长期以来，《交易所》一直是币圈最火的赛道之一。就像团购时代，上一次牛市，币圈涌现了上万家交易所。接下来，新的交易所每天都在诞生，旧的交易所每天都在倒下。

虽然不同的交易所业务侧重点不同，但都聚焦于一个关键痛点：——交易所钱包。自加入公司以来，该团队收到了许多交易所关于交易所钱包的询问，并一一作出了回应。本文将对其中的一些进行梳理。，告诉你设计钱包方案时的常见问题，希望对你有所帮助。我们对问题1的回答：exchange钱包是否应该使用托管服务？问题的答案是：

请根据自身情况慎重考虑是否使用托管服务。最近几天单词&quot主持人&quot风靡币圈，已经成为&quot前途无量&quot跟踪。在这里，我们不&#039；我不想讨论托管曲目是否有价值，只是想告诉你&quot为什么要认真考虑第三方托管&quot——看来你不&#039；除了在第三方API上管理你的钱包，你什么都不需要做。。这真的是个好主意吗？

1。第三方托管服务不是&quot安全&quot如大家所想。它的安全性依赖于钱包系统的机制以及服务器和网络的安全策略。现在托管领域最著名的服务Bitgo也曾在几年前导致12万比特币sa被盗。在那次事件中，比戈&#039；美国的服务器本身没有受到损害，但黑客攻破了它。，然后叫做Bitgo&#039轻松转账的API。计划使用第三方托管服务的交易所可能希望评估当您的服务器被黑客攻击时，调用托管API是否可以窃取资金。使用托管服务不会增加额外的安全性。因为黑客入侵了你的服务器，你的钱可能就没了；入侵托管服务商的服务器，你的钱可能还是没了；托管服务的API访问方法&#039；s和您的访问服务的API密钥被盗，您的钱可能会丢失。换句话说从原来的单点安全风险，蔓延到了多点安全风险。在例子中，大部分硬币存储在冷钱包中(当热钱包中有超过1000个比特币被盗时，冷钱包中的硬币是安全的)，但在更改为Bitgo托管模式后，几乎所有的硬币都一次性丢失。。这是同一个原理。还有与安全相关的道德风险。让&#039；让我们以Bitgo为例。盈利能力强，在一定程度上可以为盗窃付出代价，所以道德风险相对较低(最近的碧南盗窃案就是如此)。Bitgo是一家利润微薄的公司。

2。我们现在应该仔细考虑托管服务的另一个原因是，每&quot高效&quot交易所正在努力跻身顶级交易所之列。但是，在这么拥挤的赛道上(想想一万次交流的概念，你就明白了)，你应该带头。你必须更有效率。是交流最重要的环节，——&quot装钱&quot，在公链上？它对团队的效率要求极高。对于新兴的、热门的区块链资产，如果能先投入资金，就能抓住机会吸引大量用户交易。。这也是为什么经常看到最初交易所的一些钱经常被其他交易所拿走的原因。从这个角度来看，交易所使用第三方托管服务的效率取决于第三方托管服务的效率。例如，Bitgo没有&#039；不要长期支持以太坊。。如果你的交易所使用Bitgo，你需要做好交易所无法长

期支持以太坊交易的准备。像过去那些流行的公链：Cocos等。如果托管人不支持，不是&#039；你的交易所不准备支持它吗？？即使你遇到一个一直打鸡血，不断支持新公链的托管服务商，你想推出的新公链也不一定是托管服务商想先推出的公链。双方在优先级调度上还是有很大可能存在很多分歧的。所以从效率的角度来看，

