

## 超越白皮书 8：穿云而过的闪电网络

### 摘要：

近年，随着比特币一步步迈入更多人的视野，其扩展性问题一直如影随形甚至日趋严重，已经成为笼罩在比特币头顶的一大朵乌云。为此学术界和产业界提出了各种解决方案，如区块扩容、分片、侧链等。这其中，支付通道方案中的代表闪电网络恰如其名，似一道穿云而过的闪电，成为解决扩展性问题最耀眼的方案之一，其后雷声阵阵，引众人回首。

自 2015 年闪电网络白皮书发布后，Lightning Labs、ACINQ、Blockstream 作为三个主流的闪电网络技术团队使用不同的程序语言实现了闪电网络的技术框架。许多社区开发者也加入到闪电网络的生态中开发了钱包、游戏、购物、即时通讯等贴近生活场景的应用。迄今，闪电网络上已有 1.3 万多个节点，3.7 万多条支付通道，通道中容纳 1000 个上下的比特币。

技术角度而言，闪电网络是比特币二层链下的扩展性技术，由微支付通道演化而来，其核心技术包括 RSMC(Revocable Sequence Maturity Contract, 序列到期可撤销合约)和 HTLC(Hashed Time Lock Contract, 哈希时间锁定合约)。微支付通道提供链下的点对点单向支付的能力，相比链上的交易，性能有质的提升，但其缺陷在于通道有时限且资金只能单向流动；在微支付通道的基础上，RSMC 技术解决了资金单向流动的问题，且使支付通道不再有时间限制，为用户的两两交易提供了即时高性能的解决方案；HTLC 将 RSMC 进一步扩展，解决了多方参与资金路由时产生的信任问题。这些技术互相融合，形成了闪电网络。

不可否认，闪电网络的诞生为比特币的扩展性提升引入了能产生质的飞跃的技术解决方案，同时其交易费低廉、支持跨链交易的特性带来了新的应用场景，也为比特币生态注入新的活力。但与闪电网络的优点一样显眼的是闪电网络的缺点，集中化、稳定性、隐私、易用性等都是其亟待解决的问题。

新技术带来新问题，新问题又会被新技术解决，如此循环推演。闪电网络上亦是如此，针对闪电网络各个方面的问题，陆续有研究和研发团队提出新的解决方案。保障用户离线状态下资金安全的瞭望塔、实现链上链下资金便捷互通的潜交换、逾越通道支付上限的原子多路径支付等等各项扩展技术和服务陆续登场。

展望未来，闪电网络有望成为比特币生态中的技术基础之一，将吸引更多生态中甚至生态外的元素加入其中摩擦火花，更进一步地，其有可能成为个人金融业务、零售行业的重要支付工具得以应用。这个过程中，技术人员和生态运营人员也需要为闪电网络的稳定性、安全性、隐私性、易用性、开放性做出更多的努力。

## 作者

---

【火币研究院】袁煜明，赵文琦

## 作者联系方式

火币研究院：[huobiresearch@huobi.com](mailto:huobiresearch@huobi.com)

---

## 目 录

一、	闪电网络的诞生 .....	5
二、	闪电网络的技术原理 .....	7
2.1	单向支付的微支付通道 .....	7
2.1.1	高性能，低手续费 .....	7
2.1.2	安全性强 .....	8
2.1.3	通道资金单向流动 .....	9
2.1.4	通道时限 .....	9
2.2	更进一步的 RSMC .....	9
2.2.1	支付通道的建立与交易 .....	10
2.2.2	支付通道的正常关闭 .....	12
2.2.3	RSMC 中的抵赖与违约补偿 .....	13
2.3	编织网络的 HTLC .....	14
2.3.1	多方参与问题 .....	14
2.3.2	HTLC 的处理流程 .....	15
2.3.3	路由与手续费 .....	17
2.4	闪电网络 .....	17
三、	闪电网络的生态 .....	18
3.1	开发团队 .....	18
3.2	应用情况 .....	19
3.3	活跃情况 .....	22
四、	闪电网络的贡献与局限 .....	25
4.1	贡献 .....	25
4.1.1	提升比特币网络扩展性 .....	25
4.1.2	降低交易的时间和资金成本 .....	25
4.1.3	支持跨链交易 .....	25
4.1.4	促进比特币生态发展 .....	26
4.2	局限 .....	26
4.2.1	受限的支付上限 .....	26

4.2.2 节点和资金集中化明显 .....	27
4.2.3 网络稳定性问题亟待解决 .....	28
4.2.4 难以保障的数据隐私 .....	29
4.2.5 受约束的网络可扩展性 .....	30
4.2.6 较高的使用门槛 .....	30
<b>五、 闪电网络的扩展技术与服务 .....</b>	<b>31</b>
5.1 “欺诈斗士”瞭望塔 .....	31
5.2 “上下互通”潜交换 .....	33
5.3 “化整为零”AMP .....	35
5.4 还有更多 .....	37
<b>六、 总结与展望 .....</b>	<b>38</b>
6.1 未来发展 .....	38
6.2 改进方向 .....	38
<b>参考文献 .....</b>	<b>41</b>

## 一、闪电网络的诞生

2008 年比特币白皮书发布，将加密数字资产和区块链概念与技术带入大众视野。但比特币自发布以来一直伴随着若干技术问题。1.交易延时问题：每笔交易的确认需要等待至少 6 个区块，也就是至少 1 个小时，与之形成对比的是当今各类电子支付毫秒级的交易确认速度；2.吞吐量问题：受区块容量和共识算法 PoW 耗时的约束，比特币全网每秒只能处理 7 笔交易，而 2019 年天猫双十一的每秒订单峰值已达 54.4 万笔；3.存储量问题：迄今比特币区块链上已有逾 60 万个区块，约 270GB，且在可预见的将来只增不减，远高于现今各类手机和 PC 端软件的存储量。在其余区块链上，这些问题同样存在，这些技术瓶颈严重制约了加密数字资产与区块链大规模商用落地引发产业变革的能力。

由此，学术界和产业界提出和实现了各种链上和链下的改进方案。1.链上解决方案如区块扩容(比特币现金为例)、更换 PoW 中的算法减少挖矿耗时(莱特币为例)、分片(Sharding)、提出更轻量级的共识算法(PoS 为例)等；2.链下解决方案如隔离见证(SegWit)、楔入式侧链、平行链、Plasma、支付通道等。如表 1 为提升扩展性的各类技术方案的对比。

闪电网络作为支付通道中的代表，被视作解决比特币扩展性问题最闪耀的技术解决方案，自 2015 年被提出之后近几年一直备受关注。曾经使用 10,000 个比特币购买了两个披萨的 Laszlo Hanyecz，在 2018 年再次使用闪电网络支付了 649,000 聪购买了两个披萨。2019 年 1 月发起的一场名为“闪电火炬”的活动更是声势浩大，“火炬”传递途径覆盖全球几十个国家，众多科技界的大拿都作为火炬手参与传递。短短 5 年时间，已经有多个团队实现了各个语言版本的闪电网络，其上也涌现出了各类 LApp。迄今，闪电网络已经拥有了 1.3 万多个节点，3.7 万多条支付通道，通道中容纳 1000 个上下的比特币。

究竟闪电网络为什么可以为比特币的扩展性带来质的飞跃？又为什么没能一举解决比特币网络的扩展性问题？本文将从闪电网络的技术原理、贡献与局限、扩展技术及生态情况等多方面对闪电网络做深入探讨。



表1 提升扩展性的技术方案对比

	解决方案	优点	局限
链上(一层)解决方案	<ul style="list-style-type: none"> <li>• 区块扩容(比特币为例)</li> <li>• 挖矿提速(莱特币为例)</li> </ul>	<ul style="list-style-type: none"> <li>• 直接提升扩展性</li> </ul>	<ul style="list-style-type: none"> <li>• 扩展性提升十分有限</li> <li>• 降低激励</li> <li>• 带来集中化的风险(数据量增加带来维护成本提高, 减少了有资质的矿工)</li> <li>• 带来硬分叉</li> </ul>
	<ul style="list-style-type: none"> <li>• 分片(Sharding)</li> </ul>	<ul style="list-style-type: none"> <li>• 提升扩展性</li> </ul>	<ul style="list-style-type: none"> <li>• 跨片通信代价高</li> <li>• 协议复杂</li> <li>• 每个分片的安全性降低</li> <li>• 带来硬分叉</li> </ul>
	<ul style="list-style-type: none"> <li>• PoS 及其他轻量级共识算法</li> </ul>	<ul style="list-style-type: none"> <li>• 降低能耗</li> <li>• 提升扩展性</li> <li>• 交易速度更快</li> <li>• 避免 51%攻击问题</li> </ul>	<ul style="list-style-type: none"> <li>• 集中化问题</li> <li>• 造成穷者越穷</li> <li>• 带来硬分叉</li> </ul>
链下(二层)解决方案	<ul style="list-style-type: none"> <li>• 隔离见证(SegWit)</li> </ul>	<ul style="list-style-type: none"> <li>• 提升扩展性</li> </ul>	<ul style="list-style-type: none"> <li>• 带来侧链安全性问题</li> <li>• 协议复杂</li> <li>• 软分叉, 但催生了硬分叉</li> </ul>
	<ul style="list-style-type: none"> <li>• 楔入式侧链</li> <li>• 平行链</li> <li>• Plasma</li> </ul>	<ul style="list-style-type: none"> <li>• 明显提升扩展性</li> </ul>	<ul style="list-style-type: none"> <li>• 降低了每条链的安全性</li> <li>• 需要跨链通信</li> </ul>
	<ul style="list-style-type: none"> <li>• 支付通道</li> </ul>	<ul style="list-style-type: none"> <li>• 极大提升扩展性</li> <li>• 小额交易近乎实时</li> <li>• 支持跨链交易</li> </ul>	<ul style="list-style-type: none"> <li>• 大额付款方案尚不成熟</li> <li>• 需要交易双方均在线</li> <li>• 隐私问题</li> <li>• 集中化问题</li> </ul>

## 二、闪电网络的技术原理

“If a tree falls in the forest and no one is around to hear it, does it make a sound?”

这句引言来自于 18 世纪哲学家 George Berkeley，也是 Joseph Poon 和 Thaddeus Dryja 在 2015 年提出的“闪电网络(Lightning Network)”的理念根源。就像无人听闻的陨落无足轻重一样，日常重复的交易也不必人尽皆知。

对于比特币网络来说，交易双方如果有多次交易，大可不必将每次的交易都同步到网络的每个节点。只需将多次交易后，交易双方最终的资金分配状态上报给比特币网络，既可以保证资金状态的最终正确性，也可以缩减交易双方在低效的比特币网络上的等待时间提升交易频次，还可以降低对比特币网络的计算及存储资源的消耗。可以说同时解决了比特币网络高延时、低吞吐的问题，打破了困扰比特币多年的性能瓶颈，也为降低交易存储量提供了极好的方案。

本小节将探讨“闪电网络”这个看似“完美”的解决方案的技术原理。闪电网络是基于微支付通道演化而来，将其单向支付通道扩展为双向支付通道，并通过 RSMC(Revocable Sequence Maturity Contract, 序列到期可撤销合约)解决双向通道中历史合约作废的问题，通过 HTLC(Hashed Time Lock Contract, 哈希时间锁定合约)解决跨节点交易的问题，最终形成了一张比特币链下的不依赖可信第三方和可信交易对手的支持网络。

