Hyperliquid 2025 年 JELLY 攻击全解析：风险引擎、治理博弈与可验证复盘

摘要

2025 年 3 月 26 日，去中心化衍生品交易平台 Hyperliquid 经历了迄今为止最大规模的系统性冲击——**JELLY 攻击事件**。这起事件表面上看似一场由少数操盘账户引发的“投机性闹剧”，但实质上暴露了去中心化衍生品交易所内部三大核心机制的耦合失衡：**风险引擎的脆弱性、流动性供给机制的集中化、以及治理权力的边界模糊**。

一句话主张

JELLY 事件不是“单次投机闹剧”，而是去中心化衍生品交易所里 **风险引擎 × 流动性供给 × 治理权力** 三者耦合失衡的系统性暴露。

三大结论概览

1. **标记价与清算链路的可利用性**：在小市值资产叠加外部交易所情绪脉冲的场景下，价格发现机制被证明存在可行性利用空间。
2. **HLP 的系统性风险承接**：Hyperliquid Liquidity Provider（HLP）作为“最后买方+清算 backstop”的架构设计，使协议在极端行情中被迫承接巨额风险敞口。
3. **治理干预的两难**：验证人快速投票下架 JELLY 永续并以 **$0.0095** 的价格强制结算，虽保住了协议金库，却引发了关于“去中心化自治”与“合约公平性”的争议。

关键事实

- **时间节点**：2025 年 3 月 26 日，Hyperliquid 验证人紧急投票。
- **措施**：下架 JELLY 永续合约，并以 **$0.0095** 强制结算。
- **冲击规模**：HLP 浮亏一度高达 **约 1,350 万美元**。

- **攻击手法**：攻击者利用三账户，总计入金 **约 717 万美元**，通过双向对冲与外部抬价机制，成功将风险传导至协议层。

第一章 背景铺垫：Hyperliquid 是什么

要理解 2025 年 JELLY 攻击的技术背景，必须先从 Hyperliquid 的系统架构讲起。作为新一代去中心化衍生品交易所，Hyperliquid 在性能、流动性、清算与治理等方面采取了与以往 DeFi 协议截然不同的设计思路。这些创新为其赢得了高速发展，但也为后来的系统性风险埋下了伏笔。

1.1 架构鸟瞰：HyperL1、HyperCore 与 HyperEVM

Hyperliquid 自研了一条底层链 **HyperL1**，采用 **HyperBFT** 共识机制。与以太坊等通用 L1 相比，它的目标不是通用性，而是**为衍生品交易优化的高性能专用链**。在该链之上，核心功能被划分为三层：

- **HyperCore**：协议的“心脏”。负责链上订单簿的维护、清算逻辑执行、Vault 资金管理。换句话说，所有订单撮合、强平与风险转移，都在这里实现。
- **HyperEVM**：面向开发者的合约层。采用“双块架构”——一块负责状态共识，另一块负责执行与验证，从而兼顾速度与安全性。
- **外围设施**：包括验证人网络、预言机网络，以及基金会管理的治理接口。

这种垂直整合的架构，使 Hyperliquid 与传统依赖 zk-rollup 或 Optimistic Rollup 的衍生品协议有明显差异。它没有把撮合层外包给中心化撮合引擎，而是**把订单簿完全放在链上**，这是其最重要的技术标签之一。

1.2 订单簿与撮合：完全链上化的取舍

Hyperliquid 的核心卖点是 **完全链上订单簿（CLOB, Central Limit Order Book）**。所有挂单、撤单、撮合动作均在链上确认，每笔交易只需一块区块的时间即可完成。

相比之下，许多前辈协议（如 dYdX v3）采用“中心化撮合 + 链上结算”模式，或借助 zk-rollup 来加速撮合。Hyperliquid 的设计优点在于：

1. **透明性**：撮合与清算全在链上，避免“黑箱撮合”的争议。
2. **一致性**：链上状态即市场真相，消除了“撮合层与结算层不同步”的可能性。

但代价也很明显：

- **对链性能要求极高**，必须支撑毫秒级撮合与海量订单写入；
- **Gas 费用需控制**，否则无法与中心化交易所竞争。

HyperBFT 与 HyperCore 的结合，正是为此而生。

1.3 标记价与预言机：风险引擎的核心

在任何衍生品交易所，清算机制依赖于“标记价（mark price）”，而不是用户下单的瞬时成交价。Hyperliquid 在这方面设计了**三源合成中位数模型**，意在增强抗操纵能力：

1. **预言机源**：取各大 CEX 现货价格的加权中位数，约每 3 秒更新一次；
2. **内部源**：计算 Hyperliquid 内部中价（mid price）与预言机价格的偏差，并用 **150 秒指数滑动均值（EMA）**平滑，避免短时噪音；

3. **外部永续源**：汇聚主要中心化交易所的永续合约中价，按权重 **3/2/2/1/1** 进行加权。

最终标记价取这三源的中位数（median-of-three）。这意味着：

- 在多数情况下，标记价较难被单一市场操纵；
- 但在小市值资产上，若外部 CEX 永续价格剧烈波动，内部机制可能被动跟随。

正是这一点，为 JELLY 攻击提供了操作空间。

1.4 清算机制：分层与 backstop

Hyperliquid 的清算逻辑遵循分层触发：

- **初始条件**：当账户权益 < 维持保证金时触发清算；
- **大额仓位**：当头寸规模超过 100k USDC 时，系统首先对其进行 **20% 部分清算**，降低风险暴露；
- **极端条件**：当权益跌破维持保证金的 **2/3**，进入 **backstop 清算**环节，由系统性的承接者来接管。

这套机制的设计初衷，是尽量用市场流动性解决清算问题，仅在极端情况才调用协议金库。但在 JELLY 事件中，backstop 触发成为风险集中爆发的导火索。

1.5 HLP（Hyperliquidity Provider）：协议金库的双重身份

Hyperliquidity Provider (HLP) 是 Hyperliquid 独特的制度创新。它兼具两重角色：

1. **做市商**：HLP 资金池在日常交易中作为被动流动性提供者，从点差与交易费中获利；

2. **清算 backstop**：当用户仓位在市场无法被完全清算时，HLP 承接剩余头寸，并在后续市场修复中尝试获利。

在常态下，这一机制能有效提升市场深度，同时为 HLP 参与者带来稳定回报。但它也意味着：**极端行情下，HLP 会被动承接系统性风险**。在 JELLY 事件中，HLP 一度浮亏超过 1,350 万美元，正是这种机制的直接后果。

1.6 ADL（Auto-Deleveraging）：最后的保险阀

如果在清算与 backstop 承接之后，仍然存在负权益账户，Hyperliquid 会启动 **ADL（自动减仓）** 机制：

- 根据“**未实现 PnL × 杠杆倍数**”排序，选择盈利最高、杠杆最高的对手方账户；
- 对其进行强制减仓，以填补系统亏损；
- 保证协议不出现“坏账”，即用户资产不会因协议资不抵债而受损。

这套设计体现了 Hyperliquid **“不社会化亏损”**的理念，但也在极端情况下带来了对用户体验与公平性的冲击。

小结

从整体来看，Hyperliquid 在架构、撮合、清算和风险兜底上的创新，确实解决了前代 DeFi 衍生品平台的一些顽疾。但这种设计的另一面，是风险在极端行情下**高度集中于协议层**。JELLY 攻击正是利用了这些机制之间的张力，将市场波动放大为协议层面的系统性危机。

