Galaxy：比特币 L1 是数据可用性层吗？

作者：Gabe Parker，Galaxy；编译：五铢，本站

## 前言

比特币的区块空间极其稀缺，每个区块的大小上限为 4MB。这种稀缺性对寻求利用比特币作为数据可用性层的 Rollups 提出了重大挑战。基于比特币的新兴 Rollups 格局主要基于 ZK，旨在每 6-8 个区块发布一次 ZK 证明输出和状态差异。然而，这种方法面临一个关键障碍；每个数据发布最多消耗 400KB（0.4MB）的区块空间，实际上占据了整个区块的 10%。

鉴于比特币自 2023 年 1 月以来一直处于满负荷状态，多个 Rollups 之间对区块纳入的竞争将加剧，可能会使比特币的交易费市场紧张到不可持续的水平。比特币基础层的当前限制，加上正在开发的 Rollups 的激增，可能会创造一个 L2 难以负担数据发布的环境。为了保持可行性，比特币上的 Rollups 将需要通过有用的应用程序从交易费中获得可观的收入。本报告通过研究以太坊 ZK-Rollups 的数据并预测使用比特币进行 Rollups 的成本（以实现数据可用性），分析了 Rollups 在比特币上的经济可行性。该分析探讨了这些项目在主网上启动后对比特币区块构成的潜在影响，并讨论了如果将数据发布到比特币的成本过高，Rollups 可能采用的替代策略。

## 比特币 L1 是数据可用性层吗？

将数据发布到基础层的比特币 Rollups 将面临一个重大问题：发布数据的成本。比特币区块空间是所有链中每字节最昂贵的。此外，比特币的区块大小被严格限制在 4MB，费用与交易的数据权重挂钩，这使得任何数据密集型交易的执行成本都很高。序数（附在单个 Satoshi 上的铭文）的出现突显出，占据区块大小很大一部分的交易需要支付额外费用并推高交易费用。例如，Taproot Wizards 团队（区块 774,628）铭刻的第一笔 4MB 比特币交易的费用为 14.7 万美元。

根据与在比特币上构建 ZK-Rollups 的几个团队的对话，Rollups 预计每 6-8 个区块（1 小时 - 1.2 小时）将 ZK-Proof 输出和状态差异以铭文的形式发布到比特币 L1，铭文是存储在交易隔离见证部分中的任意数据。这些数据将使任何运行比特币节点的参与者能够重建 Rollup 的最新状态。根据测试网和与开发人员的对话，我们估计，每次将证明输出和状态差异发布到比特币的第 1 层区块链时，最多需要 400KB (0.4MB)。

当将比特币与以太坊和 Celestia 每秒处理的兆字节数进行比较时，很明显比特币从未被设计为 DA 层。



## 验证证明的成本 – 以太坊 ZK-Rollups

从以太坊的 Rollup 生态系统中汲取经验，ZK-Rollups 因使用有效性证明而成为资本密集型运营。这种方法要求证明者发布 ZK-Proof 以及每次 L2 状态更改的交易数据或状态差异。与仅在发生欺诈纠纷（罕见发生）时支付验证成本的 Optimistic Rollup 扩展解决方案不同，ZK-Rollups 通过发布有效性证明预先支付验证成本。ZK Rollup 的前期成本较高，可实现即时终结（而 Optimistic Rollup 的挑战窗口约为 7 天）。下面的图表显示了以太坊上 ZK-Rollups 的每周数据发布成本。



ZK-Rollups 通过 L2 交易费收入来支付数据发布费用。自推出以来，ZK-Sync Era 已证明该模式的可行性，从 L2 交易费中获得了 6690 万美元的总收入。其中 5120 万美元用于 ZK 验证和 L1 呼叫数据成本。ZK-Sync 已成功为 540 万用户处理了超过 4.176 亿笔交易，平均每笔交易成本为 0.16 美元。这种高效的运营带来了 1570 万美元的总利润。

## 估算将数据发布到比特币的成本

在比特币 L1 上，每 6 个区块发布一次数据，费用为 400KB，费用低至 10 sat/vByte，比特币上的 Rollups 将为每个发布的区块支付 2,640 美元。每 6 个区块发布一次数据，比特币上的 Rollups 将每月支付高达 190 万美元，以发布到 730 个区块（每年 2300 万美元）。使用 50 sat/vByte 级别将使每月数据发布成本增加到近 960 万美元（每年 1.15 亿美元）。需要注意的是，由于随着 Ordinals、BRC-20s 和 Runes 的出现，比特币的费率环境现在变得越来越不稳定，因此估计未来的 sat/vByte 水平极其困难。

