

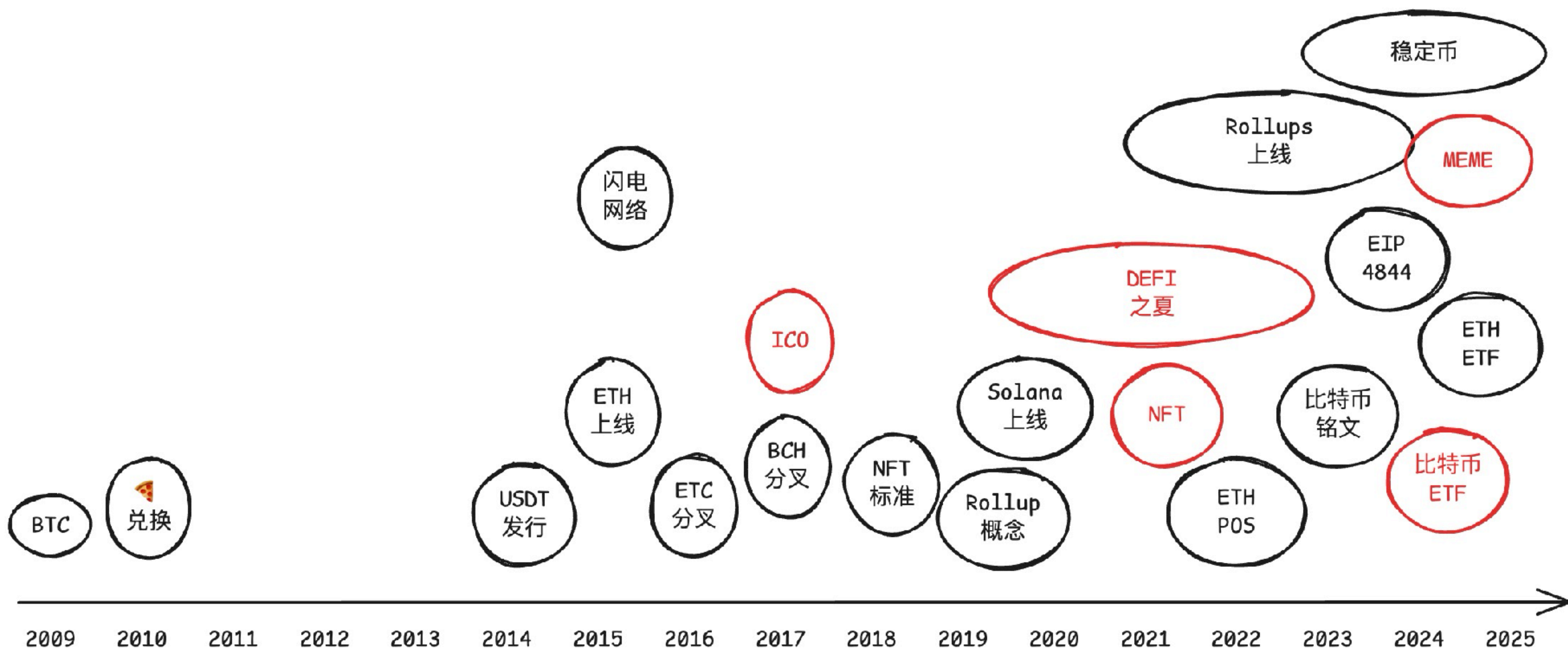
资产 (TOKEN) 发行 DEX 协议

Tiny 熊

要点

- 回顾行业重要事件，感受行业变化
- 资产（Token）发行 - IDO
- DEX - 资产交易

WEB3行业 重要事件



WEB3行业 重要事件

- BTC: 2009 年 1 月 3 日是比特币 (BTC) 的创世区块日期;
- BTC 第一次兑换: 2010年5月18日 10000枚比特币换到了两块披萨
- NameCoin: 2011年分叉BTC网络, 是比特币的第一个分叉项目;
- ETH: 2015 年 7 月 30 日上线主网;
- BCH (比特币现金): 2017年8月1日 BCH大区块扩容路线, 最高32MB的区块, 比特币现金仍然是比特币最成功的硬分叉。
- ETC:The DAO 的 ICO 被攻击损失了约 360 万 ETH。2016 年 7 月 20 日: 为挽回损失, 社区硬分叉回滚交易, 原以太坊重新命名为 ETC;
- EOS: 2017 年 6 月, EOS 开始为期一年的 ICO, 最终筹集了约 40 亿美元, 成为史上最大规模的 ICO 之一;
- USDT: 于 2014 年 10 月 6 日在 Omni Layer 协议上发行, 2019年 USDT 开始从 Omni Layer 扩展到以太坊区块链 (ERC-20 标准);
- Solana: 2020 年 3 月, Solana 上线主网, 最快的公链

WEB3行业重要事件

- DeFi: 2020 年 6 月：DeFi 夏天（DeFi Summer），Compound 在 2020 年 6 月推出治理代币 COMP，开启了“流动性挖矿”（Liquidity Mining）热潮；
- NFT: 早期萌芽（2017 年 CryptoPunks），标准确立（2018 年 ERC-721）。2021 年 OpenSea 等 NFT 交易平台交易量激增，2021 年 8 月单月交易额超过 30 亿美元。
- Layer2: 2015 年 BTC 的闪电网络，2017 年 Plasma 概念，2019 年 Rollups 概念，2021 年 8 月 Arbitrum 主网上线，9 月 Optimism 主网上线；
- 以太坊 过渡到 POS：2022.09.15，
- 比特币铭文协议：2023.01 诞生、2023 年中开始引发 BTC 上的资产发行浪潮
- 2024 年 1 月：比特币现货ETF 获 SEC 通过，确定合规性，逐步被主流市场认可
- 2024 年 3 月：坎昆升级，EIP-4844 升级降低了Layer 2的交易成本
- 2024 年7月：美国现货以太坊ETF 正式获批上市交易

资产即 TOKEN

- 资产是所有权的表示
- 链上智能合约可创建不被他人剥夺的资产，Token 即是其链上表示
- ERC20、ERC721 标准让资产发行、管理和交易变得无比简单

Token 发行

- Token发行： Initial Coin Offering (ICO), Security Token Offering (STO), Initial Exchange Offering (IEO)
- 典型发行流程：
 1. 项目构思和白皮书撰写：项目团队首先需要构思项目的具体内容和目标，并撰写白皮书，详细描述项目的技术优势、经济模型
 2. 寻求投资机构融资（根据需要）
 3. 产品开发、智能合约开发，Token 的发行和流通。
 4. 市场推广和社区建设：通过各种渠道进行市场推广，吸引潜在投资者和用户，并建立和维护社区。
 5. Token 公开发售：通过 ICO、STO 或 IEO 等方式公开发售 Token，募集项目开发所需的资金（根据需要）
 6. Token 上线交易所：将Token 上线至各大交易所，提供流动性，方便用户进行交易。

Token 发行 - TGE

Token 发行 (Token Generation Event, TGE)

发行方式	全称	定义
ICO	Initial Coin Offering	项目方直接向投资者出售代币以筹集资金。
STO	Security Token Offering	发行代表证券或金融资产所有权的代币。
IEO	Initial Exchange Offering	通过加密货币交易所平台进行的代币发行。
IDO	Initial DEX Offering	通过去中心化交易所 (DEX) 进行的代币发行。
IFO	Initial Farm Offering	通过流动性挖矿平台进行的代币发行，通常与流动性提供相关。
ICOs	Initial Coin Offerings	多次进行小规模 ICO，逐步募集资金。
Airdrop	空投	项目方将代币免费分发给特定的用户群体，用于推广项目。
ITO	Initial Token Offering	与 ICO 类似，但通常更侧重于功能型代币的发行。
ILO	Initial Liquidity Offering	在去中心化交易所通过增加流动性池进行的代币发行。

