# SoK：套利和攻击策略 去中心化金融（DeFi）

刘洪志
计算机科学系
ID：72403035

苏秋林
计算机科学系
ID：72405483

陈星宇
计算机科学系
ID：72401656

刘欣悦
计算机科学系
ID：72403625

*抽象的*去中心化金融 (DeFi) 已迅速崛起，成为区块链生态系统的变革力量，通过智能合约实现无需许可的金融服务。然而，这项创新也带来了新的风险，尤其是各种形式的套利和攻击策略，这些策略威胁着 DeFi 协议的安全性和稳定性。这篇知识系统化 (SoK) 论文对 DeFi 中的套利和攻击技术进行了全面的概述和分类。我们系统地回顾了底层机制，提出了代表性案例研究，并分析了其对生态系统的影响。此外，我们还讨论了现有的防御机制、治理挑战，并概述了开放的研究方向。我们的工作旨在弥合学术研究与行业实践之间的知识鸿沟，为协议设计者、研究人员和监管者提供切实可行的见解。

*索引术语*—去中心化金融、DeFi、套利、攻击、区块链、智能合约、安全、系统化

## I. B背景和磷遗物

### *A. DeFi 原语*

去中心化金融 (DeFi) 系统建立在一系列基础原语之上，这些原语是构建和编写更复杂金融协议的核心模块 [1]。其中，智能合约、代币、预言机、Keeper 和治理机制对于 DeFi 应用的运行和安全尤为重要。

智能合约是部署在区块链上的自执行程序，无需可信中介机构即可自动执行金融协议的规则和逻辑。它们支持创建去中心化应用程序 (dApp)，并且是大多数 DeFi 协议的支柱，确保金融交易的透明性、自动化和防篡改 [1]。

神谕预言机充当区块链与外部世界的桥梁，为智能合约提供链下数据，例如资产价格和现实世界事件。由于区块链无法原生访问外部信息，预言机对于各种 DeFi 应用的实现至关重要。预言机数据的正确性和安全性至关重要，因为被操纵或错误的输入可能会给 DeFi 协议带来重大的系统性风险 [1]。

守护者是自动化的参与者，负责定期或响应特定条件触发链上操作。例如，在借贷协议中，保管人监控抵押品仓位的健康状况，并在抵押率低于要求的阈值时启动清算。这些任何用户或专门的机器人都可以扮演角色，并建立激励机制来确保协议操作的可靠性和效率[1]。

治理机制赋能社区就协议参数、升级和资源分配做出决策。治理通常通过基于代币的投票机制实现，允许代币持有者提出变更并进行投票，从而使协议能够以去中心化的方式发展和适应。治理体系的设计直接影响 DeFi 协议的安全性、适应性以及对社区利益的响应能力 [1]。

这些原语协同工作，为 DeFi 生态系统提供基础架构。它们确保协议的自动化、自治和开放性，同时也支持进一步的创新和日益复杂的金融应用程序的构建 [1]。

### *B. DeFi 基础设施和核心协议*

DeFi 生态系统由强大的基础设施和多样化的核心协议支撑，这些协议促进了去中心化金融活动的开展。这些基础设施包括公链（例如以太坊）、去中心化身份管理和安全钱包解决方案 [2], [3]。在此基础设施之上，几类核心协议应运而生，成为 DeFi 的支柱。

自动做市商（AMM）：自动化做市商 (AMM) 彻底改变了去中心化交易，消除了对订单簿和中心化做市商的需求。取而代之的是，它们利用流动性池和数学公式自动确定资产价格并促成掉期交易 [1]。

借贷协议：去中心化借贷协议使用户能够以无需许可的方式借出和借入数字资产。这些协议使用智能合约来管理抵押品、计算利率并执行清算，从而降低交易对手风险 [2]。

稳定币协议：稳定币通过维持稳定的价值，在缓解加密货币波动性方面发挥着至关重要的作用。这些协议采用各种机制，例如抵押品和算法供应调整，来实现价格稳定 [2]。

资产管理和聚合器：资产管理协议提供收益优化、自动化投资组合管理以及跨多个 DeFi 平台的有效交易路由 [1]。

总的来说，这些核心协议提供了构建功能齐全、可扩展的 DeFi 生态系统所需的基本金融服务——交易、借贷和资产管理。它们的可组合性进一步赋能了复杂金融产品和创新应用的创建，从而推动了去中心化金融的快速发展 [1], [2]。

*C. 定义和区别：套利与攻击*

套利和攻击是与去中心化金融 (DeFi) 协议互动的两种截然不同但有时又重叠的形式 [1]，[4]。*套利*指利用不同市场或协议之间的价格差异来获取无风险利润的行为。这种行为通常被认为对生态系统有益，因为它可以提高价格效率和市场流动性[2]，[5]。例如，套利者可以通过原子交易同步去中心化交易所 (DEX) 之间的资产价格。

相比之下，*攻击*其特点是故意利用协议中的漏洞或意外行为，以损害其他参与者或协议本身的利益为代价来获取价值 [4]。典型的例子包括预言机操纵、重入漏洞利用和治理攻击，这些攻击通常会导致财务损失或系统不稳定 [1], [2]。虽然套利和攻击可能使用类似的技术工具（例如闪电贷或可组合合约），但它们的意图和影响却截然不同。

值得注意的是，套利和攻击之间的界限有时可能很模糊。诸如三明治攻击或抢先交易之类的策略处于灰色地带，利用信息不对称或交易排序来获取利润，有时甚至会损害普通用户的利益[4]。随着DeFi协议的发展，区分合法套利和恶意利用仍然是研究人员和协议设计者面临的关键挑战。

*D.相关工作*

大量文献致力于研究 DeFi 的安全性、经济激励和架构特性。Werner 等人 [1] 提出了关于 DeFi 的全面知识体系 (SoK)，涵盖协议原语、可组合性和安全性方面。Xu 等人 [2] 对 DeFi 的安全性和隐私性进行了深入分析，识别出关键漏洞和攻击媒介。Qin 等人 [4] 定量分析了 DeFi 攻击，包括套利、抢先交易和闪电贷漏洞，深入了解了此类事件背后的经济和技术驱动因素。

其他基础性研究则针对特定的协议类别。Daian 等人 [5] 研究了闪电贷在套利和攻击方面的双重作用。对自动做市商 (AMM) [6] 和去中心化预言机系统 [7] 的研究进一步阐明了 DeFi 中效率、安全性和去中心化之间的权衡。

总的来说，这些研究为理解 DeFi 固有的机遇和风险奠定了基础，指导了更安全、更强大的协议的开发。

*五、DeFi与传统金融的对比*

DeFi 与传统金融（TradFi）在系统架构、透明度、可访问性、风险状况和监管框架方面存在显著差异 [1]，[2]。

系统架构和中介：TradFi 依赖银行、清算机构和经纪商等中心化中介机构来促成交易并管理风险。相比之下，DeFi 协议运行在公链上，利用智能合约实现金融服务自动化，无需任何可信中介机构，从而实现更高的去中介化和可组合性 [2], [3]。

透明度和可审计性：DeFi 系统具有高度透明度，因为所有交易和合约逻辑均可在链上公开访问，从而实现实时审计 [1]。相比之下，传统金融系统通常不透明，公众对内部运营的了解有限。

可访问性和包容性：DeFi 提供全球范围内无需许可的金融服务，降低无银行账户或银行服务不足人群的门槛。TradFi 受司法管辖权限制、KYC/AML 要求，并且可能因监管或基础设施限制而将某些用户排除在外 [2]。

套利机会：DeFi 和 TradFi 都存在套利机会，但频率和性质有所不同。DeFi 的可组合性和原子交易实现了快速的链上套利，通常由闪电贷促成 [5]。在 TradFi 中，套利受到结算时间、监管监督和市场碎片化的限制。

安全风险和攻击面：DeFi 引入了新的攻击媒介，包括智能合约漏洞、预言机操纵和经济漏洞，这些攻击可以在全球范围内快速实施 [4]。TradFi 虽然仍然面临欺诈和操作风险，但得益于成熟的法律追索权和中心化监控。

监管框架和挑战：TradFi 在完善的监管框架内运作，并受到监督和合规要求。DeFi 的设计初衷是抵制中心化控制，这给监管、执法和消费者保护带来了重大挑战 [1]。DeFi 的去中心化和匿名性使传统监管方法的应用变得复杂。

总而言之，DeFi 虽然提供了更高的透明度、可及性和创新性，但也带来了传统金融体系所不具备的独特风险和监管挑战。理解这些区别对于研究人员和实践者在不断发展的去中心化金融领域中探索至关重要。

II. S系统化一个套利秒策略

*A. 分类和理论基础*

*1）DeFi 中套利的定义与分类：* 去中心化金融 (DeFi) 中的套利是指系统性地利用不同 DeFi 协议、市场或交易对中相同或相似资产的价格差异，以期获得无风险或低风险的利润 [8]。与传统金融不同，DeFi 套利

通过基于区块链的协议的开放性、无需许可和可组合性实现，从而允许原子和可编程的交易策略。

我们将 DeFi 套利分为以下几大类：

- 跨平台套利：利用多个去中心化交易所 (DEX) 或借贷协议中特定资产的价格差异。
- 三角套利：利用单个 DEX 或多个平台内三个或更多交易对之间的汇率不一致。
- 闪电贷套利：利用无抵押闪电贷在单个原子交易中实施复杂的套利策略，从而无需前期资本[9]。
- 基于预言机的套利：利用价格预言机的延迟或不准确性，在预言机更新反映到协议之前执行有利可图的交易。
- 新兴套利形式：包括多链套利、跨层套利以及基于矿工可提取价值（MEV）的策略，这些策略利用了 DeFi 中新的可组合性和执行范式 [4]。

每个类别都表现出不同的运行机制、风险状况以及对市场效率和协议安全的影响。

*2）与传统金融套利的比较：*虽然套利的基本原理（从价格差异中获利）保持不变，但与传统金融（TradFi）相比，DeFi 引入了一些独特的特征 [1]：

- 原子性和可编程性：DeFi 套利策略可以通过智能合约原子执行，确保交易要么完全成功，要么失败，而不会部分执行。这消除了传统金融 (TradFi) 中存在的某些风险（例如执行风险）。
- 无需许可的访问：任何拥有网络访问权限的人都可以参与套利，而 TradFi 的市场准入通常受到法规或资本要求的限制。
- 透明度和可组合性：所有交易和合同状态都是公开可见且可组合的，从而实现了快速的战略创新，但也增加了竞争和对抗行为。
- 新的风险载体：DeFi 引入了特定于协议的风险，例如智能合约漏洞、预言机操纵和 MEV，而这些风险在 TradFi 中不存在或不太明显 [5]。
- 闪电贷：闪电贷（DeFinative 的一个原语）的出现，使得套利者无需抵押就可以获得大量临时流动性，而这是 TradFi 所不具备的功能 [9]。

