比特币技术复兴：释放万亿价值

作者：Leeor Shimron编译：Block unicorn

在这一轮加密牛市周期中，一个日益重要的主题是比特币二层网络（Bitcoin L2）的兴起。比特币通常被认为是最大、去中心化程度最高、且最安全的加密资产，拥有超过1亿全球持有者，市值高达1.2万亿美元。

然而，作为一种技术平台，它也存在一些局限性，如交易速度缓慢（区块确认时间约为10-30分钟）、可扩展性低（每秒只能处理约7笔交易）以及可编程性有限（其脚本语言和智能合约功能较为受限）。

历史上，最成功的技术网络通常是分层构建和扩展的，这在互联网的发展中尤为明显。互联网的分层方法被称为开放系统互连模型（OSI模型），包括七层：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。每当终端用户访问电子邮件或在社交平台上发布评论时，这些技术都会在后台运行并相互作用，而用户对此一无所知。



OSI 模型概述了互联网堆栈的各层

同样，为了应对比特币的局限性，同时仍然继承其宝贵的网络安全性和去中心化特性，比特币生态系统正在积极开发比特币二层网络。这些项目引发了一场开发和可编程性的复兴，将去中心化金融（DeFi）、NFT、游戏以及其他在竞争区块链生态系统中蓬勃发展的应用场景带入比特币。

这种分层方法与那些试图在基础层提供区块链所有核心功能（共识、数据可用性、执行）的集成区块链形成鲜明对比。像Solana、Near和Algorand这样的区块链旨在扩展并提供高性能计算，而不需要将数据可用性或执行转移到其他网络上，这与比特币和以太坊所采用的“模块化”方法不同。

总锁仓价值（TVL）是衡量特定生态系统中DeFi增长的主要指标。它代表了以各种方式部署的资本，例如借出资产以赚取收益、在资金池中提供流动性、作为抵押品来获得链上信贷等。虽然比特币二层网络的发展使DeFi应用场景在比特币上得以繁荣，但其增长仍然有限，相比之下，以太坊等更加成熟的生态系统要更为领先。



目前，在领先的比特币二层网络上的去中心化金融（DeFi）总锁仓价值（TVL）约为15亿美元。这个数字看起来可能很大，但仅占以太坊当前锁仓价值813亿美元的2%。此外，如果你看TVL与网络市值的比率，比特币的比率仅为0.13%，而以太坊的这一比率则高达27%。

考虑到比特币中存储的潜在价值超过1万亿美元，领先的比特币二层网络在解锁这一价值以用于各种金融用例方面有着巨大的市场机会。如果比特币的DeFi增长达到与以太坊相当的比例，这意味着按当前市场价格计算，将有3000亿美元的可部署资本。

基础协议与二层解决方案

Ordinals和Runes是比特币上的基础协议，分别于2023年1月和2024年4月推出。特别是Ordinals协议，引发了对比特币开发的更大兴趣，通常被认为是“比特币第二季”开始的催化剂。

像Ordinals和Runes这样的基础协议直接在比特币的基础层上运行，而不改变核心协议。它们在比特币交易中嵌入了额外的功能，适用于可以直接用比特币现有脚本框架构建的应用程序（如铸造在单个聪上的NFT和meme币）。

相比之下，比特币二层解决方案在与比特币锚定的独立区块链上运行。它们通常使用比特币的安全性来确保最终性，但通过自己的共识机制提供更复杂的功能。

二层解决方案使智能合约、去中心化应用（dApps）和跨链交互成为可能，通常还带有自己的代币（如DeFi、游戏、社交媒体和其他需要更复杂逻辑的应用）。

无论是基础协议还是二层解决方案，这两种方法都旨在通过启用新用例和应用来增强比特币的实用性，这将推动对比特币区块空间的需求增加。这种需求的增加反过来将提高比特币基础层的交易费用，对维持比特币的安全模型至关重要，尤其是在区块补贴每四年因减半而下降的情况下。



序数和铭文产生的网络费用

在过去的两年中，Ordinals（序数协议）曾多次导致比特币的交易费用激增，但迄今为止，Ordinals尚未成为比特币矿工的可持续费用收入来源。自最近一次在2024年4月减半期间的费用激增以来，Ordinals铸造的平均每日交易费用已从约200万美元下降了98.8%，如今仅为约2.5万美元。为了在长期内保持健康的交易费用，其他比特币二层项目需要取得更大的进展。

微支付、游戏或DeFi等低价值交易需要较低的交易费用。只有二层解决方案才能将交易费用保持在足够低的水平，使这些经济活动具有可行性，同时仍然为矿工带来更多收入。相比之下，元协议会膨胀比特币的状态，推高基础层的交易费用，从而将此类交易排除在外。

