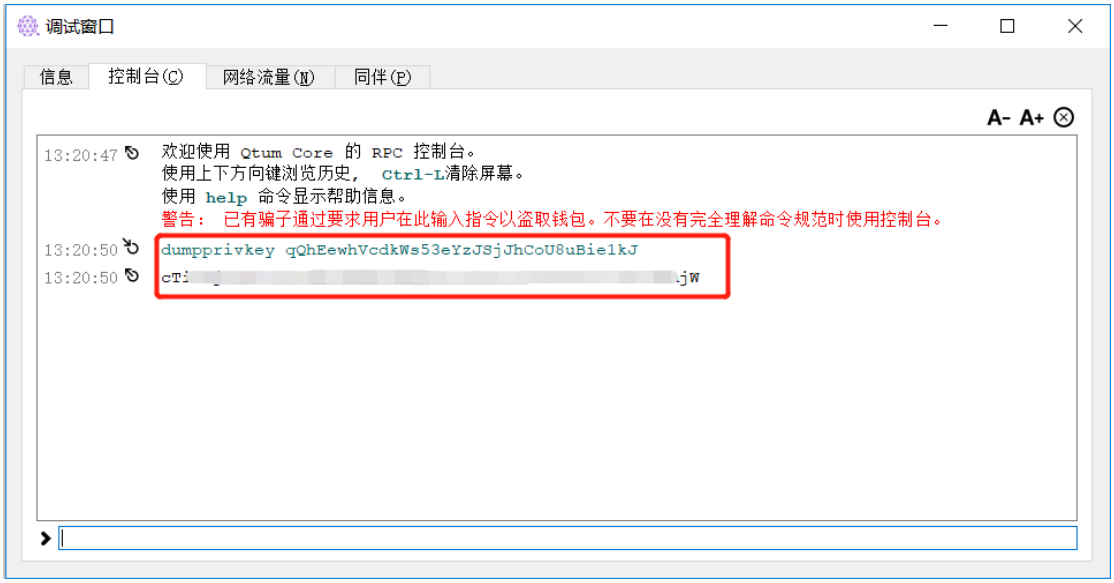
在输入栏中输入：

dumpprivkey + 生成多签钱包地址时用的钱包地址

以本次为例：

dumpprivkey `qQhEewhVcdkWs53eYzJSjJhCoU8uBie1kJ`

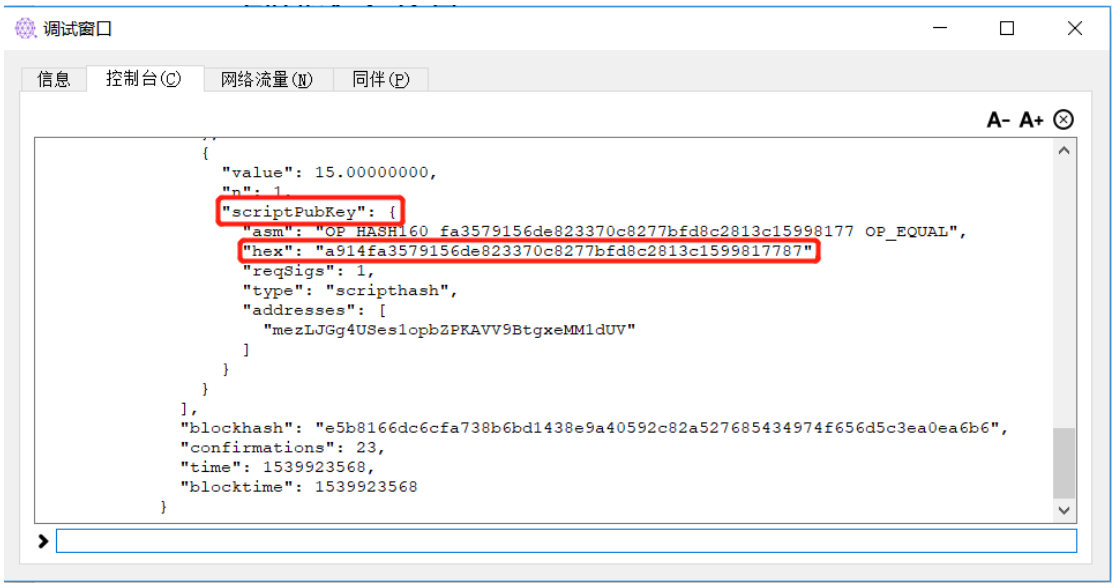
点击“enter”执行命令，获取对应地址的私钥；



客户端将返回对应钱包地址的私钥;

