闪电网络之我见：比特币网络的飞跃

**[printemps](http://www.8btc.com/author/10109" \o "由 printemps 发布) 2016-03-31 18:13 发布在**[**比特币**](http://www.8btc.com/bitcoin)[**16**](http://www.8btc.com/ln-network-glass-is-half#comment)**4377**

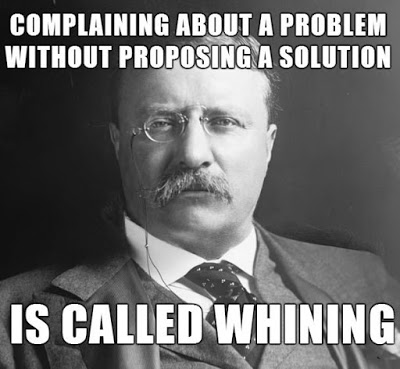
大约在三周前，我以“[闪电网络非常伟大，但它也面临各种类型的问题](http://www.8btc.com/lightning-network-so-great" \o "lightning-network-so-great)”写了一篇帖子，结果引起了大量讨论。那篇帖子的目的是为了表达我的观点：尽管闪电网络技术很了不起，但是它并非某种魔法，可以解决比特币网络扩展上的所有问题。

到现在我仍然这么认为，不过那篇文章语气的确有点消极，后来这种消极的语气在/r/btc/上面陷入了消极反馈循环。我花费太多的时间在闪电网络的消极方面，可能导致忽视了积极方面。本篇帖子将会专注于闪电网络的积极方面并提出一些能帮助我们进步的新观点。



上周，我接受了“Let’s Talk Bitcoin”播客有关闪电网络的采访。在采访中我试图全程保持积极。我在采访中指出比特币布道者Andreas Antonopoulos，Andreas非常的乐观，并且具有大局观念。

Andreas曾经不止一次讲到，即使比特币失败了，也不会对“大局”有太大影响。因为你不可能让数字货币全部“泯灭”。与加密货币革命的最终走向相比，比特币现在面临的短期政治或技术斗争真是相形见绌。与许多其他人一样，我不仅在情感上和智力上支持比特币，而且还在经济上投资比特币。另一方面，因为我对比特币进行了个人投资，所以我的很多观点难免会带有色彩。我希望比特币能够成功，而不是莱特币，狗狗币或者其他的加密货币。我把赌注压在比特币，自然是希望它能够获得长期的成功。



如上面引用的那句据称是泰迪罗斯福所说的：“抱怨问题却不提出解决方案，这叫做发牢骚。”我将这句话当作是警钟。与其把精力集中在消极方面，倒不如尽自己的努力寻找解决方案。这也是今天这篇帖子的目的，我希望你能够如此。这是一条几乎能够使所有投资比特币生态系统的人实现目标的前进道路。这条道路并非畅通无阻，并且没有保证。不过这至少是一种解决方案，并且还有我们能够努力的清晰共同目标。

**所以，首先，让我们看看这些共同目标，然后找出是否有实现的方法。**

比特币目标：

•比特币应该保持去中心化并且不受任何中央机构的压制。这是比特币最关键也是最重要的特性。如果失去，比特币的其他性质也会变得无关紧要。

•比特币应该成为地球上每一个人都能够使用的价值存储方式。

•比特币应该作为一种安全的价值存储方式，并且在通常情况下还能够不断升值。

•比特币规模应该能够容纳更多用户和更多支付交易，因为这样可以有利于比特币其他可取的属性。

•比特币应该不仅能够进行人对人交易，也应该能够进行机器对机器交易，并且能够几乎免费支持小额交易。

以上几点获得了大多数比特币支持者的赞同，而现在的问题是如何实现？

简单来说就是：通过网络层。今天，我们提到“比特币”（从技术层面上），大多数都会联想到比特币网络和区块链。就目前而言，比特币的确如此，但是从长远看比特币不只是比特币网络和区块链。

未来的比特币网络将由一层叠着一层的网络组成，就像是俄罗斯套娃。几乎所有的网络都是这样建造的。每一层的设计通常专注于一件事。如果你尝试设计一个单层网络，并且想让它做所有的事，那么通常会出现功能混乱，最终将不能完全实现目标。