Token 经济模型

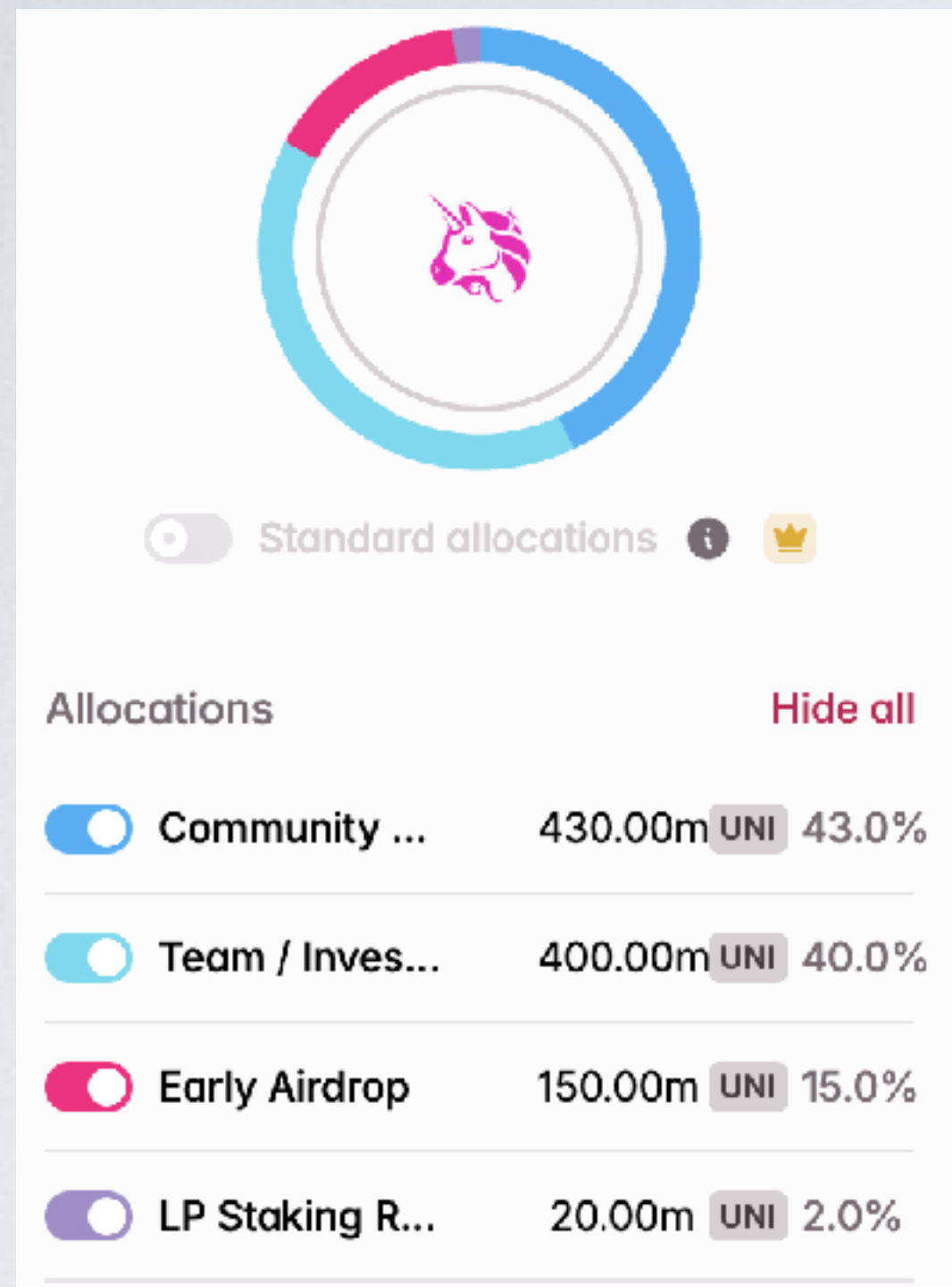
- Token 经济模型对项目成败很关键，另外一个关键因素是：团队
- 经济模型三个重要考量：
 - 项目如何捕获价值（商业模式）、或不捕获价值
 - 如何分享价值（如何激励、是否公平、公正）
 - 如何释放（如何锁仓、增发）
- 好的经济模型让项目形成正向飞轮：
 - 用户参与 → Token 激励 → 协议使用增长 → 收入上升 → Token 价值上升 → 更多用户参与（社区壮大）

Token 分类

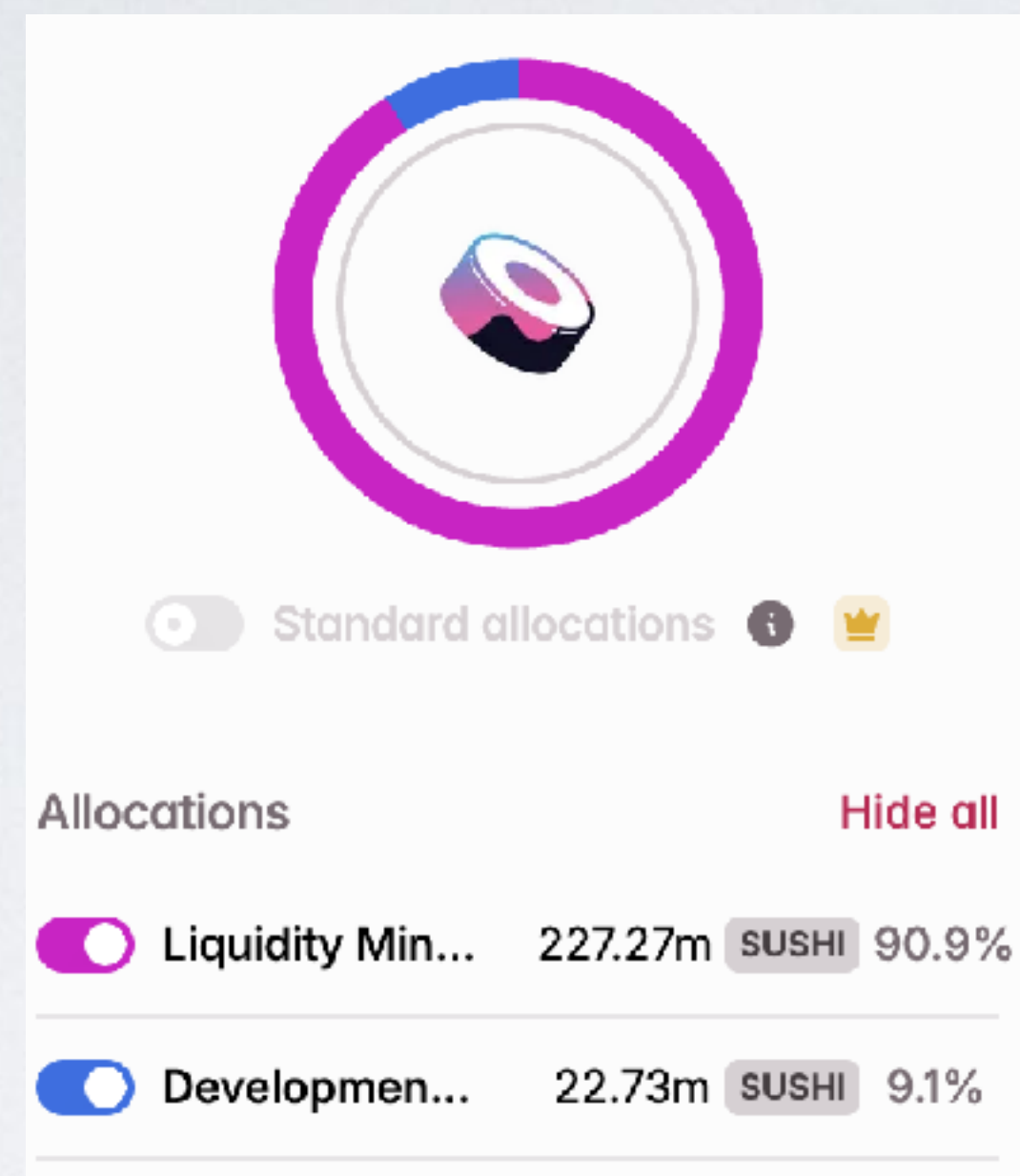
- 实用型/功能型代币(Utility tokens): 持有才可以使用某项服务 (使用权)
 - 例如: LINK、GRT、ETH (不是 ERC20)、WLD (WorldCoin)
 - 支付型代币 (Payment tokens): **稳定币** USDC、USDT、USDS (大家常说的U)
- 权益型/证券型代币(Security tokens): 代表的是所有权, 享有平台 (资产) 的未来价值, 例如: 分红、投票治理、债券等
 - 例如: **stETH**、LP Token、**UNI** (治理)、RWA 类
 - 证券发行需要满足相应的法规, 如备案、审批, 投资人 KYC、反洗钱检查, 有相应的法人主体的。(SEC 诉 Ripple)

