简介

研究比原链已经一年了，用比原链做了几个dapp，而且最近还做了一个基于他们插件钱包的dapp，总结了一些遇到的坑，还有一些技术细节，接下来我会分成三章，从dapp设计架构上，到深入到源码分析去帮各位介绍一下比原链的dapp，还有分析比原官方最近发布的dapp的架构。

Dapp架构设计

这个是所有工作的基础，从看完比原链源码使用过比原的钱包后，我们就在思考比原链的dapp如何做，应该说是区块链应用应该如何做，我们之前尝试过用以太坊、比特币、超级账本去做dapp。先总结一下区块链dapp的痛点：

1. 没办法保证上链前数据的真实性；
2. Tps很低；
3. 接入成本高，需要自己搭建节点；

我现在总结了两个基于比原链的dapp架构方案：（如果有新版或者比较好的解决方案欢迎交流）

Dapp肯定离不开复杂的业务，所以肯定会用到比原链的智能合约，以下方案都支持智能合约。

`

1. 搭建区块链node

其实就是自己搭建个节点，然后应用直接调用节点提供的接口，完成了区块链的业务内容，比原链的源码整合了钱包功能，搭建也比较方便，几句代码就可以搭建完了，但是这样的业务视乎不大合理，因为这种后端整合比原源码钱包(以下称为“pc钱包”)的方式，相当于把所有的账户信息都托管给dapp，其实就是一个集中的官方的钱包，所有的账户都归官方管，这样会有中心化问题，最后会被怀疑用不用这个区块链是否有必要。

比原链自己有一套用户的模块，用户可以使用pc钱包、客户端钱包、手机钱包等，自己的用户信息可以自己备份，交易信息全部公开全部可以到区块链浏览器里面查到。这个方案只是主要实现了交易上链。

当然其实还是可以变通一下，就是说把PC钱包的所有接口在dapp实现一次，然后结合业务，但是比原的源码是会不断更新，还要随着它的版本更新，然后更新自己的应用，显然不实际。

说一下里面的坑：

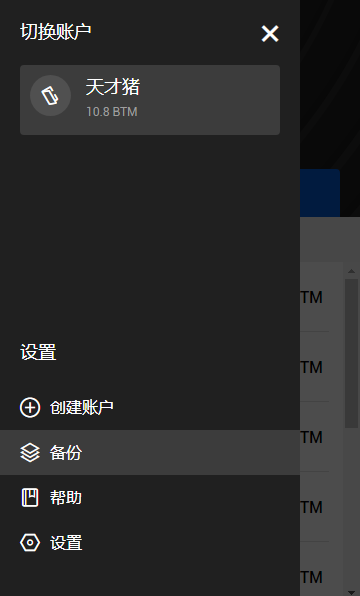
1. 账户BTM问题，这种方案每个dapp账户底层都要绑定一个钱包的用户，可以展现地址用户自己充值、直接在dapp里面充值、完成任务派送这些等，但是初始化账户拥有BTM需要有时间过程，正常应用这样的体验，早就让用户关闭了。
2. UTXO问题，比原链是基于utxo未花费输出交易模型，当自己的UTXO参与的交易没有确定是无法使用的，但是dapp这里绑定的用户，不能保证他有足够多的UTXO，除非自己转账的时候让他拆分，否则会类似单线程的操作，也是比较慢。
3. 用户无法获取自己的私钥，在比原链PC钱包，是一套私钥，派生多个账号这样，就是说一个钱包就一套私钥，这个不能给用户。这样又违背了区块链的去中心化的问题。

