揭穿关于闪电网络11个常见的谬见

[**面神护法**](http://www.8btc.com/author/1163)**2015-10-20 14:36 发布在**[**区块链**](http://www.8btc.com/blockchain)**,**[**币头条**](http://www.8btc.com/featured)[**4**](http://www.8btc.com/11-myths#comment)**6694**



今年年初，约瑟夫•朴恩（Joseph Poon)和萨帝厄斯•追亚（Thaddeus Dryja）发布了闪电网络白皮书。在白皮书中，他们从理论上提出了，如何在比特币区块链之上的层面上，实现实时和低成本的比特币交易，同时增强比特币的可扩展性。

由于区块扩容争论的影响，最近闪电网络受到了大量的关注。但不幸的是，谬见流传，遍及各处，朴恩和追亚的理念如同一个新颖的角度被抛入一场旷持日久的争论之中，有的人称之为解决一切问题的灵丹妙药，而有的人则人称之为比特币开发社区的腐败之源。

这篇文章不是要在技术层面上解释闪电网络如何实现。此类的解释可以在[这里](http://lightning.network/lightning-network-summary.pdf)和[这里](http://rusty.ozlabs.org/?p=450)看到，那些想要看到更加详细的技术细节的人，可以在[这里](https://lightning.network/lightning-network-paper.pdf)看到。

相反，这篇文章列出了围绕闪电网络的11个常见的谬见，以期正本清源。

谬见1：核心开发者故意让比特币的性能摆烂，强迫用户转移到闪电网络

朴恩和追亚等人自己的基于闪电网络的初创企业Blockstream，是目前为止唯一一个资助闪电网络开发的公司。值得注意的是，这个手握2100万美元种子轮投资的企业雇佣了保罗•罗素（Paul Rusty Russel）来从事闪电网络的开发（保罗•罗素，知名自由软件程序员和倡导者，以linux kernel和filesystem hierarchy standard的开发而知名，江湖人称生锈的罗素）。

与此同时，一些最著名的比特币开发者，比如格里高利•麦克斯韦（Gregory Maxwell）和皮特•乌里（Pieter Wuille）也在Blockstream的工资单上。这导致一些人认为Blockstream的行为是居心叵测的。他们宣称这个公司阻挡任何提高区块大小的建议，以此驱动交易费的升高，强迫比特币用户转而使用闪电网络。

然而，这个逻辑是很牵强的。

**第一**，不仅仅是Blockstream的雇员支持小区快。区块大小论战的“去中心化”派包括了很多不同类型的程序员和比特币参与者，其中包括比特币核心首席开发者范德兰（Wladimir van der Laan）、比特币核心开发者彼得•托德（Peter Todd）数字货币老兵尼克•萨博（Nick Szabo）、比特币基金会前执行董事乔恩•马特尼斯（Jon Matonis）、bitcointalk.org和r/bitcoin的管理“theymos”等等很多人。

**第二**，固然一些知名的 Blockstream 雇员和比特币核心开发者反对提高区块上限——其中最著名的是麦克斯韦和乌里，但要看到，他们在Blockstream成立之前，在闪电网络的白皮书发布之前，就对提高区块上限持怀疑态度。他们都是最早的一批区块大小保守主义者，2013年早期这个话题首次被提出时，便是如此。

**第三**，即便比特币网络的交易费真的上升了，也完全不会“强迫”人们去使用闪电网络。只要有人愿意，他还是可以直接使用比特币网络——只是多花一些钱。如果有任何原因激励人们使用闪电网络，这些原因也不应该被归类为“被强迫”。这是值得商榷的，因为在资金转账方面，存在大量的备用选择。

**第四**，最重要的是，你应该相信，小区快更加合理的说法，优于“强迫用户使用闪电网络”的说法。区块大小的问题由来已久，几乎所有的开发者都同意，超大区块会带来安全上的挑战。对于多大的区块算是“超大”尚有争议，但不能否认的是，在可扩展方面，闪电网络可以解决真实的业已存在的问题，更不用说闪电网络花费和速度的优势了。

