比特币的下一个进化：OP\_CAT深度解析

作者：Four Pillars 来源：@wowitsjun和@xparadigms 翻译：善欧巴，本站

许多人认为比特币由于其不变的架构而保持静态。没有明确的路线图超越其减半计划，预测比特币的未来具有挑战性。然而，比特币可以通过社区共识进行升级。如果大多数全节点同意，比特币可以通过软分叉实现升级，引入新的功能。

本文研究了比特币的主要过去升级，并探讨了 OP\_CAT，预计的下一个重要升级。让我们深入研究这些升级的重要性，并解释为什么它们代表着比特币历史上重要的里程碑。

## 1. 背景 - 主要升级：隔离见证（SegWit）、Taproot 和 OP\_CAT

1.1 隔离见证（SegWit）（2017 年） - 扩展比特币区块空间，诞生比特币现金

隔离见证升级于 2017 年 8 月实施，是比特币首次解决可扩展性问题的重大尝试。在隔离见证之前，比特币区块存储签名和交易数据的组合。这种方法效率低下，因为分配给签名的空间与签名数据的实际大小相比不成比例地大。

出现了两种相反的解决方案：一组倡导增加比特币的区块大小，而另一组寻求保持现有区块大小但提高效率。隔离见证，即后一种解决方案，通过核心逻辑升级将签名数据与交易数据分离。它创建了一个名为“见证区域”的单独存储空间，允许在每个比特币区块中记录更多交易数据。

由于隔离见证升级，每个区块中可以存储的交易数据量增加了四倍。这一改进导致交易处理速度更快，费用降低。

1.2 Taproot（2021 年） - 提高比特币的效率和隐私

Taproot 于 2021 年 11 月实施，是继隔离见证之后比特币的另一个重要升级。该升级通过引入 Schnorr 签名和 Merkle 抽象语法树（MAST）来增强比特币的效率和隐私。

在 Taproot 之前，比特币的签名方法依赖于椭圆曲线数字签名算法（ECDSA），每个交易需要一个签名。这种方法导致签名数据大小增加，并且当多个钱包向单个地址发送资金时，更容易跟踪交易。

Schnorr 签名通过将多个签名合并为一个唯一的签名来解决 ECDSA 的限制。这大大减少了区块中签名大小的比例。此外，即使具有多个功能的交易也显示为单个交易，从而增强用户隐私。

此外，Merkle 抽象语法树（MAST）允许 Taproot 更有效地处理复杂的比特币交易。它通过引入逻辑来提取和验证所需脚本的哈希值来实现这一点。

与隔离见证升级不同，Taproot 在比特币社区获得了几乎一致的支持。

1.3 OP\_CAT（又名 BIP-420） - 比特币生态增长的基础

OP\_CAT 被广泛认为是比特币的下一个升级。它是一段简单的 13 行代码，中本聪在 2010 年为了保护比特币免受 DDoS 攻击而停用了它。OP\_CAT 允许在比特币系统中连接多个元素。今天，人们正在推动重新引入 OP\_CAT，并采取措施防止 DDoS 攻击，例如限制复制大小。这种重新引入，称为 BIP-420，可能是比特币生态系统的一个重要里程碑，能够实现各种发展，包括第 2 层解决方案。

正如“通过 L2 扩展比特币的真正方法”中所强调的那样，比特币的脚本是无状态的。然而，将 OP\_CAT 与 Schnorr 签名结合起来可以允许比特币强制执行特定操作并验证状态更改。这至关重要，因为区块链本质上存储状态。如果可以在比特币内部确认状态更改，则为内部智能合约打开了大门。此外，OP\_CAT 可以启用 STARK 验证，通过零知识证明促进比特币存款和取款。Starkware 已经在比特币 Signet 上展示了通过 STARK 进行零知识证明。许多人预计在不久的将来将进行软分叉以引入 OP\_CAT，这可能会彻底改变比特币生态系统，甚至整个加密货币领域。

## 2. 总结

2.1 @wowitsjun\_ 来自 Hashed

比特币下一个升级的方向将是一种直接有助于扩展比特币生态系统而不是提高其效率的升级。解锁比特币潜力的意义远不止于另一个生态系统的出现。扩展比特币生态系统将为将分散的区块链空间整合为一体铺平道路，利用与以太坊生态系统的协同效应。随着通过未来的升级逐一揭开比特币可扩展性的线索，比特币生态系统将不可避免地扩展。在这里，我们需要思考一下未来的金融系统将会是什么样子。

2.2 @xparadigms 来自 Four Pillars - “数字黄金的下一阶段”

比特币以其对变化的抵抗力而闻名，过去的意见分歧导致了比特币现金和比特币 SV 等分叉。尽管备受争议，但拟议的 OP\_CAT 添加有望产生比任何之前的升级更大的影响。

将 OP\_CAT 引入比特币可以实现安全的扩展解决方案，培育强大的比特币生态系统。它能够连接多个元素，允许证明验证，包括 zkRollup 部署。例如，Starkware 最近在测试网上测试了一个基于 STARK 的 zkRollup。

黄金的价值源于其稀缺性和公认的实用性。同样，比特币作为现已确立的“数字黄金”，正在进入一个探索其应用的新阶段。随着 OP\_CAT 升级，这种数字黄金可以成为构建数字基础设施和金融的基石。