Peter Todd：比特币闪电网络也许会失败

**[kyle](http://www.8btc.com/author/14244" \o "由 kyle 发布) 2016-07-06 15:19 发布在**[**比特币**](http://www.8btc.com/bitcoin)[**6**](http://www.8btc.com/lighting-network-may-fail#comment)**1116**

[闪电网络](http://www.8btc.com/lightning-network)被很多比特币社区的人认为是最有希望的比特币网络长期扩容方案。这种概念使用支付渠道在链下执行比特币交易，而区块链则是作为一种备用的处理系统，当有人行为不轨时才会发挥作用。闪电网络的创建者估计这种网络最终将能够每秒处理数十亿笔交易。



尽管智能合约和博弈论的结合被用来确保系统能够正确运行，但是在上月末的Bitcoin in Use会议上，Bitcoin Core贡献者Peter Todd解释了一种闪电网络可能会出现的失败模式。

在本篇文章中讨论的这种可能的失败模式早在闪电网络的早期开发过程中就已经被发现了，并且在闪电网络白皮书中还进行了讨论。本文并非是尝试赞扬Todd发现了这种失败模式。他在最近的谈话中也只是给了简单的概述。

闪电网络的失败模式

Todd所描述的闪电网络可能会失败的情形发生于：当大量的比特币网络上的人需要在短时间内解决他们的闪电网络争端时。

“闪电网络确实会出现失败的情况：想象一下，同时出现了一大堆需要结算的交易，而比特币网络能够处理的数据有限，如果我们迅速关闭了大量闪电网络渠道，我们将如何确认这些交易呢？在这一点上，已经超出了能力范围。”

还有一种情景，当大量的人需要在区块链解决闪电合约的时候，收取的费用可能会大幅攀升，因为比特币区块可用的空间已经所剩无几。Todd说：

“在某一时刻，人们就会开始遭受损失，因为交易成本超出他们能够承受的范围。如果你大量使用了闪电网络，那么这个成本是相当高的。这就可能造成闪电网络的失败。”

根据闪电网络的运行机制，用户必须能够发行一种违约救济交易，以此让其同行诚实。如果用户无法在特定的时间内在区块链上进行正确的交易，他的竞争对手便可以控制与双方之间智能合约绑定的比特币。

可能的解决方案

任何可能会造成比特币被盗的情况都需要避免，根据Todd所说，针对这个问题，有一些理论上的解决方案。其中一个就是，一种适应性区块大小限制可以在这些失败的情形下，允许矿工提升区块容量。另一种方案就是允许闪电网络矿工预先储备未来区块的空间，来确保矿工能够在时间同步到期之前在区块链上对交易进行广播。



话虽如此，Todd表示目前还没有一种真正的经过审查的解决方案。

“这是一个非常复杂的过程，我们还没有达到可以自信地说：‘是的，我们将让全世界的人都用闪电网络系统购买咖啡’。现在还有很多工作需要做，我认为要弄清所有的工作是一个非常缓慢的过程。”

是什么可能导致这种情景？

Todd担心出现这种灾难情景的原因之一就是用户可能会自鸣得意，因为他们忽视了网络上其他人正在做的事。

Todd解释说：

“作为一个闪电用户，我很难知道会有多少人遭受大量闪电渠道同时失败。这一点我并不清楚；我不一定能够对这种情况做出反应。”

有一种因素可能会促使闪电网络失败模式出现，BitGo工程师Jameson Lopp同样清楚地表达了这一点，那就是网络拓扑结构过于中心化。如果许多比特币网络大玩家同时遭遇失败，所有的连接节点的同行都必须及时在区块链上解决他们的智能合约。