谬见2：被Blockstream雇佣的核心开发者不涉及利益冲突。

另一个极端是，一些既被Blockstream雇佣，又从事比特币核心开发的开发者声称他们同时参与的两个工程是完全独立的，不涉及任何利益冲突。

事实上，这并不是真的，他们的声明可能是术语混淆的结果。

根据维基百科的说法“利益冲突”（COI）是指这样一种情形，一个人或组织涉及不同的利益，这里的利益可以是经济利益也可以是其他利益，其中之一可能会腐蚀个人或组织的行为动机。

在这个定义中，”可能“这个词是关键。利益冲突不是说，这些被Blockstream公司雇佣的开发者在做关于比特币的工作时，一定会受到公司影响、存在利益冲突。而是他们有可能受到影响，这就够了。即便麦克斯韦、乌里和其他人可以完美地区分两个身份，可以尽力诚实得体地同时为Blockstream和比特币核心工作，他们的两方参与依然构成了利益冲突。

然而，值得注意的是，对比特币开发者来说，由于不存在独立的和可持续的资助模式，开发社区也许总是会置身于利益冲突的尴尬之中。这是否成为问题，又会成为多大的问题，尚需讨论。但是对这个问题，迄今尚没有提出清晰可行的解决方案。

谬见3：闪电网络将会被Blockstream控制

有时会有人说，Blockstream会有效地控制闪电网络，因此他们将能控制人们如何使用闪电网络，闪电网络能被用来做什么。

这种说法不完全是错误的。如果Blockstream开发了功能完全的闪电网络，他们会在技术上控制代码库。

然而，闪电网络是一个开源项目。不像比特币，在协议规则上，这个开源项目甚至不需要像比特币那样获得所有比特币用户的共识。这意味着任何人都可以在他们想要的时候分叉闪电网络，以他们想要的方式调整代码，发布自己的版本。只要存在互相联系的节点，甚至有可能，人们使用不同版本的闪电网络互相交易。

事实上，在朴恩、追亚等人建立自己公司的同时，竞争性的闪电网络，比如[Amiko Pay](https://github.com/cornwarecjp/amiko-pay)，已经在实施了。除此之外，还有两种闪电网络实施方案Thunder Network和[Stroem](https://www.strawpay.com/docs/stroem-payment-system.pdf" \o "stroem-payment-system.pdf)也在实施当中。

谬见4：闪电网络需要的大型支付中枢将会控制网络

有一些讨论认为，闪电网络将损害比特币具有的一些最有价值的特点，比如“去中心化”和“审查免疫”。根据这种说法，闪电网络需要大型的中枢来执行绝大多数的交易。这就可能屏蔽特定的交易，比如给维基泄密和其他政治异见人士的捐款。

这种说法很大程度上是基于这样的前提，绝大多数有效的网络配置（配置需要最少的中枢从任意一个节点连接到其他节点）都是中心辐射模型（hub-and-spoke model）。因此，闪电网络也许也会自然地进化出相似的中心辐射模型。这个网络中的中枢可能是几乎每个人都要用到的大型比特币实体。比如交易所、钱包服务商或者支付处理服务商。

重要的是，要认识到，就像比特币自身一样，闪电网络中的任何人都可以在任何时间，同任何人开启支付通道。因此，如果闪电网络中枢浮现出来，他们也不能控制网络。如果所有存在的中枢都拒绝开启给维基解密捐款的通道，其他任何人都可以自行开通，绕过这些中枢。事实上，维基解密自身也可以成为一个中枢。

谬见5：闪电网络的中枢会侵犯用户隐私

既然闪电网络中潜在的中枢控制资金流是明显不可能的，那么对这个系统更精准一点的批评就是，这些中枢可能会追踪网络上的支付。因为绝大多数日常交易会通过这些节点，他们可能会观察到资金流，进而侵犯用户的隐私。

这种说法可能是对的，但是如今在比特币网络上的所有交易，都已经是公开的，任何人都可查询。另一方面，在闪电网络上，很多交易都仅仅是中枢运行人才可以看到的。因此，闪电网络只可能比比特币网络提供了更多的隐私性，而不是更少。

