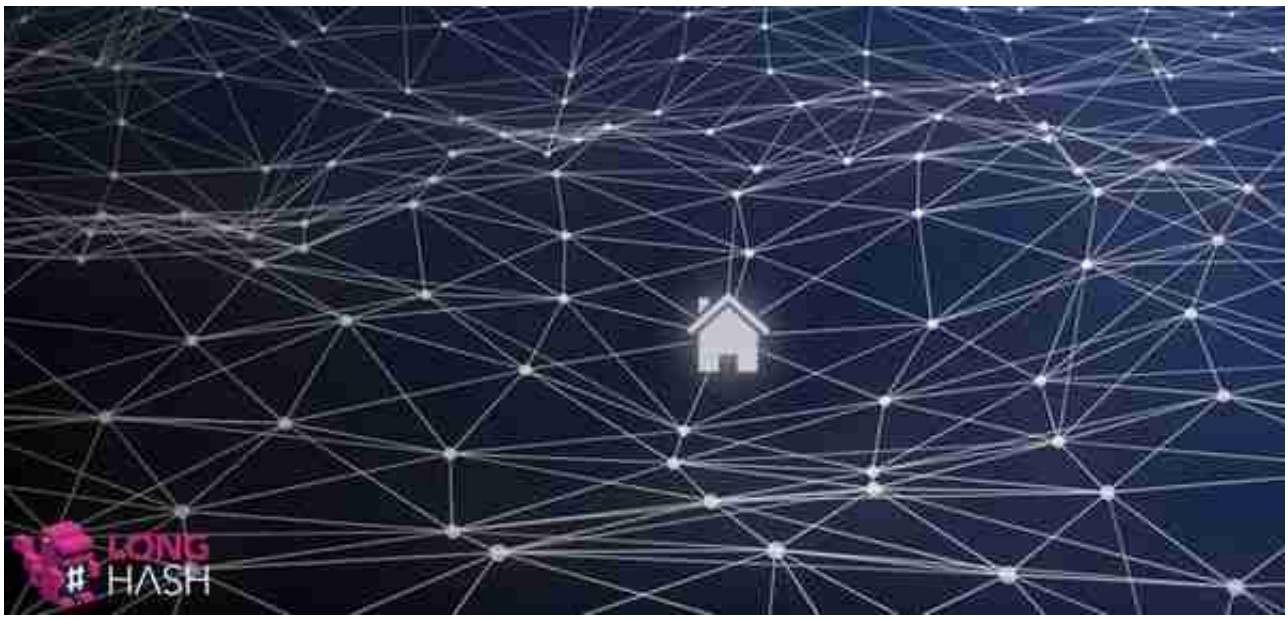
来源/LongHash



比特币的安全并不在于其代码库、算力、投入工作量证明的电力、或者什么椭圆曲线密码学的数学特性等。比特币之所以安全，是因为有我们这群用户守护着它。就像数据中心或金库最终还是需要依靠人来抵御入侵者一样，比特币节点和钱包最终也只是依靠一种物理力量来保护它，而有物理访问权限的人能够重新定义这个机器的功能，或者获取相关功能的知识与内容。

因此，网络的安全受到了不少威胁。如果只有一个人运行自己的节点，那这个人就能左右包括区块奖励在内的网络规则，他们能够轻易地审查或撤回交易。但如果很多人都运行自己的节点，那么这个威胁在用户眼里就变得微不足道，而每增加一个节点对网络及其安全似乎也多少能起到帮助。

有些技术能够帮助我们轻松保护我们的比特币。像 Tor 这种匿名网络就能够隐藏我们的节点。一个隐藏得够深的节点类似于金库，就不需要再叠加特别好的物理防护了。密码学的存在就是，当秘密被盗时它更容易保护这个秘密。而当你的节点被定位并控制后，像加密硬盘一类的东西会让私钥的破解特别困难。最终，通过在现成硬件上的开源软件，你能轻松地换个隐秘的地方另起炉灶。

