

@title 区块链实验报告三

@author 18374480-黄翔

基础实验

实验一

1.1

regtest目录截图

```
(base) └─(kali@kali) - [~/bitcoin/alice/regtest]
└─$ ls
banlist.dat  blocks  chainstate  db.log  debug.log  fee_estimates.dat  mempool.dat  peers.dat  wallet.dat
```

思考题：

- 16Mib(signature cache)+16Mib(script execution cache) + 2Mib(block index database)+8Mib(chain state database) + 440.0MiB(in-memory UTXO set) + 286.1MiB(UNUSED mempool space) = 786.1Mib
- ```
2021-10-30 13:09:00 keypool added 2000 keys (1000 internal), size=2000 (1000 internal)
2021-10-30 13:09:00 keypool added 1 keys (0 internal), size=2000 (1000 internal)
```

最终保持了2001对密钥

- - 首先从regtest/peer.dat中读取P2P节点，初始化时由于没有该文件，读取失败，创建peer.dat文件
  - 开始尝试链接到网络中P2P节点信息，由于在回归测试模式下，只会寻找本地网络节点

#### 1.2

```
alice:
regtest = 1
port = 10086
addnode=127.0.0.1:10087
addnode=127.0.0.1:10088
rpcport=20086

bob:
regtest = 1
port = 10087
addnode=127.0.0.1:10086
addnode=127.0.0.1:10088
rpcport=20087

network:
regtest = 1
port = 10088
addnode=127.0.0.1:10086
```

```
addnode=127.0.0.1:10087
rpcport=20088
```

## 连通结果

```
2021-11-02 11:53:19 connect() to 127.0.0.1:10088 failed after select(): Connection refused (111)
2021-11-02 11:53:30 receive version message: /Satoshi:0.15.2/: version 70015, blocks=152, us=[::]:0, peer=0
2021-11-02 11:53:30 Leaving InitialBlockDownload (latching to false)
2021-11-02 11:54:20 connect() to 127.0.0.1:10087 failed after select(): Connection refused (111)
2021-11-02 11:54:20 receive version message: /Satoshi:0.15.2/: version 70015, blocks=152, us=[::]:0, peer=1
2021-11-02 11:55:21 connect() to 127.0.0.1:10087 failed after select(): Connection refused (111)
2021-11-02 11:56:21 connect() to 127.0.0.1:10087 failed after select(): Connection refused (111)
2021-11-02 11:57:22 connect() to 127.0.0.1:10087 failed after select(): Connection refused (111)
2021-11-02 11:58:22 connect() to 127.0.0.1:10087 failed after select(): Connection refused (111)
2021-11-02 11:59:19 receive version message: /Satoshi:0.15.2/: version 70015, blocks=152, us=[::]:0, peer=2
2021-11-02 11:59:23 receive version message: /Satoshi:0.15.2/: version 70015, blocks=152, us=[::]:0, peer=3
```

## 实验二

### 实验截图

- 为alice生成至少150BTC的可用余额

```
(base) └─(kali㉿kali)-[~]
└─$ alice-cli getbalance
2550.00000000
```

- - 首先查看bob和network账户地址

```
(base) └─(kali㉿kali)-[~]
└─$ bob-cli listaccounts
{
 "": 0.00000000
}
(base) └─(kali㉿kali)-[~]
└─$ bob-cli getaddressesbyaccount ""
[
 "muqq1aCjbZimbpQL7iZtcsRWRHjRL9e71J"
]
(base) └─(kali㉿kali)-[~]
└─$ network-cli listaccounts
{
 "": 0.00000000
}
```

```
(base) └─(kali㉿kali)-[~]
└─$ network-cli getaddressesbyaccount ""
[
 "mpAgKngkXXEgAJ9QTfU3CGkj6qez6T6MoR"
]
```

使用 getbalance 指令可以查询账户的余额。生成新的地址，尝试以上命令，我们可以发现余额中，这是由于比特币规定挖矿的收入只有让 alice 拿到第一笔 50BTC 收入的方法只有

