

No Sandwich Swap

by WHU Web3 Club & ZJUBCA



团队介绍



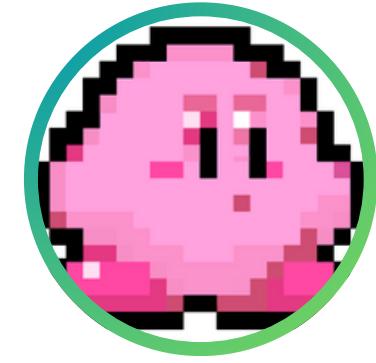
Treap

WHU Web3 Club Builder



Xi77jWhy

WHU Web3 Club Builder



Jawk

WHU Web3 Club Builder



Artist Zhou

ZJUBCA President



Fox

WHU Web3 Club Builder



SegmentOverflow

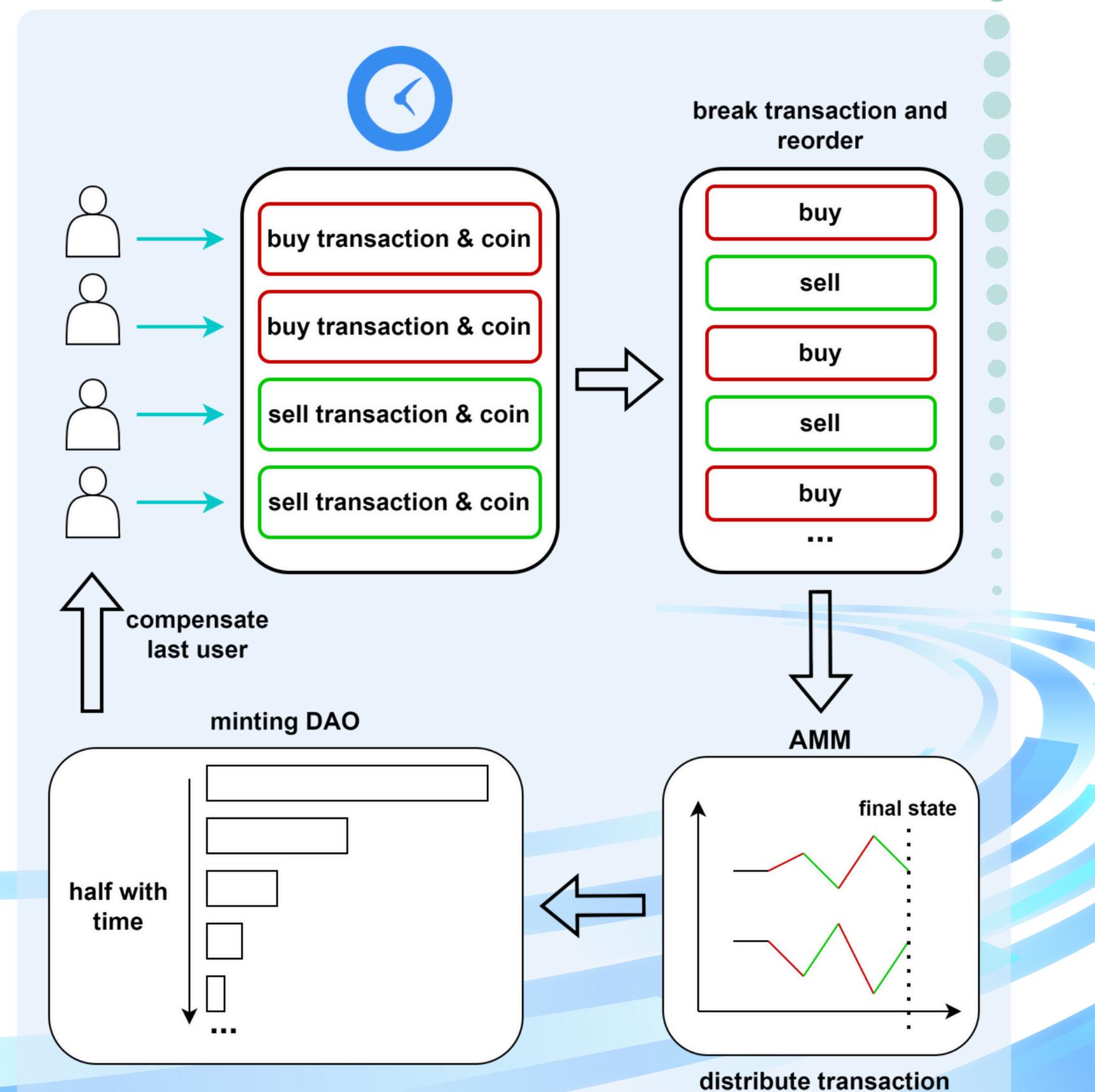
WHU Web3 Club Builder

概述

这是一个抗 MEV 的 DEX，使用**双曲集合竞价**的方式，将一段时间内的若干笔交易加总后无限细分并均匀交错排列，从而摊平了单笔交易的价格冲击效应，将 MEV 攻击者的交易分散至整个周期中使得套利收益大幅降低。

核心价值

- 对市场：减少价格冲击，让实际成交价更加贴近公允价格
- 对攻击者：有效防范 MEV 攻击，使得三明治攻击变得无利可图
- 对交易者：有效降低普通交易者遭遇的滑点，提高用户体验
- 对LP：抑制价格的波动性，减少 LP 遭遇的无常损失
- 对生态：通过治理代币激励机制鼓励多交易，提高市场流动性