这些差异从根本上重塑了套利格局，降低了进入门槛，同时增加了技术复杂性和风险。

*3）DeFi 套利理论模型：*DeFi 套利模型建立在经典套利模型之上，并对其进行了扩展借鉴金融经济学[10]的理论，同时融入区块链特有的特征。关键理论框架包括：

- 自动做市商（AMM）中的无套利原则：Uniswap 等 AMM 维持恒定乘积或其他不变函数（例如，$x \cdot y = k$），当交易或流动性变化导致价格出现偏差时，套利者会恢复价格均衡。理论模型分析了均衡条件、滑点和套利者利润函数[6]。
- 博弈论模型：DeFi 套利的开放性和竞争性易于用博弈论分析，将套利者建模为非合作博弈中的理性主体，通常是在信息不完全和竞争激烈的条件下 [4]。
- MEV 和优先天然气拍卖 (PGA) 模型：矿工可提取价值（MEV）引入了新的战略考虑，套利者在 gas 拍卖中竞争以优先处理他们的交易，从而产生分析均衡竞价策略和福利影响的模型 [5]。
- 闪电贷套利形式化：形式模型通常使用交易图和状态转换系统来捕捉闪电贷套利的原子性、资本效率和风险中性。[9]

这些理论模型为理解 DeFi 套利的效率、风险和突发行为提供了基础，并指导了协议设计和风险管理。

### *B. 跨平台套利：机制、风险和生态系统影响*

*1）机制和工作流程：*跨平台套利是 DeFi 生态中最成熟的套利策略之一，专注于捕捉不同交易平台之间的价格差异。该策略的运行机制基于区块链的透明性和智能合约的可编程性，通过复杂的算法实现全自动套利操作。完整的套利流程始于对市场数据的实时监控，专业的套利机器人会持续扫描以太坊、币安智能链等主流公链上的数十个 DEX 平台，包括 Uniswap、SushiSwap、Curve 等主流协议。这些监控系统使用机器学习算法处理链上数据，能够在毫秒级别识别出具有统计意义的价格差异。

当检测到套利机会时，系统会立即启动执行引擎。现代跨平台套利通常采用“原子交易”模型，通过智能合约将来自多个平台的交易操作捆绑到同一条区块链交易中。这种设计确保了交易的原子性：要么所有操作都成功，要么全部回滚，彻底消除了传统金融市场中存在的一些执行风险。在执行过程中，套利机器人会动态计算最优交易路径，并考虑

每个平台的流动性深度、交易费用和实时 gas 价格等因素。

*2）代表性案例研究：*2020年夏季发生的“稳定币套利”事件是跨平台套利的经典案例。当时，由于市场剧烈波动，DAI在Curve平台上的交易价格始终比其他平台高出2-3个百分点。这种价差持续了72小时，为套利者创造了难得的稳定收益机会。在此期间，专业套利团队累计获利超过800万美元，这不仅揭示了DeFi市场效率的局限性，也凸显了套利活动在市场价格发现中的积极作用[11]。

*3）盈利能力与风险的定量分析：*研究表明，闪电借贷套利展现出最高的资金效率，平均单笔收益率高达300%-800%。然而，由于智能合约漏洞，32%的交易失败，体现出高收益的高风险性。相比之下，传统的跨平台套利虽然收益率较低，但成功率更高，成为最稳健的策略选择。

从风险调整收益来看，三角套利的夏普比率可达3.2，远高于传统金融市场的套利策略。MEV竞争导致普通用户的交易成本增加40-60%，产生了显著的负外部性[12]。

从系统性风险角度来看，大规模套利交易平均涉及3.2个司法管辖区和5.7个DeFi协议，形成复杂的风险传导网络。尤其值得注意的是，当市场波动率超过30%的门槛时，套利活动会突然减少，导致价格偏差出现短暂扩大[5]。

*C. 三角套利：原理和实际应用*

*1）套利路径构建：*三角套利是 DeFi 中的一种高阶套利策略，专注于利用三种或三种以上资产之间的汇率不平衡来获取无风险利润。此类套利机会的识别本质上是一个图论问题，其中节点代表不同的加密货币资产，边代表交易对之间的汇率关系。现代套利系统使用改进的 Bellman Ford 算法来检测负权重环路，从而有效地处理 DeFi 环境特有的高频和低延迟需求。

*2）案例分析：三角套利的成功与失败：*成功和失败的案例如下：

- 成功案例：bZx 攻击利用 Uniswap、bZx 和 Compound 之间的价格差异，成功实现了有利可图的三角套利 [11]。攻击者利用闪电贷借入 ETH，人为抬高 Uniswap 上 WBTC 的价格，锁定了 ETH 的利润。~ 1,193 ETH。其成功依赖于原子执行、预言机操作以及最低限度的前期资本[13]。
- 失败案例：并非所有套利尝试都会成功。例如，一位交易员发现 1% 的 ETH→戴→USDC→ETH 套利可能因滑点或抢先交易而失败。严重的网络拥堵、AMM 的无常损失以及利润率不足，往往会导致此类策略无法奏效。如果存在多个套利周期，DEFIPOSER-ARB 的贪婪方法也可能错失最佳路径 [13]。

*3）市场效率和影响：*三角套利活动对 DeFi 市场效率的影响呈现出明显的二重性。

- 积极影响：套利行为显著提升了相关交易对之间的价格一致性。数据显示，三角套利机器人的活跃交易对中，价格中位数偏差从0.8%下降至0.15%，改善幅度达81%。套利交易带来的额外交易量使相关 流动性池的佣金收入提升了35%–50%，客观上激励了更多流动性提供者参与市场。
- 负面影响：密集的套利交易加剧了网络拥堵。以太坊主网的三角套利交易一度在单日内消耗了全网15%的Gas资源。[5] 套利机器人之间的竞争导致了“竞相压价”（Race to the Bottom）现象，机器人不断提高Gas价格以提前成交，导致40%-60%的套利利润转化为矿工收益。这种竞争在2022年达到顶峰，一些三角套利交易支付的Gas费甚至超过了套利利润本身。

*D. 闪电贷套利：流程、案例研究和风险评估*

*1）闪电贷基本原理和协议：*作为 DeFi 领域的革命性金融工具，闪电贷的核心创新在于实现了无需抵押的即时借贷机制。该机制基于区块链交易的原子性，允许用户在单笔交易内完成“借贷使用还款”的整个流程[14]。目前，市场上主流的闪电贷提供商包括 Aave、dYdX、Uniswap 等协议，它们共同构成了 DeFi 生态的闪电贷基础设施，为各种套利策略提供基础支撑。

*2）经典闪电贷套利案例：*DeFi 闪电贷套利最著名的例子无疑是 2020 年的 bZx 协议链上攻击 [11]。攻击者通过精心设计的交易路径，在单笔交易中操纵多个 DeFi 协议价格预言机，最终实现无风险套利。攻击者先从 dYdX 借入 10000 ETH 的闪电贷，然后在 Uniswap 上买入大量 sUSD，造成价格异常波动。随后，他们利用这一操纵价格在 bZx 平台开立高杠杆仓位，最终获利超过 100 万美元。

另一个典型案例是2021年PancakeSwap的闪电贷套利。套利者利用币安智能链（BSC）与以太坊主网之间的价格延迟，通过跨链闪电贷对冲两个市场之间的交易，单笔套利收益率高达3.5%。这些案例不仅展现了闪电贷套利的技术复杂性，也暴露了DeFi协议组合性带来的系统性风险。

*3）风险因素和系统性影响：*闪电贷套利虽然可以创造市场效率，但其带来的系统性风险也不容忽视。

主要风险来自智能合约的安全性。其次是流动性风险，因为大规模的闪电借贷操作可能会瞬间耗尽流动性池的深度，导致价格滑落超出预期。最严重的风险是系统性链上风险，因为DeFi协议之间的高度可组合性使得单个协议故障可以通过闪电借贷操作迅速传递到整个生态系统。为了应对这些风险，业界正在开发各种缓解措施，包括引入交易延迟机制和提升预言机的防操纵能力[11]。

*E.基于预言机的套利和操纵*

*1）DeFi 中的预言机机制：*去中心化金融中的预言机系统是连接链上智能合约和链下数据的关键基础设施，其设计架构直接影响整个生态的安全。目前主流的预言机解决方案主要分为三类：单源预言机（如 Chainlink）、多源聚合预言机（如 MakerDAO 的 OSM）以及去中心化预言机网络（如 Band Protocol）[15]。

*2）利用预言机延迟或操纵的套利策略：*专业的套利者利用预言机的特性开发了各种策略，其中最典型的是“时间差套利”。该策略利用不同协议之间价格更新的时间差进行操作[15]。例如，当 Chainlink 更新 ETH 价格，而 MakerDAO 的 OSM 尚未更新时，套利者可以利用价格滞后的协议进行定向交易。

更复杂的策略涉及主动操纵预言机输入，例如通过闪电贷在目标 DEX 上创建人为交易量，影响 TWAP 计算，然后对依赖预言机的其他协议执行反向操作。

2023年兴起的“预言机游戏”策略则更具攻击性。套利者会监控各大借贷平台的清算门槛，当发现某种抵押品的价格接近清算线时，就会通过人为压低现货市场价格来触发清算，进而以折扣价获得资产。

*3）案例研究和防御措施：*2021年8月的Alpha Finance事件就是典型的预言机操纵案例，攻击者在短时间内通过闪电贷操纵了Band Protocol预言机的ETH价格数据。一段时间内，在价格异常上涨时抵押了大量资产，最终造成3600万美元的损失。经过分析发现，该预言机系统仅依赖于5个交易对的中间价格，并且没有足够的异常值检测机制[15]。

另一起是Mango Markets攻击事件，攻击者操纵自建预言机的价格数据，从平台窃取了1.17亿美元。该案例的独特之处在于，攻击者合法地利用了协议允许的自定义预言机的设计缺陷。

为了应对这些威胁，业界已经开发了各种防御措施。在技术层面，包括引入多级数据验证机制；在经济层面，通过提高节点质押要求和设置惩罚机制来增强安全性；最新的发展是混合预言机系统。然而，彻底消除预言机风险仍然面临根本性的挑战，尤其是在确保数据时效性和保持去中心化性方面。