第二章 事件脉络与时间线

2025 年 3 月 26 日，Hyperliquid 平台在短短数小时内经历了一场前所未有的系统性危机。表面上，这似乎是一场围绕小币种 JELLY 的“拉盘与清算博弈”，但实际上，它揭示了链上订单簿、清算机制与治理干预三者之间的复杂交互。以下将以分钟级时间线的方式，重建这起事件的全过程。

2.1 攻击的起手式：三账户入金与仓位构造

当天早晨（UTC 时间），三个可疑账户陆续向 Hyperliquid 注入约 **7.17 百万美元 USDC**。与普通投机不同，这些账户采取了极为精巧的仓位结构：

- **账户 A**：建立大额空头头寸，对 JELLY 永续做空；
- **账户 B 与 C**：分别在 Hyperliquid 与外部市场构建多头头寸。

这一组合相当于“两多一空”的自对冲结构。攻击者的意图是通过在外部市场推高价格，迫使 Hyperliquid 的标记价机制跟随上调，从而让账户 A 的空单快速进入清算状态。

2.2 空头清算与 HLP 承接

随着外部市场 JELLY 价格被推高，Hyperliquid 标记价迅速偏离。账户 A 的空单触发清算，但由于仓位过大，订单簿流动性不足，**市场无法消化全部清算订单**。

根据清算规则，当权益跌破维持保证金的 **2/3**，系统会将剩余头寸移交给 **Hyperliquidity Provider（HLP）** 承接。于是：

- HLP 被迫接下大规模 JELLY 空单；
- 市场继续上行，导致 HLP 浮亏急剧扩大，峰值一度高达 **1,350 万美元**。

这标志着风险不再停留在攻击者与普通交易者之间，而是上升为**协议层系统性风险**。

2.3 外部利好消息与价格脉冲

几乎在同一时间，市场传出 **OKX 与 Binance 准备上线 JELLY 合约**的消息。该消息迅速引发投机热潮，推动 JELLY 在现货与永续市场双双飙升，涨幅一度达到 **400–560% 区间**。

价格的进一步上扬，反过来加剧了 HLP 的亏损曲线，使得协议层的资金压力急剧恶化。此时，Hyperliquid 内部已经出现“是否暂停市场”的紧急讨论。

2.4 验证人紧急治理：下架与强制结算

危机持续发酵数小时后，Hyperliquid 验证人启动紧急会议。根据治理结果：

- **决定下架 JELLY 永续合约**，防止风险继续扩大；
- **强制结算价格锚定在 $0.0095**，恰好与攻击者空单的开仓价一致。

这一决策在技术层面遏制了 HLP 的进一步损失，相当于“人为切断风险链条”。但同时，它也立即引发了关于**去中心化交易所是否应由少数验证人干预市场**的争议。

2.5 事后安排：补偿与争议

事件结束后，Hyperliquid 基金会宣布：

- **普通用户**（未被标记为攻击相关的钱包）将得到基金会补偿，避免直接损失；
- **攻击者账户**被限制提取部分资金，约 **900 万美元中的 626 万美元被提出**，剩余约 **90 万美元被冻结**；
- 攻击者的最终结果被估算在 **-100 万美元到 -4,000 美元之间**，几乎是一次“空忙一场”的失败攻击。

然而，外部质疑并未平息。批评者指出：

- “强制结算”本质上是一种中心化行为，与 DeFi 强调的自治与不可篡改相冲突；
- 在公平性上，结算价 $0.0095 过于接近攻击者建仓价，可能构成“政策性救助”；
- 对 HLP 的巨大浮亏，暴露了其“做市+清算 backstop”双重身份的风险集中性。

2.6 侧线因素：CEX 宣布与情绪共振

除了 Hyperliquid 内部的链上清算，事件的另一条关键脉络是 **CEX 公告与市场情绪的共振**：

- 攻击者在外部现货/永续推高价格；
- OKX 与 Binance 的“上线预期”加速了价格脉冲，使标记价跟随失真；
- 最终形成了一种“外部消息推动—内部清算加速”的正反馈回路。

这说明 JELLY 攻击不仅是链内博弈，还与链外市场的行为紧密耦合。

2.7 时间轴复盘

以下为 2025 年 3 月 26 日关键节点复盘：

Code block

```
timeline
    title JELLY 攻击事件时间轴
    2025-03-26 08:00 : 三账户入金 ~7.17m USDC，建立“两多一空”结构
    2025-03-26 09:00 : 外部市场被推高，JELLY 价格快速上行
    2025-03-26 09:30 : 空头仓位触发清算，市场流动性不足，移交 HLP
    2025-03-26 10:00 : HLP 浮亏突破 1,000 万美元
    2025-03-26 11:00 : OKX/Binance 上线预期扩散，JELLY 飙升至 +400-560%
    2025-03-26 12:00 : 验证人紧急会议，决定下架 JELLY 永续
    2025-03-26 12:30 : 强制结算价定为 $0.0095，市场关闭
    2025-03-26 14:00 : 基金会声明补偿机制，冻结攻击者部分资金
```

小结

整个 JELLY 攻击事件，虽然持续时间仅数小时，却浓缩了去中心化衍生品市场最核心的三重矛盾：

1. **标记价与流动性**：在小币种中存在被利用的可能性；
2. **HLP 的双重身份**：做市与 backstop 让协议在极端行情中暴露于巨额亏损；
3. **治理的两难选择**：验证人投票下架，既是止损手段，也是“去中心化信仰”的一次挑战。

这一事件不仅改变了 Hyperliquid 的发展轨迹，也为整个 DeFi 衍生品生态敲响了警钟。

第三章 对手方建模：攻击路径与收益函数

JELLY 事件并不是一次单纯的“莽撞豪赌”，而是一套经过精心设计的结构化攻击。攻击者深刻理解了 Hyperliquid 的风险引擎与清算链路，利用账户分拆、价格传导与清算机制耦合，制造出一个能把亏损传递到协议层的自对冲结构。

3.1 仓位结构设计：三账户与“两多一空”

攻击者在事件开始前准备了三个核心账户：

- **账户 A（空头账户）**：在 Hyperliquid 上开立大额 **JELLY 空头**，仓位远超正常市场流动性承载范围。
- **账户 B（多头账户）**：在 Hyperliquid 内部建立多单，用于对冲部分风险。
- **账户 C（外部账户）**：在 CEX/DEX 上拉抬 JELLY 现货或永续，制造价格上行压力。

这样，攻击者就形成了**“两多一空”的自对冲组合**。

- A 的空单是“风险转移工具”；
- B 与 C 的多头是“价格推手 + 盈利出口”。

其核心目标并不是直接靠方向性盈利，而是通过 **清算传递** 把风险甩给 **HLP**。

3.2 价格驱动手段：外部市场 → 标记价 → 清算引擎

Hyperliquid 的标记价机制由三部分组成（预言机中价、内部中价 EMA、外部永续加权）。这意味着：

- 如果外部现货/永续市场出现剧烈上行，**标记价会被动跟随**；
- 只要推高外部成交与中价，就能影响 Hyperliquid 的清算触发逻辑。

攻击者利用账户 C，在外部市场用资金拉升 JELLY，使其价格短时间内上涨数倍。随后，这一涨幅被标记价模型传导到 Hyperliquid → 账户 A 的空单权益迅速缩减 → 进入清算流程。