获取 scriptPubKey

在之前获取的余额信息中，找到**“scriptPubKey”**字段下的**“hex”**字段的内容;



按照一下的格式拼接签名命令:

signrawtransaction

交易的 hex 码 '''

```
[
  {
    "txid": "'之前返回的 txid'",
    "vout": '创建裸交易时的 vout 字段数据',
    "scriptPubKey": "'余额数据中 scriptPubKey 字段的数据'",
    "redeemScript": "'生成多签钱包地址时返回的多签钱包地址签名脚本'"
  }
]
```

''' '''

[

"'自己的私钥'"

]'''

以本次为例，拼接之后的命令如下：

signrawtransaction 02000000011036e36a2cba601c5867fee8ef9231eff5a6ee4da4a0db4e57813b05b571a7070100000000ffffffff018098cf58000000001976a914f7d443f7ab0cd41ad94509851f4cca04f14b2ee388ac00000000 '''

[

{

"txid": "'07a771b5053b81574edba0a44deea6f5ef3192efe8fe67581c60ba2c6ae33610'",

"vout": '1',

"scriptPubKey": "'a914fa3579156de823370c8277bfd8c2813c1599817787'",

"redeemScript": "'522103b517d716c792ee610ad052c2485318051769a6124eaa235e349849e25e81073b2102d2c882f6f6bbf2cdcc74e3d86cfdf2edad7e54c88254835534de2aa49698415c52ae'"

}

]

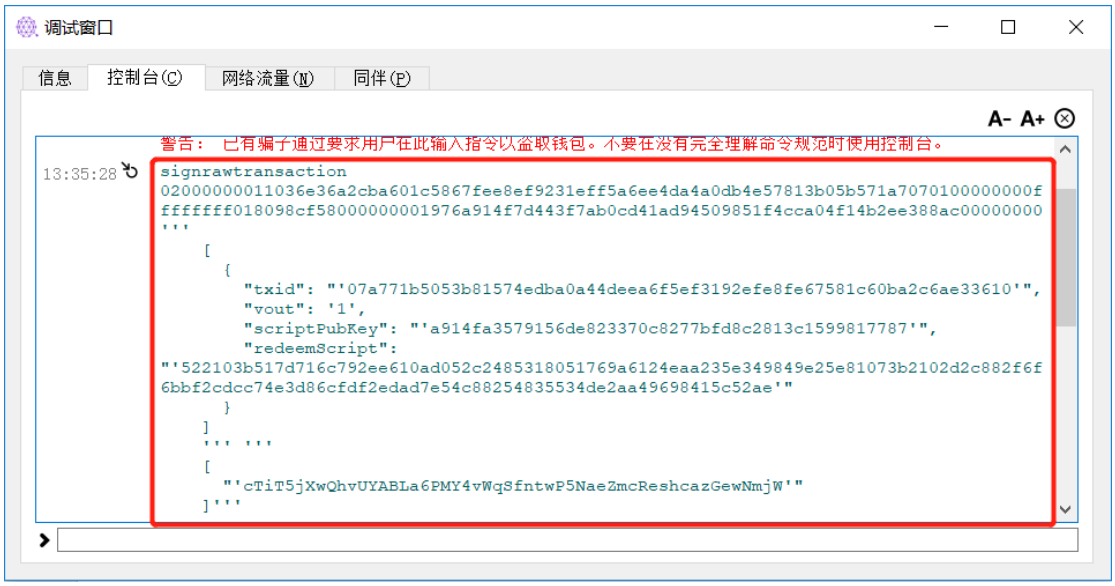
''' '''