- 交易

```
(base) └─(kali㉿kali)-[~]
└─$ alice-cli sendtoaddress "muqq1aCjbZimbpQL7iZtcsRWRHjRL9e71J" 2.5
ae2celad7c0f6308ae6ab534f5685e0a506ffecc8d9978b13e7accc0e2281099

(base) └─(kali㉿kali)-[~]
└─$ alice-cli sendtoaddress "mpAgKngkXXEgAJ9QTfU3CGkj6qez6T6MoR" 1.5
64a246beb622559e952d96160a8473a1c92e3364fb95f06b9bbf47715126d8fe
```

- 交易账单上链

```
(base) └─(kali㉿kali)-[~]
└─$ bob-cli getbalance
0.00000000

(base) └─(kali㉿kali)-[~]
└─$ bob-cli generate 1
[
 "27a8a125798f62e58f1b8918324bd75cff4b50e94d9ed23477db9c3748606167"
]

(base) └─(kali㉿kali)-[~]
└─$ bob-cli getbalance
2.50000000

(base) └─(kali㉿kali)-[~]
└─$ network-cli getbalance
1.50000000
```

- 区块原始数据

```
└─$ alice-cli gettransaction "ae2celad7c0f6308ae6ab534f5685e0a506ffecc8d9978b13e7accc0e2281099"
{
 "amount": -2.50000000,
 "fee": -0.00003840,
 "confirmations": 1,
 "blockhash": "27a8a125798f62e58f1b8918324bd75cff4b50e94d9ed23477db9c3748606167",
 "blockindex": 2,
 "blocktime": 1635853548,
 "txid": "ae2celad7c0f6308ae6ab534f5685e0a506ffecc8d9978b13e7accc0e2281099",
 "walletconflicts": [
],
 "time": 1635853449,
 "timereceived": 1635853449,
 "bip125-replaceable": "no",
 "details": [
 {
 "account": "",
 "address": "muqq1aCjbZimbpQL7iZtcsRWRHjRL9e71J",
 "category": "send",
 "amount": -2.50000000,
 "vout": 0,
 "fee": -0.00003840,
 "abandoned": false
 }
],
 "hex": "0200000001ffee18ee59ad59b2bad3279dc92d9a6367d632981dde4e129c990df400e8dc210000000049483045022100963cef9e0803607b55907ea569fc183fe184083062a621d7dbeb1c52cb105ee30220126f2b05987f9428e36015a7a1fcdb6f718cc12aa01a803b6895e1fa91c229f601fefffff0280b2e60e000000001976a9149d2395703e46222d771ae69c2944af14d03a0f388ac80301f1b010000001976a914df0177c472d4b9a497e5301f6830d002cee369fb88ac97000000"
}
```

## 实验三

```
"010000000156211389e5410a9fd1fc684ea3a852b8cee07fd15398689d99441b98bfa76e29000000
0000ffffff0280969800000000001976a914fdc7990956642433ea75cabdcc0a9447c5d2b4ee88a
cd0e89600000000001976a914d6c492056f3f99692b56967a42b8ad44ce76b67a88ac00000000"
```

a. 该交易有一笔输入，两笔输出，一笔转给 n4epMtJQQE2WkvjgspLnyoTww6z9qbvdWF 0.1BTC，另一笔转给 n16YP4DTiYAbYbdd7f3G7UjwCoCkwwheIiN 0.0989BTC

b. 数据量大小为119

# 扩展实验

## 拓展实验4.2

### 实验原理

多方签名交易有时候也被叫做 M-of-N 交易。M 指的是交易生效所需要的签名数量，N 指的是和本次交易相关的各方的总数量。只有当交易账单有足够的签名时，交易才能完成。

### 实验流程

建立四个节点alice, bob, network, samrito, 计划使用其中alice, bob, network作为2of3参与者，多签地址与samrito交易

### 节点建立

```
#alice
regtest = 1
port = 10086
addnode=127.0.0.1:10087
addnode=127.0.0.1:10088
addnode=127.0.0.1:10089
rpcport=20086
rpcuser=alice
rpcpassword=alice

#bob
regtest = 1
port = 10087
addnode=127.0.0.1:10086
addnode=127.0.0.1:10088
addnode=127.0.0.1:10089
rpcport=20087
rpcuser=bob
rpcpassword=bob

#network
regtest = 1
port = 10088
addnode=127.0.0.1:10086
addnode=127.0.0.1:10087
addnode=127.0.0.1:10089
rpcport=20088
rpcuser=network
rpcpassword=network

#samrito
regtest = 1
port = 10089
addnode=127.0.0.1:10086
addnode=127.0.0.1:10087
addnode=127.0.0.1:10088
rpcport=20089
rpcuser=samrito
rpcpassword=samrito
```