3.3 清算链路的关键拐点

清算不是一次性完成，而是逐层触发的：

市场清算（Market Liquidation）

系统先将空单挂入订单簿，尝试由市场承接。但 JELLY 市场深度有限，仅部分成交。

部分清算（Partial Liquidation）

对 >100k USDC 的头寸，先进行 20% 部分清算。但规模依旧过大，剩余头寸难以消化。

权益跌破 2/3 维持保证金

当 A 的权益进一步缩水，触发 **Backstop 条件**。

Backstop → HLP 承接

剩余仓位强制移交给 HLP（协议资金池）。这一步至关重要：

> 亏损从攻击者个人转移到协议层；
>
> 攻击者“卸包袱”，而 HLP 接过了巨额空头。

HLP 风险内生化

市场继续上行，导致 HLP 浮亏滚大（峰值约 1,350 万美元）。

序列图：攻击路径与清算传递

Code block

```
sequenceDiagram
    participant A as 账户A（空头）
    participant B as 账户B（HL 多头）
    participant C as 账户C（外部多头）
    participant HL as Hyperliquid清算引擎
    participant M as 市场订单簿
    participant HLP as HLP资金池

    C->>M: 外部抬价（现货/永续推高）
    M->>HL: 标记价上升
    HL->>A: 空头权益缩水，触发清算
    HL->>M: 挂清算单（部分成交）
    M-->>HL: 流动性不足，未完全成交
    HL->>HLP: 剩余仓位移交
    HLP->>HL: 承接空头，开始浮亏
    B->>HL: 多头账户获利
    A->>HL: 空头账户仓位被剥离
```

3.4 收益函数建模

攻击者的收益可以抽象为：

$$\Pi_{attacker} = PnL_B + PnL_C - L_A$$

其中：

- PnL_B：在 Hyperliquid 内部的多头盈利；
- PnL_C：在外部市场（CEX/DEX）拉盘后的套利/出货收益；
- L_A：空头账户的损失，但在 HLP 承接后大部分被转移。

换句话说，攻击者通过账户 A 制造一个**“负资产甩锅”**，把真实损失交给 HLP，自身则通过 B 和 C 实现盈利。

关键收益函数特征：

- **风险非对称**：亏损有限（被强制平仓即可止损），潜在收益取决于能否把 HLP 拉下水；
- **收益上限受限于治理干预**：如果验证人不人为收盘，价格继续拉升，攻击者可能大赚；一旦收盘，收益被截断。

3.5 退出路径与最终结果

攻击者的退出过程经历了几个阶段：

1. **HLP 承接后**，账户 B 和 C 的多单盈利迅速增加；
2. **提款阶段**：攻击者尝试提取抵押品，成功提走约 **6.26 百万美元**；
3. **资金限制**：约 **0.9 百万美元**被冻结，部分资金无法提出；
4. **市场收盘**：验证人以 $0.0095 强制结算，攻击通道被截断。

最终，攻击者的净结果在 **-100 万美元至 -4,000 美元之间**，几乎空忙一场。

3.6 小结

通过账户分拆、价格操纵与清算传递，攻击者成功把 Hyperliquid 的风险引擎“打穿”，让本该属于个人的损失转移到了协议金库（HLP）。虽然最终由于治理干预未能成功获利，但整个攻击路径表明：

- **仓位结构设计**：三账户协同，形成自对冲；
- **价格驱动手段**：利用外部市场影响标记价；
- **清算链路拐点**：市场流动性不足导致风险移交；
- **退出路径**：盈利账户提款，失败原因在于人为收盘。

这一模型揭示了 Hyperliquid 事件的核心逻辑：攻击者并不需要“对赌价格方向”，而是利用制度空档，把系统设计本身变成收益工具。

第四章 风险引擎技术细剖

Hyperliquid 的风控设计是其最具特色的部分，也是 JELLY 攻击得以实施的关键。其风险引擎由 **标记价体系 → 保证金曲线 → 清算层级 → Backstop 承接 → ADL** 五个环节串联。整体目标是确保平台无坏账，但在极端小币种行情下，部分设计反而成为攻击者可利用的“系统性杠杆”。

4.1 标记价数学：三源合成与 EMA 平滑

在衍生品市场，标记价（mark price）决定了清算是否触发。Hyperliquid 的标记价采用“三源合成中位数”机制，公式如下：

$$MarkPrice_t = \text{Median}\left\{ P_{oracle},\ EMA_{150s}(Mid_{HL} - P_{oracle}),\ \sum_{i=1}^{n} w_i P_i^{perp} \right\}$$

其中：

- P_{oracle}：由各大中心化交易所（CEX）现货价格加权中位数，每 3 秒更新一次；
- EMA_{150s}(Mid_{HL} - P_{oracle})：Hyperliquid 内部中价与预言机价格差值的 150 秒指数滑动均值，用于平滑短时偏差；
- P^{perp}_i：来自主要 CEX 永续合约的中价，权重比为 3:2:2:1:1；
- Median\{\}：取三者的中位数，以减少单一来源操纵的风险。

优点：

- 在大币种（BTC、ETH）中，外部永续与现货价格深度充足，不易操纵；
- EMA 平滑可避免短时尖峰直接触发清算。

脆弱点：

- 在小市值资产中（如 JELLY），外部永续流动性薄弱，稍有成交就能显著推高中价；
- 权重偏向外部永续，意味着一旦外部被拉升，Hyperliquid 的标记价被动跟随 → 清算触发。

这正是攻击者在 3 月 26 日利用外部市场“推价—传导—清算”的路径。

4.2 保证金曲线与杠杆限制

Hyperliquid 允许不同资产设置不同的杠杆上限与保证金曲线。其核心是：

- **初始保证金（IM, Initial Margin）：开仓时必须具备的抵押率；**
- **维持保证金（MM, Maintenance Margin）**：仓位存续所需的最低抵押率；
- **杠杆倍数上限**：根据资产流动性与波动性动态设定。

保证金关系式

$$IM = \frac{Notional}{Leverage_{max}}$$

$$MM = \alpha \cdot IM \quad (0 < \alpha < 1)$$

其中 α 通常在 0.5–0.7 之间。

部分清算与冷却窗口

- 对单笔 >100k USDC 的仓位，系统会先做 **20% 部分清算**，以降低冲击。
- 每次部分清算之间有 **30 秒冷却窗口**，避免过度连续抛压。

隐含风险：

- 在小币种剧烈波动时，30 秒窗口可能给攻击者时间继续推高外部价格，使清算难以及时追上风险扩散。

4.3 Backstop 承接与 HLP 收益函数

当账户权益跌破 **维持保证金的 2/3**，市场清算不足的仓位进入 Backstop，由 **Liquidator Vault/HLP** 承接。

HLP 收益逻辑

在常态下，HLP 的预期收益函数：

E[Profit] = Fees + Spread\;PnL + \sum_{liq} (Discount_{liq})

- **Fees**：手续费分成；
- **Spread PnL**：日常做市点差收益；
- **Discount_{liq}**：清算承接折扣，理论上是低风险套利。