你的交易所应该慎重考虑第三方托管服务。

3。交易所还需要考虑&quot成本&quot在选择托管服务时。第三方托管服务通常是按照数量收取服务费，无论是库存还是流量。对于一个新的交易所来说，托管服务的初始金额很小，所以托管的成本似乎比建立钱包服务的成本要低。但是老实说，你开始交换是因为你希望你从未测量过它吗？即使是现在的无头交易所，也必须设计自己的钱包解决方案来管理硬币，因为只有好的成本解决方案才能让你走得更远。简而言之，第三方托管服务可能不适合交易所&#039；的钱包模型。托管服务可能更适合其他场景。但对于交易所来说，无论是安全、效率还是成本，交易所钱包都必须慎重考虑是否使用第三方托管服务。即使你最终决定使用托管服务，重要的是要记住，你应该只把它作为热门钱包的替代品。冷钱包还是要分开管理。

问题二：交易所的热钱包系统应该如何设计？这是我们经常被问到的问题。我们在这方面有很多不同的解决方案(比如当时的Bite企业版，后来的区块链云服务)。。我们还为Bite开发了钱包内兑换系统和银行安全充值模块。经过这么多年的实践，我对这个问题的回答很简单：

请使用公链官方全节点钱包，搭建交易所的热钱包系统！比如比特币使用-核心以太坊用geth/，算了，这是成本最低，效率最高的方案，没有之一！首先，每一个公链，无论是主上线还是后续升级，最早都必须是官方全节点钱包，因为所有的改动都在这里，公链只能在全节点运行。。从这个角度来说，如果你想尽快支持一个新的公链，官方全节点其实是你热钱包的首选。其次，下一个公链节点通常可以提供相对完善的RPC调用支持。这意味着你的交易所网站存取款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。开发成本低。由于各公链官方全节点钱包都是热钱包，切记只能用于满足交易所日常充值的热钱包模块。大部分要定期汇总到冷钱包里，确保安全。另外，热钱包系统也要做好相应的主机安全加固和网络安全加固，做好攻防防护，保证钱包系统的安全。热钱包里的硬币也要尽量避免。如果你的交易是&quot像几个主要的交易所一样&quot没必要自己开发热钱包框架，因为这个工作是个无底洞。即使拥有像Bite这样的世界级钱包研发团队，也需要公链支持的大量精力。自己开发钱包系统是不可能的。如果你必须这么做，建议致力于开发主要货币(如BTC、瑞士法郎、美元等)的热钱包系统。).对于其他公链，交易所热钱包建议使用官方全节点钱包。因为对于交易所来说，第一时间支持新链是非常重要的。像几大交易所。没必要自己开发热钱包框架，因为这个工

作是个无底洞。即使拥有像Bite这样的世界级钱包研发团队，也需要公链支持的大量精力。自己开发钱包系统是不可能的。如果你必须这么做，建议致力于开发主要货币(如BTC、瑞士法郎、美元等)的热钱包系统。).对于其他公链，交易所热钱包建议使用官方全节点钱包。圆周率币在公链上吗？因为交易所在第一时间支持新链是非常重要的。。因为这个工作是个无底洞，即使你有世界一流的钱包R&amp像Bite这样的d团队，需要投入大量的精力在公链的支持上。自己开发钱包系统是不可能的。如果你必须这么做，建议致力于开发主要货币(如BTC、瑞士法郎、美元等)的热钱包系统。).对于其他公链，交易所热钱包建议使用官方全节点钱包。因为交易所在第一时间支持新链是非常重要的。。因为这个工作是个无底洞，即使你有世界一流的钱包R&amp像Bite这样的d团队，需要投入大量的精力在公链的支持上。自己开发钱包系统是不可能的。如果你必须这么做，建议致力于开发主要货币(如BTC、瑞士法郎、美元等)的热钱包系统。).对于其他公链，交易所热钱包建议使用官方全节点钱包。因为交易所在第一时间支持新链是非常重要的。。自己开发钱包系统是不可能的。如果非要做，建议你把精力放在主要货币(如BTC、ETH、usdt等)的热钱包系统开发上。).对于其他公链，交易所热钱包建议使用官方全节点钱包。因为对于交易所来说，第一时间支持新链是非常重要的。自己开发钱包系统是不可能的。如果非要做，建议你把精力放在主要货币(如BTC、ETH、usdt等)的热钱包系统开发上。).对于其他公共链，交换&#039；s热钱包建议使用官方全节点钱包。因为对于交易所来说，第一时间支持新链是非常重要的。