为使用方便，设置别名

```
#temp
alias alice-d='bitcoind -regtest -datadir=~/.bitcoin/alice'
alias alice-cli='bitcoin-cli -regtest -datadir=~/.bitcoin/alice'
alias alice-qt='bitcoin-qt -regtest -datadir=~/.bitcoin/alice'
alias bob-d='bitcoind -regtest -datadir=~/.bitcoin/bob'
alias bob-cli='bitcoin-cli -regtest -datadir=~/.bitcoin/bob'
alias bob-qt='bitcoin-qt -regtest -datadir=~/.bitcoin/bob'
alias network-d='bitcoind -regtest -datadir=~/.bitcoin/network'
alias network-cli='bitcoin-cli -regtest -datadir=~/.bitcoin/network'
alias network-qt='bitcoin-qt -regtest -datadir=~/.bitcoin/network'
alias samrito-d='bitcoind -regtest -datadir=~/.bitcoin/samrito'
alias samrito-cli='bitcoin-cli -regtest -datadir=~/.bitcoin/samrito'
alias samrito-qt='bitcoin-qt -regtest -datadir=~/.bitcoin/samrito'
```

## 2of3多签地址

首先为本次实验交易的alice, bob, network生成新的address

```
alice-cli getnewaddress
bob-cli getnewaddress
network-cli getnewaddress
```

四个节点接收地址如下

| node    | address                            |
|---------|------------------------------------|
| alice   | mkVukreQbzGzxJjF5FqnCtZTR5uGHMjfap |
| bob     | mgRPFLffmtLWXhHJGaUDuZLAseXvgY1LdQ |
| network | mtSF8ShGjc1vntzMpAN12Sa1PDufr75hAM |
| samrito | mzGVGQ71NveZfzYnSDT5VsjoX72NiS8F75 |

根据地址获得公私钥

```
validateaddress <address>
dumpprivkey <address>
```

```
validateaddress mkVukreQbzGzxJjF5FqnCtZTR5uGHMjfap
{
 "isvalid": true,
 "address": "mkVukreQbzGzxJjF5FqnCtZTR5uGHMjfap",
 "scriptPubKey": "76a91436a6182d1e18abbe7b2cf55b39211426b592346488ac",
 "ismine": true,
 "iswatchonly": false,
 "isscript": false,
 "pubkey": "03c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c256",
 "iscompressed": true,
 "account": "",
 "timestamp": 1635860074,
 "hdkeypath": "m/0'/0'/11'",
 "hdmasterkeyid": "667b178de6d78b39c5e193d6d14c527c5e962d81"
}
dumpprivkey mkVukreQbzGzxJjF5FqnCtZTR5uGHMjfap
cPjFuE8JpMwGM1SwhHDWufcyzZ6DDqZ6CXy3wqv3HpGdZVhQyQbe
```

```
dumpprivkey mkVukreQbzGzxJjF5FqnCtZTR5uGHMjfap
cPjFuE8JpMwGM1SwhHDWufcyzZ6DDqZ6CXy3wqv3HpGdZVhQyQbe
```

- alice
  - public key:  
03c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c256
  - private key:  
cPjFuE8JpMwGM1SwhHDWufcyzZ6DDqZ6CXy3wqv3HpGdZVhQyQbe
- bob
  - public key:  
02d7a32ccae3d059148e69b2696911fb6e2e333c86156774dbfb209781aeeda6d5
  - private key:  
cTr14CZsCkkBXbH4SgiAhkiwLLJb5So8QGYcfrQ3zwSiMFsmRvJF
- network
  - public key:  
0386893f2657abe3a4f793bfff369594ed48e134fecdd253a43371ace414317c1d6
  - private key:  
cUd8bzwQ4L11GwaLdinDGtTCMUPAQv4Hwv7Ch11frGwDaQTYQxj2

