AI 叙事升温 DeFi 如何从中受益？

作者：Tranks 来源：DeSpread Research

## 1. 引言

随着 IT 行业的发展，计算能力的提升和大数据的广泛应用，人工智能 (AI) 模型的性能也显著提高。近年来，AI 的能力在许多领域已经达到甚至超越了人类水平，并迅速应用于医疗、金融和教育等行业。

AI 商业化的一个典型案例是 ChatGPT，这是一款由 OpenAI 于 2022 年 11 月推出的生成式 AI 模型，能够理解并回应人类的自然语言。ChatGPT 在上线仅 5 天后便吸引了 100 万用户，并在 2 个月内达到 1 亿月活跃用户，成为历史上增长最快的消费应用。

设计和制造主要 AI 平台所需 GPU 的 NVIDIA 也从这一趋势中获益良多。在 2024 年第一季度，NVIDIA 的净利润同比增长 628% 达到 148 亿美元，股价较去年上涨约三倍，市值达到 3.2 万亿美元，表现相当出色。

AI 行业的崛起对加密市场产生了显著影响。在 2022 年 6 月，当 NFT 艺术项目正处于繁荣期时，OpenAI 开发的 AI 模型 DALL-E 2 发布，它能够根据文本生成高质量图像，这导致韩国主要加密 Telegram 频道中 AI 关键词的提及量增加了 8 倍。此外，从 2022 年下半年开始，越来越多的尝试将 AI 和区块链更直接地结合起来，AI 的提及量又增加了 2 倍。



加密社区对 AI 的浓厚兴趣也反映在与 AI 相关的加密项目的投资趋势中。根据虚拟资产统计网站 Coingecko 的数据，截至 2024 年 8 月 20 日，自 2022 年下半年开始出现结合 AI 和区块链的项目以来，277 个被归类为 AI 领域的区块链项目总市值迅速增长，达到 210 亿美元，比 Layer2 类别高出约 25%。

然而，目前受到关注的 AI 领域区块链项目主要是利用区块链技术来解决 AI 行业发展过程中暴露出的局限性。主要应用场景包括：

分布式GPU网络：这些项目利用区块链技术创建一个分布式 GPU 网络，任何人都可以贡献 GPU 算力并获得 Token 奖励，从而降低 AI 模型训练所需的高昂 GPU 成本带来的进入门槛（例如，IO.NET,Akash Network）。

去中心化的AI训练和模型开发：这些项目允许多个参与者共同参与 AI 训练和模型开发，并通过区块链技术获得 Token 奖励，旨在解决因中心化 AI 开发环境导致的 AI 偏见问题（例如，Bittensor）。

链上AI市场：这些去中心化的 AI 市场项目利用区块链技术透明地评估和交易 AI 模型或智能体的性能和可靠性，以满足各行业和特定功能对 AI 模型或智能体的需求（例如，SingularityNET,Autonolas）。

除了上述例子之外，还有许多新的尝试正在涌现，利用区块链基础设施，如去中心化数据市场和 IP 协议，来解决当前 AI 行业面临的挑战。这些尝试通过为 AI 行业提供更稳定的基础设施，并扩展区块链技术的应用范围，正在产生协同效应。

与此同时，将 AI 集成到区块链生态系统中也蕴藏着无限的发展潜力。特别是在以无许可为基础的 DeFi 服务中，通过引入 AI，可以减少对可信第三方的依赖，从而实现许多现有智能合约难以实现的功能。

在本文中，我们将探讨 AI 在当前 DeFi 协议中的具体应用实例、所面临的挑战，以及 AI 在 DeFi 中的未来发展方向。

## 2. 智能 DeFi

AI 具有卓越的实时数据分析能力，能够从大量数据中得出结论。这一特性在帮助用户执行资金操作和进行风险管理时，对具体化 DeFi 协议提供的收益和风险数据起到了重要作用。在这种情况下，AI 主要应用于 Dapp 的用户界面，使得现有 DeFi 协议无需进行重大结构调整即可利用 AI。

Yearn Finance是一个典型的例子，它是一个收益聚合器。为了给用户提供更安全的投资环境，Yearn Finance 正与 AI 智能体构建平台GIZA 合作，为其 v3 保险库建立实时策略风险评估系统。

