



# 要点

- 稳定币分类：抵押及算法稳定币
- 抵押型稳定币是如何保持稳定的
- 算法稳定币是如何通过算法来保持币价稳定

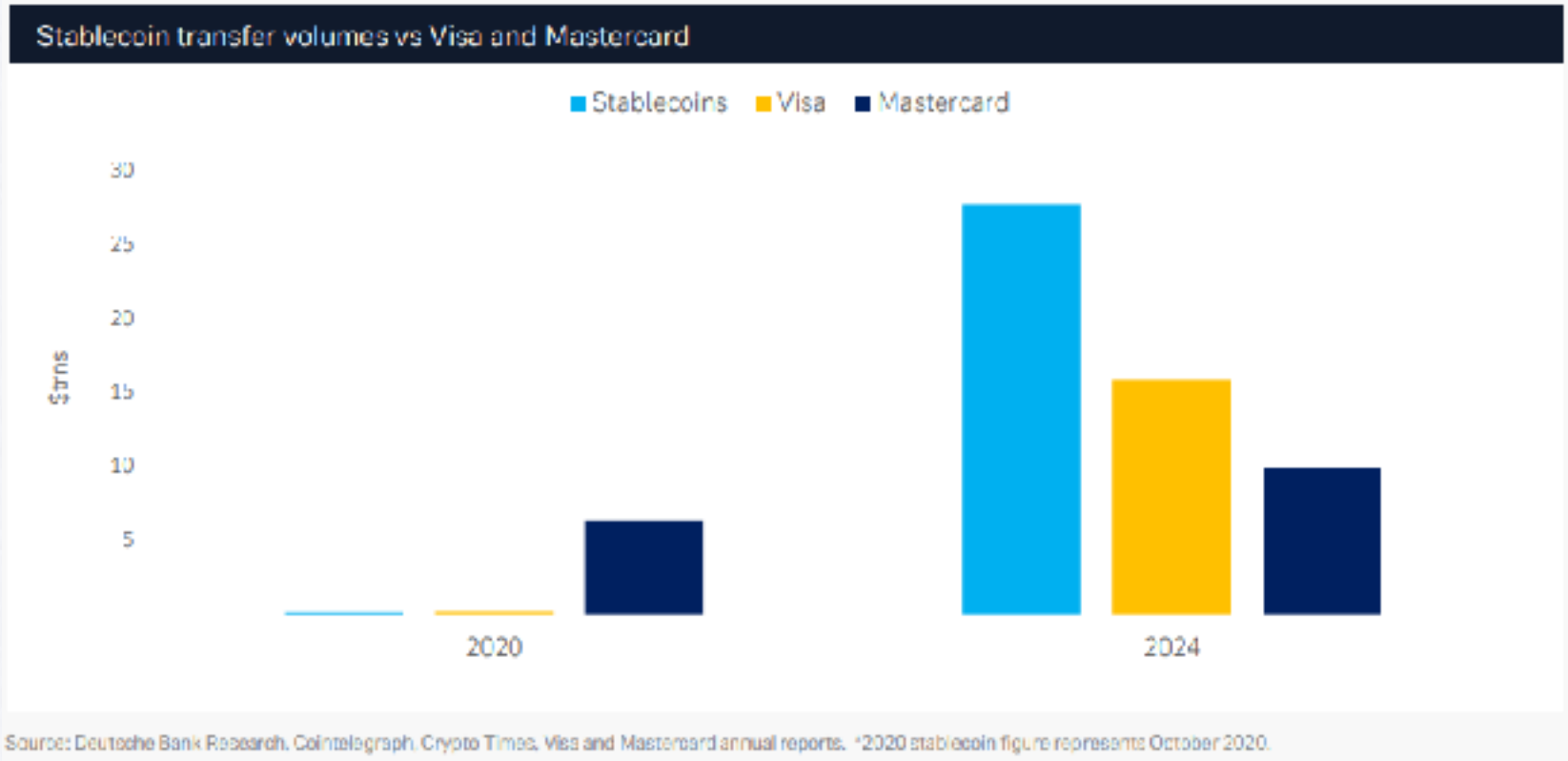


# 稳定币

- 稳定币（以美元稳定币为主）：当前 Web3 最大应用场景，是数字资产交易的中介，是支付工具
  - 稳定币正在以很快速度进入主流支付系统，当前已经超过 Visa 交易量
- 相比法币（美元）的优势：
  - 24/7 全天候全球实时结算，且费用更低
  - 无需许可、无国界限制、只需要有一个钱包
- 相比 BTC、ETH：
  - 稳定（波动性小） - 锚定法币美元



<https://defillama.com/stablecoins>



# 稳定币

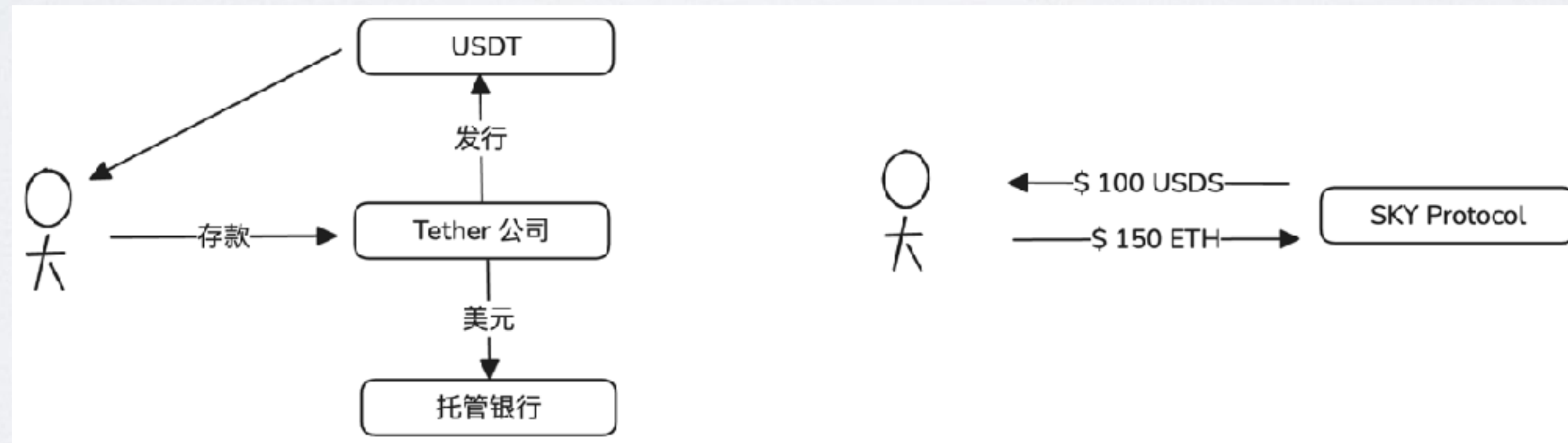
## • 稳定币分类





# 稳定币

- 抵押型稳定币，稳定币作为债务形式存在。
  - 链下以美元抵押（中心化），如：USDC， USDT
  - 以链上资产做抵押，通过利息调节供应，如：USDS(DAI)

