探索比特币闪电网络的中心化风险

[**alexander**](http://www.8btc.com/author/14583)**2016-05-10 14:39 发布在**[**比特币**](http://www.8btc.com/bitcoin)[**2**](http://www.8btc.com/lighting-network-centralization-risk#comment)**2020**

绝大多数的比特币核心贡献者认为，对于无数的新用户来说，[闪电网络](http://www.8btc.com/lightning-network)被视为比特币扩展的最好选择。但是该系统还未在比特币[区块链](http://8btc.com/article-44-1.html)上实施，所以致使很多人产生疑惑，对没有经过测试的解决方案抱有如此大的希望和信任是否明智。

[](http://7fvhfe.com1.z0.glb.clouddn.com/%2540%252F%2F/wp-content/uploads/2016/05/QQ%E6%88%AA%E5%9B%BE20160510143525.png)

最近在旧金山的Coinbase办公室的一个活动中，闪电网络的创造者Joseph Poon和Tadge Dryja展示了他们通过广义的网络支付渠道扩展比特币的设计。在他们的谈话中，Dryja和Poon回应了观众对于闪电网络通过某种称为超级节点（supernodes)的可能最终变为中心化的担心。

一些节点会比其它节点连接的更好

Coinbase联合创始人 Fred Ehrsam在闪电网络展示过程中提出了超级节点问题，Poon回应称：

“我认为某些节点比其它节点连接的更好。使这些节点不可辨认和容易更换是很重要的。当它成为高度连接的节点，它不会如此的廉价，也不会成为像BitTorrent或者 Skype之流的超节点（Skype五年前或十年前运作的方式），仅仅是因为它们的成本涉及其中。”

这里Poon提到的成本主要指为了进行网络支付而“锁定”比特币。从消费者的角度来讲，Dryja和Poon提出锁定钱这种说法是不恰当的，因为使用者仍然可以在闪电网络上使用这些钱。对于那些希望通过网络支付赚钱的人来说，存在一个时间价值的成分。

虽然许多比特币的持有者希望通过闪电网络让他们的持有能有所回报，Dryja和Poon解释说这个网络不会像某些人期望的那样成为淘金热。且两人都认为在网络上的费用将会为零。

Poon：对于这些超级节点并没有什么益处

Ponn没有过于担忧这些潜在的良好连接的节点的主要原因在于创造这些超级节点并没有太多的经济刺激。他解释说：“这并不是不可能，而是在于，你能从中得到什么。”

Poon对于这一观点解释说：

“如果你有无穷的钱且想要接触到每一个人，那么，这是可以实现的，但这对你来说并没有什么真正的好处，作为一个节点，也是同样的。这就是为什么我并不真正去担忧节点拓扑结构正在中心化，因为并没有什么网络影响是有利于你的。因为它们是相对可以改变的，所以如果你开始对它收取一定的租金，其他人也会做同样的事。”

Poon提到说在网络中良好连接的节点可能会被用于小额支付。这是因为与路由支付有关的更低的预支付费用价值大约在一便士左右所以可以用在买一杯咖啡这样的事情上。

Dryja说在两个对手方间这样的直接支付渠道可能更有优势，但这样的支付方式由两个对三个或者四个的情况下就没有太多的区别。

BitGo的Jameson Lopp的进一步分析

BitGo工程师和 Statoshi.info创造者Jameson Lopp最近一直在考虑和撰写关于闪电网络面临的技术挑战文章。比特币杂志接触到Lopp关于他对于Poon评论的观点。关于去运行一个超节点的刺激（或缺乏），Lopp认为：

“如果你认为有路由费用是积极的（因为在有些情况下它们是消极的），为了去收取费用那么就有了刺激去运行一个高度连接的路由节点。从另一方面来说，就会有了抑制去运行普通路由节点因为当机器连接网络时就要求保持私匙“暴露”，这是相当冒险的。”

Lopp提到“这些相反的动力之间的平衡如何稳定下来还有待观察。”

Lopp还提出对于闪电网络的恐惧不仅仅是基于中心化问题，更多是与某一特定中心化类型相联系的风险，这种风险可能会出现问题。他说，“对于任何的中心化争论的问题是你需要解释对于潜在结果的恐惧。”

Lopp继续解释说那些使他担心的闪电网络的可能中心化方面是节点网络的拓扑中心化，因为它会导致网络在有压力的情况下更脆弱和倾向于坍塌。

Lopp说到一些实体在网络上路由大多数的支付，如果这些实体运行许多的节点就可能不会有这么多的问题。但是，他接着说：

“将会有一个担忧就是有些实体可以选择将所有的节点关掉，会造成严重破坏直到闪电网络的使用者通过链上交易重新建立起新的渠道去“治愈”网络。”

Lopp还提到可能会有审查机构和隐私问题会被牵连到对于一小部分的实体的中心化：

“有一小部分的实体集中化将会导致审查和隐私问题，导致这更加困难去路由不配合的实体或那些为了去匿名化而去收集数据。”

Blockstream的Rusty Russell，就致力于自己的闪电网络的安装启用，提出说他认为 layer-2协议将有可能成为在那些希望保持隐私和废止它的人之间的一场Tor式军备竞争的特征。Russell和其他闪电网络发展者也致力于对于网络的Tor式洋葱路由。

Lopp告诉比特币杂志说对于闪电网络的许多担忧只有和内存池储存联系在一起才会显现出来，它会使得在闪电网络上重新建立渠道很困难。

Coinbase担忧着中心化风险

Coinbase的代表在Dryja 和Poon的展示中更担忧在闪电网络中的潜在中心化风险。闪电网络的创造者们很感激对于在比特币交换中的去中心化的重要性的承认。

至少一个Coinbase的代表提到这家公司没有必要朝着从闪电网络中赚钱看去。目前，它被简单的视为一种改善产品和服务的途径。