因此，HLP 平时是“正期望值生意”。

极端尾部风险

在极端行情（如 JELLY 攻击）下：

- 单一资产敞口超出 HLP 风险预算；
- 承接价格与市场继续上涨价差拉大，浮亏集中化；
- 最终导致 HLP 在短时间内浮亏 >1,350 万美元。

这里暴露出 **“保险基金角色 + 做市商角色”重叠** 的风险：在小币种里，HLP 承接风险不可分散，集中化严重。

4.4 ADL（Auto-Deleveraging）：最后的兜底

如果即使 HLP 承接后仍然存在负权益账户，Hyperliquid 会启动 **ADL（自动减仓）**。

触发条件

当某些账户的权益无法覆盖亏损时：

- 平台按照 **未实现 PnL × 杠杆倍数** 进行排名；
- 盈利最高、杠杆最高的账户会被优先减仓；
- 所得资金用于填补负权益。

公式化

Priority_i = PnL_i \times Leverage_i

账户 i 的优先级越高，被减仓的概率越大。

与 CEX 对比

- **Bybit/Deribit** 等 CEX 也有 ADL，但通常有庞大保险基金缓冲，ADL 触发概率极低；

- **Hyperliquid** 的理念是“无坏账”，即使没有大基金，也保证通过 ADL 把风险锁回交易者。

公平性争议

- 从系统角度看，ADL 确保“不社会化亏损”；
- 从交易者角度看，被动减仓会打断盈利头寸，尤其在高杠杆下显得不公平；
- JELLY 事件中，虽然未到全面触发 ADL，但已经让社区担心“小币种风险最终可能殃及无辜交易者”。

4.5 参数表：风险引擎关键参数

模块	参数/机制	默认值/特性	潜在脆弱点
标记价	三源合成中位（预言机、HL EMA、CEX 永续）	权重 3/2/2/1/1，3 秒更新，150s EMA	小币种外部永续易操纵
初始保证金	IM = Notional / Leverage_max	动态随资产设定	高杠杆资产放大脆弱性
维持保证金	MM = α × IM	α = 0.5–0.7	MM 太低时清算延迟
部分清算	>100k USDC 仓位先清算 20%	冷却窗口 30 秒	极端行情下追不上价格
Backstop	Equity < 2/3 MM 触发，HLP 承接	平时赚溢价，极端时集中爆亏	HLP 风险预算缺乏上限
ADL	PnL × Leverage 排序减仓	确保系统无坏账	高盈利用户被动受损

小结

Hyperliquid 的风险引擎设计初衷是：**链上透明 + 无坏账 + 用户不摊平**。但在 JELLY 事件中：

1. **标记价机制**在小币种被外部操纵；
2. **部分清算与冷却窗口**未能及时拦截风险；
3. **Backstop** 把风险集中到 HLP，引发系统性浮亏；
4. **ADL** 虽未全面触发，但其潜在公平性问题被放大。

这表明，Hyperliquid 的风控逻辑在主流大币种上表现稳健，但在小市值资产上存在结构性脆弱性。

第五章 流动性与做市：HLP 的系统角色

在去中心化衍生品交易所 Hyperliquid 的生态中，**Hyperliquidity Provider（HLP）** 是一个独特的制度性角色。它既不是传统意义上的做市商，也不是单纯的保险基金，而是两者的结合体。HLP 平时为市场提供稳定的深度与点差，极端情况下则充当“最后买单侠”，承接清算无法成交的残余仓位。正因如此，HLP 在 Hyperliquid 的架构中具有双重身份。

5.1 常态下的 HLP：做市与收益分享

在正常市场环境中，HLP 的运作逻辑类似于一个 **协议级别的被动做市资金池**：

- **流动性供给**：HLP 资金按照预设策略在订单簿挂单，缩小买卖点差，提升交易深度；
- **收益来源**：

    a. **交易费分成**：所有用户交易手续费的一部分归入 HLP；

b. **点差收入**：在多空双边做市过程中获取价差；

c. **清算溢价**：在承接部分清算仓位时，以折扣价买入/卖出，理论上可赚取无风险收益。

- **社区参与**：任何用户都可以将资金存入 HLP，按份额分享其 PnL。这让 HLP 既是做市工具，也是社区收益共享池。

在多数时间里，HLP 的收益曲线相对平滑，是平台稳定性的关键支柱。

5.2 极端情况下的 HLP：清算 Backstop

当市场深度不足以完全消化清算仓位时，HLP 就会进入另一重身份：**清算 backstop**。

- 当权益 < 维持保证金的 2/3 时，仓位剩余部分移交给 HLP；
- HLP 直接接过头寸，从此开始承担未实现盈亏；
- 这避免了系统坏账，但等于把个人风险转化为协议风险。

这一机制的设计逻辑是“集中风险、避免社会化亏损”。对普通交易者而言，这是友好的；但对 HLP 本身而言，则是一次“黑天鹅下注”。

5.3 JELLY 事件中的 HLP：风险集中化的极限暴露

在 JELLY 攻击事件中，HLP 的弱点被彻底放大。

- **单资产风险过度集中**

- 攻击者构建了超大规模空单；
- 市场流动性不足，大部分仓位被强制移交给 HLP；
- HLP 在单一资产上累积了异常庞大的敞口，无法分散。

- **无法快速对冲**

  - HLP 是协议金库，不具备像传统做市商那样的灵活外部对冲能力；
  - 即便想要在外部市场对冲，JELLY 这样的小币种在 CEX/DEX 的深度本来就不足；
  - 这意味着 HLP **被迫裸露风险**，在价格继续飙升时浮亏急剧扩大。

- **浮亏规模前所未有**

  - 峰值浮亏超过 **1,350 万美元**，远远超过 HLP 平时的利润缓冲；
  - 这让整个协议处于“系统性不稳定”状态，直接触发验证人治理干预。

5.4 系统性启示

JELLY 事件说明了 HLP 在 Hyperliquid 架构中的两难：

- 平时是市场稳定器，提供深度和收益；
- 极端情况下却可能成为“风险吸尘器”，被动吞下市场无法承接的风险。

这对协议提出了新的挑战：

1. **单资产风险限额**：未来必须对 HLP 在单个资产上的风险敞口设置上限，避免过度集中；
2. **分层 backstop**：设计多级保险池，让风险逐层分散，而不是一次性压在 HLP 上；
3. **动态对冲机制**：探索让 HLP 在极端行情下，能与外部 CEX 建立自动对冲桥梁。

小结

HLP 在 Hyperliquid 中扮演的是“常态下赚钱、极端时救火”的双重角色。JELLY 事件之所以造成如此大的冲击，并非因为 HLP 机制本身完全错误，而是因为它在小市值资产的极端行情中，承接了超出设计预期的风险敞口。如何在保持 HLP 正期望收益的同时，降低其在极端场景下的系统性风险，将是 Hyperliquid 风控演进的关键。

第六章 治理与合约公平性：验证人“熄火”是否正当？

JELLY 攻击事件的另一个核心冲击点，并不在交易链路本身，而是在 **治理层面的应急处置**。当 Hyperliquid 的 HLP 出现超过千万美元的浮亏时，验证人网络紧急介入，选择下架合约并以 **$0.0095** 的价格强制结算。这个决定让平台躲过了潜在的“协议破产”，但也引发了关于 **去中心化边界、公平性与治理合法性** 的激烈讨论。

6.1 谁在投票：验证人格局与权重分配

当时 Hyperliquid 主网的验证人网络规模相对有限，约 **16 个活跃验证人**。其中：

- **基金会节点**与早期核心团队成员占据较大权重；
- 社区节点比例有限，整体治理权力结构呈现出“半去中心化”状态；
- 由于链上交易对撮合需要高性能，验证人门槛偏高，进一步限制了小型独立参与者的进入。

