模块化叙事的演变：DeFi借贷的模块化转型

作者：YBB Capital 研究员 Ac-Core，编译：0xjs@本站

### TLDR

模块化借贷的本质不只是跨链和聚合，但跨链和聚合在模块化借贷中都发挥着重要作用。

模块化借贷利用基础层提供的安全性、共识和数据可用性，重点实现执行层和应用层的功能模块化。

模块化借贷将流程分解为几个独立的模块，例如抵押品管理、利率计算、风险评估和清算机制，各个模块通过标准化接口进行通信。

目前模块化DeFi协议的特点与OP Stack一键部署上链的逻辑类似，部署需要在协议本身之上建立模块组合，从而创造出新的金融产品和服务。

### 一、模块化的起源

模块化区块链的概念源自两份白皮书，2018 年 Mustafa Albasan 和 Vitalik Buterin 合作撰写了《数据可用性采样和欺诈证明》论文，提出了一种允许轻客户端接收和验证全节点欺诈证明的系统，并设计了一种数据可用性采样协议，以减少链上容量和安全性之间的权衡，在不损害安全性和去中心化的情况下解决区块链可扩展性问题。

随后，2019 年，Mustafa Albasan 在《Lazy Ledger》白皮书中详细介绍了一种新架构。该架构使用区块链进行排序并确保交易数据可用性，而无需处理交易执行和验证。这种新架构旨在解决现有区块链系统中的可扩展性问题，最初被称为“智能合约客户端”。智能合约的执行由该客户端上的另一个执行层执行，形成了第一个模块化数据可用性层项目 Celestia 的原型。

随着 Rollup 技术的出现，这一概念变得更加具体，遵循在链下执行智能合约并将结果作为证明上传到“客户端”执行层的逻辑。在区块链架构和新扩展技术的反思下，Celestia 应运而生，定义了“模块化区块链”的新范式。

### 二、模块化区块链的出现

模块化区块链旨在通过解耦和重构来解决区块链领域的“不可能三角”困境。简单来说，它将单体链的主要功能分解为多个层，每层专注于特定的功能，从而实现可扩展性。一般来说，单体链的基本功能可以分为以下四层：

数据可用性层：确保网络中的数据可访问和验证，包括数据存储、传输和验证功能，维护区块链网络的透明性和信任。代表性的 DA 项目包括 Celestia、Avail、EigenDA 等。以太坊和 Solana 等整体单体链也可以满足 DA 需求（比特币由于非图灵完备性，缺乏针对传统 Rollups 的良好验证解决方案，但其扩容能力正在迅速进步）。

共识层：处理节点之间的协议，以实现网络中数据和交易的一致性。通过共识算法（如 PoW 或 PoS），它验证交易并创建新区块。大多数 DA 项目也需要其共识层，通常设计用于低硬件要求和简单的验证轻节点。

执行层：处理交易并执行智能合约，包括交易验证、执行和状态更新。Layer2 项目（如 Arbitrum、Optimism、ZKsync）充当模块化区块链的执行层，通过主链验证交易的正确性并继承主链的安全性。

结算层：完成交易，确保资产转移和区块链上的永久记录。模块化结算层的主要作用是验证 Rollup 有效性证明和状态数据，其中著名的项目包括 Dymension 和 Cevmos。

早期围绕比特币提出的闪电网络、侧链等解决方案可谓“模块化先锋”，然而由于比特币的非图灵完备性，这些扩容方案进展缓慢且存在各种缺陷，并未得到广泛采用。传统区块链试图通过重构底层框架来解决三难困境，但收效甚微。为了解决这个问题，Vitalik Buterin 提出了围绕 Rollups 的改进。随着错误性证明和零知识证明的成熟，通过类似乐高的方式在以太坊上构建执行层变得现实。以太坊已经将自己的最终目标设定为以 Rollups 为中心的分层扩容之路，这种以 Rollups 为中心的升级方式有望超越以往的扩容方案，成为区块链扩容的终极解决方案。