有一点很重要，每次你在网络上添加网络层的时候，你并不是在创造一些与比特币分开的东西，而是在扩展比特币的定义。所有相结合的网络层仍然是整个比特币生态系统的一部分。

在未来，我们今天看到的核心比特币网络和区块链将会是整个比特币网络最底部的网络层。尽管比特币网络受到限制，但是比特币网络上的每一个网络层都能够减少或消除这些限制。

这就是我们未来几年所要做的。但是如果我们变得没有耐心而尝试从根本上改变核心比特币协议，使它成为“一刀切”的网络层，那么这样无异于杀鸡取卵。我认为没有人希望这种事情发生。

核心比特币网络决不会允许我们直接将比特币用户扩大到亿万人，同时还不失去防审查和不受国家监管的重要属性。然而，我们可以通过添加额外的网络层来扩大用户规模。

比特币网络不会单独这样做。闪电网络不会单独这样做。侧链同样不会单独这样做。但是，如果将这些网络系统结合起来，以一种展开的并且详细计划过的方法就能够实现这些目标。

当你听到如何从技术层面来完成的时候，听起来好像势不可挡。除此之外，别无他选。比特币网络相当的复杂，需要有合适的计算机科学背景才能够理解。当你把侧链、智能合约和其他先进的加密方法和网络拓扑结构带入到比特币网络时，比特币的门槛也升高了。这不应该被理解为一种问题或者消极现象。在世界各地，随时都会由新的大型软件项目被编写和部署。在人工智能和神经网络领域中，我们正在进行着一些惊人的工作；从自动驾驶汽车到能[创造艺术品](http://www.boredpanda.com/inceptionism-neural-network-deep-dream-art/)的计算机。



事实上，发展以完成这些事情的软件很复杂，但这不是一种困难，而是将要面对的挑战。那些功能酷炫的软件，其背后是许多工程师很长一段时间的辛勤工作。最后，无论有多复杂，一旦他们生产出了他们的产品，这些产品就可以改变世界。

接下来，让我们开始谈一谈比特币网络在哪些地方做得很好，而在哪些地方做得还不够好。

•比特币网络十分出色，它提供了一种分布式、免审查而又无需第三方的方式来储存和在世界各地转移价值。这是一个真正伟大的发明。

•比特币网络的支付费用还不够低，尤其是对于那些需要即时确认的支付。

•比特币网络不能很好地扩展到大量链上的活跃用户。

比特币网络维持了一个被称为“区块链”的不可篡改的数据库，其中记录了在其历史上的每一笔交易。维持这一分布式和防审查的数据库并不是免费的，它有现实世界中的固定成本，并试图将目前的风险包含到该网络最重要的特性中——去中心化和免审查特性。多年来，在该网络上已经发生了许多恶意攻击，如今该网络上已经充斥着被攻击者企图破坏该系统而留下的垃圾交易。这些恶意攻击的垃圾交易每一笔都被记录在区块链上，而且所有的发生时间被永远记录下来。[Satoshi Dice](https://www.satoshidice.com/) 做过的每一笔交易都被记录在区块链上，每个人都能查看。

直观地说，这几乎对任何人来说都是没有意义的。为什么每一笔小额交易（价值低至一分钱的百万分之一）都要被永远地记录在区块链上？如果区块链是免费的，或许这不会有问题。但区块链不是免费的。它是一种日益增长的网络资源，它增长得越大，就越难保持充分的去中心化。

幸运的是，这个问题的解决方案是一种被称为“[闪电网络](http://www.8btc.com/lightningnetwork-2)”。“闪电网络”能够从一条区块链（任何具有足够加密功能的区块链）上卸载所有低价值交易。它不仅可以将卸载掉低价值交易，而且可以实现比特币核心区块链永远无法实现的新功能。它可以提供即时防欺诈确认。它可以支持无限价值的小额交易，而且几乎是免费的。

闪电网络不是、也不应该被认为是与比特币网络分离的某种事物。它只不过是比特币网络的进一步发展，可以扩展和增强整个比特币生态系统。

正如在以前的贴子中指出的那样，闪电网络不是魔法（奇迹般的解决方法）。它并不能解决所有的问题。只是能够容易地卸载大批日常的低价值支付交易；这些交易是任何支付网络上所有交易中的大多数，但绝对不是全部。高价值的交易和需要开启或关闭支付通道的交易，仍然由核心比特币区块大小决定。

