

API 文档.md

本文介绍如何基于呆马区块链开发智能合约程序

功能一览

1. 创建账号
2. 查询余额
3. 批量查询余额
4. 获取交易 ID (txnId)
5. 创建转账交易
6. 查询交易列表
7. 查询交易详情
8. 查询 token 详情

api 网址

接口地址：

<https://node5.daima.mobi>

在下面的内容中将用 **server** 来代表服务器地址

通用返回参数说明

参数	说明
status	状态标识符：0 未成功；1 成功；2 失败
info	接口返回信息描述，如错误信息等
data	接口返回数据

消息体签名说明：

所有的签名消息都需要首先通过接口 17. 获取交易 ID (txnid) 来获取 交易 ID (txid)、随机数 (nonce)。

消息体结构为多个参数拼接而成的字符串

转账消息体 (6. 创建转账交易)：txid + cc + from + to + amount 交易 tx、转账货币英文、转账人、收款人、转账数量 拼接而成的字符串。发布 token 消息体(10. 发布 token)：txid + cc + acc 交易 tx、发布 token 的英文名+发布人账户地址 拼接而成的字符串。

签名步骤：

1. 消息体转为字节数组，然后转为 16 进制字符串后，转小写，即是需要进行签名的消息体。
2. 消息体进行 sha3 的 Keccak 256 hash，得到 hash 消息。

3. 利用私钥进行 ECDSA 算法签名。

1.创建帐号：

接口路径: server/acc

请求方法: get

参数	是否必填	说明
psw	必填	账号密码

返回数据说明

字段	说明
info	钱包地址或错误信息
data	钱包 keystore 内容
data->address	钱包地址
data->crypto->ciphertext	加密后的账号私钥

返回样例

成功时

```
{"status": "1", "info": "0xF1D0dFbC41F3FD3aeD603bef2A80e6d2c6CB8Ec7", "data": {"address": "f1d0dfbc41f3fd3aed603bef2a80e6d2c6cb8ec7", "crypto": {"cipher": "aes-12
```

```
8-ctr","ciphertext":"51ea5e39c1faccca12f172e25c8446bcb772e86768c5b4b0c9135
b2257a4a300","cipherparams":{"iv":"e3873fb38fb0724d2c9d985af229fbaa"},"kdf":"
scrypt","kdfparams":{"dklen":32,"n":262144,"p":1,"r":8,"salt":"34f455a5464bf53a855
62a17a24919f4f980a8c3f63265096d06c251f1e43a06"},"mac":"0a59135abf7322ab5
3be6305b95b4fa0e5babb2affba09a2793d0e050040dd66"},"id":"c32f0c2a-5744-46
3d-812f-66bf7aaafb9f","version":3}}
```

失败时

```
{"status":0,"info":"参数 psw 不可空","data":""}
```

2.查询余额：

接口路径: server/qry

请求方法: get

参数	是否必填	说明
cmd	必填	固定填写 qryBal
args	必填	钱包地址
cc	必填	token 名称

返回数据说明

字段	说明
----	----

字段	说明
info	错误信息
data	钱包余额

返回样例

成功时

```
{"status":"1","info":"","data":999922179}
```

失败时

```
{"status":"0","info":"错误信息","data":""}
```

3.批量查询余额：

接口路径: server/bal

请求方法: get

参 数	是否 必填	说明
ar g	必填	钱包地址与 token 英文名对应的 Json 串
		格式 demo : {"clist":[{"cc":"dmc","addr":"0x5fe071ffc42eeb0535af2

参数	是否必填	说明
		b7dd96cdf8a89b8265d"}, {"cc": "dm", "addr": "0x5fe071ffc42eeb0535af2b7dd96cdf8a89b8265d"}]}
--	--	json 串字段说明：
cli	必填	对应的 json 串数组
cc	必填	token 英文名
addr	必填	查询账户地址

返回参数 data 说明：

返回的数据是一个 json 格式串，其中 key 是由参数串中的 cc+下划线"+"addr 拼接而成。

value 是当前查询地址的钱包余额

返回样例

成功时

```

{"status": "1", "info": "", "data": [{"dmc_0x5fe071ffc42eeb0535af2b7dd96cdf8a89b8265d": "996421.2700000000"}, {"dm_0x5fe071ffc42eeb0535af2b7dd96cdf8a89b8265d": "57500"}]}

```

失败时

```
{"status": "0", "info": "错误信息", "data": ""}
```

4. 获取交易 ID (txnId) :

接口路径: server/crtTx

请求方法: get

参数	是否必填	说明
cnt	选填	获取的数量

返回数据说明

字段	说明
status	1: 调用成功 0: 调用失败
info	错误信息
data	
data[n]->txId	交易 ID
data[n]->nonce	随机数

返回样例

成功时

```
{"status": "0", "info": "success", "data": [{"txnID": "f0c54cdab34fc366b2e959335b88a4d49dc8e0282ed56fcf2dadd717b8be911e", "Nonce": "DIaPpcvyD4HzXPRDGxuAyD9ma8rsX/Sp"}, {"txnID": "1bec40a2a1cb87641b3e73e7c67783bbe4a36c8c4f676fbdaec236ef11e75dd4", "Nonce": "bfpxru/vgWw3Rg4/L9r9HA57hqpdFsXn"}]}
```