根据公钥获得2of3多签地址

```
createmultisig 2
'["03c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c256", "02d7a32ccae3d059148e69b2696911fb6e2e333c86156774dbfb209781aeeda6d5", "0386893f2657abe3a4f793bfff369594ed48e134fecdd253a43371ace414317c1d6"]'
{
 "address": "2N6ny6sb4PN93ZnUcZPuoZGUXBWAdXaEv6X",
 "redeemScript":
"522103c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c2562102d7a32ccae3d059148e69b2696911fb6e2e333c86156774dbfb209781aeeda6d5210386893f2657abe3a4f793bfff369594ed48e134fecdd253a43371ace414317c1d653ae"
}
```

```
createmultisig 2
'["03c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c256", "02d7a32ccae3d059148e69b2696911fb6e2e333c86156774dbfb209781aeeda6d5", "0386893f2657abe3a4f793bfff369594ed48e134fecdd253a43371ace414317c1d6"]'
```

返回结果：

```
{
 "address": "2N6ny6sb4PN93ZnUcZPuoZGUXBWAdXaEv6X",
 "redeemScript":
"522103c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c2562102d7a32ccae3d059148e69b2696911fb6e2e333c86156774dbfb209781aeeda6d5210386893f2657abe3a4f793bfff369594ed48e134fecdd253a43371ace414317c1d653ae"
}
```

此时，已经得到2of3的多签地址：2N6ny6sb4PN93ZnUcZPuoZGUXBWAdXaEv6X

向bob节点添加该多签地址作为发送地址，并导入该多签地址到接受地址方便分析：

```
addmultisigaddress 2
'["03c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c256", "02d7a32ccae3d059148e69b2696911fb6e2e333c86156774dbfb209781aeeda6d5", "0386893f2657abe3a4f793bfff369594ed48e134fecdd253a43371ace414317c1d6"]'
2N6ny6sb4PN93ZnUcZPuoZGUXBWAdXaEv6X
importaddress 2N6ny6sb4PN93ZnUcZPuoZGUXBWAdXaEv6X
null
```

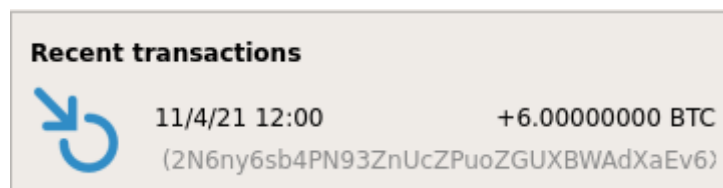
```
addmultisigaddress 2
'["03c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c256","02d7a32ccae3d059148e69b2696911fb6e2e333c86156774dbfb209781aeeda6d5","0386893f2657abe3a4f793bfff369594ed48e134fecdd253a43371ace414317c1d6"]'
importaddress 2N6ny6sb4PN93ZnUcZPuoZGUXBwAdXaEv6X
```

## 节点与多签地址交易

alice向多签地址发送BTC:

```
sendtoaddress 2N6ny6sb4PN93ZnUcZPuoZGUXBwAdXaEv6X 6
generate 3
```

由于之前已经将多签地址导入到bob的接收地址中，可以在bob账单上看到该笔交易



## 多签地址与第四方的交易

首先查找bob UTXOs

```
listunspent
```

```
{
 "txid": "e5c290f965d2c4ab078702b41e8a35a0f972ed94d44f38b380481412500e1bfff",
 "vout": 1,
 "address": "2N6ny6sb4PN93ZnUcZPuoZGUXBwAdXaEv6X",
 "account": "",
 "redeemScript":
"522103c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c2562102d7a32ccae3d059148e69b2696911fb6e2e333c86156774dbfb209781aeeda6d5210386893f2657abe3a4f793bfff369594ed48e134fecdd253a43371ace414317c1d653ae",
 "scriptPubKey": "a914949a84f94f0eaf51c289d070795c71a070bf192887",
 "amount": 6.00000000,
 "confirmations": 3,
 "spendable": false,
 "solvable": true,
 "safe": true
}
```

```
{
 "txid": "e5c290f965d2c4ab078702b41e8a35a0f972ed94d44f38b380481412500e1bfff",
 "vout": 1,
 "address": "2N6ny6sb4PN93ZnUcZPuoZGUXBwAdXaEv6X",
 "account": "",
 "redeemScript":
"522103c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c2562102d7a32ccae3d059148e69b2696911fb6e2e333c86156774dbfb209781aeeda6d5210386893f2657abe3a4f793bfff369594ed48e134fecdd253a43371ace414317c1d653ae",
 "scriptPubKey": "a914949a84f94f0eaf51c289d070795c71a070bf192887",
 "amount": 6.00000000,
 "confirmations": 3,
 "spendable": false,
 "solvable": true,
 "safe": true
}
```



