改善比特币隐私保护的主要途径之一，是通过升级该区块链网络的 底层
。比特币网络已经趋于保守，通常回避与传统版本不兼容的、修改共识的硬分叉。但是，向后兼容软分叉进行的升级，仍然允许传统节点验证区块链的有效性，这种做法通常是被接受的。

这意味着通过软分叉升级网络是一项艰巨的任务。升级被拒绝的原因有很多，例如与比特币的 核心愿景
、与软件的现有组件存在技术冲突等等。从构思到实施，即使是成功的分叉也可能需要数年时间才能完成。

底层升级

尽管比特币区块链网络升级可能难度较高，依然有几个升级隐私保护的途径值得探讨。一个颇具潜力的升级方案是 Dandelion++（意为蒲公英）
，它修改了比特币交易的路由方式。

当前，未经确认的比特币交易通过传播扩散来广而告之，在这种传播中，节点以随机的、指数级延迟的速率向其对等节点连续广播其中的交易。由于比特币用户的 IP 地址暴露于网络中，因此攻击者可以推断出发送交易的 IP
地址，攻击者最终可以将 IP 地址与比特币地址相关联，实际上破解用户的匿名。

DandeLion++
提议使用另一种传播方法代替扩散传播，在新的传播方法中，交易首先在
主干阶段（stem phase）依次传递给各个对等节点，然后在绒毛阶段（fluff phase）进行扩散传播。由于每个节点在主干阶段仅与一个对等节点共享交易，并且主干的长度是随机确定，因此交易对方很难确定交易的来源。

CT 不仅仅是存在于理论中的构造，还被包括 Monero和Grin
在内的多种替代币所采用。在 Monero 中，CT 与环签名（Ring Signature）
结合使用，ringsignatures
模糊了交易签名者
，向观察者隐藏交易规模和发送者。由此产生的交易比比特币交易要大得多，但理论上的隐私保障要好很多。除了占用更大区块空间之外，CT
还有一个更实质性的问题，使它们与比特币的基本构想相互抵触。CT
使对区块链的审查变得困难，并且 CT
实施中的错误可能导致通货膨胀漏洞，让个人可以偷偷地让货币供应量膨胀。

这些漏洞将很难检测，并且会损害区块链的 诚信度
。比特币社区中的许多人对这种可能性深感担忧，包括人权基金会首席战略官 CSO Alex
Gladstein，他认为
「尽可能优先考虑隐私是非常重要的。
当然可审核性
在这个问题上是绊脚石。我们不能在比特币区块链拥有一个完整节点无法审计其货币供应量的系统，毕竟这一审计对于比特币系统的价值至关重要，」

「否则这不是货币创新，而只是技术创新。归根结底不会真正有用，」Gladstein 补充说。

因此，CT 在不久的将来似乎 不太可能被纳入比特币区块链中。

出于类似的意识形态或实际原因，其他针对比特币底层的多个提议升级也已停止。但是其中一些更改可以
在侧链上实现，侧链为解决比特币底层更新的障碍提供了一种大有可为的方式。

侧链

侧链是与基础链 （ 例如比特币区块链 ） 平行运转并从中获得安全性的区块链。

Liquid
是当今最引人注目的侧链之一，它使用联邦安全模式
。在该模式中，用户通过将主链资金存入由联邦成员控制的合同中，从而在侧链上获得资金。一旦用户在侧链上控制了资金，他们就可以自由地在该链上进行交易，而无需在基础链上进行交易确认。用户可以在侧链上焚毁其资产，以将资金返还给主链。

就目前而言，闪电网络可以显著改善用户的隐私保护。闪电网络允许用户
批量结算交易
，不再需要向观察者透露单笔交易的详细信息。此外，目前已经提出了针对闪电网

络的几种升级方案，目的是进一步改善闪电网络提供的隐私利益，而这些都不需要更改比特币底层的行为。

闪电网络经中介通道路由付款，使观察员很难确定两方是否已进行交易。闪电网络最令人激动的潜在升级之一是 蚁群路由
的实现，这将改变闪电网络计算付款路由的方式。闪电网络当前使用最短路径路由，这要求节点跟踪全球路由表。这种方法的扩容性很差，并且使对手可以学习其网络拓扑，因此可以战略性地放置节点以实现监视流量的最佳效果。蚁群路由建议用完全分布式、可高效扩容、并且对图学习攻击具有鲁棒性的路由机制，取代当前的路由机制。

另一项功能则是
原子多路径支付
AMP，使用户可以拆分支付，并通过几个通道完成支付。这些付款将以原子方式执行，无论是成功还是失败，都不会部分收到付款。AMP 使支付路径上的中介机构更难确定支付的总金额，这将改善该网络中的隐私。此外，AMP
支持在非流动性通道上进行大笔支付，将增加可用流动性。

蚁群路由和 AMP 的主要目的分别是 扩大规模和流动性
，并随之为隐私保护带来次级好处。另一方面，Bolt Labs
目前正在开发的zkChannels
是一项在设计时明确考虑隐私的功能。这些通道使用高级加密技术，允许用户在收款人不知道原始发件人身份的情况下发送付款，前提是付款已通过至少一个中介进行路由。这种类似于现金的功能可用于在不需要透露个人身份
的情况下进行谨慎的付款。