

比特币闪电网络正变得越来越流行。闪电的普及正在进行：闪电网络中现在有 4,800 多个比特币，价值超过 9,000 万美元。此外，围绕闪电网络的机构活动有所增加。例如，闪电协议的主要贡献者闪电实验室在今年早些时候获得了 7,000 万美元的 B 轮融资。提供闪电网络相关服务的公司数量也正在迅速增加。

本文将阐述：为什么需要闪电网络，以及如何使用？

比特币作为全球支付系统？

比特币作为去中心化支付系统提供了许多优势，它可以在没有中介的情况下在全球范围内转移资金。

其中最重要的是参与者的低门槛：世界上任何拥有互联网设备的人都可以使用比特币，没有人可以被排除在外，这对金融包容性产生了积极影响。而且，比特币代表了一种稀缺的数字资产，一种“数字黄金”。每个比特币可以分成 1 亿聪，就像你可以将 1 美元分成 100 美分一样。与法定货币不同，比特币的供应量上限在 2,100 万枚。因此，通过稀释比特币贬值是不可能的。

尽管有这些优点，但比特币网络的当前状态也有局限性。网络的去中心化是以牺牲交易吞吐量为代价的，吞吐量即网络每秒可以执行的交易数量。目前，比特币网络每秒最多可以确认七笔交易。

作为支付系统，这种低交易吞吐量是不够的。成熟的支付服务提供商，如 Visa 或 Mastercard，每秒可实现数千笔交易，因此可扩展性更好——即使是完全中心化的。比特币网络上的交易通常需要更长的时间才能被确认，因此不适合日常支付交易。

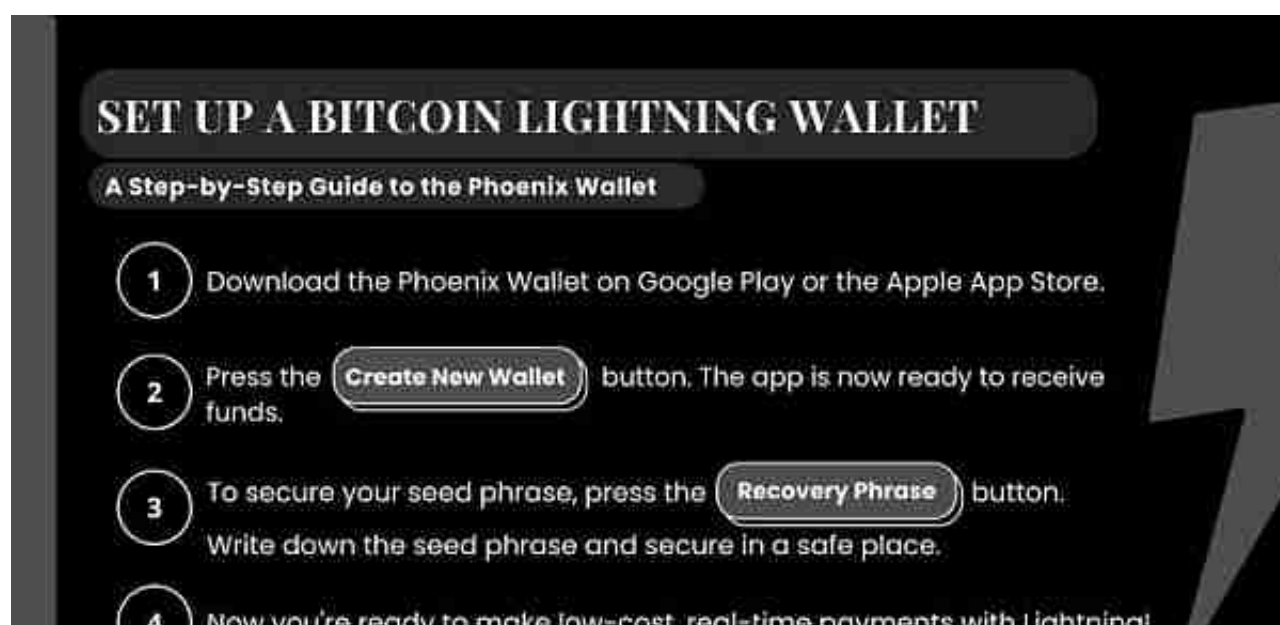
另一个限制是通过比特币进行小额支付。因为每笔交易都会根据其存储大小产生费用。使用的存储空间越多，支付的费用就越高。平均而言，今天的交易，无论交易额如何，成本约为 1 美元。在需求增加的时候，比如 2017 年，交易费用达到了 60 美元以上的峰值。对于大额付款，交易费用似乎相对便宜；然而，对于小额支付来说，成本有些过于昂贵了。