可以根据需要发行多个 Token 或一个 Token 具备多种属性 (Hybrid)

Token 分配



Uniswap



Sushiswap (社区模式)

通常用户和社区占大多数份额
价格回归的体现：用户创造的价值，回归用户

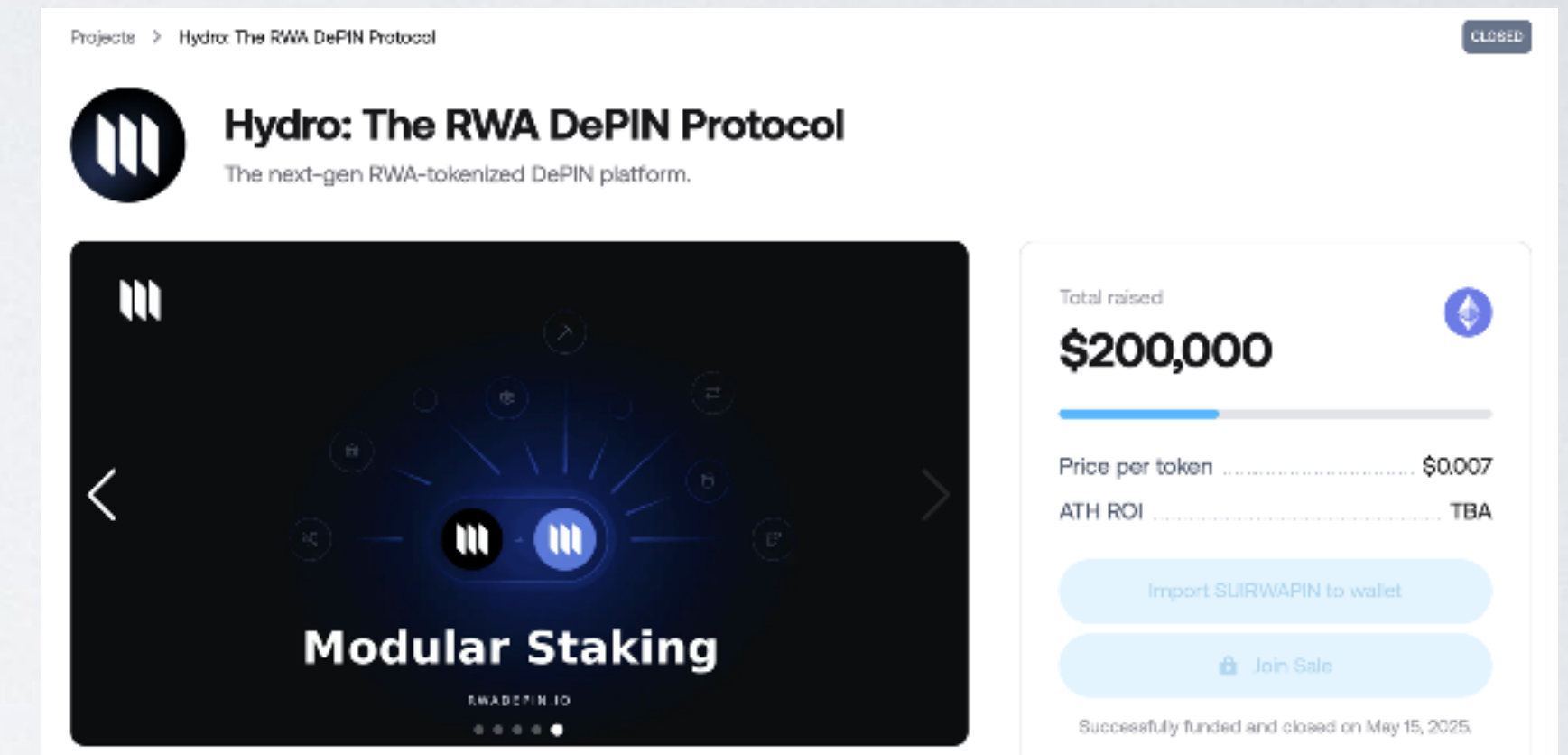
用户获取 Token 方式（发行方式）：

1. 买 - IDO / 私募
2. 挖矿挖（作为奖励发放）
3. 空投

<https://tokenomist.ai/uniswap>

IDO - Launchpad

- IDO： 在 DEX 上进行的代币发行方式（一级市场，直接卖）
- Launchpad 为 IDO 提供发行服务的平台
 - <https://polkastarter.com/>
 - <https://www.pump.fun/>
 - <https://four.meme/>
- 中心化交易所也可能有自己的 LaunchPad ， 如币安



<https://polkastarter.com/projects/hydro>
以 \$0.007 的价格公开出售

IDO - 常见逻辑

1. 以 0.0001 eth 的**单价**预售 100 万的 OPS Token
2. 在**某时间**内**目标**凑集 100 ETH, 最多 200 ETH
3. 预售**门槛**为 0.001 ETH
4. 预售用户可 claim Token, 预售失败 refund 本金

https://github.com/lbc-team/hello_foundry/blob/main/src/IDO.sol

私募 - 锁仓

- 私募投资人或项目团队，通常持有的 Token 数量较大，为了避免大量的抛售压力，通常会设定锁仓释放机制
- 锁仓：指某部分 Token 不能立即出售，而是按照既定节奏逐步解锁（Vesting）
- 锁仓方式：
 - 线性释放（Linear Vesting）：按时间等额释放（如每月解锁 1/24）
 - 周期释放（Step Vesting）：每季度或每半年释放一次
 - 参与型（milestone）释放：根据任务、指标释放，如作为社区激励
- 有一些机制会设置 Cliff（悬崖期） - “首次解锁等待期”：在 cliff 期内，受益人一分钱都拿不到。Cliff 结束后才开始释放。