建立raw transaction，目标地址为samrito，小费0.002BTC

```
createrawtransaction
' [{"txid": "e5c290f965d2c4ab078702b41e8a35a0f972ed94d44f38b380481412500e1bfff", "vout": 1, "scriptPubKey": "a914949a84f94f0eaf51c289d070795c71a070bf192887", "redeemScript": "522103c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c2562102d7a32ccae3d059148e69b2696911fb6e2e33c86156774dbfb209781aeeda6d5210386893f2657abe3a4f793bffff369594ed48e134fecdd253a43371ace414317c1d653ae"}] '
' {"mzGVGQ71NveZfzYnSDT5VsjoX72NiS8F75": 5.998} '
```

```
createrawtransaction '[{"txid": "e5c290f965d2c4ab078702b41e8a35a0f972ed94d44f38b380481412500e1bfff", "vout": 1, "scriptPubKey": "a914949a84f94f0eaf51c289d070795c71a070bf192887", "redeemScript": "522103c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c2562102d7a32ccae3d059148e69b2696911fb6e2e33c86156774dbfb209781aeeda6d5210386893f2657abe3a4f793bffff369594ed48e134fecdd253a43371ace414317c1d653ae"}]' '{"mzGVGQ71NveZfzYnSDT5VsjoX72NiS8F75": 5.998}'
0200000001ff1b0e5012144880b3384fd494ed72f9a0358a1eb4028707abc4d265f990c2e5010000000ffffffffff01c038c02300000001976a914cdae010f997aed0afed18286ceb7cc9895ddd65d88ac00000000
```

Alice用私钥对账单签名

```
signrawtransaction(_____)
{
 "hex":
 "0200000001ff1b0e5012144880b3384fd494ed72f9a0358a1eb4028707abc4d265f990c2e501000000b40047304402207042bd3518fd655ad87e2a9d5bc3ce5b18e8332e54fd7edf3636aed55b9829dd0220011bfcd2aede7b6891fa0fef237ff894a2df6dd5c29359b2b5f30b92a1b34a4014c69522103c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c2562102d7a32ccae3d059148e69b2696911fb6e2e33c86156774dbfb209781aeeda6d5210386893f2657abe3a4f793bffff369594ed48e134fecdd253a43371ace414317c1d653aefffffffff01c038c02300000001976a914cdae010f997aed0afed18286ceb7cc9895ddd65d88ac00000000",
 "complete": false,
 "errors": [
 {
 "txid": "e5c290f965d2c4ab078702b41e8a35a0f972ed94d44f38b380481412500e1bfff",
 "vout": 1,
 "witness": [
],
 "scriptSig":
 "0047304402207042bd3518fd655ad87e2a9d5bc3ce5b18e8332e54fd7edf3636aed55b9829dd0220011bfcd2aede7b6891fa0fef237ff894a2df6dd5c29359b2b5f30b92a1b34a4014c69522103c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c2562102d7a32ccae3d059148e69b2696911fb6e2e33c86156774dbfb209781aeeda6d5210386893f2657abe3a4f793bffff369594ed48e134fecdd253a43371ace414317c1d653ae",
 "sequence": 4294967295,
 "error": "Operation not valid with the current stack size"
 }
]
}
```

```
signrawtransaction
"0200000001ff1b0e5012144880b3384fd494ed72f9a0358a1eb4028707abc4d265f990c2e5010000000000ffffffffff01c038c0230000000001976a914cdae010f997aed0afed18286ceb7cc9895ddd65d88ac00000000"
' [{"txid": "e5c290f965d2c4ab078702b41e8a35a0f972ed94d44f38b380481412500e1bfff", "vout": 1, "scriptPubKey": "a914949a84f94f0eaf51c289d070795c71a070bf192887", "redeemScript": "522103c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c2562102d7a32ccae3d059148e69b2696911fb6e2e33c86156774dbfb209781aeeda6d5210386893f2657abe3a4f793bffff369594ed48e134fecdd253a43371ace414317c1d653ae"}] '
' ["cPjFuE8JpMwGM1SwhHDWufcyzZ6DDqZ6CXY3wqv3HpGdZVhQyQbe"] '
```