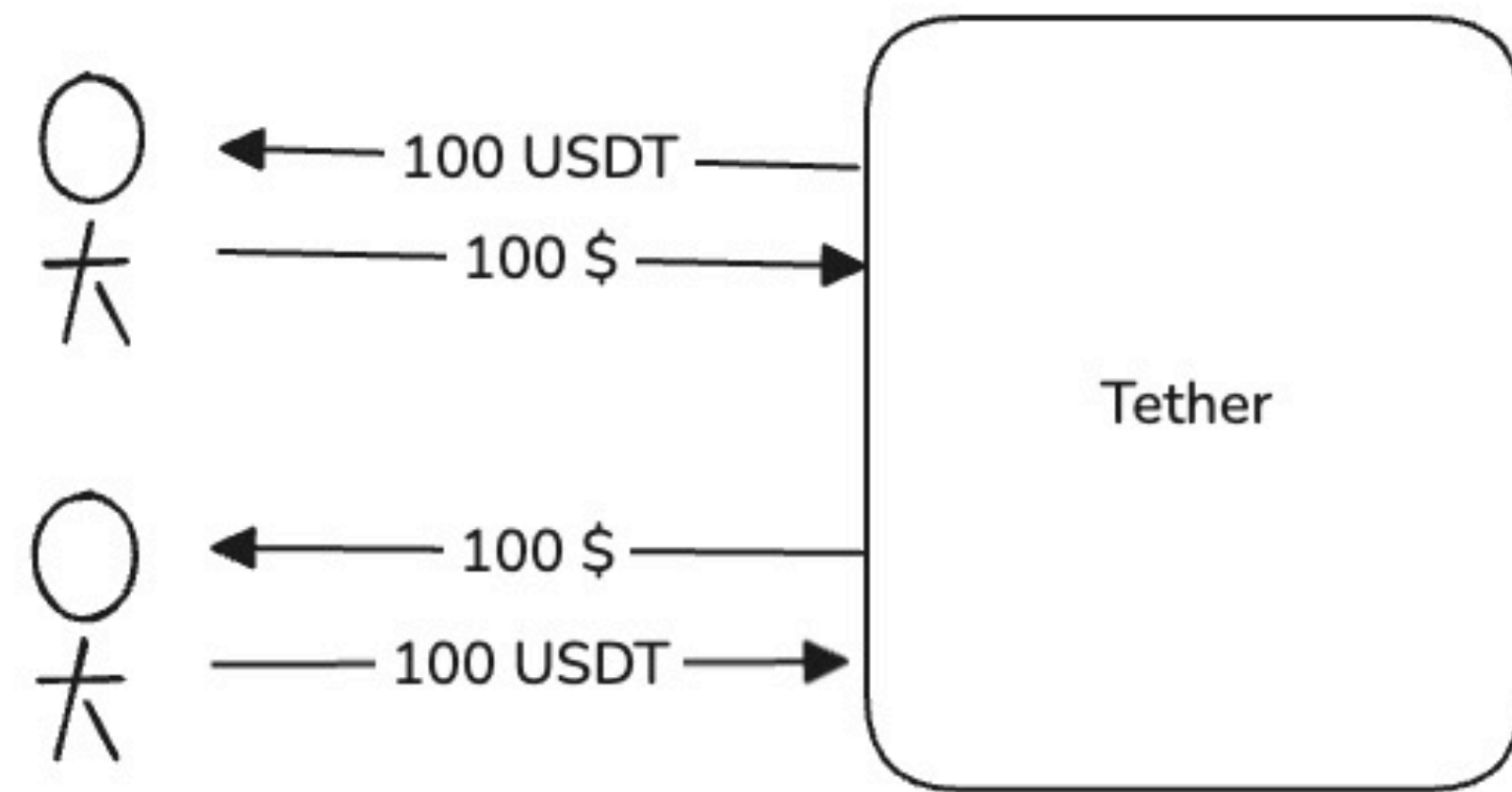


收益来源:

法币利息 + 手续费

手续费

# 美元抵押 – 稳定机制



若二级市场 跌至 0.98 美元，则套利者可以：

可以买入 0.98 美元的 USDT，赎回获得 1 美元，赚取 2 分利润。

增加 USDT 的购买需求，价格随之回到 1 美元。

若二级市场 高至 1.02 美元，则套利者可以：

可以用 1 美元铸造 USDT，卖出获得 1.02 美元，赚取 2 分利润。

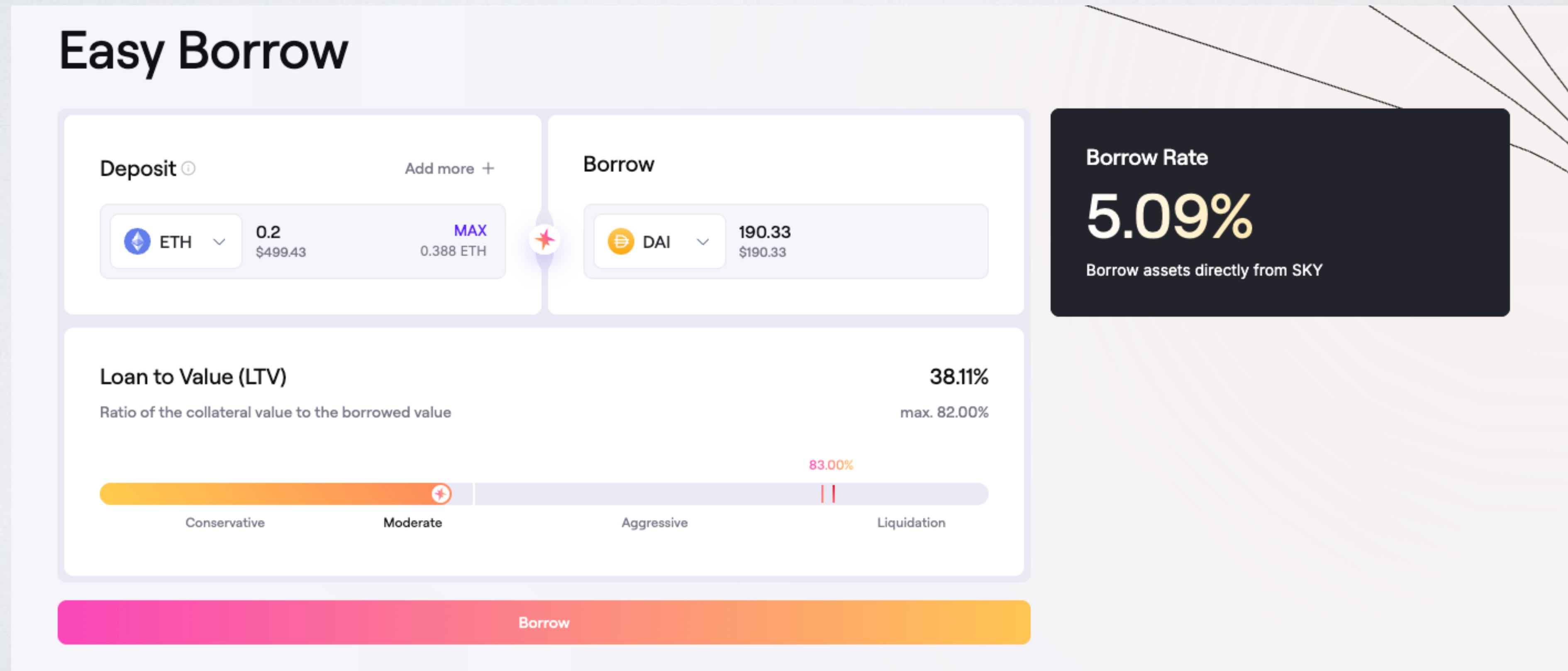
卖出 USDT 增加，价格随之回到 1 美元。

如果市场下跌，没有套利者，Tether 可用储备资产回购



# USDS (DAI)

- USDS 是 Sky（之前叫 MakerDAO）发行的去中心化稳定币，是最大的去中心化稳定币
- USDS 本质是一个借贷协议，所借资产是 mint 出来的稳定币



# USDS – 稳定机制

- USDS 维持稳定有一系列组合拳
- 清算机制保证每个 USDS 有足额的抵押
- PSM (Peg Stability Module) 模块：
  - 存入 USDC, 铸造等额 USDS
  - 销毁 USDS, 提取等额 USDC
  - 如果二级市场 (Uniswap 等) 偏离 1 美元, 套利者可以通过 PSM 进行无风险套利
- 补充策略：
  - SSR 激励 - 允许用户存入 USDS 赚取利息, USDS 价格低于 1 美元, 治理可能提高 SSR 利率以激励持有, 增加需求
  - 借款利率调整 - USDS 价格低于 1 美元, 治理提高利率, 抑制供给, 反之增加供给
  - 借款利息部分会盈余缓冲池 (Surplus Buffer), 会进行稳健投资, 如果套利者套利者, 必要时可回购 USDS



# AAVE 稳定币 GHO

- AAVE 2023 推出的稳定币 GHO
- 友谊翻船小故事：Aave 和 Sky 是 DEFI 借贷和稳定币龙头
  - 早期：Aave 支持 DAI 作为抵押品和借贷资产，互惠互利关系
  - GHO 的诞生和 Sky 子协议 Spark 构建自己的借贷生态，导致友谊翻船。

# 抵押型稳定币主要问题

- 中心化依赖（法币抵押）
  - 冻结或审查权限
  - 金融系统本身不稳定（USDC 曾受SVB破产影响，拖锚 10%）
- 资金利用率不高（超额抵押型）



# 算法稳定币

- 能否有一个去中心化、无许可、高资金利用率的稳定币？
- 算法稳定币：
  - 通过算法调节供需关系（及激励方式），实现价格稳定
  - AMPL BAS FRAX FEI UST ... 等

# 算法稳定币先驱 – Ampleforth

- 基于供需影响价格的理论
  - 价格  $>$  \$1, 增加 AMPL 供给 (所有用户余额变多)
  - 价格  $<$  \$1, 减少 AMPL 供给
- 每天 Rebase (函数)
- 正向、反向 (死亡) 螺旋 -> 价格偏移大
- Rebase 引起的余额变化, 影响生态发展。



# 算法稳定币先驱 – Ampleforth

- 如何调控每个账号的余额？

# Rebase 机制

- 如何做到增加 AMPL 供给，所有用户余额变多，减少时余额变少？

看到的余额

$$y = \frac{1}{k} * x$$

保存的

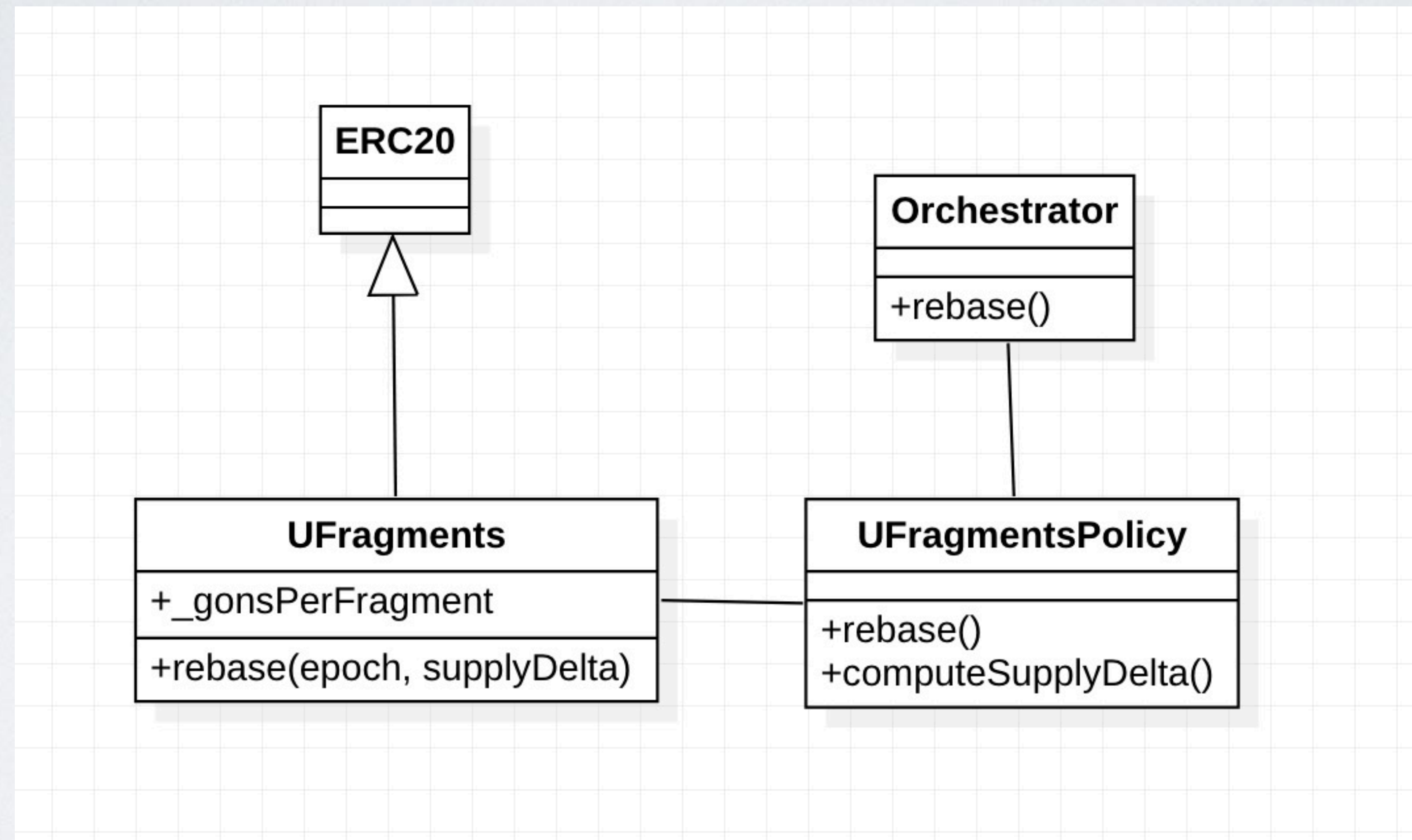
rebase 调节

```
function balanceOf(address who) external view returns (uint256){
    return _gonBalances[who].div(_gonsPerFragment);
}
```