闪电网络可以解决这一缺陷

开发闪电网络的目标是让比特币作为可以日常使用的支付手段。目标是在不中心化的情况下提高吞吐量，这是成为合格的支付网络的基础。更具体地说，这意味着用户可以用更便宜的价格、更快的速度支付更多款项。虽然比特币的白皮书早在

2008 年就由中本聪发布，但闪电网络的构想可以追溯到 2015 年，第一次开发始于 2016 年。2018 年，第一批用户开始使用闪电网络。从那时起，该技术迅速发展。然而，尽管交易量很大，并且最近在采用方面取得了进展，但它在 2022 年仍处于起步阶段。

闪电网络如何解决交易吞吐量低、交易费用相对较高的问题？那就是并非所有交易都写入区块链（即“链上”）。大多数付款都是在“链下”相互支付的，只有在极端情况下或两个网络参与者之间的支付关系终止时，它们才会写入区块链（“结算”）。因此，用户的付款可以实时且低成本地处理。通过闪电网络转账的用户无需等待比特币网络的确认，付款将会即时处理。



2. 将资金存入钱包

下一步是将资金存入闪电钱包。因此，你需要将比特币从自托管比特币钱包或你在托管服务提供商（如 Coinbase 和 Binance）的账户转移到闪电网络钱包。你所要做的就是输入闪电网络接收地址，并通过使用私钥签名来授权付款。

出于安全原因，你应该等待比特币区块链的多次确认（通常是 6 次确认，大约需要 60 分钟），以确保存款的最终结算。

3. 开通支付通道

接下来，你需要与你的交易伙伴开通支付渠道。例如，如果你想用闪电网络支付咖啡，你可以在咖啡馆打开一个支付通道。

在打开支付通道的过程中，你的资金被存入支付通道。存入的资金可用于在支付渠道内的支付。

4. 开始支付

资金存入后，可以在支付通道内相互进行交易。为此，咖啡馆可以开具闪电网络发票（二维码的形式），通过钱包（例如上面提到的 Phoenix 钱包）进行扫描。之后，你只需在钱包中确认付款即可。

总结

设置闪电网络钱包只需几分钟；闪电网络钱包和支付通道的初始存款平均每个大约需要一个小时。一旦钱包和支付通道中的比特币资产可用，就可以通过闪电彼此实时进行支付。如此一来，闪电网络的主要优势就会充分显现：以低交易费用进行快速支付。当你想进行小额支付（例如，一杯咖啡）时，这一点尤其重要。

在实践中，你不需要为你最喜欢的每一家咖啡店打开支付通道。闪电钱包并不是打开新通道，而是通过可用通道将资金路由到所需的目的地。路由取决于通道容量以及流动性的分布。为了确保大量成功支付和可靠性，参与者不应将路由费用最低化。所谓的“自私路由策略”会消耗通道容量，最终可能导致闪电网络可以处理的支付数量减少。

风险提示：

根据央行等部门发布的《关于进一步防范和处置虚拟货币交易炒作风险的通知》，本文内容仅用于信息分享，不对任何经营与投资行为进行推广与背书，请读者严格遵守所在地区法律法规，不参与任何非法金融行为。