公开正式网络-智能合约技术设计

1、背景

平台中实现公开正式网络合约的部署。

2、名词解释

3、设计目标

3.1、实现的功能

* 支付并创建合约账户
* 合约账户列表
* 合约创建
* 合约安装
* 合约状态更新---合约接口(mysql)

3.2、性能指标

4、系统环境

4.1、假设与其它模块联系

4.2、相关软件及硬件

4.3、模块限制

4.4、数据规模估计

5、设计思路及折衷

6、模块设计

6.1、模块流程图及说明

6.2、数据结构及说明

6.2.1 网络

使用一个预留的网络id表示公开网络

需要在文件  phplib/common/xuperserv/dao/BcNet.php 中添加:

const NET\_ID\_OF\_PUBLIC\_NET = 5;

6.2.2 链

链信息写入xchain\_blockchain表

相关的数据暂定

| **net\_id** | **5** |
| --- | --- |
| name |  |
| cn\_name | 公开正式网络 |
| bcoin\_amount | 0 |
| bcoin\_precision | 0 |
| creator\_address |  |
| symbol |  |
| version | 1 |
| token\_name |  |
| init\_total |  |
| award\_ratio |  |
| tech\_based | 4 |

6.3、算法描述（可选）

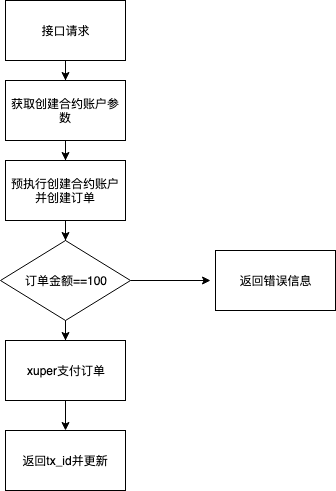
6.4、与其它模块的接口

6.4.4创建合约账户

处理和测试版一样由前端封装，需要实名认证+查询余额并比较是否>=100的逻辑，

依赖:实名认证、燃料余量信息接口

6.4.5 支付并创建合约账户



复用原接口，由net\_id区分正式网络

|  |  |  |  |
| --- | --- | --- | --- |
| **接口描述** | **创建公开正式网络下的合约账户** | | |
| 请求路径和类型 | /xuper/api/contractaccount /create | | |
| **请求参数** | **类型** | **是否必须** | **描述** |
| address | string | 是 | 用户地址 |
| net\_id | int | 是 | 网络id 5正式网络 |
| bcname | string | 是 | 链名称 |
| pwd | string | 是 | 交易密码 |
| tpl | string | 是 | 产品线名称 |
| sign | string | 是 | 签名 |
| **返回参数** | **类型** | **是否必须** | **描述** |
| code | int | 是 | 返回状态值 |
| msg | string | 是 | 返回状态说明 |
| data | json：  {"gas\_need":"", //需要消耗的gas "transaction\_no":"", //订单编号 "pay\_channel":"", //支付渠道 "callback\_url":"", //@deprecated 兼容旧接口  "pay\_url":"",// 支付链接  "account":"", //合约账户  } | 是 | code=0时的返回该值 |

6.4.7 合约账户列表 (查询区块链)

复用原接口，由net\_id区分正式网络

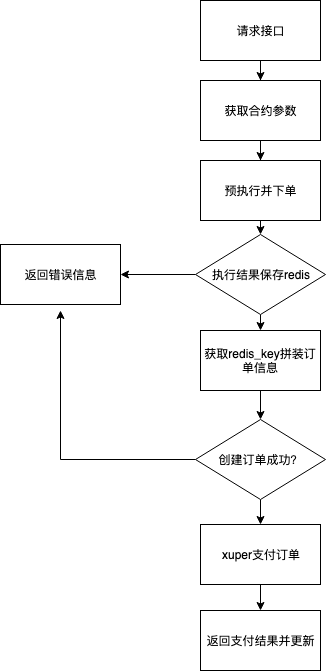
|  |  |  |  |
| --- | --- | --- | --- |
| **接口描述** | **获取一个用户的公开正式网络合约账户列表** | | |
| 请求路径和类型 | /xuper/api/contactaccount/list | | |
| **请求参数** | **类型** | **是否必须** | **描述** |
| address | string | 是 | 用户地址 |
| net\_id | int | 是 | 网络id |
| bcname | string | 是 | 链名称 |
| tpl | string | 是 | 产品线 |
| sign | string | 是 | 签名 |
| **返回参数** | **类型** | **是否必须** | **描述** |
| code | int | 是 | 返回状态值 |
| msg | string | 是 | 返回状态说明 |
| data | Json:  {      "list":["acount1", "acount2"]  } | 否 | code=0时返回 |

6.4.7 创建智能合约

复用公开测试网络的接口， 通过net\_id 区分

|  |  |  |  |
| --- | --- | --- | --- |
| **接口描述** | **合约创建** | | |
| 请求路径和类型 | /xuper/api/contract/create | | |
| **请求参数** | **类型** | **是否必须** | **描述** |
| address | string | 是 | 用户地址 |
| net\_id | int | 是 | 正式网络net\_id =5 |
| contract\_name | string | 是 | 合约英文名 |
| bcname | string | 是 | 区块链名称 |
| account | string | 是 | 合约帐号 |
| language | int | 是 | 智能合约的语言版本3：wasm字节码 |
| save\_type | int | 是 | 保存类型2:提交 |
| contract\_cnname | string | 是 | 合约中文名 |
| version | string | 是 | 合约版本 |
| description | string | 否 | 合约描述 |
| compiler\_output | string | 是 | wsam文件bos地址 |
| tech\_based | int | 是 | 4 xuper3.X |
| tpl | string | 是 | 产品线 |
| sign | string | 是 | 产品线签名 |
| **返回参数** | **类型** | **是否必须** | **描述** |
| code | int | 是 | 返回状态值, 为0时创建成功 |
| msg | string | 是 | 返回状态说明 |
| data | string | 否 | {"info":"success"} |

6.4.11 合约安装



|  |  |  |  |
| --- | --- | --- | --- |
| **接口描述** | **合约预安装接口** | | |
| 请求路径和类型 | /xuper/api/contract/preinstall | | |
| **请求参数** | **类型** | **是否必须** | **描述** |
| address | string | 是 | 用户地址 |
| net\_id | int | 是 | 网络id |
| bcname | string | 是 | 链名称 |
| contract\_name | string | 是 | 合约名称名 |
| account | string | 是 | 合约账号 |
| version | string | 是 | 合约版本 |
| args | string | 是 | 初始化参数 json |
| tpl | string | 是 | 产品线 |
| sign | string | 是 | 产品线签名 |
| **返回参数** | **类型** | **是否必须** | **描述** |
| code | int | 是 | 返回状态值, 为0时创建成功 |
| msg | string | 是 | 说明 |
| data | string | 否 | {      "gas\_need":1000, //安装需要消耗      "transaction\_no":1111, // 订单id      "pay\_channel": 4,   //支付通道 xuper  "callback\_url":"xxxxxx",  } |

7、风险评估及对其它模块/系统影响（可选）

8、设计评审意见

| **No** | **问题描述** | **提出人** | **处理方式/说明** | **状态** |
| --- | --- | --- | --- | --- |
| 1 |  |  |  | Open |
| 2 |  |  |  | Close |
| 3 |  |  |  |  |

9、附件及参考资料