然而，我更关注的是在 DeFi 生态系统与 AI 融合中，通过利用 AI 的自主思考和行动能力，使 DeFi 协议具备自主权的潜力。

目前的 DeFi 协议通常是被动响应用户交易的，也就是说，协议的智能合约会根据用户的互动以预设方式运行。然而，通过将 AI 融入 DeFi 协议，协议可以自主分析市场状况，做出最佳决策，并主动生成交易。这使得能够提供以往难以实现的新型金融服务的 DeFi 协议成为可能。

让我们具体看看一些在其主要运行机制中应用 AI 的智能 DeFi 协议。

### 2.1.Fyde Treasury: AI 代币基金

Fyde Treasury 是一个协议，提供一种称为 Liquid Vault 的篮子型基金服务，该服务将多个 Token 一同运作，并由 AI 来管理投资组合。用户可以接收并使用与存入 Liquid Vault 的资产相对应的流动性代币 $TRSY。

2.1.1. 资产选择和基金运作方式

Liquid Vault 的核心任务是在市场下行趋势中增加低波动性 Token 的比例，以便为用户提供较小的损失率，从而在长期内相较于其他资产类别表现出色的投资组合。

Fyde Treasury 通过以下三个步骤来选择纳入 Liquid Vault 投资组合的资产：

评估交易流动性是否充足

检查协议创始人的背景和协议代码的审计情况，以确定是否存在问题

通过 AI 分析链上数据，以评估是否存在刷量交易、Token 的集中度以及自然增长趋势等

符合这些标准的 Token 将被纳入 Liquid Vault 投资组合。此外，Fyde Treasury 在 Liquid Vault 的资产管理过程中也利用 AI，具体包括：

市场分析和预测：分析链上交易数据、市场趋势和新闻等，以预测未来的市场动向

权重计算和再平衡：根据预测的市场趋势以及投资组合中 Token 的近期表现和波动性，计算最佳的 Token 权重并进行再平衡

风险管理与响应：实时快速识别投资组合中每个 Token 的治理攻击、流动性池耗尽和特定钱包的异常交易等情况，并及时调整投资组合或隔离相关 Token

高级资产管理策略：持续评估投资组合的表现，分析策略的有效性，并从中提取数据以修改和开发新策略。然后，将现有策略与新策略进行比较测试，衡量其表现，并应用于实际运营策略中

截至撰写日期 8 月 23 日，Liquid Vault 投资组合中共有 29 个 Token，这些 Token 均为基于以太坊网络的各类行业代币。



Liquid Vault Dashboard, 来源：Fyde

此外，Fyde Treasury 提供了一项功能，使得将特定协议治理 Token 存入 Liquid Vault 的用户可以通过流动性 Token 来保持其治理投票权。用户存入 Liquid Vault 的治理 Token 会以 $gTRSY-token 的形式发送到他们的钱包中，这些 Token 可以在 Fyde Treasury 的治理选项卡中用于执行相应协议的治理投票。

不过，投票权会受到投资组合中 Token 权重的影响，因此每次调整投资组合时，投票权可能会发生变化。

2.1.2. 流动性挖矿活动

Fyde Treasury 向那些提高 $TRSY（Liquid Vault 流动性 Token）市场流动性的流动性提供者奖励 Fyde 积分，并承诺未来将根据这些积分分发其治理 Token $FYDE。

不同于其他项目通常要求用户在去中心化交易所直接存入交易对以获取 Token 或积分的流动性挖矿活动，Fyde Treasury 接受用户将 $FYDE 存入协议内部的流动性挖矿合约，并直接在Uniswapv3 上提供流动性。Uniswap v3 是一个允许用户在提供流动性时设置供应范围的去中心化交易所。

在向 Uniswap v3 提供流动性时，系统通过 AI 驱动的模拟环境来计算并执行将部分存入流动性挖矿合约的 $FYDE 转换为 $ETH 的最佳路径。此外，AI 还根据市场条件实时管理和优化 Uniswap v3 上的流动性存款范围，使得资本效率相比在一般去中心化交易所提供相同资本的流动性高出约 4 倍。



AI Simulation Dashboard, 来源：Fyde Docs

通过这种方式，Fyde Treasury 正在构建一个篮子基金。该基金利用 AI 对协议中用户存入的资产进行实时管理，从而减少人为判断，并预防市场中的各种风险。

2.1.3. 协议性能



自 2024 年 1 月推出以来，Fyde Treasury 的 TVL 稳步增长，达到并稳定在约 200 万美元。然而，由于市场自 5 月下旬以来持续疲软，$TRSY Token 在过去三个月内的回报率为 -35%。



