闪电网络非常伟大，但它也面临各种类型的问题

[**next**](http://www.8btc.com/author/11008)**2016-02-29 10:31 发布在**[**比特币**](http://www.8btc.com/bitcoin)[**2**](http://www.8btc.com/lightning-network-so-great#comment)**2301**

在这篇文章中，我想跟大家分享我关于闪电网络的一些看法。首先，我认为闪电网络的这个理念非常先进。这是一个非常惊人的‘智能合约’应用，它能够实现世界上从未有过的一种新的金融系统。这是一个技术概念，无法简单地适用于现实生活中的银行和法院。



如果你认可比特币作为交易验证、交易时间序列、所有签名完整性的最终仲裁人的话，那么就可以创建这样一个新的金融系统；这个系统是世界上从未出现过的。

它是如此的新颖和独特，以至于人们很难理解这些概念。这是闪电网络面临的一个实际挑战；这种独特性也存在这样的问题。目前现存的金融法律都无法适用于闪电网络的功能。

我之前已经用非技术语言的文章解释过闪电网络的操作原理了。如果你想了解的话，可以阅读[这篇文章](https://letstalkbitcoin.com/blog/post/the-lightning-network-elidhdicacs)。

**首先我要澄清有关闪电网络比较值得肯定的几点：**

1. 闪电网络的目的是实现安全地进行链下交易。不幸的是闪电网络使用了这个特别的名字。使用这个名字的原因是因为系统需要一个‘网络’来在这第2个层级中进行通信。然而，它并未指定任何特定的网络。任何人都可以实施一个闪电网络；不仅仅是一个特定的公司。以后可能会有很多共存、互相竞争的闪电网络存在。

2. 因为闪电网络需要点对点的第2层级的通信网络，这会导致很多人误解闪电网络的交易到底是什么，或者在特定的时间中谁来持有保管这些资金。

3. 闪电网络的交易就是比特币交易。这一点是至关重要的。闪电网络从未持有保管任何人的资金。所有的资金都存放在比特币网络中的多重签名资金交易中。闪电网络所做的只是让参与方之间的签名交易更加方便，但是只有比特币网络本身才持有或释放这些资金。

4. 闪电网络交易是未确认的比特币交易。它本质上是使用了哈希时间锁定智能合约来安全地进行0确认交易的一种机制。首先，所有未确认的闪电网络交易都是基于现有的已确认的资金交易的。这些资金已经在比特币网络上多重签名地址中得到了的确认，未确认的 闪电网络交易就是基于这些已确认的交易的；其次，使用了一些非常聪明的‘智能合约’功能，用户能够感觉到这些未确认的交易和黄金一样安全（或者和比特币一样安全）。

6. 关于未确认的交易是如何安全地被接受的技术细节是极其复杂的，但是却非常可靠。当然了，没有人能够立刻就信任这样一个系统。毫无疑问，社区需要时间来创建一个新的可信赖的金融层级。人们将需要很长的时间才愿意在闪电网络上委托大额的交易。

正是因为这些原因，我强烈地感觉到闪电网络是用于链下去中心化交易的‘杀手级应用’。如果我们能够免费、实时地执行数十亿的小额交易（如果我们愿意的话，交易价值可以是一美分的百万分之一），那么闪电网络则解决了很多问题。这真是一个非常惊人和振奋的发明。

不幸的是，小额交易是闪电网络仅有的比较清晰的应用案例，而其它使用闪电网络涉及到小额金额的交易都存在很多很难解决的实际问题。

因此，我觉得闪电网络小额交易使用案例就像是扣篮，理解它存在的问题也很重要，以及为什么没有人希望闪电网络很快能承载大量的支付交易。需要知道，在比特币网络中真正的小额交易是不可能的，因为最小费用已经大于小额交易的平均交易额了。这意味着我们已知的闪电网络的唯一使用案例实际上无法在比特币网络中承载任何交易，因为比特币网络无法处理小额交易使用案例。

**因此，闪电网络面临的问题是什么？**

**闪电网络尚不存在。这是明摆着的事实。**但是这个理念是非常了不起的，用一页幻灯片就能总结完，但是实际上创建这样一个可用的网络则需要大量的工作。目前闪电网络还不存在，在相当长的时间中都不会存在可用的闪电网络。创建一个完全去中心化的点对点的层级2网络面临很多技术挑战，实现它是极其困难的，尽管不是不可能实现。