失败时

```
{"status": "0", "info": "参数 cnt 非数字!", "data": ""}
```



5. 创建转账交易：

接口路径: server/ivk

请求方法: post

参数	是否必填	说明
cc	必填	token 名称
from	必填	转出地址
to	必填	转入地址
amo	必填	转账数量
sign	必填	签名
remark	选填	转账备注

参数	是否必填	说明
txid	必填	交易 ID
nonce	必填	交易随机数

返回数据说明

字段	说明
info	错误信息
data	



返回样例

成功时

```
{"status": "1", "info": "success", "data": "b31a2f170c7626d4a2405934fdad375688547a6cbaf3e66862f3ef2126730384"}
```

失败时

```
{"status": "0", "info": "出错了", "data": ""}
```



6.查询交易记录列表：

接口路径: server/trade

请求方法: get

参数	是否必填	说明
method	必填	固定填写 history
cc	选填	token 名称
acc	必填	钱包地址
page	必填	页数
number	必填	每页显示记录数(最多 100)
status	选填	记录类型(全部 0, 转出 1, 转入 2, 失败 3; 默认不填查询全部。)

返回数据说明

字段	说明
info	错误信息
data	json 数组
data[n]->out	转出账号
data[n]->in	转入账号

字段	说明
data[n]->txId	交易 id
data[n]->token	token 名称
data[n]->flag	交易类型 1 转出 0 转入
data[n]->sum	数量合计(含手续费)
data[n]->fee	手续费
data[n]->amount	交易数量(不含手续费)
data[n]->time	时间(字符串)
data[n]->authority_sign	司法鉴定编号(可能为空)
data[n]->type	交易类型 1 表示 token 发布扣费, 0 表示正常转账
data[n]->blockNum	所属块号
data[n]->remark	转账备注
data[n]->error	错误日志
data[n]->status	状态 0 处理中,1 成功,2 失败

返回样例

成功时

```
{"status": "1", "info": "", "data": [{"out": "0x5fe071ffc42eeb0535af2b7dd96cdf8a89b8265d", "in": "0x468a2acc04a9d01f462eae7e155d7a8bdf2694d4", "txId": "caab97fe743f0cc159187cdec48da0b77f32ee6803c52d3703b779781c63d9db", "token": "dm", "blockNum": "3319", "fee": "0", "amount": "100", "remark": "转账备注", "time": "2018-04-30 19:26:59", "status": "1", "error": "错误日志" }]}
```

失败时

```
{"status": "0", "info": "出错了", "data": ""}
```

7. 查询交易详情 :

接口路径: server/trade

请求方法: get

参数	是否必填	说明
method	必填	固定填写 txrst
tx	必填	交易 txid

返回数据说明

字段	说明
----	----

字段	说明
info	错误信息，如果 tx 查询不到，则展示 invalidTxid
data	json
data->out	转出账号
data->in	转入账号
data->txId	交易 id
data->token	token 名称
data->sum	数量合计(含手续费)
data->fee	手续费
data->amount	交易数量(不含手续费)
data->time	时间(字符串)
data->authority_sign	司法鉴定编号(可能为空)
data>type	交易类型 1 表示 token 发布扣费，0 表示正常转账
data->blockNum	所属块号
data->remark	转账备注
data->error	错误信息
data->status	0 正在处理中 1 交易成功 2 交易失败

返回样例

成功时

```
{"status": "1", "info": "success", "data": {"out": "转出账号", "in": "转入账号", "txId": "交易id", "token": "token 名称", "fee": "手续费", "amount": "交易数量", "time": "时间", "blockNum": "所属块号", "remark": "转账备注", "error": "错误信息", "status": "状态"}}
```

失败时

```
{"status": "0", "info": "参数 tx 不可空", "data": ""}
```

8. 查询 token 详情 :

接口路径: server/tkinfo

请求方法: get

参数	是否必填	说明
cc	必填	token 名称

返回数据说明

字段	说明
status	1: 调用成功 0: 调用失败
info	错误信息

字段	说明
data	json
data->name	token 中文名称
data->cc	token 英文名称
data->creator	token 创建者
data->total	货币总量
data->mineral	年化自动挖矿百分比
data->decimal	小数点精确位数
data->award	预挖数量
data->logo	token 的 logo(http url)
data->desc	token 说明
data->url	官方网址

返回样例

成功时

```
{
  "status": "1",
  "info": "success",
  "data": {
    "name": "货币",
    "chaincode": "token2",
    "creator": "0xbd0f20927c86ee910961d0e98db20d8760464",
    "desc": "",
    "total": "10000000",
    "url": "http://daima.mobi",
    "decimal": "10",
    "logo": "/"
  }
}
```

```
img?id=0xbd0f20927c86ee910961d0e98db20d8760464461_token_001.jpg", "miner  
al": "1000000", "award": "35", "email": "xxx@163.com"}}
```

失败时

```
{"status": "0", "info": "错误信息", "data": ""}
```