### 2.1 单向支付的微支付通道

微支付通道的提出为交易双方建立小额的支付通道提供了解决方案，其具有高性能低手续费、安全性强、通道内资金单向流动及通道有时限等 4 个特点：

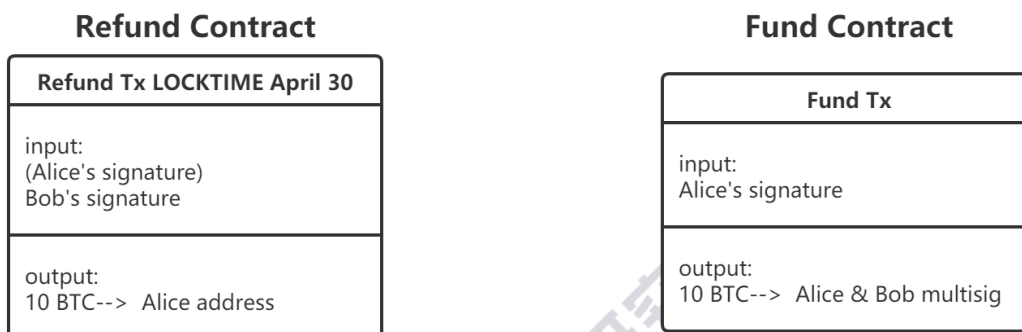
#### 2.1.1 高性能，低手续费

- 1) 仅需发生 2 笔与比特币网络上的通信(即 2 次发生在比特币网络上的交易)。  
交易双方仅需在建立和关闭通道时与比特币网络通信，第一次通信建立微支付通道，第二次通信将在通道内发生的交易的最后结果发布到比特币网络上。
- 2) 通道内的资金交易以点对点通信方式进行。通道内的支付只需交易双方签名认可，免去了复杂的网络传播与验证，交易速度近实时。且点对点的交易手续费几乎可以忽略。

### 2.1.2 安全性强

- 1) 交易双方利用双签名账户构建支付通道。支付通道内的交易需要有交易双方的签名认可否则无法被发布到主链上。
- 2) 付款方在收款方消失的情形下仍能取回余额，保障付款方权益。如下图 1 所示，Alice 在签署存款合约(Fund Contract)将 10 BTC 存入双签名账户之前，会要求 Bob 先签一份退款合约(Refund Contract)，合约中会确定一个拿回余额的时间点。在这个例子中退款合约表示在 4 月 30 之后，Alice 可以将这份合约签名并发布到比特币网络上，成功后双签名账户中的 10 BTC 将退至 Alice 的账户。如此，Bob 无法通过拒绝发布交易合约阻止 Alice 拿回通道中的余额而进行敲诈。

图1 微支付通道的建立



说明：图中对于签名，加括号的部分表示待签名，不加括号的部分表示已签名

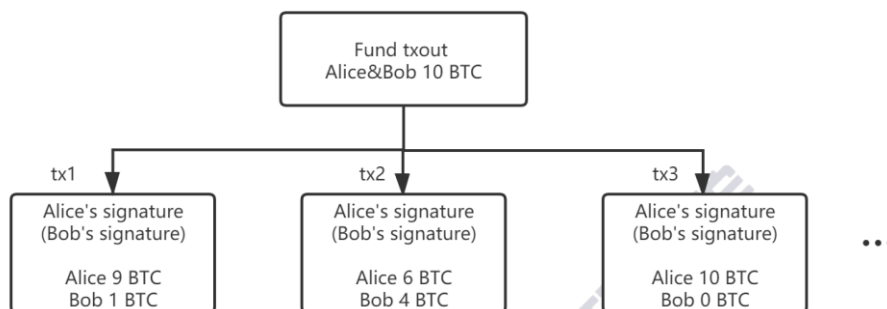
来源：Dryja 在 MIT 的授课内容，火币研究院整理

- 3) 付款方无法对已发生的交易抵赖，保障收款方权益。如图 2 所示，每次发生新的交易，Alice 都会签署一份余额重新分配的合约发给 Bob。图中的 tx1 表示 Alice 向 Bob 付款 1 BTC，tx2 表示 Alice 再向 Bob 付款 3 BTC。但如果此时 Alice 期望通过 tx3 将 10 BTC 全部拿回来，抵赖掉之前的两次付款，是做不到的。因为 tx3 尚未得到 Bob 的签名，无法发布，而 Bob 只需忽略 tx3，将 tx2 签名并发布到比特币网络上就可以拿到应得的 4 BTC。同时可以注意



到，微支付通道对试图抵赖者(此处为 Alice)没有惩罚机制，剩余的 6 BTC 仍将回到 Alice 的账户。

图2 微支付通道的交易



说明：图中对于签名，加括号的部分表示待签名，不加括号的部分表示已签名

来源：Dryja 在 MIT 的授课内容，火币研究院整理

### 2.1.3 通道资金单向流动

微支付通道只适用于 Alice 向 Bob 付款的场景，不适用于 Alice 与 Bob 互相转账的情形。通道在能力上并没有限制资金的双向流动，但从资金 Bob 流向 Alice 的交易是不可信的交易，即便 Bob 签署了一份付款合约发送给 Alice，Bob 仍可以将发生该份合约之前的合约签署发布，从而抵赖掉这次付款。

### 2.1.4 通道时限

微支付通道通过时间锁机制保障了付款方的权益(上文 2.1.2 小节中提到)，但同时会使通道最长只能保留到时间锁的到期时间。一旦到达截止时间，即便通道内的金额并没有完全被支付或者交易双方仍存在支付需求，通道会被关闭。如果不关闭，上例中，通道中的 10 个 BTC 将全部返还给 Alice，Bob 显然不会允许这样的情况发生，其会在截止时刻之前发布通道中最新的合约并关闭通道。

## 2.2 更进一步的 RSMC

为了给交易双方提供双向的及更长期的支付通道，闪电网络在微支付通道的基础上设计了 RSMC(Revocable Sequence Maturity Contract，序列到期可撤销

合约)。随之带来的是更复杂的签约机制和防抵赖机制。

RSMC 中主要涉及了 5 种交易：

- 1) **存款(fund)**: 建立通道之初通过“存款”交易将双方的资金存入双签名钱包，将存款交易广播到比特币网络就意味着双方建立了支付通道。但在广播之前需要先签署一份“提交”交易，保证对手方消失的情况下仍能取回双签名钱包中的资金(上文的微支付通道中通过“退款”交易实现)。
- 2) **提交(commit)**: 支付通道建立后，交易双方在通道内进行资金往来时通过“提交”交易来实现。该交易的特征是一式两份，每一方都会签署好交易信息递交给对手方。参与者如果想终止支付通道可以将对方署过名的合约签字并广播到区块链网络，进行资金分配并关闭支付通道。
- 3) **分配(delivery)**: “分配”交易是具体执行资金派送的交易，该交易执行完成后资金将抵达目标账户。通常指的是不可撤销的分配。
- 4) **可撤销的分配(revocable delivery)**: 同样是资金派送的交易，但该交易的执行可能因为其他交易的执行而被撤回。在 RSMC 中主要会因为“违约补偿”交易的执行而被撤回。
- 5) **违约补偿(breach remedy)**: RSMC 中核心的防抵赖机制，当对手方企图通过发布历史交易而抵赖后续交易时，可以通过发布“违约补偿”交易罚没对手方的所有资金。

本小节将在 Alice 与 Bob 的交易中详细探讨这 5 种交易如何相互配合实现高效可信的支付通道。

### 2.2.1 支付通道的建立与交易

#### 1) 存款交易与信任问题

如图 3 所示，是 Alice 与 Bob 支付通道的建立与通道内的资金往来的流程。最初，Alice 出资 2 BTC，Bob 出资 8 BTC，双方签订“存款”交易，计划将钱存储到二人的双签名钱包中。但由于双签名钱包中的资金只有在双方均签名认可的情况下才能被动用，二人都会担心，尤其是出资更多的 Bob，如果对方消失自己将无法取回钱包中的余额，甚至对方可能会以不签名为要挟进行敲诈。因此，在广播“存款”交易之前，双方都需要得到能拿回账户余额的保证，这份保证通过

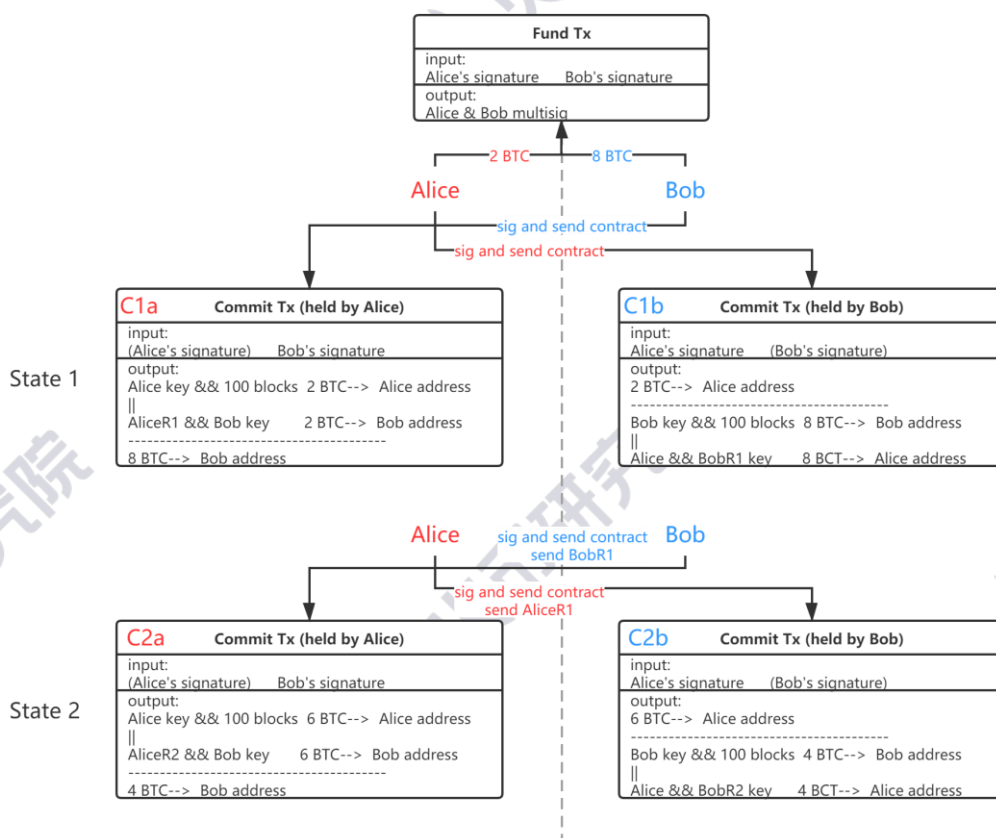
一份“提交”交易实现。

## 2) 提交交易与通道建立

如图 3 所示，State 1 的时候，Alice 和 Bob 各会签署一份提交交易给对方持有。以 Alice 持有的提交交易 C1a 为例，该交易输入为双方的签名，此时 Bob 已经签名但 Alice 自己尚未签名。

该交易的输出为资金的分配方案的脚本，该脚本此时并不会执行生效，只有当 Alice 签名并广播该交易时输出中的脚本才会执行。其思想类似于员工与公司签订了竞业协议，但在签订之时协议中的索赔条款并不会被执行，只有当员工违反条款触发竞业时，公司才会起诉员工并执行索赔条款的内容。

图3 支付通道的建立与交易流程



来源：Dryja 在 MIT 的授课内容，火币研究院整理

输出脚本的能力包含，1.将 8 BTC 归属给 Bob；2.剩余 2 BTC 分两种情况处理，如果使用 Alice 的钥匙取款，则在等待 100 个区块后 2 BTC 才能归属给 Alice，

如果使用 AliceR1(这把钥匙将在下文中介绍)和 Bob 的钥匙共同取款, 则 2 BTC 会立即归属给 Bob。因此, 即便对手方 Bob 消失, Alice 也可以通过广播 C1a, 在等待 100 个区块之后将自己的资金取回。

通过 C1a 和 C1b 交易的签订, 双方建立了打款的信任基础, 此时存款交易会被广播到区块链网络, Alice 和 Bob 之间的支付通道就建立了。

### 3) 支付通道内的交易

在支付通道建立之后 Alice 与 Bob 的交易就可以在通道内进行, 不必广播到区块链上。每笔交易只需通过签订“提交”交易并传递给对方即可, 在交易双方均在线的情况下可以实时完成, 对比区块链上 10 分钟的等待是一个质的提升。

如图 3 所示, State 2 时 Alice 与 Bob 开始了新一轮的交易, 通过互换签字后的“提交”交易 C2a 和 C2b, Bob 向 Alice 付款 4 BTC。值得注意的是, 在 Alice 与 Bob 互换合约时, 也向对方公布了自己上一轮交易的撤回密钥 AliceR1 和 BobR1, 用于向对方声明上一轮持有的“提交”交易 C1a、C1b 作废, 资金的分配以 State 2 的“提交”交易 C2a、C2b 为准。