**闪电网络扩展了交易而不是用户。**经常会看到这样的说法，即闪电网络将会解决比特币的扩展问题，事实则是它绝对无法扩展用户。目前比特币的区块容量是有上限的，只能支持十万人的半规则使用。最多，只能支持几百万人一个月使用两次。当你意识到这些问题后，你就会知道比特币社区其实是很小的。的确，很多人会说他们是比特币用户，但是从未在链上（Coinbase,Circle,客户）进行过操作，这些人从未获得比特币网络的好处。Coinbase和Circle的用户受制于反洗钱法/知晓你的客户的约束和很高程度的政府监管。如果我们真的想要比特币网络能够让人们安全地在链上持有资产，区块容量就必须要大幅增加。尽管闪电网络能够处理数十亿的交易，但目前它也只能满足十万人在比特币网络上持有资产。闪电网络需要链上交易来开启和关闭一个通道，比特币区块容量决定了人们能够打开的通道数目的最大值。在闪电网络的幻灯片中，他们建议平均每个人在每6个月中需要打开的通道数不超过1个。**这篇文章会继续讨论为什么这是一个不合理的建议。**

**如果闪电网络存在，人们不会立即就信任它。**信任是赚取来的，而非授予的。而且，实事求是地讲，承诺创建第一个闪电网络的Blockstream公司其实在与社区结合方面做得并不好。从这一点看，其它公司实施闪电网络的机会可能会更好。已经留下了不好的影响，很难擦除。有多少人愿意使用Blockstream创建的闪电网络？可能不会很多。人们愿意在闪电网络上委托多少资金价值？不会很多。事实上，我预测需要很多年人们才能形成对闪电网络的信任而愿意将大量的价值委托给网络；到目前为止对其它密码学货币也是这样，包括比特币。你可以告诉人们，闪电网络的交易就是比特币交易，但是人们在没有看到网络安全运行很长时间之前他们是不愿意将大额的价值委托给系统的。

**如果存在闪电网络，短时间内不会有钱包或支付供应商支持它。需要**很多年你才能真正在线花费你的比特币。我记得以前当我们听到有商家接受比特币支付时，我们都会很兴奋。很多比特币爱好者甚至帮助其他人进行他们的业务，因为他们是接受比特比支付的其中一员。需要很多年来开发软件基础设施来将一种全新的支付系统整合进去；毫无疑问，闪电网络就是一种全新的支付系统。即使发布了，比特币钱包也需要很长时间才能无缝发送和接收闪电网络的支付，而且单独的支付处理商（Bitpay,Circle,Coinbase,交易所，以及其它商业网站）也需要很长时间来支持闪电网络。因此，即使Blockstream有人宣称在接下来的6个月中他们会有可运行的闪电网络版本，这也不能说明什么。因为网络要获得人们的信任需要很多年的时间，从而才能将其整合到生态系统中去。

**闪电网络处理大额价值的交易时存在问题。**闪电网络的运行需要用户和企业锁定在交易期间他们所需数目的比特币。对于小额交易的使用案例，这不是大额交易。锁定5美金或10美金的价值很明显不是问题。然而，如果按照闪电网络幻灯片上所建议的‘合理使用案例’中每个人在每6个月中只开启1个通道的话，显然是行不通的。每个人在每6个月中只开启1个闪电网络通道意味着该通道需要锁定这个用户在该时间段内所持有的最大数目的价值额度。首先，这需要充分信任网络，我已经在之前说过了这需要很长时间才能实现。其次，人们无法预测每两个星期的薪资单，更别说6个月的资金使用额度了。本质上你可以将闪电网络看做是预支付的信用卡。你需要提前充值，你需要猜测你将花费多少额度，以及何时花费。人们在6个月中只开启1个通道是不切实际的。

**闪电网络的支付通道会导致一定程度的中心化。**无论工程师们如何努力来创建一个完全去中心化的闪电网络，但是支付通道的经济属性通常都会向着中心化的方向。支付通道需要锁定交易资金来处理交易。尽管在技术上每个Tom,Dick和Harry都可以合伙将他们自己的比特币锁定到支付通道中，以获得交易费，现实情况就是个体用户无法为闪电网络提供大规模操作时的流动性。在大规模情况下唯一起作用的支付通道将来自于主要的企业和金融服务提供者。世界上将会存在为你服务的‘Circle’,’Bitpay’和’Coinbase’。毫无疑问，所有这些企业都将受制于政府的密切监管。你可以一直重复说，“因为从技术上闪电网络上不需要人来监管其他人的资金”（技术上确实是这样子），现实情况则是金融监管者不会理睬这些言论。底线原则就是，如果企业要使用闪电网络来处理大额的交易，它们将受到金融监管。这个问题是无解的。如果闪电网络的支持者声称，’因为实际上没有人监管其他人的资金‘，它是一个’完全点对点的去中心化网络‘，监管者无需监管它，那么表明这些支持者太过理想化了。同样的，还是这些同样的人一直在声称说保持比特币网络的完全去中心化而避免政府的威胁是多么的重要，但是却没有意识到在闪电网络上的商业活动也无法逃脱监管。金融监管者可能会将过时的法律不正确地应用于闪电网络，或者他们干脆重写新的法规。底线原则就是如果主要的企业在闪电网络上处理数十亿美金价值的交易，它们将受制于政府的反洗钱法/知晓你的客户法规。为什么或者如何Blockstream认为它们能够幸免于此，这对我来说还是个谜题。