除此之外，最近闪电网络协议的更新显示，闪电网络上的日常交易可以通过类似信息在洋葱网络（Tor network）上传递的方式进行。这样，闪电网络上的所有节点都只知道一个交易从哪一个直接相连的节点来，发送到哪一个直接相连的节点去。但是却不知道是哪一个节点发起了交易，哪一个节点最终接受了交易。如果这一点改进得以实现，闪电网络将比如今的比特币网络提供更多的隐秘性。

谬见6：Blockstream将利用闪电网络赚钱

有时候有人会说，Blockstream力推闪电网络（同时阻碍提高区块上限），是因为他计划通过运行闪电网络中枢来收费。

可能闪电中枢真的会为自身的中间人服务收取费用。既然任何人都可以开设一个中枢，Blockstream也可能会这么做。

但正是由于任何人都可以建立一个中枢并且收费，这就意味着任何人都不可能通过这个牟取暴利。在自由市场里面，竞争会最小化每一个参与者的利润。

事实上，没有什么理由可以相信，Blockstream渴望参与金融中间人的业务。到目前为止，没有任何迹象表明，他们想要或者部分地参与金融中间人。

谬见7：Blockstream通过闪电网络赚不到钱

既然Blockstream将不会有能力控制闪电网络，看起来也不会通过收取闪电中枢服务费谋取暴利，那么问题来了，为什么公司要投钱开发这个网络呢？

要回答这个问题，我们首先应该明确，Blockstream并没有将巨额的资金投入到闪电网络，公司只是为生锈的罗素（Rusty Russel）提供一份薪水，仅此而已。假设罗素的工作非常出色，但闪电网络并不是什么几百万美元的大动作。

但是问题还没有回答，到底为什么Blockstream要资助闪电网络的开发？

最可能的答案是（Blockstream 也并不完全确定），到目前为止公司的解释是，他们相信这个东西最终会很有价值。在一个数百万或数十亿美元使用闪电网络的世界里，Blockstream相信总能以某种方式获取利润，比如通过支持、培训和咨询服务。

红帽公司（Red Hat）已经提供了一个范例。红帽公司是美国的一家跨国软件公司，与其他开源项目有着相似的商业模式，并主要以Linux操作系统知名。该公司主要向分布在全世界的客户提供各种Linux相关服务。年收入达到10亿美元以上。红帽公司的业绩可能是任何一个闪电中枢永远也不会达到的。

谬见8：闪电网络会要求比特币网络进行硬分叉

另一个反对闪电网络的说法是，闪电网络还远不到确定会施行的地步。就像对区块扩容争论一样，他们说施行闪电网络会要求比特币协议进行有争议的改变，甚至是硬分叉。

为了支持闪电网络，比特币网络确实需要几个升级。其中最著名的是，延展性问题（比特币改进提议62）和锁定时间的选择（比特币改进提议65）。然而，所有这些升级都不需要硬分叉。他们可以采用软分叉的方式，在技术层面上，没有任何一个上述软分叉是有争议的。

（当然，如果人们愿意，这些升级也可以通过硬分叉的方式来实施，但这是不必要的。）

谬见9：有了闪电网络，就没有必要进行区块扩容了

闪电网络是在两个相连的用户之间进行几乎无限的交易，同时只在比特币区块链上留下两个交易记录。因此，有时候闪电网络就像突然杀出的英雄，好像可以解决比特币存在的所有可扩展性方面的问题，引起人们或明或暗的欢呼。

固然，闪电网络在很大程度上可能有助于解决比特币可扩展性的问题，但是认为将来完全不需要进行区块扩容，还是太过言过其实了。如果比特币的潜力完全发挥出来，每天全球数以十亿的人使用比特币，这些用户依然需要在比特币区块链上写入交易才能开启和关闭闪电网络通道。在这样的场景下，可以负责任地说，1M的区块容量确实太小了。