$$k = \frac{TOTAL}{supply}$$



# 算法稳定币先驱 – Ampleforth

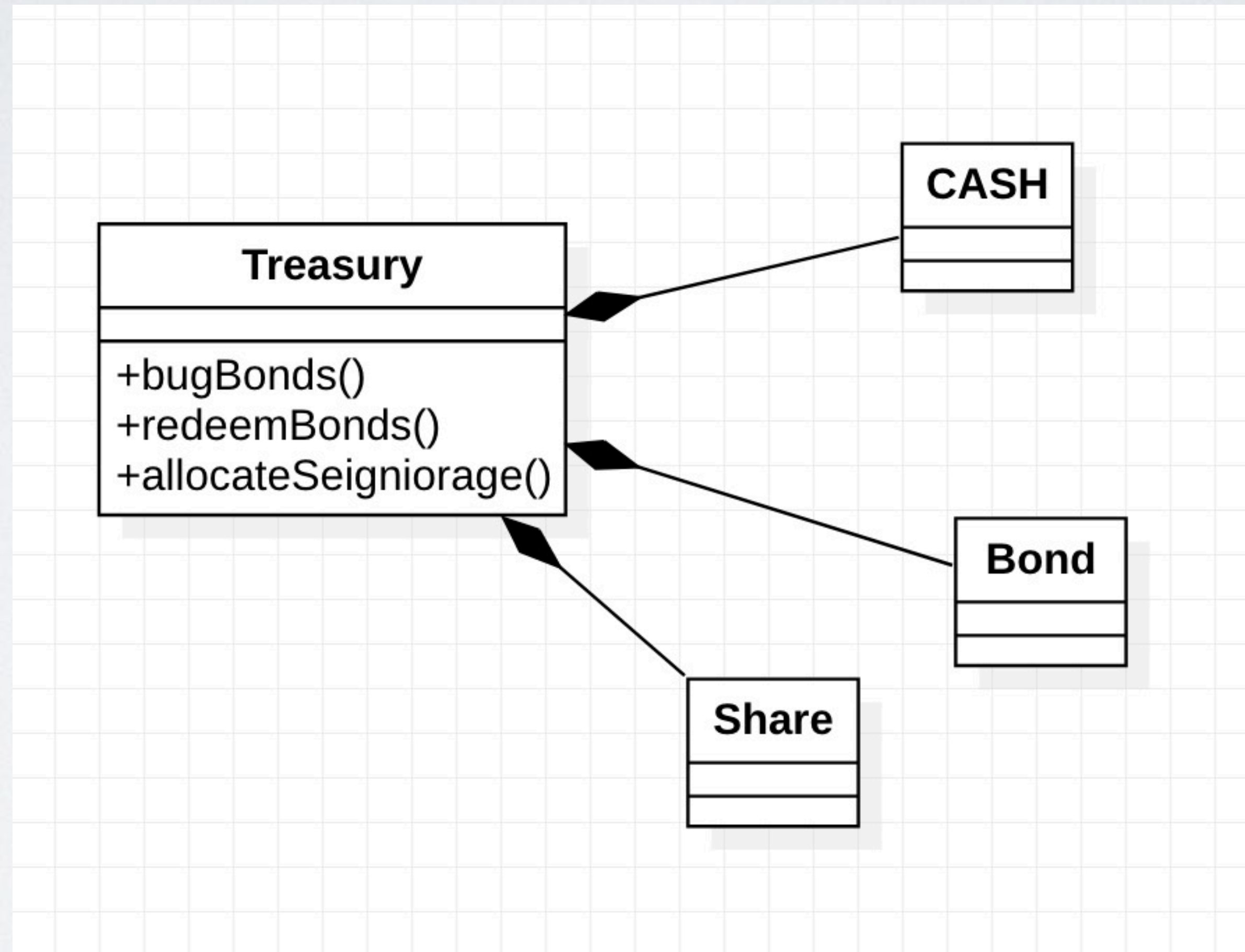


# 稳定币改良 Basis Cash

- 除 BAC 外，引入债券 Basis Bond (BAB) ， Basis Shares (BAS)
- 当  $BAC < \$1$  时， 可折价兑换 BAB( BAB 价格 = BAC 价格的平方)， 等 BAC 回到 1 美元的时候， 可以用 BAB 1: 1 赎回 BAC (减轻用户币变少的心理负担)
- 当  $BAC > \$1$  时， 若赎回之后， 仍  $> \$1$  增发 BAC 作为分红给质押的 BAS
- 号称“野生美联储”



