不断发展的比特币：DeFi 机会和可扩展性解决方案

作者：Greythorn Asset Management，编译：白话区块链

作为最早和市值最大的区块链，比特币不仅引领了数字资产的发展，还在市值方面继续主导市场。不过目前被视为“数字黄金”的比特币，主要因其作为价值储存手段而受到认可，而非其在去中心化应用中的作用。

然而，近期的发展表明，比特币在构建活跃的去中心化金融（DeFi）生态系统方面的潜力比之前预期的要大。这一变化发生在市场对比特币的兴趣和技术能力发展前所未有地契合的背景下。



SEC批准了在所有注册证券交易所上市的比特币ETF，并将对其进行持续监管以保护投资者。来源：x.com

未来几年可能对比特币至关重要，因为它有可能从一个被动的价值储存手段转变为一个充满创新和投资机会的活跃生态系统。我们相信这是一个值得探索的机会，特别是考虑到大多数人尚未投资于这个新兴生态系统，并且一些新功能，如 Runes 即将推出。

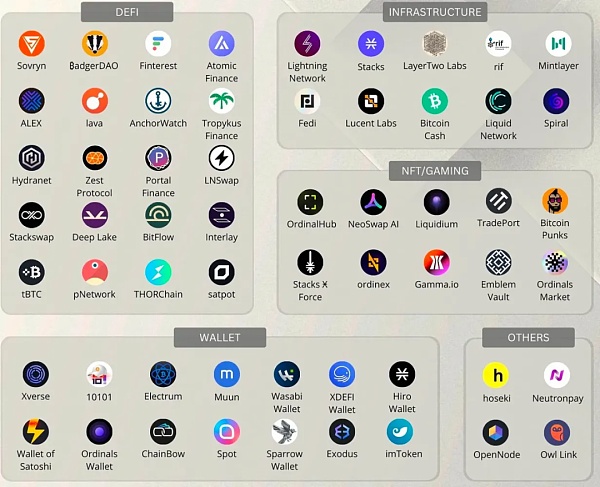
这将是首次人们能够直接投资于比特币区块链上的协议和资产的牛市。这些资产预计会随着比特币价格的上涨而获利，当人们出售比特币时，利润将逐渐显现。本文将重点分析一下比特币未来可能带来的潜在机会。

## 01比特币生态系统

比特币协议的核心代码多年来几乎没有变化，主要用于交易的媒介。2017年，比特币协议实施了SegWit升级，将数字签名（“见证”）从交易数据中分离出来。这种分离有效地释放了空间，使得更多交易能够包含在区块链中。

随后，在2021年，引入了Taproot升级。这一改进允许将多个签名和交易组合在一起，促进了签名的聚合。本质上，这意味着可以将多个签名组合在一起进行验证。尽管有这些升级，比特币仍面临着可扩展性、交易速度慢和成本高等挑战。

目前，比特币网络包括矿工、节点、利益相关者、开发者，以及各种第二层解决方案、侧链和DApp。矿工和节点通过验证交易和确保共识来维护网络，这通过工作量证明机制实现（POW）。开发者社区则通过扩展本地生态系统和偶尔的核心协议更新来贡献力量，因为这些更新可能难以达成共识，因此变化较少。以下是比特币生态系统的简要概述表：



## 02Layer2 解决方案

针对比特币的可扩展性问题，已经提出了多个解决方案，但绝大多数比特币用户视工作量证明系统（PoW）为比特币身份的核心部分，并通常不愿支持对协议进行重大更改。

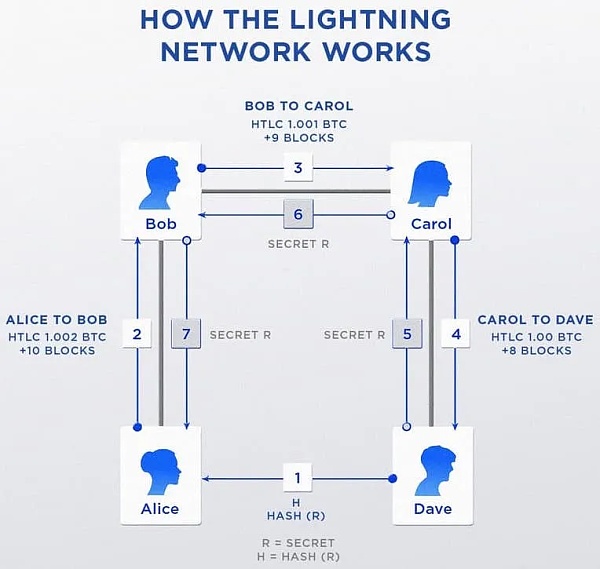
尽管如此，Layer2 解决方案提供了一种更实用的方法，因为它们不涉及对核心区块链的重大修改。这些解决方案作为独立的区块链层叠在比特币主网络之上，使其更容易实现，并且更现实地解决可扩展性问题。