总的来说，这个方案是单纯保证了dapp交易上链，但是各方面明显不足。

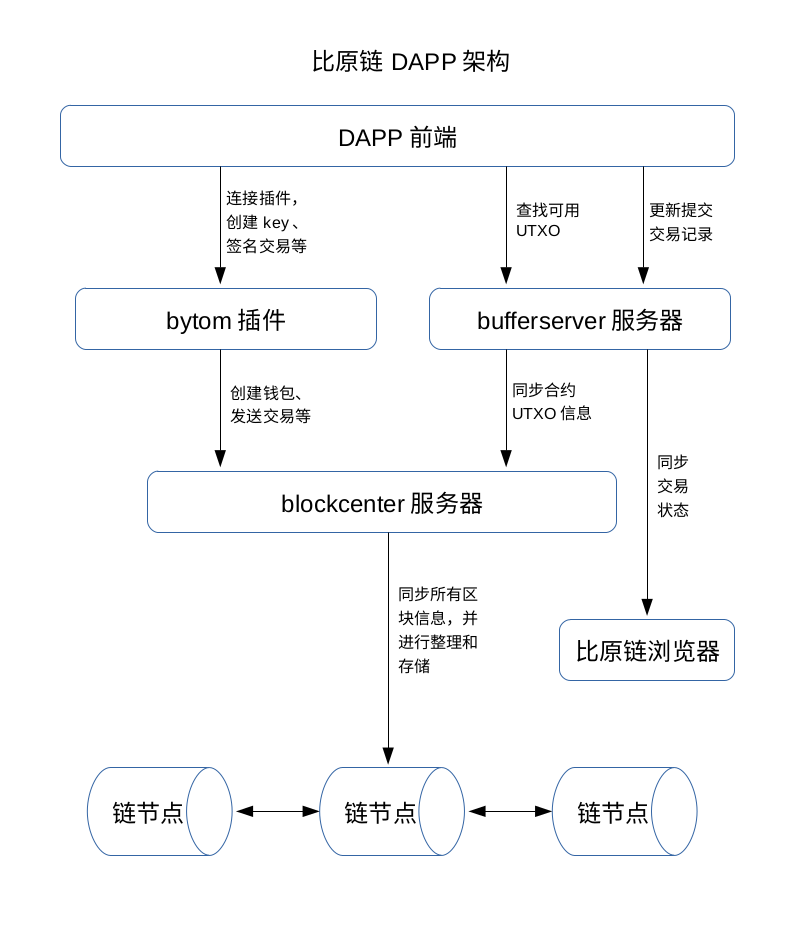
1. **插件钱包（Byone）方案**

这个方案是今年比原链推出的dapp新型的解决方案，有解决到方案一的痛点，这个也是我比较提倡的方案，现在比原链的智能合约功能已经非常强大，如果做复杂的dapp，用这个方式比较好。

简单来说就基于chrome开发了一个插件钱包，安装完插件，用户直接可以创建账户，使用账户的转账功能，里面有BTM的转账功能，账户的备份功能....是比较完整的一个钱包，这个钱包最大的作用就是包含了丰富的开发者api，可以支持开发者去实现智能合约交易。



我们重点说一下这个结构的技术原理，如图



1. Dapp前端，就是前端页面，插件钱包是基于chrome的，所以这里代表的就是新的页面集成了插件钱包（Byone）的api。
2. Byone，就是在chrome应用商店里面可以搜索到，点击安装就行，当前版本是2.0.0，非常好用。
3. Bufferserver服务器，官方提供demo里面这模块属于缓存服务器，其实这个应该改成Dapp后端，实际业务逻辑还有很多需要后端辅助，例如排行榜、非BTM比原资产交易等。（这块后面重点开一章去说清楚），现在理解称为后端就可以。
4. Blockcenter，其实就是官方提供的服务，直接提供接口可以触发比原链的交易功能，这样解决了上面的方案，避免需要自己搭建node节点，让dapp开发者更加容易接入。

总结：

两套方案里面，方案一个人认为属于早期的方案，随着比原链的发展，我们可以适当了解有助于我们理解比原链的架构设计，而且在方案二里面，也一定要用到PC钱包，它可以协助我们开发者提高开发效率100倍，没有夸张，是100倍。

插件钱包现在还在推广还有完善当中，不过功能已经非常成熟了，所以Dapp开发者赶紧抓紧去使用来开发属于自己的dapp吧。

下一章我们重点说一下Dapp的开发流程。以及遇到的一些坑，还有粘贴源码。