比特币开发者推出BitVM2 进一步增强比特币可编程性

作者：Bradley Keoun，CoinDesk；编译：白水，本站

## 摘要

Robin Linus 和合著者团队撰写的新“BitVM2”论文标志着从初始设计向前迈进了一步。

该项目将依靠先进的加密技术和新颖的设计来促进将比特币从主网络转移到辅助网络（称为“Rollup”）的安全“桥梁”。

与早期版本不同，BitVM2 是“无需许可的”，允许任何人质疑可疑交易，而不仅仅是一组固定的操作员。

比特币开发者罗宾·林纳斯 (Robin Linus) 去年以理论方法让最古老、最原始的区块链更具可编程性，震惊了加密技术领域。他推出了第二个版本“BitVM2”，宣称其有了重大改进，可能让这一概念更接近实际实施。

根据林纳斯和五位合著者周四发布的白皮书，基本设置包括使用加密技术将程序压缩为子程序，然后可以在比特币交易中执行。

然后，在三个链上交易中对程序进行“验证”，基本上确保没有人试图作弊或盗窃。据联合创始人之一阿列克谢·扎米亚京 (Alexei Zamyatin) 称，在之前的版本中，验证可能需要 70 笔交易，扎米亚京还为一个名为 BOB（Build on Bitcoin 的缩写）的项目工作。

新版本的一个关键改进是，任何人都可以质疑可疑交易，这一功能被称为“无需许可的挑战”。在去年 10 月发布但从未真正投入实际实施的原始 BitVM 中，只有一组固定的操作员可以发起挑战。

“这种设计为我们带来了重大改进，”Zamyatin 在接受采访时表示。“我们现在对 BitVM 范式有了全面的描述。”

Linus 是 ZeroSync Association 的核心贡献者，该协会是一家位于瑞士祖格州的非营利组织。除了 Zamyatin 之外，其他合著者还包括 Lukas Aumayr、Andrea Pelosi、Zeta Avarikioti 和 Matteo Maffei。

Linus 的项目被誉为一项突破，部分原因是它不需要对底层比特币代码进行任何更改。这一点至关重要，因为与大多数后续区块链项目相比，比特币在治理上更加完全去中心化；比特币并没有像以太坊或 Solana 那样真正有一个指导基金会、管理机构或首席开发人员。

即使是像备受讨论的 OP\_CAT 这样看似温和的提案，也难以被比特币代码的维护者采纳，因为几乎完全的共识已经发展成为建议更新的事实标准。



BitVM2 协议的高层概述。（Linus 等人）

BitVM2 的初始应用是启用“rollup”——本质上是比特币之上的独立辅助网络，可以处理更快、更便宜的交易，但具有类似的安全保障。

Linus 的原始设计的发布就激发了在比特币上构建项目的热情；截至 7 月，CoinDesk 统计至少有 83 个比特币第 2 层项目正在筹备中，具有各种设置，包括 rollup 和侧链。

新范式可用于创建区块链“桥”，可用于安全地将比特币转移到 rollup，然后安全地将其带回，以便可以提取存款。

虽然比特币的工作量证明共识机制（确认交易的方法，本质上涉及数据中心不间断地解决加密难题，耗电量很大）因其对环境的影响而受到批评，但大多数区块链专家都认为它是最安全的区块链。

这种优点得到了所有未偿还比特币 1.2 万亿美元市值的强调——超过所有其他加密货币的总和。

Linus 在 Telegram 消息中指出：“我们新的桥梁设计更简单，资本效率更高。”“以前的设计造成了流动性问题，无论是桥梁运营商需要锁定多少抵押品，还是锁定多长时间。现在，它需要的资本更少，锁定时间更短。”