### 三、模块化贷款的演变



### 图片来源：Legendary Quant

模块化 DeFi 借贷利用基础层提供的安全性、共识和数据可用性，专注于执行层和应用层的功能模块化，并在区块链上运行这些模块。关键的模块化部分包括：

抵押物管理模块：负责存储、管理和处理用户的抵押物，保障其安全、合规。

利率计算模块：根据市场供求、用户信用评分等因素动态调整借贷利率。

风险评估模块：评估借款人的信用风险，以决定是否批准贷款申请并确定所需的抵押金额。

清算机制模块：当借款人未能按时还款时，启动清算程序，保护平台和其他用户的利益。

模块化借贷系统需要从数据可用层获取所有必要的交易和合约数据，以实现模块之间的交互和验证。各模块的运行结果需要经过共识层的确认和记录，确保所有模块状态变化的安全性和一致性。模块化借贷的大部分逻辑都运行在执行层，通过智能合约实现各个模块的功能。借贷交易的最终结算和清算都依赖于结算层，确保借贷和清算交易的最终性。

### 3.1 核心概念

模块化设计：将借贷流程分解为多个独立模块，如抵押物管理、利率计算、风险评估、清算机制等，每个模块均可独立开发、测试和部署。

互操作性：标准化接口允许模块之间进行通信，从而可以轻松地组合不同的模块，甚至跨平台使用某些模块。

可升级性：由于每个模块都是独立的，因此可以单独升级任何模块而不会影响整个系统。此功能使系统能够快速响应市场变化和技术进步。

安全性：模块化设计可以隔离风险。例如，如果某个模块出现安全漏洞，则只需修复该模块，而不会影响整个系统。

### 3.2 关键部件

抵押品管理模块：处理抵押品的存入、提取和管理，确保用户抵押品的安全且合规。

利率计算模块：根据市场供求、借款人信用评分等因素动态调整贷款利率。

风险评估模块：评估借款人的风险，决定是否批准贷款请求以及确定所需的抵押金额。

清算机制模块：当借款人未能按时还款时，启动清算程序，确保借贷平台的资金安全。

### 3.3 优点

灵活性：可以根据需要组合不同的模块，以满足不同的贷款需求。

效率：优化每个模块的性能，提高整个系统的效率。

创新：开发人员可以通过引入新模块来增强功能，从而针对特定问题进行创新。

透明度：模块化系统提供更高的透明度，允许独立审核和验证每个模块的操作逻辑和状态。

### 3.4 跨链与聚合在模块化借贷中的作用



图片来源：跨链桥详解

模块化借贷的本质不只是跨链和聚合，虽然跨链和聚合都发挥着重要作用。模块化借贷的核心思想是通过模块化借贷流程的各个功能来增强系统的灵活性、可扩展性、安全性和创新性。跨链和聚合是实现这一核心思想的一部分，但不是全部。

