

迅雷链测试接入流程

测试接入流程

注册开发者账号

1. 开发者根据测试接入 API 调用 *开发者注册* 接口。
2. 测试平台根据开发者接口提交的邮箱地址(必须)和回调地址(非必须)，向开发者邮箱发送一份邮件，内含 service_id 和 secret。
3. **后续所有的测试接口请求，都需要带上此邮箱地址以及由邮箱地址、service_id 和 secret 拼接字符串的 md5 值。测试平台的所有接口都将校验此 md5。**
4. 此接口不提供额外查询功能，如开发者信息遗失，需走客服流程找回。

调用充值接口

1. 开发者根据测试接入 API 调用 *测试账号充值* 接口。
2. 调用充值接口成功后，测试平台会向接口所提交的 address 账户转入 1 个链克。
3. 测试平台的区块链环境完全独立，所以此测试链克只能用于测试环境，转入其他区块链环境无效。
4. **每个 email 地址每天最多发起 10 此转账申请。**

开发合约应用和上层业务

1. 开发者开发合约应用，并通过上层业务(App, H5 等实现)功能封装对合约的调用。
2. 合约的开发可参考《迅雷区块链大赛合约开发指南》。

部署合约到迅雷链测试环境

1. 迅雷链测试和正式环境不提供直接 RPC 连接执行合约发送交易的过程，合约的发布和调用都需要通过调用 API 接口实现。
2. 开发者通过调用合约发布接口，部署合约到迅雷链测试环境。
3. **由于合约的部署是由平台方执行的，所以在合约的 constructor 方法里，避免使用 msg.sender，如有权限和调用者限制需用到 msg.sender，可通过参数传入用户的 address 代替。**

例：

```
contract HelloWorld {
  address owner;
  constructor(address ownerArg) public {
    //owner = msg.sender; 使用 ownerArg 代替 msg.sender
    owner = ownerArg;
  }
}
```

4. 发布合约 API 接口需要提供合约 bytecode 和 params，bytecode 为合约编译的 bytecode，params 是构造函数的参数经过 sign 后可直接拼接在 bytecode 后用于部署的编码。

这里可以使用 [remix](http://remix.ethereum.org/#optimize=false&version=soljson-

v0.4.23+commit.124ca40d.js) create 合约，控制台里的这一条交易的 detail 里 input 即合约部署的 data。但为了兼容测试环境和正式环境的输入，需要将 input 里的合约 bytecode 和最后的 params sign 分开传入。

```
![constructor](./img/constructor.png)
```

调用合约方法

合约调用当前分为两种形式：通过链克口袋 App 扫描二维码发送合约调用的交易；通过业务方 App 唤起链克口袋发起合约调用的交易。

唤起链克口袋

根据 API 实现业务 APP 唤起链克口袋，并传入合约调用的交易。

****从玩客云调用链克口袋****

otst://contract/?tx-
data=ZGVzYz3nlXLlvbFYWFhYJnRvPTB4MTIzNDU2Nzg5MDEyMzQlNjc4OTAm dmFsdWU9MTIzLj
QwJmdhc2xpbWl0PTUwMDAwJmRh dGE9MHgwMTAyMDMwND AwMDAwMDAwMDAwMDAwMD
AwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDEmc2lnbj0wNEI3QTU1Qz Q3NDQwRDk4NU E0NDgzNkZENTVFQkVC Nw==&resource=d2
t5&x-source=wky&x-success=wky://x-callback-url/contractSuccess&x-error=wky://x-callback-
url/contractError&x-cancel=wky://x-callback-url/contractCancel&&cb-data=base64 编码后的回调透传参
数

****具体解析****

1. 合约执行业务 otst://contract

1. 源 app 名字，resource=d2t5, 解码后是 wky
2. 源 app 回调前缀，x-source=wky
3. 成功回调 &x-success=wky://x-callback-url/contractSuccess
4. 失败回调 &x-error=wky://x-callback-url/contractError
5. 取消回调 &x-cancel=wky://x-callback-url/contractCancel
6. 回调时，直接回传 &cb-data=abcdefg
8. 交易信息 tx-

data=ZGVzYzNlLXlvBFYWFhYJnRvPTB4MTIzNDU2Nzg5MDEyMzQ1Njc4OTAmdmFsdWU9MTIzLj
QwJmdhc2xpbWl0PTUwMDAwJmRhGE9MHgwMTAyMDMwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDEmc2lnbj0wNEI3QTU1QzQ3NDQwRDk4NUUE0NDgzNkZENTVFQkVCNW==

data=ZGVzYzNlLXlvBFYWFhYJnRvPTB4MTIzNDU2Nzg5MDEyMzQ1Njc4OTAmdmFsdWU9MTIzLj
QwJmdhc2xpbWl0PTUwMDAwJmRhGE9MHgwMTAyMDMwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDEmc2lnbj0wNEI3QTU1QzQ3NDQwRDk4NUUE0NDgzNkZENTVFQkVCNW==

****解码后包含如下信息****

1. 支付地址 &to=0x12345678901234567890
2. 支付玩客币数量 &value=123.4

3. 最大支付费用 &gaslimit=50000

4. 调用代码

[illegible]

5. 用于标题 &desc=电影 XXXX

6. sign 交易签名 &sign=04B7A55C47440D985A44836FD55EBEB7

****返回（成功）****

wky://x-callback-url/contractSuccess?cb-

data=abcdefg&hash=0x12345678901234567890123456789012&data=base64 编码后的回调透传参数

****返回(失败)****

wky://x-callback-url/contractError?x-source=otc&errorCode=1&errorMessage=message&data=base64 编码
后的回调透传参数

****返回(取消)****

wky://x-callback-url/contractCancel?x-source=otc&data=base64 编码后的回调透传参数

****合约调用****

合约调用指需要改变合约状态的函数调用，执行函数的同时也可以转账到合约账户。用户界面输入用户请求后，触发合约调用。

```
![contract interactive](./img/contract_interactive.png)
```

****步骤如下：****

1. 第三方应用接受用户输入，启动合约调用流程
2. 用户使用链克区块链分配的 `service_id`，到区块链后台请求，分配一个 `prepay_id`。
3. 后台收到请求后，产生一个 `prepay_id` 给第三方应用。
4. 第三方应用打包交易，主要包括合约地址、`gas_limit`、转账金额、执行的函数和参数编码(ABI)、签名等信息。
5. 唤醒链克钱包 app，将交易信息发送给链克口袋。
6. 链克口袋打包交易发送给区块链交易处理中心，最终交易转发给区块链服务器处理。
7. 返回请求结果给链克口袋。
8. 链克口袋将结果通知给第三方 APP。(合约调用交互完成)

****第三方应用可以同步数据到其后台服务。（第三方功能）****

区块链后台将合约调用请求处理完后，如果用户有填写回调信息，回调中心通知第三方应用后台。第三方应用界面会同第三方应用后台同步信息，展示交易后的结果。