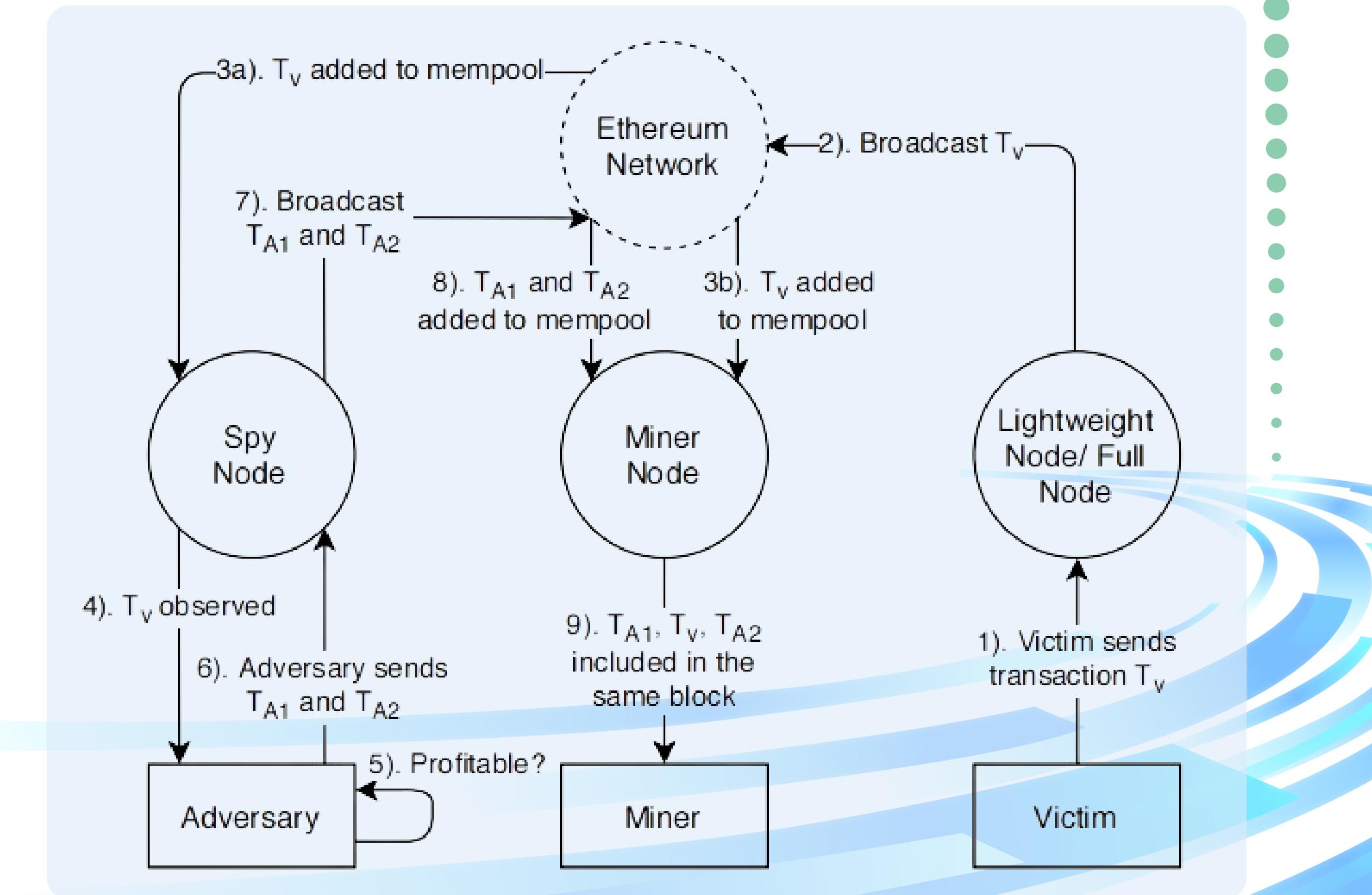


MEV的原理

MEV（最大可提取价值）是指区块生产者通过优先、重排或插入交易来最大化其收益的能力，通常发生在去中心化金融交易中。

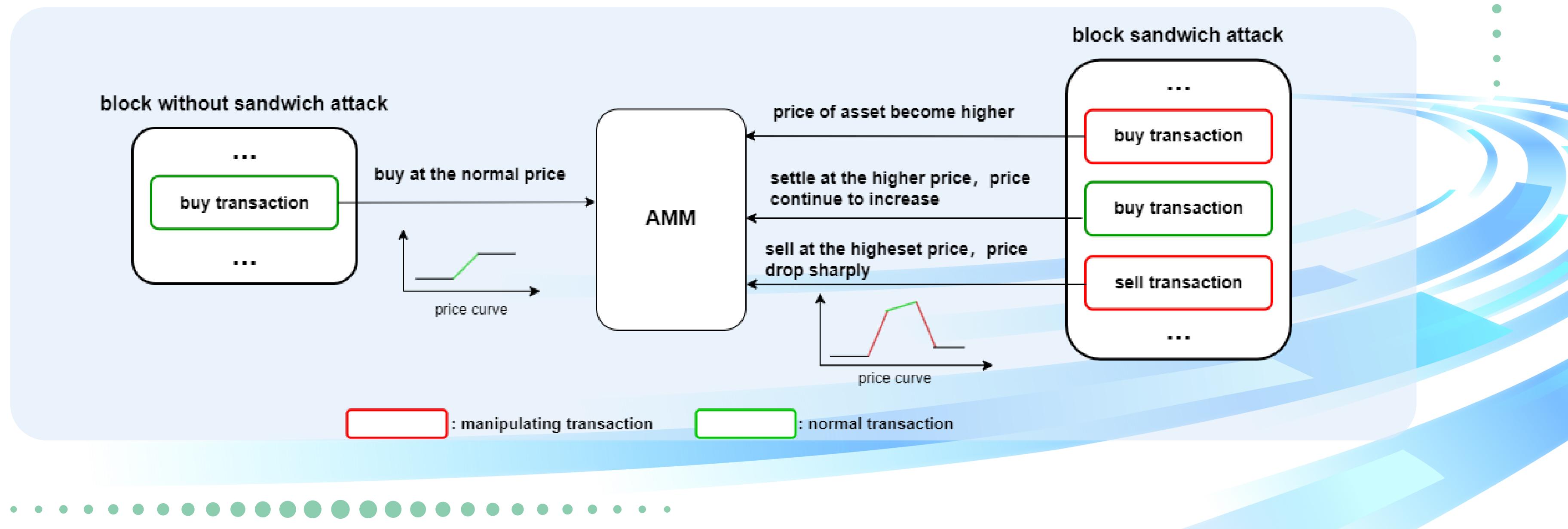
MEV的危害

MEV的危害在于它破坏了区块链交易的公平性，导致用户交易成本增加、去中心化金融中的套利和清算行为不透明，甚至可能引发网络拥堵和链上攻击。



