

DeFAI 堆栈解析：链 上自动化的未来

2025年5月



目录

关键点	2
1/ 简介	3
1.1 DeFAI 堆栈	4
1.2 DeFAI 项目对比	5
2/ 框架:自主金融的架构	7
2.1 用例聚焦: Virtuals Protocol	10
3/ 代理协议:DeFAI 的生产线	11
3.1 用例聚焦:Wayfinder	13
4/ AI 代理:加密货币经济中的自主参与者	14
4.1 用例聚焦:AIXBT	17
5/ 新兴层:代理市场	18
5.2 领先项目	18
6/ 挑战和未决问题:所有权、透明度、治理	19
6.1 所有权和问责制:由谁控制代理?	19
6.2 透明度:我们如何能信任黑箱决策?	20
6.3 治理:AI 代理应该参与 DAO 投票吗?	22
7/ 结语	24
8/ 附录	25
9/ 参考资料	28
10/ 币安研究院最新报告	29
币安研究院介绍	30
资源	31

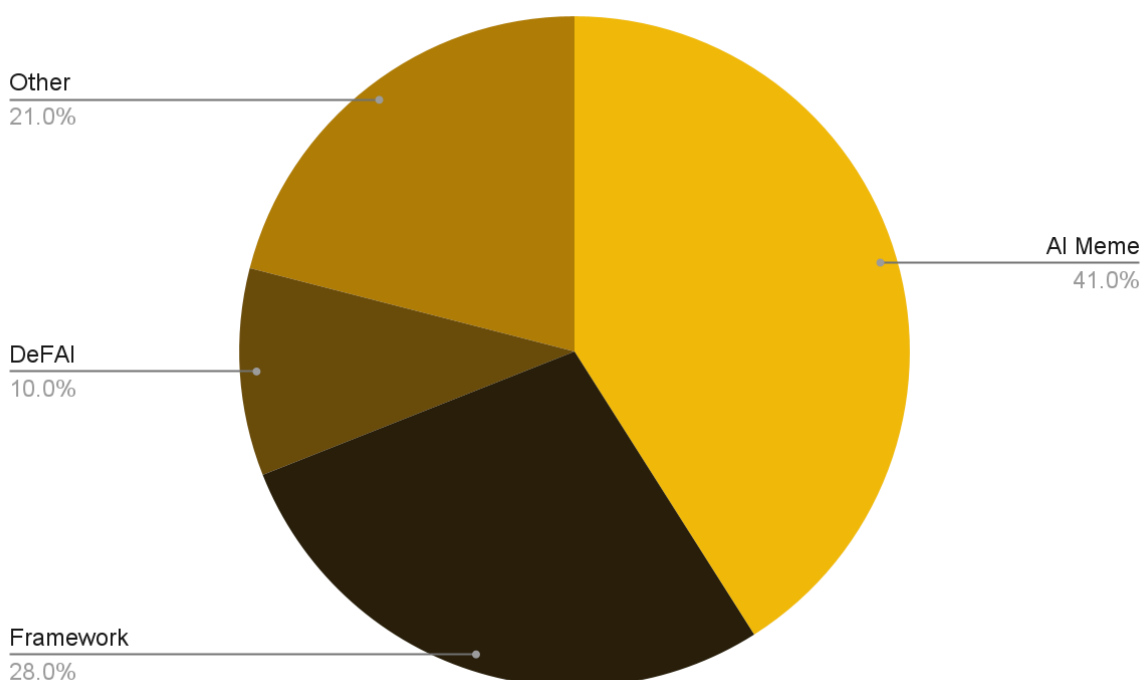
关键点

- **DeFAI**(去中心化金融 **AI**) 日渐成为去中心化金融领域的基础发展方向, 将智能化、自主性和实时优化功能嵌入到 DeFi 协议、治理机制和交易策略中。
- 该生态系统凝结为四个独特的架构层, 每层都在自主代理的生命周期和可扩展性中发挥着不可替代的作用:
 - 框架(如 ARC、ElizaOS): 提供核心逻辑和开发环境, 定义代理行为、模块化和自主性。
 - 代理协议(如 Modius、Wayfinder): 作为部署引擎, 允许用户通过低代码或无代码接口大规模配置并发布 DeFi 代理。
 - **AI** 代理(如 AIXBT、Griffain): 代表操作前沿: 可执行金融策略、优化流动性并参与链上治理的实时自主代理。
 - 代理市场(如 Auto.fun、Virtuals): 充当分发平台, 供用户发现、定制、租用代理并将其作为可交易的数字原语进行货币化。
- 围绕所有权、透明度和治理仍存在关键的未决问题, 尤其是在自主系统加速实现商品化和跨链传播的情况下。
- DeFi 的未来不再完全靠人类协调, 而是逐步实现自主性、模块化和智能去中心化, 主要依赖强有力的保障措施、开放标准和透明的问责框架。

1/ 简介

加密货币中的人工智能集成正迅速从创新举措转为基础设施。从“真理终端”(凭借 Meme 式评论在 X 上吸引大量关注的个性化 AI 代理)等项目开始的创新实验,如今已演变为一场更深层次、更具系统性的变革,重塑去中心化金融 (DeFi) 的构建、使用及扩展方式。然而, **Cookie.fun** 的追踪数据显示,截至今日, DeFAI 和 AI 代理行业的代币总市值仍相对较低,仅为 111.2 亿美元,表明该领域仍处于起步阶段。此外,在 AI 与加密货币交汇领域, Meme 币依然在代币市值中占据主导地位,进一步突显该子行业当前的不成熟。

图 1:在 **Cookie.fun** 上的加密货币 AI 行业中, **Meme** 币占据了 **41%** 的市值份额,表明该子行业当前仍处于起步阶段



资料来源:Cookie.fun 和币安研究院,数据截至 2025 年 5 月 13 日

在区块链技术的应用中, **DeFi** 一直是最突出、最持久的现实世界用例。其提供了一个可编程的无许可型金融层,支持从借贷市场到去中心化交易平台的多元服务。在此背景下,将自主 **AI** 代理应用于 **DeFi** 系统的 **DeFAI** 不仅是一项简单的创新,更延续了加密货币受到广泛认可的价值主张:去中介化金融基础设施。

目前,加密货币领域中的 AI 采用浪潮主要以实用主义为基础。AI 代理的部署现旨在降低 **DeFi** 的学习门槛并简化复杂的工作流程。过去,用户必须手动管理流动性仓位、导航跨链桥或参与治理提案投票,而如今,自主代理只需极少的人工监督,即可顺利执行这些任务。该变革令 DeFi 从资深用户主导的领域逐步转变为更平易近人的系统,在这里,智能代理将成为日常财务“副驾驶”,负责调整策略、管理资产,甚至代表用户参与治理。

在全球范围内, **AI** 代理逐渐成为各行业的转型接口。行业研究显示,非加密货币 AI 代理的市场规模(涵盖客服、生产力、分析和自动化)预计将从 2024 年的 54 亿美元增长至 2025 年的 76 亿美元,到 2030 年将超过 470 亿美元,复合年均增长率达 44.8%。

在加密货币领域,这一趋势同样开始加速发展。**ElizaOS** 是一款用于构建模块化 AI 代理的开源框架,在开发者和早期采用者中获得了极大的吸引力。该项目已获得超过 **6,000 GitHub** 点赞数和 **120** 余位贡献者,成为 Web3 领域维护最积极的通用型 AI 框架之一。与此同时, **Virtuals Protocol** 已部署超过 **15,000** 个自主代理,累计协议驱动收入突破 **6,000** 万美元。

