第28讲 | 弄懂数字货币交易平台（二）

2018-05-28 陈浩

深入浅出区块链 进入课程 >

讲述：黄洲君
时长 09:25　大小 4.32M

在上一篇文章中，我们介绍了数字货币交易平台的概念，那么今天我们就来重点聊聊数字货币交易平台的技术。如果你有过设计或实现传统金融交易系统的经验，那么你阅读本篇就会更加容易。

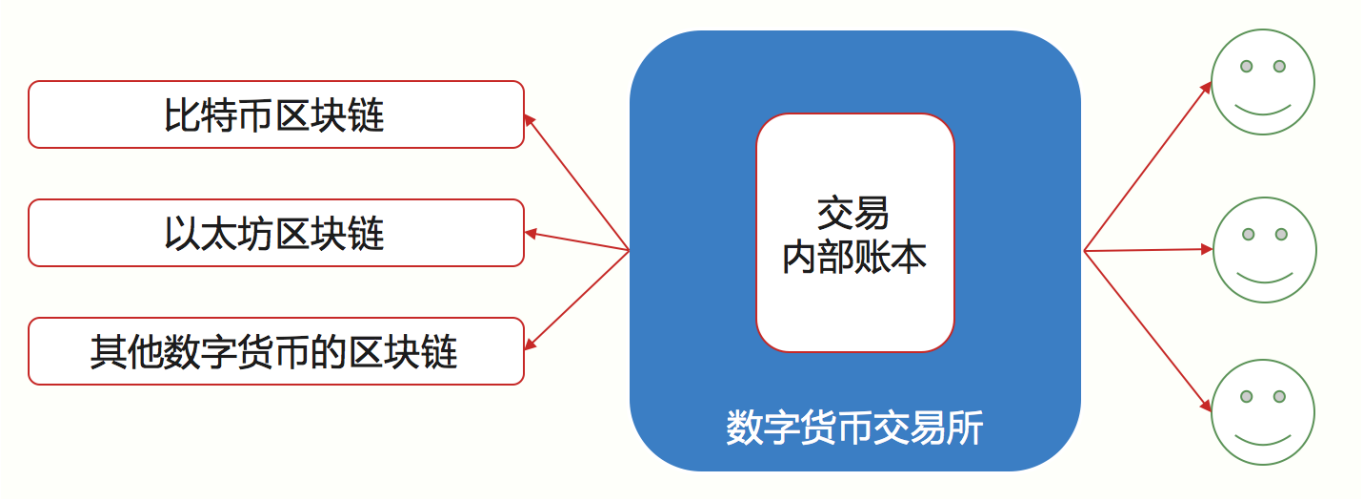
由于中心化交易所是主流应用，所以今天我主要介绍的是中心化模式下的数字货币交易平台。

两套账本

数字货币交易平台的技术基本沿用了金融交易技术中的系统架构，只是把原来针对法币和证券（或平台代币）的部分，也就是我们通常称作资金管理系统的部分，完全替换为针对数字货币的数字货币管理系统，换句话说，就是换了一套内部账本。

然而我们知道，区块链本身也是用来记账的，也算作一种金融账本，所以一套内部账本，一套区块链本身的账本，这里就出现了两套账本，如何管理这两套账本，就是资金管理系统的首要任务。

如下图所示。由于中文语境下的交易有多重含义，本篇会用英文单词标注，以示区别。



(图示 数字货币交易所)

解释一下这张图，图的左边表示了多个区块链账本，右边的数字货币交易所有自己的内部账本，这两套账本是独立的。

交易所内部的账本记录的是交易 Trade，这个交易是由用户挂单，接着被撮合引擎撮合成交而产生的，而区块链账本上的交易 Transaction，是当且仅当用户发起充币提币请求并被执行时，才会产生的。

这两种交易都用了中文“交易”来表示，但是它们所属的语境不同，前者的交易表示的是金融交易语境下的资产交换，也就是 Deal；后者表示的是区块链上的技术概念，表示资产转移的一次记账过程，上述特意用英文以表区别，希望你能够区分。