Alice 与 Bob 可以按照此规则在支付通道内进行资金往来, 不同于微支付通道的是此处没有时间锁, 因此通道理论上可以永远存在, 直到交易的一方主动关闭支付通道。

#### 2.2.2 支付通道的正常关闭

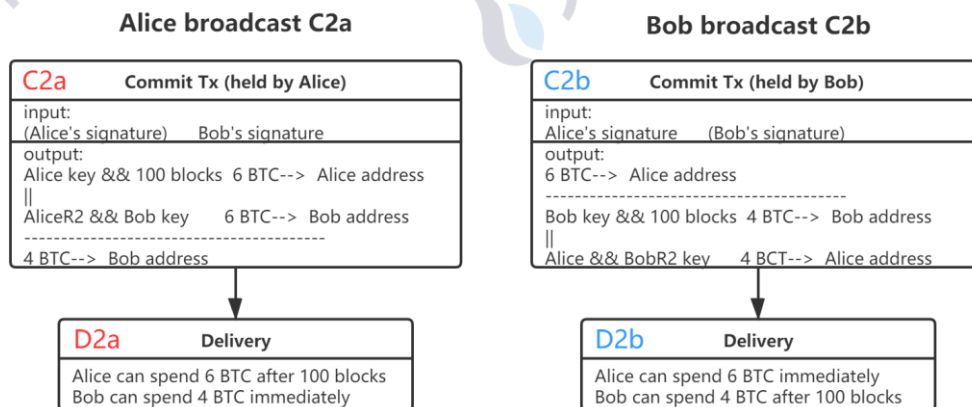
当 Alice 或者 Bob 认为二者的资金交易结束或者想要取回双签名钱包中的资金时, 可以将最新的“提交”交易在区块链上广播进行资金分配。

如图 4 所示, 以 Alice 为例, 她可以将 C2a 广播, C2a 中的输出脚本将会执行触发 D2a “分配”交易。分配时, Bob 会立即取回 4 BTC, 但 Alice 还需等待 100 个区块的时间才能取回 6 BTC。这是 RSMC 对率先提出结束交易一方的“惩罚”。

“分配”交易执行结束后, Alice 和 Bob 关闭了交易通道并在比特币网络上登记了自己的最终资金状态。



图4 支付通道的正常关闭

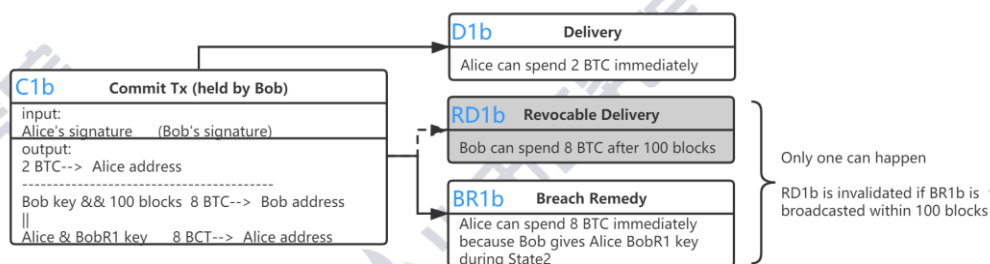


来源：Dryja 在 MIT 的授课内容，火币研究院整理

### 2.2.3 RSMC 中的抵赖与违约补偿

由于基于 RSMC 建立的支付通道并没有在物理上作废历史状态的交易，理论上，参与者仍可以通过广播历史交易来抵赖后续的付款交易。但 RSMC 巧妙设计了惩罚机制阻止此种情形发生。

图5 抵赖与违约补偿



来源：Dryja 在 MIT 的授课内容，火币研究院整理

如图 5 所示，假设 Bob 企图通过发布 State 1 的 C1b 来抵赖 State 2 发生的付款交易并关闭支付通道，D1b 将会被触发执行，Alice 在 State 1 中的余额 2 BTC 将立即被分配到 Alice 的账户中。剩下的 8 BTC 将通过 RD1b “可撤回分配”交易，在 C1b 发布后 100 个区块分配到 Bob 的账户中。但 100 个区块的产生是很长的一段时间，如果 Alice 在此期间发现了 Bob 的抵赖行为，可以拿着 Bob 给她



的 BobR1 撤回钥匙广播 BR1b “违约补偿” 交易，将双签名电子钱包中剩余的 8 BTC 全部拿走，同时使 RD1b 交易失效。被抵赖者既拿回了自己的资金，也通过罚没钱包中所有资金的方式惩罚了抵赖者。由此消除了支付通道内交易对手风险。

值得一提的是，2019 年瞭望塔机制已经开始逐步应用到闪电网络的节点中，即便用户处于离线状态，也可委托瞭望塔为其监控资金是否遭到窃取，一旦遭到窃取，瞭望塔会代替用户广播“违约补偿”交易。用户不再需要隔一段时间就上线检查对手是否作弊，大大降低了用户对闪电网络的使用成本。关于瞭望塔会在本文的 5.1 小节做更深入的探讨。

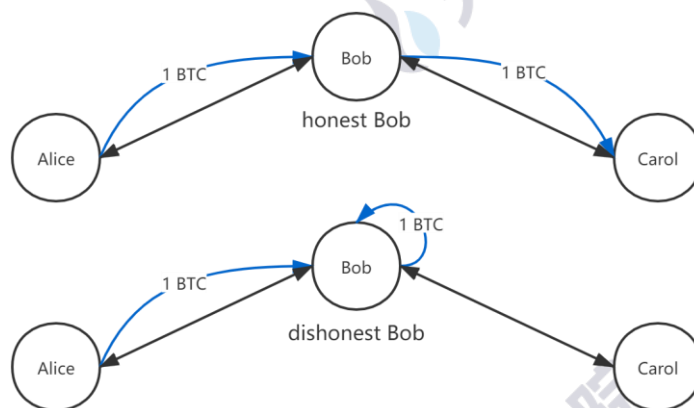
## 2.3 编织网络的 HTLC

RSMC 在微支付通道的基础上为用户两两之间的资金交易提供了长期、高效的解决方案。但如果每两个用户需要交易时都需要建立新的支付通道，将会大幅增加网络中的连接数，每个通道的建立也都需要比特币网络的处理(必然就涉及了等待和交易费用)，这并不经济。HTLC(Hashed Time Lock Contract, 哈希时间锁定合约)提供了借用网络中已经建立的连接，使未直连的用户能够进行可信的资金交易的解决方案。只要网络中有一条路径能连接交易双方就可以进行可信交易，大幅提升了网络的扩展性。

### 2.3.1 多方参与问题

如图 6 在没有 HTLC 的情况下，如果未建立支付通道的 Alice 想向 Carol 转账 1 BTC，就需要与二人都建立过支付通道的 Bob 的帮助。Alice 先将 1 BTC 转给 Bob，Bob 再将其转给 Carol。这需要一个可信的 Bob 才能保证支付顺利完成，因为 Bob 可能会将这 1 BTC 中饱私囊。即便 Bob 可信，这种交易方式也违背了比特币的初衷——通过分布式账本避免依赖可信的第三方。

图6 多方参与的情况



来源：Dryja 在 MIT 的授课内容，火币研究院整理

### 2.3.2 HTLC 的处理流程

HTLC 通过巧妙利用哈希时间锁保证了中间的路由节点无法扣留路过的资金，也不需要依赖可信的第三方来做担保。如图 7 所示为 HTLC 的处理流程。

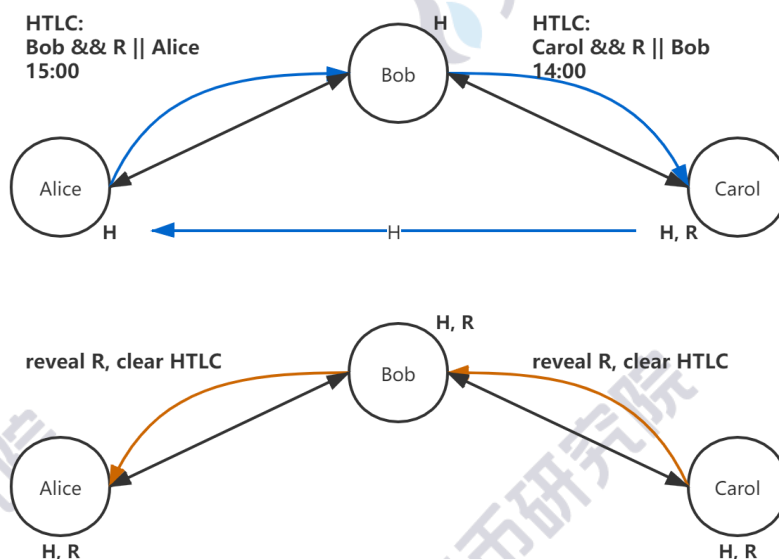
**交易的发起。**当 Alice 要向 Carol 付款 1 BTC，正式发起交易之前，Carol 会先自己准备好一个 R，然后对其哈希加密生成 H(注意无法通过 H 反推出 R)，即  $H = \text{Hash}(R)$ ，并将这个 H 传输给 Alice。

**正向传递 H 建立 HTLC。**Alice 拿到 H 后，会将 H 发送给 Bob，并向 Bob 发起 HTLC 的转账交易。如果 Bob 能在 15:00(仅是一个示例时间)之前告诉 Alice H 对应的 R 是多少，Bob 就可以拿到 1 BTC，否则，Alice 可以拿回 1 BTC。Bob 在与 Alice 签订 HTLC 合约并拿到 H 之后，会对 Carol 进行相同的操作，签订合同并传递 H，同时设立一个更早的截止时间 14:00。

**反向传递 R 清除 HTLC。**Carol 拿到 H 后发现与自己持有的 H 相同，于是将 R 匹配到 HTLC 中拿到 1 BTC，并告知 Bob R。同理，Bob 可以凭借 R 拿到 Alice 的 1 BTC 同时结束与 Alice 的 HTLC。整个交易结束。

这个过程中，路由节点 Bob 要通过 R 才能拿到 Alice 的 1 BTC，但为了拿到 R，他不得不先向 Carol 交出 1 BTC，无法中饱私囊，由此解决了中间节点作恶的问题。

图7 HTLC 处理流程



来源：Dryja 在 MIT 的授课内容，火币研究院整理

值得注意的是，链路上的锁定时间必须是递减的，假设 Alice 和 Bob 约定的截止时间是 15:00 而 Bob 与 Carol 的约定时间是 16:00，则 Carol 可以在 15:30 时通过 R 拿走 Bob 的 1 BTC，而 Alice 的 1 BTC 已经在 15:00 时取回了，Bob 就会遭受损失。但由于 Bob 和 Carol 交易的截止时间是由 Bob 定的，所以 Bob 自身通过合理安排时间可以避免这种情况的发生。

