长久以来，“交易所”一直都是币圈最火的赛道之一。如同当年团购时代的万团大战，在上一轮牛市里，币圈也曾一口气涌现出了上万家的交易所，一直到今天仍然是每天都有新交易所诞生，每天也都有老的交易所倒下。

不同的交易所虽有不同的业务侧重，但都同时关注着一个至关重要的痛点——交易所钱包。从业以来，比特派钱包团队曾经接受过众多交易所的关于交易所钱包相关的问询。

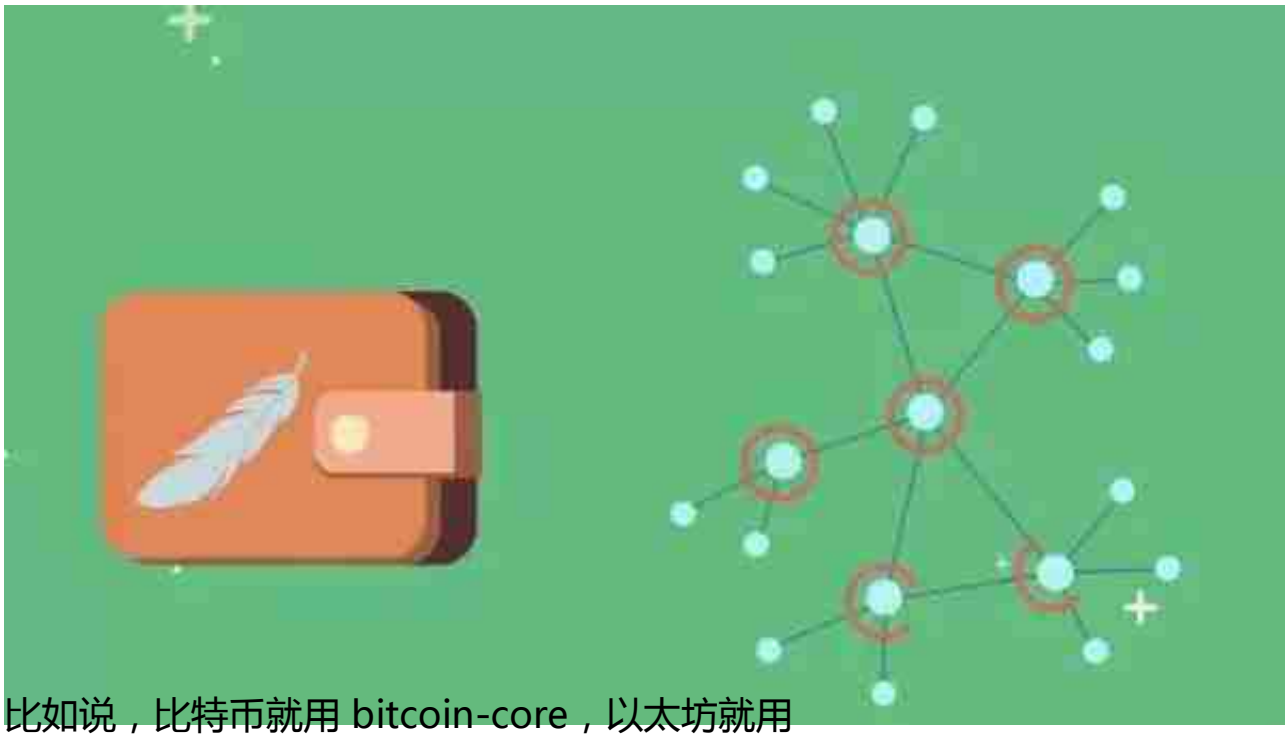
本文会将部分内容整理出来，与大家讲述设计交易所钱包方案时的常见问题，希望能对您有所帮助。

问题一：交易所钱包应该使用第三方托管服务吗？

对于这个问题，我们的答案是：

请根据自身情况，谨慎考虑是否采用托管服务。

最近这段时间，“托管”这个词在币圈很火，俨然成了一个“很有希望”的赛道，这里我们不想去讨论托管这个赛道是否有价值，只想给大家说说“为什么您应该谨慎考虑第三方托管”——这种看起来自己啥都不用干，只靠第三方 API 就能把钱包都管理起来了，这种方式真的好吗？



比如说，比特币就用 bitcoin-core，以太坊就用 geth/parity，别琢磨了，这是成本最低、效率最高的解决方案，没有之一！

首先，各个公链无论是主网上线还是后续升级，最早能用的一定是官方的全节点钱包，因为所有的改动都是在这里做的，全节点能跑了，公链才有意义。从这个角度上讲，您如果想第一时间最快的支持一个新公链，官方全节点其实是您热钱包的首选方案。

其次，今天的公链全节点通常都能提供比较完善的 RPC 调用支持，也就是说您的交易所网站充值提现模块可以通过调用全节点 RPC 来完成地址生成、余额查询、交易监控等操作，总体来讲开发成本较低。