Network用私钥对账单签名

```
signrawtransaction(_____)
{
 "hex":
 "0200000001ff1b0e5012144880b3384fd494ed72f9a0358a1eb4028707abc4d265f990c2e501000000fc0047304402207042bd3518fd655ad87e2a9d5bc3ce5b18e8332e54fd7edf3636aed55b9829dd0220011bfcd2aede7b6891fa0fef237ff894a2df6dd5c29359b2b5f30b92a1b34a40147304402204891bb5d16d212fa3f522770a8a980e406f5c58cb66cd11caeaddfb84e9fcacf80220370be5bab8a9aabf76655bc5ad911d1df0b0f0ad1d7533ef91817b7fc3f54ba9014c69522103c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c2562102d7a32ccae3d059148e69b2696911fb6e2e33c86156774dbfb209781aeeda6d5210386893f2657abe3a4f793bffff369594ed48e134fecdd253a43371ace414317c1d653aefffffffff01c038c02300000001976a914cdae010f997aed0afed18286ceb7cc9895ddd65d88ac00000000",
 "complete": true
}
```

```
signrawtransaction
"0200000001ff1b0e5012144880b3384fd494ed72f9a0358a1eb4028707abc4d265f990c2e5010000
00b40047304402207042bd3518fd655ad87e2a9d5bc3ce5b18e8332e54fd7edf3636aed55b9829dd0
220011bfcdd2aede7b6891fa0fef237ff894a2df6dd5c29359b2b5f30b92a1b34a4014c69522103c3
10a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c2562102d7a32ccae3d0591
48e69b2696911fb6e2e333c86156774dbfb209781aeeda6d5210386893f2657abe3a4f793bfff3695
94ed48e134fecdd253a43371ace414317c1d653aefffffffff01c038c023000000001976a914cdae010
f997aed0afed18286ceb7cc9895ddd65d88ac00000000"
' [{"txid": "e5c290f965d2c4ab078702b41e8a35a0f972ed94d44f38b380481412500e1bfff", "vou
t": 1, "scriptPubKey": "a914949a84f94f0eaf51c289d070795c71a070bf192887", "redeemScrip
t": "522103c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c2562102d7a
32ccae3d059148e69b2696911fb6e2e333c86156774dbfb209781aeeda6d5210386893f2657abe3a4
f793bfff369594ed48e134fecdd253a43371ace414317c1d653ae"}] '
' ["cUd8bwQ4L11GwALdinDGtTCMUPAQv4Hwv7Ch11frGwDaQTYQxJ2"] '

```

Bob将签名完成的账单发送给第四方Samrito

```
sendrawtransaction
0200000001ff1b0e5012144880b3384fd494ed72f9a0358a1eb4028707abc4d265f990c2e50100000
0fc0047304402207042bd3518fd655ad87e2a9d5bc3ce5b18e8332e54fd7edf3636aed55b9829dd02
20011bfcdd2aede7b6891fa0fef237ff894a2df6dd5c29359b2b5f30b92a1b34a4014730440220489
1bb5d16d212fa3f522770a8a98e04e6f5c58cb66cd11caeeddffb84e9fc80220370be5bab8a9aabbf
76655bc5ad911d1df0b0f0ad1d7533ef91817b7fc3f54ba9014c69522103c310a8899c33639a18a11
ab440df8de3929f7f0be11253832dc00074f431c2562102d7a32ccae3d059148e69b2696911fb6e2e
333c86156774dbfb209781aeeda6d5210386893f2657abe3a4f793bfff369594ed48e134fecdd253a4
3371ace414317c1d653aefffffffff01c038c023000000001976a914cdae010f997aed0afed18286ce
b7cc9895ddd65d88ac00000000