**那么，我们能做些什么呢？**

答案有一个，它相当于拼图的另外一块，是被称为“侧链”的概念。那么，什么是“侧链”？“侧链”是另一种区块链，相对于比特币区块链主链，它有自身的价值。

侧链几乎等同于现有的“竞争币”，但有一个关键的区别。侧链上表示的值是直接源自于比特币区块链的父链；使用了一种被称为“双向锚定（two-way-pegging）”的技术。

如今，绝大多数熟悉比特币的人也熟悉“竞争币”的概念。由于比特币仅仅是一种软件，任何人都可以制作一个副本，并推出自己的竞争代币。当然，这种新的代币并没有现实的价值，也不会具有最初所内置的任何安全性。今天已经有数百种竞争币，它们在独立的网络上运作并且相对其它竞争币有自己的价值。

侧链与竞争币相比的不同在于其代币的价值是直接来源于其父链上对应的价值。它还使用了一种名为“合并挖矿”的技术来获得它的安全性，充分利用其现有父链网络的安全性。

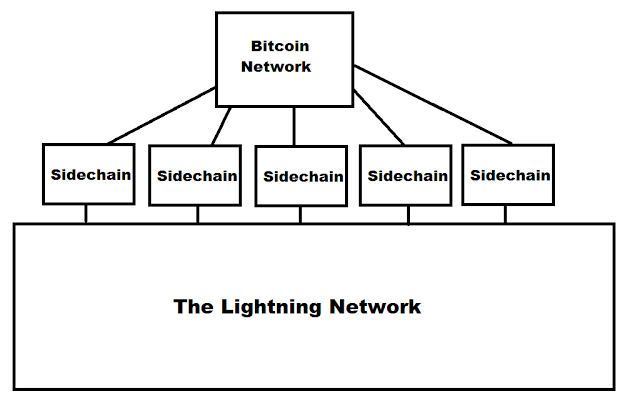
以这种方式，“侧链”相当于是比特币之上的另一层形态。在侧链上交换的代币的价值与比特币价值息息相关；因此，用户可以像比特币一样交易这些代币，因为它们是有效的比特币。

那么，接下来的问题是，合适的侧链可以有多少？答案是，我们需要多少就有多少。我们可以根据需要而只创建适量的侧链。

现在，对于拼图的最后一块，如果我们想将所有的低价值支付交易卸载并转移到闪电网络上，有一些重要的事需要注意。

闪电网络使用一系列相互连接的双向支付通道以促进资金流动，这些支付通道是基于使用哈希时间锁定的智能协议而建立的。这里有件令人惊讶的事。闪电网络与哪些区块链连接是完全不可知的！它不仅与比特币网络一同运作，而且对象还可以是任何加密数字货币网络，只要这些网络提供必要的智能协议功能。这意味着，闪电网络不仅可以对比特币网络实现，而且可以对任何侧链实现。

而且，这里是拼图的最后一块，因为闪电网络直接促进智能协议之间签名的更新，所以它还可以自由地在多个侧链同时进行互操作！



所以，解决扩容问题的方法类似于我们在解决其它网络系统中采用的解决方案。而不是试图使底层变得越来越大，越来越大，相反，针对日益增多的用户的要求，我们只是后台增设侧链数量，并将所有小的低价值交易移动到完全可互操作的闪电网络中。

这听起来是不是很复杂？嗯，的确。然而，当这个或类似的系统被充分执行，这对于最终用户而言将是完全不可见的。正如今天，尽管完全没有网络底层的基础知识，一般人还是可以浏览网站，同样，类似的一般人可以活跃在比特币网络上，而无需知道任何的底层技术细节及对其任何操作的理解。到底是会简单地打开他们的比特币钱包，还是会通过一些侧链来使用闪电网络，这对于他们来说都是完全不可见的。

这次讨论的目的，只是提出了可以解决比特币全球扩容问题的建议，我们或许应该这样做，而不是试图通过增加它使它变得过于庞大，失去了它的最重要的属性并使核心比特币网络面临风险。相反，我们通过在其上添加附加层，扩展以发展比特币生态系统。这就是今天计算机网络中大多数事情如何重新规定的方式。你不会通过构建规模越来越大的电脑来解决问题，而是使越来越多的计算机投入到该问题中。一旦你可以创建一条侧链，你就可以创建数十条或数百条。一旦你有一个闪电网络能够对某一条区块链实现，那么它就可以很容易地对数百条区块链实现。通过多个网络层的互操作，问题的解决就可以、将会、应会完成。而不是试图发展单层网络来做一些设计时没有考虑的事情，不然运行中所遇到的风险可能会在过程中摧毁它的关键价值。