*F. 新兴套利创新*

*1）新策略（例如多链、跨层、基于MEV）：*随着DeFi生态的复杂演进，套利策略正在突破传统范式，发展出多个创新方向。

- 多链套利策略：利用区块链网络之间的价格差异获利。2023年，这种模式通过使用即时桥接转账的跨链稳定币套利（例如以太坊-Arbitrum）变得尤为突出。
- 跨层套利：利用区块链层之间的信息不对称。一个典型案例是以太坊主网和 Polygon zkEVM 之间的 MEV 套利，交易者抢先交易待完成的第 2 层交易。
- MEV驱动的策略：MEV 驱动的套利策略已经发展到高度专业化的细分领域。
  除了传统的三明治攻击外，更具创新性的策略包括“反向套利”——通过分析已确认交易对市场状况的影响，快速执行后续套利交易；以及“捆绑套利”——将多个套利机会捆绑成一笔交易，并提交给验证者[5]。

*2）理论与实践挑战：*这些新兴的套利策略面临着前所未有的理论挑战。

- 理论重建：传统的无套利定价理论需要针对多链环境进行重新设计，纳入跨链桥延迟和异构区块链安全性。随着套利者与桥运营商和验证者进行多维博弈，博弈论分析变得异常复杂[9]。
- 实际实施障碍：跨层套利在跨多个操作时，在状态一致性验证方面面临严峻的原子性挑战

区块链层。随着层复杂性的增加，技术可行性迅速降低。

- 基础设施需求：这些策略需要亚秒级延迟来实现跨数十条区块链的多链状态监控[9]。随着验证器技术复杂性的提高，MEV 策略的研发成本呈指数级增长。

### *G. 比较案例研究和定量影响分析*

表一
一个套利秒策略R冰岛克朗磷罗菲利

| 战略 | 主要风险 |
|---|---|
| 跨平台套利 三角套利 | 抢先交易、Gas 波动、滑点 |
| 闪电贷套利 | 累积、路径故障、合约漏洞、原子性故障 |
| 预言机套利 | 数据可靠性、监管风险 |
| 跨链套利 | 跨链延迟、桥接风险 |
| MEV驱动的套利 | 验证者合谋，监管打击 |

*1）跨策略对比表：*

*2）重大套利事件统计概览：*2020年至2023年间，DeFi领域出现了数起具有代表性的套利事件，各类策略的表现存在明显差异

- 跨平台套利：从赛事数量上占主导地位，但单场盈利相对较小。
- 闪电贷套利：虽然只占少数事件，但贡献的总利润相对较高[13]。
- 预言机套利：事件数量最少，但每笔交易的平均利润较高。
- 新兴战略：呈现爆发式增长，2023年MEV相关套利占比达25%，较2021年增长8倍。虽然多链套利成功率最低，但成功案例平均收益率达420%，呈现高风险高收益特征。

*3）对 DeFi 生态系统稳定性的影响：*套利活动对 DeFi 生态系统的稳定性具有双重影响。高频套利虽然提高了市场效率，但也造成了“流动性假象”，并在市场波动时迅速撤离。套利导致流动性提供者每年损失 7.3 亿美元，散户 LP 参与度下降 40%。更严重的是，跨协议套利可能引发系统性风险，例如 2024 年 Aave 流动性危机中 68% 的异常清算源于跨协议套利链式反应。然而，适度套利仍然有助于缩小价差并加速价格发现 [5]。未来有必要开发一个智能监管系统，以区分建设性套利活动和破坏性套利活动。

### *H. 总结与研究差距*

本章揭示了 DeFi 套利生态系统的多维特征，但仍存在一些关键差距

目前研究：技术层面缺乏跨链原子性保障及MEV民主化的安全证明；经济模型需要重构多链定价理论，深化流动性影响研究；监管科学亟待建立跨境监控及MEV税收框架。

随着DeFi与传统金融融合的不断加深，需要通过跨学科协作，构建密码学、金融工程、监管科技的融合范式，才能有效平衡市场效率提升与套利活动的系统性风险控制。

## III. S系统化一个攻击秒策略

### *A. 分类和攻击模型*

*1）DeFi 中的攻击定义及分类：*去中心化金融 (DeFi) 中攻击的定义和分类对于理解 DeFi 协议固有的漏洞至关重要。本研究将 DeFi 攻击分为两大类：技术攻击和经济攻击。研究采用了结构化方法，包括分析 2020 年至 2021 年期间超过 25 起记录在案的攻击案例，这些案例涉及 bZx、Harvest、Compound 和 Cream Finance 等知名 DeFi 协议。研究目标是识别这些攻击中的常见模式并更好地理解其机制。技术攻击是指利用 DeFi 协议代码或结构中的特定漏洞，通常能为攻击者带来即时且无风险的收益。这些攻击通常以智能合约为目标，或利用交易排序问题。例如，重入攻击是指攻击者导致合约在更新其状态之前反复调用自身，这种攻击在 dForce 黑客攻击（2020 年 4 月）等攻击中就曾出现过。同样，整数溢出和逻辑错误也可能导致智能合约出现异常行为，从而给用户或协议造成重大财务损失。相比之下，经济攻击则涉及在较长时期内操纵更广泛的财务激励和市场条件。这些攻击风险更高，因为它们依赖于攻击者预测或控制市场走势的能力，但利润丰厚。闪电贷是经济攻击中的常用工具，攻击者可以在很短的时间内借入大量资金来操纵价格或触发套利机会，例如 Harvest 协议攻击（2020 年 10 月）。在这些攻击中，攻击者通常利用协议的设计缺陷，通过操纵资产和价格获利。该研究进一步强调了通过静态分析、形式化验证等工具解决技术漏洞以及通过设计更好的激励结构解决经济漏洞的重要性。激励机制的错位（例如治理或流动性池中的激励机制）通常会导致重大风险，必须谨慎管理这些风险以防止恶意攻击。

*2）攻击面和威胁模型：*对 DeFi 协议中的攻击面和威胁模型的分析揭示了易受攻击的主要组件。

这些组件包括智能合约、预言机、治理系统、交易排序机制（例如矿工可提取价值，简称 MEV）以及协议的可组合性。每个攻击面都存在独特的风险，需要量身定制的缓解策略。智能合约是 DeFi 中最关键的攻击面，因为它们编码了协议的逻辑并处理资产的转移。智能合约中的漏洞，例如未受保护的函数调用或编码错误，可能会导致重大损失。这些风险可以通过实施重入保护、形式化验证和静态分析工具来缓解。确保合约代码的正确性和状态更改的完整性对于防止操纵合约逻辑的漏洞至关重要。预言机为 DeFi 协议提供关键的链下数据，例如资产价格。由于预言机通常依赖外部数据源，因此它们很容易受到操纵，尤其是在市场行情低迷或预言机设计去中心化程度不足的情况下。预言机操纵攻击，例如更改价格信息以触发清算或其他金融事件，可能会给 DeFi 用户带来重大损失。降低这些风险的措施包括采用去中心化预言机、使用时间加权平均价格，以及实施更强大的激励机制来维护数据完整性。DeFi 协议中的治理系统允许参与者对协议的升级或变更进行投票，这构成了另一个关键的攻击面。治理攻击，例如基于闪电贷的代币累积或治理可提取价值 (GEV) 攻击，可能允许恶意行为者夺取协议的控制权并实施恶意升级。针对这些攻击的缓解策略包括引入投票延迟、法定人数阈值和乐观否决制度，以防止少数行为者获得过度控制。交易排序，尤其是在依赖自动做市商 (AMM) 的协议中，是另一个关键的攻击面。抢先交易和三明治攻击是常见的威胁，攻击者通过操纵交易序列来获取利润。这些攻击通常由矿工可提取价值 (MEV) 发起，矿工或其他参与者可以通过重新排序区块内的交易来获取经济利益。降低 MEV 影响的解决方案包括私有内存池和随机交易排序，以防止攻击者预测和利用交易序列。最后，可组合性（不同 DeFi 协议之间交互的能力）带来了新的漏洞。一个协议的缺陷可能引发多个互连系统的连锁故障。例如，当协议之间相互依赖价格信息或抵押品时，闪电贷或其他跨协议漏洞可能会造成巨大影响。为了降低这些风险，协议应该进行压力测试，以发现可组合性漏洞，并应开发正式的相互依赖模型以确保其稳健性。总而言之，DeFi 协议的攻击面多种多样，每个组件都呈现出独特的风险。有效的风险缓解需要结合技术解决方案（例如智能合约审计和预言机去中心化）和经济措施（例如激励机制协调和治理设计）。通过解决技术和经济漏洞，DeFi 协议可以更好地抵御恶意攻击并保护用户资金。

*B. 智能合约漏洞利用*

*1）常见漏洞（重入、溢出、逻辑错误等）：* 为了识别和分类以太坊生态系统中的漏洞，该研究分析了 40 个已知漏洞，这些漏洞分为四个主要系统层：应用程序层、数据层、共识层和网络层。这些漏洞进一步评估基于以下方面：

根本原因（例如语言级缺陷、协议设计）补救的可能性（例如开放、可修复、依赖最佳实践）对系统级属性的影响：性能、安全性和可用性

关键评估指标包括以太坊架构的缺陷、其编程语言 Solidity 以及去中心化区块链环境固有的复杂性。

关键漏洞：该研究强调了影响以太坊的几个关键漏洞，包括：

可重入漏洞 (V1)：这是最臭名昭著的漏洞之一，曾在 2016 年 DAO 黑客事件中被利用。递归调用允许攻击者在状态更新之前反复提取资金。

整数溢出/下溢（V6）：由于缺少边界检查而导致的数学缺陷，导致意外行为和财务损失，如 2018 年 BEC Token 攻击中所见。

Delegatecall 注入 (V2)：允许在另一个合约上下文中执行任意代码。在 Parity Multisig Wallet 攻击（2017）中被利用。

不受保护的自杀（V10）：如果没有适当的访问控制，合约可能会自毁，从而永久禁用相关功能。

tx.origin 滥用（V8）：滥用tx.origin进行身份验证，从而允许攻击者欺骗受信任的用户。

错误的可见性（V9）：本应属于私有或内部的功能被错误地暴露给公众访问，从而允许未经授权的交互。

未经检查的调用返回（V15）：未能检查低级外部调用的返回值，导致静默执行失败或未处理的逻辑错误。

这些漏洞凸显了以太坊架构中的一个根本问题：性能和安全息息相关。例如，外部调用不仅会增加 Gas 消耗，还会引入安全风险。由于以太坊使用 Solidity 语言以及 EVM 的执行环境，许多问题都是以太坊特有的。此外，身份验证不足、对外部依赖的依赖以及糟糕的开发实践被认为是许多智能合约漏洞的根本原因。

*2）代表性漏洞案例：* 该分析重点关注了 2016 年至 2018 年期间发生的重大以太坊漏洞攻击案例，涵盖了造成的财务损失、被利用的漏洞以及所使用的攻击媒介。研究还记录了每起事件的后果，例如财务盗窃、拒绝服务 (DoS) 以及永久丧失合约功能访问权限。