同时，RSMC 和 HTLC 可以在同一个“提交”交易中拟定的，具体形式如图 8 所示。

图8 RSMC 与 HTLC

RSMC without HTLC	RSMC with HTLC																																
<b>C1a</b> Commit Tx (held by Alice) <table border="1"> <tr> <td>input:</td><td>(Alice's signature)      Bob's signature</td></tr> <tr> <td>output:</td><td>Alice key &amp;&amp; 100 blocks    6 BTC--&gt; Alice address</td></tr> <tr> <td></td><td>  </td></tr> <tr> <td></td><td>AliceR2 &amp;&amp; Bob key      6 BTC--&gt; Bob address</td></tr> <tr> <td></td><td>-----</td></tr> <tr> <td></td><td>4 BTC--&gt; Bob address</td></tr> </table>	input:	(Alice's signature)      Bob's signature	output:	Alice key && 100 blocks    6 BTC--> Alice address				AliceR2 && Bob key      6 BTC--> Bob address		-----		4 BTC--> Bob address	<b>HT1a</b> Commit Tx (held by Alice) <table border="1"> <tr> <td>input:</td><td>(Alice's signature)      Bob's signature</td></tr> <tr> <td>output:</td><td>Alice key &amp;&amp; 100 blocks    5 BTC--&gt; Alice address</td></tr> <tr> <td></td><td>  </td></tr> <tr> <td></td><td>AliceR2 &amp;&amp; Bob key      5 BTC--&gt; Bob address</td></tr> <tr> <td></td><td>-----</td></tr> <tr> <td></td><td>4 BTC--&gt; Bob address</td></tr> <tr> <td></td><td>-----</td></tr> <tr> <td></td><td>HTLC Bob &amp;&amp; R    1 BTC--&gt; Bob address</td></tr> <tr> <td></td><td>  </td></tr> <tr> <td></td><td>Alice &amp;&amp; 15:00    1 BTC--&gt; Alice address</td></tr> </table>	input:	(Alice's signature)      Bob's signature	output:	Alice key && 100 blocks    5 BTC--> Alice address				AliceR2 && Bob key      5 BTC--> Bob address		-----		4 BTC--> Bob address		-----		HTLC Bob && R    1 BTC--> Bob address				Alice && 15:00    1 BTC--> Alice address
input:	(Alice's signature)      Bob's signature																																
output:	Alice key && 100 blocks    6 BTC--> Alice address																																
	AliceR2 && Bob key      6 BTC--> Bob address																																
	-----																																
	4 BTC--> Bob address																																
input:	(Alice's signature)      Bob's signature																																
output:	Alice key && 100 blocks    5 BTC--> Alice address																																
	AliceR2 && Bob key      5 BTC--> Bob address																																
	-----																																
	4 BTC--> Bob address																																
	-----																																
	HTLC Bob && R    1 BTC--> Bob address																																
	Alice && 15:00    1 BTC--> Alice address																																

来源：参考闪电网络白皮书及 Dryja 在 MIT 的授课内容整理而得

### 2.3.3 路由与手续费

读到这里读者心中可能会有疑问，Alice 如何知道 Bob 可以连接到 Carol，而 Bob 又为什么要帮助 Alice 向 Carol 转账呢？这就涉及到 HTLC 的路由机制与费用机制了。

#### 路由

针对路由，HTLC 使用了源路由与洋葱路由的机制。网络上所有的节点会发布自己路由信息和资金限制形成支付通道表。交易的源头(发起方)通过该表计算起点到终点的路径并指定交易通过该路径执行。同时，利用洋葱路由的机制，使得每一个路由节点都只知道相邻的节点，无法了解整条路径，由此达到保护隐私的目的。这两种机制均是已有的路由机制，被应用到了闪电网络的构建中。

#### 手续费

实际上，作为中间节点的 Bob 可以标明他路由的手续费，如 0.01 BTC，那么 Alice 在向 Carol 转账 1 BTC 的交易中，会在与 Bob 签订交易时向其支付 1.01 BTC，而 Bob 向 Carol 支付 1 BTC，达到了手续费收取的效果。如果 Bob 是一个天价手续费收取者，Alice 在计算路由方案时就会将 Bob 排除在外，选取别的路由节点。

## 2.4 闪电网络

由此，RSMC 与 HTLC 互为助力，RSMC 解决资金单向流动的问题，HTLC 解决多方参与的问题，在比特币二层链下形成了高扩展性的支付通道——闪电网络。

## 三、闪电网络的生态




### 3.1 开发团队

自 2015 年 Joseph Poon 和 Thaddeus Dryja 发布第一个版本的闪电网络的白皮书以来,陆续有团队加入到闪电网络核心技术研发的行列中来,详细信息参考表 2。其中最主流的 3 个团队(或公司)是 Lightning Labs、ACINQ 及 Blockstream,他们基于不同语言研发了闪电网络的协议及其关联核心技术,稍晚一些, Nayuta 也加入了他们的行列。下面将对这四支团队做一些介绍。


Lightning Labs 创建于 2016 年,是一支围绕闪电网络进行技术、产品研发的国际团队。其开源产品包括(Loop、LND、Neutrino 等)旨在提供安全、可扩展的闪电支付系统,帮助用户高效的进行日常转账、支付操作。此外, Lightning Labs 还进一步提供基于闪电网络的可验证、非托管衍生金融服务。从开源开发者社区来说, Lightning Labs 从实践上打通了开源软件生态和下一代比特币金融软件生态。

ACINQ 成立于 2014 年,是一个来自法国巴黎的创业团队,主要为比特币生态进行面向扩展性优化的技术研发并提供相关产品、服务。ACINQ 基于 Scala 语言开发了闪电网络的实现 Éclair(该单词在法语中正是“闪电”的意思),被认为是最主流的闪电网络协议实现之一。此外,基于 Éclair 网络, ACINQ 推出了相应的产品栈,包括 Phoenix、ACINQ Node、Strike 等。

表2 闪电网络核心技术主要产品及开发团队

标志	产品名称	开发团队	实现语言	开始时间	持续维护	开源
	LND - Lightning Network Daemon	Lightning Labs	Golang	2016.01	是	是
	eclair - A Scala implementation of the Lightning Network	ACINQ	Scala	2016.01	是	是
	lit - Lightning Network node software	MIT Media Lab	Golang	2016.11	否	是
-	c-lightning - A Lightning Network	Blockstream	C	2015.06	是	是



	implementation in C					
-	rust-lightning - A Lightning Network implementation in Rust	Matt Corallo	Rust	2018.03	是	是
-	lightning-onion - Onion Routed Micropayments for the Lightning Network (Golang)	Lightning Labs	Golang	2016.01	是	是
 Ptarmigan	ptarmigan - C++ BOLT-Compliant Lightning Network Implementation	Nayuta	C++	2017.07	是	是

说明：开始时间根据项目在 GitHub 上的初次有效提交时间确定

来源：公开资料，火币研究院整理

Blockstream 创建于 2014 年，是比特币生态领先的技术、服务提供商，专注于包括密码学、分布式系统方向上的研究。Blockstream 的核心产品 c-lightning 是闪电网络最主流的实现之一。其他主要产品包括 Elements、Blockstream Satellite、Liquid Network 等。其技术愿景是打造基于比特币区块链的加密金融基础设施框架。利用前沿的密码、安全技术，Blockstream 旨在降低金融市场上的信任成本从而大幅提高交易效率。经过长时间的实践积累，该团队对于在 P2P 开放网络环境下构建高性能、可扩展、普惠的金融交易协议具有重要的研发经验。

Nayuta 是一支来自于日本的技术产品团队，建立于 2015 年，主要面向比特币生态进行软、硬件系统研发。围绕闪电网络，Nayuta 推出了包括协议实现以及上层应用端的不同产品，如 Ptarmigan、Nayuta Wallet 等。其中，其核心产品 Ptarmigan 节点软件实现了闪电网络标准，并提供在不同硬件平台上的支持，从而能够良好对接基于物联网设备的新一代支付需求。此外，Nayuta 正在研发面向企业用户的联盟链闪电网络，提供企业间高性能支付、结算服务。

### 3.2 应用情况

闪电网络应用(LApps, Lightning Network Apps)目前还处于发展的早期，但其即时性和低手续费也吸引了众多开发者贡献了很多支持闪电支付的应用，覆盖钱

包、游戏、购物、加密数字资产兑换、餐饮、即时通讯等等。

**加密数字资产钱包。**据 Lightning Network Stores 的数据统计，迄今为止，市面上共有 30 款左右的加密数字资产钱包支持闪电网络，这一数字在 2019 年初是仅为 6 款。这些钱包分为托管钱包和非托管钱包两类，支持的终端主要是 Android 和 iOS，少部分钱包还支持 Windows、Mac、Linux 及浏览器插件。值得注意的是，在 7 月初，老牌钱包 Electrum 发布新版本，也支持了闪电网络、瞭望塔及潜交换等功能。

图9 部分支持闪电网络的加密数字资产钱包

Name	Open source	Requires own node	Custodial	Mainnet launch date	Web wallet
<a href="#">eclair wallet</a>	yes	no	no	April 2018	no
<a href="#">BlueWallet</a>	yes	no	yes	December 2018	no
<a href="#">Wallet of Satoshi</a>	no	no	yes	January 2019	no
<a href="#">bitcoin lightning wallet</a>	yes	no	no	May 2018	no
<a href="#">Sats app</a>	no	yes	no	September 2019	no
<a href="#">Phoenix</a>	yes	no	no	November 2019	no
<a href="#">LightningPeach</a>	yes	no	no	March 2019	no
<a href="#">Breez</a>	yes	no	no	April 2019	no
<a href="#">Muun</a>	yes	no	no	May 2019	no
<a href="#">Lightning Labs' wallet</a>	yes	no	no	June 2019	no
<a href="#">Nayuta wallet</a>	no	no	no	October 2019	no
<a href="#">Budda.com</a>	no	no	yes	June 2019	no
<a href="#">Bitpie</a>	no	no	yes	March 2019	no

来源：Lightning Network Stores，火币研究院整理

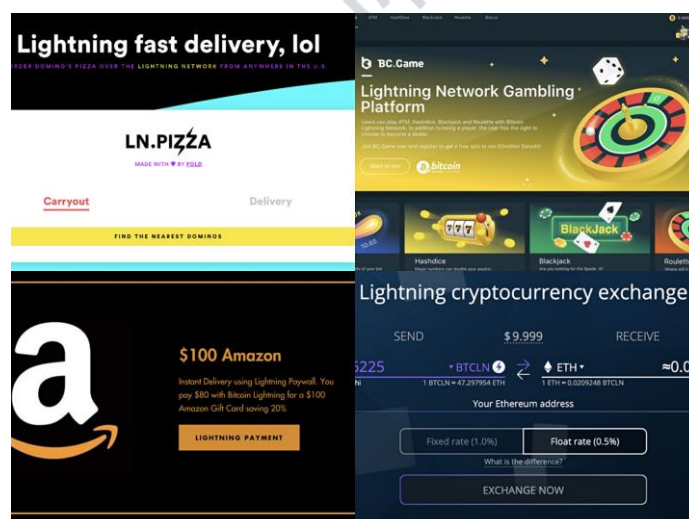
**即时通讯。**有开发者利用闪电网络的特性开发了即时通讯软件，如 Lightning Labs 团队开发的 Whatsat，该 App 能通过非直接连接提供匿名发送信息的能力。洋葱路由会使得信息的路径和源头变得难以追踪增强匿名性；另一方面，由于没有中心化的服务器，用户两两之间通过建立直接连接的聊天内容也难以被外界追

查。类似的应用还有 LnSMS.world、Receive SMS、Paypercall 等。

**线上购物。**闪电网络快速支付和低手续费的特性为使用比特币进行购物提供了新的生命力,有开发者提供了基于闪电网络的网上购物中心, Bitrefill、Paid.co、CoinMall 等,以及线上销售平台,如 Nanopos 等,也有团队支持了使用闪电网络钱包到现有电子商务平台(如 Bitcard 支持在 Amazon 上使用比特币购买礼品卡)或餐饮店上购买商品或服务,如 LN.Pizza、Starblocks 等。

**游戏。**闪电网络的即时性为在线轻量级游戏提供了可能,各类游戏如棋类(Lightning Chess 为例)、纸牌类(Lightning Poker 为例)、博彩类(BC.game、Luckdice 为例)等都出现在了应用商店中并吸引了大量玩家的眼球。

图10 部分支持闪电网络的应用



来源: Lightning Network Stores, 火币研究院整理

**跨链交易。**闪电网络点对点网络传输模式使其天然支持原子交换,这就使得跨链交易十分便捷。相关的应用如 Sparkswap、ZigZag 等也出现在市场上,提供非托管的去中心化的买卖及加密数字资产交易的服务。

除了这些之外,闪电网络之上还活跃着大量其他应用,如小费支付、广告,甚至还有嵌入硬件的尝试(如 PolloFeed,一款通过闪电网络远程喂鸟的应用)。

可以看到,闪电网络的诞生为区块的生态注入了新的生命力。由于不支持智能合约,相比于以太坊等,区块链的去中心化应用生态一直没有得到很好的发展。闪电网络的诞生使得我们日常生活中经常使用的应用或服务开始有了比特币网