由于各公链的官方全节点钱包是热钱包，所以切记只能将其用于满足交易所日常充提的热钱包模块，其中的大额部分要定期的汇总到冷钱包里以确保安全。

另外，热钱包系统也应做好相应的主机安全加固和网络安全加固，并做好攻防保护，以确保钱包系统的安全。热钱包里的币也应该做到能不丢尽量不要丢。

如果您的交易所像几大交易所一样“研发资源溢出”，那也没必要自行研发热钱包框架，因为这个活儿干下去是个无底洞，即便是像比特派这样拥有全球顶尖的钱包研发团队，在公链支持上也要投入巨大的精力，自行开发钱包系统不是说做就能做的。如果非要做，建议将精力投入到主要币种（如 BTC、ETH、USDT 等）的热钱包系统开发，其它的公链建议在交易所热钱包这块还是使用官方全节点钱包，因为对于交易所来说，能第一时间支持新链太重要了。

问题三：交易所的冷钱包方案应该如何规划？

交易所的热钱包可以用各个公链的全节点钱包，那么交易所应该如何安全的冷存储大额的区块链资产呢?

答案其实也很简单，那就是“请使用安全、可靠的硬件冷钱包来存储大额资产”。这里要特别说明一下，即便是您的交易所真采用了第三方托管服务，您仍然应该把大额资产定期的转到自己掌握的硬件冷钱包中，因为“安全”，同时也因为“您也需要评估第三方托管服务的道德风险”。

关于硬件冷钱包的选择呢，我们曾专门写过一篇文章《正确选择硬件钱包的几个要点》来讨论过这个事情，原则嘛，不外乎“开源”、“不断迭代”、“有屏幕”、“架构安全合理”、“有良好的安全历史和口碑”这几点。

在这几个关键点上，Trezor、Ledger 和我们团队开发的 BITHD.com 比特护盾、刀锋硬件钱包都能很好的满足需求，而有很多在上一轮牛市里新出来的硬件钱包团队往往在“开源”这两个字上就已经不能满足要求了，在这一点上，小白可能还会

胡乱选择，而作为交易所来说，选错了是很不应该也很不专业的。

相比起 Trezor、Ledger 来说，BITHD 在产品功能和体验上有着很大的优势，在币种支持和多重签名等功能上也要领先的多，因此，交易所们可以优先选择比特护盾或刀锋作为自己的冷钱包方案。

另外，对于那些 BITHD、Trezor、Ledger 都没有支持的公链，交易所又该如何进行冷存储呢？即便我们已经很努力的让 BITHD 尽可能多的支持公链了，但仍然很难做到每一条公链都支持，这种情况下，您该怎么办呢？

这里我们建议您对那些当前没有硬件钱包支持的公链，使用专用的电脑来存储大额资产，并且平时在不用的时候关机，以确保安全。虽然这种方案不够完美，毕竟这是您当前能选择的还算是比较合理的模式。

当您需要对私钥、助记词进行备份时，建议使用钢铁助记词板——冰甲，用来抵抗水灾、火灾等不确定因素，这会比单纯用纸做备份拥有更高的安全等级。

问题四：交易所的冷钱包管理如何避免单个人的资产管理风险？

单点故障（单个人的资产管理风险）是交易所必须要考虑的点，在这一点上，我们其实强烈建议交易所用正确的方案使用多重签名功能，具体原则如下:

1、在使用多重签名功能之前，您首先应该使用的是开源冷钱包（开源硬件钱包），也就是说，大额资产存储设备最重要的是“代码开源”，其次是足够“冷”，最后才是“多签”；

2、根据内部的资产管理方案，合理设计多签模型，比如：2/3、3/5 等都是很好的多签模式；

3、不要低估单点故障（单人风险）；

4、不要低估单个人的道德风险，在我们六年的钱包研发历史中，所遇到的“内鬼”盗币、熟人盗币并不少，远比大家想象中的要多；

在硬件冷钱包的多重签名功能方面，BITHD 当前是具备绝对的领先优势的，我们不仅支持 BTC、ETH、EOS 等币种的多重签名，还支持 USDT（包括 ERC20、Omni 两种格式）的多重签名功能，最近还新增支持了 ERC20 全 Token

的多重签名功能，而对于大部分交易所来说，除了比特、以太、USDT
这几大币种以外，ERC20 全 Token 基本上已经能涵盖 90%
的热门交易品种了，也就是说，如果您的交易所使用了 BITHD
多重签名来管理大额资产，基本上大部分币种和 Token
都能纳入到相关的管理框架了，这么说您就该明白这里面的意义到底有多大了吧？

总结

对于一个交易所来说，首先您应该谨慎选择是否要使用第三方托管服务，我们建议您使用各个公链的全节点来搭建交易所的热钱包系统，因为采用这种方案能让您在交易所的竞争中占据公链支持的先机（比别人更快的上币），并且成本更低，更不依赖于第三方的安全性和稳定性。

另外，您还应采用像 BITHD、Trezor、Ledger 这样的开源的、安全可靠的硬件冷钱包来作为交易所的冷钱包管理方案，并且，还应合理使用多重签名冷钱包来多人共管大额资产，避免单点故障和单人风险（包括道德风险）。