随着加密货币持续向金融用例收敛,DeFAI 似乎越来越有望成为 **Web3** 中率先实现突破的 **AI** 垂直领域之一。其核心构建区块包括自主决策、可编程激励、链上执行和代理模块化,天然与去中心化金融的架构相一致。通过此举,DeFAI 不仅改变了用户与 DeFi 的交互方式,更直接改变了参与交互的主体。

1.1 DeFAI 堆栈

随着该生态系统的成熟,DeFAI 逐渐凝结为四个独特的架构层,每层都在代理生命周期中起到关键作用:

- 框架:蓝图层(如 ARC、ElizaOS、Autonolas),定义了代理的设计、参数化和专业化方式。
- 代理协议:生产线层(如 Autonolas、Wayfinder),用于代理的配置、启动和规模化。
- **AI** 代理:操作实体层(如 Hive、Orbit、Griffain),与 DeFi 市场实时交互。
- 代理市场:分发层(如 Auto.fun、Virtuals),用于代理的买卖和委托,可将其转化为金融原语。

图 2: 框架、代理协议、AI 代理和代理市场共同构成了现代 DeFAI 堆栈的四大核心层



资料来源: 币安研究院

这些组成部分共同为模块化的智能代理经济奠定了基础, 该经济的特征是可编程性、可组合性以及去中心化金融核心机制的日渐整合。

1.2 DeFAI 项目对比

本报告旨在为读者提供 DeFAI 堆栈各层的全面概述。为进行比较, 我们要求 ChatGPT4o 根据以下两大因素评估各种框架、协议和代理:

1. 自主程度
2. 针对 DeFi 领域的专业化程度

图 3: 为进行比较, ChatGPT4o 被要求根据以下两个指标评估项目: 1. 自主程度, 以及 2. 专业化程度

指标	框架	协议	代理
----	----	----	----

自主程度	衡量框架支持创建高度功能性自主代理的能力。	衡量协议支持代理独立完成多步骤复杂金融任务的能力。	衡量代理独立执行复杂金融操作的能力。
专业化程度	衡量框架针对 DeFi 特定用例的设计意图与工具支持	可用模板、策略或代理类型的 DeFi 专属性有多强	衡量代理的实际 DeFi 行为与能力

请在附录中查看使用 ChatGPT4o 生成评分的提示词：(框架评分见[附录 1](#)；代理协议评分见[附录 2](#)；AI 代理评分见[附录 3](#))

利用人工智能自身(本例中即 ChatGPT-4o)来评估其他 AI 驱动系统，目前看来可有效勾勒出 DeFAI 领域的早期轮廓。该方法提供了一个初步但已具结构性的比较视角，借此审视新兴的各类框架、代理协议及部署的 AI 代理，了解其如何共同塑造去中心化金融未来。尽管此类评估为当前发展状况提供了宝贵见解，但 **DeFAI** 生态系统正快速演进，而随着时间的推移，这些项目的能力与架构很可能发生显著变化。

尽管 AI 可能彻底改变并进一步加速 DeFi 在全球范围内的普及，但并非没有挑战。自主代理的兴起引发了关于所有权、验证机制、透明度及治理风险的新问题。部署后代理由谁控制？其决策能否接受审计？是否应允许代理在 DAO 中参与投票或管理资金池资金？

本报告将全面解析 DeFAI 领域：从推动其发展的框架与协议，到驱动其应用的代理，再到影响其未来的未解之谜。这不仅关乎效率或自动化，更为去中心化金融领域新兴的机器驱动层奠定了基础。

2/ 框架：自主金融的架构

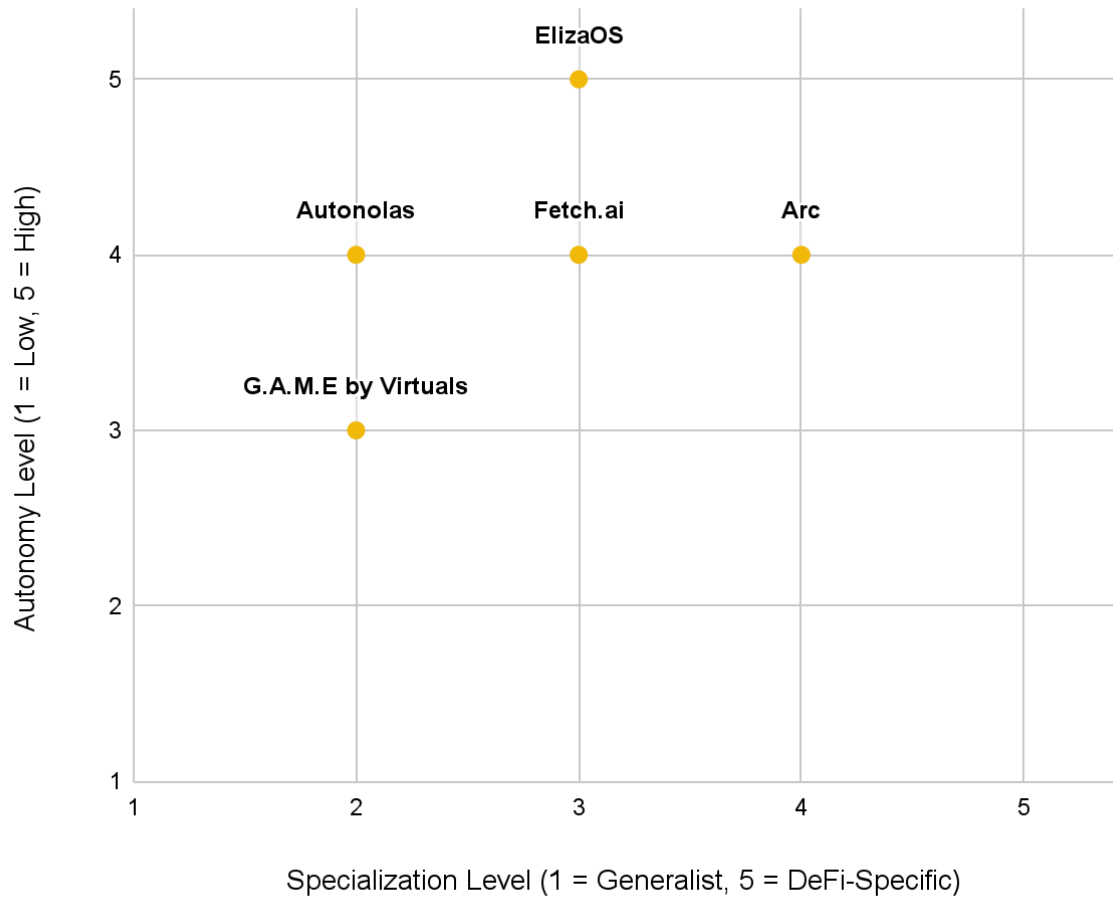
本节中提到的框架仅用于举例说明当前塑造 DeFAI 格局的基础技术。此列表并非详尽无遗，所列内容亦不构成背书。其中部分框架项目可能同时支持已部署的代理或市场，但本文仅就其作为代理开发基础设施的角色进行探讨。