因此，在 3 月 26 日的紧急会议中，虽然形式上是“去中心化投票”，但实质上 **基金会和少数大验证人** 的意见起到了决定性作用。

事件之后，团队宣布计划逐步扩容验证人网络，开放更多无许可参与，并提高投票过程的透明度。这被视为对“治理过度集中化”批评的直接回应。

6.2 紧急处置的边界

合约自治 vs 安全停牌

Hyperliquid 的品牌价值之一，正是“完全链上自治、规则即合约”。然而在 JELLY 事件中，验证人选择：

- **下架 JELLY 永续合约**；
- **强制结算价锚定 $0.0095**。

这相当于在运行中的合约上 **人为按下“熄火开关”**。

支持者认为：

- 如果不这么做，HLP 浮亏可能扩大到不可控范围，危及整个协议存续；
- 这与中心化交易所的“临时停牌/熔断”类似，本质是风险控制。

反对者则指出：

- 这背离了 DeFi “合约自治、不可篡改” 的核心信条；

- 一旦有了先例，用户无法确认未来是否还会遭遇类似“人为干预”。

$0.0095 的价格公平性

更具争议的是 **结算价的锚定点**：

- 该价格与攻击者空单的开仓价高度接近；
- 对攻击者来说，等于“刚好锁定了亏损，不再扩大”；
- 对多头用户而言，潜在的更多盈利被直接截断。

这种做法引发了“选择性救助”的质疑：为何要以如此有利于攻击者的价位结算，而不是取事件时的市场中价或其他更透明的规则？

一部分社区声音认为，这相当于协议为了自保，牺牲了市场公平性。

6.3 “去中心化”预期管理

JELLY 事件后的另一大课题，是 **如何与社区沟通和修复信任**。

- **官方声明与补偿承诺**
  - 基金会第一时间承诺：除被标记为攻击相关的钱包外，**其他用户将获得补偿**；
  - 这在短期内稳定了普通用户的信心，避免了大规模流动性撤离。
- **数据透明度**

- 团队公布了攻击者地址、入金与提现规模（约 7.17m 入金，6.26m 提走，0.9m 冻结）；
- 还披露了 HLP 的浮亏曲线（峰值 ~13.5m），为“治理干预的必要性”提供佐证。

- **预期管理与长期信任**

- 团队强调：“这是一次极端个案，而非常态”；
- 同时承诺扩容验证人、改进风险引擎、建立透明的紧急治理流程；
- 试图把此次事件包装成“系统升级的契机”。

然而，部分用户仍对“人为干预的正当性”保持怀疑：如果协议可以随时改变合约逻辑，那么去中心化的价值主张是否还成立？

6.4 正当性辩论

从治理学角度看，JELLY 事件中的“熄火”既有现实正当性，也有制度缺陷：

- **现实正当性**：

- 防止 HLP 爆仓 → 维护协议整体存续；
- 补偿大多数无辜用户 → 缓解社会性损失。

- **制度缺陷**：

- 投票过程集中化，基金会权重过大；
- 强制结算价缺乏透明规则，存在“临时拍脑袋”嫌疑；
- 破坏了“规则不可篡改”的预期，削弱了长期信任。

这种两难，恰恰反映了 **DeFi 协议在自治与安全之间的张力**。

小结

JELLY 事件不是单纯的技术性清算事故，更是一场 **去中心化治理危机**：

- 验证人紧急投票的“熄火”行为救了协议，却也伤害了“不可篡改”的信条；
- 结算价 $0.0095 的选择让公平性受到质疑，成为长期争论点；
- 社区补偿与治理扩容虽修补了短期信心，但能否恢复长期信任，仍取决于协议如何定义“去中心化治理的边界”。

Hyperliquid 最终要面对的问题是：**它究竟是一个完全自治的链上衍生品协议，还是一个在危机时刻仍然需要人为干预的“半去中心化交易所”？**

第七章 对比案例：从 Mango Markets 到 Hyperliquid

在 JELLY 攻击的复盘中，很多人第一时间联想到了 2022 年的 **Mango Markets 攻击事件**。这两起事件在结构设计上有诸多相似点：都利用了 **低流动性资产** 与 **清算机制缺陷**，通过操纵价格输入源，把个人损失转嫁给协议。但也存在显著差异，尤其在清算承接方式与治理处置逻辑上。

7.1 Mango 2022 攻击回顾

2022 年 10 月，一名攻击者在 Solana 上的 Mango Markets 平台，利用 **MNGO 代币的低流动性**，通过外部市场拉高价格，导致平台的预言机价格严重偏离。

- 攻击者先大规模做多 MNGO 永续；
- 再在外部市场通过资金推高现货价格，预言机将高价同步到 Mango；
- 结果导致攻击者账户的抵押品价值虚高，得以抵押借出约 1 亿美元资产。

最终，Mango 社区只能通过治理提案与攻击者谈判，回收部分资金，留下“DeFi 历史上最著名的预言机操纵案”之一。

7.2 Hyperliquid JELLY 攻击的相似性

JELLY 攻击与 Mango 的逻辑相似：

- **攻击基础相同**
  - 都是 **小市值资产**（MNGO/JELLY）；
  - 都通过外部市场推高价格 → 内部标记价/预言机被动跟随。
- **收益模式相似**
  - 攻击者都没有靠方向性投机赚钱；
  - 而是利用“抵押/清算机制”把系统推到一个反常状态，然后提走资金。
- **风险转移方式**

- Mango：通过虚高抵押借款，把坏账留给协议；
- Hyperliquid：通过清算传递机制，把巨额空头甩给 HLP。

7.3 关键差异

虽然结构相似，但两者存在关键差异：

- **清算承接主体不同**
  - Mango：系统允许攻击者直接借走协议资金，风险由全体用户摊平；
  - Hyperliquid：风险集中到 HLP，由金库承担，不波及普通用户。
- **治理动作不同**
  - Mango：事后治理，社区投票与攻击者谈判，补救为主；
  - Hyperliquid：事中治理，验证人直接“熄火”，下架合约并强制结算。
- **风险集中度不同**
  - Mango：坏账社会化，整个协议生态受损；
  - Hyperliquid：坏账集中化，HLP 独吞风险，但引发“中心化治理”质疑。

7.4 对比结论

Mango 与 Hyperliquid 的对照揭示了去中心化衍生品平台面临的共同困境：

- **小币种与价格输入**是天然的攻击切口；
- **清算机制**决定了风险最终落在“谁的头上”。

Hyperliquid 的设计避免了 Mango 式的社会化亏损，但引入了 **治理干预的先例风险**。某种意义上，Mango 是“协议没管住攻击者的钱”，而 Hyperliquid 是“协议管住了攻击者，但动摇了自治信仰”。

第八章 根因分析：从“可被利用”到“可被工程化防御”

JELLY 攻击不是偶然事件，而是 DeFi 衍生品在 **市场结构—风险引擎—治理模式** 三个维度叠加脆弱性的必然结果。通过根因分析，可以看出哪些是短期修补问题，哪些是长期架构性挑战。

