闪电网络是如何工作的 （1）？

来源：字节元 CKB

作为构建在比特币区块链之上的 P2P 网络，闪电网络不仅能够有效解决比特币 “又慢又贵” 的难题，而且在加密支付领域有着其他解决方案无可比拟的优势，是我们实现 P2P 经济的基础，也是我们憧憬的 Web5 世界的重要组成部分。

今天这篇文章，我们将继续介绍闪电网络，讲清楚闪电网络的运行原理和相关技术。

## 闪电网络的基石：支付通道

闪电网络本质上是一个精心设计的支付通道系统。以 Alice 和 Bob 之间的交易为例，他们使用闪电网络进行结算时，会经历以下三个关键阶段：开启通道、进行交易、关闭通道。

1、开启通道：构建信任的桥梁

所谓开启通道，实质上是创建一个由参与双方共同控制的多签钱包，并向该钱包注入资金。这个钱包接收的资金总额即为这个通道的余额。

我们假设 Alice 和 Bob 各自持有 10 万聪 BTC。首先，他们需要将各自的 10 万聪转入一个由两人共同控制的多签钱包地址，作为建立通道的质押金。这笔交易，被称为 “Funding Transaction（充值交易）” 或者 “Anchor Transaction（锚点交易）”，需要广播到网络并记录在比特币区块链上，以表明通道的正式开启。在这个例子中，连接 Alice 和 Bob 的支付通道实质就是一个普通的 2-of-2 多签名钱包，里面包含 20 万聪的余额（为简化说明，我们暂不考虑开启通道时需要支付的矿工费）。

2、开始交易：链下交易的艺术

通道开启后，参与双方的后续交易将全部在比特币区块链之外进行，实现了高效的链下结算。让我们假设 Alice 和 Bob 之间进行了以下 3 次交易：

Alice 向 Bob 转账 1 万聪，此时 Alice 拥有 9 万聪，Bob 拥有 11 万聪。

Alice 继续向 Bob 转账 2 万聪，此时 Alice 拥有 7 万聪，Bob 拥有 13 万聪。

Bob 向 Alice 转账 1 万聪，此时 Alice 拥有 8 万聪，Bob 拥有 12 万聪。

从上面的例子中，我们可以看到，无论 Alice 和 Bob 之间进行多少次转账，他们之间的通道余额始终保持不变，都是 20 万聪。

每次 Alice 和 Bob 发生交易时，双方需要更新通道中各自的余额，并交换经过签名的 “承诺交易（Commitment Transaction）”。这些交易本身都是有效的，可以随时发送到比特币网络中，但双方通常会将其保存而不广播，除非他们打算关闭通道。如此一来，通道内 Alice 和 Bob 的余额状态，一秒内变动几十次、几百次都没问题，更新的速度仅受限于双方创建、签名和向对方发送承诺交易的速度。

3、关闭通道：最终结算的时刻

关闭通道可以通过两种方式进行：一是双方一致同意关闭，将一笔结算交易（Settlement Transaction）发送到比特币网络中；二是单方决定关闭，将最后一笔承诺交易（Commitment Transaction）发送到比特币网络中。后者的设计是为了防止某一方离线导致另一方在通道中的余额一直被锁定的情形。

在 Alice 和 Bob 的例子中，他们在进行了3 笔交易后决定关闭通道。关闭后，Alice 取回 8 万聪，Bob 取回 12 万聪（同样，为简化说明，我们不考虑关闭通道时产生的矿工费）。

## 双向支付通道的安全保障：从 LN-Penalty 到 eltoo 再到 Daric

上文提到，关闭通道既可以双方一致同意关闭，也可以是单方决定关闭。那么，在双向支付通道中，如何防止某一方欺诈呢？比如上面的例子中，如何防止 Bob 拿着第 2 次而不是第 3 次承诺交易来关闭通道呢？如果使用第 2 次的承诺交易关闭通道，Bob 可以抵赖掉最后付给 Alice 的 1 万聪付款，这显然看上去很有诱惑力。

比特币闪电网络引入了 LN-Penalty 机制来防止某一方把一个过时的但对自己有利的状态发送的链上来关闭通道。LN-Penalty 使用 “不对称的承诺交易” 和 “撤销密钥” 等复杂技术，确保如果 Bob 试图使用过时的承诺交易关闭通道，Alice 将有权获得通道内的全部资金 —— 20 万聪。这种惩罚机制有效遏制了潜在的欺诈行为。

然而，LN-Penalty 也存在一些不足，除了自身的复杂性之外，还造成了存储负担 —— 用户必须保存过去每一次更新通道状态时候的资料，还有一些罕见的情形可能会导致它意外地惩罚诚实的用户。

为了克服这些缺点，早在 2018 年，比特币社区就提出了名为 “eltoo” 的解决方案，来消除存储负担和意外惩罚的风险。在这个方案中，用户只需保存最新一笔承诺交易及其结算交易即可。然而，eltoo 方案至今还不可用，因为它的实施需要对比特币进行软分叉，引入一个新的签名哈希类型 —— SIGHASH\_ANYPREVOUT。

Nervos CKB 推出的闪电网络 Fiber Network则选择了 2022 年提出的Daric方案。Daric 在 eltoo 的基础之上，有效解决了瞭望塔（Watchtower）的成本和安全性问题。瞭望塔是运行在独立机器和网络上的闪电网络节点，会监控支付通道，并在检测到恶意行为时帮助受害方执行罚没交易，从而保护用户的资金。节点操作者通常会运行自己的瞭望塔，以保护自己的节点。

## 结语

闪电网络作为比特币扩容解决方案，其核心在于巧妙设计的支付通道系统。通过开启通道、链下交易和关闭通道三个阶段，闪电网络大幅提升了交易速度并降低了成本。

为确保双向支付通道的安全，闪电网络采用了 LN-Penalty 机制，比特币社区还提出了 eltoo、Daric 等更优的安全机制，来有效防范潜在的欺诈行为。

这些创新使得闪电网络在保证安全性的同时，为比特币网络带来了显著的性能提升，为实现快速、低成本的小额支付铺平了道路。