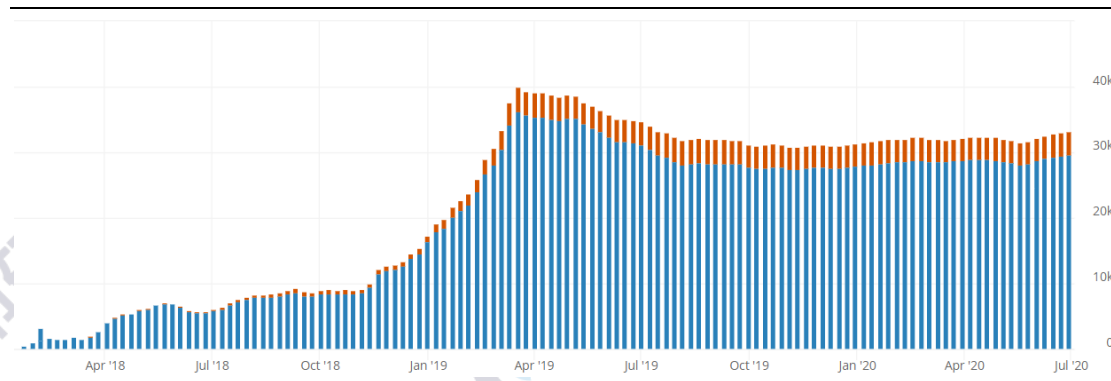
络下的翻版，虽然其易用性和用户规模还远不能相比，但至少提供了起点。

### 3.3 活跃情况

2015 年，闪电网络的概念一经推出就收获到了区块链领域热烈的讨论和开发人员的投入。2017 年 12 月 27 日，Alex Bosworth 使用 Bitrefill 支付电话费诞生了闪电网络上第一笔商业交易。2018 年初，闪电网络正式在比特币主网上线，在经历短期的快速增长后增速就趋于平缓。

2018 年 10 月到 2019 年 3 月，闪电网络经历了一轮快速的增长，通道数和容量均增长了数倍，分别从近 1 万条通道、容纳 100 个左右的 BTC 增长至 4 万条通道、容纳 1000 多个比特币。该增长一部分得益于声势浩大的“闪电火炬”传递活动，一度火出圈外；另一部分原因是该时间段内比特币的价格一直在低位徘徊，持币人变现意愿大幅下滑，推动一部分比特币沉淀到闪电网络中。此后，通道数和容量均经历了小幅的下跌而后上涨的趋势，这也可能是比特币的投资属性带来的波动。迄今，闪电网络通道数 3.7 万余条，容纳资金在 1000 BTC 上下浮动，尚未回到 19 年的巅峰水平。

图11 闪电网络通道数

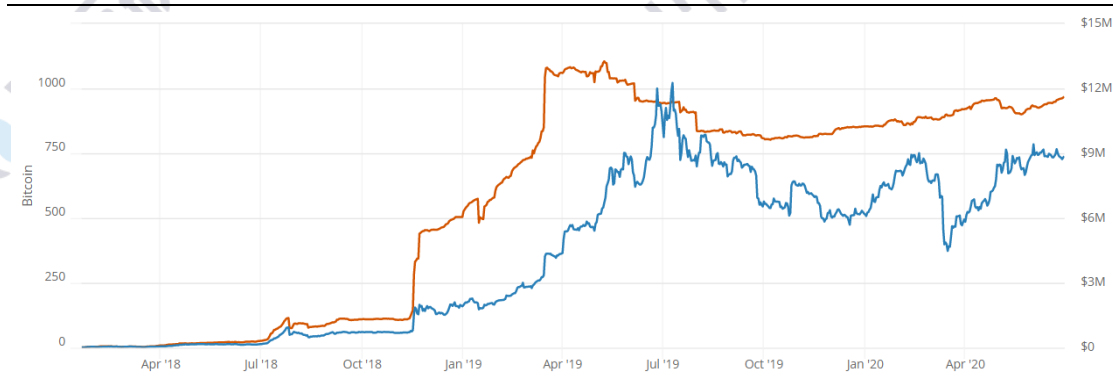


说明：红色表示通道是复用通道，蓝色表示节点间的通道是初次建立

来源：Bitcoin Visuals，火币研究院整理



图12 闪电网络容量



说明：红色表示通道的比特币容量，蓝色表示通道中比特币对应的美元价值

来源：Bitcoin Visuals，火币研究院整理

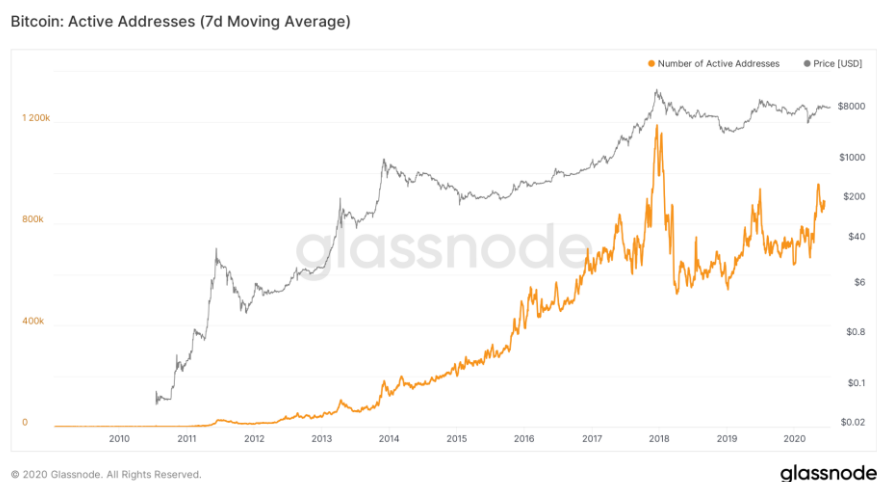
图13 当前闪电网络分布情况



说明：数据时间为 2020 年 7 月 13 日

来源：Lightning Network Explorer，火币研究院整理

图14 比特币活跃地址数





说明：红色为比特币活跃地址数，灰色为比特币兑美元价格

来源：glassnode，火币研究院整理

当前，闪电网络上的节点数约 1.3 万个，根据 Lightning Network Explorer 的数据，其大多集中在西欧和美国，基本和比特币的活跃地区一致。闪电网络是比特币网络的二层网络，而闪电网络的用户主也要来自于比特币网络用户的转化，参考近期在 90 万上下波动比特币的活跃地址数(地址数和用户数不能等价)，闪电网络还有很大的成长空间。新技术的研发带来的闪电网络的实用性和用户友好性的提升或是后续闪电网络扩张的原动力。

## 四、闪电网络的贡献与局限

### 4.1 贡献

#### 4.1.1 提升比特币网络扩展性

闪电网络能为比特币带来的扩展性的提升是毋庸置疑的，其设计的初衷就是为了解决比特币区块大小限制和交易等待时间长带来的扩展性困境——每秒仅能处理 7 笔交易，这个困境也是制约比特币发展的重要因素之一。闪电网络创新性的设计了 RSMC 和 HTLC，提供在链下进行近实时小额交易的能力，既缓解了比特币主链的压力，又为用户提供了便捷的支付方式，一举多得，为区块链更大规模的扩张提供了可能性。

#### 4.1.2 降低交易的时间和资金成本

降低交易成本主要从两个方面体现。**1.降低交易等待时间。**原本在比特币主链上，每笔交易需要 10 分钟才能提交，1 个小时才能确认，而在闪电网络上，点对点的通信模式，用户之间只需签署双方均认可的交易协议就可以提交，双方均在线的情况下实时就可达成。且通道的持续时长不受限制，用户可在通道内反复交易，在交易结束后再将资金分配状态广播到主链确认资金分配，将原本多次的确认等待时间压缩到 1 次。**2.降低交易手续费。**比特币主链上每笔交易都需要收取一定的手续费，其峰值一度达到 55 美元(后续有所回落，近期在 1 美元上下浮动)；而在闪电网络上只有打开和关闭通道需要在主链上进行交易，其余交易均在闪电网络内进行，而目前网络内主要路由节点一天的收入也才在 10 万聪(约 7 美元)左右，可见路由佣金之低。由此，闪电网络为比特币生态拓展了中高频小额交易的场景，也为用户提供了中高频小额交易的更优选择。

#### 4.1.3 支持跨链交易

区块链上主流的跨链机制主要有三种，公证人(Notary schemes)、侧链/中继链(Sidechains / Relays)和源自闪电网络的哈希锁定(Hash-locking)。相比于其他两类，哈希锁定的方式不需要依赖可信的第三方，不会受到 51%攻击，实现也最为

轻量级。闪电网络使用了哈希时间锁的技术，天然就支持了跨链交易，使得闪电网络能为用户提供去信任化的多方跨链交易的能力。

#### 4.1.4 促进比特币生态发展

比特币作为一种加密数字资产，比特币网络作为一种点对点的电子现金系统，其生态系统的基础就是便捷的支付。无疑，闪电网络技术的诞生为破除比特币支付因性能带来的瓶颈有重大现实意义。虽然相比传统的支付宝、VISA 等支付方案其还有一定差距，但就比特币自身来说，实则是迈出了即时支付从不可能到可能的一大步，为其进入日常生活的支付场景提供了重要技术支持。

此外，比特币生态一直饱受诟病的一点是其未能发展出像以太坊等的去中心化应用(decentralized app, DApp)的生态，以致其应用场景蜷缩在支付和投资(目前更多的可能是投机)上，也将其开发群体和用户群体限制在一个很小的范围内。而闪电网络的诞生催生了 LApps，为完全分布式的应用在比特币生态上的发展铺好了上升的阶梯。交易成本(时间成本和金钱成本)的降低和小额支付的高性能支持，吸引了更多的社区开发者的加入，因而贡献了更多元化的应用场景，从而能吸引更多用户加入其中，形成积极的正向循环。

### 4.2 局限

#### 4.2.1 受限的支付上限

非直连的用户在闪电网络上支付时，实际上是通过支付接力实现的，因而会产生路由节点资金不够完成接力的情况，导致越大额的资金越难支付成功。19 年初声势浩大的“闪电火炬”接力活动也因遭遇流动性问题显得有些意兴阑珊。

但值得注意的是，2019 年 12 月底 Blockstream 宣布原子多路径支付(Atomic Multi-Path Payments)技术已通过互操作性测试，目前还未正式上线。c-lightning 在今年 5 月中旬发布的 0.8.2 版本中也支持了大通道支付，移除了 0.16 个 BTC 的付款上限。虽然这两项技术，目前还没有在闪电网络中大规模落地，但这些扩展技术的发展有望切实解决闪电网络支付通道上限问题，为闪电网络引入更多的金融、贸易等领域应用场景。

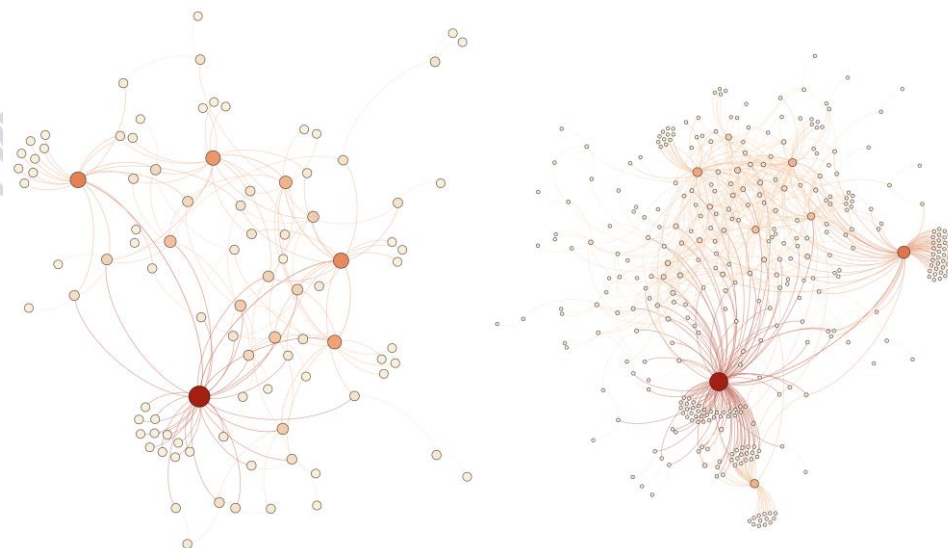
### 4.2.2 节点和资金集中化明显

闪电网络上线以来，其集中化问题一直受到广泛关注，该问题主要体现在两个方面。**1.路由节点集中化。2.资金集中化。**

闪电网络利用 HTLC 机制实现了无直接连接的用户之间的支付通道，但中间路由节点的创建和维护需要一定的技术门槛，同时低廉的佣金也难以激励用户节点承担路由的工作，因此催生了路由节点的集中化。集中化的路由节点一定程度上降低了路由的路径长度，提升了交易的稳定性，但会带来**单点问题、负载问题、隐私问题**等，违背了区块链去中心化的思想同时也一定程度上催生了资金集中化的问题。