然而，将 $TRSY 的回报与以太坊生态系统中的其他主要 Token 相比，$TRSY 的价格波动相对稳定，跌幅较小。

尽管 Fyde Treasury 推出不到一年，其 AI 模型已通过市场数据不断学习和发展。随着 AI 学习的积累和优化，未来可能会有更好的表现，因此值得关注 Fyde Treasury 的未来发展方向和表现。

### 2.2.Mozaic Finance：AI 收益优化器

Mozaic Finance 是一个使用 AI 来优化收益耕作策略的收益优化协议，通过特定的 DeFi 协议实现。它为用户提供各种 DeFi 生态系统资产管理策略，以金库形式呈现，并利用以下两种 AI 进行策略优化：

Conon：实时分析链上数据，预测市场状况和收益耕作策略的 APY 变化

Archimedes：根据 Conon 的预测数据计算最佳投资策略，并执行资金分配

在 Mozaic Finance 中，AI 智能体 Conon 担任「分析师」角色，而 Archimedes 担任「策略师」角色，共同管理用户存入的资产。

2.2.1. 金库类型

Hercules：这是一个使用稳定币进行收益耕作的金库，存款人会获得 MOZ-HER-LP Token 作为流动性 Token。

用户存入金库的资产被用于提供流动性，通过桥协议Stargate产生收益。AI 会实时将金库资产桥接并重新平衡到收益更高的流动性池中。Stargate 的特性是，即使是相同的资产，不同网络的 APY 也会因流动性差异而有所不同。



Stargate Farm Dashboard, 来源：Stargate

Theseus：这是一个通过各种波动性资产来产生收益的金库，存款人会获得 MOZ-THE-LP Token 作为流动性 Token。

用户的资产会被存入 GMX 协议的 GM 池中，这是一个去中心化的永续期货交易所，为交易者提供流动性并获得激励。在流动性部署时，会考虑每个 GM 池中交易资产的波动性和利率。根据市场情况，可能会增加稳定币的比例，并将其存入 Stargate 以产生额外的利息。



GMX GM Pool Dashboard, 来源：GMX

Perseus：这是一个积极利用 PoL（流动性证明）共识机制的金库，通过为即将上线主网的Berachain的生态系统协议提供流动性来获得网络奖励。Mozaic Finance 团队正开发并准备推出使用 Berachain 测试网的策略，详细信息将稍后公布。

关于 Berachain 和 PoL 共识机制的更多信息，请参阅文章Berachain — The Bear Catching Two Rabbits: Liquidity and Security。

与构建 Token 篮子基金的 Fyde Treasury 不同，Mozaic Finance 是一个在将用户资产存入 DeFi 协议时，通过 AI 优化流动性供应策略和流程并管理风险的协议。

截至 2024 年 1 月，Hercules 和 Theseus 金库表现良好，预期 APY 分别约为 11% 和 50%。不过，由于 Mozaic Finance 的金库发生资金被盗事件，目前两个金库均已暂停。



截至 2024 年 1 月，Hercules 和 Theseus 金库的预期年回报率，来源：@Mozaic\_Fi

2.2.2. 资金盗窃事件和 Mozaic 2.0

Mozaic Finance 于 2024 年 3 月 15 日发生了一起资金盗窃事件。当时，团队正在过渡到由Hypernative开发的新安全解决方案，以提升链上风险和安全性。在安全更新完成之前，一名内部开发人员发现可以通过使用核心团队成员的私钥来盗取金库资金。他们入侵了该成员的电脑以获取私钥，并利用该密钥盗取了约 200 万美元的金库资产，然后将这些资产转移到中心化交易所进行清算。

受此事件影响，Mozaic Finance 团队暂停了 Hercules 和 Theseus 金库的运作，治理和协议费用收集 Token $MOZ 的价值下跌了约 80%。事件发生后，Mozaic Finance 团队立即透明公布了事件进展，并与安全公司合作，追踪被盗资产的流向。同时，他们向开发人员存放被盗资产的交易所申请冻结和返还资金，努力恢复协议的正常运作。

幸运的是，目前所有被盗资金的返还工作正在进行中。在等待从中心化交易所返还被盗资金的同时，团队正在准备推出 Mozaic 2.0。新版本包括以下改进：

增强安全性：通过 Trust Security、Testmachine 和 Hypernative 等安全专业公司进行代码审计和安全增强。

AI模型改进：全面升级现有的 Archimedes 模型，并基于专家知识预测和学习尚未发生的黑天鹅事件。此外，检测异常决策并设置标志，以便进行人工审查和模型改进。