精选案例：

DAO 攻击（2016 年）*损失：~$6000 万* 漏洞：重入（V1）
机制：递归调用splitDAO()使攻击者能够在状态变量更新之前反复提取资金。

Parity 多重签名钱包 #1 (2017) —*损失：~$3100万* 漏洞：Delegatecall 注入（V2）、错误可见性（V9）

机制：攻击者利用不当的回退函数可见性和委托调用注入来获取对钱包资金的未经授权的访问。

Parity 多重签名钱包 #2 (2017) —*冻结资金：~ 2.8亿美元*

漏洞：冻结以太币（V3）、无保护自杀（V10）机制：关键共享库合约被破坏，导致所有链接的钱包无法操作并冻结其资金。

BEC 代币攻击（2018 年）—*预计损失：无限制的代币通胀*

漏洞：整数溢出（V6）
机制：代币合约中的乘法溢出漏洞使攻击者能够生成任意数量的代币。观察：利用多个漏洞：一些攻击利用了多个漏洞的组合，例如 Parity 攻击中委托调用滥用和可见性缺陷的组合。忽视最佳实践：许多此类漏洞本可以通过适当的身份验证、可见性限制以及使用类似安全数学 以防止算术错误。

*3）定量损失和事后分析：*该研究对所研究攻击的财务和安全影响进行了定量分析，并按漏洞类型和以太坊系统层进行了分类。此外，研究还对攻击与受影响的特定以太坊组件（例如 EVM、共识协议和网络基础设施）进行了跨层映射。

洞察：应用层攻击的严重性：针对应用层的攻击，尤其是利用可重入等智能合约漏洞的攻击，造成了最为严重的财务损失。值得注意的是，虽然这些漏洞造成了重大的财务损失，但由于底层以太坊虚拟机 (EVM) 和主机的隔离，它们并未受到攻击。

代码重用风险：智能合约中的代码重用（例如 Parity Wallet 事件）带来了重大风险，凸显了更强大的审计实践的必要性。
以太坊的安全局限性：以太坊的无许可特性允许任何人与智能合约交互，再加上其不可篡改性，使得部署后修补漏洞变得非常困难。这给事后平台的安全保障带来了巨大的障碍。

结论：以太坊的安全性本质上很复杂，这归因于其设计和编程语言（Solidity），这引入了传统软件开发中通常不会出现的独特漏洞。一系列备受瞩目的攻击，其中许多都利用了智能合约漏洞表明迫切需要标准化的安全实践、强大的审计机制以及主动减轻潜在威胁的措施。

*C. 经济和 MEV 相关攻击*

*1）闪电贷攻击：超越套利：*闪电贷攻击，尤其是在 DeFi 领域，因其能够操纵价格并利用市场低效而成为重大风险。这些攻击利用了闪电贷的原子性，使攻击者能够无需抵押就从 DeFi 协议中借入资产，在单笔交易中跨多个平台执行多笔交易，然后偿还贷款。这些操作在交易可撤销之前完成，使其成为恶意行为者的有力工具。

该研究采用数据收集方法，分析了各种备受瞩目的闪电贷攻击事件。这些攻击针对价格预言机的漏洞，使攻击者能够操纵资产价格并获取人为利润，通常是通过套利机会。诸如 *FlashDeFier*被引入来检测这些价格操纵漏洞，重点关注合同间数据流的静态分析并利用污点分析来追踪恶意活动。

主要发现：闪电贷攻击不仅限于简单的套利，攻击者试图利用不同交易所之间代币价格的差异来获利。他们经常利用跨合约依赖关系——协议对价格预言机的依赖或不同智能合约之间的交互会导致漏洞。

研究发现，使用以下方法检测此类攻击的准确率为 76.4% *FlashDeFier*，其表现明显优于早期的工具，例如 *DeFiTainter*。这一改进凸显了闪电贷攻击日益增长的复杂性和精密性，其攻击已经超越了简单的套利，还包括价格操纵和基于抵押品的攻击。

*2）夹心攻击和抢先交易：*三明治攻击和抢先交易是 DeFi 领域中利用交易排序机制的相关技术。三明治攻击通常涉及在目标交易（通常是大额交易）之前下达买入订单，并在目标交易之后立即下达卖出订单，利用大额交易造成的价格滑点。相比之下，抢先交易是指攻击者预先了解即将进行的交易，并在交易之前执行自己的交易，通常以此获利。

研究这些攻击的方法包括监控 DeFi 协议中的交易序列，尤其是像 Uniswap 这样使用自动做市商 (AMM) 的协议。该研究评估了内存池 (mempool) 如何被用来执行这些攻击，并分析了它们对资产市场价格和潜在财务损失的影响。

*3）主要发现：*三明治攻击和抢先交易都由矿工可提取价值 (MEV) 促成，矿工或验证者可以通过重新排序内存池中的交易来最大化自身利润。通过分析多个此类攻击实例，该研究强调，此类行为通常由 DeFi 协议中嵌入的激励机制驱动。

例如，领先者可能会操纵交易顺序以从即将到来的价格变动中获利，而三明治攻击者则利用大额交易造成的滑点来从暂时的价格波动中获利。

该研究提出了几种缓解策略，包括随机化交易排序和使用私有交易池来降低交易流的透明度。此外，解决 DeFi 治理中的激励错位问题可以减少此类攻击的动机，并增强协议级安全性。

*4）MEV提取技术及其影响：*MEV（矿工可提取价值）提取技术是指攻击者或矿工通过重新排序区块链中的交易来获取价值的方法。这些技术包括三明治攻击、抢先交易和其他交易操纵策略。该研究系统地绘制了各种 DeFi 协议中的 MEV 提取方法，重点关注它们的经济影响及其对流动性提供者和交易者的影响。

评估指标和方法：评估 MEV 技术的关键指标包括：

交易成本和执行延迟；市场影响和波动性；攻击者的盈利能力与诚实参与者的损失；系统范围的因素，例如区块链吞吐量、延迟和可扩展性

模拟模型估计了不同区块链配置和协议实现下 mev 提取的盈利能力。

主要发现：MEV 提取的影响深远，远超单个交易。它会导致市场效率低下，恶意行为者可以操纵价格，通常以牺牲诚实用户的利益为代价。随着 MEV 活动的增加，它会对合法市场参与者产生不利影响，并由于矿工在交易排序中的主导地位而导致中心化风险。

缓解策略：研究提出了几项对策：

算法解决方案，例如*mev-boost*试图分散区块生产，减少垄断控制；监管监督，以解决激励失调问题，促进公平交易实践；交易匿名化技术，包括私人内存池，以限制抢先交易，减少对内存池透明度的利用。

*5）案例研究和统计损失：*闪电贷攻击、三明治攻击和 MEV 提取技术已成为 DeFi 生态系统的重大威胁，近年来造成的经济损失总计达数十亿美元。这些攻击通常利用设计不良的价格预言机、缺乏交易隐私以及薄弱的治理模型中的漏洞。这些漏洞带来的财务风险巨大，因为攻击者能够操纵价格、重新排序交易并利用治理系统获取经济利益。

这些攻击最令人担忧的是其影响的系统性。DeFi 协议的互联性意味着，一个协议中的一个漏洞可能导致连锁故障会波及到其他平台。例如，价格预言机操纵可能会扭曲多个平台上的资产价值，触发自动清算或制造人为的价格波动，而这些波动可能会被攻击者利用。此外，交易隐私仍然是一个关键问题，因为公共区块链中交易排序的透明度使得抢先交易和夹心攻击成为可能。

为了应对这些挑战，DeFi 平台迫切需要更强大的审计机制和增强的安全协议。这包括开发混合攻击检测系统，该系统集成了静态和动态分析工具，能够在潜在漏洞被执行之前识别它们。利用机器学习来预测和预防新的攻击媒介也是一个很有前景的途径，它使协议能够实时适应新兴威胁。

另一个关键问题是 DeFi 治理中激励机制的错位。恶意行为者可以利用治理漏洞，例如通过闪电贷获取大量代币来操纵投票机制。这凸显了建立更强大的治理结构以平衡权力并确保决策符合协议的最佳利益，而非受短期经济利益驱动的必要性。

最终，解决这些安全问题需要采取全面的方法，包括采用隐私增强技术（例如私有交易池），以减少交易订单操纵。去中心化预言机和更高的数据准确性可以降低价格操纵风险，而治理模式中的经济改革将有助于防止治理攻击。通过加强这些方面，DeFi 生态系统可以变得更加安全、透明，并能抵御未来的攻击。

*D. 预言机操纵攻击*

*1）操作技巧：*DeFi 协议中的操纵技术大致可分为两大类：价格操纵和交易排序操纵。这些攻击利用了 DeFi 协议获取价格数据（通常通过预言机）或区块链内交易排序方式的弱点。价格操纵通常涉及利用预言机系统中的漏洞，预言机系统向智能合约提供资产价格等外部数据。如果预言机被攻陷或不可靠，攻击者可以操纵他们输入系统的数据，从而引发意外结果，例如虚假清算或价格虚高，从而使攻击者受益。

交易排序操纵，例如抢先交易和三明治攻击，允许攻击者通过重新排序交易来获利，从而最大化自身经济利益。这种情况通常发生在攻击者能够预测一笔大额交易，并在其前后下单，从而利用由此产生的价格滑点获利。这些技术依赖于交易排序的透明度，即将待处理的交易在内存池中可见，这为攻击者提供了操纵事件顺序以谋取私利的机会。

DeFi 协议固有的激励机制，尤其是“矿工可提取价值”（MEV）的概念，助长了这些攻击。MEV 激励矿工重新排序区块内的交易以获取利润。攻击者能够以极少的资金（例如闪电贷）利用这些系统，这放大了操纵的风险，因为攻击者可以暂时借入大量资金，在不拥有资产的情况下进行大规模操纵。

确保预言机的安全性和可靠性对于减少价格操纵至关重要。如果没有强大且去中心化的预言机，价格数据很容易被篡改，从而给用户和协议带来巨大的经济损失。此外，改进交易排序系统（例如通过实施私有交易池和随机排序）可以帮助防范抢先交易和夹心攻击，使恶意行为者更难预测和利用待处理的交易。

*2）值得注意的案例和后果：*现实世界中的 DeFi 攻击凸显了智能合约、预言机和治理系统中的漏洞所带来的巨大金融风险。这些攻击的后果表明，协议设计缺陷可能导致灾难性的财务损失，并破坏人们对去中心化系统的信任。