中心的路由节点为了保证能承担更多的路由负载必然会存放大量资金在节点上。一篇研究论文<sup>[1]</sup>对闪电网络从2018年1月14至2019年7月13期间的数据分析表示，闪电网络内的资金分布十分不均衡，基尼系数高达约0.88，这表明网络上10%的节点持有了80%的资金，50%的节点持有了99%的资金。这不是一个健康发展的生态环境的表现。

图15 闪电网络的集中化问题



来源：Lightning Network: a second path towards centralisation of the Bitcoin economy, 火币研究院整理

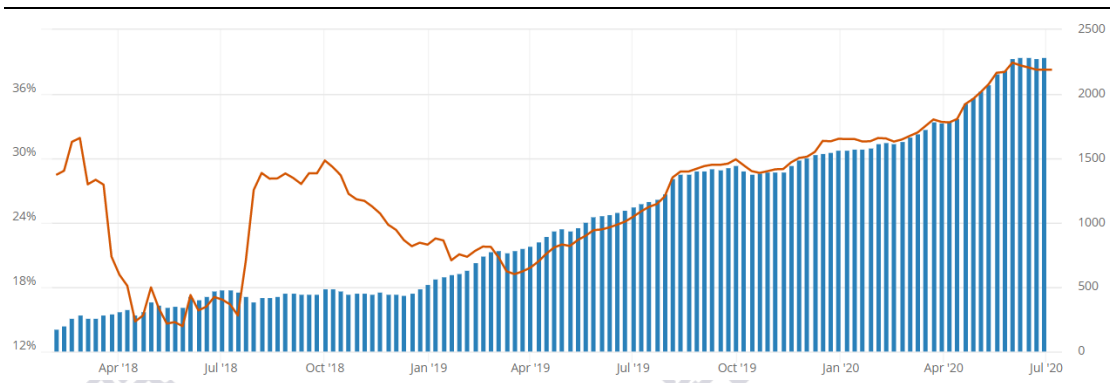


### 4.2.3 网络稳定性问题亟待解决

对于支付系统来说，稳定性是重中之重，没有人愿意将资金放在一个三天两头崩溃或者业务失败的平台。但年轻的闪电网络确实还面临着一系列稳定性问题。其中单点问题、流动性攻击问题、支付成功率问题可能是目前最显著的几个稳定性问题。

前文中有提到闪电网络的中心化问题，单点问题是中心化问题的延伸，一旦中心节点或者通道遭到攻击或者丢失连接会导致很多节点变成孤立节点，将大大降低整个网络的可用性甚至导致网络瘫痪。如图 16 所示，当前关键通道(如果通道断连会导致有节点无法形成支付路径)的数目已达两千两百余条，约占总通道数的 38%。

图 16 关键通道数量与占比

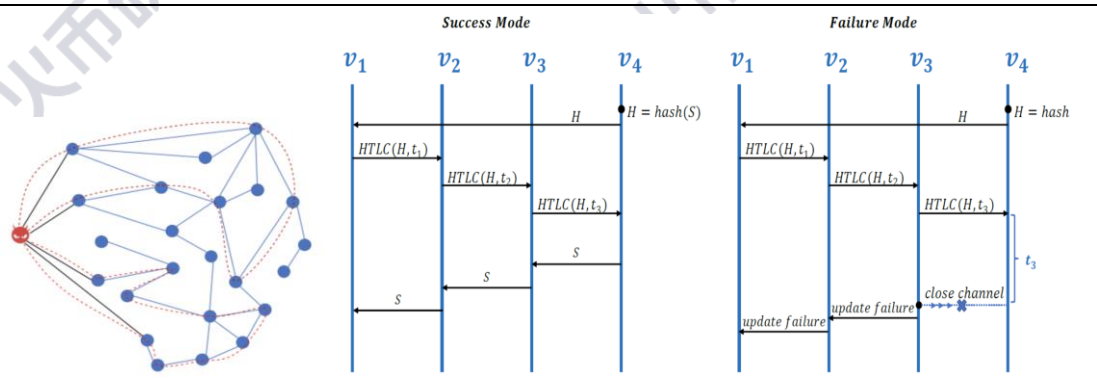


来源：Bitcoin Visuals，其中蓝色表示关键通道数目，红色表示关键通道占比

另一个值得担心的稳定性问题就是流动性攻击的问题，论文<sup>[2]</sup>中提到在现有的闪电网络技术条件下，攻击者可以使用少于 0.25 BTC 使闪电网络中高达 650 BTC 丧失流动性达 3 天之久。该种攻击的主要思想是，攻击节点同时作为支付的发起方和接受方，以小额资金发起转账请求，但接受方在签订 HTLC 之后不为前继节点提供 R，使整条链路都处于等待状态，通道上节点的流动性被锁定。通过循环这种操作，达到锁死网络内大量流动性的目的，可导致网络瘫痪。



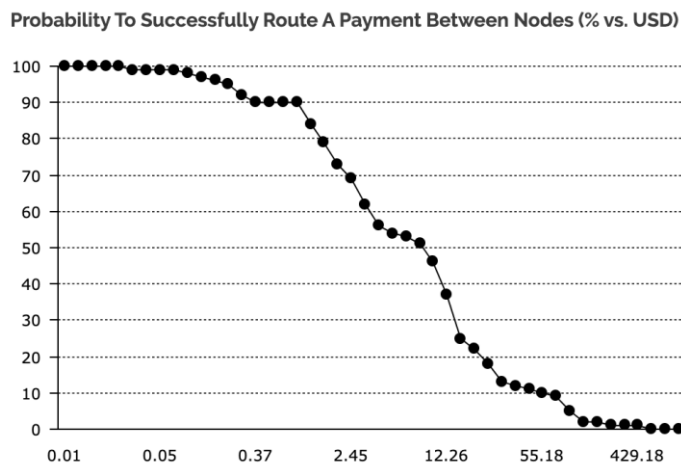
图17 流动性攻击原理



来源：Congestion Attacks in Payment Channel Networks, 火币研究院整理

支付成功率也是衡量支付通道稳定性的重要标准。据 Diar 在 2018 年 6 月底的一份报告中显示，仅数美金的支付的成功率也仅在 70% 左右，随着金额的增加会有显著下滑，交易金额超过 300 USD 时，成功率仅有 1%。这也呼应了前文提到的“支付通道上限问题”。同时，中间路由节点的下线也是造成支付失败的原因之一，闪电网络的交易成交要求交易双方同时在线签订协，一方下线会导致交易搁置，一旦一方下线时长超过了时间锁的约定时间，交易就会失败。

图18 闪电网络的支付成功率



来源：Diar, Lightning Strikes, But Select Hubs Dominate Network Funds, 火币研究院整理

#### 4.2.4 难以保障的数据隐私

闪电网络借由洋葱路由一定程度上加大了支付路径追踪的难度，但是随着集

中化问题的产生，大部分交易都会经由中心节点达成，这大大增加了暴露交易方的风险，几位研究人员也在研究中<sup>[3]</sup>指出了这一问题。同时，闪电网络应用到更多的线上线下的支付环境中时，在大数据技术成熟的当下，支付节点的主人也更容易暴露其身份。如果闪电网络的集中化问题能得到解决，隐私问题也能在一定程度上得到缓解。

#### 4.2.5 受约束的网络可扩展性

闪电网络本身的扩展性问题也值得关注。由于闪电网络采用了源路由的机制，网络中的每一个节点都有需要维护一份支付路径路由表用于规划交易的路由路径。这在闪电网络现有规模下并不是什么问题，但是当网络规模扩大后，全网节点的连接信息和可支付金额信息的存储及实时更新问题，高并发情况的路径选择余额分配问题，等等都会带来扩展性问题并制约闪电网络的发展。

#### 4.2.6 较高的使用门槛

降低用户门槛提高使用的友好度是应用型技术能普及的重要先决条件。即便对于比特币用户，要理解使用闪电网络交易或者如何成为一个路由节点赚取佣金，并不是一件很容易的事情，更不用说广大的非比特币用户群体。由于闪电网络的发展还在早期，没有成熟的商业化包装，用户在使用闪电网络进行交易时不得不去了解一些其中的技术细节，还要经历并不友好的操作过程，最后还可能遭遇支付失败，这大大提升了用户的门槛降低了用户的使用意愿。

## 五、闪电网络的扩展技术与服务

通过前文的剖析可以看到，闪电网络为比特币技术和生态的发展均有裨益，但由于其技术完整度尚不高，不可避免地也引入了一些问题。针对这些问题，研究人员和开发社区持续研究和引入各项闪电网络的扩展技术和服务，本章将以瞭望塔、潜交换以及原子多路径支付为代表进行探讨。

### 5.1 “欺诈斗士”瞭望塔

#### 背景

为了消除闪电网络中的对手风险，RSMC 技术设计了惩罚机制，不仅可以追回资金还能罚没抵赖者在通道中的所有资金补偿受害者。但是该惩罚机制的运行要求用户定期上线检查，以确认是否遭遇到对手方的抵赖。如果用户错过了可以实施惩罚的时间窗口期，其损失的资金将无法被追回。但作为一项支付技术，要求用户定期上线检查资金安全状况，其使用感之差不言而喻。可以认为，这个问题得不到解决，闪电网络的支付解决方案在市场化竞争上毫无优势可言。瞭望塔技术的提出就是为了解决这个问题，保障用户在持续离线状态下资金不被对手方盗取。

#### 发展

瞭望塔技术的雏形，在闪电网络的白皮书中就有提及。其核心思想是在不泄露用户隐私信息的情况下，通过第三方代理代替用户监察对手抵赖行为并发布违约补偿交易。在白皮书之后不断有研究者和开发团队针对瞭望塔技术提出更细致的技术解决方案和闪电网络节点激励方案。McCorry 等人提出的 Pisa 协议<sup>[4]</sup>、Avarikioti 等人提出的瞭望塔的分布式服务协议 DCWC<sup>[5]</sup>和瞭望塔激励兼容的 Cerberus 通道<sup>[6]</sup>。除了学术研究之外，业界也一直有团队在尝试落地瞭望塔。2019 年 6 月，Lightning Labs 团队首次将瞭望塔技术集成到闪电网络中<sup>[7]</sup>。紧随其后的 2019 年 7 月，BitMEX 将其闪电网络节点升级至包含瞭望塔功能的版本<sup>[8]</sup>。