跨链（互操作性）：

跨链技术：使不同区块链上的资产和功能模块能够互操作。这对于模块化借贷至关重要，因为它允许用户跨区块链转移资产并使用各种去中心化应用程序 (dApp)。

多链支持：通过支持多条区块链，借贷平台可以增强其可用性和灵活性，吸引更多用户和资产。

聚合：

聚合协议：聚合多种借贷协议和流动性池，提供统一的界面和更好的用户体验。例如，用户可以通过一个聚合平台访问多个借贷市场，以获得最佳的借贷利率。

流动性聚合：通过聚合多种流动性来源，提高资金使用效率和市场流动性。

### 3.5 模块化借贷的其他关键方面

模块化设计：

功能模块化：将借贷流程分解为独立的功能模块（如抵押品管理、利率计算、风险评估、清算机制等），各模块可独立开发、部署、升级。

标准化接口：模块通过标准化接口进行通信，确保模块之间的兼容性和互操作性。

安全和风险管理：

风险隔离：模块化设计可以将风险隔离在特定模块内，如果某个模块出现问题，不会影响整个系统。

安全审计：每个模块都可以独立审计，增强整个系统的安全性。

灵活性和可扩展性：

灵活组合：用户和开发者可以灵活组合不同的模块，满足多样化的借贷需求。

可扩展性：可以通过添加或更换模块来扩展系统的功能和性能，而无需重建整个系统。

一些成熟的 DeFi 平台，如 Aave、Compound 和 MakerDAO，也采用了模块化设计理念。例如，MakerDAO 正在转向更加去中心化的 SubDAO 模型，而 Aave 的协议由多个智能合约组成，用于处理借贷、抵押品管理、清算等。开发人员和用户可以根据需要组合这些合约，甚至可以开发新合约来扩展平台的功能。

## 四、模块化贷款项目

### 4.1 Morpho 实验室

Morpho Labs 旨在通过技术创新和优化来提升去中心化借贷市场的效率和用户体验，促进 DeFi 生态系统的增长。Morpho Labs 凭借其模块化设计和无摩擦交易机制，寻求吸引更多用户和资金进入去中心化金融领域。关键创新包括 Morpho Blue 和 Meta Morpho，它们可提高 DeFi 借贷效率和互操作性。



图片来源：Morpho Labs 官方

Morpho Blue

Morpho Blue 是 Morpho Labs 提供的借贷协议的高级版本。它旨在最大限度地减少加密资产（ERC20 和 ERC4626 代币）在以太坊虚拟机上的部署，并创建独立的借贷市场。Morpho Blue 为贷方、借款人和应用程序提供了一个无需信任的基础层，在双重许可（BUSL-1.1 和 GPLv2）下运行。一旦部署，它将永久运行在以太坊区块链上。（1）主要功能和组件包括：

抵押品：用户必须提供协议支持的抵押品才能借入资产。

清算贷款价值比（LLTV）：协议为抵押品相对于借入资产设定了最低价值要求。例如，如果比率为 90%，则借入资产的价值不得超过抵押品价值的 90%，否则头寸将被清算。

借贷：用户通过与协议交互来启动借贷流程。他们指定希望借入的资产金额并提供必要的抵押品。

利率：借款人根据协议的利率模型支付借款金额的利息。利息随时间累积，并在偿还贷款时支付。

还款：借款人可以随时偿还借入的资产和应计利息以结清贷款。一旦链上确认还款，借款人就可以从智能合约中取回其抵押品。

清算机制：为降低违约风险，协议包含清算机制。如果借入资产的价值因市场波动或应计利息而超过 LLTV，则可部分或全部清算头寸以偿还贷款和任何未偿还利息。

借贷：用户通过与协议交互、指定想要借出的资产数量并将这些资产转移到智能合约来启动借贷流程。

提取：只要市场流动性充足，贷款人可以随时提取其借出的资产和应计利息。

Morpho Blue 的一个显著特点是能够创建无需许可的交易市场，允许用户建立由贷款资产、抵押资产、LLTV、预言机和利率模型 (IRM) 组成的独立市场。每个参数都是在市场创建期间选择的，并且是不可变的，LLTV 和利率模型是从 Morpho 治理批准的一组选项中选择的。

Meta Morpho

Meta Morpho 是一种独立的元协议，旨在基于 Morpho Blue 创建 MetaMorpho Vault，实现不同 DeFi 平台和协议之间的无缝集成和互操作性。主要功能包括：

