闪电网络是比特币的第 2 层协议，专为廉价、快速和私密的支付而设计。作为一个由支付通道组成的覆盖网络，闪电支付并未记录在比特币的区块链上——只有通道资金交易和通道关闭交易记录在案。这实际上意味着许多闪电交易可以用更少的链上比特币交易来结算。

有关构建闪电网络的网络的更多信息，请访问我们的“什么是比特币？” 指导。

通过将许多闪电交易结算为更少的比特币交易，比特币网络上的用户和矿工不必验证和存储所有这些闪电交易。这也许是主要的好处，这意味着闪电网络用户的费用较低。此外，闪电网络用户不再需要等待比特币区块链上的确认：交易是即时的。

最后，作为一个额外的好处，交易没有记录在区块链上（结合用于闪电支付的类似 Tor 的路由算法）这一事实意味着闪电用户通常享有一些额外的隐私。

要了解有关闪电网络如何工作的更多信息，请访问我们的独立指南。

谁创建了闪电网络？

闪电网络最早于 2015 年在由 Joseph Poon 和 Thaddeus Dryja 撰写的闪电网络白皮书（全称：《比特币闪电网络：可扩展的链下即时支付》）中被提出。闪电网络的各个设计方面的历史甚至比白皮书还要早。

从那时起，几个团队开发了不同的闪电网络实现，包括 Blockstream 的 c-lightning、Lightning Labs 的 lnd 和 Acinq 的 Eclair。所有实现都通过 BOLT 协议规范兼容。

闪电网络每天都在改进；这是一项正在进行的工作。

有关闪电网络创建的更多信息，请阅读我们的文章“闪电的历史：从头脑风暴到 Beta”

什么是周六？

Sats，或“satoshis”，是记录在比特币区块链上的最小比特币面额。一个 sat 代表 0.00000001 BTC，或 1
个比特币的亿分之一。这个名字取自比特币的匿名创造者中本聪。

有关中本聪的更多信息，请阅读我们关于比特币创造者的指南。

由于比特币的价值已经上升到仅 BTC
的一小部分就足以支付许多商品和服务、定期投资和微任务支付，因此 BTC
通常以 sats 计价。使用 sats 还可以让用户进行价值低于 1 美分的交易。

社交媒体上使用#StackingSats
标签来指代聪的习惯性累积。像Carrot这样的赚钱平台会在 sat
中为完成任务支付奖励。

有关 sats 的更多信息，请访问我们的独立指南。

闪电网络费用如何运作？

在比特币上，向矿工支付费用以将交易包含在一个区块中。但是闪电网络本身没有矿工，也没有区块。（当然，作为第 2 层解决方案，它最终确实依赖于矿工和区块；没有矿工和区块，就不会有比特币，因此也就没有闪电网络。）

相反，费用会支付给网络上的闪电节点，这些节点负责提供流动性（资金渠道）和转发交易。有些节点会比其他节点收取更高的费用，但费用通常很低，并且由于任何人都可以建立竞争节点，因此竞争可能会使费用保持在相当低的水平。

支付费用通常在钱包中抽象出来，而不是你需要担心太多的事情。与链上交易不同，不存在包含过低费用的风险——您的交易要么立即通过，要么根本不通过。

如果你想自己赚取费用，你将不得不设置一个闪电节点，理想情况下是与闪电网络上的许多其他节点连接良好，并且在不同渠道具有大量流动性的节点。它还有助于使该节点尽可能在线。

如何设置闪电网络节点

与比特币节点一样，闪电网络节点是连接到网络以通过闪电从其他节点发送和接收 BTC 的软件。本质上，闪电网络就是由这些节点组成的。

要真正参与闪电网络，用户应该考虑运行自己的节点。您不必运行节点即可通过闪电网络通道发送 BTC，但运行您自己的节点有助于网络发展、增加流动性并可能帮助您获利（如下所述）。