# Basis Cash



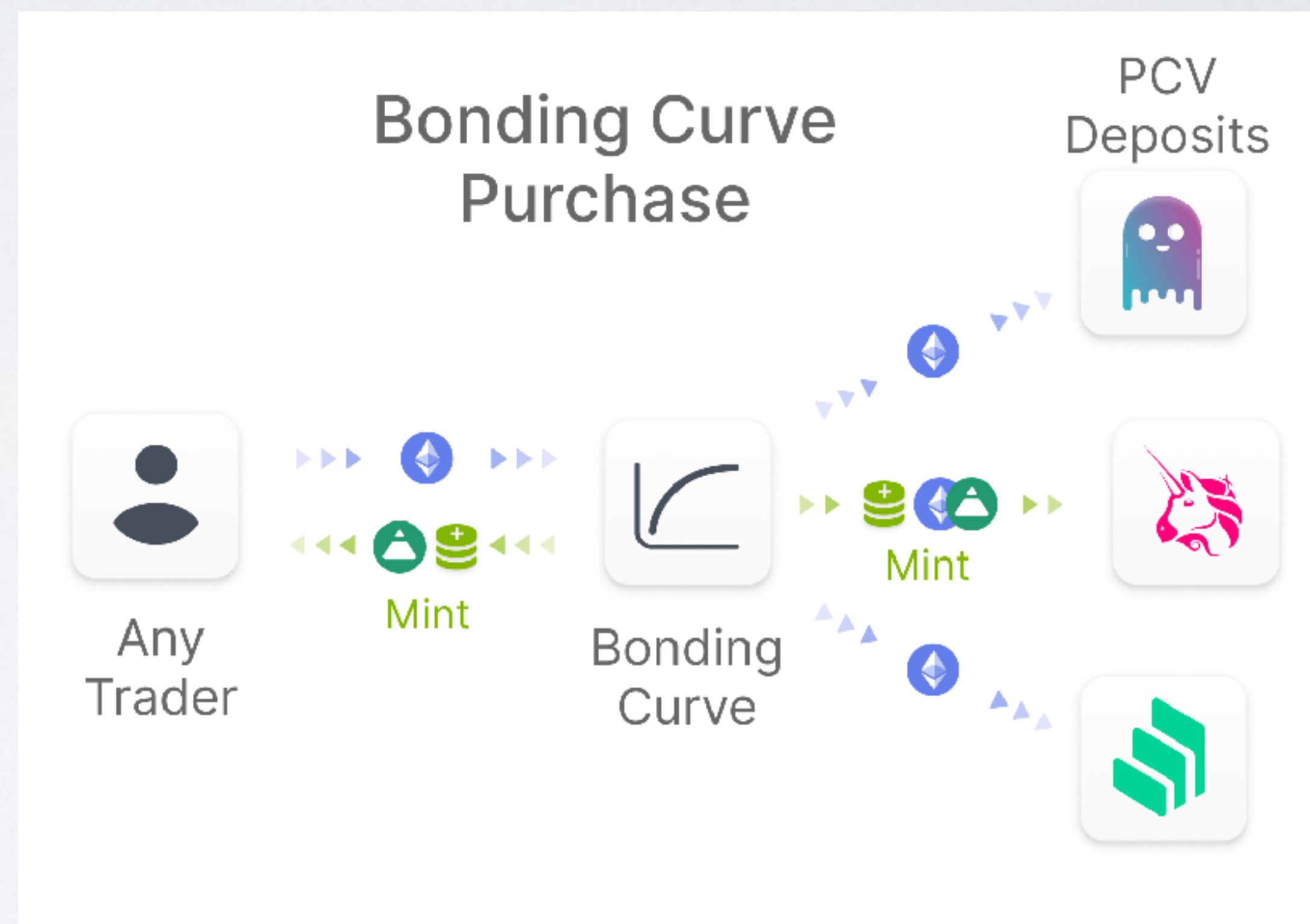
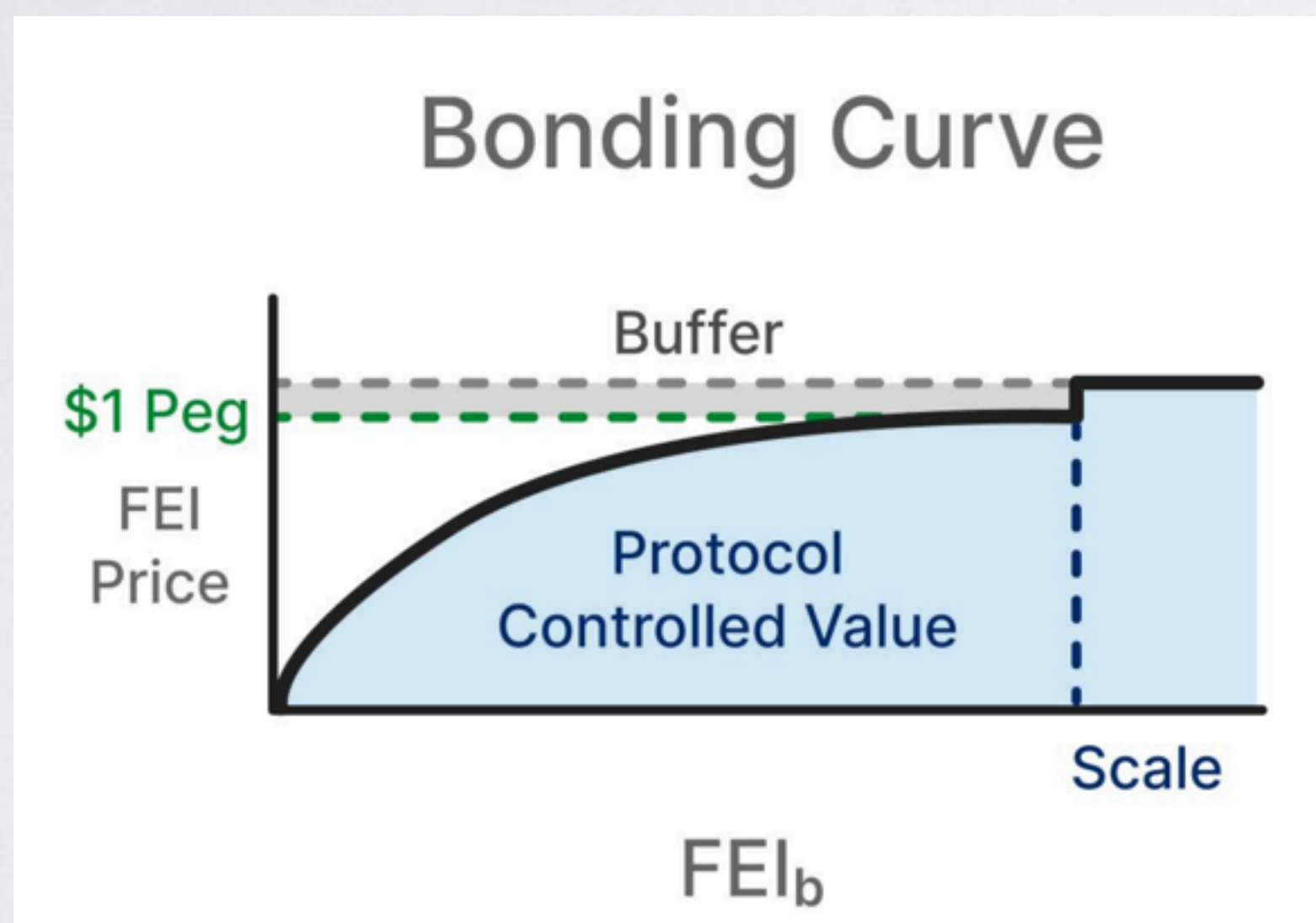
# 稳定币改良 Basis Cash

- 失败分析：完全依赖用户对系统的信心， 当市场信心不足时，无法维持与美元挂钩。
- 发生挤兑时， 没有做流动性 LP， 也不会有用户兑换为 BAB(债券)