数字货币交易所包含哪些系统模块

一个数字货币交易所的后端其实至少有四部分构成：Web 业务逻辑系统、交易撮合系统、运营后台管理系统、资金管理系统。资金管理系统其实就是刚才说到的内部账本。

1. Web 业务逻辑系统：这个模块通常包含了用户账户模块、登录网关、账户安全管理、KYC 认证、行情推送等等，这个模块更偏向用户，也与通常的电商账户系统十分类似。
2. 交易撮合系统：这个模块是一个交易所的核心模块，为所有的用户提供订单撮合。
3. 运营后台管理：这个模块是一个交易所运营人员使用的系统，交易所内部人员才能访问。
4. 资金管理系统：这里的资金管理其实包含了三部分，第一部分是法币的支付网关，可能需要对接银行或第三方支付机构；第二部分就是数字货币钱包管理，它提供了大部分主流数字货币的支付功能；第三部分是用户持仓信息，所谓持仓就是用户持有多少数字货币，这个是记录在数据库中的，不需要与区块链保持一致，但是要求交易所的总账是平的。

各自模块的特征

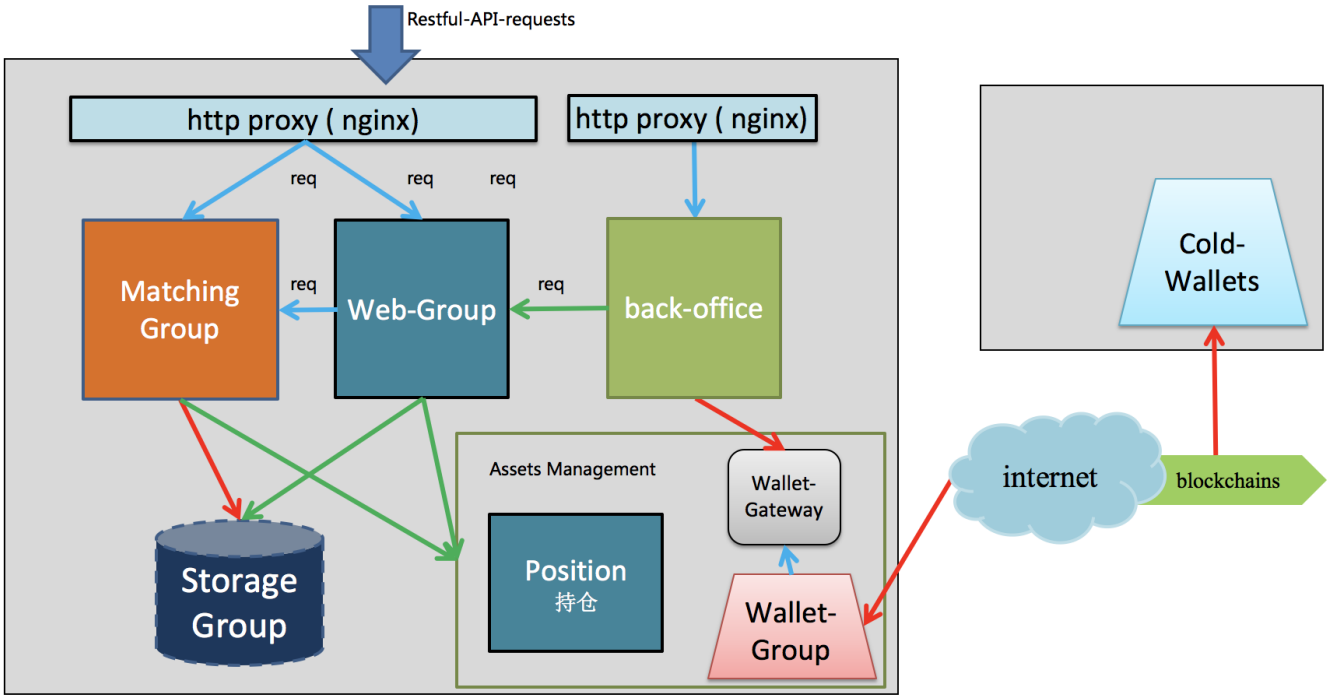
Web 业务系统与我们常见的电商系统无异，主要是用户账户以及简单的业务逻辑，重点是可扩展性，业务要求比较弹性。

交易撮合系统本质上是一个高并发的计算系统，特点是系统性能高和稳定性好，其中订单队列可以是编程语言中的数据容器，也可以是内存数据库。

运营后台系统在整个交易所生命周期的早期并不凸显重要性，但是运营后台系统恰恰是交易所中后期发展的核心系统，重点在数据准确，要求网络安全性高和可扩展性好。

资金管理系统包含用户持仓状态，以及数字货币钱包服务，它是一个交易平台中安全性要求最高的系统，资金管理系统往往要搭配一个内存数据库，其中数字货币钱包服务也可以拆出来做成独立子系统，甚至可以改造成整个公司的内部区块浏览器，因为钱包服务需要设计成多个钱包实例，并统一所有的币种钱包接口。