1. 机器/设备

你需要一台你信得过的机器。可以用树莓派那么小的微型机，但迷你电脑或者自己组装的计算机会更好。不需要太大的存储空间，也不需要接入高速网络，当然这些东西也会起到帮助。

理想情况是，计算机运行一个开源操作系统，并对硬盘驱动进行加密，还可以通过防火墙等方式拦截未授权的访问。

这台设备必须是你自己的，其他任何人都不能访问，且最好放在一个只有你能打开的地方。

2. Tor 网络（洋葱路由器）

你的机器最好就完全放在 Tor 上，这样任何人都很难定位到你并发起物理攻击。同时，它还能隐藏你在使用比特币这个事实，因为在某些情况下，使用比特币会不经意间在你背上留下靶心。

如果你想要在你的机器上跑一些服务，比如闪电网络或比特币轻钱包，那么选择隐藏的服务或者洋葱网络，能够让你轻松地获取家庭网络外的节点，而不需要再检测或进一步配置网络。

点击获取源代码。

3. 比特币节点

你的比特币节点验证的是点对点网络里每笔交易与区块传递的完整性。这让每个投资者和持币者都有机会了解到现有多少比特币，以及整个系统是否还在正常运行。虽然节点不能阻止链上的分裂，但能帮助验证当前的规则是否被遵守。

或许最重要的一点是，节点会给你一个准信，让你知道发给你的比特币是否已经被网络确认，而不会被双花。如果没有自己的节点，你就只能信任别人的节点。但别人可能会作恶，所以没有自己的节点，就无法验证这些节点是否在同一条链上，是否有按照同一套规则好好运行。

通过自己的节点来检查钱包余额并广播比特币交易，也能够保留一定的匿名性，尤其是当你把节点藏在 Tor 上。

点击获取比特币核心（Bitcoin Core）源代码。或者 Libbitcoin 源代码。

4. 闪电网络节点

闪电网络承诺在不造成比特币网络拥堵的情况下，进行近乎即时且低费用的比特币交易。但伴随这些好处的代价是，要使用独立的网络和独立的软件，并且安全前提也不一样。和比特币钱包不同，比特币钱包可以安全地长期关闭，甚至是进入纯模拟状态；而闪电网络钱包需要大多数时间都在线，并与比特币全节点连接。

另一方面，一旦设置好了，你就可以赚取微薄的路由费，并享受不公平的低价交易。你也可以在旅游时远程控制这个节点，比如使用 Zap 等。

点击获取 LND 源代码。或者 lightning-c 源代码。

点击获取 Zap 源代码桌面版、安卓版以及 iOS 版。

5. 轻钱包

要在硬盘上保存整个比特币区块链，并随时保持连接，这在你的移动设备上通常是做不到的。好在通过一些配置，我们可以在外出时也用上家里的节点。这里最好用的就是 Electrum Personal Server ，这是一个易于安装的软件包，可以装在你的比特币节点上。之后你就可以在笔记本电脑或手机端运行 Electrum 钱包并连接到家里的节点（可能是通过 Tor ）。

这么做可以保护你的隐私，因为其他 Electrum 节点将无法看到你的地址和余额。此外，它还能够让你在移动端上验证进账的交易是否被确认。

点击获取 Electrum Personal Server 源代码以及 Electrum Wallet 源代码。

6. 通讯

一旦你在家里拥有了个人服务器，根据服务器的容量和网络速度，你就可以配置它来改善生活的方方面面。比如，你可以用自己的 Jitsi Meet 服务器来主持视频会议，作为 Zoom 和 Google Hangout 等工具的替代方案。

你也可以运行你自己的 Jabber
服务器进行安全的端到端加密聊天。发起群聊的话，IRC 比较受欢迎，你也可以用 InsIRCd 自己跑。

现在你知道了这些，何不尝试建立个网站来存放你的加密密钥？或者自己搭个博客告别 Medium 或 Wordpress ？

你会发现，要在网上夺回自己的主权并没有看起来那么难。

LongHash，用数据读懂区块链。