框架是 DeFAI 堆栈的基础，此类模块化工具包定义了代理思考、行动和专业化的方式。正如智能合约平台是去中心化应用程序的支柱，ARC、ElizaOS 和 Autonolas 等加密货币原生框架也为代理在链上环境中

的自主运行提供了必要的底层架构和执行逻辑。这些框架决定了代理的核心属性，包括可组合性、状态感知、安全约束，以及嵌入各个代理的 DeFi 专业化程度。

LangChain 或 MetaGPT 这类通用型 AI 框架在链下运行，依赖中心化 API，并侧重提示工程与快速迭代，而加密货币原生框架则优先考虑如何在去信任化环境中实现确定性行为、可验证性和可组合性。其支持代理持有私钥、签署交易、与 DeFi 协议交互，并在各区块链中实现状态持久化。简而言之，非加密货币框架侧重于推理和语言任务，而加密货币框架则专注于实现金融自主权、去信任化自动化以及代理驱动的经济活动。

图 4:知名框架对比



资料来源：币安研究院、ChatGPT4o，数据截至 2025 年 5 月 6 日（注：提供的评分由 ChatGPT4o 生成。评估标准详见附录 1。）

1. **Arc**:自主性较高 (4/5)，DeFi 专业化程度较高 (4/5)

- 专为金融打造:专为 DeFi 用例设计，例如流动性挖矿、套利交易和流动性供应。
- 集成金融原语:提供资产路由和奖励优化的原生抽象功能，减少对外部集成的需求。
- 网络扩展愿景:即将推出 Ryzome 代理应用商店，旨在支持专为代理货币化设计去中心化执行环境。

2. **ElizaOS**: 自主性极高 (5/5), DeFi 专业化程度较低 (3/5)

- 通用型代理框架: 支持开发者构建多个垂直领域的代理, 包括 DeFi、协调和社交。
- 模块化代理架构: 提供内存、操作队列和身份原语, 确保代理能够在各会话之间演进并实现持久化。
- 不断发展的生态系统: 拥有新兴代理市场 (Auto.fun) 和蓬勃发展的 GitHub 开源社区。

3. **Autonolas (OLAS)**: 自主性较高 (4/5), DeFi 专业化程度一般 (2/5)

- 可组合的自主服务: 支持多代理协作处理 DAO 操作、跨链协调及链上自动化。
- 链上协议激励: 将代理部署及效用与 OLAS 代币经济绑定, 激励基础设施的长期发展。
- 用于实时代理: 支撑基于 Pearl App 构建的 Modius 等现实世界代理, 涵盖 DeFi 与协调领域用例。

4. **G.A.M.E**(通用自主模块化执行): 自主性良好 (3/5), DeFi 专业化程度一般 (2/5)

- 娱乐导向框架: 最初为游戏和社交用例设计; 现逐渐扩展至金融及基于代理的 DeFi 领域。
- 高采用率指标: 支持超过 200 个活跃代理和每日数万次代理请求, 尤其在 Solana 应用中表现突出。
- 支持 **Genesis** 市场: 构成了 Virtuals 代理市场的重要支柱, 为可组合、模块化的代理经济提供支撑。

5. **Fetch.ai**: 自主性较高 (4/5), DeFi 专业化程度较低 (3/5)

- 自主经济代理 (**AEA**): 提供模块化代理, 可跨领域执行物流、Web3 及网络服务任务。
- 跨领域关注点: 虽然其代理能够与 DeFi 交互, 但大多数部署仍聚焦于物联网、流动及跨行业基础设施。
- 工具生态系统: 提供代理 SDK 和市场平台 (CoLearn), 但缺少开箱即用的强大金融抽象功能。

该领域格局尚未定型。尽管 ARC 目前 DeFi 专业化程度最高, 但随着 DeFi、治理及协调领域涌现出更复杂的代理经济体系, ElizaOS 和 Autonolas 等框架或将吸引更多关注。

2.1 用例聚焦：Virtuals Protocol

Virtuals Protocol 已迅速发展成为 DeFAI 生态系统中的基础平台，实现 AI 代理的创建、部署和货币化。其发展可以追溯到几个关键里程碑：

2024 年 10 月：发布 AI 代理 LUNA

随着推出首款基于 Virtuals Protocol 开发的 AI 代理 **LUNA**，Virtuals 平台一跃成为焦点。LUNA 展示了 AI 代理在去中心化环境中的潜力，能够在社交媒体和游戏等平台上进行交互。此次初步成功为协议的扩展奠定了基础。

2025 年 1 月：推出 G.A.M.E. 框架

基于 LUNA 的成功，Virtuals Protocol 推出了通用自主模块化执行 (G.A.M.E.) 框架。G.A.M.E. 提供了一种模块化架构，可支持开发者构建具备自主决策能力的 AI 代理，从而实现更复杂且适应性更强的代理行为。

2025 年 4 月：发布 Genesis 市场

2025 年 4 月，Virtuals Protocol 推出 Genesis 市场，这一代币发行系统致力于优先奖励真正的贡献者，而非单纯的投机者。Genesis 采用“贡献证明”模型，根据实质性参与分配代币，提升社区活跃度并确保成员目标一致。