要了解有关设置闪电网络节点的更多信息，请查看我们的完整指南。

要了解如何通过运行闪电网络节点获利，请访问我们的节点盈利指南。

什么是闪电网络钱包？

比特币钱包是允许用户发送和接收比特币的程序或应用程序。支持闪电网络的比特币钱包允许用户进行和接收闪电支付。

要阅读有关比特币钱包的更多信息，请访问我们的完整指南。

与一般的比特币钱包一样，有不同版本的支持闪电网络的钱包，每个版本都有自己独特的属性和权衡。例如，桌面闪电钱包可能是某些人的首选，因为他们希望经常查看他们的频道。但闪电网络的设计初衷是为了方便相对较小的 BTC 交易，许多用户并不强调全节点的安全性。对于许多人来说，移动闪电钱包是首选，尽管很难在移动设备上托管完整节点，因为它们最方便。

如何设置闪电通道？

要设置 Lightning 通道，您需要运行 Lightning 节点或拥有 Lightning 钱包。热门选项包括c-lightning和lnd（节点）以及Eclair、Zap和Lightning App（钱包）。设置完成后，您可以通过与该节点对应的唯一代码与另一个闪电网络节点或钱包建立支付通道。一种解决方案与另一种解决方案的具体实现方式略有不同。

设置完成后，只要渠道资金允许，您就可以通过渠道和网络的其余部分进行交易。根据您的设置，您还可以为其他用户转发交易并可能赚取费用。

我可以在不开通自己的频道的情况下发送或接收闪电支付吗？

严格来说，您需要至少开通一个支付通道才能发送或接收闪电支付。也就是说，如果出于某种原因你不想打开 Lightning 通道（还），有一些方法可以解决它。

例如，一些闪电钱包——比如Blue Wallet——提供托管解决方案。这实质上意味着当用户收到付款时，实际上是钱包背后的运营团队代表他们收到了付款。钱包用户可以提取资金，但在此之前它真正由 Blue Wallet 团队控制。这样做的好处是用户可以立即开始接受付款，但也有明显的缺点，即用户必须信任钱包团队，让他们在选择时提取资金。

或者，像Submarine Swaps这样的服务可以让用户在不打开 Lightning 通道的情况下进行支付。相反，用户向该服务发送常规的链上交易，然后该服务将付款作为闪电支付转发给预期的收件人。虽然这些类型的支付可能是无信任的——这意味着服务提供商不能放弃转发支付——但这确实意味着用户需要支付链上费用和额外的服务费用

什么是 WUMBO？

Wumbo 是一个 Lightning 实现，旨在消除闪电通道中可以持有的 BTC 数量限制（最初限制为 0.16777215 BTC）和个人支付的上限。这些限制最初是由于与闪电网络相关的风险而制定的，当时它是一项全新且相对未经测试的技术。对于通过 wumbo 规避上限的支付渠道，双方的用户必须表达他们的愿望。

该开发项目以卡通海绵宝宝的一集中创造的术语命名，其中角色 Patrick Star 通过在一系列示例中使用它来定义“wumbo”这个词：“我 wumbo，你 wumbo，他，她，我：wumbo，”他说。

在 2018 年 11 月的一次峰会上，这个词被用于 Lightning 开发，似乎是因为这句话暗示了协议要求超过原始渠道和支付上限的双方同意类型。然而，根据峰会的规则，不允许将本次峰会的直接引述和想法与特定个人联系起来，以鼓励思想的自由交流。

“如果新通道的双方同意通过设置 'option_i_wumbo_you_wumbo' 来互相 wumbo，他们可以建立容量高于 167.77216mBTC 的通道，”正如 Lightning 开发人员 ZmnSCPxj 当时向 Lightning Dev 邮件列表解释的那样。“宣传‘option_wumborama’的节点允许任何节点建立容量超过限制的通道。请责怪参加[第二届闪电网络发展峰会]的其中一位人士。”

Eclair 和 c-lightning 客户在 2020 年初采用了 wumbo 支持，LND 于 2020 年 8 月开始支持 wumbo 频道。

闪电网络如何扩容比特币？

正如网络白皮书所说，闪电网络最初是作为解决“比特币区块链可扩展性问题”的解决方案提出的。正如作者所描述的，比特币无法有效地充当世界支付平台，因为它向所有网络参与者广播所有交易。