8.1 小市值资产与单边深度

症结 1：小市值 + 单边深度不足

- JELLY 在 CEX/DEX 的现货与永续市场，本身深度有限；
- 攻击者用较少资金即可推高中价，足以影响 Hyperliquid 的标记价。

跨场景联动效应

- 当 CEX 公布“即将上线合约/现货”的消息时，投机情绪同步爆发；
- Hyperliquid 的标记价机制无法区分“真实需求”与“外部脉冲操纵”，被迫跟随。

这让 **外部消息与内盘清算**形成了强耦合的正反馈回路。

8.2 HLP 风险集中与风控颗粒度

症结 2：HLP 风险集中化

- 作为 backstop，HLP 理论上能承受中等规模的个别清算；
- 但在单资产极端行情下，HLP 被迫承接巨额仓位，风险集中到一个资金池。

风控参数颗粒度不足

- Hyperliquid 没有对单一资产设置 **开放仓位上限（OI cap）** 或 **移交限额**；
- 缺少分仓器，导致攻击者可通过单账户或多账户堆叠巨仓；
- 结果是风险在毫无缓冲的情况下全压到 HLP。

8.3 治理延迟与信息披露缺口

症结 3：治理链路存在延迟

- 从市场异动到 HLP 巨额浮亏，再到验证人开会、投票、执行，有数小时延迟；
- 在这段时间里，攻击者已经完成了提款操作。

信息披露缺口

- 普通用户无法实时看到 HLP 的头寸风险暴露；
- 直到官方公告与链上分析机构披露，社区才知道浮亏规模。

这种“事后才知道真相”的模式，削弱了社区对治理决策的信任。

8.4 三大根因总结

1. **外部输入源脆弱**：小市值资产被外部脉冲轻易劫持，标记价失真；
2. **内部风险预算缺乏**：HLP 无单资产限额，风险过度集中；
3. **治理与信息透明度不足**：紧急会议的流程和数据披露缺口，导致社区质疑。

8.5 工程化防御方向

要避免类似事件重演，需将防御手段工程化：

- **价格输入层**
    - 对小币种降低外部永续权重；
    - 引入异常检测与熔断机制。

- **风险预算层**
  - 为 HLP 设置单资产 OI/移交流限额；
  - 增设“分层 backstop”，将风险分散到多个池子。
- **治理执行层**
  - 建立明确的“停牌与重启”规则，而非临时投票拍板；
  - 实时公开 HLP 的风险敞口与浮亏曲线。

小结

JELLY 事件的根因不在某个 bug，而在于：

- **市场结构脆弱**（小市值易操纵）；
- **协议架构集中风险**（HLP 集中承接）；
- **治理机制反应慢与透明度不足**。

这表明，DeFi 协议要想在长远上稳健，必须从“被动应对”走向“工程化防御”，把每个可被利用的点都用制度化、参数化、透明化的方式加固。

第九章 数据复盘与可重复验证（工程手册）

要让 JELLY 攻击事件真正成为“可研究、可改进”的案例，仅靠新闻描述是不够的。工程师和研究人员需要能够 **从链上/链下数据重建全过程**，并模拟不同参数下的风险敞口。以下提供一份可操作的复盘手册。

9.1 数据抓取清单

- **Hyperliquid 内部数据**
  - **区块数据**：区块高度、交易哈希、时间戳（可通过官方 explorer 或 API 获取）；
  - **成交事件**：买卖方向、成交量、成交价、账户地址；
  - **清算事件**：触发时间、清算金额、仓位规模、承接方；
  - **HLP vault 状态**：资金池余额、已承接仓位、浮盈/浮亏曲线；
  - **标记价时间序列**：三源数据的实时更新值（预言机、内部 EMA、外部永续）。
- **外部市场数据**
  - **CEX 永续合约价格**：Binance/OKX 等的分钟级中价、盘口深度；
  - **现货价格数据**：外部成交与中价，用于验证预言机源；
  - **公告与新闻时间戳**：OKX/Binance 上线 JELLY 的公告时间，配合链上波动。

9.2 复盘步骤

- **时间线重建**
  - 将 Hyperliquid 区块数据与外部价格数据按分钟级对齐；

- 标记关键事件：入金、建仓、清算触发、HLP 承接、提款、治理投票、收盘。

- **标记价计算**

  - 逐分钟重建三源合成：
  - MarkPrice_t = Median \{ P_{oracle}, \; EMA_{150s}(Mid_{HL} - P_{oracle}), \; \sum w_i P^{perp}_i \}
  - 分析各源的贡献度，确认外部永续在事件中的“主导作用”。

- **清算链路模拟**

  - 还原账户 A（空头）的权益曲线，确定清算触发点；
  - 模拟部分清算（20%）与冷却窗口（30s）的执行效果；
  - 重建“市场成交不足 → Backstop 承接”的仓位流转。

- **HLP PnL 曲线**

  - 计算 HLP 每分钟的承接仓位与浮盈浮亏；
  - 绘制峰值浮亏 ~1,350 万美元的动态曲线。

- **最坏情况估计**

  - 假设验证人未干预：
    - 市场继续拉升至公告预期价（如 0.05–0.06 USDC）；
    - 估算 HLP 最坏浮亏范围；
    - 判断 ADL 是否会触发（计算对手方未实现 PnL × 杠杆分布）。

9.3 可视化与图表建议

1. **分钟级时间轴**：入金 → 抬价 → 清算 → HLP 浮亏 → 收盘 → 补偿声明。
2. **标记价 vs 外部中价曲线**：展示三源合成如何跟随外部市场。
3. **HLP PnL 曲线**：浮亏随时间扩大的动态图。
4. **ADL 排序模拟**：展示若触发 ADL，哪些账户会被减仓。

9.4 参考接口与工具

- **Hyperliquid API**：行情、清算、标记价序列。
- **Hyperliquid Explorer**：区块与交易追踪。
- **CEX 公共 API**：Binance/OKX 永续与现货数据。
- **链上分析工具**：Dune/Flipside，可建立跨源数据表。
- **时间对齐工具**：Python + Pandas，建议统一到 UTC。

小结

通过上述数据抓取与模拟流程，任何研究者都可以在本地复盘 JELLY 攻击事件。这样不仅能验证新闻报道的准确性，还能在“若不干预”的假设下，量化 HLP 的极端损失与 ADL 的触发概率，为协议未来改进提供客观依据。

第十章 改进建议（面向协议）

JELLY 事件揭示了 Hyperliquid 风控与治理的薄弱环节。为避免类似情况重演，需要从 **小币种风控、标记价鲁棒性、清算引擎迭代、治理合规** 四个方面进行工程化改进。

10.1 小币种风控分层

- **单资产 OI 限额**
  - 设置单一资产的最大开放仓位 (Open Interest Cap)，超过即禁止新增仓位；
  - 动态调整上限，与该资产的外部流动性挂钩。
- **移交流程限额**
  - 限制单一资产的清算移交流量，超过阈值时触发分段承接；
  - 避免 HLP 在极端时一次性吞下所有仓位。
- **HLP 承接上限与动态分配**
  - 设计多层 HLP 池：主池承接主流资产，子池承接小币种；
  - 风险分散而非集中在一个资金池。
- **熔断/停牌机制**
  - 当价格偏离预言机或外部中价超过设定阈值，自动停牌；
  - 重启市场需经过治理投票与参数披露。