跨平台集成：允许用户跨不同的 DeFi 协议无缝转移资产和策略。

增强的互操作性：通过标准化接口和协议提供更好的互操作性，促进不同 DeFi 协议之间更顺畅的协作。

自动化管理：使用智能合约和自动化工具提高资产管理和策略执行的效率和可靠性。

流动性聚合：聚合来自不同平台的流动性，提高整体市场的流动性和效率。

### 4.2 Euler Finance



图片来源：Euler Finance Official

2024 年 2 月 22 日，借贷协议 Euler Finance 宣布即将重新启动并发布其 v2 版本。这个模块化借贷平台主要包括两个主要组件：Euler Vault Kit (EVK) 和 Ethereum Vault Connector (EVC)，旨在增强协议的灵活性和功能性。

Euler Vault 套件 (EVK)

EVK 是一个工具包，允许用户创建和管理自定义“保险库”系统。EVK 允许用户将资产存入保险库，并根据需要设置不同的策略和规则。它与 EVC 集成，允许开发人员自由构建 ERC-4626 保险库。EVK 的主要功能包括：

自定义策略：用户可以根据自己的需求和风险偏好设置不同的策略，例如特定的借贷利率和清算规则。

多资产支持：EVK 支持各种资产，允许将不同类型的加密资产存入保险库。

灵活管理：用户可灵活管理和调整保险库设置，以适应市场变化和个人需求。

安全性：EVK通过智能合约和去中心化技术提供高安全性，保证用户资产的安全。

以太坊保险库连接器 (Ethereum Vault Connector，EVC)

EVC 是一种用于连接以太坊上的 EVK 的工具。它允许用户在不同的 DeFi 协议之间无缝转移资产和策略，赋予金库超级权力以充当其他金库的抵押品，促进 ERC-4626 金库与其他智能合约之间的无缝通信。EVC 的主要功能包括：

统一互操作层：EVC 允许用户将资产从一个保险库转移到另一个保险库，无论它们是否属于同一协议。这大大提高了资产的流动性和灵活性。

策略共享：用户可以在不同的保险库之间共享和应用相同的策略，从而简化管理流程。

自动化管理：EVC 通过智能合约实现资产的自动化转移和策略的应用，降低了人工操作的复杂性。

增强流动性：通过连接不同的金库，EVC 提高了整体 DeFi 生态系统的流动性，使用户能够更有效地利用其资产。

Euler Vault Kit（EVK）和 Ethereum Vault Connector（EVC）是 Euler Finance 推出的重要功能，旨在提供更大的灵活性和管理效率。通过 EVK，用户可以创建和管理自定义金库；通过 EVC，他们可以在不同金库之间无缝转移资产和策略。这些工具增强了用户对资产的控制和管理能力，有助于提高 DeFi 生态系统的流动性和效率。

## 五、对当前模块化借贷的看法

DeFi 协议是指一系列基于区块链网络构建的去中心化应用程序 (dApp)，这些应用程序无需依赖传统金融机构即可提供借贷、交易和保险等传统金融服务。模块化 DeFi 协议将这些服务分解为独立模块，从而提高灵活性和创新性，让用户和开发人员可以混合搭配不同的功能。

目前，DeFi 主要由收益聚合器、借贷协议、衍生品和期权、保险协议等组成，这些模块可以自由组合，创造出新的金融产品和服务。但它们的本质类似于 OP Stack 的“一键上链”逻辑，模块化的 DeFi 协议需要在自己的框架内建立模块组合，创造出新的金融产品和服务。

模块化 DeFi 带来灵活性的同时，也伴随着潜在的风险。UniSwap 点燃了 DeFi 热潮，成为如今各种 DeFi 协议的“蓝图”。自成立以来，UniSwap 从未被黑客攻击过，这主要是因为它依赖于一个简单的核心不变量（tokenBalanceX \* tokenBalanceY = k）并与不可变的智能合约集成。

然而，模块化的灵活性也带来了相对的复杂性。不同 DeFi 协议之间的高度互联互通意味着，如果一个协议中的可升级合约失败，则可能引发影响其他协议的连锁反应，从而可能导致整个生态系统的系统性风险。这是一个需要考虑的重要方面。