比特币去中心化金融现在进展如何了？

作者：CoinMarketCap Research & Footprint Analytics；来源：白话区块链

比特币在 DeFi（去中心化金融）中的角色正在发生巨大变化。从最初只是简单的点对点转账，这个世界上首个加密货币如今正在逐渐崛起，成为DeFi领域中的一支强大力量，开始挑战以太坊长期以来的主导地位。

通过链上数据全面解读比特币生态的现状、增长轨迹，我们发现了一幅清晰的图景：BTCFi（比特币与DeFi的结合）不仅仅是一次技术上的转变，更可能引发比特币在DeFi中角色的范式转变。正如我们将深入探讨的那样，这一转变的影响可能重新定义整个DeFi领域的格局。

## 01BTCFi 的兴起

2008年，中本聪推出了比特币，最初的设计目的是作为一种点对点的电子现金系统。虽然这一架构在加密资产领域具有革命性意义，但在更复杂的金融应用（比如 DeFi）方面却存在明显的局限性。

## 02比特币的原始设计及其在DeFi中的局限性

核心设计要素及其局限性：

1）UTXO模型：比特币使用未花费交易输出（UTXO）模型，这种方式在处理简单转账时很有效，但缺乏支持复杂智能合约所需的灵活性。

2）有限的脚本语言：比特币的脚本语言设计上受限，主要是为了避免安全漏洞。然而，这种限制也妨碍了它支持复杂的 DeFi 应用，因为它可执行的操作码（opcodes）数量有限。

3）缺乏图灵完备性：与以太坊不同，比特币的脚本并不是图灵完备的，这使得实现依赖状态的复杂智能合约变得困难，而这些智能合约对许多DeFi协议至关重要。

4）区块大小和交易速度：比特币的1MB区块大小限制和10分钟的区块生成时间，导致其交易处理速度远低于专注于DeFi的其他区块链。

这些设计选择虽然增强了比特币的安全性和去中心化程度，但也给在比特币区块链上直接实现DeFi功能带来了障碍。缺乏对循环、复杂条件和状态存储等特性的原生支持，使得在比特币上构建DEX、借代平台或流动性挖矿协议等应用变得非常困难。

## 03在比特币上引入DeFi的早期尝试与发展

尽管面临这些局限性，比特币强大的安全性和广泛的应用促使开发者寻找创新解决方案：

1）彩色币（2012-2013）：这是扩展比特币功能的早期尝试之一。彩色币通过给特定的比特币“着色”并附加独特的元数据，来表示和转移现实世界的资产。虽然这并不算真正的 DeFi，但为比特币上开发更复杂的金融应用打下了基础。

2）Counterparty（2014）：这个协议在比特币区块链上引入了创建和交易自定义资产的能力，包括第一个 NFT。Counterparty展示了在比特币上开发更复杂金融工具的潜力。

3）闪电网络（2015年至今）：闪电网络是一个旨在提升交易扩展性的二层协议。它通过引入支付通道，为更复杂的金融互动开辟了可能性，包括一些初步的DeFi应用。

4）离散日志合约（DLC）（2017年至今）：由Tadge Dryja提出，DLC允许在不改变比特币基础层的情况下实现复杂的金融合约，为衍生品和其他DeFi工具提供了新的可能性。

5）Liquid网络（2018年至今）：这是由Blockstream开发的一个基于侧链的结算网络，支持加密资产的发行以及更复杂的比特币交易，为类似DeFi的应用铺平了道路。

6）Taproot升级（2021）：通过引入梅克尔化替代脚本树（MAST），Taproot将复杂交易压缩成一个单一哈希，降低了交易费用并减少了内存使用。虽然它本身不是DeFi解决方案，但提升了比特币的智能合约能力，使得实现复杂交易变得更简单高效，为未来的DeFi发展奠定了基础。

这些早期的发展为比特币的功能从简单的转账扩展到更多应用奠定了基础。尽管在比特币上引入DeFi面临挑战，这些创新也展示了比特币生态系统的潜力。这些基础为二层解决方案、侧链以及比特币DeFi的创新浪潮铺平了道路，接下来我们将深入探讨这一领域。