**不平衡的通道和锁定的大量比特币会使得闪电网络面临经济挑战。**闪电网络是使用双向支付通道建立的。每一个通道都是基于比特币区块链上已存在和已确认的资金交易的。一旦一个用户开启一个通道，他们就可以进行不超过预先锁定在资金通道中价值额度的交易了。因此，如果有人开启了一个100美金的支付通道，那么他能发送的最大额度就是100美金。如果想要发送101美金，这是不可以的。通道已经满了，他们可以关闭该通道，并创建一个新通道，或者进行链上交易；当然了，他们无法很容易地进行链上交易，因为他们的比特币已经锁定在闪电网络通道中了。如果用户开启了一个100美金的支付通道，他们最多可以发送100美金的价值，但是他们无法收到一美分！如果用户想要收到支付的话，则第二个参与方也必须要进行资金委托。因此，如果用户想要同时能发送和接收100美金的价值，另外一方也必须愿意委托100美金的价值。现在，一旦最初的用户发送了100美金，理论上他可以从其它参与方收到最多200美金的价值。‘通道‘允许他们互相转移当前的余额；但是需要在自己的初始交易限制内。然而，当整个网络运行起来时，这会变得很糟糕。这个内连的支付通道网络会立即变得不均衡。现在，如果你想要从某人发送资金至其他人，你必须要在大量不均衡的通道中找到一条可运行的通道。除非这些通道都受托了大量的资金，否则将很难找到这样的通道。这导致的问题就是如果要处理闪电网络上大量的交易，人们就需要委托大量的比特币，这样的话这些通道才能保持畅通并且拥有足够的流动性。我们不得不问，为了供流动性而将大量的比特币锁定在支付通道中是好事吗？从大规模来看，似乎在经济上是行不通的。

**通道中锁定资金意味着它们受制于市场的波动。**我们都希望比特币能成为主流货币，由于它的通缩属性，我们都希望能增值。如果真是这样的话，那么将比特币长时间锁定在支付通道中是没有问题的。为什么不呢？你既可以收取交易费又可以看到你的比特币增值。不幸的是，情况不是这样子。事实就是，尽管现在的比特币已经不像以前那样容易波动，但它仍然具有很大的波动性。想象一下，如果数十亿美金价值的比特币锁定在支付通道中，突然比特币出现了巨大的市场波动。你能想象到大量的闪电网络支付通道关闭吗？市场的力量将会阻碍大量的委托资金开启支付通道，因为这会使他们遭受很大的波动风险。当市场波动剧烈时，将会给支付通道带来不稳定性，因为他们会大量关闭通道，从而给比特币网络形成了很多积压的交易，导致交易无法确认。

**闪电网络的用户要有‘热钱包’。**目前，对比特币用户来讲，最佳和最安全的操作就是将每天的花费金额存放在’热钱包‘中（该钱包可以连接到互联网，托管在电脑或智能手机上），其它的资金可以使用’冷存储‘或其它离线方法存储。用户可以通过使用像’Trezor’硬件钱包来讲资金安全地转到他们的热钱包中。然而，因为整个闪电网络操作的是锁定在支付通道中的资金，因此这些资金必须要足够多以维持通道开启时间段内的经济活动，而且如果你想要成为网络中的参与者，那么软件就必须要作为热钱包来签名网络中的交易，这显然是很多比特币用户要避免的风险。闪电网络通过在参与者之间分流大量已签名的交易来运行。为了能正常运行，所有这些参与者都需要运行软件，并一直连接到网络以便能签名交易。如果一个用户的设备受到了病毒感染或攻击，理论上攻击者是可以盗取资金的。很明显，这是个体用户需要管理的风险，对于小额交易的使用案例，热钱包只含有少量的资金，这是可以接受的风险。但是，你能想象将6个月中的所有交易都保存在热钱包中吗？这对黑客来说是很有吸引力的。

总之，闪电网络是一个很好的概念，为小额交易使用案例提供了广阔的前景，但在能够承担大量日常的比特币网络交易之前，它也面临很多挑战。更重要的是，闪电网络并不会扩展用户，因此即使它能增加交易能力，它也只能满足目前的这十多万极客用户的日常使用。

唯一可能扩展更多用户的层级2系统是替代币或侧链。这意味着你可以将资金价值转移到一个完全不同的网络中。