值得注意的是，很多基础协议并不是比特币的新事物，历史上比特币网络中也曾出现过多个此类协议。Omni Layer（前身为Mastercoin）于2013年推出，允许发行新代币和稳定币，如Tether。Counterparty于2014年推出，同样允许发行新代币和去中心化应用。Rootstock于2018年推出，是一个与比特币合并挖矿的智能合约平台。

比特币二层网络的下一个时代

近年来，我们见证了数十个新项目加入“比特币第二季”的叙事，并声称以某种方式集成了比特币。最近的例子包括Build on Bitcoin (BOB)、Bitlayer、CoreDAO、Babylon、Botanix、Merlin、BEVM、Citrea等。这些新进入者与现有的先驱者如Stacks、闪电网络（Lightning Network）和Rootstock一起，推动了这一领域的发展。

这些项目的终极目标是以信任最小化的方式，让开放且无许可的应用程序能够利用持有者的比特币价值。例如，想象一下能够将你的比特币借出以赚取原生比特币收益，或是用你的比特币作为抵押来获取信贷，或者通过比特币的价值支持铸造稳定币，而不必担心跨链风险或二层网络丢失你的比特币。

判断一个比特币层是否为“真正的二层网络”的关键在于用户是否能够在使用这些应用程序的同时，也能单方面退出。这意味着用户可以将她的比特币从比特币二层网络桥接回比特币基础层，而不需要任何权限。真正的比特币二层网络还完全继承了比特币的安全性，受益于网络上矿工生成的算力。

目前，唯一能够实现单方面退出的协议是闪电网络和状态链（statechain）。其他协议如侧链和汇总（rollup），目前在桥接方面存在限制，尚不符合这一标准。然而，提议的桥接协议相较于现状有所改进，并为更灵活的二层设计铺平了道路。

比特币二层项目遵循不同的框架，具有不同的信任假设，主要结构为侧链、状态通道、ZK汇总或乐观汇总（BitVM）。以下是每种框架的概述以及它们的信任假设和局限性：

侧链：独立的区块链，通常具有自己的代币、共识机制和验证者集，与主区块链连接，允许在两者之间转移资产，同时实现额外的功能和可扩展性。

信任假设：依赖于由核心团队控制的多签名合约，通过比特币基础层和二层解决方案之间的中心化管理桥接，比特币基础层的状态和交易最终性由侧链而非比特币基础层验证。

状态通道：链下交易方法，允许参与者私下和即时地进行多次操作，仅将最终状态广播到主区块链，从而增强可扩展性并降低费用，但需要信任参与者之间的合作并防范欺诈。通常不具有自己的代币或共识机制。

信任假设：假设参与者在链下将会合作，持续监控区块链以防止欺诈，依赖足够的流动性和诚实的节点运营者，并信任有效的争议解决机制以关闭通道。

ZK汇总：一种扩展解决方案，将多个交易批量处理在链下并生成简洁的密码学证明，然后在链上验证以确保正确性和安全性，同时显著减少主区块链上的数据和计算负担。

信任假设：由于无法在比特币上执行ZK验证，涉及中心化的排序者，依赖去中心化的验证者网络准确验证由证明者检查的交易，并且由于需要将数据发布回比特币，汇总在交易处理能力方面有限。

BitVM：类似于以太坊上的乐观汇总，BitVM是一种通过将合约分解为逻辑门并使用欺诈证明进行无信任执行的概念框架。作为一种新的概念框架，BitVM尚未在生产环境中被任何区块链采用，预计首批解决方案将于2025年初上线。

信任假设：假设其无信任桥接机制，使用基本计算单元让欺诈证明者检测不准确之处将有效运作，但面临经济挑战，因为运营者必须用等量的抵押物匹配被桥接的流动性，使得可扩展性变得困难。

L2的分类：



即将到来的催化剂

让我们来看看几个领先的比特币二层网络及其即将推出的一些发展。

Stacks 是一个领先的比特币二层网络，于2021年1月首次启动主网，允许创建与比特币锚定的智能合约。Stacks支持着一个不断增长的dApp、DeFi平台、NFT和其他基于区块链的应用程序生态系统，所有这些都由比特币的底层网络提供安全保障。

Stacks的DeFi生态系统一直在稳步增长，包括核心协议如流动质押协议（Stacking DAO）、借贷市场（Zest Protocol）、去中心化交易所（Bitflow、Velar）以及加密资产支持的稳定币（Arkadiko、Hermetica、BSD）。

Stacks的独特之处在于其转移证明（PoX）共识机制。Stacks矿工通过消耗比特币来竞争挖掘新Stacks区块的权利，并获得STX奖励。STX持有者还可以通过锁定他们的STX代币并获得BTC奖励来参与其中。历史上，参与共识的STX代币持有者的年化回报率约为8%。