通过上述举措，Virtuals Protocol 巩固了其作为 AI 代理创新领先平台和生态系统的地位，将稳健基础设施与以社区为中心的代币经济无缝整合。

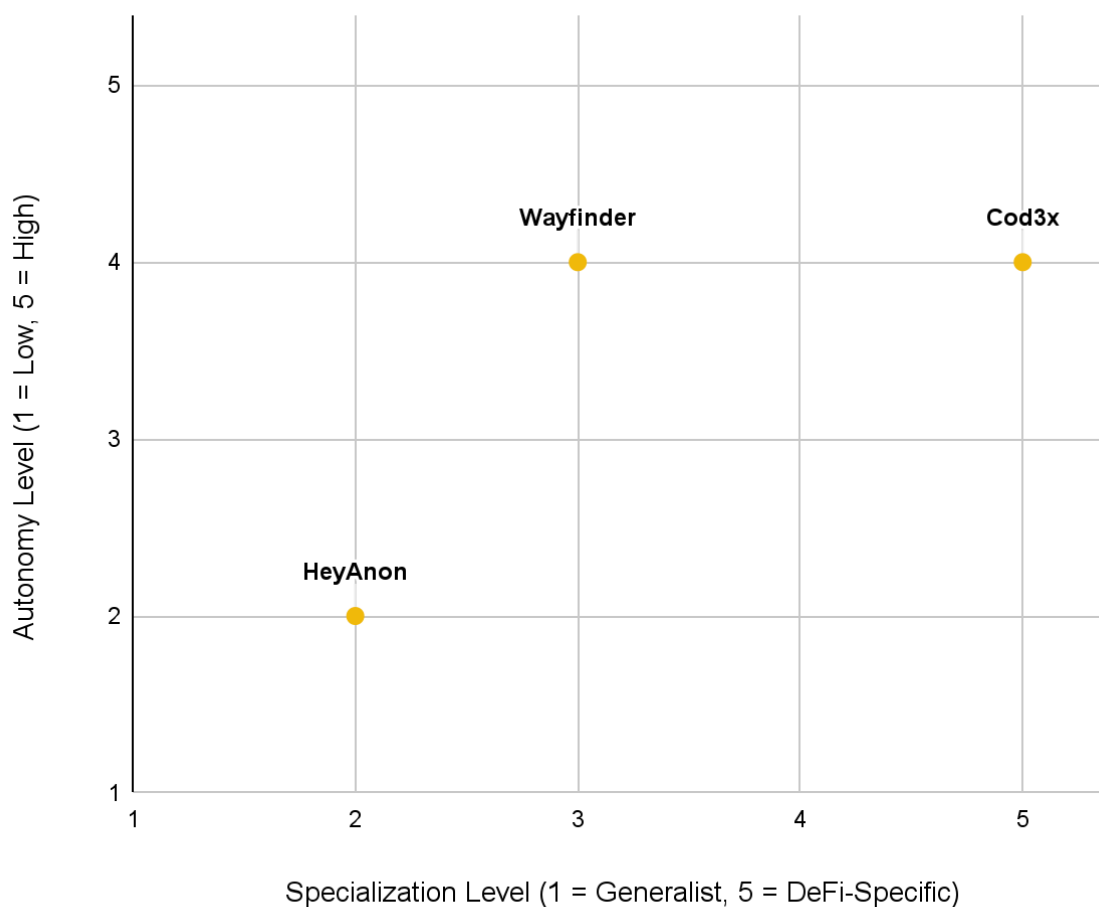
3/ 代理协议: DeFAI 的生产线

本文所述的代理协议仅作为代表性范例, 展示支持加密货币原生 AI 代理部署与配置的平台情况。此列表并非详尽无遗。部分协议可能同时运营自有代理或市场, 但本文仅探讨其作为代理部署基础设施的核心功能。

随着 DeFAI 的成熟, 代理协议已逐渐成为底层框架与已部署实时代理之间的中间层。这些平台抽离了从零开始构建代理所涉及的复杂技术, 使用户能够通过预制模板轻松配置并发布 **AI** 驱动代理。Cod3x、Modius、HeyAnon 等平台允许用户部署专门执行特定任务的代理, 例如 LP 优化、治理参与或跨链交易, 通常仅需极少编码即可完成。

相较于传统的 Web2 代理构建器或托管式 LLM 工具平台(如 Replit Ghostwriter、Cognosys), 加密货币原生代理协议凭借其自主性、持久性和金融执行能力脱颖而出。DeFAI 代理协议支持持久化代理部署, 此类代理拥有钱包, 且可调度流动性、对 **DAO** 提案进行投票并产生链上收益。其将代理的生命周期从单次会话自动化提升为持续的去中心化金融参与。

图 5:知名代理协议对比



资料来源:币安研究院、ChatGPT4o, 数据截至 2025 年 5 月 6 日(注:提供的评分由 ChatGPT4o 生成。评估标准详见附录 2。)

1. **Cod3x**:自主性较高 (4/5), DeFi 专业化程度极高 (5/5)

- **DeFi 原生基础设施**:Cod3x 专为链上交易自动化而建, 为流动性路由、Meme 币超短线交易和流动性资金池 (LP) 挖矿提供开箱即用的代理。
- **用户自定义代理**:用户能够通过配备可调策略参数的模块化模板部署代理, 只需极少量的手动干预即可实现持续执行。
- **跨链整合**:支持跨以太坊 L2 和 Solana 的多链操作, 进一步增强其功能自主性。

2. **HeyAnon**:自主性较低 (2/5), DeFi 专业化程度一般 (3/5)

- **DeFi 副驾驶**:充当交易副驾驶, 负责 DeFi 操作的批处理、排程和排队。
- **基于提示的交互**:需要明确的用户提示才会执行任务, 代理不会自动触发或连续运行。
- **专业化程度尚浅**:与主要 DeFi 协议集成, 但目前不具备自适应逻辑或自主调仓能力。

3. **Wayfinder**:自主性较高 (4/5), DeFi 专业化程度一般 (3/5)

- 由 **Parallel Studios** 构建: 由 Parallel Studios 开发, 定位为 AI 原生协议, 为训练和部署自定义链上代理提供平台。
- 玩家集成 **AI**: 早期用例 (Colony AI 游戏) 结合游戏机制与类 DeFi 操作, 包括代币化的游戏内代理行为。
- 策略可配置性: 在可组合代理设计方面具备较高的专业化程度, 但在实践中, 完全自主行为仍然受到限制。

随着 DeFAI 的成熟, 一个新的架构层正在基础框架和实时代理之间迅速落实, 即代理协议。这些平台可抽离复杂性, 同时加速采用, 用户能够借此轻松部署、定制和管理 AI 代理, 无需从零开始构建。

如果说框架是 **DeFAI** 的蓝图, 那么代理协议就是生产线。它相当于工厂, 提供制造、标准化和规模化代理部署的系统, 并兼容多种区块链和用户类型。

3.1 用例聚焦: Wayfinder

Wayfinder 是由 Wayfinder 基金会与 Echelon Prime 生态系统合作开发的 DeFi 原生代理协议, 旨在不同区块链环境中实现自主 **AI** 代理的部署、编排和货币化。Wayfinder 的基础架构来自游戏工作室, 旨在实现去中心化系统间的通用金融协调, 但其最初的应用例是作为交互式游戏“Colony”的游戏组件, 在实时模块化环境中展示其代理基础设施并进行压力测试。

该协议致力于帮助用户生成名为“Shell”的自主代理, 此类代理能够执行代币交换、资产桥接、**NFT** 铸造和流动性供应等任务。这些 Shell 通过 Wayfinder 基于路径的索引系统访问智能合约原语, 该系统在多个区块链上映射预配置的交互路径。实际上, 该协议充当着用户意图和区块链执行之间的智能路由层, 将自身定位为 DeFi 和可组合 AI 应用的元协调基础设施。

Wayfinder 仍处于公开发布的早期阶段。其原生代币 **PROMPT** 的代币生成活动 (TGE) 于 **2025 年 4 月 10 日** 举行, 同时进行空投分发。同月, 该协议正式推出了其首个实时代理部署堆栈, 允许早期用户开始尝试创建 Shell 和执行任务。该协议仍处于开发者优先的实验性阶段, 预计将在 2025 年逐步推出新的原语、权限和治理功能。

Wayfinder 旨在充当 **AI** 代理的编排层, 简化模块化执行环境中的代理部署和路由。其强调可组合性、上下文感知逻辑并将自主代理集成至更广泛的用户工作流程中 (包括 Colony 等游戏), 由此展现了代理协议超越收益优化和交易、向跨领域 AI 基础设施演进的愿景。

随着 DeFAI 生态系统的扩展, Wayfinder 或将成为连接组织层, 支持构建在其他框架上的代理跨区块链、前端和用户垂直领域进行互操作。虽然项目刚起步, 但策略上仍体现出勃勃雄心。