#### 原理

瞭望塔在闪电网络上的实现主要涉及三个角色，交易双方及瞭望塔。仍以 Alice 和 Bob 的支付通道为例进行讨论，假设 Alice 使用了瞭望塔服务。

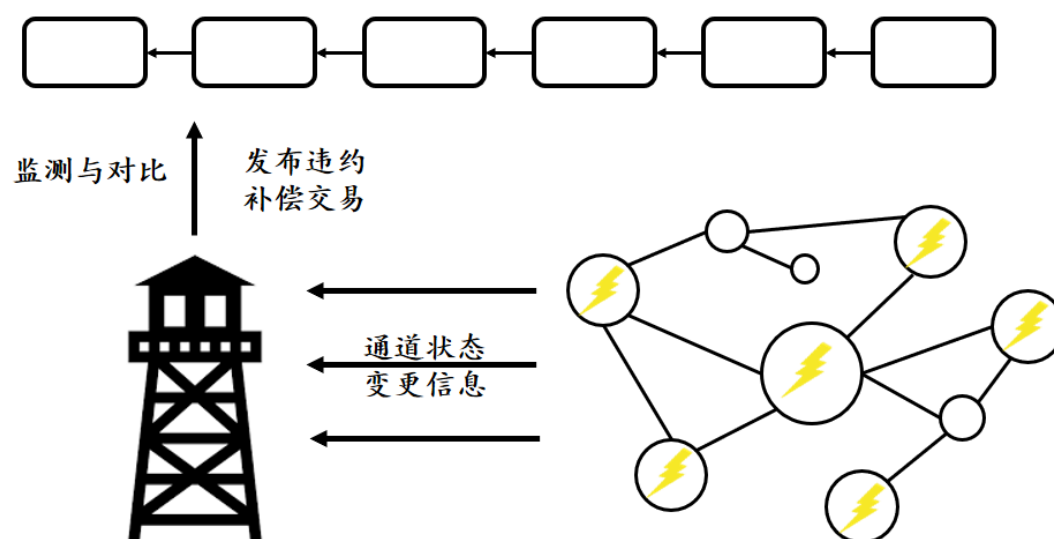
Alice: 每次当二者之间发生了交易更新了支付通道的状态，Alice 均会向瞭

望塔发送签名消息授予瞭望塔代为执行违约补偿交易的权利,同时告知瞭望塔交易的哈希信息。

**Bob:** Bob 是 Alice 的对手方,可能会在给 Alice 转账后通过发布历史交易上链,来抵赖当前的转账交易。

**瞭望塔:** 瞭望塔会利用 Alice 提供的哈希信息与链上交易对比,并持续监测是否有抵赖行为。一旦发现历史状态的交易被 Bob 发布上线,就会解密 Alice 发送的与历史交易对应的签名消息,并代替 Alice 发布违约补偿交易,将通道内的所有资金都转移给 Alice。

图19 瞭望塔功能示意图



图片来源：火币研究院

瞭望塔技术提出与应用对于提升闪电网络的易用性至关重要,但其本身也面临着技术和运营上的各类挑战,其中最受关注的是扩展性、隐私和运营模式。

为了实现监测抵赖交易的能力,瞭望塔需要实时搜集与存储闪电网络中所有支付通道的状态变更,并与链上新打包的交易进行比对。这意味着瞭望塔不仅需要存储和维护全量的链上数据,同时也要实时搜集和监测和存储链下数据,当闪电网络规模不断扩大,瞭望塔自身的扩展性就成为了问题。

同时,随着瞭望塔服务时间的增长,对于每一个用户其存储和计算成本会持续上升。在这个过程中,用户开放给瞭望塔的信息越少,用户的隐私性就越强,



但瞭望塔的开销就会越高。隐私导向型的瞭望塔不会获取每条发送至瞭望塔的消息的账户和通道信息,但这样也就意味着无法以账户模式对用户进行管理及收取费用,盈利会非常困难,使瞭望塔缺少持续经营的激励机制。业务导向性的瞭望塔可以将消息与账户联系起来,制定合理的营收模式,但这种方式会暴露用户的资金流动情况及其他个人习惯和信息,带来隐私保护的挑战,甚至可能将瞭望塔演变成金融监管中心,丧失公有区块链完全分布式的特点。

## 5.2 “上下互通”潜交换

### 背景

用户两两之间的支付通道可以想象成是一个沙漏,沙漏的每一端代表一个用户,沙漏中的沙子代表锁定在支付通道中的资金。沙子可以在沙漏的两边自由分配,但是如果向沙漏中增加沙子或者把沙漏中的沙子取出,只能选择将沙漏打破。这就是用户在使用闪电网络的支付通道时另一个易用性问题所在,通道中的资金容量在通道建立之初就确定了,无法向通道中追加资金,也无法在不关闭通道的情况下取回通道中的资金,各个通道间及链上的资金无法与实现相互流转。这极大限制了用户的资金流动性。为了改善这个问题,再平衡技术实现了同一用户在其多个通道中进行资金划转,但仍未实现链上链下余额的统一管理。在此背景下,潜交换(Submarine Swap)技术被提出,实现了在不关闭支付通道的情况下,完成链上链下的资金交换,对通道中的资金进行充提。最终,大大降低了同一用户在链上、链下及链下的各通道间资金统一管理的难度。

### 发展

潜交换技术最早由 Lightning Labs 的 Alex Bosworth 和 Olaoluwa Osuntokun 提出。之所以被命名为潜交换,是因为他可以实现将链上资产传递到链下的闪电网络中,就像潜水艇可以将水面上的信息传递到水面下。目前,潜交换技术已经开始逐步应用到现有的闪电网络中。Lightning Labs 开发的 Loop<sup>[9]</sup>项目支持 loop in (链上向链下转账)及 loop out (链下向链上转账)功能,该功能可以被用于单个用户自身的链上链下资金转移,也可以被用于链上用户向闪电网络中的商户支付等。除了比特币和闪电网络内部,由于潜交换技术只要求交易双方中的一方在闪电网络中,其可以被应用在跨链转账的场景,如 REDSHIFT<sup>[10]</sup>提供了可视化的利用潜交换做资产转移的服务等。



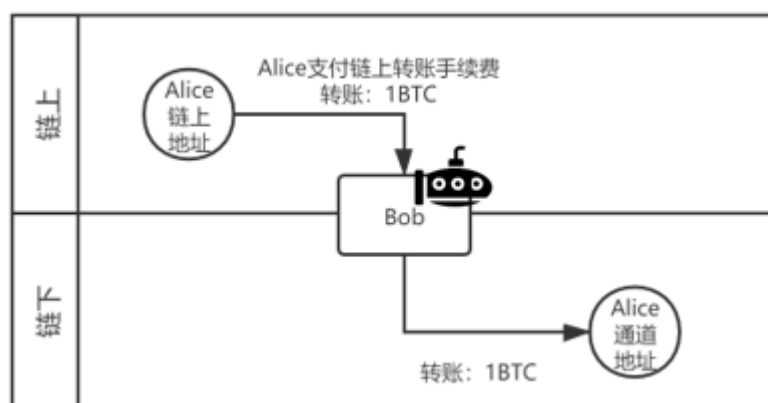
## 原理

通常，在提到潜交换时，其语义通常包含了（正）潜交换和反潜交换。（正）潜交换指用户将链上资金转移到链下的过程，反潜交换则反之。两种交换实现原理基本一致，技术上以 HTLC 为基础，应用上以潜交换服务商为核心。

具体来说，潜交换的原理与前文 2.3 中讲述 HTLC 的原理基本一致，区别在于，前文中讲述的 HTLC 技术仅应用在了链下场景，潜交换技术中，利用 HTLC，通过潜交换服务提供商，实现了链上与链下的互通。

以（正）潜交换为例，如图 20 所示，假设 Alice 希望将自己的链上资金“充值”到闪电网络通道中，Bob 是潜交换服务提供商。那么 1. Alice 自己准备好 R，并对其进行哈希计算得到 H；2. Alice 在链上与 Bob 建立 HTLC，并向其转账 1 BTC 同时告知 Bob H，Bob 需要在约定时间内提供与 H 对应的 R 才能使用这笔资金，否则资金将退回给 Alice；3. Bob 与 Alice 在闪电网络中也建立 HTLC，在这个之中，Bob 向 Alice 支付 1 BTC，同时也要求 Alice 在约定时间内提供 R。4. 当 Alice 在闪电网络中收取 1 BTC 时，就向 Bob 揭示了 R 的值，Bob 利用该 R 可以获取到链上 Alice 转账的 1 BTC。与前文所述的“正向传递 H 建立 HTLC，反向传递 R 清除 HTLC”的过程是完全一致的。只不过由于发生了链上交易，Alice 需要再支付一笔链上交易的手续费。

图20 （正）潜交换示意

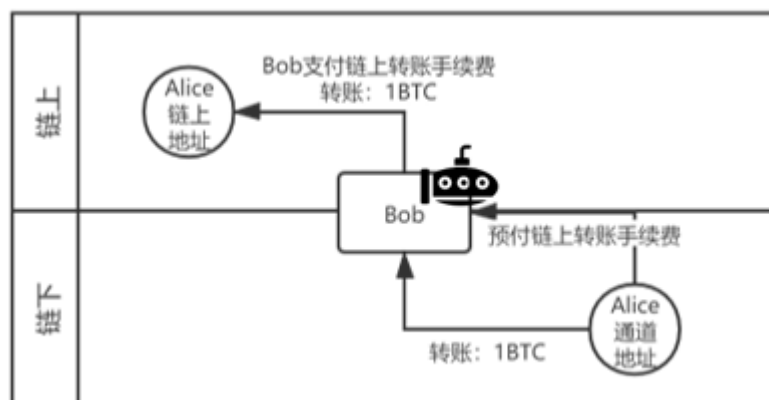


图片来源：火币研究院

反潜交换的过程与正潜交换正好相反，如图 21 所示，过程不再赘述。但值得

注意的是，在反潜交换中，由于链上交易是由 Bob 发起（Bob 向 Alice 的链上地址转账），Bob 需要支付链上交易的手续费。所以 Bob 会要求 Alice 在链下预付一笔链上交易的手续费，这笔预付款是与 Alice 实际的转账款分开支付的，即便 Alice 的潜交换转账失败或者取消，在技术上也并没有设计机制取回这笔预付款。

图21 反潜交换示意



图片来源：火币研究院

### 5.3 “化整为零” AMP

#### 背景

通道的支付上限问题也是当前闪电网络面临的重大易用性问题之一。因为非直连的用户需要经过网络中的多个节点才能完成支付，而路径上任意一个节点的通道中的余额小于支付额都会造成支付失败。闪电网络中的支付成功率会随着支付金额的上升而迅速下降。另外，同一个用户的资金可能分散在多个闪电网络节点的多个通道中，无法实现跨通道合并支付。原子多路径支付(Atomic Multi-Path Payments, AMP)技术的提出即是为了解决这两个问题。

#### 发展

原子多路径技术最早是在 2018 年由 Lightning Labs 的工程负责人 Olaoluwa Osuntokun 首次提出<sup>[11]</sup>。在 2019 年 12 月底，Blockstream 宣布该项技术已经通过互操作性测试，但还未正式上线。2020 年 5 月上旬，Lightning Labs 旗下的 LND 0.10 版本发布，支持了多路径支付<sup>[12]</sup>。可以看到，该项技术已经逐步落地到闪电

网络中。

## 原理

原子多路径支付的原理并不复杂，简单来说，就是将原本由一条路径传递的支付改由多条路径完成。其核心在于实现**原子性**、**支付哈希不可重用**、**顺序无关性**、及**无交互**<sup>[1]</sup>。

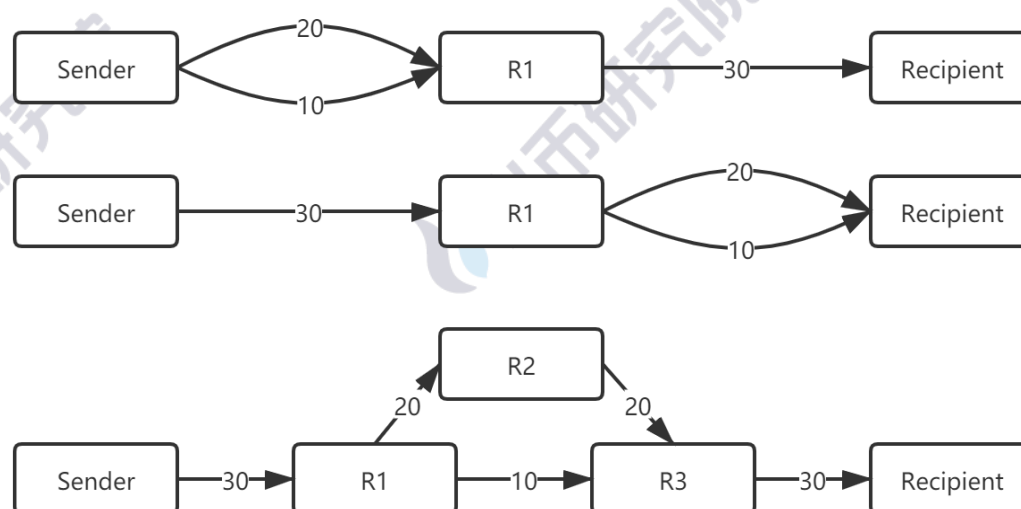
**原子性**：“原子多路径”中的“原子”，指的就是此处的原子性。它指的是，即便支付被拆解到多个路径进行传递，但最终，支付的金额是一个不可分割的原子，要么全部被支付给接受方，要么全部被退回发送方，不能存在部分支付成功的情况。