Stacks Proof of Transfer（PoX）共识机制图解

Stacks即将进行一次名为中本聪升级（Nakamoto Upgrade）的重大升级，该升级将为协议带来多项改进。预计在8月28日进行的升级旨在为Stacks交易带来真正的比特币最终性。这意味着一旦Stacks交易被确认并锚定到比特币区块链上，它就会获得与比特币交易相同的安全性和不可篡改性。

升级还将加强Stacks与比特币之间的集成，确保Stacks区块的任何重组都将需要比特币区块的重组，从而显著增加Stacks交易的安全性。

此外，升级引入了sBTC，这是一种在Stacks网络上的比特币等价代币，将以一比一的比例由BTC支持。这使用户能够在Stacks生态系统中直接使用比特币，实现与比特币流动性更无缝的集成，并增强BTC在智能合约和dApp中的实用性。

这些功能使得Stacks，特别是在中本聪升级后，相比于许多其他项目，成为一个更为纯粹的比特币二层解决方案，通过更全面地利用比特币的安全性、经济模型和去中心化特性。

Build on Bitcoin (BOB) 和 Botanix 是另外两个领先的比特币二层项目，它们采取了与Stacks不同的方法。BOB是第一个由比特币和以太坊共同驱动的混合二层网络。BOB的汇总生态系统旨在利用比特币的安全性，同时让用户能够访问以太坊虚拟机（EVM）提供的所有功能，如进出通道、稳定币、NFT、DeFi等。

BOB已经完成了其路线图的第一阶段，包括使用Optimism (OP) 框架启动乐观ETH汇总。结算发生在以太坊一层，而BOB通过比特币轻客户端跟踪比特币的状态，使跨链交换和合约能够在以太坊和比特币之间执行。

第一阶段于5月1日启动，支持Sovryn去中心化交易所、LayerBank借贷市场和Velodrome去中心化交易所等。未来阶段将引入比特币工作量证明安全性到ETH汇总，最终BOB的路线图将以其自己的BitVM汇总实现为终点。

BOB的联合创始人Alexei Zamyatin表示：“BOB已经在主网上线并拥有一个不断增长的生态系统，我们与团队紧密合作，优先解决产品问题，而不是谈论炫酷技术或通过不可持续的激励措施来推高总锁仓量（TVL）。”

“我们将以太坊上的新技术带到了比特币，包括意图（BOB Gateway，一键式BTC部署）和智能账户（BOB Pay，无需钱包即可通过电子邮件或Telegram发送BTC）。通过BOB Gateway，BOB是从BTC到包裹BTC、BTC流动质押代币以及即将推出的BTC收益头寸的最便捷途径。”

Botanix Labs 旨在建立第一个完全去中心化的EVM等效二层网络在比特币上。利用比特币作为结算和去中心化的基础层，Botanix将使用权益证明共识模型，其中的权益（以比特币表示）将安全存储在Spiderchain上，一个由随机参与者子集保护的去中心化多重签名合约分布式网络。

Botanix Labs的创始人Willem表示：“Botanix完全运行在比特币上，这意味着它不连接到任何其他链，且燃气费以比特币支付。它与汇总的不同之处在于，第一天就有15个不同节点运营者组成的去中心化排序者，而汇总则采用更中心化的单一运营者模式。Botanix将拥有极低的燃气费和抗审查性。”

Botanix于2023年11月启动了其测试网，目前已拥有超过20万个活跃地址。尽管其主网尚未上线，用户仍然可以通过Botanix的测试网进行交互，允许用户连接钱包、接收资金并进出Botanix网络。主网预计将在9月上线，已经宣布的合作伙伴包括Frax、Vertex、Kiln和Supra Oracles。

BOB和Botanix都利用EVM来实现智能合约的创建和执行。这确保了与以太坊上已经构建的开发工具和基础设施（如钱包、区块浏览器、数据分析工具和消费者应用程序）的兼容性。这使得开发人员、工具和应用程序能够轻松移植到他们各自的生态系统中。

相比之下，Stacks开发了Clarity虚拟机，采取了从基础原理出发的方法来发展其开发者社区。这对区块链开发人员来说有更高的学习曲线，但可以更容易吸引那些已经熟悉Web 2.0友好技术的开发者。长期来看，哪个方法更能鼓励开发者的采用还有待观察。

未来是比特币时代

比特币二层网络的出现标志着区块链生态系统的一个重要进化。这些解决方案旨在通过利用比特币强大的安全性和去中心化特性，同时实现广泛的应用和增强的功能，从而解决比特币的固有局限性。

比特币二层网络与元协议的共同发展，代表了释放比特币内在巨大价值的一条有希望的道路，可能将其转变为一个更具多样性和强大功能的金融平台。

随着这些项目的不断成熟并与比特币无缝集成，它们有望推动加密领域的重大进展，使比特币变得更具可扩展性、可编程性，并能够支持多种用例。