1. DAO 攻击（2016）：DAO 黑客攻击是重入漏洞的一个标志性案例，攻击者利用智能合约在处理外部调用之前未能更新自身状态这一漏洞。这使得攻击者能够在资金被记录之前反复提取资金，从 DAO 窃取了 6000 万美元。该事件导致以太坊硬分叉，将网络分裂为以太坊 (ETH) 和以太坊经典 (ETC)，凸显了智能合约漏洞对区块链生态系统的深远影响。

2. Harvest Finance (2020)：攻击者利用闪电贷漏洞，利用了 Harvest Finance 使用的预言机中的价格操纵漏洞。这使得他们能够操纵资产价格，并从该协议中盗取 3380 万美元。此次攻击凸显了价格预言机安全性不足所带来的风险，而价格预言机对于 DeFi 协议的正常运行至关重要。在 DeFi 系统中操纵价格的能力不仅造成了巨大的财务损失，还损害了协议的声誉，并引发了人们对类似协议安全性的担忧。

3. Ronin Bridge（2022 年）：近期发生的一次攻击涉及 Ronin Bridge，攻击者利用私钥泄露窃取了超过 6.24 亿美元的资金。此次攻击暴露了 DeFi 协议中心化控制带来的风险，尤其是在密钥管理等关键基础设施不够去中心化的情况下产生的漏洞。此次事件凸显了安全密钥管理实践和去中心化控制机制的必要性，以防止此类高价值漏洞的发生。

这些案例凸显了 DeFi 的固有风险，其激励机制（包括矿工奖励和交易费）有时会鼓励参与者利用漏洞牟取经济利益。这些案例也凸显了 DeFi 协议中的一个重大问题：缺乏标准化的审计和安全机制。

措施。如果没有严格的审计，安全漏洞就会一直未被发现，直到被利用，从而造成重大损失。

预言机是 DeFi 运作不可或缺的一部分，因为它们为智能合约提供外部数据，使协议能够与现实世界的信息（例如资产价格或利率）进行交互。然而，对这些预言机的依赖带来了一些安全挑战，可能对 DeFi 生态系统造成严重后果。

1. 单点故障：许多 DeFi 协议依赖于单个预言机来获取定价数据，这会导致单点故障。如果该预言机被攻破，可能会导致错误数据被输入系统，造成大范围损害。例如，Synthetix 事件就因预言机错误定价而造成 300 万美元的损失，凸显了中心化预言机的风险。这些故障可能导致以不公平的价格强制清算，损害用户的利益，并削弱人们对协议的信心。

2. 价格操纵：预言机容易受到操纵，尤其是在依赖有限数据源或缺乏去中心化的情况下。攻击者可以操纵预言机提供的数据，导致价格信息不准确，从而触发不良的自动操作，例如清算或创建不稳定资产。这种漏洞在借贷协议中尤其危险，因为错误的价格数据可能导致重大财务损失，正如过去发生的攻击中看到的那样，操纵价格导致抵押品被意外清算。

3. 预言机合谋：当多个预言机提供商合作或受到攻击时，他们可以共同操纵价格，同时影响多个 DeFi 协议。如果没有一个强大的去中心化预言机系统，这种攻击很难检测和防御。对少数数据源的依赖增加了这种合谋的可能性，使预言机成为 DeFi 系统中一个关键的漏洞点。

*3）预言机安全性的理论局限性：*预言机安全性的理论局限性在于去中心化与可靠性之间的权衡。虽然去中心化预言机有助于缓解单点故障，但它们的价格信息准确性较低且延迟较高，这使得它们在快速变化的市场中可靠性较低。提升预言机安全性需要开发更具弹性的系统，以整合多个数据源，降低操纵风险，并确保准确及时的定价。

价格操纵、三明治攻击和 MEV 提取是 DeFi 生态系统中的关键漏洞，对安全和金融稳定具有重大影响。预言机系统和交易排序机制的利用会导致巨额损失，并可能破坏去中心化平台的完整性。激励结构失调和缺乏健全的治理机制往往会加剧这些漏洞。

为了解决这些问题，迫切需要更安全、更去中心化的预言机，以提供准确的价格数据并降低操纵风险。此外，通过私有内存池和

随机排序系统可以降低抢先交易和夹心攻击的风险。治理体系改革，例如引入投票延迟和法定人数门槛，对于降低治理漏洞的风险至关重要。

整合安全审计系统、自动化测试框架和机器学习模型来预测和预防攻击，有助于增强 DeFi 协议抵御不断演变的威胁。随着 DeFi 领域的不断发展，采取全面的安全措施并建立行业标准至关重要，这样才能保护用户和协议免受针对 DeFi 平台日益增多的攻击。

*E. 值得注意的案例、损失分析和经验教训*

*1）热门攻击事件：时间线和损失排名：*DeFi 协议遭受了大量安全漏洞的攻击，每次都造成了不同程度的财务损失。这些事件通常由智能合约、治理机制或经济模型的缺陷所致，凸显了去中心化金融领域亟需更强大的安全框架。

从攻击时间线中可以清晰地看出一个规律：某些事件的影响范围更大，这取决于所利用的漏洞类型及其造成的后果。例如，闪电贷攻击是最常见的攻击之一，它利用价格预言机和流动性池中的漏洞。2020 年的 Harvest Finance 攻击就是最显著的例子之一，该攻击造成 3380 万美元的损失。在这次攻击中，闪电贷促成的价格操纵使攻击者能够利用价格预言机集成中的漏洞，造成巨额财务损失。另一次重大攻击发生在 Cream Finance，攻击者利用了与闪电贷相关的漏洞，造成了 1.3 亿美元的巨额损失。这起事件表明攻击者的手段日益复杂，他们不仅瞄准单个协议，还瞄准 DeFi 生态系统中的经济激励机制。

2016 年的 DAO 攻击事件造成约 6000 万美元损失，是 DeFi 安全的另一个关键时刻。此次攻击凸显了重入攻击的风险，即智能合约的功能允许攻击者在系统更新状态之前递归提取资金。这次攻击开创了先例，表明在部署之前需要对智能合约功能进行更严格的测试和验证。

其他重大事件，例如2017年的Parity Multisig Wallet漏洞，由于无保护的自杀和委托调用注入等漏洞，造成了2.8亿美元的损失。这些事件凸显了智能合约设计中即使是轻微的疏忽，尤其是在处理外部交互和功能权限方面，也可能导致灾难性的后果。

这些案例表明，DeFi 安全漏洞的主要来源包括薄弱或有缺陷的合约逻辑、用户资产处理不当以及治理系统漏洞。随着这些攻击的不断演变，它们不仅对个人用户构成严重风险，也对 DeFi 领域的长期可持续性构成威胁。

*2）协议设计者的经验教训：*从这些备受瞩目的事件中，DeFi 协议设计者们汲取了一些重要的经验教训，以提升其系统的安全性。首先，深入了解智能合约漏洞至关重要。诸如可重入、整数溢出和预言机操纵等常见问题必须通过严格的测试来解决，并实施可靠的安全措施，例如可重入保护和 SafeMath 库。此外，协议应采用形式化验证技术，以确保智能合约的逻辑和执行在部署之前不存在可利用的漏洞。

此外，设计人员必须考虑协议中嵌入的激励机制。上述许多攻击都利用了经济漏洞，例如通过闪电贷操纵价格，或通过代币积累进行治理漏洞。显然，激励机制失调会促使攻击者利用这些系统牟利。为了降低这些风险，协议必须设计与系统长期安全性和稳定性相符的激励机制，并纳入反操纵功能和治理保障措施，例如投票延迟和法定人数要求，以防止通过治理机制进行恶意收购。

另一个重要启示是可组合性在DeFi协议中的重要性。虽然可组合性允许不同的协议交互并创建更复杂的金融产品，但它也放大了风险。一个协议中的漏洞可能会波及整个生态系统，引发连锁反应。因此，压力测试和模拟工具对于评估互连协议在极端条件下的行为至关重要。此外，使用具有适当数据验证机制的去中心化预言机可以帮助防止价格操纵，而价格操纵仍然是DeFi领域的一个重要攻击媒介。

最后，需要建立监控和事件响应策略。协议不仅应着眼于预防攻击，还应做好在发生违规事件时快速响应的准备。持续监控以及实时审计和安全更新有助于识别新兴威胁并减轻损失。

总而言之，保护 DeFi 协议的安全需要采取多管齐下的方法，既要考虑技术漏洞，也要考虑经济激励。通过整合强大的安全实践、增强治理模型，并考虑可组合性和外部数据依赖性带来的更广泛的系统性影响，设计人员可以帮助增强其协议，抵御持续针对 DeFi 生态系统的日益复杂的攻击。

*F. 总结和未决挑战*

去中心化金融 (DeFi) 引入了创新的金融模式，但也创造了一个极易受到各种攻击的复杂环境。系统地了解这些攻击对于保护生态系统至关重要。最突出的攻击策略包括技术攻击（针对智能合约代码中的漏洞）和经济攻击（利用市场条件）。

或治理结构被操纵以牟取恶意利益。诸如闪电贷、重入漏洞和预言机价格操纵等工具通常被用来实施此类攻击，从而利用 DeFi 系统开放透明的特性。

智能合约因其在自动化交易和资金管理中的作用而成为主要的攻击面。诸如编码错误或逻辑缺陷之类的漏洞可能会造成严重的财务影响。为智能合约提供实时数据的预言机是另一个关键漏洞。攻击者可以操纵这些预言机，导致错误数据被输入系统，并触发强制清算或价格扭曲等事件。矿工可提取价值 (MEV) 问题，即攻击者通过操纵交易顺序获利，是另一个破坏去中心化交易所 (DEX) 稳定性并造成不公平市场条件的挑战。

尽管在检测和缓解此类风险方面取得了一些进展——例如通过 FlashDeFier 等用于检测闪电贷攻击的工具以及智能合约的形式化验证流程，但整个 DeFi 领域的安全实践仍然存在差距。这些差距导致解决漏洞的努力分散，从而使协议暴露在风险之中。隐私增强技术可以减少抢先交易和 MEV 提取等问题，但这些技术仍处于早期开发阶段，面临着可扩展性和与现有协议集成方面的挑战。

治理体系和激励机制失调是 DeFi 面临的重大风险。恶意行为者可以利用薄弱的治理模型，尤其是通过操纵闪电贷等手段，从而控制协议并实施有害的变更。解决这些治理漏洞的解决方案非常复杂，需要在去中心化和安全性之间取得平衡，以确保决策权分散，但仍能避免被操纵。

DeFi 协议固有的可组合性也增加了一层风险。协议间的互联性意味着一个协议中的漏洞可能会引发连锁反应，影响多个系统。这种互联性放大了攻击的潜在影响。为了降低这些风险，有必要进行压力测试并规范化协议间的依赖关系，以评估发生系统级故障的可能性。

