链问接口文档

|  |  |  |  |
| --- | --- | --- | --- |
| 2018-09-03 | 创建文档 | 李乐，王熙，徐卿 | V0.1.0 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[账户模块： 3](#_Toc523828592)

[1．创建账户 3](#_Toc523828593)

[2．登录账户 5](#_Toc523828594)

[3．moac兑换token 6](#_Toc523828595)

[4．token兑换moac 7](#_Toc523828596)

[5. 充值token 8](#_Toc523828597)

[6. 提币 8](#_Toc523828598)

[7.查询主链的MOAC和主链ERC20余额 9](#_Toc523828599)

[业务模块（全部子链方法）： 10](#_Toc523828600)

[1．链问问题列表 10](#_Toc523828601)

[2. 创建链问问题 11](#_Toc523828602)

[3. 回答列表页 12](#_Toc523828603)

[4. 创建回答 14](#_Toc523828604)

[5. 点赞 15](#_Toc523828605)

[6. 问题结算 15](#_Toc523828606)

[7. 查询子链token余额 17](#_Toc523828607)

[管理模块（TODO）： 18](#_Toc523828608)

[1. 设置合约地址 18](#_Toc523828609)

# 账户模块：

## 1．创建账户

方法名：registerUser(pwd)

说明：用户注册功能。

传入：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| pwd | 字符串 | 注册所设置的密码 |

返回：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| userAddr | 字符串 | 用户钱包地址 |
| keystore | 字符串 | 私钥加密串 |

返回示例：

**{**

**“userAddr”**:"0x764C0e7a183F9c5245f2904f66EED1c671"**,**

**"keystore"**: “{

**"version"**: 3**,**

**"id"**: "b7467fcb-3c8b-41be-bccf-73d43a08c1b7"**,**

**"address"**: "540f18196da5a533fa36577a81de55f0a2f4e751"**,**

**"Crypto"**: **{**

**"ciphertext"**: "78ed11b8b6bf29b00f52b42b8542df0e4a6ac07"**,**

**"cipherparams"**: **{**

**"iv"**: "4516579601d96695fe30ace985a9066f"

**},**

**"cipher"**: "aes-128-ctr"**,**

**"kdf"**: "scrypt"**,**

**"kdfparams"**: **{**

**"dklen"**: 32**,**

**"salt"**: "6276cfda7d40872352c801db5871e5a3368a8d0994"**,**

**"n"**: 1024**,**

**"r"**: 8**,**

**"p"**: 1

**},**

**"mac"**: "d889a5dc609c3f312a41394cc476"

**}**

**}”**

**}**

## 2．登录账户

方法名：loginUser(userAddr, pwd)

说明：用户登录功能。

传入：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| userAddr | 字符串 | 当前用户钱包地址 |
| pwd | 字符串 | 用户密码 |
| keystore | 字符串 | 私钥加密串 |

返回：

1 成功

0 失败

3．moac兑换token

方法名：buyMintToken(userAddr, value)

说明：主链方法。将MOAC原生币兑换成主链ERC20。

传入：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| userAddr | 字符串 | 当前用户地址 |
| value | 小数 | 传入的moac数 |

返回：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| refund | 小数 | 找零，当购买数大于可购买数时候，返回剩余的moac |
| isSuccess | 整数 | 1 |

返回示例：

**{**

**"refund"**:10**,**

**"isSuccess"**: 1

**}**

4．token兑换moac

方法名：sellMintToken(userAddr, value)

说明：主链方法。将主链的ERC20兑换成MOAC。

传入：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| userAddr | 字符串 | 当前用户地址 |
| value | 小数 | 传入的token数 |

返回：

1 成功

0 失败

5. 充值token

方法名：chargeMintToken(userAddr, value)

说明：主链方法。将主链ERC20兑换成子链原生币（异步）

传入：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| userAddr | 字符串 | 当前用户地址 |
| value | 小数 | 传入的moac数 |

返回:

1 成功

0 失败

6. 提币

方法名：redeemToken(userAddr, value)

说明：子链方法。将子链的原生币提到主链ERC20（异步）

传入：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| userAddr | 字符串 | 当前用户地址 |
| value | 小数 | 提取的token数 |

返回:

1 成功

0 失败

7.查询主链的MOAC和主链ERC20余额

方法名：getBalance(userAddr)