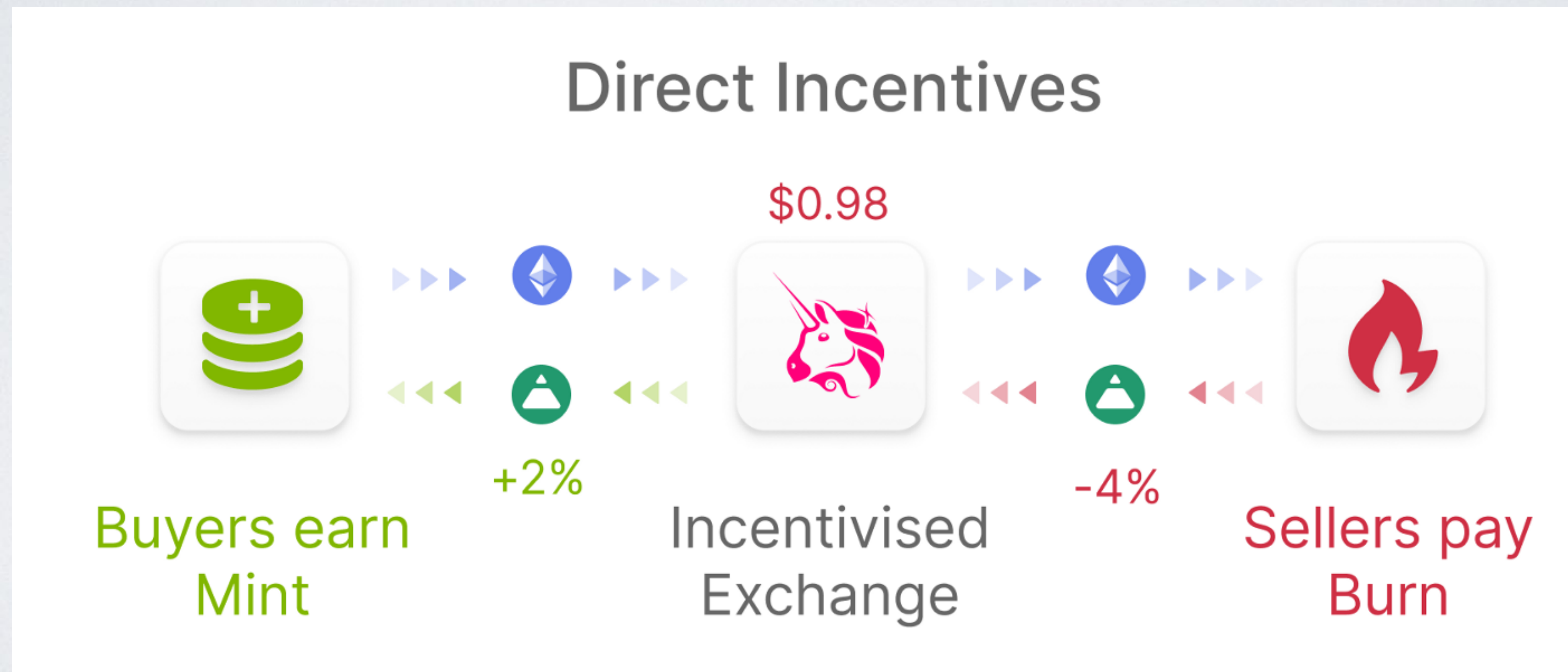
# FEI

- PCV : 协议控制价值 (FEI )