10.2 标记价鲁棒性增强

- **动态权重调整**
  - 在极端异动时，降低外部永续源的权重；
  - 提升内部订单簿—EMA 的作用，以减少外部冲击。
- **多路独立喂价**
  - 引入更多独立预言机，交叉验证价格；
  - 异常源自动剔除，避免单点操纵。
- **异常偏离检测**
  - 实时监测 HL 内部成交价与标记价偏差；
  - 超过阈值时触发预警或自动熔断。

10.3 清算引擎迭代

- **更细颗粒的部分清算**
  - 将 20% 部分清算改为分级机制（如 10%+10%），缩短冷却窗口；
  - 避免大额仓位在 30s 窗口中继续失控。
- **撮合/回收窗口自适应**

- 根据资产流动性自动调整清算速度；
- 小币种更谨慎，大币种更激进。

- **Backstop 竞价化**

  - 清算仓位优先抛向外部流动性提供者，HLP 仅作最后承接；
  - 避免 HLP 一家独吞全部风险。

10.4 治理与合规

- **验证人集扩容**

  - 降低验证人门槛，增加社区节点比例；
  - 减少基金会的中心化权重。

- **权限无许可化路线图**

  - 明确治理流程：合约上新、下架、熔断，全部链上公开执行；
  - 减少临时人为干预的随意性。

- **投票透明化**

  - 公布所有验证人的投票记录与理由；
  - 引入链上可审计的治理追踪。

- **补偿/黑名单规则的事先披露**

  - 明确规定何种情况下用户可被补偿或列入黑名单；

- 避免事件发生时“边走边定”的不确定性。

- **外部合规对接**

  - 在接入 CEX 数据与价格时，建立合规披露接口；
  - 减少因公告/预期带来的情绪冲击。

小结

通过以上改进，Hyperliquid 可以在维持“高性能链上衍生品交易”优势的同时，显著降低小币种带来的系统性风险。尤其是：

- **风控分层** 避免 HLP 成为“风险黑洞”；
- **标记价优化** 提升抗操纵能力；
- **清算引擎升级** 改善尾部风险应对；
- **治理与合规改造** 恢复去中心化的长期信任。

JELLY 攻击是一次“压力测试”，而不是终点。能否将其转化为制度化防御，将决定 Hyperliquid 在下一轮 DeFi 竞争中的地位。

第十一章 交易者 / LP 的实务清单

JELLY 攻击事件说明，即便协议层有风险引擎，交易者和 LP 仍需主动管理风险。以下是一份面向实务操作的清单。

11.1 市场监控指标

- **单资产深度 / 换手率**
  - 查看盘口挂单量、24h 成交额；
  - 若成交额小于潜在清算仓位的 10%，需谨慎开杠杆。
- **标记价 vs 中价偏离**
  - 标记价过快跟随外部市场，可能是被操纵信号；
  - 偏离超过 ±3% 应提高警觉，尤其在小币种。
- **HLP 资产集中度**
  - 监控 HLP 在单一资产的敞口比例；
  - 若 >15–20%，说明协议层风险已集中。
- **ADL 排序指标**
  - 关注自身在“未实现 PnL × 杠杆”中的排序；
  - 若在前列，一旦系统触发 ADL，就可能被减仓。

11.2 仓位管理与跨场景对冲

- **仓位 Sizing**

- 单资产仓位不超过账户净值的 20–25%；
- 杠杆不超过协议最大允许值的一半。

- **跨场景对冲**

  - 在公告/新合约上市等高波动窗口，避免裸露过度杠杆；
  - 可通过 CEX 永续或现货进行对冲，降低“单点失真”风险。

- **流动性环境选择**
-

  - 优先在主流币种进行高杠杆操作；
  - 小币种仅适合低杠杆或方向性试探。

11.3 风控仪表盘指标

- **EMR (Excess Margin Ratio)**：可用保证金与维持保证金之比；保持 >1.5。
- **NLV (Net Liquidation Value)**：账户权益，随时观察回撤。
- **净/毛杠杆比**：控制净杠杆 <3 倍，毛杠杆 <6 倍。
- **可用保证金率**：若 <20%，应主动减仓，避免被动清算。

建议：将这些指标做成个人风控面板，配合止损/止盈规则执行。

小结

对于交易者与 LP，事件的经验是：**不要只依赖协议风控，必须自建仪表盘与仓位纪律**。在链上衍生品市场，风险管理能力本身就是竞争优势。

第十二章 对行业的启示

JELLY 攻击不仅是 Hyperliquid 的教训，更对整个 DeFi 衍生品、稳定币和 RWA 市场提供了可迁移的经验。

12.1 做市与清算保险功能的剥离

- **问题**：HLP 既做日常做市，又充当清算 backstop，风险集中；
- **经验**：应将两者剥离，设计多层保险池：
    - L1：日常清算折扣池，覆盖小额；
    - L2：风险基金池，应对中等规模；
    - L3：治理兜底，仅限极端情况。

类似结构可迁移至 **稳定币清算、RWA 抵押** 等场景。

12.2 风险预算与分层

- **设置单资产 OI 限额**，防止小币种爆仓拖累全局；

- **动态风险预算**：资金池对不同资产设不同承受上限；
- **风险分层**：大额仓位进入分仓器，强制拆分清算，避免一次性集中。

这对 **RWA 协议** 尤为重要，因为底层资产的流动性异质性更强。

12.3 治理的可预期性

- **紧急处置必须程序化**：预设停牌、再开盘的触发条件，而不是事后投票“拍脑袋”；
- **价格公平性基线**：预先设定“异常结算价”的计算公式，避免选择性。

这种程序正义对 **稳定币锚定机制**、**合成资产协议** 等尤为关键，能避免治理的随意性。

小结

JELLY 事件的经验可迁移为行业共识：

- 把“做市收益”与“极端保险”剥离；
- 在风险分层与治理程序化上形成制度化设计；
- 从而让 DeFi 协议不仅能 **“可用”**，还要 **“可预期”**。

结语

从“可用”到“可信”，是去中心化衍生品必须跨越的最后一公里。

Hyperliquid 以高速链上撮合和创新的 HLP 机制，证明了去中心化衍生品可以具备中心化交易所的性能。但 JELLY 事件也提醒我们：**性能不是护城河，风险与治理才是。**

- 性能让用户进来；
- 风控与治理决定用户是否留下。

真正的护城河，不是 TPS 或撮合速度，而是能否在极端行情中 **公平、透明、可预期地化解风险**。只有这样，DeFi 才能从一次次攻击事件中走向成熟，成为全球金融体系中 **可信赖的基础设施**。

你问的是：**Hyperliquid 是如何吸取教训、修补此前事件中暴露出的漏洞的？**这个问题非常关键，我查阅了多家权威源头来为你系统整理 Hyperliquid 的后续改进措施。下面是详细回顾和分析：

JELLY 攻击后的修复举措

1. **分离 Liquidator Vault 风险、改进 ADL 触发机制**

原先，Liquidator Vault 的损失与整个 HLP 池共同核算，导致 ADL 未能触发，即便大量亏损发生在单一仓位中。事后，团队优化了逻辑：

- **限额划分**：为 Liquidator Vault 设置更严格的价值上限，并减少再平衡频率；
- **精准触发**：现在 ADL 会根据该 Vault 自身的损失比例触发，而不再基于整个 HLP 的总损益来判断。