**重温我对闪电网络的评价**

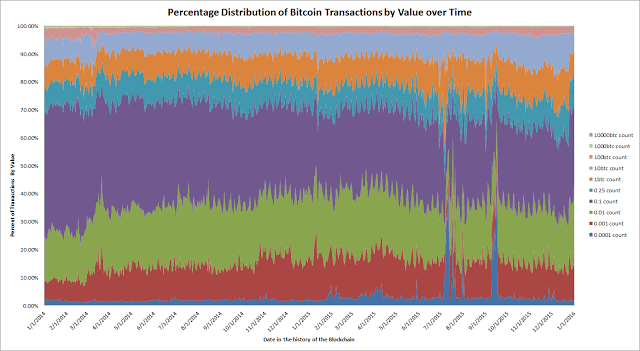
最后，我想从“半满的杯子”（从积极的一面看）的角度来重申一下我对闪电网络的评价。坦率地说，我的评价主要归结为两点：

（1）闪电网络尚未真正存在，而且很可能在很长一段时间里，它都不会有能力处理相当大比例的比特币交易；

（2）闪电网络没有能力去卸载几乎所有的比特币交易，并且在较大数额的交易上存在风险。

尽管这两点仍然生效，但我们应该关心，一旦它准备就绪能起到什么作用。

我在以前的帖子和LTB播客中多次指出，闪电网络在卸载比特币网络中的低价值交易上起到了出色的作用。这就产生了一个问题，实际上现在每天到底有多少低价值交易发生呢？我从区块链中找到了一些统计数据，以下是这些数据所得出的结果。



*此图表是按价值大小将2014至2015年的比特币网络上的交易进行百分比分布划分*

你应该能够看到的是，比特币网络上的所有交易中30％左右是0.01个比特币以下；这些交易的价值比5美元还低。所有比特币交易中大约60％小于0.1个比特币（价值约40美元），70％的交易价值低于0.25个 BTC；或者说低于100美元。

虽然我仍旧相信，闪电网络在卸载高价值交易时容易出现问题，但是，我还是认为它在价值大约100美元或更多的交易发生时能够很好地运作。这意味着，一旦有了一个功能完整的闪电网络，它或许能够卸载所有支付交易中的约70％；腾出空间为更多的用户存储价值，进行高价值的支付，或着打开和关闭支付通道。

毫无疑问，这对于推广比特币的目标而言显然十分有利。

**那么，这将会实现什么？**

•它将允许现有的比特币网络支持可能4倍于今天的用户数。

•这将为所有低价值支付提供以闪电网络的形式的即时确认。

•这将实现目前不可能的各种新型支付方式（真正的小额交易）。

一旦隔离见证（SegWit）正式展开，而且钱包升级至支持该技术，我们将实现1.7MB有效区块的大小限制，反过来看，这将支持更多的用户。如果在此之后的发展过程中提升至2MB硬叉，那么它将会支持更多的用户。

这是一条清晰的路径，而无需调用任何侧链，并在未来几年使比特币大规模扩展（10倍以上的用户数量）。

这就是说，就算我们没有指出，它还是可以发展到支持100倍，甚至1000倍以上的人的地步。要做到这一点，我们将需要为那些进入生态系统的人提供附加层。我的主意是，为人们保有价值而提供附加的侧链，使用闪电网络作为中介为他们提供桥梁。无论是我的构想还是其它关于侧链的想法，都还有待观察。问题是，如果我们给工程师足够时间来解决这些问题，那么比特币扩容将会没有限制，避免大幅增加核心区块大小的限制至极端或者有些人说的危险水平。

所以，我建议比特币社区应表现出一定的耐心。我们不应该做任何过于冒险或危险的事，威胁到“下金蛋的鹅”（the goose that lays the golden eggs，即摇钱树）。为了帮助实现我们所有人的共同目标，存在技术上的解决方案，虽然，不可否认这些技术上的解决方案的构建需要时间和耐心。