为了抵消在每个帖子为 400KB 的世界中发布数据的高成本，使用比特币提供数据的 ZK-Rollups 每月需要从 L2 交易费中产生约 190 万美元至 963 万美元的收入。下面的敏感度表估算了比特币 Rollup 在扣除数据发布成本后实现收支平衡所需的交易活动和费率水平。我们的模型预测，截至 2024 年 7 月 23 日，Rollup 每 6 个区块向比特币 L1 发布 400KB 数据的每周成本为 10、20 和 50 sats/vByte。如果比特币 Rollup 每月处理 2000 万笔交易（与 ZK-Sync 过去一年的每周交易量相当），则需要收取 0.096 美元、0.193 美元和 0.482 美元的交易费才能在 10、20 和 50 sats/vByte 的水平上实现收支平衡。需要注意的是，由于测试网上缺乏可用数据，此敏感度表假设 400KB 数据发布大小固定在每月 100 万至 8000 万笔交易之间。我们理解，根据状态差异中包含的交易数量，数据发布大小可能大于或小于 400KB。



无法提供足够交易费来支付数据发布成本的 Rollup 将需要动用其金库来支付 L1 交易费，并可能最终被迫不再使用比特币作为 DA 层。其他选择包括在更具成本效益的 DA 层（如 Celestia、Near 或 Syscoin）上发布 ZK 证明和状态差异。但是，使用比特币以外的其他东西作为 DA 层会降低该层自称为“比特币 Rollup”的能力。如果第 2 层网络不汇总到比特币，它是否仍被视为比特币 Rollup，还是会转变为替代 DA 网络的 Validium 链？对于难以支付成本的 Rollup，另一个潜在的解决方案是重组为第 3 层解决方案。在这种情况下，Rollup 会将状态差异发布到第 2 层或侧链，而只有 merkle 根哈希会发布到第 1 层。这种方法可以显著降低数据发布成本，同时保持与比特币网络的连接。

## Rollups 启动时的比特币区块空间

自 2023 年初出现 Ordinals 和 BRC-20 以来，比特币的每日平均区块重量一直略低于其 4m 重量单位限制（4MB 数据）。区块重量是区块“大小”的无量纲测量，在 SegWit 升级中引入，以包含折扣见证数据。由于大量铭文相关交易的涌入，每日平均区块重量显著增加，其中包括交易隔离见证字段中的任意数据（文本、图像等）。自 2023 年 2 月以来，比特币区块的平均饱满度为 98%。



如果每个证明输出和状态差异总计为 400k 重量单位，则如果 Rollup 的数据大小保持一致，则单个 Rollup 将数据发布到区块，这将占用区块重量限制的 10%。鉴于区块始终处于满负荷状态，引入 Rollup 将改变每个数据发布区块内交易数据的组成。下图展示了 2024 年 7 月 18 日 30 个区块样本的区块组成，假设两个 Rollup 处于活动状态，并且每 6 个区块发布一次数据。



Rollups 每 6-8 个区块在比特币 L1 上发布一次数据，对区块空间的持续需求将迫使时间敏感型交易在数据发布区块之前或期间支付溢价。下图强调了 Runes 和 Ordinals 链上活动竞争加剧如何迫使时间敏感型交易（也称为金融交易）支付最高的费率溢价。



## 为什么比特币 DA 很重要

为了使 Rollup 与比特币完全一致，它必须利用比特币来实现数据可用性。这种选择虽然成本高昂，但却充分利用了比特币无与伦比的安全性、不变性和去中心化。选择替代 DA 解决方案的 Rollup 会在比特币网络之外引入额外的信任假设，可能会损害其完整性和“比特币 Rollup”的分类。比特币作为 DA 层的优势不仅在于其强大的安全性，还在于其广泛的节点分布和设置轻节点或完整节点的低门槛。这种可访问性确保任何运行比特币完整节点的人都可以重建 Rollup 的最新 L2 状态，从而增强透明度和去中心化。

尽管费用高昂且存在潜在的长期可行性挑战，但比特币作为 Rollup 的原始 DA 层的角色凸显了一个基本的权衡：利用比特币基础设施的高成本与其提供的无与伦比的安全性和去中心化。成本和安全性之间的这种平衡可能会塑造比特币网络上 Rollup 实施的未来格局。

## 使用比特币进行 DA 的 Rollups 展望

使用比特币进行数据可用性的 ZK-Rollups 需要从 L2 交易费中产生大约 190 万美元至 960 万美元的月收入，才能在 10-50 Sat/vByte 费率环境中运营。

费用估算引擎对于比特币上的 Rollups 实现盈利最大化至关重要。

比特币区块空间根本无法支持每 6-8 个区块发布 400KB 证明的 4-8 个 Rollups。

将在比特币上构建主权 Rollup 的团队将需要使用应用程序执行上市策略，让用户在 L2 上进行交易。

一些比特币 L2 将探索 L3 环境以执行交易，并使用 L2 和比特币 L1 的组合来提供数据可用性。

比特币上的 Rollups 将增加区块纳入的竞争，从而提高所有人（包括 Rollups 本身）的 L1费用。

使用比特币 L1 进行 DA 的比特币 L2 将需要通过费率衍生品市场和带外挖矿交易来对冲意外的波动费用飙升。