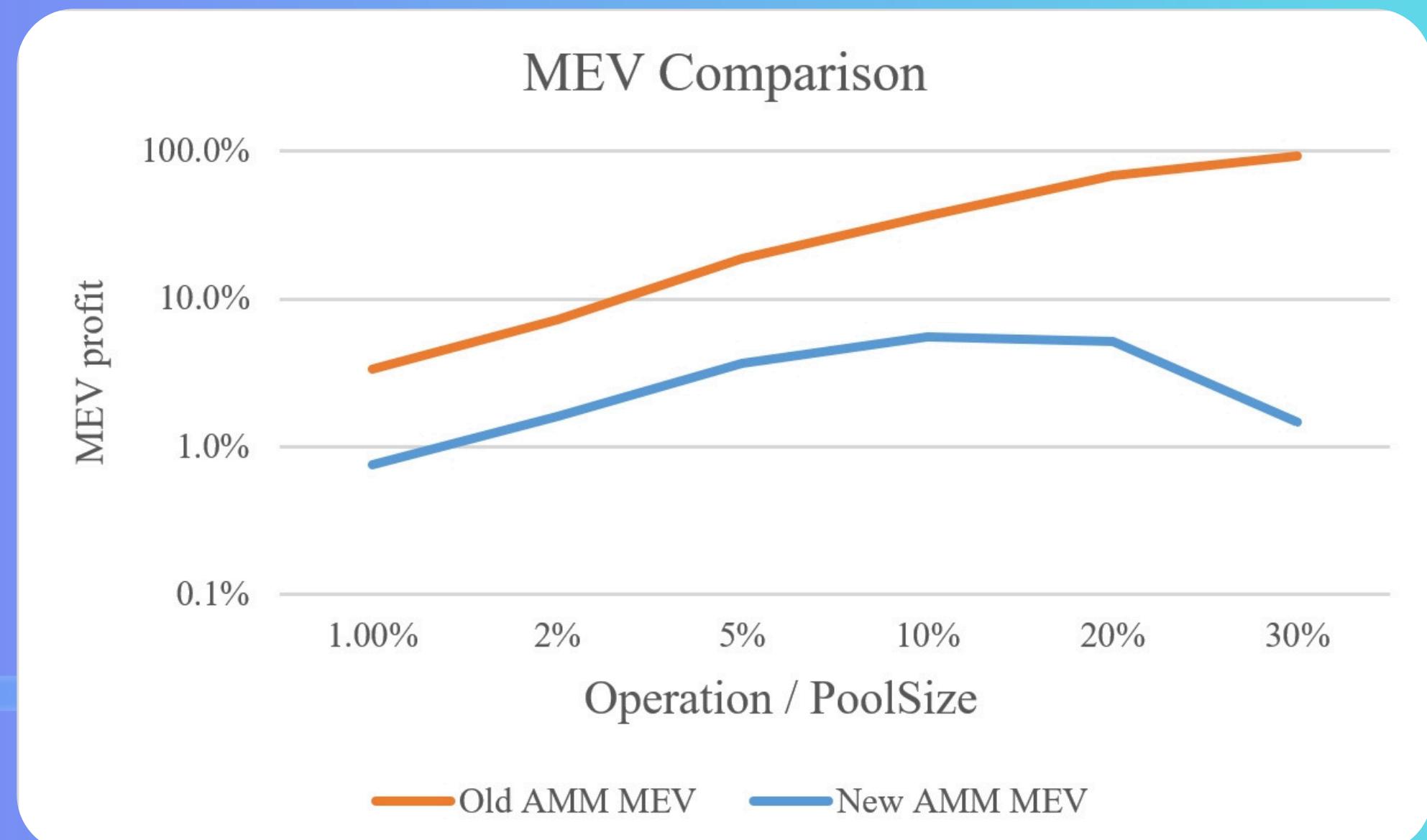
典型的 MEV 策略：三明治攻击

- 攻击者通过在目标用户交易之前插入一笔买单、在目标交易之后立即卖出，从而操纵价格并赚取差价。
- 三明治攻击是目前大多数普通交易者最常遭遇的 MEV 攻击形式



优化效果

- 双曲集合竞价可以将攻击者的交易均摊到交易周期的所有时点
- 攻击者将承担巨大的存货风险
- 我们的AMM可以将三明治攻击的获利可能性降低超过75%



AMM数学证明

设期初流动性池满足 $x_0 \times y_0 = k$ 。对于每一个结算周期，流动性池收到的基准货币和计价货币数量

分别为 $\{a_1, a_2, \dots, a_A\}, \{b_1, b_2, \dots, b_B\}$ ，设 $\alpha = \sum_{i=1}^A a_i, \beta = \sum_{i=1}^B b_i$ 。