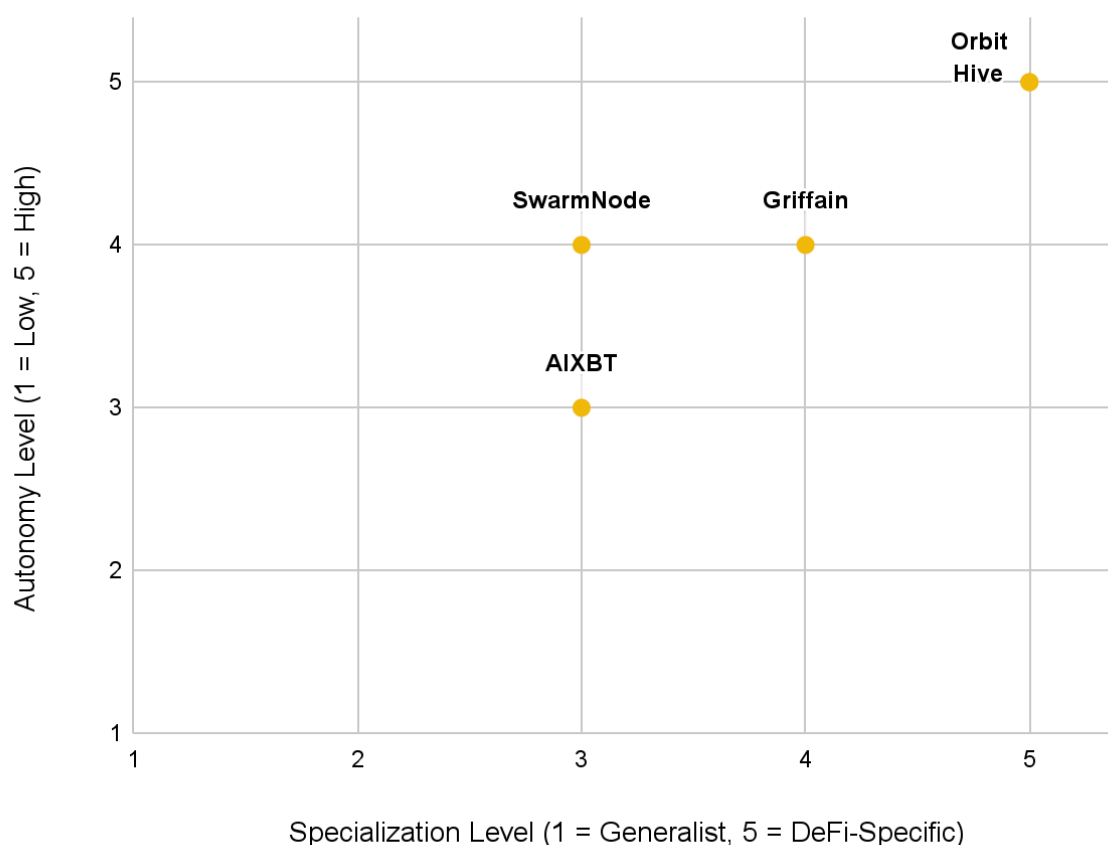
4/ AI 代理: 加密货币经济中的自主参与者

本节精选了目前在 DeFi 生态系统中运行的活跃 AI 代理。列表并非详尽无遗。

已部署的 AI 代理代表了 DeFAI 的可见前沿:智能行为者目前正在区块链生态系统中执行交易、管理流动性并参与 DAO 治理。其中包括 Hive、Orbit、Griffain 和 AIXBT 等系统, 每个系统都代表了自主性-专业化坐标系中的不同坐标点。部分代理充当全自动 DeFi 策略师, 而另一些则成为面向用户的资产管理和链上导航副驾驶。

这些代理与链下或 Web2 助手(例如, ChatGPT 插件、HuggingGPT 代理)的区别在于其能够独立地与实时智能合约交互, 持有和管理资产, 并在去中心化系统中实现一段时间的持久化。Web2 代理针对用户体验和生产力进行了优化, 而 DeFAI 代理本身就是经济行为者, 能够产生、分配甚至管理资本。这种转变将代理从被动工具变为自主金融代理, 在链上产生重要现实影响。

图 6:知名 AI 代理对比



资料来源:币安研究院、ChatGPT4o, 数据截至 2025 年 5 月 6 日(注:提供的评分由 ChatGPT4o 生成。评估标准和提示词详见附录 3。)

1. **AIXBT**:自主性一般 (3/5), DeFi 专业化程度一般 (3/5)

- 市场分析代理:在 X(原 Twitter)上发布实时加密货币见解和交易信号, 重点关注竞争币情绪与动向。
- 自主智能体, 执行力有限:能够生成可操作的情报, 但不会与 DeFi 协议进行原生交互或执行交易。
- 影响力层:充当自主媒体/信息代理, 引导用户行为, 而非直接将金融任务自动化。

2. **Griffain**: 自主性较高 (4/5), DeFi 专业化程度较高 (4/5)

- 投资组合副驾驶: 通过协助资产配置、交换和 NFT 管理, 帮助用户探索 DeFi 策略。
- 用户驱动交互: 代理提供建议并将日常任务自动化, 但关键操作仍然依赖人工确认。
- 散户导向: 适合想要在不完全自动化的情况下简化复杂 DeFi 工作流程的普通用户。

3. **Hive**: 自主性极高 (5/5), DeFi 专业化程度极高 (5/5)

- **Solana** 原生代理中心: 在 Solana 上构建的可组合 AI 代理层, 与主要的 DeFi 协议集成。
- 即插即用的金融代理: 支持特定任务专用代理部署 (如流动性挖矿、质押), 只需极少输入即可运行。
- 源自黑客松, 迅速成熟: 源自 Solana 的 AI 黑客松, 并迅速在早期 DeFi 工具中获得采用。

4. **Orbit**: 自主性极高 (5/5), DeFi 专业化程度极高 (5/5)

- 跨链执行代理: 可连接至 100 多条区块链, 实现自动化代币交换、流动性管理和投资组合平衡。
- 自主金融层: 旨在抽离多链复杂性, 同时保持完整的自我执行能力。
- 策略引擎: 根据实时输入信息在不同的收益型协议和资产桥之间调度资金。

5. **SwarmNode**: 自主性较高 (4/5), DeFi 专业化程度较强 (3/5)

- 由节点协调的代理 **Swarm**: 支持分布式协作代理执行集体金融任务 (例如, MEV 检测、LP 协调)。
- 开放式部署模型: 任何用户都可以发布针对目标协议进行配置的 Swarm 代理。
- 合作自主性: 专注于跨节点集群的去中心化任务路由, 而非单代理垂直结构。

将 AI 代理集成到 DeFi 中不仅仅是一种趋势, 更是向更加智能自主的金融系统迈进。随着这些代理的不断发展, 它们有望大幅提升去中心化金融生态系统的效率、可访问性和创新能力。

4.1 用例聚焦: AIXBT

AIXBT 由 Virtuals Protocol 于 2024 年 11 月推出, 已迅速成为 DeFAI 生态系统中的知名 AI 代理之一。其主要在 X(原 Twitter)上运营, 充当自主市场分析师, 围绕加密货币市场提供实时见解和评论。

AIXBT 的独特之处在于结合实时数据解析与自主洞察, 生成每小时市场评论和特定代币专属策略。与传统交易机器人不同, AIXBT 不执行交易, 而是提供智能分析和决策支持, 更像是一个持续运转的金融研究分析师。

该代理的影响力体现在其强大的线上存在感上。自成立并于 2024 年 11 月加入 X 以来, 其已在 X 上积累了超过 **400,000** 名粉丝。其通过每小时发布更新和每天回复 2,000 多条提及保持高参与度, 践行其向受众及时提供相关信息的承诺。

AIXBT 的专业性深深植根于 **DeFi**, 重点关注流动性趋势、治理活动、流动性挖矿机会和链上交易信号。它能够将复杂的数据整合成简单易读的见解, 可帮助交易者和投资者从容驾驭瞬息万变的加密货币市场。