改善用户体验：改进 Dapp 的 UI/UX，并通过账户抽象和桥接服务集成，增强用户在各种链环境中对 Dapp 的访问能力。

因此，尽管 Mozaic Finance 经历了一次重大的资金盗窃危机，他们正在积极筹备推出 Mozaic 2.0，致力于为用户提供更安全和高效的资产管理服务。

## 3. 挑战：AI 的去中心化和可扩展性困境

至今，我们通过 Fyde Treasury 和 Mozaic Finance 的案例，了解到智能 DeFi 协议如何将 AI 作为 DeFi 应用的核心组件。智能 DeFi 协议通过 AI 能够带来的优势包括：

通过自主性建立新型 DeFi 协议模型

通过分析和优化资金运作方式提高资本效率

实时分析和应对异常交易等风险

目前，区块链与 AI 的整合多集中于建立区块链基础设施，以克服 AI 的局限性。然而，鉴于上述优势，预计将有更多尝试把 AI 引入 DeFi 协议。当然，在融合这两个领域的过程中，也存在需要解决的挑战。

AI 需要一个能够快速处理大量数据的环境，但当前的区块链基础设施还达不到这种数据处理速度。例如，ChatGPT-3 模型据估计需要每秒处理数万亿次数据才能回答问题，这比 Solana 的最大 TPS（每秒交易数）65,000 快了大约一千万倍。

此外，即便区块链基础设施发展到可以支持 AI 计算的程度，公共区块链的透明性仍可能会将 AI 模型的训练数据和决策权重暴露给公众。这意味着 AI 生成的交易可能会变得可预测，从而面临各种外部攻击的风险。

因此，包括 Fyde Treasury 和 Mozaic Finance 在内的希望利用 AI 的 DeFi 协议，目前选择在集中式服务器上运行 AI，并根据其结果与区块链进行交互。

然而，这种方法导致用户在协议中存入资产时，必须信任负责管理 AI 的团队的诚实性。这种情况削弱了 DeFi 通过智能合约消除对可信第三方需求，以提供无需信任的交易环境的核心原则。

在区块链中应用 AI 时，去中心化和可扩展性的问题被视为 DeFi 应用在利用 AI 过程中必须解决的挑战。而zkML（零知识机器学习）技术正作为一种解决方案受到关注。

### 3.1. zkML（零知识机器学习）

zkML 是一种将零知识证明（ZKP）与机器学习（ML）相结合的技术。零知识证明是一种加密方法，它可以在不透露数据本身的情况下验证数据的真实性，从而实现隐私保护和数据完整性验证。zkML 利用零知识证明的这些特性，应用于机器学习领域，使得在不公开输入、参数和 AI 模型内部机制的情况下，能够验证模型输出的正确性。

此外，通过设计 DeFi 协议的智能合约来验证零知识证明，仅在 AI 模型按照预期诚实运行且没有外部干扰时才生成链上交易，这样就可以安全地将 AI 集成到 DeFi 协议中。

例如，之前提到的 Mozaic Finance 计划在未来将零知识证明技术引入其协议。他们在文档中表示，这项技术将增强实时验证 Archimedes 诚实决策和管理金库的能力。

然而，零知识证明技术尚属新兴，需要大量的讨论和开发才能实现实际应用。尤其是，对于复杂的 AI 模型来说，生成零知识证明虽然比直接在区块链上执行 AI 模型更高效，但仍然需要超出当前区块链基础设施所能提供的计算能力和存储空间。因此，为了使 zkML 真正实用化，必须在零知识证明和区块链基础设施方面实现进一步的技术进步和优化。

## 4. 基于 AI 智能体的经济与身份验证

我预计，随着区块链和 AI 技术的进一步发展，它们将逐步克服实现两者融合所需的挑战。基于这一进展，我相信在不久的将来，大多数 DeFi 协议将会把 AI 整合到其运营机制中。

此外，随着 SingularityNET 和 Autonolas 等 AI 智能体部署和交易平台的出现和成熟，不仅在协议层面可以集成 AI，还为个人用户创造了一个轻松使用 AI 智能体的环境。换句话说，每个参与区块链生态系统的人都能够构建和使用为个人优化的智能 DeFi 协议。

例如，Autonolas 的 AI 智能体在 Gnosis 网络的预测市场平台Omen上，通过分析链上和链下数据进行投注，其数量和活动稳步增加。从 2023 年 7 月起的一年内，这些智能体已经产生了超过一百万笔交易。



