了解 DeFi 中智能合约可升级性的利弊

作者：Liam 'Akiba' Wright，Cryptoslate；编译：白水，本站

智能合约代理可升级性允许开发人员更新已部署智能合约的逻辑，同时保留合约的状态和地址。这提供了修复错误或添加功能的灵活性，但也带来了潜在的风险。

智能合约是区块链网络上的自动执行协议，传统上一旦部署就会作为不可变代码运行。这种不变性是区块链技术信任的基石，确保合约条款不能单方面更改。然而，部署后无法修改合约可能会带来挑战，主要是在发现错误或需要改进时。

## 智能合约中的代理可升级性

代理可升级性通过引入双合约系统解决了这一限制。代理合约存储状态并持有用户资金，而单独的逻辑合约包含实际功能。代理将函数调用委托给逻辑合约，逻辑合约可以用升级版本替换，而无需更改代理的地址或干扰存储的数据。

这种方法具有显著的优势。开发人员可以修补漏洞，实现新功能并优化性能，而不会中断用户交互或需要资金迁移。包括Compound，Aave和Uniswap V3在内的主要DeFi协议都采用了可升级合约，利用这种灵活性随着时间的推移增强其平台，同时通过严格的安全措施和透明的运营相结合将自己确立为相对值得信赖的实体。

这些协议已经实施了全面的安全实践，包括彻底的审计，正式验证和持续的漏洞赏金计划。他们的智能合约是开源的，允许公众审查和验证功能。此外，他们还采用了去中心化的治理系统，代币持有者可以参与决策，从而提高透明度并降低可能损害用户的单方面变化的风险。

他们既定的业绩记录进一步增强了这些协议的可信度。他们已经成功运营了很长一段时间，管理着数十亿美元的资产。他们根据社区反馈和不断变化的市场条件不断更新和改进他们的系统。强大的监控和警报系统以及详细的事件响应计划表明了他们对安全的承诺。

此外，尽管他们处于新兴领域，但他们在监管合规方面的努力从监管机构的角度来看又增加了一层可信度。这些协议的高流动性也有助于它们抵御某些类型的攻击和市场操纵。然而，没有一个系统是完全没有风险的，用户在与任何 DeFi 协议交互时应始终保持谨慎并进行自己的尽职调查。

## 可升级智能合约的风险

修改智能合约逻辑的能力引入了新的潜在利用途径。中心化风险成为主要关注点，升级能力通常由一小群管理员或治理参与者控制。如果不与透明的 DAO 实践相结合，这种权力集中可能会与许多区块链项目的去中心化精神形成鲜明对比。

恶意升级是另一种潜在威胁。如果受到攻击或恶意行事，管理员理论上可以改变合约逻辑来窃取用户资金或操纵协议操作。虽然治理流程和安全措施旨在降低这种风险，但随着复杂的人工智能网络钓鱼诈骗的兴起，这种可能性仍然是社区内部争论的焦点。

升级过程本身的技术漏洞带来了额外的危险。升级过程中的错误可能导致资金损失、数据损坏或使合约无法运行。代理模式的复杂性增加了攻击面，可能会引入一些微妙的错误，这些错误可能在被利用之前不会被注意到。

## 如何安全地与 DeFi 交互

对于浏览 DeFi 领域的用户来说，识别和评估可升级合约变得至关重要。检查合约代码中的代理模式（例如 OpenZeppelin 的代理模式）可以揭示可升级性功能。协议文档通常会披露升级功能，但用户应该知道这些信息可能并不总是突出显示。

评估可升级合约的安全性需要仔细考虑治理结构和升级流程。升级的时间锁延迟允许用户对提议的更改做出反应。管理功能的多重签名控制可以分配权力并减少单点故障。协议团队的声誉和过往记录为评估可信度提供了额外的背景。

对于规避风险的用户，在与可升级合约交互时，可能建议限制这些系统中的暴露和长期存储大量资金。积极监控升级提案并在可能的情况下参与治理流程，使用户能够随时了解情况并可能影响协议决策。

围绕智能合约可升级性的争论反映了区块链领域创新与安全性、灵活性和不变性之间更广泛的紧张关系。虽然可升级合约为协议开发提供了强大的工具，但它们要求用户信任人类系统，而不是仅仅依赖不可变的代码。

在可升级性和安全性之间取得适当的平衡仍然是一个核心挑战。用户必须保持警惕，仔细评估与可升级系统交互的风险和好处。自主主权并非免费；安全的成本和风险由最终用户支付。在传统金融中，这些成本由银行和金融机构等中心化机构处理。正是出于这个原因，“银行级安全”是一个用来定义高端安全系统的术语。

自主托管意味着责任最终落在用户身上，而传统的对安全和风险的自由放任态度与 Web 3 不相容。

为了支持这一点，开发人员和协议团队负责实施强大的治理机制和透明的升级流程，以维护用户信任。