---

2. **动态调整 Open Interest 上限**

JELLY 攻击时，交易者开仓规模巨大，但仍在当时设置的 OI cap 范围内。为避免类似风险，Hyperliquid 引入了：

- **动态 OI 限额**：根据市场流动性和资产市值自动调整可持仓上限。

---

3. **正式机制化资产下架流程**

之前“人为干预”的下架操作被质疑不透明、中心化。为此，Hyperliquid 增设了：

- **链上验证人投票流程**：资产下架需在链上由验证人集投票执行，无需离线协调。

---

4. **引入外部价格源与 Mark Price 限制机制**

XPL 事件再次暴露缺乏外部价格锚定的风险。平台新增两大防护机制：

- **对标记价设 10× 上限**（Hard Cap），防止因“外部价格炸裂”导致清算失控；
- **接入外部永续合约数据源**，增强价格鲁棒性。

---

5. **改进风险管理流程与社区沟通**

针对 JELLY 风波，Hyperliquid 推出了一系列综合措施：

- **用户补偿机制**：使用基金会资金对非攻击地址持仓进行补偿；

- **暂停交易并统一结算**：对 JELLY 强制结算价格并关市，避免进一步损失；
- **加强社区沟通**：发布透明声明、强调正在迭代提升协议治理和风控。

以上改进措施总结：

改进点	描述
Liquidator Vault 限制	限制其风险暴露，独立判断 ADL 触发
动态 OI 上限	防控超大持仓风险
链上投票下架机制	提升治理透明度和机制化
外部价格接入 + Mark Cap	避免价格操纵和极端清算
补偿流程 + 治理沟通	修复信任、安定社区情绪

总结一说

Hyperliquid 在 JELLY 和 XPL 事件后做出的修复，不仅解决了单点风险，还提升了系统的整体鲁棒性。从明确 ADL 触发逻辑、资产管理、价格保护机制到链上治理流程化，Hyperliquid 正在逐步从“可用”走向“可信”。虽然其仍需不断迭代，但已有明确方向与工程行动。

如你需要，我可以进一步帮你画图展示这些安全模块如何介入风险链路，或者整理成工程规范。

后续：Hyperliquid XPL 攻击事件

一、XPL 在 Hyperliquid 上发生了什么？

2025 年 8 月，Hyperliquid 上的 XPL 期货市场爆发了异常剧烈的操纵事件：

- 一只鲸鱼账户搭载大量资金，迅速大买 XPL 多头，价格从约 $0.60 在几分钟内飙升至 $1.80（+200%），引发了大量短线仓位强制平仓。
- 主要操盘账户抓住机会迅速平仓，收益高达 **$15–16 M **。共有四名鲸鱼合力从中获利，累计 **$47.5–48 M** 利润。
- HLP 在此次波动中并未承担重大损失，反而通过提供流动性赚取了约 **$47,000** 的交易利润。
- 多个对冲中的交易者被动平仓产生巨大损失，或达几十百万美元。
- 该事件暴露了 Hyperliquid 在**薄流动市场预合约交易**中的脆弱性，随后平台陆续推出了 EMA 硬限制（10x cap）与外部价格接入机制等防护措施。

二、JELLY 事件的复盘（3月）

在 XPL 事件发生之前，Hyperliquid 在 2025 年 3 月也曾经历过类似情况：

- 攻击者通过操纵 JELLY 永续合约和外部现货涨价路线，迫使 HLP 接盘，导致 HLP 一度浮亏 **约 $13.5 M**。
- 因应这一事件，Hyperliquid 验证人进行了治理干预，下架 JELLY 永续，并以特定价格强制结算，同时对普通用户进行了补偿。

三、共性与对比：XPL vs JELLY

比较项	XPL 事件	JELLY 事件
发生时间	2025年8月	2025年3月
操作形式	鲸鱼集中做多、清算触发短线爆炸性上涨	小市值资产双向操纵，HLP 接盘亏损
风险承受者	交易者爆仓，操盘者获利，HLP 微利	HLP 承接主损失（百万美元）
平台应对	添加 EMA 限价+接入外部价格信号等安全升级	验证人停盘干预+补偿+合约下架
风控盲点	薄流动性、预合约操纵、缺乏 OI 限制	单币种深度不足、清算机制未防护

四、总结与核心启示

- **薄流动性预合约市场，极容易被鲸鱼操纵**，即使整个平台基础架构稳健，也难以抵抗集中特权账户的联动操作。
- **较弱的风控参数（如无开放仓位上限、无外部价格锚定）是主要漏洞点**。两波事件都触发平台调整策略，但方式差异显著。
- **HLP 在不同事件中表现不同**：在 XPL 中“吃得起波动赚点差”，但在 JELLY 中被动接盘带来重负。表明市场机制同样决定承接风险与能否承压的能力。
- **治理干预是双刃剑**：它可以在危机时刻挽救协议，但扭曲去中心化原则、破坏交易公平性。未来应偏向参数化机制（如 circuit breaker）而非事后人工干预。

Hyperliquid 的合约价格（特别是 **永续合约的标记价与清算价**）和 CEX 有所不同，它是 **三层价格体系** 决定的。简单说：**盘口成交价（交易价格）** 和 **标记价（清算参考价）** 是两个不同维度，前者由订单簿决定，后者由一套混合机制决定。

我帮你拆开：

---

1. 交易价格（Trade Price）

- Hyperliquid 是一个 **链上订单簿 (CLOB)**，用户挂单、吃单完全链上撮合。

- 所以 **实时交易价格** = 订单簿上买卖双方达成的最新成交价。
- 这一部分和 CEX 一样：由市场供需决定，哪怕成交很小也能瞬间把成交价推高/推低。

---

2. 标记价（Mark Price）

—— 决定清算 & PnL

为了防止被恶意“拉一笔成交价就清算”的操纵，Hyperliquid 采用 **三源合成中位数** 来生成标记价：

$$MarkPrice_t = Median \{ P_{oracle},\; EMA_{150s}(Mid_{HL} - P_{oracle}),\; \sum w_i P^{perp}_i \}$$

三个来源：

- **外部预言机中价 (Oracle)**
  - 来自主要 CEX 的现货价格，加权中位，每 ~3 秒更新；
  - 保证和外部真实市场不脱节。
- **内部订单簿 EMA**
  - Hyperliquid 内部中价 (mid price) 与外部预言机的差值；
  - 取 150 秒指数滑动平均 (EMA)，用于平滑短时波动。
- **外部永续合约价格**
  - 来自 Binance、OKX 等大交易所的永续中价；
  - 权重分配大致是 3:2:2:1:1。

最后取这三者的**中位数**，作为清算和未实现盈亏 (PnL) 的参考价。

---

3. 清算价（Liquidation Price）

- 对每个账户，清算价是根据 **保证金曲线** 算出来的：
- Equity < MaintenanceMargin \;\;\Rightarrow\;\; Trigger Liquidation
- 其中的价格输入就是 **Mark Price**，而不是市场瞬时成交价。
- 这样设计是为了避免单笔小成交就能引发连锁清算。

---

4. 总结一张表

价格类型	决定方式	作用
交易价格	链上订单簿撮合	实际成交
标记价 (Mark Price)	预言机现货 + 内部 EMA + 外部永续（取中位）	决定 PnL & 清算
清算价	根据账户杠杆、保证金计算，输入是标记价	触发清算逻辑

✅ **一句话总结**：

Hyperliquid 合约的价格本质上有两套：

- **交易价** 由链上订单簿成交决定；
- **清算 & PnL 用的标记价** 由“外部预言机 + 内部 EMA + 外部永续”合成。