## 04关键创新：在比特币上实现智能合约

近年来，比特币生态系统出现了多个协议，旨在为这款全球首个加密货币引入智能合约和 DeFi 功能。这些创新正在改变比特币的用途，使其不仅仅是一个价值存储或交换媒介。以下是一些推动比特币实现智能合约的主要协议：

1）Rootstock：作为比特币智能合约的先驱，Rootstock是运行时间最长的比特币侧链，已经成为 BTCFi 生态系统的重要基础。

它利用比特币60%的算力，支持双重挖矿，并与以太坊虚拟机（EVM）兼容，这样以太坊的智能合约就可以在比特币上运行。Rootstock独特的Powpeg机制确保了比特币（BTC）与Rootstock比特币（RBTC）之间的无缝转换，而且它的“纵深防御”安全模型强调简单和稳健。

自2018年主网启动以来，Rootstock的链上活动稳步增长，Footprint Analytics指出，它在比特币生态系统中确立了一个稳定且可扩展的解决方案地位。2）Core：Core是一个以比特币为基础的区块链，它与比特币紧密结合，并兼容以太坊虚拟机（EVM）。



Core以其创新的双重质押模型而引人注目，这种模型将比特币和Core结合在一起。通过非托管的比特币质押，Core为比特币建立了无风险的收益率，有效地将比特币转变为一种收益资产。Core报告称，55%的比特币挖矿算力被委托给其网络，这有助于增强其在 DeFi 应用中的安全性。

3）Merlin Chain：Merlin Chain是一个相对较新的比特币二层网络，致力于释放比特币的DeFi潜力，正受到越来越多的关注。它集成了ZK-Rollup技术、去中心化预言机和链上防欺诈模块，为比特币持有者提供了一整套DeFi功能。Merlin推出的M-BTC是一种可赚取质押奖励的包装比特币资产，为收益生成和参与DeFi开辟了新的途径。

4）BEVM：BEVM代表着将以太坊广泛的DeFi生态系统直接引入比特币的重要进展。作为首个完全去中心化且兼容EVM的比特币二层网络，BEVM以比特币作为燃料，允许在比特币上无缝部署以太坊的去中心化应用（DApps）。BEVM得到了矿业巨头比特大陆的支持，开创了“算力RWA”的概念，可能为比特币生态系统解锁新的价值维度。

比特币二层网络和侧链的关键创新：

Token化比特币资产;

智能合约和EVM兼容性;

带收益的比特币;

可扩展性和隐私增强。

这些协议不仅仅是在比特币上复制以太坊的DeFi策略，而是在利用比特币独特的特点开辟新的方向。从Rootstock的深度防御机制，到Core的双重质押模型，再到Merlin提供的全面DeFi解决方案和BEVM的算力RWA创新，BTCFi领域正在迅速发展。

截至2024年9月8日，比特币的二层解决方案和侧链的总锁定价值（TVL）达到了10.7亿美元，自2024年1月1日以来增长了5.7倍，自2023年1月1日以来更是惊人地增长了18.4倍。Core领先，拥有27.6%的总锁定价值（TVL），紧随其后的是Bitlayer，占25.6%；Rootstock占13.8%；Merlin Chain占11.0%。







## 05比特币DeFi的现状

随着比特币DeFi生态系统的不断发展，一些关键项目应运而生，成为重要参与者，推动着创新和用户采用。这些项目依托于比特币的二层解决方案和侧链，提供各种 DeFi 服务：

1）主要BTCFi项目

Pell Network（多链）



Pell Network 是一个跨链再质押协议，旨在提升比特币生态系统的安全性并优化收益。用户通过质押比特币或流动质押衍生品（LSD）来获得回报，而去中心化的运营商则负责运行验证节点，确保网络的安全性。Pell 提供了一系列主动验证的服务，如预言机、跨链桥和数据可用性，支持更广泛的比特币二层生态系统。凭借其强大的基础设施，Pell 旨在成为提供流动性和保障加密经济安全的重要参与者，推动比特币经济的可持续增长。