# FEI

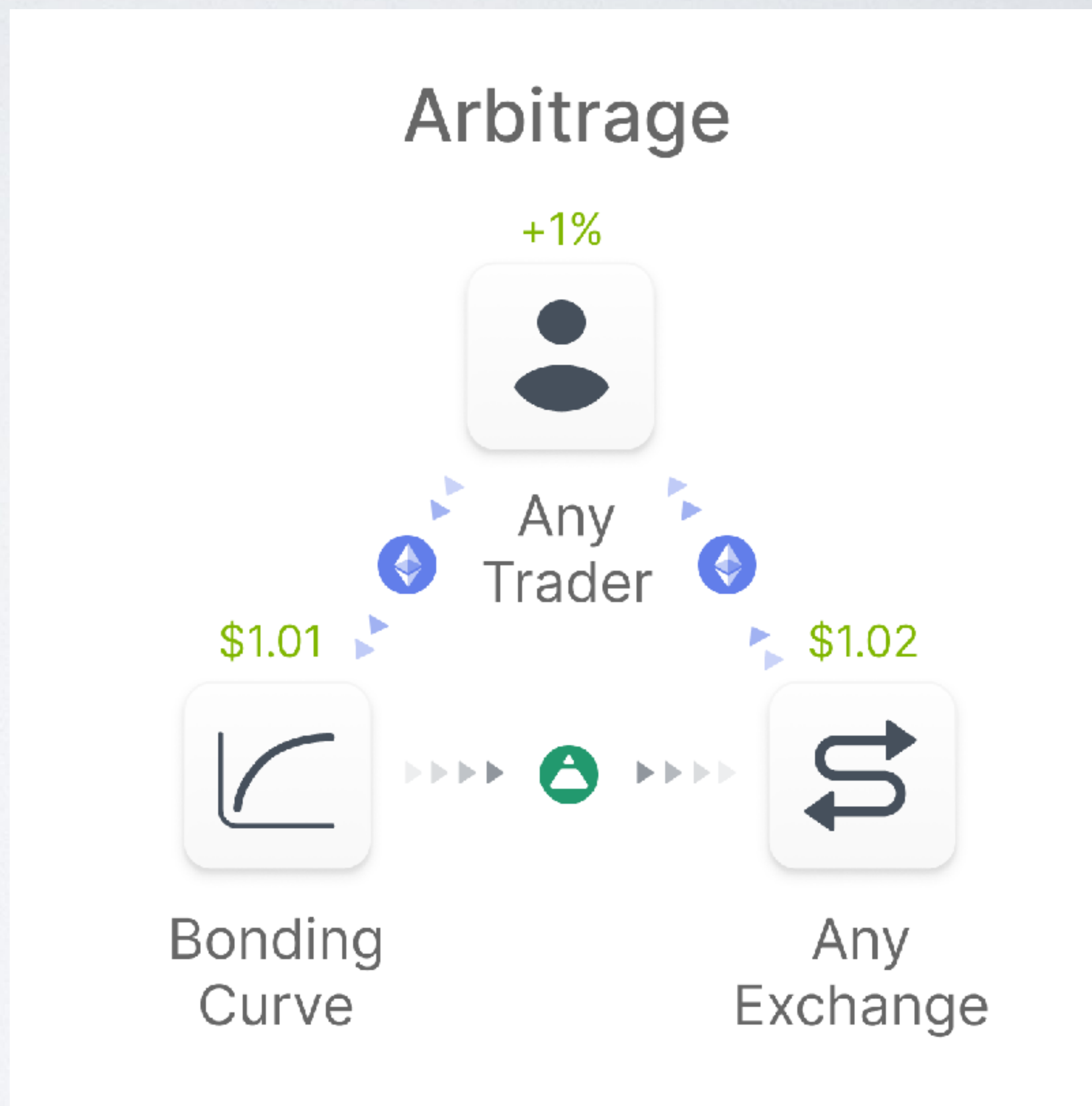
- (若外部低于\$1) 直接激励: 促使价格回归





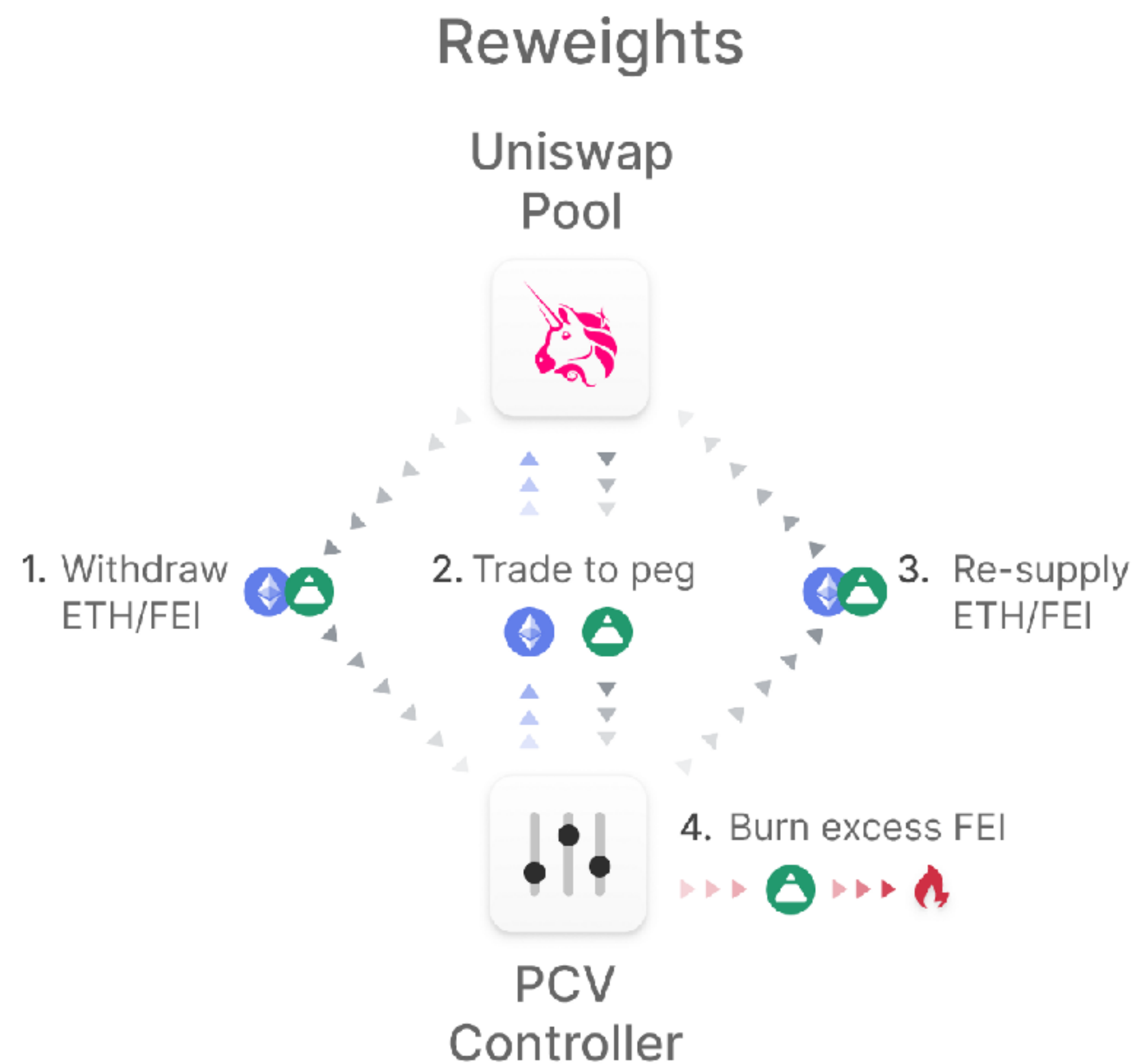
# FEI

- 若外部高于1美元是通过套利空间回归



# FEI

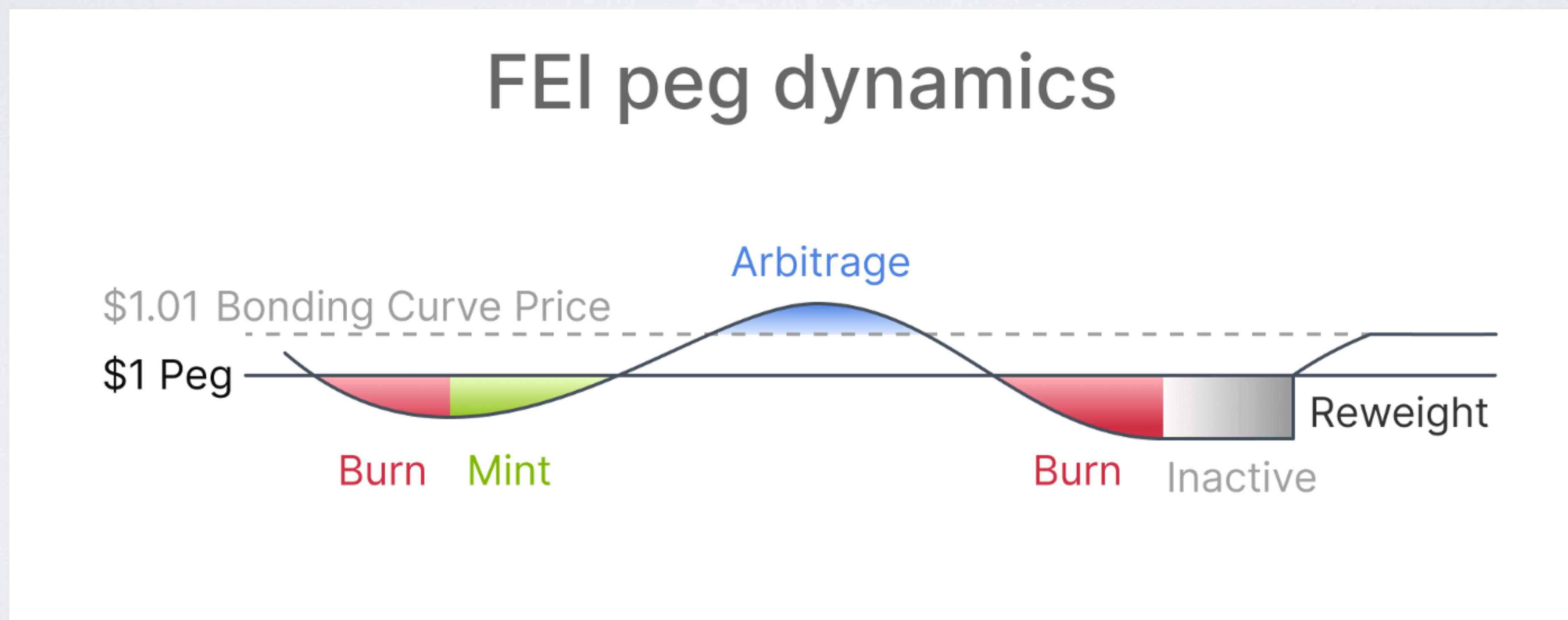
- PCV: 协议控制价值
  - 确保流动性不流失
  - Reweight 调节价格 (UniswapPCVController)