```

此时账单详情：

```
{
 "txid": "d1064142c368d7af0bed05adf9e8e74267c390aa5da918d7c19c054815f1159b",
 "hash": "d1064142c368d7af0bed05adf9e8e74267c390aa5da918d7c19c054815f1159b",
 "version": 2,
 "size": 337,
 "vsize": 337,
 "locktime": 0,
 "vin": [
 {
 "txid": "e5c290f965d2c4ab078702b41e8a35a0f972ed94d44f38b380481412500e1bfff",
 "vout": 1,
 "scriptSig": {
 "asm": "0
304402207042bd3518fd655ad87e2a9d5bc3ce5b18e8332e54fd7edf3636aed55b9829dd0220011bf
cdd2aede7b6891fa0fef237ff894a2df6dd5c29359b2b5f30b92a1b34a4[ALL]
304402204891bb5d16d212fa3f522770a8a98e04e6f5c58cb66cd11caeeddffb84e9fc80220370be
5bab8a9aabbf76655bc5ad911d1df0b0f0ad1d7533ef91817b7fc3f54ba9[ALL]
522103c310a8899c33639a18a11ab440df8de3929f7f0be11253832dc00074f431c2562102d7a32cc
ae3d059148e69b2696911fb6e2e333c86156774dbfb209781aeeda6d5210386893f2657abe3a4f793
bfff369594ed48e134fecdd253a43371ace414317c1d653ae",

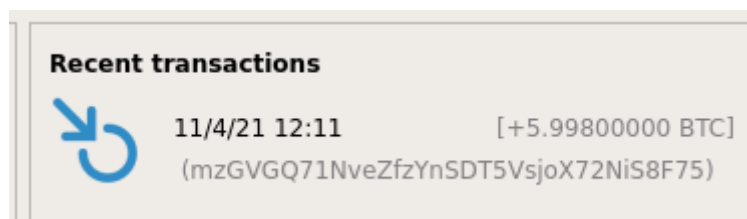
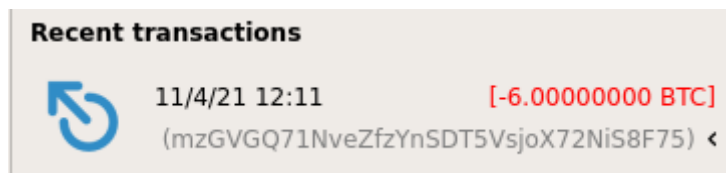
```

```

 "hex":
 "0047304402207042bd3518fd655ad87e2a9d5bc3ce5b18e8332e54fd7edf3636aed55b9829dd0220
 011bfcdd2aede7b6891fa0fef237ff894a2df6dd5c29359b2b5f30b92a1b34a40147304402204891b
 b5d16d212fa3f522770a8a98e04e6f5c58cb66cd11caeaddfb84e9fc80220370be5bab8a9aabbf76
 655bc5ad911d1df0b0f0ad1d7533ef91817b7fc3f54ba9014c69522103c310a8899c33639a18a11ab
 440df8de3929f7f0be11253832dc00074f431c2562102d7a32ccae3d059148e69b2696911fb6e2e33
 3c86156774dbfb209781aeeda6d5210386893f2657abe3a4f793bfff369594ed48e134fecdd253a433
 71ace414317c1d653ae"
 },
 "sequence": 4294967295
 }
],
"vout": [
 {
 "value": 5.99800000,
 "n": 0,
 "scriptPubKey": {
 "asm": "OP_DUP OP_HASH160 cdae010f997aed0afed18286ceb7cc9895ddd65d
OP_EQUALVERIFY OP_CHECKSIG",
 "hex": "76a914cdae010f997aed0afed18286ceb7cc9895ddd65d88ac",
 "reqSigs": 1,
 "type": "pubkeyhash",
 "addresses": [
 "mzGVGQ71NveZfzYnSDT5VsjoX72NiS8F75"
]
 }
 }
]
}

```

交易完成结果截图：



`getunconfirmedbalance`

5.99800000

`generate 6`

```

[
 "3bf8071373ae86a8bf683ffbd436d58edafd3f6a165c4ec7d4b15cecace53ecf",
 "0f587282991b839bf28eb5a0a34b80dcafe6df3a93dd67dcadc8034a2907f079",
 "18f8cba0f852075f6c3ef06f8897d530f0383618f5b92fa02720955bff51ed58",
 "4116db2879fbe736250529ef7b6c2d50b651aafa35bfd4bb3a77ebe4c73668ff",
 "61da6c6e84381a316fc83fec4a5f8d3dfcbef3d2fdfac84a49d9432dba22b976",
 "0aacd6c8cff5b9035e40c8cecf38cb34297ada905f7db7b29a5efc1a6efaec30"
]

```

`getbalance`

5.99800000

