闪电网络究竟是什么，现在怎么样了？

[**面神护法**](http://www.8btc.com/author/1163)**2015-09-22 10:18 发布在**[**币头条**](http://www.8btc.com/featured)**,**[**比特币**](http://www.8btc.com/bitcoin)[**6**](http://www.8btc.com/lightningnetwork-2#comment)**12714**



2015年2月份，约瑟夫·朴恩 （Joseph Poon）和萨帝厄斯·追亚（Thaddeus Dryja）发布了一篇他们称之为“[闪电网络](http://www.8btc.com/trustless-off-blockchain)”的草稿。当时它仅仅是一份不完整的建议，并且没有代码，但它引起了比特币技术社区相当的兴奋：这不足为怪，因为这个构想允许近乎即时的任意方之间的[比特币](http://www.8btc.com/what_is_bitcoin)支付！本文总结那篇草稿中提到的想法，以及它打响了发展非信任依赖的链下比特币交易第一枪之后，闪电网络最近的发展。

闪电网络是什么：比特币的一个缓存

一件可能的事情是，两方建立一个交易链，交易链中的交易只有最后一笔需要真实的进入比特币区块链。这就是简单的支付通道背后的思路，而这种支付通道，现在已经存在了；你可以一直向某人发送可替换的交易，每次额度比上一次大一点点，一旦达到某种条件，通道被终结，只有最后一笔支付向全网广播。

事实证明，只需要少量几乎没有争议的比特币升级，人们就可以生成更加通用的的支付通道，它允许双向支付，也允许“条件支付”。条件支付允许你构建一个支付网络。实际上，你可以通过安全和非信任依赖的方式设定“如果鲍勃支付了卡罗尔，我就支付给鲍勃”。一些事情发生之后，你的钱包就会自动向比特币网络广播这个条件支付交易，然后等待。

闪电网络论文提出了生成通道和支付网络的机制。不过相似的想法已经流传了一段时间了，是论文将他们汇集在了一个有力的聚焦点上。最近在苏黎世，克里斯坦·迪克和罗杰·沃顿华夫（Christian Decker and Roger Wattenhofe）提出了做同样的事情的不同的机制，所以，如今这是比特币创新的一个热点。

进展如何？

2015年5月，[Blockstream](http://www.8btc.com/blockstream-sidechains)雇用了我（经验丰富的Linux内核和开源开发者），随即我投身闪电网络的开发。我已经提交了一系列关于闪电网络初始论文草稿的技术解释，并与约瑟夫·朴恩 （Joseph Poon）就闪电网络如何实施的可能性，进行了数次探索性的交谈。

我们创建了一个公共邮件列表，6月份我开始在Github上提交原型代码。这些用于实现上文提到的通用通道和条件支付，更加技术的说法是，哈希时间锁定合约（Hash Time Locked Contracts ）。采用的方法是最近公布的起草阶段的论文上提到的方法（有少许变化）。这些代码在Blockstream的α元素侧链（[Elements Alphasidechain](http://www.8btc.com/elements) ）上运行，该侧链已经具备了比特币需要的支持闪电网络的必要特征。我们现在正在完成节点间网络协议的第一版草稿，其中包括一个完整的状态机，还有已经在邮件列表上宣布的处在不同开发阶段的两个不同的应用。我们还在尝试和选择一些问题的解决方案，比如中间节点如何发现和负载以及其他的技术问题。

有的人问，为什么我们让一个开发人员全力投入闪电网络的开发？Blockstream致力于提升比特币，使比特币能够支持更多的应用和使用场景。基于我们的工程开发工程和协议的经验背景，像闪电网络这样提高比特币的易用性就是我们的核心兴趣所在。作为一家专注于开源发展的公司，显然闪电网络这个新的技术领域也是开源和免授权许可的，就像比特币本身那样。

还有些人从比特币的可扩展性对闪电网络表达关注：闪电有助于比特币的拓展性吗？长期看来可能是吧，当小额支付在闪电网络中成为常态，只有锚定交易和最终交易进入区块。但是如果闪电网络取得广泛的成功，由于大量用户涌向比特币，也会不可避免的对区块链造成可观的压力。也许支出艺术家的小额支付会成为比特币的杀手级应用呢？也许即时支付会引发比特币的第二次创新浪潮呢？只不过目前没人能知道。

将闪电网络变成一个真实的可用的产品的底层工程正在完成，在不远的将来，它将是开发者的游戏场。这是一项令人兴奋的工作，欢迎其他人加入进来。

在‘实测’之前，要哪些步骤？

除了书写闪电代码和定义协议之外，还有一些特征要事先被比特币采纳：

1.OP\_CHECKLOCKTIMEVERIFY ( BIP 65 )（比特币改进提议65）

2.OP\_CHECKSEQUENCEVERIFY ( BIP 112 , which needs BIP 68，比特币改进提议112，并需要比特币改进提议68为前提 )

3.Malleability fixes ( BIP 62 比特币改进提议62)

闪电网络看起来会是什么样子？

我和闪电网络论文的原始作者约瑟夫·朴恩最令人心驰神往的交谈之一就是，当我们畅想，一旦付诸实现，闪电网络是什么样子的。我们设想，通过与5个随机节点建立通道，你的手机可以与闪电网络建立实时的联系，然后，你可以用它想网络上的任何人做不等的小额支付。

更有趣的是，通过将[比特币](http://www.8btc.com/what_is_bitcoin)移回自身，你的手机APP也可以为网络提供流动性。举例说，中本聪自传的闪电销售，引发了指向销售者的单向的大量交易，过载的交易通道可能会向往相反方向移动资金的人提供小费，因此这些人就能收集更多的小费。如果你的五个随机通道正好做了这件事，你的手机APP就能向自身发送一些币，获得一些小收益。

这真的会发生吗？我不知道！但这正好说明了，如果一个可用的，快速的点对点微支付网络存在的话，我们的世界会有怎样的不同。