示例：

项目 A 团队总共获得 10% 的代币，采用如下锁仓结构：

- **Cliff: 12 个月**
- **线性释放：接下来的 24 个月**

意味着前 12 个月团队完全拿不到任何代币，第 13 个月起开始每月解锁 1/24。

质押挖矿

- 例如, Sushi 所有的 Token 的都是质押 LP 通过奖励 mint 出来的。

作业

- 编写一个 Vesting 合约（可参考 OpenZeppelin Vesting 相关合约）， 相关的参数有：
 - beneficiary: 受益人
 - 锁定的 ERC20 地址
 - Cliff: 12 个月
 - 线性释放: 接下来的 24 个月
 - 从 第 13 个月起开始每月解锁 1/24 的 ERC20
- Vesting 合约包含的方法 `release()` 用来释放当前解锁的 ERC20 给受益人
- Vesting 合约部署后，开始计算 Cliff，并转入 100 万 ERC20 资产
- 要求在 Foundry 包含时间模拟测试， 请贴出你的 github 代码库

<https://decert.me/quests/58aec80f-8980-434a-b549-566003367694>

DEX

什么是DEX?

- 交易所：资产买卖金融市场，证券(股票)交易所、期货交易所、大宗商品交易所...
- DEX：Decentralized Exchange 去中心化交易所（Token 兑换 Token）
- DEX 优势：用户始终掌握资产、互操作性好（作为金融底层基础设施）、抗审查 ...
-

DEX 类型

订单簿

- 类似于传统的中心化交易所，通过买卖订单的撮合来完成交易。
- 以 0x 协议为代表，链下订单撮合和链上结算

流动性池

- 流动性池合约作为交易对手方，用户可以将资金存入流动性池，作为流动性提供者（LP），并通过提供流动性赚取交易费用。
- 以 Uniswap 为代表（开创者），自动作市商协议，类似的还有：SushiSwap/Balancer/Curve/ Pancakeswap/dodo

当前 DEX 数据

<https://dune.com/hagaetc/dex-metrics>

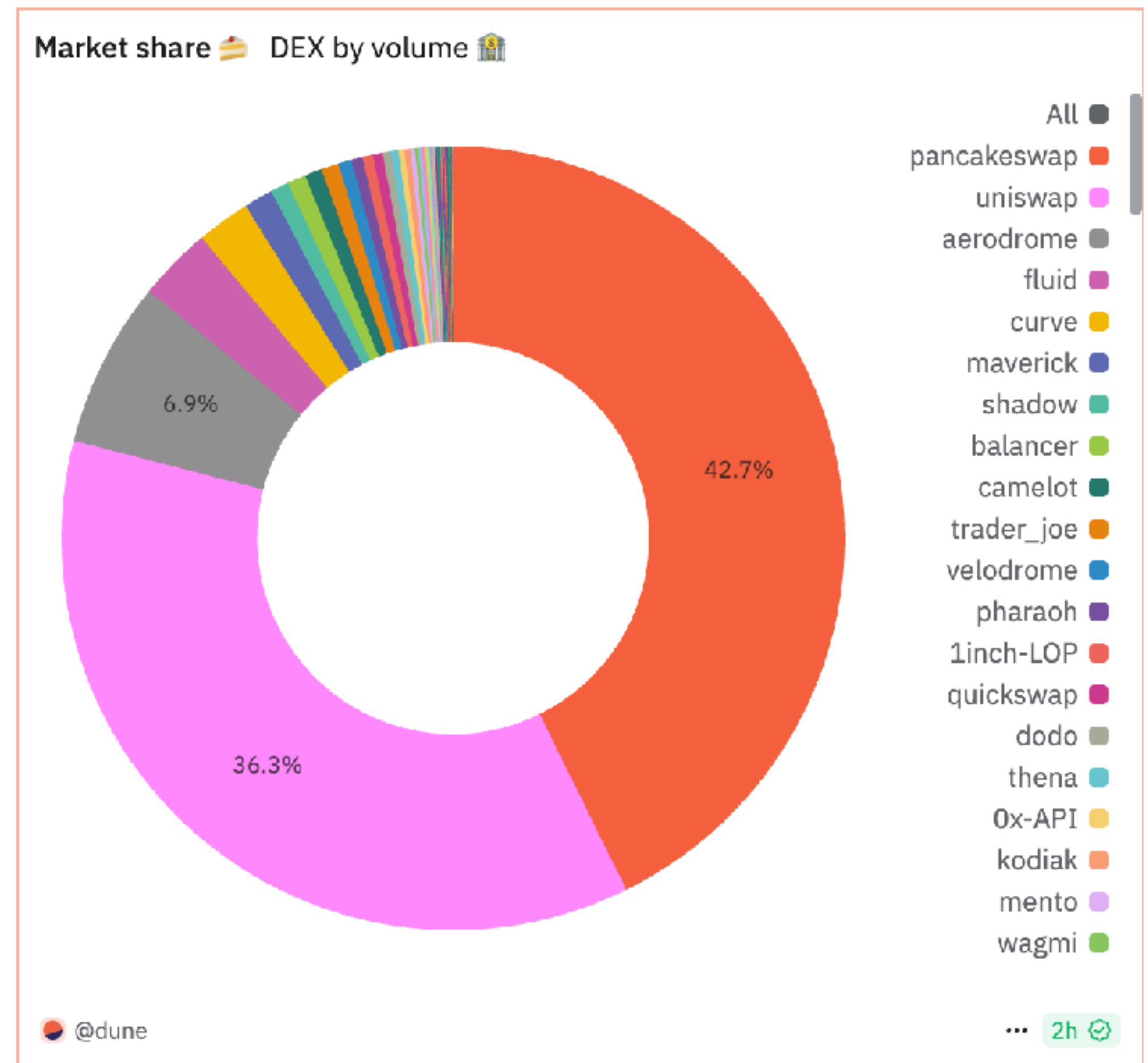


Ranked 🏆 DEX by volume 🏠

Rank	Project	7 Days Volume 📈	24 Hours Volume 🏠
1	pancakeswap	\$28,521,272,163	\$5,382,717,027
2	uniswap	\$24,237,369,678	\$4,396,251,667
3	aerodrome	\$4,584,022,593	\$755,362,127
4	fluid	\$2,031,307,797	\$285,825,798
5	curve	\$1,478,639,420	\$178,257,160
6	maverick	\$795,026,503	\$103,233,956
7	shadow	\$510,133,180	\$83,862,990
8	balancer	\$506,581,725	\$62,044,533
9	camelot	\$479,504,733	\$86,151,607
10	trader_joe	\$477,119,903	\$69,270,076
11	velodrome	\$368,375,715	\$68,217,899
12	pharaoh	\$307,130,969	\$33,920,260