“如果比特币网络中的每个节点都必须了解全球发生的每一笔交易，这可能会对网

络涵盖所有全球金融交易的能力产生重大拖累，”白皮书称。“相反，希望以一种不牺牲网络提供的去中心化和安全性的方式包含所有交易。”

正如作者继续指出的那样，像 Visa 这样的传统支付网络每秒可以管理 47,000 笔交易，而比特币每秒支持不到 7 笔交易，其 1 MB 的块限制。他们针对这个扩展问题提出的解决方案是闪电网络，这是一种第二层协议，允许用户与 BTC 进行交易，同时仅在渠道获得资助或关闭时将这些交易记录在比特币区块链上。

要阅读有关使用闪电网络扩展比特币的更多信息，请访问我们的独立指南。

闪电网络有哪些风险？

虽然闪电网络为比特币提供了巨大的扩展潜力，并成为世界传统支付系统的替代品，但它仍然是一项相对较新的技术，采用率较低。大规模采用闪电网络可能带来的所有风险可能尚未确定。而且，即使在这个初期阶段，承认该技术的一些缺点也很重要。

由于闪电网络的运营节点相对较少，因此资金可能会集中在某些节点上——这种情况会带来比特币网络不应该发生的集中风险。如果一个资金高度集中的节点试图同时欺骗许多用户，可能会对网络造成严重破坏。

此外，如上所述，这些交易相对较慢，因为它们作为比特币公共和去中心化分类账的一个特征在整个网络中传播。从本质上讲，闪电网络通过允许在未广播到整个网络的通道内进行交易来提高速度，这本身就是一种安全权衡。这为这些渠道中的不良行为者提供了潜在的机会。

“假设 Molly 和 Angela 有一个频道，他们每人存入 10,000 sats，总共 20,000 sats，”根据比特币杂志描述的场景 2019 年。“在频道的生命周期中，安吉拉向莫莉支付了 5,000 坐席，使莫莉的总数达到 15,000 坐席，安吉拉支付了 5,000 坐席。但是突然间，不知出于什么原因，Molly 无法访问她的闪电网络钱包（可能是她的节点离线，她的电脑出现故障或者她正在度假），所以 Angela 决定调皮捣蛋——到了播出决赛的时候将通道的状态发送到区块链，她决定广播通道的第一个状态（他们都存入的原始 10,000 sat 余额）以骗取 Molly 的报酬。由于 Molly 在墨西哥湾的一个偏远岛屿上，而不是在她的电脑前，她无法检查 Angela 的不良行为并验证频道的实际状态，因此她失去了 5,000 sat。”

什么是闪电网络瞭望塔？

为了减轻这种风险，闪电网络开发人员引入了一种称为“瞭望塔”的技术功能来监控通道。

当频道更新时，包含与用户公钥相对应的秘密签名的加密“blob”被发送到瞭望塔。同时，watchtower 收到通道先前状态的交易 ID 的一半，用作 blob 的解密密钥。瞭望塔存储这些 blob 和解密密钥，这样如果坏人试图向 mempool 广播一个较旧的通道状态，它就可以识别出交易 ID 与它持有的另一个交易 ID 的一半相匹配。有了两半的交易 ID，了望塔可以解密相应的 blob，然后拒绝坏人并将资金发送到诚实通道用户的钱包。

在我们的文章中阅读更多关于闪电网络瞭望塔的信息。

闪电网络上有多少比特币？

在任何给定时间闪电网络通道内持有的 BTC 的确切数量很难估计。正如BitMEX Research在其关于闪电网络的 2020 系列文章中所解释的那样，可以通过区块链数据以不同方式识别不同类型的交易，并且并非所有交易都非常明确地归因于闪电网络。

总结其报告的一部分，可以通过公共区块链数据分析三种闪电网络交易类型：开通通道、“合作”通道关闭和“非合作”通道关闭。当闪电网络节点启动支付通道关闭而不直接与通道链接的节点通信时，就会发生“非合作”闪电通道关闭。同时，“合作”通道关闭意味着两个通道参与者都同意关闭通道并将通道的最终状态结算到区块链上。