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使用各公链的全节点钱包。那么，该交易所应该如何安全地储存大量区块链资产呢？答案其实很简单，就是&quot请用安全可靠的硬件冷钱包存放大量资产&quot。这里需要注意的是，即使你的交易所确实使用了第三方托管服务。你还是应该定期把大量资产转移到你的硬件冷钱包里，因为&quot安全性&quot和&quot你也有道德风险&quot托管服务需要评估。"关于硬件冷钱包的选择，我们曾经写过一篇文章《正确选择硬件钱包的几个要点》()讨论过这个事情。。原则无非是&quot开源&quot，&quot连续迭代&quot，&quot屏幕&quot，&quot安全合理的建筑&quot和&quot良好的安全记录和声誉&quot。在这些关键点上，我们团队开发的Bit和Blade硬件钱包可以很好的满足需求。在上一次牛市中，许多新的硬件钱包团队往往&quot开源&quot。两个字已经不能满足要求了。在这一点上，小白可能还是会随意选择，而作为交换，选错了是非常不专业和不专业的。与BITHD相比BITHD在产品功能和体验上有很大优势，在货币支持、多签等功能上也处于领先地位。因此，交换可以优先考虑钻头或刀片。你自己的冷钱包解决方案。另外，对于那些BITHD不支持的公链。交易所应该如何进行冷藏？虽然我们已经努力让BITHD支持尽可能多的公链，但是要支持每一个公链还是很难的。这种情况下你该怎么办？这里对于目前不支持硬件钱包的公链，我们建议您使用专用电脑存储大量资产，并且通常在不使用时关闭，以确保安全。虽然这个方案并不完美，但毕竟是目前可以选择的合理模式。当私钥和助记符需要备份时建议使用钢助记板——冰甲抵御洪水、火灾等不确定因素

，比单纯使用纸张作为备份更安全。等级。

问题四：如何规避交易所冷钱包管理中的单一资产管理风险？？单点故障(单一资产管理风险)是交易所必须考虑的一点。在这一点上，我们强烈建议交易所使用正确的方案来使用多重签名功能。具体原则如下：1。在使用多签名功能之前，先使用开源冷钱包(开源硬件钱包)。也就是说，大型资产存储设备最重要的是&quot开放源代码&quot，第二个是&quot够冷&quot最后一个是&quot多重签名&quot；2.根据内部资产管理方案，合理设计多标志模型。比如2/3，3/5都是不错的多签模式；3.唐&#039；不要低估单点故障(单人风险)；唐&#039；不要低估一个人&#039；道德风险。在我们六年的钱包发展过程中，我们遇到了许多&quot内部人士&quot偷币和熟人偷币。，远远超出所有人&#039；的想象力；在多签名功能方面，BITHD目前拥有绝对的领先优势。我们不仅支持BTC、ETH、EOS等币种的多重签名，还支持usdt(包括ERC20和Omni格式)的多重签名功能。最近增加了支持ERC20全令牌的多重签名功能。对于大多数交易所来说，除了Bit、Ether、usdt等主要货币外，ERC20全令牌基本可以覆盖90%的热门交易品种。也就是说，

总结对于交易所来说，首先要慎重选择是否使用第三方托管服务。我们建议你使用每个公链的所有节点来构建交易所的热钱包系统，因为这个方案可以让你在竞争中进行交易。，它的优势是支持公链(加载钱的速度比别人快)，而且成本低，不依赖第三方的安全性和稳定性。此外，还应该使用BITHD等开源、安全可靠的硬件冷钱包作为交易所的冷钱包管理方案。并合理使用多签名冷钱包管理大量资产。人们避免单点失败和个人风险(包括道德风险)。