早在一年多前，BiteMission的安全实验室曾经写过一篇文章《以太坊DeFi生态当前最大的安全隐患》，文章中提到目前的DeFi项目方&#039；s对用户的合约授权需求过高，成为以太坊最大的安全隐患。

一年多过去了，合同授权过度的隐患仍未消除。相反，随着多个公共链与EVM的兼容，危机已经蔓延到了各处。再加上很多偷钱贼对授权机制的利用，合同授权已经从一种安全风险变成了一种每天都在发生的资产盗窃形式。

顾名思义，就是把自己资产的支配权授予他人。合同授权的本意是使项目各方签订合同以&quot操纵用户&#039；资产更方便&quot，因为你真的可以&#039；未经授权，不要动你的财产。，就无法进行DeFi中常见的对换、压桩等一系列操作。

It&#039；有点像生活APP问你自动扣费的权利。例如，你不&#039；做完车后不需要做任何自动扣钱的事情。正常地自动扣款功能会有限制，所以小资产操作风险可控，真的方便。然而，在区块链世界，几乎所有的DeFi项目都在要求用户授权，甚至要求无限授权。大多数用户实际上并不&#039；我还不知道。这以项目方分享资产所有权为代价简化了操作，因此无限制的合同授权也可以有更直接的翻译，

&quot；从现在开始，这种货币的所有余额由我负责。你同意吗？"

风险显而易见，因为项目方有权支配你的资产，所以一旦它作恶，你的资产就不再是你的资产了。此外，项目方的所有者密钥泄露、合同被黑客攻击等。你的资产很难生存。

可以说，授权后，你的资产安全取决于项目方的技术水平和道德水准，我是鱼，我是刀。

对于以太坊这样的庞然大物，短时间内通过代码彻底解决相关隐患并不现实；

我们也不能希望每个合同背后的项目方都是道德上完美的人；

我们只能量力而行，抵御合同授权的风险，重点如下：

第一招：不要授权不熟悉的项目合同

。

目前主流的DeFi项目通常都是开源的，都经过了完整的代码审核，所以风险相对较低，每一个陌生的合同都是风险极大的。目前每天都有层出不穷的新合同产生，骗

取用户授权。

第二招：区分地址参加不同的DeFi项目

如果一个地址参加了多个DeFi项目并获得授权，就相当于你的地址上有多个风险敞口。如果任何项目有风险，那么你的资产也会面临损失的风险。

使用不同的地址分别参与高风险、低风险、超高风险的项目并做笔记，这样即使一个项目出了问题，也只能影响到这个地址的资产，其他地址的资产仍然是安全的。多地址是隔离风险的有效手段。(听说单个钱包比专用钱包能创造1000个地址，而且只需要一套助记符就能保存。)

第三招：按需授权，有限授权项目。

降低授权额度也是降低风险暴露的有效手段。如果需要将1000美元兑换成ETH，最好只授权1000美元。

第四招：定期检测授权，收回风险授权

与专用钱包5.0047版本相比，用户可以在这里检测自己授权的物品、币种、限额，实时收回授权。目前已经支持ETH、BSC、HECO、OKT、MATIC、FTM、xDAI、AVAX链的授权检测和恢复，小白用户也可以自行维护自己的资产。

感谢DEBANK对任务授权检测功能的支持。

第五招：提前输钱

这一招虽然不推荐，但确实是很多人用来抵抗偷币的主要手段。所以你没有&#039；不会被偷，因为你做得足够好。仅仅因为你钱少。

因此，如果授权地址较多，且后续有大量资产转移，最好在此之前完成授权恢复。

以上仅是防御DeFi授权风险比专用钱包五招的详细内容。有关特殊钱包的更多信息，请关注www.dadaqq.coMDadaqq.Com的其他相关文章！

本站提醒投资有风险。入市需谨慎。此内容不作为投资理财建议。

标签：DeFithan专用钱包。