闪电网络是如何工作的 （2）？

来源：字节元 CKB

在上一篇《闪电网络是如何工作的 （1）》中，我们探讨了闪电网络（Lightning Network）的运行原理和双向支付通道的安全保障相关技术。今天这篇文章，我们将继续介绍闪电网络，讲清楚将双向支付通道扩展成闪电网络的相关原理和技术。

## 将双向支付通道扩展成闪电网络：多跳路由技术

我们同样使用 Alice 和 Bob 建立通道作为基本背景，但这个世界上除了 Alice 和 Bob，其他人也想接入闪电网络该怎么办？有什么办法可以把所有人都接入网络并保证可以向网络中的任一一个人发起支付？

为了解决这一问题，我们需要将双向支付通道扩展成闪电网络，并使用多跳路由技术。“路由（routing）” 的字面意思是 “寻找路径”，在闪电网络中，就是要找出由通道前后连接而成的、给特定对象支付的路径。

以 Alice 向 David 支付 2000 聪为例，假设他们之间没有建立支付通道，不过 Alice 和 Bob 之间、Bob 和 Carol 之间、 Carol 和 David 之间都已经建立了支付通道。在这种情况下，Alice 可以先把钱转给 Bob ，再由 Bob 转给 Carol，最后 Carol 转给 David，这样看起来就实现了从 Alice 到 David 间的支付通道，其中 Bob 和 Carol 充当了网络中的路由节点。如果 Alice 和 Eva 之间、Eva 和 David 之间也建立了支付通道，那么 Alice 也可以选择先把钱转给 Eva，再由 Eva 转给 David。



从路径上来看，显然 Alice 通过 Eva 转钱给 David 是路径最短的选择，但在实际操作过程中，看上去最短的路径并不总是最佳选择，因为还需要考虑其他因素，比如通道的容量、路由节点的收费标准、路由节点是否在线，等等。

目前，主流的比特币闪电网络实现（客户端），如 Lightning Labs 开发的 LND 和 Blockstream 开发的 CLN（Core Lightning），在路由算法上都使用了 Dijkstra 算法的某个变种，Nervos CKB 推出的闪电网络 Fiber Network 同样会使用 Dijkstra 算法来寻找最优路由路径。

## 保障路由安全：从 HTLC 到 PTLC

在上面 Alice 要给 David 付款的例子中，我们如何保证中间的路由节点不会耍赖，不会恶意扣留资金呢？传统金融系统通常依赖大型知名金融中介机构的信用担保，但闪电网络是一个 P2P 网络，并没有这样一个独立于交易者的第三方去提供信用担保，我们需要一种不同的机制来保障交易安全。这就是 HTLC（哈希时间锁合约）的作用所在。

HTLC 由两部分组成：哈希验证和过期验证。让我们以 Alice 要给 David 支付 2000 聪，选择 Bob 和 Carol 充当网络中的路由节点为例，理解 HTLC 的工作原理：



首先，David 要生成一个秘密值 R，任何词语、任何数字都可以充当这个秘密值，然后计算出其哈希值 H 并把它发给 Alice。这个哈希值 H 会放在交易输出的锁定脚本中，只有知道 H 所对应的秘密值 R 的人才能使用这个输出，而 R 在闪电网络中被称为 “原像（preimage）”。如果秘密值 R 没有及时地公开，这笔支付就用不了了，发送者会收回所有的资金。

然后，Alice 使用收到的哈希值 H 创建一个 HTLC，时间锁设置成未来 5 个区块，输出的数额是 2020 聪，其中 20 聪是给路由节点 Bob 的手续费。用大白话来表述就是，Alice 会给 Bob 支付 2020 聪，只要他能在 5 个区块内提供秘密值 R，否则这些钱会返回给 Alice。

Bob 在自己和 Carol 的通道中，使用跟 Alice 所提供的同样的哈希值 H 创建一个 HTLC，时间锁设置成未来 4 个区块，输出的数额是 2010 聪，其中 10 聪是给路由节点 Carol 的手续费。用大白话来表述就是，Bob 会给 Carol 支付 2010 聪，只要他能在 4 个区块内提供秘密值 R，否则这些钱会返回给 Bob。

Carol 在自己和 David 的通道中，使用同样的哈希值 H 创建一个 HTLC，时间锁设置成未来 3 个区块，输出的数额是 2000 聪。用大白话来表述就是，Carol 会给 David 支付 2000 聪，只要他能在 3 个区块内提供秘密值 R，否则这些钱会返回给 Carol。

David 用秘密值 R 解锁 Carol 设置的 HTLC，拿走 2000 聪。

David 拿走资金之后，Carol 也会知道这个秘密值 R，他用 R 解锁 Bob 设置的 HTLC 并拿走 2010 聪。

Carol 拿走资金之后，Bob 也得到了秘密值 R，他用 R 解锁 Alice 设置的 HTLC 并拿走 2020 聪。

通过这种机制，Alice 成功向 David 支付了 2000 聪，而无需直接建立支付通道。整个过程中，各方无需相互信任，路由节点也获得了应得的手续费。即使支付在某个环节中断，由于时间锁定机制的存在，各方都不会遭受损失，资金会在锁定时间过后自动返回。

然而，HTLC 也存在一个潜在的隐私问题：整条路径使用的都是同一个秘密值（原像）。如果某个实体控制了支付路径上的多个节点，就可能通过比对不同节点的输入和输出，推断出完整的交易信息，甚至猜测出付款方和收款方，这就削弱了闪电网络通过洋葱路由实现的隐私保护。

为了解决这个问题，比特币社区提出了 PTLC（点时间锁合约）。在 PTLC 方案中，路径中的每一跳都使用不同的秘密值，这样一来，通过洋葱路由实现的隐私性就得到了保护。Nervos CKB 推出的闪电网络 Fiber Network 计划在未来引入 PTLC，进一步增强闪电网络的隐私保护能力。

## 结语

随着技术的不断进步，闪电网络还在持续优化和改进。从 LN-Penalty 到 eltoo 再到 Daric，从 HTLC 到 PTLC，我们看到了闪电网络在安全性、隐私保护等方面的不断提升。未来，随着更多创新技术的应用和生态系统的完善，闪电网络有望成为推动加密货币普及的关键基础设施，为实现真正的 P2P 经济贡献力量。

参考资料

https://www.btcstudy.org/2021/09/15/lightning-network-in-depth-part-1-payment-channels/

https://www.btcstudy.org/2021/09/15/lightning-network-in-depth-part-2-htlc-and-payment-routing/

https://www.btcstudy.org/2022/01/27/breaking-down-the-bitcoin-lightning-network-eltoo/

https://www.btcstudy.org/2024/02/07/lightning-network-technology-improvement-and-users-experience-part-2/

https://www.btcstudy.org/2024/02/23/lightning-network-technology-improvement-and-users-experience-part-3/

https://www.btcstudy.org/2022/08/19/what-are-ptlc/