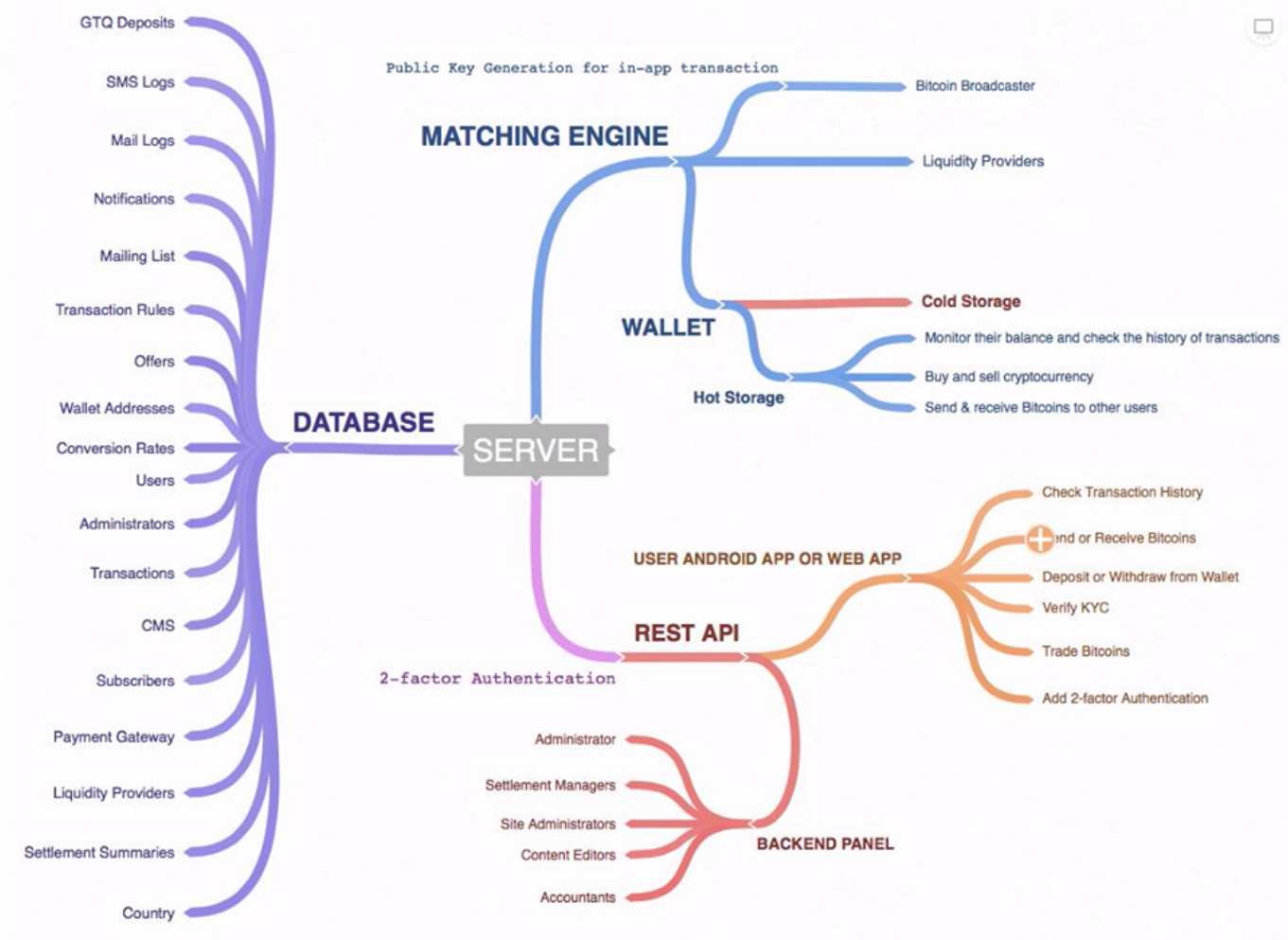
一个交易所可能的结构如下图。



上图中，MatchingGroup 相当于是交易撮合系统；Web-Group 相当于 Web 业务逻辑系统；Back-office 相当于后台管理系统；AssetsManagement 相当于是资金管理系统。