**最后，针对以前我在一篇关于闪电网络的帖子中提出的问题，让我来增加一些额外的评注。**

•闪电网络尚不存在。这仍然是真的，而且仍然值得关注。现实情况是，闪电网络在相当长的一段时间内都不能卸载大量的比特币交易。这就是为什么社区如今正试图提高区块大小的上限，先是隔离见证（SegWit），后是2MB HF，就是为了让我们有一些喘息的空间，直到核心网络可以提供一个真正的扩展效应和卸载小额支付交易功能。

•闪电网络扩展的是交易而不是用户：这不完全准确。由于闪电网络需要链上交易以运行，所以开通支付渠道的用户数量仍然要由核心比特币区块大小来决定。但是，如果你把比特币网络中70％的小额交易移到链下，这确实能在我们达到上限之前容纳更多的用户，比我们今天预计的要更多。更重要的是，使用侧链锚定价值，闪电网络在侧链之间互操作，都是我们在比特币网络一旦达到上限时，我们可以接入更多的用户的一个例子。现实情况是，我们很想在比特币网络上拥有更多的用户。这自然会导致价格和整体效用的增加。不过，这些都是“好问题”。如果我们有这么多的人进入，我们需要发展比特币生态系统，这将一定是个很好的状态。我建议使用侧链或者其他我们安全地插入到网络堆栈中的层，因为我相信软件工程师能解决这个问题。尤其是现在我知道闪电网络能够自由地在多个区块链之间同时进行互操作。

•如果闪电网络存在，人们不会立即相信它。这种说法仍然是正确的。不过，我只是提出了用闪电网络来分担100美元以下的小额交易。我想大多数比特币用户愿意拿出少量的比特币来测试一个早期推出的闪电网络测试版本，也许只有5美元，但随着时间的推移，人们看到系统功能运作良好，我相信那时他们将有自信在一段较长的时间内开通一个价值更大比如100美元的支付渠道。

•如果闪电网络存在，将有一段时间没有钱包商或支付商愿意支持它。这句话也是对的。这就是为什么即使闪电网络的一些版本推出了6个月，仍然需要很长一段时间，它才能被完全整合到生态系统中。虽然完成这个整合的过程需要一段时间，但是考虑到该技术的前景，我想我们应该去尝试一下。

•闪电网络在处理大额交易上也存在问题。我仍然认为这是对的，但我认为这不重要。在我看来，闪电网络的目标是将小额交易移动到比特币链下，而大额交易仍然发生在链上。

•闪电网络支付渠道不仅无法推动而且会导致一定程度的中心化。我仍然相信这对于大额交易使用案例来说是对的，但是对于小额交易来说不是问题。自从我开始写关于闪电网络的文章，我了解到闪电网络的工程师们正在尝试鼓励一种网状网络模型，在这个模型中，每一个用户都不仅维护一个单一的支付渠道，而是四个或更多。用户之间维护的联系越多，闪电网络就越可能保持去中心化、真正点对点。只要这些通道仅锁定相对少量的价值，就不会出现我先前讨论过的中心化风险。

•不平衡的支付渠道和锁定大量的比特币交易使得闪电网络面临经济上的挑战。再次强调，当你的目标是利用闪电网络转移所有的支付交易，包括大额交易时，这才会成为问题。相反，如果你的目标是为了方便小额价值转移的话，并且每个参与者都维护多个支付渠道，这不应该是一个需要担忧的重大问题。

•把资金锁定在支付渠道中意味着会承受市场波动的影响。和前面一样，如果你开通一个大额支付渠道，这当然是一个问题，但是，对于一个小数目比如100美元，那么大多数人就更容易忍受一段时间内的一定波动。

•闪电网络的用户有效地拥有“热钱包”。和前面一样，如果你把所有的钱都锁定在闪电网络支付渠道内，那么这是一个合理的担忧。然而，对于少量的资金来说，大多人都视之为一种可接受的风险，就类似于我们今天在手机热钱包中存储少量的资金，以便随时使用。

我之前在文章中提到那些反对意见都是针对那些想要将所有的支付交易从比特币网络上转移到闪电网络中，这都是不切实际或者说存在太大风险。我今天仍然这么认为，但对于小额交易来说，是没有问题的，如上图所示，小额交易占了比特币网络上交易的近70％。

当我们发现我们的比特币网络已经被高价值的交易或者更多的用户完全填满，甚至在SegWit和2MB HF实施后，那么我们可以安全地在比特币生态系统中增加额外的层，便能适应这些新用户的需求。