第六周周报

汪子龙

本周根据学长指出的问题，对上周的交易系统进行优化，修改了系统中存在问题的地方。具体修改的内容如下

一、优化的内容

1.取消地址绑定

上版本系统注册时用户需要绑定自己的地址，这样在系统的充值和提币操作只能和这个绑定的地址进行。对比已有的交易系统（如支付宝），绑定一个地址的设定不符合实际需求也很不方便，所以新版本取消了用户绑定地址的设定。用户提充值和提币可以对任意地址进行。

2.交易通过 hash 监控

上版本系统是通过遍历所有区块来监控交易信息，会占用大量资源和时间，新版本改为直接通过 hash 来监控交易。

3.提币时的费用问题

提币时的 gasPrice 由系统提供，系统主地址通过不断挖矿获取以太币，同时处理系统产生的交易打包上链。

4.修改回笼时无限转帐的 bug

上版本系统回笼时，每个账户地址会向主地址发起和账户余额等值的交易，从而实现以太币的转移，但这部分转移的以太币并没有进行记录，所以每次回笼操作所有账户地址都会转移和余额等值的以太币，造成回笼时无限转帐的 bug。新版本修复了此问题（见二、5.回笼）。

5.修改交易阻塞后无限提币的 bug

上版本系统发起提币操作后，如果交易被阻塞，用户在系统的余额就不会减少，此时用户可以发起无限次提币操作。新版本修复了此问题（见二、3.账户状态更新）。

二、各操作的具体变动

1.注册

注册时不再需要提供用户地址。系统直接从地址池中获取一个未被注册的账户，将助记词反馈给用户，并修改地址池对应账户的 status 字段。同时取消下之前的用户信息文件 users.txt。

地址池信息以 json 格式存放在 addresses.txt 中，列表中各键含义如下

address：系统中的账户地址

mnemonic：助记词

status：账户地址状态（-1 为主地址，0 为空闲地址，1 为已分配地址）


```
{
"accounts": [
{
"address": "0xc0093215beC3Cbb9522352DCB4E3fa8fd5b665D1",
"mnemonic": "inmate energy transfer mesh cinnamon educate slide latin veteran excess dance say scissors provide reveal link have caught orphan fruit can clog degree damp",
"status": "-1"
},
{
"address": "0x8bf8fb9Cfd048dE2645539F5007D12Ae6465623B",
"mnemonic": "bright best hello addict year awful salmon liar hurdle proof else today brick rose front dress digital base upon unaware foot gold crucial divorce",
"status": "1"
},
{
"address": "0x297fCA8450553A3C9103Dd410B59e79CDf6F4a0A",
"mnemonic": "bottom theme muscle dune trigger blossom apple wing inform weekend tourist lava rate seminar tribe twist help reduce enlist window reform shy sport update",
"status": "0"
},
```


2.充值/提币

充值时需要提供源地址的 keystore 文件路径和密码即可，发起充值交易后后将交易信息保存到账户信息文件中；提币时需要提供目的地址，发起提币交易后将交易信息保存到账户信息文件中。

```
please choose your option:
0: check balance        1: recharge     2: withdraw     3: exit
1
please input your key file path:
D:\Projects\GethProgram\chain_10\keystore\UTC--2020-07-31T04-44-41.315101100Z--b05c4d5cb3679b1b9e2a3e937806c84c06bb7df7
please input your password:
testuser
please input the value:
500000000000000000
transaction submitted:0x721b0067a8d5b3900bc7b2a1185433f1032fe354c2758947847161adb14708db
```

新版系统账户信息以 json 格式存放在相应文本文件中，各键含义如下：

addrbalance：账户地址中存储的用户余额

balance：持有账户地址的用户在系统中的余额

pendingbalance：持有账户地址的用户在系统中的余额（变化后）

transactions：所有的交易记录

transactions.amount：交易额度

transactions.hash：交易的 hash

transactions.status：交易状态，0 为阻塞，1 为完成

transactions.type：交易类型，0 为充值，1 为提币，2 为回笼

```
{
"addrbalance": "0",
"balance": "0",
"pendingbalance": "0",
"transactions": [
{
"amount": "500000000000000000",
"hash": "0x721b0067a8d5b3900bc7b2a1185433f1032fe354c2758947847161adb14708db",
"status": "0",
"type": "0"
}
]
}
```


3.账户状态更新（余额查询）

遍历账户信息文件中存储的所有阻塞的交易，根据 hash 值监控交易的状态。

```
please choose your option:
0: check balance        1: recharge     2: withdraw     3: exit
0
your balance is:
12500000000000000000
```

如果交易仍处于阻塞状态，且交易类别为：

提币，则修改 pendingbalance 值减去交易额度。

如果交易处于完成状态，且交易类别为：

充值，则修改 balance 和 addressbalance 值加上交易额度；

提币，则修改 balance 和 addressbalance 值减去交易额度；

回笼，则修改 addressbalance 值减去交易额度。

若所有交易都是完成状态，则同步 pendingbalance 值为 balance。


```
{
"addrbalance": "500000000000000000",
"balance": "500000000000000000",
"pendingbalance": "500000000000000000",
"transactions": [
{
"amount": "500000000000000000",
"hash": "0x721b0067a8d5b3900bc7b2a1185433f1032fe354c2758947847161adb14708db",
"status": "1",
"type": "0"
}
]
}
```


5.回笼

更新所有账户的状态后，从每个账户地址向系统主地址发起交易，额度为账户地址 addressbalance 的值。

```
please choose your option:
0: centralize   1: exit
0
refresh accounts done
0x414734d37be14a5ca0a5f97b4a7059e5c4298865ce8b198750fd9f9993f92dba
[0x8bf8fb9Cfd048dE2645539F5007D12Ae6465623B] transaction submitted: 0x4147
34d37be14a5ca0a5f97b4a7059e5c4298865ce8b198750fd9f9993f92dba
```