事实上，朴恩和追亚在他们的白皮书中承认，区块大小限制需要上升，他们估算：

”如果假设在去中心化支付网络中，一个人平均每年进行3次区块链交易，在理想情况下，1M大小的区块限制能够支持3.5亿用户的使用（假设每兆含2000交易）。这是不够的，为了满足全世界每一个人都能使用比特币，区块扩容还是非常必要的……尽管闪电网络看上去会在短期内缓解区块扩容的压力，但如果比特币在全球范围被广泛使用，长期来看，增加区块大小是必要的。“应该提出的是，闪电网络不仅仅是一个比特币可扩展问题的解决方案。它可能首次提出了安全即时确认的机制，也使价值很小的小额交易又一次在经济上成为可能。事实上，如果大量的比特币新用户采用了这些特征，闪电网络的发展可能会对比特币的可扩展性提出挑战。

谬见10：闪电网络很简单

当人们在争论区块扩容的问题时，一些去中心化派的人士指出，闪电网络可以轻易地解决绝大部分比特币的可扩展性问题。有时候这听起来让人觉得，闪电网络轻而易举。事实不是这样的。

首先，闪电协议本身只是一件进行中的事情，生锈的罗素、朴恩、追亚等人正在尽其所能实现它，但这是一个长期缓慢的过程。即使是概念本身，也不是一成不变的。一些问题尚待解决，基于此，不能言之凿凿地说，闪电网络最终一定会实现。

还有，像上面提到的，为了闪电网络的安全实施，比特币协议本身也需要改进。一些要求的改进，就像闪电网络本身一样，不是那么容易实现。基于以上，闪电网络可能需要相当长的时间才能实现（如果真能实现的话）。

最后，钱包软件也需要调整。最可能受影响的是个人用户的钱包——Core、XT、以太、移动钱包等等。他们将需要某种插件。用户届时才能选择，在比特币区块链上进行交易，还是在闪电网络上进行交易。但就像闪电网络一样，这将如何实现，它会是个什么样子，都还是未知数。

谬见11：迫切需要闪电网络

第十一个谬见与其说是谬见，不如说是争议。

首先应该说明，即时和廉价的交易有多大的迫切性，是很难说清楚的。到目前为止，比特币区块链不具备这样的特征，因此也很难说清楚这些特征有多大的需求。

常见的说法是，为了解决比特币的扩展性问题，急需闪电网络。有一些进步派人士也以闪电网络远没有准备好的理由，论证区块大小急需提升。他们说，如果区块满了，交易费会上升到令人难以忍受的水平，交易的确认会变得很慢（甚至得不到确认），比特币甚至会变得过载。没有闪电网络这样的选择，结果将会很坏——也许会是灾难性的。

就像上面提到的，闪电网络远远没有准备好，无疑是一个事实。幸运的是，区块尚没有填满，至少没有以引发大麻烦的方式上升。即便是Bitcoin XT的开发者迈克•赫恩（Mike Hearn）和加文•安德森（Gavin Andresen）——两个最著名的大区块鼓吹者——也承认大概一年之后麻烦才会出现（还有人认为需要更长的时间，麻烦才会出现）。这意味着闪电网络可能有至少一年的时间来部署和获得支持。

一年的时间是否够用，是有争议的。在一篇帖子中，赫恩表示，没有任何可行的技术协议可以在一年之内获得广泛接受，闪电网络也不行。而另一些人，则乐观一些，尽管大范围内部署闪电网络这样的东西，一年时间并不是很长的时间，但在比特币的世界里，一切皆有可能。

更重要的是，很多论战中的去中心派表示，从一开始，区块变满就不像另一方说的那样严重。交易费可能会上升一点，但并不是所有的交易都会在第一个区块获得确认，这不是不能接受的局面。如果是这样的话，基于比特币扩展性的理由论证闪电网络的迫切性，可能需要更长的时间。

感谢闪电网络白皮书的共同作者萨帝厄斯•追亚（Thaddeus Dryja）和Blockstream的闪电网络工程师生锈的罗素（Rusty Russell）为本文早期的草稿提供的反馈意见。