147 rows Search... < < > >>

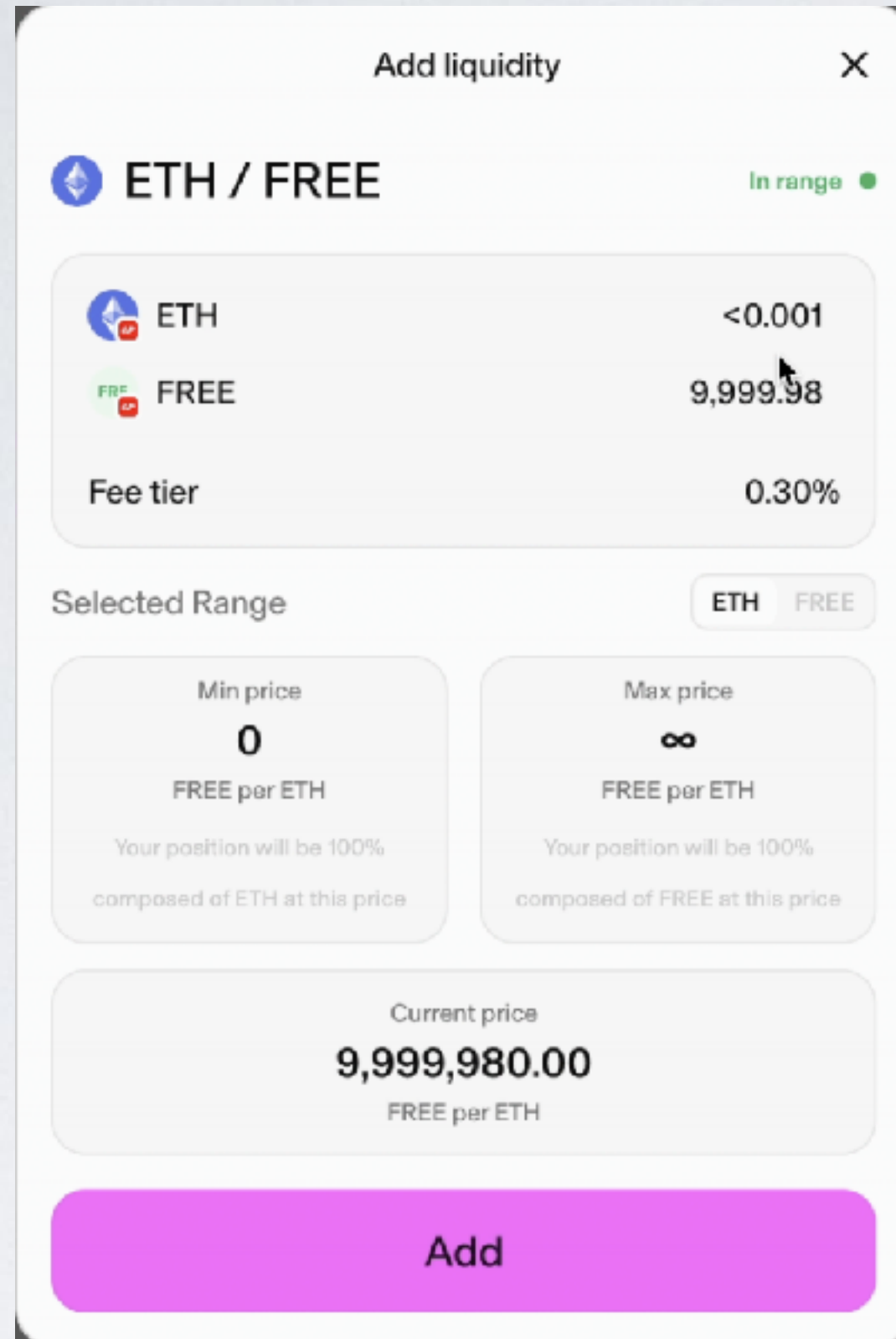
@dune ... 2h 🔄



Uniswap AMM

- AMM协议: AutoMated Market Making
 - AutoMate(d): 自动, 没有中间机构进行资金交易
 - Market Making: 做市商 (保证订单得以执行), 也称为流动性提供者 (LP: liquidity providers)
 - 流动性指的是如何快速和无缝地购买或出售一项资产
 - LP 是提供资产的人以实现快速交易。
- Uniswap 使用常量乘积模型: $K = x * y$

UNISWAP 演示



提供流动性
(首次也是上架 Token)

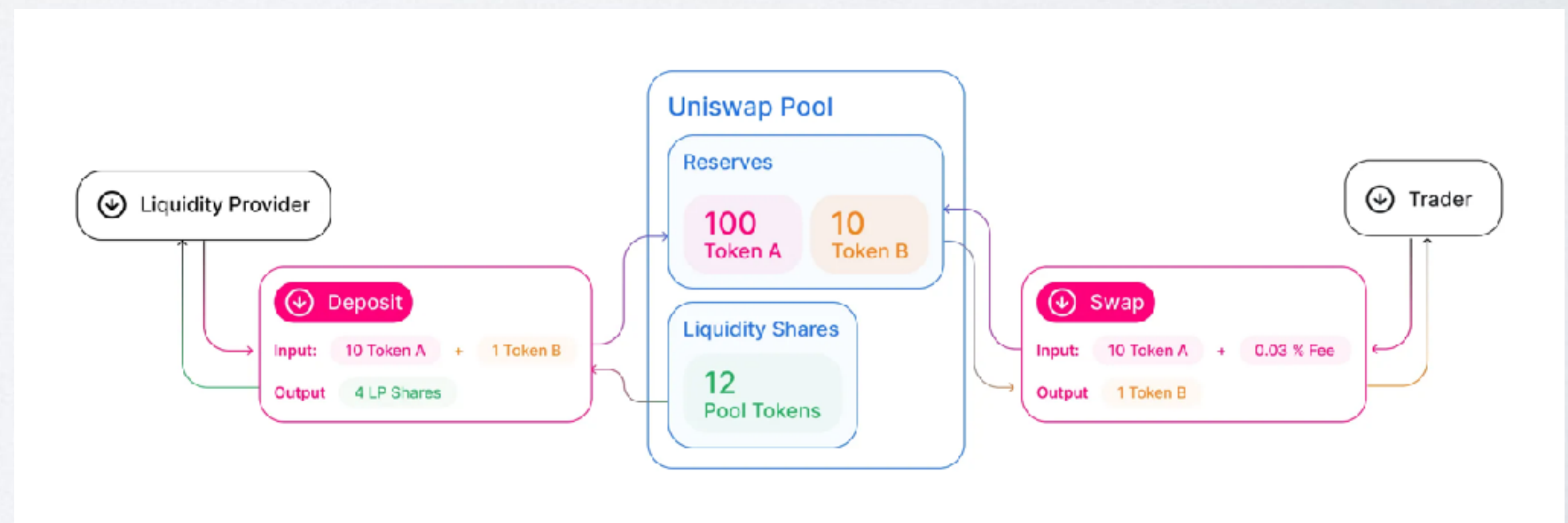


兑换

<https://app.uniswap.org/>

Uniswap V2 AMM 原理

- 常量乘积模型: $K = x * y$
 - AMM 的执行引擎, 没有价格预言机, 价格用公式推导
 - x : token0 的储备量 (reserve0)
 - y : token1 的储备量 (reserve1)
 - 提供流动性:
 - 转入token0、token1, 增加reserve0、reserve1, 拿到流动性凭证 (LP Token) $= \sqrt{x * y}$
 - 兑换时, K 保持不变
 - 减少reserve0, 就必须增加reserve1
 - 减少reserve1, 就必须增加reserve0
 - 移除流动性



AMM – 提供流动性

添加流动性 增加 K

交易前:

$x = 1000$

$y = 1000$

$K = 1000000$

Lp token = \sqrt{K}

100 A : 100 B

交易后:

$x' = 1100$

$y' = 1100$

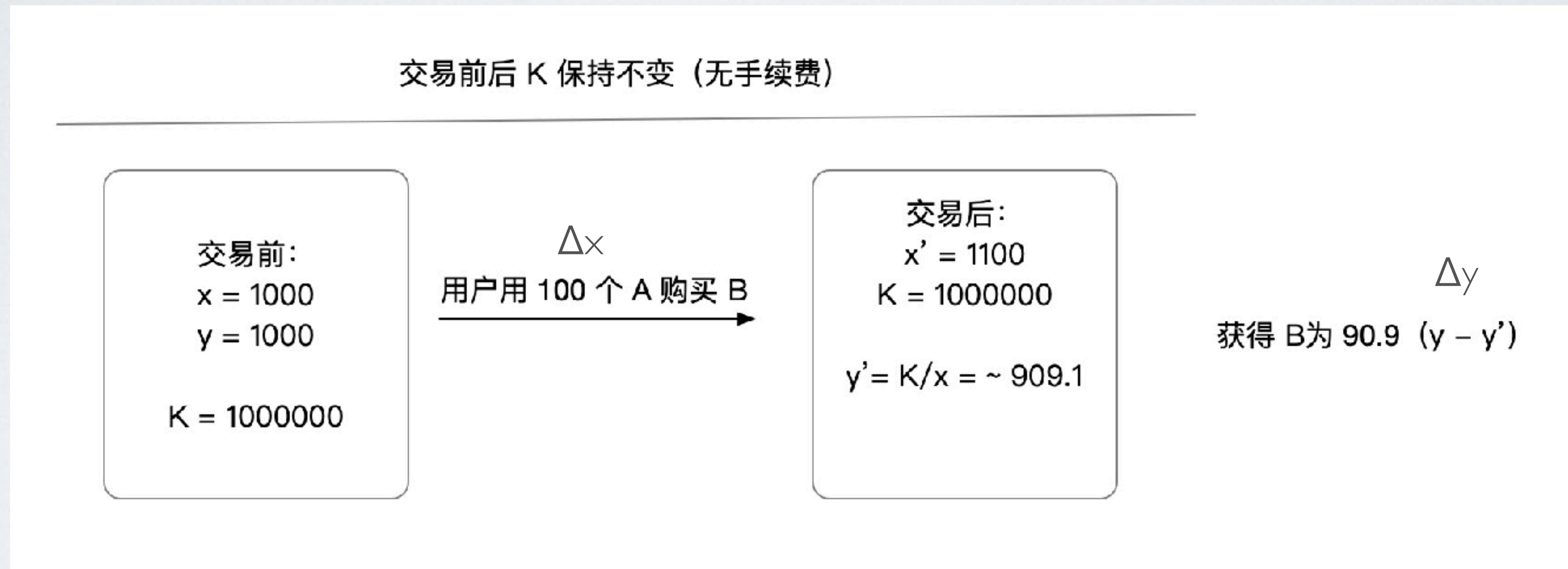
$K' = 1210000$

获得 lp token: 100

第一次添加流动性（上架 Token），需要自己设置价格，

Uniswap V2 – 兑换

- 常量乘积模型: $K = x * y$



价格滑点 (slippage) : 一次交易使价格改变的程度, 单笔交易量越大对价格的影响越大

Mini AMM Demo

- 100 行代码理解AMM

`hello_foundry/src/MiniSwapPool.sol`

为什么MiniSwapPool 是 ERC20 ?

Uniswap V2

交易前后 K 保持不变 (扣除0.3%费)

交易前:

$$x = 1000$$

$$y = 1000$$

$$K = 1000000$$

用户用 100 个 A 购买 B
→
用于交易的A 为 99.7

交易后:

$$x' = (1000 + 99.7) + 0.3$$

$$y' = K / (1000 + 99.7) = 909.33$$

$$K = 1000000$$

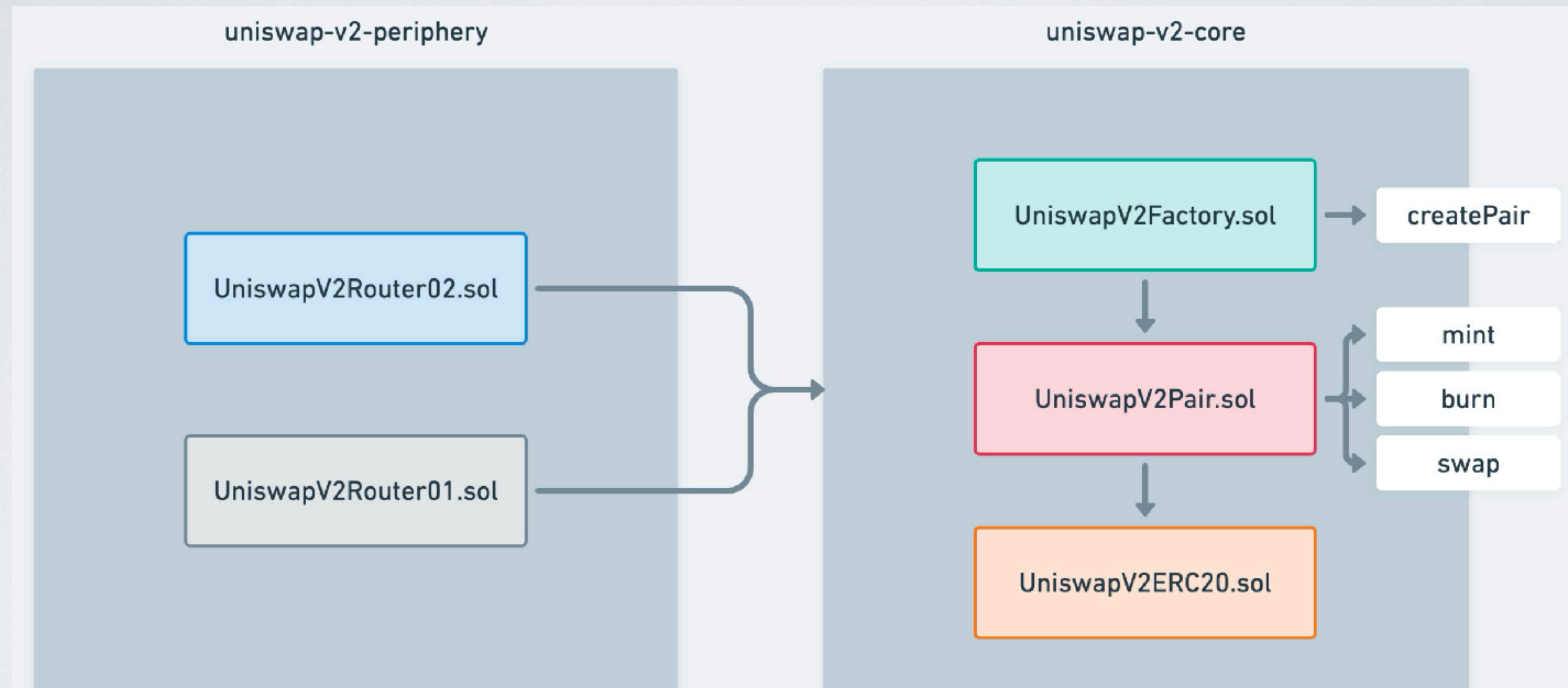
$$K' = 1000263$$

获得 B: 90.67 ($y - y'$)

$$x \cdot y = (x + \Delta x)(y - \Delta y) = k$$

$$\Delta y = y - \frac{x \cdot y}{x + \Delta x} = \frac{\Delta x y}{x + \Delta x}$$