涉及的技术栈

如果我们再将刚才提到的各个模块细分，会看到以下的功能。



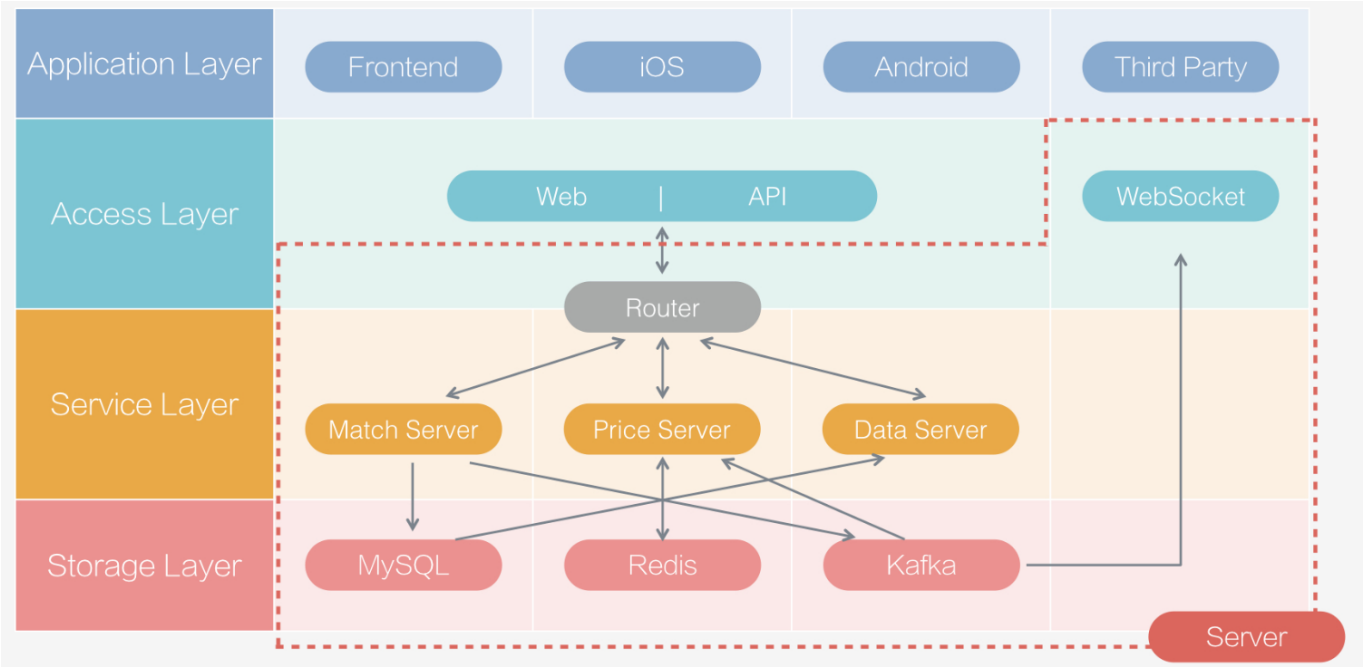
（图片来自网络）

按照上图的细分功能，我们可以得到哪些技术支持一目了然。

首先是 Server 需要数据库作为支撑，其次是 Restful API 作为基础通讯协议，并且集成钱包相关的技术，撮合引擎为 Sever 提供撮合服务。

在这里面，例如需要 SMS 系统，所以可以使用云服务中的 SMS 组件，这些都可以是成熟的通用组件技术。我们可以发现中心化交易使用的技术与互联网技术并无不同。

把这些通用组件塞到下图中各个层次和大模块当中，所以最终一个交易所的详细架构可能是下图的样子。



（图片来自网络，缺失了资金管理部分）

我们来解释一下这张图。

首先是存储，持久存储通常可以选择 MySQL，撮合相关的模块由于要避免接触磁盘 IO，所以需要为撮合模块提供 Redis 类型的内存存储，二者需要保证最终一致性。

撮合和行情部分，几乎与传统技术无异，行情推送可以类比到其他推送系统，只是频率更高，一般首选 Websocket 技术。

这与传统互联网应用的最大区别里主要是数字货币钱包管理，这块完全是新的内容，对安全性、易用性提出了相当高难度的挑战，这里也是交易所资金托管的根本，所以如何管理好大量数字货币，往往要结合运营、内部管理制度、冷热钱包技术一起才能做好交易所的资金管理。