将 α 和 β 皆均分成 N 个等份，然后将其交错均匀排列，形成一个虚拟的交易序列，形如：

在第 i 笔交易后，流动性池中的 x_i, y_i 为

- 若 i 为奇数， $x_i = x_{i-1} + \frac{\alpha}{N}, y = \frac{k}{x_{i-1} + \frac{\alpha}{N}}$
- 若 i 为偶数， $x_i = \frac{k}{y_{i-1} + \frac{\beta}{N}}, y_i = y_{i-1} + \frac{\beta}{N}$

随着 N 的增加， $\lim_{N \rightarrow \infty} x_{2N}$ 必然存在，证明如下：

1. 当 i 为偶数时，易得 $x_i = \frac{kNx_{i_2} + \alpha k}{kN + (x_{i-2} + \frac{\alpha}{N})\beta}$
2. 当 N 足够大时， $\frac{\alpha\beta}{N} \rightarrow 0$ ，容易发现 x_i 是一个单调数列
3. 投入流动性池的资金数量是有限的， x_i 显然不可能无限增大，而是一个有界数列
4. 根据单调有界原理， $\lim_{N \rightarrow \infty} x_{2N}$ 必然存在

1. 投入 α/N 个代币 X；
2. 投入 α/N 个代币 Y；
3. 投入 α/N 个代币 X；
4. 投入 α/N 个代币 Y；
.....
- 2n-1. 投入 α/N 个代币 X；
- 2n. 投入 α/N 个代币 Y；

$$x_{n+2} = \begin{cases} x_n + \frac{k\alpha - \beta x_n^2}{kn + \beta x_n}, & n = 2m, \\ x_{n+1} + \frac{\alpha}{N}, & n = 2m + 1 \end{cases}$$

$$\begin{aligned} x_{n+2}^2 - x_n^2 &= (x_{n+2} + x_n)(x_{n+2} - x_n) \\ &\sim 2x_n \cdot \frac{k\alpha - \beta x_n^2}{kN} \\ &\sim 2\sqrt{k} \cdot \frac{k\alpha - \beta k}{kN} \\ &= 2\sqrt{k}(\alpha - \beta) \frac{1}{N} \end{aligned}$$

$$\begin{aligned} \sum_{i=0}^{m-1} (x_{2i+2}^2 - 2x_i^2) &= 2\sqrt{k}(\alpha - \beta) \\ \implies x_{2m} &= \sqrt{k + 2\sqrt{k}(\alpha - \beta)} \end{aligned}$$

因此，随着交易的无限均分，流动性池最终将趋于一个固定值。在数值模拟中， $N \geq 100$ 时基本可以认为数值不再变化。定义 $x' = \lim_{N \rightarrow \infty} x_{2N}$, $y' = \lim_{N \rightarrow \infty} y_{2N}$ 。

每个结算周期中，交易者可能发送多笔实际交易。对于前若干笔交易，只做数据记录而不结算；对于周期的最后一笔交易，触发结算流程，将收集的代币按贡献分配给交易者。

- 提供 X 代币的交易者获得数量为 $\frac{a_i}{b_i} (y_0 + \beta - y')$ 的 Y 代币
- 提供 Y 代币的交易者获得数量为 $\frac{\alpha}{\beta} (x_0 + \alpha - x')$ 的 X 代币
- 这种交易方式类似于 A 股市场盘前的集合竞价过程，即在结算周期内不进行实时结算，只在周期结束后形成价格并统一按相同的价格结算
- 由于最终成交依然基于恒定积自动做市商，所以任何成功将交易上链的交易者都可以获得成交
- 我们将这种交易方式称为**双曲集合竞价**

代币经济学

- 代币代码: \$SANDWICH
- 获取方式: 每个结算周期的最后一笔交易的发起人(即触发结算者)会花费更多gas, 因此将获得一笔治理代币作为补偿
- 释放模型: 初始供应为 10000 SANDWICH/周期, 半衰期为 1 个月
- 价值来源: 交易本身就是一种挖矿, 通过代币激励交易者积极交易, 提高LP收益

问题: MEV 攻击者依然可以通过交易排序来让自己成为结算触发者从而获得治理代币
回应:

- 这种 MEV 攻击并没有像以前的那种攻击一样, 直接损害到普通交易者的权益
- 随着 MEV 攻击者持有的 \$SANDWICH 代币越来越多, 他们的利益也与 NoSandwichSwap 建立绑定, 从而倒逼他们成为协议生态的维护者