Avalon Finance（多链）Avalon Finance 是一个多链 DeFi 平台，跨越 Bitlayer、Core 和 Merlin Chain，以其在 BTC DeFi 生态系统中提供全面的借代和交易服务而闻名。Avalon 的主要服务包括对主要资产和流动性较低资产的超额抵押借代，并设有专门的隔离池。该平台还集成了衍生品交易，增强了其借代服务的功能。此外，Avalon 还推出了一种算法稳定币，旨在优化资本效率，使其成为比特币生态系统中一个多功能且安全的 DeFi 解决方案。其治理Token AVAF 采用 ES Token模型，激励流动性提供和协议使用。



Colend Protocol（Core）

Colend Protocol 是一个建立在 Core 区块链上的去中心化借代平台，用户可以安全地借代比特币和其他资产。通过利用 Core 的双重质押模型，Colend 与更广泛的 DeFi 生态系统无缝集成，提升了比特币在DeFi中的实用性。其主要特点包括去中心化和不可篡改的交易、多种动态利率的流动性池，以及灵活的抵押系统。

MoneyOnChain（Rootstock）

MoneyOnChain 是一个建立在 Rootstock 上的全面 DeFi 协议，允许比特币持有者在保留私钥完全控制权的同时提升资产收益。该协议的核心是发行一种名为 Dollar on Chain（DoC）的稳定币，这是一种由比特币全额抵押的稳定币，专为希望保持其比特币持有价值与美元挂钩的用户设计。此外，MoneyOnChain 还提供Token BPRO ，使用户能够获得比特币的杠杆敞口，从而实现被动收益。



该协议的架构基于风险共担机制，采用专有的金融模型，以应对极端市场波动。同时，它还包括去中心化的Token交易平台（TEX）、去中心化预言机（OMoC）以及治理Token（MoC），使用户能够参与协议决策、质押并获取奖励。

Sovryn（多链）Sovryn 是一个DEX，也是建立在比特币上的功能最丰富的 DeFi 平台之一，旨在让用户能够使用比特币进行交易、借代和赚取收益。Sovryn 跨越 BOB 和 Rootstock 两个平台，提供多种 DeFi 服务，包括交易、兑换、流动性提供、质押和借代。该平台专注于为比特币打造一个无权限的金融层，并与其他区块链进行集成，使其在比特币 DeFi 生态系统中成为一个独特的多链平台。



Sovryn 的治理Token SOV 在通过 Bitocracy 系统管理去中心化协议中发挥着关键作用，代表投票权并奖励积极参与的用户。

Solv Protocol（Merlin Chain）Solv Protocol 处于 NFT 金融化的前沿，使用户能够创建、交易和管理链上的凭证。该协议旨在对 Merlin Chain 生态系统中各种 DeFi 协议的收益进行Token化和聚合。其旗舰产品 SolvBTC 是一种收益Token，允许比特币持有者在保持流动性的同时赚取收益。



Solv Protocol 通过质押和其他收益产生活动，致力于建立一个强大的流动性层。这种灵活性使其成为 Merlin Chain 上一个重要的 DeFi 项目，帮助在比特币生态系统中解锁新的金融机会。

这些项目突显了比特币 DeFi 领域的动态和快速发展，每个项目都为扩展生态系统的覆盖范围贡献了独特的功能。截至 2024 年 9 月 8 日，Core 在比特币 DeFi 空间中占据领先地位，其项目数量占活跃项目的 25.2%，进一步巩固了其在生态系统中的核心角色。Rootstock 和 Bitlayer 作为重要参与者，各自支持 13.0% 的项目，反映出它们在提升比特币 DeFi 生态系统中的流动性和资本效率方面的重要性。Merlin Chain 以 9.9% 的项目份额在扩展比特币 DeFi 功能中也发挥着关键作用。其他平台如 BOB（8.4%）、BSquared（6.9%）和 Stacks（6.1%）则为生态系统的多样性做出了贡献，而 BEVM（5.3%）、BounceBit（3.1%）和 MAP Protocol（3.1%）则通过其专业解决方案推动整体增长。



Avalon Finance 和 Colend Protocol 分别拥有 2.062 亿美元和 1.155 亿美元的 TVL，也是重要的参与者。其他值得关注的项目包括 MoneyOnChain 和 Sovryn，这些项目展现了 BTCFi 领域的多样性，从流动性挖矿到稳定币都有涉及。