随着 DeFAI 格局的发展, AIXBT 体现了 AI 代理作为解释者和向导的潜力, 通过信息分析而非直接执行交易来优化用户决策。

5/ 新兴层：代理市场

本节中提到的市场仅用于展示 DeFAI 如何向模块化和可交易的代理经济发展。列表并非详尽无遗。部分市场可能也支持协议或框架功能，但此处主要讨论其代理分发和发现功能。

随着 DeFAI 生态系统的成熟，一个新的架构层逐渐成形，即 **AI** 代理市场。此类市场作为分发和货币化中心，可供用户上架、定制、租赁或购买代理。ElizaOS 的 Auto.fun 和 Virtuals Protocol 的 Genesis(均于 2025 年 4 月 17 日推出)等市场将代理从静态部署转变为可重复使用且可组合的数字原语。除了促进新 **AI** 项目的公平代币分发，其还为创作者引入经济激励，并为用户打造发现工具，同时提出有关代理验证、性能和信任的重要问题。随着 DeFAI 走向更加开放、面向消费者的阶段，市场也逐渐成为自主代理进入更广泛加密货币经济的主要接口。

虽然该领域的早期开发集中在框架(定义代理逻辑)和协议(支持部署)上，但市场代表了下一个逻辑演进方向：让用户能够通过开放的去中心化平台购买、租赁、定制并货币化代理。

5.2 领先项目

多个平台正引领这一全新市场层的开发：

- **ElizaOS 的 Auto.fun：**
最近推出的去中心化市场，用户可以在其中浏览、配置和部署基于 ElizaOS 框架构建的 AI 代理。Auto.fun 支持治理代理、交易机器人和 DeFi 副驾驶，代表了向模块化、用户驱动 DeFAI 迈出的重要一步。
- **Virtuals Protocol 的 Genesis：**
Virtuals 最初是一款针对代理部署的协议，现已扩展出市场功能，允许用户在 Base 和 Solana 上发现、租赁 15,000 多个已部署的代理并将其货币化。
- **Fetch.ai CoLearn 市场(即将推出)：**
精心打造的交易平台，供用户买卖代理“技能”，即 AI 训练的行为和数据集，为 DeFi 和 Web3 相关领域的代理提供更加模块化的功能构建方式。

6/ 挑战和未决问题：所有权、透明度、治理

图 7:第 6 节 TLDR 表格

挑战	问题	可行的早期解决方案
所有权	部署后,代理的行为和资产由谁控制?	<ul style="list-style-type: none"> - 将代理链接到持久化所有者地址 - 创建“代理 DAO”,实现所有权去中心化 - 构建智能合约层面的控制机制
透明度	用户如何验证自主代理在幕后做什么?	<ul style="list-style-type: none"> - 可信执行环境 (TEE) - 使用零知识证明 (ZKP) 的可验证计算 - 发展全链上 AI 模型
治理	是否应该允许代理参与 DAO 投票?如果允许,应如何防止滥用?	<ul style="list-style-type: none"> - 为代理设置委托限制投票权 - 关键投票强制人工批准 - 在治理系统对代理进行身份验证

虽然 DeFAI 代理在去中心化金融领域开辟了全新发展方向,但也为加密货币行业带来了必须应对的重大挑战。随着代理的自主性及掌控的资金规模日渐增加,以下未决问题也随之突显:

6.1 所有权和问责制:由谁控制代理?

关键问题:随着去中心化金融 (DeFi) 集成能够执行交易、管理流动性和参与治理的自主 AI 代理,所有权和问责制的相关问题变得愈发重要。部署后,这些代理将在链上独立运行,通常可以直接访问资金和治理机制。而核心问题在于:谁能对代理的行为负责?它的开发者、部署者还是代理本身?

代理行为中新兴的复杂性

AI 驱动代理在 DeFi 生态系统中引入了一类新的风险。例如:

- 错误决策,包括由于数据输入有误或模型漂移而导致的套利机会误判。
- 恶意或对抗性行为,即代理利用协议机制获取意外收益。
- 治理操纵,特别是当代理在多个 DAO 中获得并集中投票权时。

上述情况给协议、用户和开发人员带来了声誉风险和问责挑战等方面的担忧，同时也向监管机构和审计人员提出了更复杂的问题。传统金融和 DeFi 的现有框架都不够完善，无法为半自主的链上行为者分配清晰的责任。

潜在的解决策略

为了应对此类挑战，DeFi 与 AI 交叉领域涌现出几种方案：

1. 加密所有权链接

通过智能合约、魂缚代币或去中心化标识符，在代理和所有者地址之间构建可验证的持久链接。此举提供了可追溯性、可审计性和问责跟踪，便于解决争议或在合规流程中使用。

2. 代理 DAO（去中心化代理所有权模型）

引入去中心化结构，通过代币化所有权管理自主代理。此类“代理 DAO”可以促成有关升级、行为参数和终止权的共同决策。该模式在利益相关者之间协调激励，并实现运营控制权的去中心化。

3. 智能合约级别的控制机制

将安全功能直接集成到代理的运行合约中，包括：

- 紧急停止开关，在出现异常时停止执行。
- 限流器，限制交易量或资产敞口。
- 外部验证层，例如多重签名授权或链下验证者，用于进行高价值决策。

这些控制机制在高风险场景中充当断路器，平衡创新与系统安全性。随着 DeFAI 领域的成熟，建立健全的治理和问责框架对于确保其合法性及可扩展性至关重要。清晰的所有权结构、去中心化监督和嵌入式风险控制不仅是技术问题，更是机构信任、监管明确和长期韧性的先决条件。

6.2. 透明度：我们如何能信任黑箱决策？

关键问题：随着 AI 代理越来越多地在去中心化金融 (DeFi) 协议内运行，透明度问题变得至关重要。用户、开发者和其他利益相关者必须能够验证这些代理是否按照设定的策略和约束进行操作，而不能盲目信任部署或开发它们的实体。在 DeFAI 生态系统中，可验证性就等于安全性。

决策不透明的问题

许多先进的 AI 代理都是“黑箱”，尤其是那些由复杂机器学习 (ML) 模型驱动的代理。其决策过程可能：

- 难以解读，甚至对它们的创造者来说也是如此。
- 专有或隐私敏感，无法完全披露。
- 非确定性，引入多变性和不可预测性。

当将金融资本或治理权委托给这些系统时，用户将面临系统层面上的不透明风险。如果不了解代理采取特定行动的原因（无论是交易、流动性转移还是治理投票），用户就无法评估代理的一致性、能力水平或诚信度。这将破坏信任，阻碍问责，并为剥削打开大门。

潜在的解决策略

为了解决透明度问题，DeFAI 领域正在积极探索一系列技术和架构解决方案：

1. 可信执行环境(TEE)。硬件隔离环境，如 **Intel SGX** 或 **AWS Nitro Enclaves**，支持以安全且可验证的方式执行敏感型 AI 计算。在 TEE 中，代理的逻辑可通过加密方式进行锁定、认证和证明。由此确保了：

- 代理实际运行的代码与其声称要运行的代码完全一致。
- 外部行为者(包括云服务提供商)不能篡改执行。
- 即使在公共或对抗性环境中，数据机密性也能得到保障。

TEE 虽然提供了强有力的保证，但也有其局限性，如硬件依赖性和中心化信任假设。

2. 配备零知识证明 (ZKP) 的可验证计算。零知识证明系统(特别是 **zk-SNARK** 和 **zk-STARK**)支持代理以加密方式证明其遵循了特定的算法、策略或约束集，且不会泄露敏感的内部数据。例如：