那么用户是如何挂单的，又是如何产生区块链交易的呢？我们来看一看。

交易过程

那么说，用户 A 拿 0.01BTC 换取了 B 的 10 个 ETP 的过程究竟是什么样的呢，我来举一个例子。

1. 用户 A 挂 10ETP 买单，出价 0.01BTC 经过 Web 业务系统进入撮合系统订单簿 ETP-BTC 买单队列，等待撮合成交，同时资金管理系统冻结 0.01BTC。
2. 用户 B 挂 10ETP 卖单，出价 0.01BTC 经过 Web 业务系统进入撮合系统订单簿 ETP-BTC 卖单队列，与步骤 1 中 A 的订单撮合匹配成功，生成 Trade，同时资金管理系统结算对应资产，B 的资产变化为增加 0.01BTC 并减少 10ETP， A 增加 10ETP 并减少 0.01BTC。
3. 成交 Trade 以及资产变化通过资金管理系统写 RDB 数据库，形成成交记录，同时更新行情，数据库记录可供用户和运营后台管理系统查询。 要注意的是这一步并不是登记到区块链上。
4. 用户 B 经过 Web 业务系统发起提币请求，请求提取 10ETP 进入自己的数字货币钱包，这个请求进入资金管理系统，交易所运营人员可通过运营后台观察到这笔请求，运营人员审核用户 B 的信息，比如实名认证是否正常等。
5. 提币请求进入运营系统后，如果通过审核，则资金管理系统会冻结用户 B 的 10ETP，同时将提币请求发起给数字货币钱包服务系统，也就是 WalletGroup，子系统发起区块链上的交易 x（Transaction），等待交易被打包，并根据更新提币审核状态，供用户查看。
6. 数字货币钱包服务根据区块信息查询交易 x 是否被打包，如果已经打包，则资金管理系统将完全把用户 B 被冻结的 10ETP 直接抹成 0，更新提币状态最终为完成，提供区块交易 ID 以供用户和运营后台系统进行查询。

在步骤 3 中，我们可以看到用户所持有的资产，相当于是交易所对用户的负债，但这也只是数据库中的一个数字，并不是真正的链上资产。

在步骤 6 中，我们看到区块链上的“交易”与步骤 3 中的“交易”完全不是一个概念，同时用户的资产是否安全，完全取决于交易平台的技术是否安全，对交易所是否信任。

再来看看充值阶段。

简单来说，充值是与提币相反的过程，不同的是，充值不需要审核，一般数字货币交易所的原则都是“宽进严出”，在充值过程中，交易平台通常不直接使用数字货币钱包检测用户是否充值到账，而是使用“扫块”(block_scan) 这一方法检测用户的充值。

□总结

今天我简单介绍了数字货币交易所的业务逻辑，相信你已经对数字货币交易所有了一个初步的了解，数字货币交易所是区块链行业最重要的业务，全世界每个月都有新的数字货币交易

所诞生。

今天我只讲了中心化的数字货币交易所，而去中心化的交易所，除去资金管理系统，基本业务逻辑是不变的。所以今天的问题是，□去中心化交易系统应该如何设计呢，主要会遇到哪些挑战？欢迎留言，我们一起讨论。

上一篇 第27讲 | 弄懂数字货币交易平台（一）

下一篇 第29讲 | 互联网身份与区块链数字身份

精选留言 (13)

写留言

不学习干嘛 3
2018-05-28

老师你好，有些迷惑，请帮忙解答一下：
用户之间交易只是资产转移，那真正的数字货币是存储在交易平台的冷钱包里嘛？
我知道如果是币币交易的话，平台存储的币可能是来自用户的充值
但场外交易呢？那些只有场外交易的平台他们会存储币么？随着交易额的不断增加，存储

量也要时时增加（Transaction）嘛？但这样就会产生旷工费了，是在Trade时的手续费...

展开

亮哥

2018-07-19

1

老师，您好！看了后有点迷糊，麻烦帮忙解答下。
看了区块链交易系统感觉与传统的基于虚拟账户的交易系统思路是一致的，只有在充值和提现的时候才与外部的区块链产生Transaction，这个理解对吗？
如果上面的理解是对的，那么这里交易的第一步用户A的0.01BTC是通过WalletGroup子系统发起区块链上的交易（Transaction）充值来的吗？这个充值的钱需要有个中间过度账...