2）主要BTCFi项目中的关键叙事

安全与去中心化优先：比特币的 DeFi 生态系统以安全性和去中心化为核心原则。比特币无与伦比的安全框架是 BTCFi 生态系统的基础，确保所有的创新都遵循这些基本原则。

比特币作为可编程Token：BTCFi 正在改变比特币的角色，使其不仅仅是价值存储，而是可以编程的Token。这一变化通过智能合约的使用，实现了新一代复杂金融应用的可能性。例如，Solv Protocol 的 SolvBTC 被称为“首个具有收益的比特币”，它通过收益库中的中性交易策略，以及在以太坊、Arbitrum 和 Merlin Chain 等 DeFi 协议中提供收益。

与以太坊的互操作性：BTCFi 通过与以太坊 DeFi 生态系统的 EVM 兼容解决方案建立桥梁，充分利用了两个网络的优势。这种互操作性创造了强大的协同效应，将比特币的安全性与以太坊灵活的智能合约能力结合在一起。例如，Core 通过 EVM 执行智能合约，这意味着为以太坊开发的去中心化应用（dApp）可以轻松转移到 Core 区块链，而无需进行重大修改。

解锁比特币的资本：BTCFi 生态系统正在为 DeFi 目的释放大量资本，提供收益机会，同时让用户保留比特币的投资敞口，从而扩大比特币在DeFi中的实用性和吸引力。

3）与以太坊DeFi的比较分析

随着比特币 DeFi 的不断发展，将其与以太坊 DeFi 进行比较变得越来越重要。特别是要关注比特币如何通过像 wBTC 和 renBTC 这样的包装资产在以太坊生态系统中运作，以及我们可以从以太坊的发展历程中吸取哪些经验教训。

4）以太坊DeFi VS 比特币与原生比特币DeFi

比特币与以太坊 DeFi 生态系统的整合主要通过像 wBTC 和 renBTC 这样的包装资产来实现。这些Token使比特币持有者能够将 BTC 转换为 ERC-20 Token，从而访问以太坊庞大的 DeFi 生态系统，可以在 MakerDAO、Aave 和 Uniswap 等以太坊平台上使用。

在这两个生态系统中，BTC 的使用存在显著差异。截至 9 月 8 日，锁定在以太坊 DeFi 协议中的 BTC 数量为15.34万，远远超过比特币原生 DeFi 生态系统中的0.897万。这一趋势得益于以太坊成熟且多样化的 DeFi 基础设施，提供了更广泛的金融产品，包括借代、交易和流动性挖矿。

虽然像 wBTC 这样的包装比特币 Token 可以让用户获得流动性和更高级的 DeFi 功能，但它们也依赖于托管方和跨链桥，这可能增加风险。相比之下，原生比特币 DeFi 项目虽然规模较小，但在比特币自身的安全框架内运作，避免了许多与跨链转移相关的风险。然而，比特币 DeFi 仍然处于起步阶段，提供的金融服务范围与以太坊相比依然有限。



## 06以太坊的发展对比特币的启示及反之亦然

1）比特币可以从以太坊中学习的经验：

产品多样性：以太坊在 DeFi 方面的成功很大程度上得益于它提供了各种金融产品和服务，比如DEX和合成资产。为了推动比特币 DeFi 的发展，需要扩大其产品种类，不仅限于借代和稳定币服务。开发更复杂的金融工具和互操作性解决方案，可能会吸引更多的用户。

开发者生态系统：以太坊培养了一个活跃的开发者社区，不断创新并在平台上构建新项目。比特币 DeFi 项目也可以通过促进一个更活跃的开发者生态系统，鼓励更多新协议和应用的创作，以发挥比特币的优势。

互操作性：以太坊的 DeFi 生态系统在自身内部以及与其他区块链的互操作性上表现良好。增强比特币 DeFi 与其他链（包括以太坊）的互操作性，可能为用户带来新机会，让他们能够利用这两个生态系统的优势。