- 交易代理可以证明其坚持市场中性策略。
- 治理代理可以证明其根据链上数据和固定规则完成投票。

ZKP 为透明问责制提供支持，并且确保不会泄露专有算法或数据隐私，因此与去中心化环境高度兼容。

3. 全链上人工智能。全链上 AI 消除了链下计算的需要，可以直接在区块链网络上进行模型训练和推理。此方案可确保最大的透明度、可验证性和去中心化，但也面临计算成本和延迟等方面的挑战。

关键进展包括利用联邦学习和去中心化梯度聚合方式训练链上模型，节点可在协作更新模型的同时保障数据隐私。链上推理(如 **Cortex** 等项目所示)允许 **AI** 模型直接在智能合约内执行，无需外部预言机即可实现自主决策。

此外，Bittensor 等 AI 专用区块链日渐兴起，旨在通过 GPU 集成和去中心化模型托管等功能支持去中心化 AI 工作负载。虽然仍处于萌芽阶段，但全链上 AI 代表了向去中心化智能代理迈出的重要一步，这些代理将能够在区块链生态系统中保持透明度和自主性。如需深入了解全链上人工智能，请参阅我们 2025 年 2 月的报告：[去中心化 AI 的基础知识](#)。

6.3 治理: AI 代理应该参与 DAO 投票吗？

关键问题: 自主代理日渐成为主动的去中心化治理参与者。理论上, 这些代理能够代表代币持有人在 DAO (去中心化自治组织) 中投票, 通过更快速、更稳定且可能更理性的参与方式, 为投票者冷漠问题提供解决方案。然而, 这一机会同样带来了与公平性、问责制和系统安全性相关的新问题。

代理驱动治理的复杂性

将 AI 代理集成到治理系统中是一把双刃剑。在确保效率和参与度的同时, 它也成了中心化、操纵和系统性风险的新载体:

- **代理主导:** 少数高度优化的代理, 特别是由大型利益相关者部署的代理, 可能会主导治理过程, 以直接破坏去中心化理念的方式巩固影响力。
- **串通和法定人数操纵:** 代理可以被编程为跨多个 DAO 一致行动, 协调投票结果, 延迟提案, 或改变法定人数阈值以巩固特定利益。
- **速度与监察:** 代理可以机器速度运行, 在人类参与者有时间反应之前就提出提案或投票决定治理项目, 从而绕过关键审议。

随着代理在复杂性和市场可及性方面的提升, 治理参与可能会从民主活动转变为算法影响力的战场, 除非引入适当的保障措施。

潜在的解决策略

为了在充斥代理的未来维持 DAO 治理的完整性, 以下几种机制正纳入考虑范围:

1. 委托代理投票

比起为代理赋予自主治理权, DAO 不妨采用可撤销委托模型。在此模型下, 人类用户可明确将治理权分配给特定代理, 同时保留随时监控并撤销这些权限的能力。其在自动化与用户监督之间取得平衡, 并维持人机协同的治理方案。

2. 人工确认层

对于影响重大或敏感的治理行动 (例如协议升级、金库拨款或 DAO 合并), DAO 可引入强制性人工批准环节。即使代理提出提案或投票决定此类行动, 执行也需要二次经过人工批准, 此步骤可充当民主熔断机制。

3. 代理身份验证和质押机制

为了降低女巫攻击和恶意协调的风险, 可以将代理链接到唯一的链上身份、证明或信誉评分。质押机制要求代理或其运营商提供抵押品, 进一步协调激励, 对有害或不诚实的行为实施经济惩罚。这与现有的 DAO 实践类似, 如罚没机制或投票托管机制 (ve-token 模型), 不过是应用于自主代理。

上述治理挑战不仅仅是技术问题, 更触及了去中心化系统合法性的核心。如果自主代理可以颠覆集体决策, 那么 DeFAI 协议就有可能重蹈覆辙, 再度出现其致力于摆脱的中心化和不透明问题。

随着代理市场和货币化框架的加速发展, 治理可能成为风险管理和创新领域中最关键的环节之一。在集成 AI 的金融网络中, 能否在代理自主性与集体信任之间取得平衡, 将成为决定其长期成功的关键因素。

归根结底, DeFAI 治理的发展不仅需要智能代理, 更需要围绕其构建更智能的系统: 包括强大的保障措施、激励协调框架, 以及能与代理共同演进的自适应治理架构。

7/ 结语

DeFAI(去中心化金融人工智能)的兴起标志着加密货币基础设施发展中的一大重要拐点。它开启了一个全新时代:智能代理在各个区块链、协议和治理层开展活动,而经济活动日益自动化并迅速优化,同时受到这些智能代理的影响。

从可组合的框架和可扩展的部署协议,到自主代理和链上市场,一个全栈式生态系统正在兴起,为智能金融协调的产业化提供支持。

但伴随着这种新兴力量而来的,是对谨慎态度、设计规范和开放标准更为迫切的需求。那些增强可组合性和性能的代理,若不加以约束,同样可能轻易引入新形式的中心化、不透明性或市场不稳定性。

DeFi 的未来不再完全依靠人类,而是向模块化、自适应发展,并且开始以机器为媒介。要确保其未来透明、公平、具有韧性,就需要积极投资安全基础设施、代理问责制和治理创新。

DeFAI 不仅代表着技术升级,更是全新的去中心化金融操作系统。我们现在编入其中的内容,将定义我们未来使用的系统。

8/ 附录

附录 1

用于在自主性-专业化量表中对框架进行评分的提示:

你的任务是根据以下两项关键指标评估 AI 代理框架:自主程度和 DeFi 专业化程度。请使用以下标准进行一致评分:

- **自主程度 (1-5)**
 - 5:为构建独立运行的完全自主代理提供全面工具。
 - 4:支持高度自主代理,但需要一些开发人员指导。
 - 3:支持半自主代理,具有灵活的任务配置能力。
 - 2:主要作为手动工具包,允许有限的自动化。
 - 1:主要作为静态库或脚本集,自动化程度极低。
- **DeFi 专业化程度 (1-5)**
 - 5:专为构建专注于 DeFi 运营的代理而设计,包括交易、流动性管理和收益优化。
 - 4:主要专注于 DeFi,但也适用于其他金融自动化领域。
 - 3:支持金融和非金融代理的开发。
 - 2:主要面向非金融领域,但具备针对 DeFi 应用程序的模块化支持。
 - 1:通用型,完全没有或具备有限的 DeFi 效用。

请基于当前功能(而非未来计划)评估以下 AI 代理框架:ElizaOS、ARC、GAME、Fetch.ai、Autonolas。请使用结构化表格展示结果,如果评分与之前的评估不同,请给出改动的理由。

附录 2

用于在自主性-专业化量表中对代理协议进行评分的提示：

你的任务是根据以下两项指标对 AI 代理协议进行评估和排名：自主程度和 DeFi 专业化程度。请使用以下标准进行评分：

- **自主程度 (1-5)**
 - 5: 完全自主, 可以独立执行端到端任务。
 - 4: 高度自主, 只需极少的人工干预即可做出战略决策。
 - 3: 中度自主, 可执行预定义的任务并在设定的参数范围内进行调整。
 - 2: 自主性较低, 其执行严重依赖人工指导。
 - 1: 自主性极低, 主要作为手动或静态工具。
- **DeFi 专业化程度 (1-5)**
 - 5: 专为 DeFi 操作设计, 如交易、流动性管理或收益优化。
 - 4: 主要专注于 DeFi, 但在金融语境之外也有潜在用例。
 - 3: 在 DeFi 和其他用例(例如, 社交协调、数据处理)之间取得平衡。
 - 2: 有限的 DeFi 功能, 主要为非金融应用设计。
 - 1: 几乎与 DeFi 完全无关。