展开

作者回复: 你好，你的理解是对的。平台是有跑路风险的哦。关键是平台和平台之间是互通的，平台之间的竞争压力会很大。

小可爱爱

2018-06-11

1

老师我刚学习区块链，很多还不懂，请教下如果是去中心化交易所，哪些是一定要放在公链上的？老师能不能再加餐一期专门说去中心化交易所.....真的很期待啊

展开

作者回复: 你好，我会单独发文哒，发到咱们公众号上

阿痕

2018-05-29

1

如果我在某交易平台上花1万人民币充值1比特币，这枚比特币只记录在交易所中心化的数据库里，并没有真正在区块链上产生transaction，这样理解对吗？

作者回复: 你好，充值过程是有transaction的，但是充值成功后，你在交易所显示的比特币只是一个数字啦，并不是真的比特币了。

不了峰
2018-05-29

1

360公司Vulcan（伏尔甘）团队发现了区块链平台EOS的一系列高危安全漏洞。
EOS网络负责人表示，在修复这些问题之前，不会将EOS网络正式上线。

请问不会将EOS网络正式上线是什么意思?

展开

作者回复: EOS代币预售是使用的ERC20 token，正式上线是指运行属于自己的主网，与ERC20脱离关系的过程。

Ender0224
2018-05-29

1

也就是说交易所并不一定持有和存入交易所等量的数字货币?就跟银行一样，前提所有的用户不会同时把币都提出来。
如果是这样，交易所会不会也会把币自己外借呢（借给dapp开发团队用于开发）？

作者回复: 是的，内部不透明，很难说清楚哦。

Eric
2018-12-02

陈老师，文中所说的ETP就类似传统交易所的发行的股票么？每个交易所都可以发行自己的凭证了？

Leon
2018-06-24

陈浩，你好，我在极客时间订阅你的课程，讲的很好。
我还有一个问题想请教一下，你在https://www.zhihu.com/question/61185047这个回答里面提到的
“通常的做法，可以购买一套文交所或者期货交易所的源码，只需要在资金管理系统中，把数字货币加上即可。” ...

展开

Leon
2018-06-24

陈浩老师你好，我在极客时间订阅你的课程，讲的很好。
我还有一个问题想请教一下，你在https://www.zhihu.com/question/61185047这个回答里面提到的
“通常的做法，可以购买一套文交所或者期货交易所的源码，只需要在资金管理系统中，把数字货币加上即可。” ...
展开

an7N0l
2018-06-22

老师我有个问题，既然交易平台只有充提币才会上链，是不是意味着交易平台的钱包是用户公用的，那这样的话不同用户的同一个币种的充币地址应该是一样的才对啊？
为什么我观察到的基本上不同用户的地址是不一样的呢？

合民
2018-05-29

老师，您好，我是后加入到学习队伍中的，正在努力追赶进度，学习的过程中心里一直有个疑问。对于区块链，主要是尝试解决分布式下的信任问题（共识），但这个规则是适用于用户之间的，那么对于系统的创建人是否有控制呢？假如系统的开发人员在系统上留后门，现在有什么解决方案吗？这个问题可能不局限于技术角度，期待老师的解答！
展开

> 作者回复: 主要是开源以及社区自治。创建人可能会初次获利，后续社区会逐渐监督创建人的权力。

袁克强
2018-05-29

充值是否给每个用户生成一个地址？
用户的余额查询是查询区块还是直接查询数据库，查询数据库的话有充值进来如何触发更新数据库？
展开

> 作者回复: 是的，应该是每人每次一个地址。
> 一般查询数据库，这个叫持仓。
> 通过监听充值交易transaction。

阳仔

2018-05-28

1、交易平台为何不直接使用数字货币钱包检测用户是否充值到账，而是使用“扫块”(block_scan) 这一方法检测用户的充值呢?
2、是因为扫块的方式效率高?
3、以比特币充值为例，是不是需要有6个块确认之后交易平台才显示确认到账呢?

展开

作者回复: 1和2. 首先是性能考虑，因为交易平台拥有庞大的用户基数，如果仅仅只有钱包，显然钱包的性能不足以支持庞大的查询请求。其次是风控角度，针对异常交易检测需要比较精细稳定的查询服务。后续文章会有剖析哦

3. 是的。