**支付哈希不可重用**：交易被拆解到多条路径支付后，每一份拆解的子交易都会有一个的哈希值。各子交易哈希值需要各不相同且相关性低，避免带来安全隐患。

**顺序无关性**：各个子交易的到达顺序不影响交易的合法性。

**无交互**：此处的无交互指的是发送者可以在不与接收者发生额外交互的情况下发起原子多路径支付，接收者对此不感知。

图22 原子多路径支付支持的多种场景



图片来源：Lightning Labs 工程组公告，火币研究院整理

如图 22 所示，为原子多路径支付支持的多种场景，包括流出流动性不足（支付节点单一通道中没有足够的资金进行支付）、流入流动性不足（接收节点的对对手节点单一通道中没有足够的资金进行支付）以及中间节点流动性不足（网络中除了交易的发送方、接受方及与其直接相连的对手节点外，其余的传输节点间单一通道内资金不足的情况）等。

#### 5.4 还有更多

除了上述三个以外，还有许多其他的扩展技术和服务用于解决闪电网络中的其他各类问题。如 Lightning Labs 提供的降低闪电网络用户的配置难度的 Autopilot；可以实现在一个用户的多个通道之间进行资金划转的再平衡 (Rebalancing)；保护隐私的同时降低带宽和存储，帮助实现轻量级闪电网络钱包客户端的中微子 (Neutrino) 协议；目前已经应用在 c-lightning 0.8.2 上的容纳更多资金的 Wumbo 通道；在同一笔交易中可以自动开启及关闭通道以完成通道资金转移的拼接 (splicing) 技术；降低用户建立通道和提取资金的操作成本的 lnurl 通道子协议技术；以 LightningTo.Me、LNBIG.com 和 Bitrefill 等为代表的闪电网络服务提供商 (LSPs) 等等。这些革新正将闪电网络和比特币带向更为大众化的方向。

## 六、总结与展望

### 6.1 未来发展

2019 年 12 月 3 日，加密数字资产交易所 Bitfinex 宣布对闪电网络上的存取款业务提供支持。可以预见在未来，更多主流的交易所、加密数字资产钱包将加入这一行列，完成对闪电网络的业务拓展。在将来的加密数字资产活动中，用户能够简单的通过交易所、钱包 APP 完成闪电网络的相关交易，从而更灵活的管理、配置个人的相关加密数字资产账户及资产。这样趋势的发生，将很大程度上扩大闪电网络的用户群体，进而进一步推动闪电网络的不断普及。

从比特币技术生态构成的角度来看，最近几年闪电网络能够成为生态中重要的基础服务之一，但不会是唯一。更有可能的情况是，形成多种扩容方案动态并存的局面。在提高比特币扩展性、降低交易手续费、优化用户支付体验方面，与闪电网络并存的解决方案（分片、跨链等）将会相互补充，共同建立面向特定应用领域的高度互补技术体系，共同解决比特币本身的局限和挑战。

另一方面，闪电网络的出现为 Layer-3 的上层金融应用和服务提供了有力的技术基础。随着结算实时性提高、交易手续费的降低，在未来，我们将可能看到面向比特币生态的去中心化金融市场（DeFi）的起步，如借贷、抵押、保险业务等，而可以预见的是，这一市场的发展将相当程度地依赖闪电网络提供底层的基础支付环境，并大幅度提升比特币资产的流动性。

### 6.2 改进方向

为了实现这一发展预期，闪电网络开发者和社区需要从技术研发和生态运营角度展开大量的工作。

#### 1) 提高网络安全系数，增强用户隐私程度

其中，从技术角度来看，闪电网络的设计和实现仍处于相对早期的阶段，未来的技术发展重心将聚焦在对于支付网络架构、安全性、隐私性、易用性等基础环节的不断优化。

对于网络架构，未来工作将主要聚焦在优化当前支付过程中的局限，主要集中在平衡支付通道负载减少中心化，提升其流动性，并提供更好的用户交易体验几个方面。



在提高闪电网络安全性保障方面，未来发展过程中需要对闪电网络的攻击面进行系统性研究，对潜在的安全风险进行建模，从而对闪电网络协议标准本身，以及不同版本的实现，都能够客观进行实用的安全威胁评估。具体来说，闪电网络协议本身当前面临包括流动性攻击、恶意Funding交易攻击(CVE-2019-12998、CVE-2019-12999、CVE-2019-13000)等。此外，从软件安全角度出发，相关闪电网络节点软件还可能遭到潜在代码级别漏洞利用、网络劫持等传统安全攻击。因此，在闪电网络快速发展的最近几年，相关的技术开发人员需要进一步将安全领域的前沿研究成果在闪电网络中进行适配和应用，保证对已知安全攻击的免疫性，同时尽早识别、发现尚未公开的潜在安全漏洞类型，保障闪电支付网络中的资产安全。从这个角度而言，闪电网络的安全性丝毫不亚于在比特币区块链中安全性问题的重要性。

在保护用户交易隐私方面，尽管闪电网络通过洋葱路由的原理进行交易支付，但由于闪电网络当前的网络规模较小，仍然可以通过大数据分析、机器学习等手段，有效推断出敏感的交易信息，如发送地址、接收地址、交易金额、路由信息等。为了解决隐私保护的问题，闪电网络的开发人员需要考虑更广泛的系统性技术手段，包括密码学方法、可信硬件等。相应的，对于闪电网络隐私保护的方案，必须能够良好兼容其固有的交易速度快、手续费低的核心优势，从而保证高实用性。

闪电网络目前还处于发展的早期阶段，技术创新奋力向前往往将用户的友好性落在了后面，但用户友好性是闪电网络迈向大众的关键一环。将技术细节掩盖在包装之下，给用户提供最直接明了的交互方式也显得越来越重要。

## 2) 打造开放社区，丰富应用生态

为了进一步推动闪电网络在未来的发展，其生态运营人员需要一方面**打造更加开放、活跃的开发者社区**，并与传统开源软件社区进行有效整合，从而形成更为积极的开发、研究开放群体，不断推动闪电网络标准和实现向前发展。

另一方面，也需要从应用场景的角度进行扩展，积极探索在**主流金融行业、企业中的实际应用**。这一过程不但能够扩大闪电网络的影响力，更重要的是能够利用现实业务场景的需求，不断明确闪电网络的技术发展方向，从而形成整个技术生态中的良性循环。

当然，闪电网络的进一步发展，也离不开和其他主流加密数字资产市场（如以太坊等）的开放性互动，展现闪电网络对于互操作性、跨链交易交换方面的优越性，从而增强在加密数字资产行业中的生命力。

随着闪电网络在技术研发、生态社区运营两个维度上的共同发展，未来的区块世界将在商业应用上具有更强、更丰富的扩展性方案。当然，区块链整体行业当前面临着走向主流场景的重大使命，包括如何解决在社会、经济、民生领域的落地难题。典型的主流应用包括，全球基础金融设施、电子政务、智慧医疗、数字身份等等。完成区块链行业的整体高速发展，需要包括技术、政策、法律等多领域的协同合作。随着比特币等加密数字资产在社会经济活动中不断普及，闪电网络作为比特币技术的重要补充有可能成为个人金融业务、零售行业的重要支付工具得以应用。

## 参考文献

- [1] Lin J H, Primicerio K, Squartini T, et al. Lightning Network: a second path towards centralisation of the Bitcoin economy[J]. arXiv preprint arXiv:2002.02819,
- [2] Mizrahi A, Zohar A. Congestion Attacks in Payment Channel Networks[J]. arXiv preprint arXiv:2002.06564, 2020.
- [3] Béres, Ferenc, Istvan Andras Seres, and András A. Benczúr. "A cryptoeconomic traffic analysis of bitcoins lightning network." arXiv preprint arXiv:1911.09432 (2019).
- [4] McCorry P, Bakshi S, Bentov I, et al. Pisa: Arbitration outsourcing for state channels[C]//Proceedings of the 1st ACM Conference on Advances in Financial Technologies. 2019: 16-30.
- [5] Avarikioti G, Laufenberg F, Sliwinski J, et al. Towards secure and efficient payment channels[J]. arXiv preprint arXiv:1811.12740, 2018.
- [6] Avarikioti G, Litos O S T, Wattenhofer R. Cerberus channels: Incentivizing watchtowers for bitcoin[J]. Financial Cryptography and Data Security (FC), 2020.
- [7] Lightning Labs 团队将瞭望塔集成至闪电网络中：  
<https://github.com/lightningnetwork/lnd/releases/tag/v0.7.0-beta-rc3>
- [8] BitMEX 全面采用瞭望塔功能：[https://blog.bitmex.com/zh\\_cn-lightning-network-part-4-all-adopt-the-watchtower/](https://blog.bitmex.com/zh_cn-lightning-network-part-4-all-adopt-the-watchtower/)
- [9] Loop：<https://github.com/lightninglabs/loop>
- [10] REDSHIFT：<https://ion.radar.tech/redshift>
- [11] Olaoluwa O. AMP: Atomic Multi-Path Payments over Lightning.  
<https://lists.linuxfoundation.org/pipermail/lightning-dev/2018-February/000993.html>
- [12] Lightning Labs 团队将多路径支付集成至闪电网络中：  
<https://github.com/lightningnetwork/lnd/pull/3967>

## 关于火币研究院

火币区块链应用研究院（简称“火币研究院”）成立于2016年4月，于2018年3月起致力于全面拓展区块链各领域的研究与探索，以泛区块链领域为研究对象，以加速区块链技术研究开发、推动区块链行业应用落地、促进区块链行业生态优化为研究目标，主要研究内容包括区块链领域的行业趋势、技术路径、应用创新、模式探索等。本着公益、严谨、创新的原则，火币研究院将通过多种形式与政府、企业、高校等机构开展广泛而深入的合作，搭建涵盖区块链完整产业链的研究平台，为区块链产业人士提供坚实的理论基础与趋势判断，推动整个区块链行业的健康、可持续发展。

### 联系我们：

咨询邮箱：[huobiresearch@huobi.com](mailto:huobiresearch@huobi.com)

官方网站：<https://research.huobi.cn>

微信公众号：HuobiCN

新浪微博：火币区块链研究院

<https://www.weibo.com/u/6690456123>

Twitter：Huobi\_Research

[https://twitter.com/Huobi\\_Research](https://twitter.com/Huobi_Research)

Medium：Huobi Research

<https://medium.com/@huobiresearch>

欢迎加入研究院学习交流小组



扫码添加学习小助手微信

## 免责声明

1. 火币区块链研究院与本报告中所涉及的项目或其他第三方不存在任何影响报告客观性、独立性、公正性的关联关系。
2. 本报告所引用的资料及数据均来自合规渠道，资料及数据的出处皆被火币区块链研究院认为可靠，且已对其真实性、准确性及完整性进行了必要的核查，但火币区块链研究院不对其真实性、准确性或完整性做出任何保证。
3. 报告的内容仅供参考，报告中的结论和观点不构成相关数字资产的任何投资建议。火币区块链研究院不对因使用本报告内容而导致的损失承担任何责任，除非法律法规有明确规定。读者不应仅依据本报告作出投资决策，也不应依据本报告丧失独立判断的能力。
4. 本报告所载资料、意见及推测仅反映研究人员于定稿本报告当日的判断，未来基于行业变化和数据信息的更新，存在观点与判断更新的可能性。
5. 本报告版权仅为火币区块链研究院所有，如需引用本报告内容，请注明出处。如需大幅引用请事先告知，并在允许的范围内使用。在任何情况下不得对本报告进行任何有悖原意的引用、删节和修改。