关键的开放性挑战包括：需要建立全面的框架来检测和应对复杂的攻击，提高隐私解决方案的可扩展性，解决治理问题，以及建立标准化的跨协议安全措施。随着 DeFi 协议的不断发展，攻击检测工具、经济激励模型和安全框架的持续创新对于维护 DeFi 生态系统的完整性和可信度至关重要。

总而言之，尽管 DeFi 有潜力彻底改变金融业，但确保其安全需要采取一种综合的方法，既要考虑技术漏洞，又要考虑经济激励。应对这些开放性挑战——改进隐私解决方案、增强治理模型以及实施更强大的攻击检测措施——对于 DeFi 生态系统的可持续性和长期成功至关重要。

## IV. Defense米机制和格治理

### *A. 技术防御*

*1）智能合约审计和形式验证：*智能合约审计和形式化验证是抵御 DeFi 协议漏洞的第一道防线。审计需要安全专家进行全面的代码审查，以便在部署之前发现潜在漏洞。根据 Chen 等人的研究 [16]，专业审计公司通常采用多层方法，包括手动代码审查、自动化工具扫描和攻击场景模拟。

相比之下，形式化验证则提供合约相对于形式化规范的正确性的数学证明。正如吴等人[17]所指出的，“形式化验证可以分为静态符号执行和动态符号执行”，每种方法提供不同的安全保障。静态方法分析代码而不执行，而动态方法则观察运行时行为。

最近的进展见证了两种方法的融合。例如，像 Securify 这样的工具通过将智能合约拆分成独立的部分进行验证，从而“提高了自动化程度”，并解决了形式化验证中常见的路径空间爆炸问题 [17]。

尽管这些方法有效，但也存在局限性。Ince 等人 [18] 指出：“虽然这些工具前景光明，但它们还无法取代更传统的人工审查。” 他强调，完整的安全保障仍然需要自动化和人工专业知识的结合。

*2）Oracle 安全增强：*预言机是 DeFi 系统中一个关键的漏洞点，因为它们将链上智能合约与链下数据连接起来。根据 Werner 等人的研究 [1]，不安全的预言机导致了历史上一些规模最大的 DeFi 漏洞。

为了增强预言机的安全性，已经出现了几种技术解决方案：

- 多个数据源：通过 M-of-N 报告机制，使用多种预言机，汇总来自多个提供商的价格信息。此方法计算中间价，并忽略与共识偏差较大的异常值 [17]。
- 时间加权平均价格（TWAP）：像 Uniswap V2 这样的协议实现了 TWAP 机制，可以跟踪价格的长期走势，从而提高操纵难度和成本。这要求价格操纵持续进行，而非瞬间飙升，从而降低了闪电贷攻击的风险 [19]。
- 断路器：实施价格偏差限制，当价格超出预设阈值时，暂时停止交易。这为人工验证提供了时间，并防止价格操纵期间造成灾难性的损失。
- 加密验证：像 Chainlink 这样的先进的预言机系统采用加密证明来验证数据完整性和来源真实性，大大提高了攻击者的门槛 [1]。

这些措施的有效性因具体实施而异。Cole [20] 指出：“使用多源和强大验证机制的预言机可以减少攻击面，但完全的安全需要防御措施的不断发展。”

*3）MEV缓解技术：*矿工可提取价值 (MEV) 通过交易重新排序、抢先交易和三明治攻击对 DeFi 用户构成重大威胁。目前已开发出各种技术解决方案来降低这些风险：

- 承诺-披露方案：这些协议要求用户在不透露细节的情况下承诺交易，然后仅在承诺记录在链上后才公开细节，以防止抢先交易[5]。
- 时间锁延迟：在交易提交和执行之间实施强制等待期，减少 MEV 提取的机会 [4]。
- 公平排序服务：Chainlink 的公平排序服务和以太坊提出的 MEV-Boost 等协议旨在创建公平的排序机制，防止矿工为了牟利而任意重新排序交易。
- 隐私保护交易：像 Aztec Protocol 和 zk-rollups 这样的解决方案可以在交易执行之前屏蔽交易细节，从而阻止 MEV 提取者识别获利机会 [21]。

正如 Heimbach 和 Wattenhofer [22] 所指出的，“消除三明治攻击需要采用博弈论方法来协调整个生态系统的激励措施”，这表明技术解决方案必须辅以经济设计考虑。

*4）案例研究：国防成功与失败：*对现实世界事件的分析为技术防御的有效性提供了宝贵的见解：

成功案例：MakerDAO 的韧性
MakerDAO 强大的防御机制在 2020 年 3 月的市场崩盘中经受了考验。尽管市场波动剧烈，其多层防御机制（包括价格延迟机制、紧急关闭功能以及由治理控制的风险参数）仍使该协议得以幸存，避免彻底崩溃 [2]。

正如 Cole [20] 所观察到的，“之前的审计已经发现了储备构成中的潜在风险，使得在事件发生时能够更快地做出响应和恢复。”这凸显了主动安全措施如何在危机情况下提供恢复能力。

失败案例：虫洞桥漏洞
2022 年 2 月，以太坊和 Solana 之间的虫洞桥被利用，窃取了 12 万 ETH（当时约合 3.25 亿美元）。此次攻击之所以得逞，是因为开发人员启用了一项已弃用的函数，该函数允许验证伪造的签名，从而绕过关键的安全检查 [17]。

此案例表明，即使经过形式化验证和审计，运营安全仍然至关重要。漏洞并非发生在核心逻辑中，而是发生在一个仍可访问的已弃用函数中，这凸显了安全的重要性。全面的安全审查和适当的弃用程序。

*B. 经济激励与机制设计*

*1）激励兼容的安全模型：*DeFi 协议越来越多地采用经济机制，将参与者激励与协议安全性相结合。这些方法认识到，如果没有适当的经济设计，单靠技术保障措施无法确保安全。

“经济安全”的概念表明，协议的设计应使理性行为者发现攻击系统的成本高于遵守规则的成本。这种方法依赖于将攻击成本与潜在利润进行量化，从而创建一个安全违规行为在经济上不合理的系统[19]。

主要的激励兼容安全模型包括：
- 基于权益的安全性：要求验证者、流动性提供者或其他参与者锁定抵押品，这些抵押品可能会因恶意行为而被罚没。这创造了“利益相关方”（skin in the game）的机制，从而抑制了攻击行为。
- 费用结构：在波动性较大或拥堵时期增加交易费用，使得某些攻击媒介在脆弱时期的成本过高。
- 奖励分配：设计代币奖励机制，鼓励长期参与和协议健康，而非短期剥削。这可以包括归属计划和参与乘数。

Werner 等人 [1] 指出，“激励兼容的设计必须考虑不完美信息下的理性行为”，强调了即使在参与者信息不对称或理性有限的情况下，模型也需要保持安全。

*2）博弈论方法：*博弈论提供了一个数学框架，用于分析 DeFi 生态系统中理性参与者之间的战略互动。目前已应用多种博弈论模型来增强协议安全性：

- 纳什均衡分析：设计符合纳什均衡（即任何参与者都不会从单方面改变策略中获益）且符合所需安全属性的协议。这可以在无需信任的情况下实现自我执行的安全性 [4]。
- 谢林点：创建焦点，让参与者即使没有沟通也能通过共同的知识和期望自然地聚集在安全行为上。
- 信号游戏：实施机制，让诚实的参与者能够可靠地表明他们的可信度，从而允许协议区分诚实的行为者和潜在的恶意行为者。

Daian 等人 [5] 展示了如何将博弈论应用于 MEV 问题，将优先 Gas 拍卖建模为非合作博弈，并分析了均衡竞价策略。他们的研究表明，“如果没有适当的机制

设计中，竞争均衡往往会导致浪费的结果，例如天然气价格上涨和网络拥堵。

*3）案例分析：有效的经济防御措施：*Maker 协议清算系统

Maker 协议的清算机制体现了有效的经济防御设计。清算人（称为“看管人”）受到激励，监控抵押债务头寸并清算抵押不足的贷款。该协议提供了清算折扣，使这种行为有利可图，同时保护系统免于破产。

在2020年3月的市场崩盘期间，该系统承受了极大的压力，但最终仍按预期运行。虽然由于Gas价格飙升和市场拥堵，一些拍卖以零出价清算，但随后的治理响应实施了包括荷兰式拍卖机制和熔断机制在内的改进措施[1]。

Curve Finance 投票托管代币经济学

Curve Finance 推出了投票托管 CRV（veCRV），要求用户长期锁定其 CRV 代币以获得治理权和更高的奖励。这种机制为长期参与和遵守协议健康提供了强大的经济激励。

正如 Cole [20] 所观察到的，这种设计“通过定期的安全更新、社区参与治理和透明的漏洞披露来增强用户信任和采用”，展示了经济激励如何增强协议的安全性和稳定性。

*C. 社区治理与事件响应*

*1）基于DAO的治理机制：*去中心化自治组织 (DAO) 是管理 DeFi 协议的主要治理结构。这些治理系统使代币持有者能够对协议参数、安全措施和资源分配的变更进行提议和投票。

有效的 DAO 治理机制通常包括：

- 多层次提案系统：结构化流程，提案必须经过讨论、正式提交和投票阶段才能实施。这可以对有害变更进行审慎检查。
- 代表团：允许代币持有者将其投票权委托给可能更好地理解复杂安全影响的技术熟练的社区成员。
- 延时执行：在治理决策的批准和执行之间实施强制等待期，为安全审查和必要时的应急响应提供时间。
- 专门安全理事会：创建具有安全专业知识的专门小组来审查协议变更并应对紧急情况，有时还拥有实施时间敏感的安全修复的特殊权力。

正如 Xu 等人 [2] 所指出的，“治理系统的设计直接影响 DeFi 协议的安全性、适应性以及对社区利益的响应能力。”然而，治理如果没有得到适当的保护，ernance 本身就可能成为攻击媒介。

*2）事件响应和恢复案例研究：*Compound Finance 预言机错误（2021 年 11 月）

2021 年 11 月，Compound Finance 发生了一起事件，由于价格信息流存在缺陷，用户得以以过高的抵押品价值借入资产。社区的反应凸显了去中心化治理的优势和劣势：

即时响应包括识别问题、与用户沟通以及制定技术解决方案。然而，由于强制时间锁延迟，治理流程需要数天时间才能实施解决方案。这凸显了以安全为中心的时间延迟与快速响应的事件管理之间的矛盾。

虫洞桥恢复（2022 年 2 月） 在价值 3.25 亿美元的 Wormhole 桥被攻破后，Jump Crypto（Wormhole 的母公司）介入补充被盗资金，防止了生态系统崩溃。此案例表明，许多 DeFi 恢复流程都具有混合性，尽管治理结构分散，但中心化实体往往发挥着关键作用。