说明：获取主链MOAC和主链ERC20余额。

传入：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| userAddr | 字符串 | 当前用户地址 |

返回：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| moacBalance | 小数 | 当前墨客余额 |
| erc20Balance | 小数 | 当前erc20余额 |

返回示例

**{**

**"moacBalance"**:100.01**,**

**"erc20Balance"**: 10

**}**

# 业务模块（全部子链方法）：

1．链问问题列表

方法名：getTopicList(pageNum, pageSize )

说明： 获取链问题列表

传入：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| pageNum | 整数 | 当前页码 |
| pageSize | 整数 | 每页记录数 |

返回：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| topicHash | 字符串 | 问题hash |
| desc | 字符串 | 问题内容 |
| award | 小数 | 悬赏金额 |
| duration | 整数 | 持续时间，10的倍数 |

返回示例：

**[**

**{**

**"topicHash"**: "49aa38ce18bc541366c2ce4188f60f481"**,**

**"desc"**: "Are you ok?"**,**

**"award"**: 10**,**

**"duration"**: 60

**},**

**{**

**"topicHash"**: "8600dcs218bc541366c2ce4188f60fd3re"**,**

**"desc"**: "What is blockchain mean ?"**,**

**"award"**: 20.5**,**

**"duration"**: 60

**}**

**]**

2. 创建链问问题

方法名：createTopic(award, desc, duration)

说明：创建链问问题

传入：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| award | 小数 | 悬赏金额 |
| desc | 字符串 | 问题内容 |
| duration | 整数 | 持续时间，10的倍数 |

返回：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| topicHash | 字符串 | 问题hash |
| isSuccess | 整数 | 1 成功 0 失败 |

返回示例：

**{**

**"topicHash"**: "49aa38ce18bc541366c2ce4188f60f481"**,**

**"isSuccess"**: 1

**}**

3. 回答列表页

方法名：getSubTopicList(topicHash)

说明：详情页面，获取回答列表

传入：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| topicHash | 字符串 | 问题hash |
| pageNum | 整数 | 当前页码 |
| pageSize | 整数 | 每页记录数 |

返回：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| desc | 字符串 | 回答内容 |
| owner | 字符串 | 回答人address |
| voteCount | 整数 | 点赞数 |

返回示例：

[

**{**

**"desc"**: "I think it is good...."**,**

**"owner"**: "0x123ssfdfdf33rxvs3"**,**

**"voteCount"**: 1000

**},**

**{**

**"desc"**: "I think it is bad...."**,**

**"owner"**: "0x435345vdgt34545345"**,**

**"voteCount"**: 2000

**}**

**]**

4. 创建回答

方法名：createSubTopic(topicHash, desc)

说明：回答链问问题

传入：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| topicHash | 字符串 | 问题hash |
| desc | 字符串 | 回答内容 |

返回：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| subTopicHash | 字符串 | 回答hash |
| isSuccess | 整数 | 1 成功 0 失败 |

返回示例：

**{**

**"subTopicHash"**: "03438bc541366c2ce4188f60f481"**,**

**"isSuccess"**: 1

**}**

5. 点赞

方法名：approveSubTopic(voter, subTopicHash)

说明：同意该问题的答案

传入：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| voter | 字符串 | 当前登录人address |
| subTopicHash | 字符串 | 回答hash |

返回：

1 成功

0 失败

6. 问题结算

方法名：autoCheck(userAddr， subTopicHash)

说明：倒计时结束问题结算方法。调用后，会把该问题结算掉

传入：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| userAddr | 字符串 | 当前登录人address |
| subTopicHash | 字符串 | 问题hash |

返回：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| isSuccess | 整数 | 1 成功 0 失败 |

返回示例：

**{**

**"isSuccess"**: 1

**}**

7. 查询子链token余额

方法名：getMicroChainBalance(userAddr)

说明：查询子链token余额

传入：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| userAddr | 字符串 | 当前登录人address |

返回：

|  |  |  |
| --- | --- | --- |
| 参数名 | 类型 | 说明 |
| balance | 字符串 | token余额，单位个 |
| isSuccess | 整数 | 1 成功 0 失败 |

返回示例：

**{**

**“balance”**: 100.05**,**

**"isSuccess"**: 1

**}**

# 管理模块（TODO）：

1. 设置合约地址