2）以太坊可以从比特币中学习的经验：

安全性和去中心化：比特币对安全和去中心化的重视是无可比拟的。以太坊项目可以从比特币的保守态度中获得启示，确保在快速创新的同时不牺牲这些核心原则。这一点在以太坊向更具可扩展性的解决方案（如Layer 2）过渡时尤为重要，因为在这一过程中必须谨慎处理安全问题。

简单性和稳健性：虽然比特币的脚本功能相对简单而稳健，但灵活性不足，使得它的漏洞比以太坊复杂的智能合约要少。以太坊的开发者可以优先考虑在智能合约设计中保持简单和稳健，从而降低安全风险。

价值存储的关注：虽然以太坊以其智能合约功能著称，但比特币在价值存储方面的主导地位依然强劲。以太坊生态系统可以探索增强其价值存储功能的方法，可能通过整合更多基于比特币的资产，来吸引那些重视安全和资产保值的用户。

尽管比特币 DeFi 仍处于初期阶段，但如果借鉴以太坊成熟生态系统的经验，它有着显著的增长潜力。同时，以太坊也可以从比特币在安全性和去中心化方面的优势中学习，进一步巩固其 DeFi 产品。随着这两个生态系统的发展，它们的合作与相互学习可能推动DeFi的下一个增长阶段。

## 07挑战与机遇

随着这一领域的不断发展，必须应对技术和监管的障碍，同时技术进步和新兴增长领域也带来了显著的扩展机会。

1）技术障碍

在比特币上实现 DeFi 的发展面临许多技术挑战。首先是可扩展性，这是个主要问题，因为比特币的基础层由于区块大小和区块时间的限制，交易处理能力有限。与已经拥有多种成熟Layer 2解决方案的以太坊不同，比特币的Layer 2和侧链生态系统仍在起步阶段，这限制了能够有效支持的DeFi应用范围。

其次，互操作性也是一个重大挑战。如何在不影响安全性或去中心化的情况下，将比特币与其他区块链生态系统连接起来是相当复杂的，并且需要创新的解决方案。

2）监管顾虑

随着比特币DeFi的不断发展，预计监管审查将会加剧。政府和金融监管机构可能会对DeFi服务施加更严格的法规，特别是在 AML 和 KYC 方面。比特币的去中心化和伪匿名特性使得合规性变得复杂，可能会影响比特币DeFi的采用和发展。因此，在这些监管环境中找到平衡，对于比特币DeFi的可持续增长至关重要。

## 08未来机遇

1）技术进步

比特币DeFi有很大的技术进步空间。改进Layer 2解决方案，比如更高效和安全的侧链，以及开发更具可扩展性和互操作性的框架，可能会显著提升比特币DeFi生态系统的能力。此外，像隐秘日志合约（DLCs）和隐私保护技术（例如零知识证明）的进步，可能使得更复杂和安全的金融应用成为现实。

2）未来增长领域的预测

随着比特币DeFi生态系统的不断成熟，多个领域展现出强劲的增长潜力。预计产生收益的产品、DEX 和跨链流动性池将吸引越来越多的关注。同时，随着机构对比特币的兴趣持续增加，针对机构需求的DeFi产品，如托管解决方案、合规金融工具和比特币支持的稳定币，预计也会有更高的需求。这些发展为比特币DeFi领域的早期采用者和创新者提供了高投资回报的机会。

## 09结论

展望未来，比特币DeFi生态系统将在技术进步和不断增长的机构兴趣的推动下继续扩展。开发更具可扩展性的 Layer2 解决方案、提升互操作性，以及推出更复杂的金融产品，对于这一扩展至关重要。随着生态系统的成熟，预计产生收益的产品、DEX 和面向机构的DeFi服务将吸引大量关注和资金。

然而，这一增长也将面临挑战，特别是在应对不断变化的监管环境以及克服可扩展性和安全性相关的技术难题方面。解决这些问题对于维持比特币DeFi的增长势头和确保其长期成功至关重要。

总之，比特币DeFi的未来看起来充满希望，拥有丰富的创新和增长机会。随着生态系统的不断演变，它有潜力对整个DeFi生态产生深远的影响，并使比特币成为 DeFi 的核心参与者。