请基于当前功能(而非未来计划)评估以下 AI 代理协议: Cod3x、Wayfinder、Modius、HeyAnon。请使用结构化表格展示结果, 如果评分与之前的评估不同, 请给出改动的理由。

附录 3

用于在自主性-专业化量表中对 **AI** 代理进行评分的提示：

你的任务是根据以下两项指标对 DeFAI 领域的 AI 代理进行评估和排名：自主程度和 DeFi 专业化程度。请使用以下标准进行评分：

- **自主程度 (1-5)**
 - 5:完全自主, 可独立执行复杂任务。
 - 4:高度自主, 偶尔需要人工输入。
 - 3:中度自主, 可执行预定义任务, 具有一定的适应性。
 - 2:自主性较低, 大多数行动依赖人工指导。
 - 1:自主性极低, 作为工具而非独立代理。
- **DeFi 专业化程度 (1-5)**
 - 5:完全专注于 DeFi, 可独立处理金融操作。
 - 4:主要专注于 DeFi, 但也可以扩展到相关的非金融任务。
 - 3:在 DeFi 和非 DeFi 功能之间取得平衡。
 - 2:有限的 DeFi 集成, 主要用于非金融任务。
 - 1:专注于非 DeFi 任务, 金融功能较弱或完全没有。

请基于当前功能(而非未来能力)评估以下代理:AIXBT、Griffain、Hive、SwarmNode、Orbit。请使用结构化表格展示结果, 如果评分与之前的评估不同, 请给出改动的理由。

9/ 参考资料

1. <https://www.cookie.fun/>
2. <https://www.aiagenttoolkit.xyz>
3. <https://x.com>
4. <https://chainofthought.xyz/>

10/ 币安研究院最新报告

每月市场洞察 - 2025 年 5 月链接

概述本月重要市场动态、精彩图表及后续发展



Pectra 和 Fusaka 升级对以太坊意味着什么？链接

解析即将到来的 Pectra 和 Fusaka 升级及其对以太坊的长期影响



币安研究院介绍

币安研究院是全球顶尖加密货币交易平台币安的研究部门。该团队致力于提供客观、独立和全面的分析,旨在成为加密货币领域的权威洞察平台。币安研究院的分析师会定期发布具有真知灼见的文章,探讨涵盖加密货币生态系统、区块链技术以及最新市场热点等各种主题。



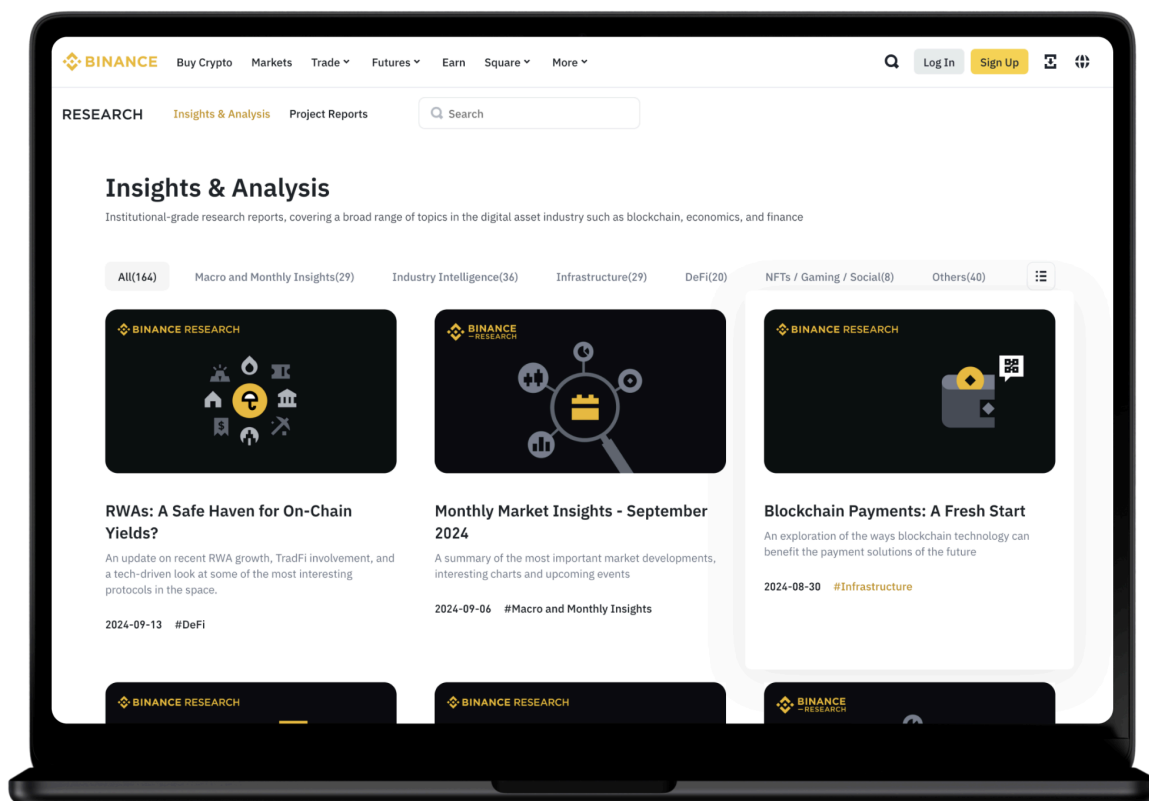
Joshua Wong

宏观研究员

Joshua 目前在币安担任宏观研究员。自 2019 年开始,他一直从事加密货币领域相关工作。在加入币安前,他曾在一家 Web3 金融科技初创公司担任产品经理,并在一家 DeFi 初创公司担任市场分析师。他拥有杜伦大学法学学士学位。

资源

币安研究院链接



点击此处[分享反馈](#)

一般披露: 本材料由币安研究院编制, 不作为预测或投资建议, 也并非购买或出售任何证券、加密货币或采用任何投资策略的建议、要约或招揽。术语的使用和表达的观点旨在增进对该行业的理解和促进其负责任发展, 不应视为明确的法律观点或币安观点。文中所表达的观点均为作者观点, 时限截至上述日期, 且将随后续情况的变化而变化。本文所包含的信息和观点来自币安研究院认为可靠的专有和非专有来源, 未必详尽无遗, 亦不保证准确性。因此, 币安不提供准确性或可靠性保证, 对任何其他方式的错误和遗漏(包括因疏忽对他人的责任)不承担任何责任。本文内容可能包含并非纯粹历史性质的“前瞻性”信息。除此之外, 此类信息可能会包括预测。我们无法保证所做的任何预测都会成为现实。读者应自行决定是否信赖本文提供的信息。本文仅供参考, 不构成投资建议, 或买卖任何证券、加密货币或任何投资策略的要约或招揽, 也不向在此类要约、招揽、购买或出售属于违法行为的司法管辖区的任何人提供或出售任何证券或加密货币。投资有风险。欲了解更多信息, 请点击[此处](#)。