正如吴等人 [17] 所指出的，恢复涉及“操作错误响应”，这强调了事件响应框架必须在恢复规划中同时考虑技术因素和人为因素。

*3）分散协调的挑战：*分散治理面临着影响安全事件响应的几个协调挑战：

- 响应速度与深思熟虑：快速响应安全事件与社区全面审议之间存在内在矛盾。时间敏感的漏洞可能需要比治理流程允许的更快的行动速度。
- 信息不对称：治理参与者的技术专长水平各不相同，这可能导致评估复杂的安全提案或理解漏洞影响的困难。
- 选民参与：治理投票的参与率低可能会导致决策由少数不具代表性的代币持有者群体做出。
- 跨协议协调：安全事件通常会影响多个相互关联的协议，需要跨具有不同流程和时间表的不同治理系统进行协调。

Werner 等人 [1] 观察到“去中心化治理机制必须平衡安全性、灵活性和包容性”，才能有效应对不断演变的威胁，同时保持社区的一致性。

*D. 局限性和挑战*

*1）技术、经济和社会限制：*技术限制：

- 形式验证边界：即使经过形式化验证的合约，如果规范本身存在缺陷或不完整，也可能存在漏洞。正如 Chen 等人[21] 所述。

注意，“形式验证不能保证不存在所有漏洞，只能保证符合指定的属性。”

- Oracle 约束：预言机系统的完全去中心化仍然具有挑战性，在原本去中心化的系统中产生了中心化点。
- 可组合性风险：DeFi 协议的互操作性创造了复杂的交互界面，难以完全保障安全。当各个协议以意想不到的方式交互时，其安全保障可能会失效。

经济限制：

- 资本效率与安全性：安全措施往往会降低资本效率，从而在短期内给更安全的协议带来竞争劣势。
- MEV 持久性：尽管采取了缓解措施，但 MEV 提取仍在不断发展，提取器开发出越来越复杂的技术来利用新的漏洞。
- 激励错位：代币分配和治理结构可能会在短期代币持有者和长期协议健康之间造成不一致的激励。

社会限制：

- 治理捕获：治理代币的集中可能导致富豪控制，从而可能破坏权力下放的原则。
- 技术壁垒：复杂的安全机制可能会将技术水平较低的参与者排除在有效的治理参与之外。
- 监管不确定性：不断变化的监管环境给实施安全措施的协议开发人员带来了不确定性。

*2）未解决的问题：*DeFi 安全方面仍有几个关键挑战尚未解决：

- 跨链安全：随着 DeFi 跨多个区块链扩展，确保跨链桥和交互的安全面临着独特的挑战，而当前的安全模型尚未完全解决。
- 扩展安全解决方案：确保安全机制能够随着协议采用的增加和交易量的增加而扩展。
- 隐私与透明度：平衡安全分析所需的透明度与用户的隐私要求和竞争性协议操作。
- 安全的经济可持续性：为持续的安全研究、审计和事件响应能力开发可持续的资金模式。
- 标准化：在整个生态系统中创建通用的安全标准和最佳实践，同时允许特定于协议的创新。

Salzano 等人 [23] 指出，在解决安全漏洞方面存在“学术文献与实践发展之间的差距”，特别是在拒绝服务、恶意随机性和时间操纵，开发人员的实践往往与学术建议不同。

### *E. 总结*

DeFi 的防御机制已取得显著发展，将技术保障、经济激励和治理流程相结合，构建了多层级的安全体系。包括形式化验证、预言机增强和 MEV 缓解在内的技术防御机制提供了基础安全保障，而经济机制设计则将参与者的激励机制与协议安全性相结合。社区治理系统能够自适应地应对新兴威胁，并在事件发生时协调恢复工作。

尽管取得了这些进展，但重大挑战依然存在。DeFi 的可组合性带来了复杂的攻击面，难以完全保障安全；同时，资本效率、可用性和安全性之间的矛盾也带来了持续的权衡。治理体系仍在努力平衡响应式决策和包容性审议。

最有前景的方法是整合多层防御，认识到单一的安全机制不足以应对所有挑战。正如 Werner 等人 [1] 总结的那样：“D eFi 协议的稳健性不仅取决于技术实现，还取决于经济激励与有效治理的协调。” 这种整体方法认为，安全性源于代码、经济和社区之间的互动，需要随着威胁形势的变化而不断发展。

未来的研发应侧重于解决已发现的未解决的问题，特别是跨链安全性、可扩展的安全解决方案以及安全融资的可持续经济模型。标准化工作可能有助于建立通用的安全基线，同时允许特定协议的创新，从而弥合Salzano等人[23]指出的学术研究与开发者实践之间的差距。

## V. D讨论和F未来D方向

### *A. 套利与攻击之间的灰色地带*

*1）案例研究：道德和法律模糊性：*在DeFi领域，套利与攻击的界限往往比较模糊。

- 在Poly Network攻击事件中，攻击者利用漏洞窃取资产，最终获得了50万美元的漏洞赏金，并保留了项目团队授予的“首席安全顾问”头衔。这起事件引发了关于“道德黑客”标准的激烈争论，称其可能使盗窃行为合法化，从而开创一个危险的先例[1]。
- 在Mango Markets事件中，攻击者通过操纵预言机价格获利，并引用协议自治规则为自己辩护，暴露出DeFi治理机制的致命缺陷：在技术可行性、社区治理和法律规范发生冲突时，缺乏权威的仲裁框架[9]。

- 从伦理角度来看，“三明治攻击”的普适化引发了更深层次的思考。2023年以太坊上约有23%的MEV收益来自于这种损害普通用户利益的策略，而当参与者被告知其套利行为将给他人造成损失时，仍有78%的人选择继续执行，这体现了DeFi匿名性在化解伦理约束方面的作用[1]。更为棘手的是，此类策略往往处于现有法律体系的灰色地带——它们严格遵循协议规则，却明显违反了公平交易原则。

*2）监管和治理影响：*这些外围案件对监管框架提出了前所未有的挑战。

- 美国证券交易委员会（SEC）于2023年10月发布的首份DeFi执法指南中，首次明确将“利用技术优势获取不正当利益”纳入证券欺诈的范畴。但该指南遭到了加密社区的强烈反对，他们认为该指南未能区分创新套利行为与欺诈行为的核心区别。

- 在治理机制方面，DAO 组织正在探索新的解决方案。Uniswap 在 2023 年推出的“MEV 回收池”机制颇具创新，通过协议层捕获部分套利利润，并将其返还给流动性提供者。该机制实施后，相关争议提案的数量有所减少 [1]。

- 从国际协调角度，金融稳定理事会（FSB）2023年报告指出，各国对DeFi套利的监管差异，可能导致严重的监管套利现象，建立全球统一的分类标准已成为国际组织的优先议程。

这些进展表明，DeFi治理正在进入“技术+法律+伦理”三方协同的新阶段。

*B. DeFi 生态系统的未来趋势*

*1）技术创新：*

- 人工智能：人工智能和机器学习正在重新塑造DeFi套利策略的竞争格局。2023年第四季度，首批基于GPT-4的套利机器人将利用自然语言处理能力实时分析新闻事件和社交媒体情绪，将事件驱动套利的响应速度提升至传统系统的三倍。在强化学习的路径优化中，AI模型能够通过模拟数百万个历史交易场景，自主发现人类开发者尚未识别的套利模式，并在回测中将三角套利收益率提升40%。

- 第 2 层：Layer 2 解决方案正在为套利策略创造新的范式。Arbitrarum Nova 的“AnyTrust”机制以及Optimism的“Bedrock”升级，将跨层套利的时间窗口从原来的12-15秒压缩到3秒，这导致传统人工套利基本退出市场，专业机构研发的“超低延迟系统”占据主导地位。

- 跨链：跨链技术的演进正在改写多链套利的风险收益率。基于Cosmos IBC和LayerZero原子交换协议，跨链套利的成功率从早期的不足20%提升至68%。然而，这些进步也伴随着新的安全风险，跨链桥已成为黑客攻击的首要目标[1]。

*2）监管演变和全球趋势：*全球监管框架正经历关键转型期。

美国证券交易委员会于2024年3月通过的《DeFi市场监管条例》率先运用“实质重于形式”原则，将符合条件的套利活动纳入证券交易监管。另一方面，欧盟则在MiCA监管条例下通过了二级立法，要求所有“专业套利者”注册并缴纳交易保证金，违反者将面临相当于年营业额10%的罚款。

发展中国家正在形成各具特色的监管路径。印度的“沙盒监管”计划允许测试高风险套利策略，但要求20%的利润存入监管保险基金。尼日利亚央行推出的“数字资产做市商许可证”将套利机构纳入正规金融体系，使该国稳定币套利利差从3%降至0.5%。

*C. 研究和产业面临的新挑战*

*1）可扩展性、隐私性和可组合性：*

- 可扩展性：可扩展性瓶颈已成为DeFi套利策略发展的首要障碍。专业的套利机器人贡献了全网32%的交易量，但仅获得了15%的区块空间。当TPS超过2000时，现有的MEV拍卖机制将彻底崩溃，从而出现“套利黑洞”现象——由于网络拥堵，高价值的套利机会无法被捕捉到[1]。

- 隐私：隐私保护要求与监管透明度要求的根本冲突。Zcash基金会于2023年开发的“零知识套利”协议，虽然能够隐藏交易路径，但却遭到FATF的强烈警告，称其违反了“旅行规则”。

- 可组合性：可组合性风险会随着协议复杂度的增加而呈指数级增长。当智能合约调用深度超过7层时，发生意外组合行为的概率高达43%。2019年发生的“组合清算风暴”

2024 年 3 月是一个典型案例：一次常规的 ETH 价格波动通过 11 个协议的连锁反应，引发了 68% 的错误异常清算，现有的安全工具根本无法检测到这种“跨协议级联效应”[1]。

*2）跨学科研究机会：*行为金融学与DeFi套利的结合，开辟了全新的研究范式。剑桥大学新兴金融中心2024年的实验显示，当套利界面融入“社交损失可视化”功能时，42%的参与者会主动放弃高达30%的获利机会。这种“链上利他”现象，彻底颠覆了传统金融的理性假设。

气候金融视角正在重塑套利基础设施的评估标准。根据碳链智库的计算，一次典型的以太坊三明治攻击所消耗的能量相当于30个美国家庭的日用电量，整个DeFi套利生态系统的年度碳足迹已经超过了冰岛，这刺激了“绿色套利”的创新[5]。