Uniswap V2 – 代码结构

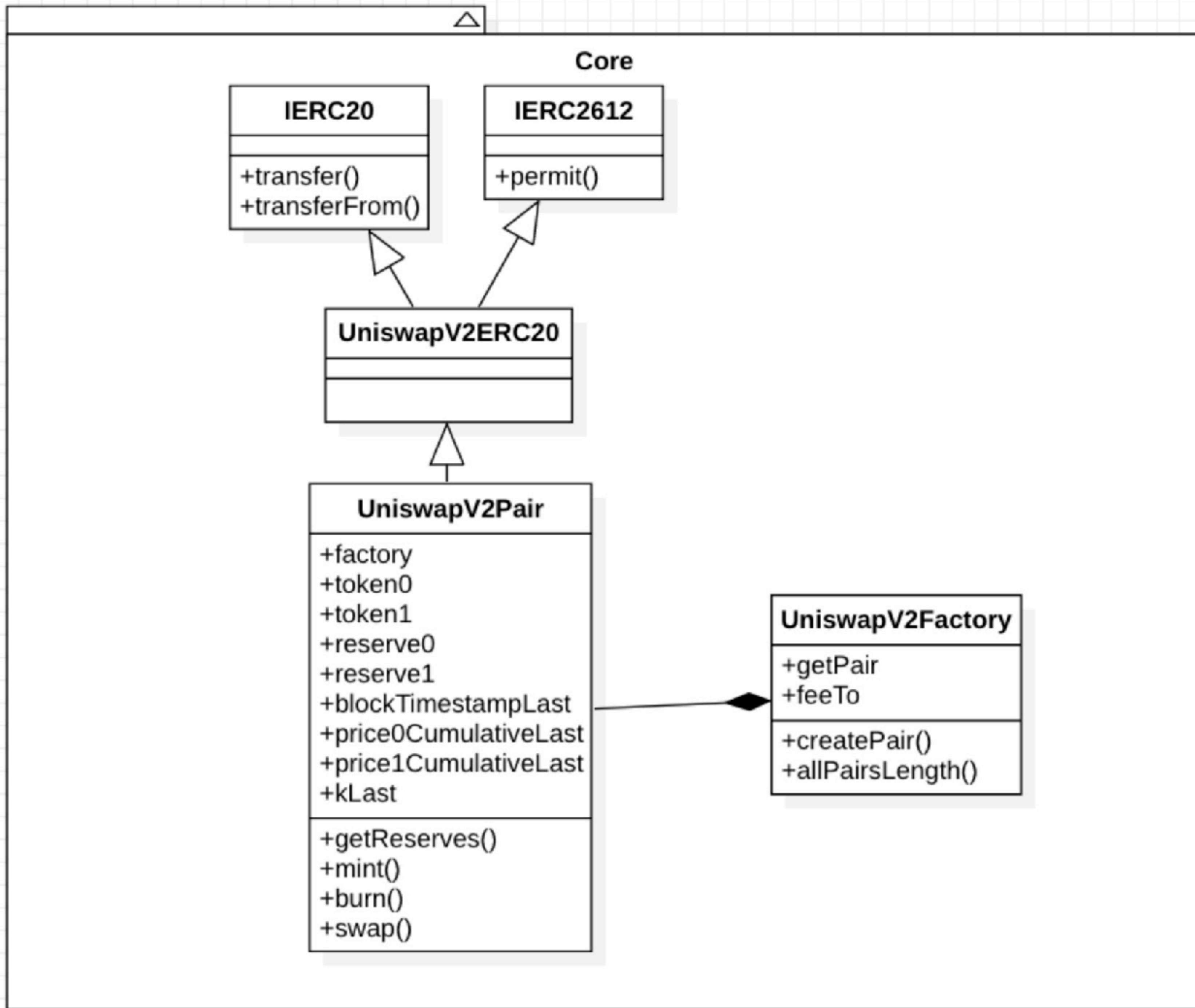


<https://github.com/Uniswap/v2-core>

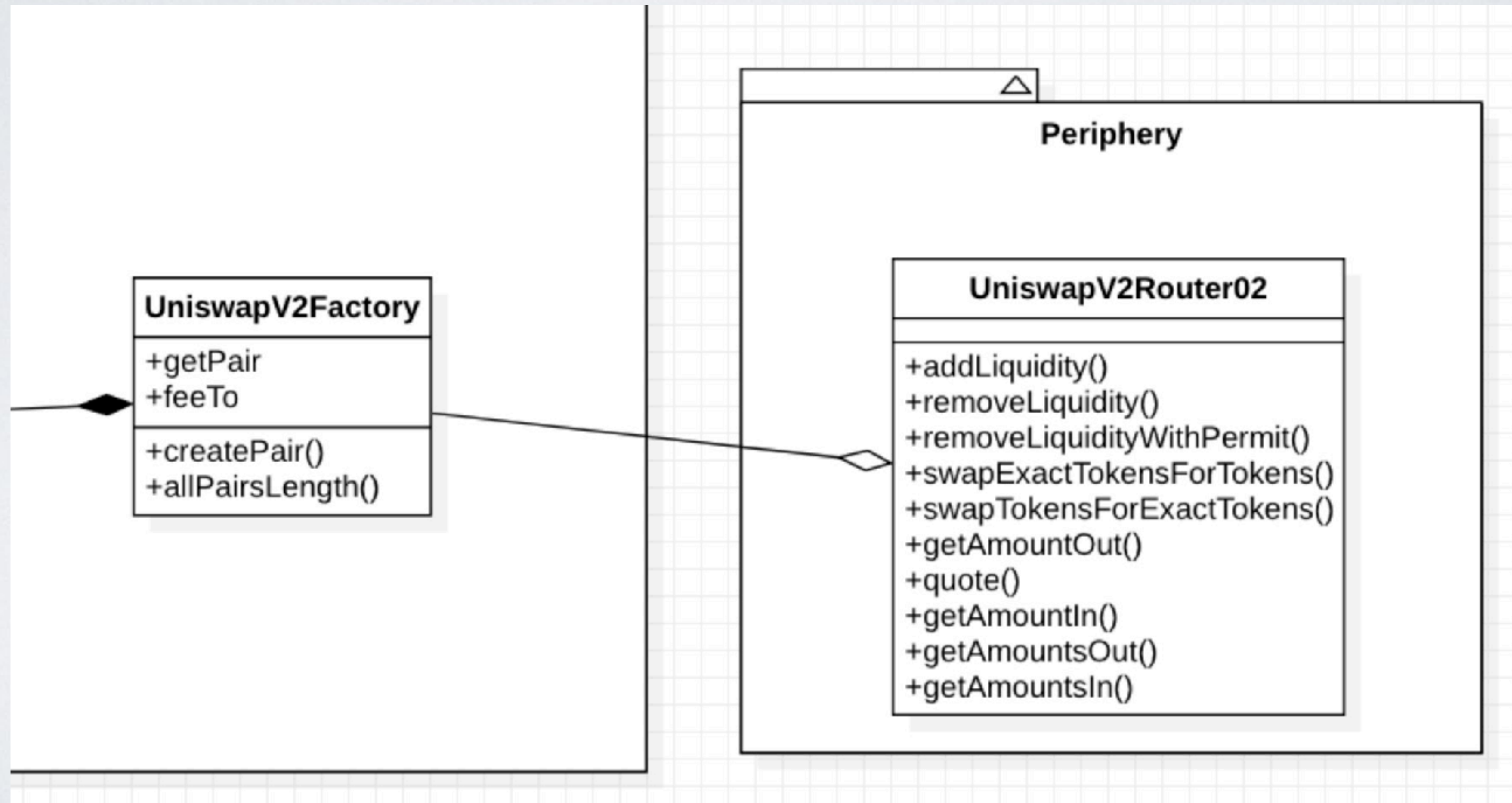
<https://github.com/Uniswap/v2-core>

<https://github.com/Uniswap/v2-periphery>

<https://github.com/Uniswap/v2-periphery>



Uniswap – 合约结构



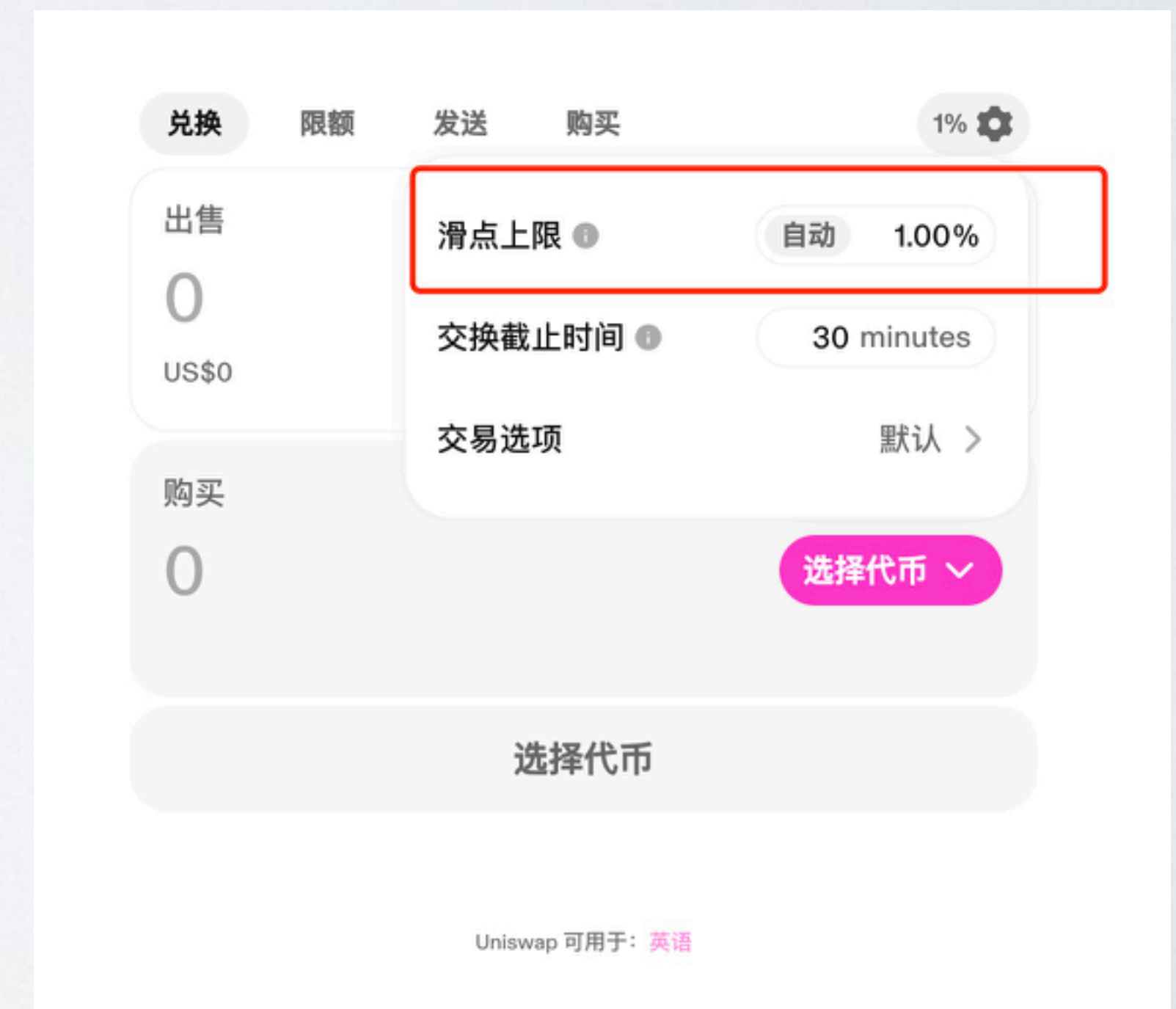
Uniswap V2 – 主要交互接口

- 添加流动性
 - AddLiquidity
- 兑换: 用 Token0 换 Token1 [兑换路径: path]
 - swapExactTokensForTokens()
- 移除流动性: 转入 lpToken 获得 Token0, Token1
 - removeLiquidity/ removeLiquidityWithPermit /

<https://github.com/Uniswap/v2-periphery/blob/master/contracts/UniswapV2Router02.sol>

滑点 – Slippage

- 与订单簿不同，在 AMM（自动做市商）模型中，他人的交易可能会影响你的交易价格，滑点是预期的交易价格的差异，在流动性较小（也称为 LP 深度）或交易金额较大时滑点更为明显。
- 在交易函数中，amountOutMin 是控制滑点参数，以便在滑点过大时，停止交易，作为主动防御机制。
- 深度更大池子设置更小的滑点，小池子设置大一点的滑点



三明治攻击 – 夹子机器人

- 当滑点设置较大时，交易容易被夹 - “三明治攻击”
- 攻击者通过操纵交易排序，从中牟取利益。
- 原理：