以下是三家主要的参与者：

1）闪电网络（The Lightning Network）

于2016年推出，是首个在比特币区块链上开发的第二层支付协议，旨在提高交易速度和降低成本，利用比特币的智能合约功能实现接近即时的支付。虽然闪电网络成功提高了交易效率，吸引了超过3.47亿美元（截至7月31日）的总锁定价值（TVL），但它并未提供开发多样化DApp生态系统所需的高级智能合约功能，而是专注于其点对点支付网络能力。

来源：闪电网络



2）Stacks

Stacks是目前市场领导者，并且已在7月13日完成 Nakamoto 升级，该升级能显著提升安全性和速度。Stacks由计算机科学家Muneeb Ali于2013年在普林斯顿创立，他在该技术上研究了四年。除此之外，该项目还拥有一支极其优秀的团队，其技术已由斯坦福和普林斯顿的专家进行过同行评审。

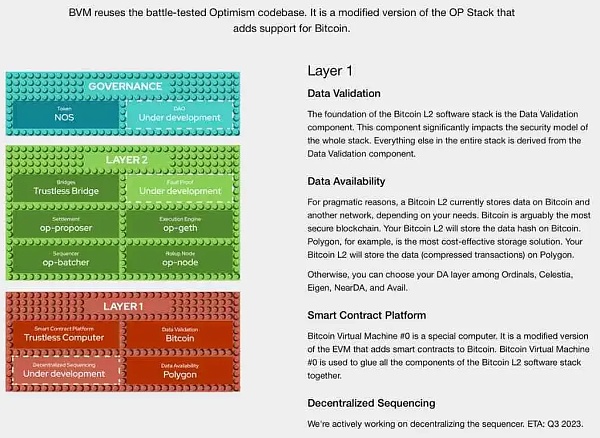
Stacks使智能合约和Dapp能够利用比特币作为资产，并在比特币区块链上结算交易，Stacks层上的所有交易都自动被哈希并结算到比特币上。

3）BVM 网络

通过其Layer2元协议可以解决比特币的智能合约和可扩展性限制。BVM支持DApp和智能合约的创建，并促进比特币Layer2区块链的扩展。目前，BVM在链上作为一个领先解决方案正在崛起，特别是在最近的市场低迷期间表现明显。其相对强劲的表现显示出潜在增长，尤其是在对比特币Layer2解决方案兴趣上升的背景下。

作为一个Rollup-as-a-Service (RaaS) 协议，BVM允许用户轻松启动新的比特币L2区块链，所有价值都回流到BVM Token持有者，因为新的Layer2不断用 BVM Token支付费用。值得注意的进展包括利用BVM SDK推出的Tuna链和Naka链。此外，计划集成Runes功能预示着BVM的进一步增长。

BVM 重新使用了经过实战检验的 Optimism 代码库。它是 Op Stack 的一个修改版，添加了对比特币的支持。该软件栈包括数据验证、数据存储选择、智能合约平台（比特币虚拟机）和即将推出的去中心化排序器。来源: BVM



其他几种扩展解决方案已被开发，用于在比特币上实现智能合约：

RGB: 一个链下层，利用比特币的UTXO来创建数字资产，如Token和NFT，完全兼容闪电网络。

Counterparty: 允许Token创建和众筹；通过像Ordinals这样的创新得到了复兴。

Rootstock (RSK): 一个合并挖矿的侧链，支持与以太坊虚拟机（EVM）兼容的智能合约，使用与比特币挂钩的RBTC。

Liquid Network: Blockstream推出的侧链，支持去中心化交易和资产发行，包括NFT和稳定币。

Omni Layer: 支持Token铸造和DEX；通过Omni Bolt增强了闪电网络的交易速度。

Mintlayer: 将权益证明（Proof of Stake）与比特币的工作量证明（Proof of Work）结合在一个侧链上，支持智能合约和跨区块链转账。

## 03比特币上的DeFi

以太坊一直是DeFi的首选Layer1区块链。然而，近期的发展可能使比特币成为主流DeFi采纳中的重要玩家。随着美国的监管变化、对2024年比特币减半的预期以及比特币 Ordinals 的引入，比特币正逐渐获得更多可能。

比特币网络正在超越简单的交易功能，通过各种扩展解决方案为丰富的DeFi生态系统铺平道路。这一发展催生了支持更复杂金融应用的项目，挑战了以太坊的主导地位。

例如，Sovryn在基于比特币的Layer2 EVM智能合约区块链RSK上，提供了一个非托管、无需许可的环境，用于交易、借代和放代比特币及其他精选资产。

此外，Zest Protocol由Primal Capital支持，正在开创基于比特币的点对点去中心化借代。同时，比特币 DEX 如Bisq Network在去中心化自治组织（DAO）下运行，支持点对点交易。