复杂系统科学为风险管理提供了新的工具。圣达菲研究所与Maker-DAO合作的项目首次将生态系统的韧性理论应用于DeFi压力测试。他们发现，套利活动实际上在协议之间建立了“金融传染通道”，其网络拓扑特征与流行病的传播极其相似。基于此开发的“风险传播模型”成功预测了2024年1月的Aave流动性危机，并提前72小时发出预警。

### *D. 开放研究方向*

*1）关键开放性问题：*跨协议套利的原子性问题仍然是 DeFi 领域最紧迫的未解难题。目前尚无解决方案能够真正保证涉及三个或更多协议的复杂套利交易的原子性执行。核心挑战在于，当某些协议采用确定性共识，而其他协议采用概率性共识时，如何设计一个通用的原子性框架 [5]。

动态成本市场对套利策略的影响机制亟待深入研究。2024年EIP-7623实施后，以太坊基础费用的波动性增加了四倍，但套利机器人的适应策略却呈现出令人费解的分化。这种双峰分布违背了传统拍卖理论的预测，暗示着更深层次的博弈均衡的存在。

长期生态影响评估框架完全缺失。目前所有的套利研究都侧重于短期市场影响，但DeFi协议作为“可编程货币乐高”的特性，可能会导致套利活动发生深刻的系统性重构。

*2）建议的方法和途径：*大规模多智能体仿真应该成为一种基础研究工具。与传统金融研究不同，DeFi 套利涉及数百个异构智能体之间的实时交互。伯克利大学开发的“DeFiSim”平台的仿真结果表明，某些套利策略可以产生类似量子纠缠的网络效应。该方法尤其适用于研究新兴的跨链 MEV 问题。通过构建虚拟的跨链环境，可以提前识别潜在的套利危机点 [1]。

跨学科知识图谱的构建对于理解复杂的影响至关重要。剑桥大学发起的“DeFi认知图谱”项目首次系统地建模了套利活动对技术栈、经济模型、法律框架和社会影响的四维效应。

量子计算实验应该提前规划。尽管目前的量子计算机无法在实际规模上处理DeFi问题，但将套利机会识别转化为量子支持向量机（QSVM）问题，理论上可以在对数时间内完成传统计算机需要多项式时间才能解决的任务。这种指数级的加速可能会彻底改变高频套利的竞争 格局。

## VI.C结论

### *A. 主要发现和贡献*

这篇关于知识系统化 (SoK) 的论文对去中心化金融 (DeFi) 中的套利和攻击策略进行了全面的概述和分类。我们的主要发现如下：

- 我们提出了 DeFi 套利的统一分类法，涵盖跨平台、三角、闪电贷、基于预言机和新兴的 MEV 驱动策略，并分析了它们的机制、量化影响和系统性风险。
- 我们系统地将 DeFi 攻击分为技术和经济类别，详细说明常见的智能合约漏洞、预言机操纵、MEV 提取和可组合性引起的级联故障。
- 通过比较案例研究和定量分析，我们揭示了套利和攻击在提高市场效率和放大系统性风险方面的双重作用。
- 我们审查并评估最先进的防御机制，包括形式验证、预言机增强、MEV 缓解、激励兼容机制设计和社区治理框架。
- 我们确定了关键的研究差距，例如跨链原子性、可扩展的安全解决方案以及整合密码学、经济学和监管科学的跨学科方法的必要性。

### *B. 对 DeFi 安全和生态系统的影响*

我们的分析强调，DeFi 虽然开启了前所未有的金融创新和普惠性，但也引入了新的攻击面，并因可组合性和自动化而加剧了系统脆弱性。套利策略和攻击策略之间的相互作用挑战了道德和法律行为的界限，需要建立适应性治理和监管框架。DeFi 的有效安全不仅需要强大的技术解决方案，还需要激励机制的协调、透明的治理和持续的监控。

### *C. 与相关SoK和基础著作的比较*

与先前的 SoK 研究 [1]、[2]、[4] 相比，我们的研究提供了更细致的套利和攻击策略分类，融合了 MEV 和跨链套利的最新进展，并强调了合法套利与恶意利用之间的灰色地带。我们进一步弥合了学术理论与现实世界协议事件之间的差距，为研究人员和实践者提供了切实可行的见解。

### *D. 关键洞察汇总表*

表二
秒摘要钾安永我来自的见解T他的秒哦钾

| 方面 | 关键洞察 |
|---|---|
| 套利分类法 | 多维，随着 MEV、跨链和 AI 驱动范式的发展而发展技术（合约、预言机）、经济（MEV、治理）、可组合性风险多层次：形式验证、预言机设计、MEV 缓解、激励协调 |
| 攻击向量 | |
| 防御机制 | |
| 治理 | DAO 至关重要，但在协调、响应和捕获方面面临挑战；跨链安全性、可扩展隐私、可组合性、跨学科框架；多智能体模拟、知识图谱、量子计算、气候影响 |
| 开放挑战 | |
| 研究方向 | |

### *E. 结语*

DeFi 代表着金融基础设施的变革性转变，但其安全性和稳定性取决于对套利和攻击策略的全面理解。随着生态系统的不断发展，未来的研究应优先考虑跨链和可组合性风险，开发标准化的安全框架，并促进跨学科合作。通过整合技术、经济和治理创新，DeFi 社区可以构建一个更具韧性、公平和可持续性的去中心化金融体系。

## R参考文献


[1] S. Werner、D. Perez、L. Gudgeon、A. Klages-Mundt、D. Harz 和 W. Knottenbelt，“SoK：去中心化金融（defi）”，*第三届 ACM 金融技术进步会议 (AFT '21) 论文集*，2021 年，第 1-15 页。

[2] J. Xu、B. Livshits 和 A. Gervais，“Sok：去中心化金融安全与隐私” *arXiv 预印本 arXiv:2104.08739*，2021 年。[在线]。可访问网址：https://arxiv.org/abs/2104.08739

[3] G. Wood，“以太坊：一个安全的去中心化通用交易账本”，https://ethereum.github.io/yellowpaper/paper.pdf，2014 年。

[4] K. Qin, L. Zhou, 和 A. Gervais，“量化区块链可提取价值：森林有多黑暗？”*2022 IEEE 安全与隐私研讨会（SP）*. IEEE，2022 年，第 198-214 页。

[5] P. Daian、S. Goldfeder、T. Kell、Y. Li、X. Zhao、I. Bentov、L. Breidenbach 和 A. Juels，“闪客小子 2.0：去中心化交易所中的抢先交易、交易重排序和共识不稳定性”，*2020 IEEE 安全与隐私研讨会（SP）*. IEEE，2020 年，第 910-927 页。

[6] G. Angeris 和 T. Chitra，“改进的价格预言机：恒定函数做市商”，*第二届 ACM 金融技术进步会议（AFT）论文集*. ACM，2020 年，第 80-91 页。

[7] F. Zhang、E. Cecchetti、K. Croman、A. Juels 和 E. Shi，“城镇公告员：智能合约的认证数据馈送”，*2016 年 ACM SIGSAC 计算机与通信安全 (CCS) 会议论文集*ACM，2016 年，第 270-282 页。

[8] 徐建*等人*，“SoK：去中心化金融（DeFi）”，*第四届 ACM 金融技术进步会议论文集*，2022年。[在线]。获取方式：https://dl.acm.org/doi/10.1145/3558535.3559780

[9] K. Qin, C. Zhou, 和 A. Gervais，“利用闪电贷攻击 DeFi 生态系统，既有趣又有利可图”，*arXiv 预印本 arXiv:2003.03810*，2021 年。[在线]。可访问网址：https://arxiv.org/abs/2003.03810

[10] A. Shleifer 和 RW Vishny，“套利的限度”，*《金融杂志》*，第 52 卷，第 1 期，第 35-55 页，1997 年。

[11] Y. Cao, C. Zou, 和 X. Cheng, “Flashot: DeFi 生态系统中闪电贷攻击的快照”, 2021 年。[在线]。可访问网址：https://arxiv.org/abs/2102.00626

[12] M. Bichuch 和 Z. Feinstein，“对冲流动性代币中的 DeFi 套利”，2024 年。[在线]。可访问网址：https://arxiv.org/abs/2409.11339

[13] L. Zhou, K. Qin, A. Cully, B. Livshits 和 A. Gervais，“论 DeFi 协议中盈利交易的即时发现”，2021 年。[在线]。可访问网址：https://arxiv.org/abs/2103.02228

[14] D. Wang, S. Wu, Z. Lin, L. Wu, X. Yuan, Y. Zhou, H. Wang 和 K. Ren，“迈向理解闪电贷及其在 DeFi 生态系统中应用的第一步”，SBC '21 系列。美国纽约州纽约市：计算机协会，2021 年。[在线]。可访问网址：https://doi.org/10.1145/3457977.3460301

[15] X. Deng、SM Beillahi、C. Minwalla、H. Du、A. Veneris 和 F. Long，“保护 DeFi 智能合约免受预言机偏差影响”，ICSE '24 系列。美国纽约州纽约市：计算机协会，2024 年。[在线]。可访问网址：https://doi.org/10.1145/3597503.3639225

[16] J. Chen、X. Xia、D. Lo、J. Grundy、X. Luo 和 T. Chen，“定义以太坊智能合约缺陷”，*IEEE 软件工程学报*，第 48 卷，第 1 期，第 327-345 页，2022 年。

[17] X. Wu、J. Xing 和 X. Li，“探索 Solana 智能合约中的漏洞和担忧”，*arXiv 预印本 arXiv:2504.07419*，2025年。

[18] P. Ince、J. Yu、JK Liu 和 X. Du，“生成式大型语言模型在智能合约漏洞检测中的应用”，*arXiv 预印本 arXiv:2504.04685*，2025年。

[19] AT Aspembitova 和 MA Bentley，“去中心化金融中的预言机：攻击成本、利润和缓解措施”，*熵*，第 25 卷，第 1 期，2023 年。

[20] J. Cole，“理解 Dai 智能合约审计：安全性、治理和影响”，*BlockApps*，2024年。

[21] Z. Chen、SM Beillahi、P. Barahimi、C. Minwalla、H. Du、A. Veneris 和 F. Long，“具有控制流完整性的安全智能合约”，*arXiv 预印本 arXiv:2504.05509*，2025年。

[22] L. Heimbach 和 R. Wattenhofer，“利用博弈论消除三明治攻击”，*2022年ACM亚洲计算机与通信安全会议论文集*，2022 年，第 153-167 页。

[23] F. Salzano、L. Marchesi、CK Antenucci、S. Scalabrino、R. Tonelli、R. Oliveto 和 R. Pareschi，“弥合差距：学术界和开发者对智能合约漏洞处理方法的比较研究” *arXiv 预印本 arXiv:2504.12443*，2025年。