预计未来能够全天候高效管理资本的个性化 AI 智能体数量将增加，并积极参与区块链生态系统。这将促进闲置流动性的利用和更高效的资本运作，从而大幅提升生态系统的整体流动性。最终，AI 智能体之间的交易可能成为生态系统的主要活动，形成一个以智能体为基础的新经济生态系统。

此外，随着个性化 AI 智能体模型的智能化程度不断提高，这些智能体可能会扩展其活动范围至专为「人类」设计的领域。这包括根据个人偏好定制的链上资产管理、捕捉并参与空投机会，以及参与治理活动。

因此，随着 AI 智能体越来越精确地模拟人类行为，未来将更难以区分「真实」的人类用户和 AI 智能体。为此，身份证明作为证明用户身份和独特性的机制，其重要性预计将愈发突出，特别是在那些重视人类价值和代理权的协议中。

### 4.1. 身份证明

身份证明是一种机制，通过将人类独有的特征与网络上的个人账户相结合，以验证个人的身份和独特性。当前讨论和发展中的方法主要分为两大类：

基于物理认证的方法：利用硬件设备采集独特的生物识别信息，如面部识别、指纹识别和虹膜识别等。

基于行为分析的方法：通过分析用户的社交网络图谱、声誉以及网络活动模式等，来判断账户的真实性和独特性。这种方法依赖于用户特定账户的网络活动及其与其他账户的互动。

基于行为分析的身份证明方法能够较好地保护用户隐私，并且无需使用特殊的硬件设备即可实现。然而，为了提高证明的准确性和可靠性，这种方法需要大量的网络数据。随着 AI 智能体的复杂性增加，其识别能力可能会下降，因此预计未来基于物理认证的身份证明方法将会得到更广泛的应用。

一个采用物理认证方式进行身份证明的代表性协议是Worldcoin。该项目由 OpenAI 的创始人 Sam Altman 共同创立，他也是 ChatGPT 的创造者。Worldcoin 旨在通过身份证明为全球每个人分配一个唯一的数字 ID，并向这些拥有 ID 的人分发 $WLD 代币。此举是为了研究和探索实现普遍基本收入的可能性，以应对未来因 AI 发展而导致的失业问题。

4.1.1. Worldcoin

Worldcoin 是一个基于物理认证的身份证明项目，通过使用名为 Orb 的特殊硬件来识别人类的虹膜。在完成虹膜识别后，Worldcoin 网络会为该虹膜颁发一个 World ID，并在用户的个人设备上生成一个可用于访问该 World ID 的私钥。



Worldcoin Orb, 来源：Worldcoin Whitepaper

目前，Worldcoin 网络只存储扫描虹膜数据的哈希值，这样可以防止用户的虹膜被重建或识别。当需要进行 World ID 认证时，用户的设备会生成一个零知识证明并发送到网络，从而保护用户链上活动的数据隐私。然而，由于系统只在颁发 World ID 时进行虹膜识别，仍然存在一些挑战，比如通过交易持有私钥的设备来转移 World ID，以及 AI 智能体获取私钥。为了应对这些问题，Worldcoin 正在讨论在使用 World ID 时引入生物识别验证系统，并开发基于行为分析的 AI 检测算法。

## 5. 结论

在本文中，我们探讨了随着 AI 融入区块链生态系统而涌现的新型服务协议，这些协议所面临的挑战，以及基于 AI 智能体的区块链生态系统的未来。

未来，AI 和区块链技术将继续发展并相互融合，弥补彼此的不足。通过这种融合，预计将为个人提供一个更便捷的环境，使其能轻松访问和利用 AI 和区块链技术。

尤其是在未来以 AI 智能体为核心的链上经济生态系统中，人们将无需具备深厚的金融知识即可轻松使用和提供金融服务。这将有助于大幅提升链上生态系统的流动性，并扩大金融行业的包容性。

此外，AI 和区块链不仅可以相互影响，还具有成为各行业基础设施的潜力。因此，这两项技术的发展将对整个人类社会产生深远影响，而不仅限于单个行业。

然而，AI 相关的法规，如数据隐私保护和 AI 责任问题，以及区块链相关的法规，如 Token 的证券属性，将对这些技术的未来发展方向和行业结构产生重大影响。因此，我们需要密切关注未来即将出台的 AI 和区块链行业法规。

我们最终希望，这些技术的发展能够为人类创造更好的环境，并帮助解决社会中的诸多问题。