## 04序数（Ordinals）与符文（Runes）

虽然符文（Runes）协议之前获得广泛关注，但许多人仍对其如何利用UTXO会计简化比特币交易不甚了解。与传统方法如Unisat市场相比，符文提供了更经济的入门点。在此之前，比特币交易主要通过账户模型管理，需要特定的交易金额，相较于以太坊上的Token交易，用户体验较差。

由Ordinals的创始人创建的Runes意在成为比特币版的以太坊ERC20，便于发行可替代的Token。该协议计划在比特币减半后的4月19日推出，可能会提高比特币Layer1上的交易费用，并可能促进比特币Layer2解决方案的活动。

Ordinals将数据存储在交易见证中，并将信息附加到单个satoshi上。与Ordinals不同，Runes则将Token记录嵌入比特币的未花费交易输出（UTXOs）中。这种方法能够无缝对接比特币现有系统，提升其功能性和区块链的完整性，并特别设计方便在各种Layer2平台（如Stacks）上轻松实施。

以下是一些与Runes协议相关的关键项目：

PUPS / Rune Pups：这是一个NFT系列，在Post-Runes激活后，将通过Airdrop的方式分发23%的PUPS供应量。

WZRD：这是Ordinals生态系统中的早期文化Token，已迅速增长。

Runestones：该项目将在比特币减半后转型为Runes Token。它已经被Airdrop到多个Ordinals收藏中，包括Bitcoin Puppets。

当你购买BRC20 Token时，你实际上是在购买可以在减半后转换为Runes等效Token的BRC20s。随着生态系统的推出，将会有更多类似的项目，请保持关注。

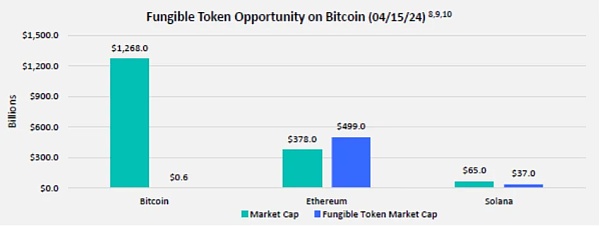
相关Runes的看涨观点如下：

比特币可替代性的创新：Runes在比特币区块链上引入了新的Token标准，旨在改进当前的BRC-20可替代Token标准。这一创新被认为足以促使对比特币在去中心化应用领域潜力的重新评估。

效率与设计：Runes Token标准通过使用基于UTXO的设计，更为高效。这与比特币的BRC-20和以太坊ERC-20 Token的基于账户的设计不同，可能减少当前过程中的‘垃圾’UTXO创建带来的膨胀和高费用。

市场定位：比特币的可替代Token市场市值相对较小，与以太坊和Solana相比。尽管如此，更高效的Token标准如Runes的引入可能有助于缩小这一差距。

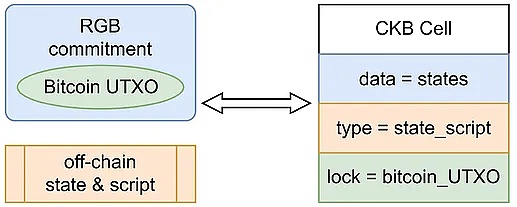
兼容性与隐私：Runes设计为与闪电网络兼容，并承诺提供更高的隐私，因为数据隐藏在UTXOs中。这一兼容性和隐私特性被视为对现有标准的重要改进，可能使比特币成为DeFi领域更具吸引力的平台。



比特币上的同质化Token的潜力最大，来源: Franklin Templeton

## 05RGB++

RGB++通过将智能合约集成到Nervos CKB区块链上，增强了比特币的功能。RGB++的亮点是其同构绑定（isomorphic binding），它实现了比特币与CKB Nervos区块链之间的资产管理同步。在实际操作中，每个比特币UTXO（未花费交易输出）与CKB区块链上的相应Cell（可以理解为“区块”）绑定在一起。因此，当使用UTXO进行比特币交易时，该交易会自动记录在CKB区块链上，并且CKB上的相应Cell会被更新。



通过RGB比特币与CKB Nervos区块链之间的资产管理同步示意图

该系统无需第三方多重签名桥接，能够实现无信任的跨链交易，同时确保两个网络上的活动准确映射。RGB++被认为是一个有前景的比特币 Layer2 解决方案。

在投资方面，直接与RGB++相关的Token是CKB，其市值达到15亿美元（截至7月31日），超过99%的Token已经流通。这减少了对新Token发行可能对市场产生影响的担忧。

## 06结语

这些信息量很大，理解起来可能有些复杂。但比特币生态系统值得关注，因为比特币仍然在所有加密货币中拥有最高的采纳率，并且被个人和机构投资者认可，这可能带来更多的稳定性和增长潜力。

由于像闪电网络这样的持续发展（加快交易速度）和像符文（Runes）这样的举措（提升Token的可替代性），比特币正不断改进和扩展其应用。