 - 1. 监听内存池（`eth_subscribe: newPendingTransactions`），发现用户(Bob)买入交易之后
 - 2. 攻击者用更好的 gas 发起一笔买入交易（从而推高价格） - 抢先交易（front-run）
 - 3. 执行 Bob 买入交易（但原本能以较低价格买入，现在应该价格升高拿到了更少的目标 Token）
 - 4. 攻击者反向操作卖出（Bob 的买入交易进一步推高了价格，攻击者此时卖出可获取差价收益。）
- 如何防御：设置合理滑点、分批交易、使用私人交易路由广播(BloXroute)

攻击者通常使用 Flashbots 来提交三明治交易，保证两笔攻击交易和用户交易在一个区块中连续执行；

练习题

- fork 阅读 Uniswap V2 源代码，为 Uniswap V2 主要方式添加代码注释
- （可选）发布一篇文章阐述自己对 Uniswap 理解的文章，如代码解读等，积累自己的个人 IP
- 在本地部署 Uniswap V2 源代码
 - 需要修改 UniswapV2Library 的 pairFor , init code hash , 参考: <https://learnblockchain.cn/article/3915>

<https://decert.me/quests/fa82f574-7f3e-4566-8916-dd7aff17cb01>

练习题

- 实现一个 LaunchPad 平台：
- 修改之前最小代理工厂 1% 费用修改为 5%， 然后 5% 的 ETH 与相应的 Token 调用 Uniswap V2Router AddLiquidity 添加MyToken与 ETH 的流动性（如果是第一次添加流动性按mint 价格作为流动性价格）。
- 除了之前的 mintMeme 可以购买 meme 提价一个方法: buyMeme(), 以便在 Unswap 的价格优于设定的起始价格时，可调用该函数实现购买 Meme.

<https://decert.me/quests/df4886bc-65c6-45fb-ad0c-3389a9f99bf2>