[

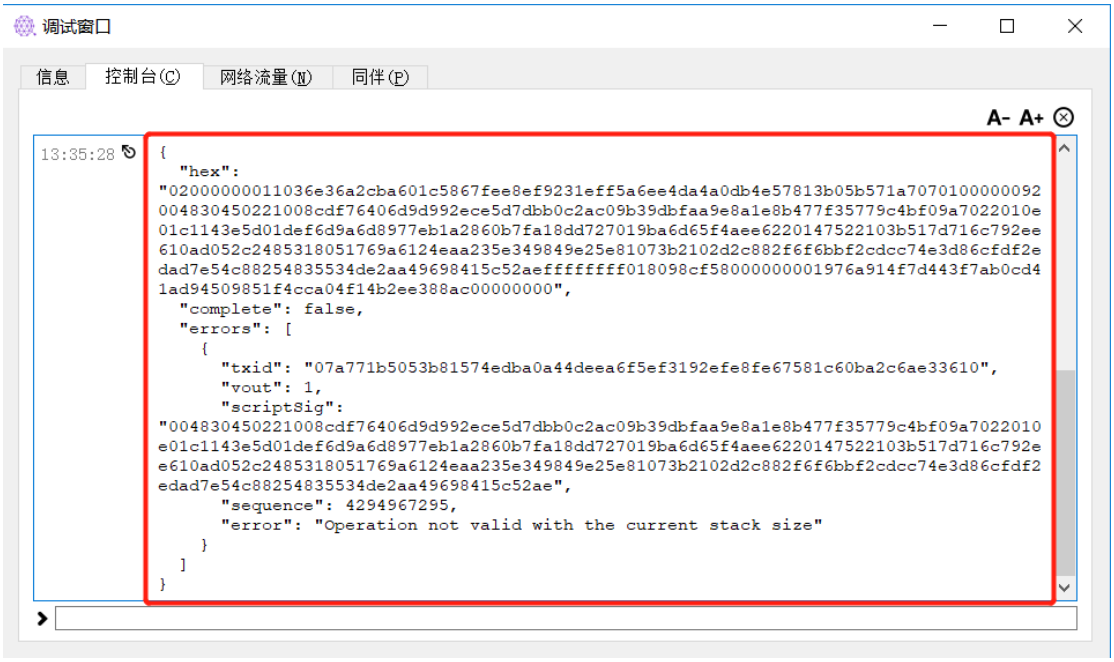
"'cTiT5jXwQhvUYABLa6PMY4vWqSfntwP5NaeZmcReshcazGewNmjW'"

]'''

点击“enter”执行命令，对交易进行一次签名；



客户端将返回完成一次签名的交易：



用户将返回的未完成交易复制到 txt 文档中保存，发送给 SPC 官网提供的邮箱，申请卫星签名即可。

2.5 返回签名结果

网站收到交易后，会将用户签名一次的交易上传到卫星签名节点，卫星签名节点签名后会将签名结果数据下发到地面。网站会将签名结果通过邮件的形式发送给用户在官网上绑定的邮件地址。

若签名成功，用户可以自行决定是否将交易广播到公网中。

2.6 广播交易

若用户想要将签名成功的交易广播到公网上，以本次实验为例，用户收到 SPC 官网邮箱发送的完整签名交易的 hex 码如下：

02000000011036e36a2cba601c5867fee8ef9231eff5a6ee4da4a0db4e57813b05b571a707010
00000db004830450221008cdf76406d9d992ece5d7dbb0c2ac09b39dbfaa9e8a1e8b477f3577
9c4bf09a7022010e01c1143e5d01def6d9a6d8977eb1a2860b7fa18dd727019ba6d65f4aee62
20148304502210080fd1f4f98ed9132cfaffc19166df2c7367da06138dafb5e6fcb86b6482a5eb3
022027ba8431d35ac47fff001e1a0ec1e2b0f17d725b1918206af7cf03120e260421014752210
3b517d716c792ee610ad052c2485318051769a6124eaa235e349849e25e81073b2102d2c882
f6f6bbf2cdcc74e3d86cfdf2edad7e54c88254835534de2aa49698415c52aeffffffff018098cf580
00000001976a914f7d443f7ab0cd41ad94509851f4cca04f14b2ee388ac00000000

在输入栏住输入：

sendrawtransaction + 交易的 hex 码

即：

sendrawtransaction
02000000011036e36a2cba601c5867fee8ef9231eff5a6ee4da4a0db4e57813b05b571a70701000000db004830450221008cdf76406d9d992ece5d7dbb0c2ac09b39dbfaa9e8a1e8b477f35779c4bf09a7022010e01c1143e5d01def6d9a6d8977eb1a2860b7fa18dd727019ba6d65f4aee6220148304502210080fd1f4f98ed9132cfaffc19166df2c7367da06138dafb5e6fcb86b6482a5eb3022027ba8431d35ac47fff001e1a0ec1e2b0f17d725b1918206af7cf03120e26042101475221 03b517d716c792ee610ad052c2485318051769a6124eaa235e349849e25e81073b2102d2c882f6f6bbf2cdcc74e3d86cfdf2edad7e54c88254835534de2aa49698415c52aeffffffff018098cf58000000001976a914f7d443f7ab0cd41ad94509851f4cca04f14b2ee388ac00000000

点击**“enter”**执行命令，将交易广播到公网上，若广播成功，客户端会返回交易的 txid；若广播失败，客户端返回错误信息。