

基于BCH实现发Token的功能

实现的思路是把Token的内容放在BCH脚本中, 依附在交易上, 通过BCH的交易来转移Token

扩展opcode: OP_TOKEN

添加rpc:

createtokenscript

createtokentx

signtokentx

gettokenbalance

listtokenunspent

按照以下步骤就可以实现Token的分发

1. 创建Token脚本

脚本内容是:

```
OP_TOKEN <tokenname> <tokensupply> OP_DROP OP_DROP OP_DUP OP_HASH160 <pubkey> OP_EQUALVERIFY  
OP_CHECKSIG
```

比如我想发代号为gon的代币10000个

```
./bitcoin-cli createtokenscript gon 10000
```

```
{  
  "address": "pzvcadtl6epnjenp4n6gvzum8tjp7gu5ng0ehkh2ps",  
  "token": "b303676f6e021027757576a914c8ad0da40b0ff475cd749a3aa455f5af3dc3f0f388ac"  
}
```

2. 向Token脚本中打BCH

```
./bitcoin-cli sentoaddress pzvcadtl6epnjenp4n6gvzum8tjp7gu5ng0ehkh2ps 1
```

交易上链后就实现了Token的发行, 在这个例子中地址 pzvcadtl6epnjenp4n6gvzum8tjp7gu5ng0ehkh2ps 内有10000个gon, 同时也有1个BCH

3. 查看Token数量

gettokenbalance 和 listtokenunspent 是用来查看Token余额的rpc

```
./bitcoin-cli gettokenbalance
```

```
[  
  {  
    "tokenName": "gon",  
    "tokenAmount": 10000  
  }  
]
```

```
./bitcoin-cli listtokenunspent
```

```
[  
  {  
    "txid": "d1ed9b0b375e39859266a31d6f89d12a1b8371f6a8a9159323bcfac57d54892d",  
    "vout": 0,  
    "address": "bchreg:pzvcadtl6epnjenp4n6gvzum8tjp7gu5ng0ehkh2ps",  
    "scriptPubKey": "a914998eb57fd643396661acf4860b9b3ae41f23949a87",  
    "redeemScript": "b303676f6e021027757576a914c8ad0da40b0ff475cd749a3aa455f5af3dc3f0f388ac",  
    "satoshi": 100000000,  
    "amount": 1.00000000,  
    "confirmations": 1,  
    "spendable": true,  
    "tokenName": "gon",  
    "tokenAmount": 10000  
  }  
]
```

4. 交易Token

假如我想往地址 qq493drnameufw7t2wc40tk57clut83gcg02aek8nm 上转移4000个gon,
qzrsn9dhyvpgcwvrc28vkaylqee47amnacp2mt6ayp 上转移6000个gon, 可以这么操作

```
./bitcoin-cli createtokentx  
'[{"txid":"d1ed9b0b375e39859266a31d6f89d12a1b8371f6a8a9159323bcfac57d54892d","vout":0}]'  
'[{"address":"qq493drnameufw7t2wc40tk57clut83gcg02aek8nm","amount":"0.5","tokenamount":"4000","tokenname":"gon"},  
{ "address":"qzrsn9dhyvpgcwvrc28vkaylqee47amnacp2mt6ayp","amount":"0.49","tokenamount":"6000","tokenname":"gon"}  
']
```

接着对createtokentx的交易进行签名

```
./bitcoin-cli signtokentx <hex>
```

广播上链后可以调用listtokenunspent再次查看token

```
./bitcoin-cli listtokenunspent  
[  
  {  
    "txid": "e563405c43f28cbde89269de89eed3c045792917a9ad6e0686eca91b0d1bafcc",  
    "vout": 0,  
    "address": "bchreg:qq493drnameufw7t2wc40tk57clut83gcg02aek8nm",  
    "scriptPubKey": "b303676f6e02a00f757576a9142a58b473eef3c4bbcb53b157aed4f63fc59e28c288ac",  
    "satoshi": 10000000,  
    "amount": 0.10000000,  
    "confirmations": 1,  
    "spendable": true,  
    "tokenName": "gon",  
    "tokenAmount": 4000  
  }  
]
```

例子中的第一个地址是我的地址, 所以可以看到4000gon在我的账上, 而6000gon在其它人的账上
重复第4步就可以像BCH交易一样转移Token