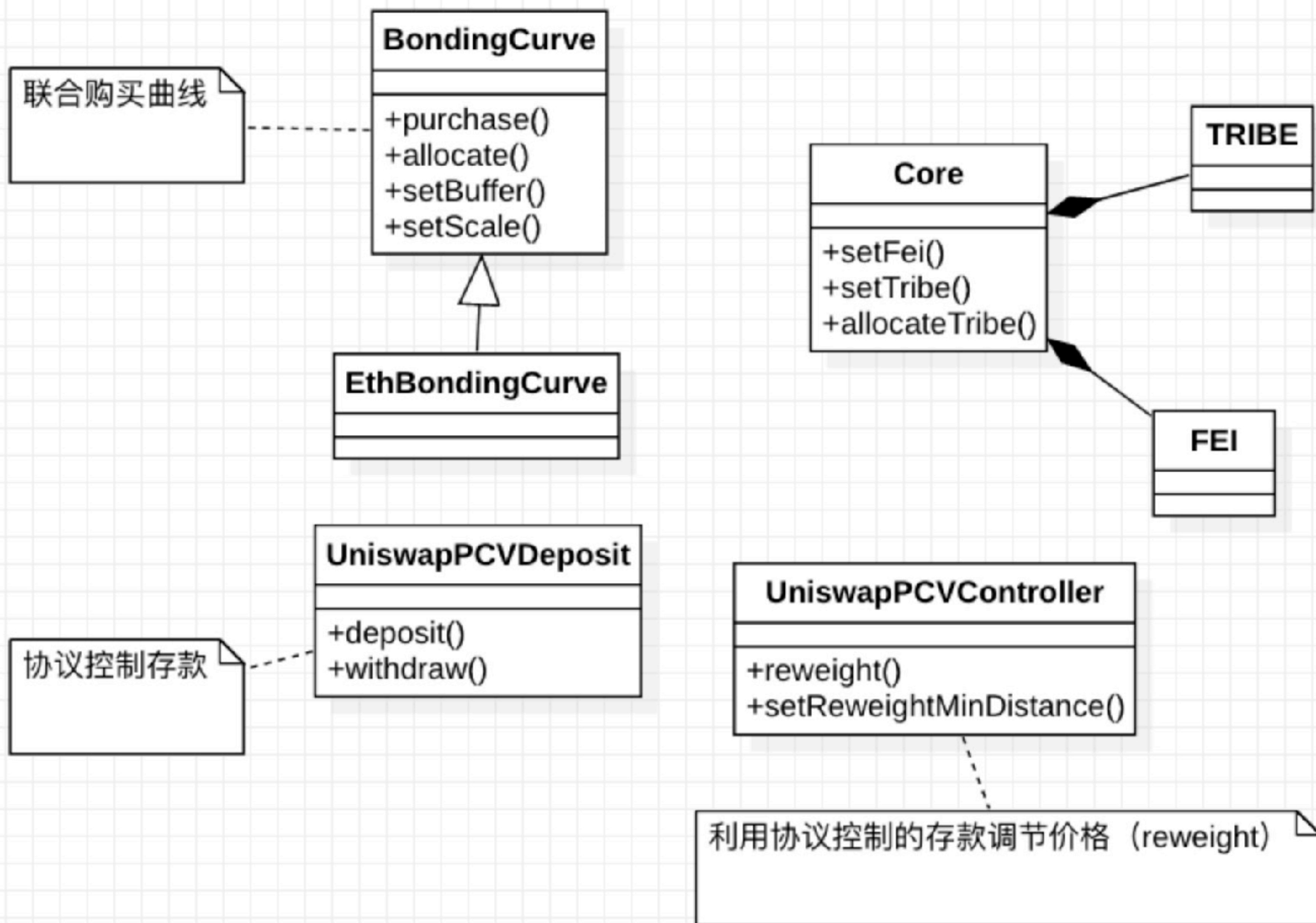




# FEI

- 最终实现动态锚定

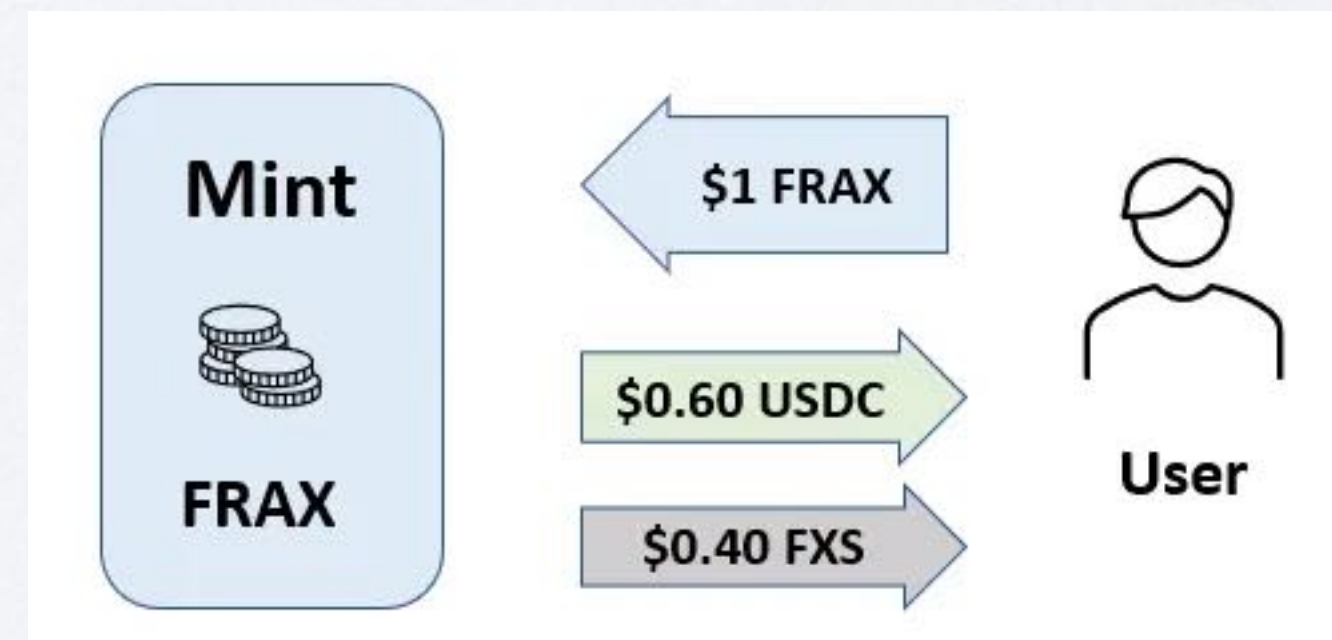
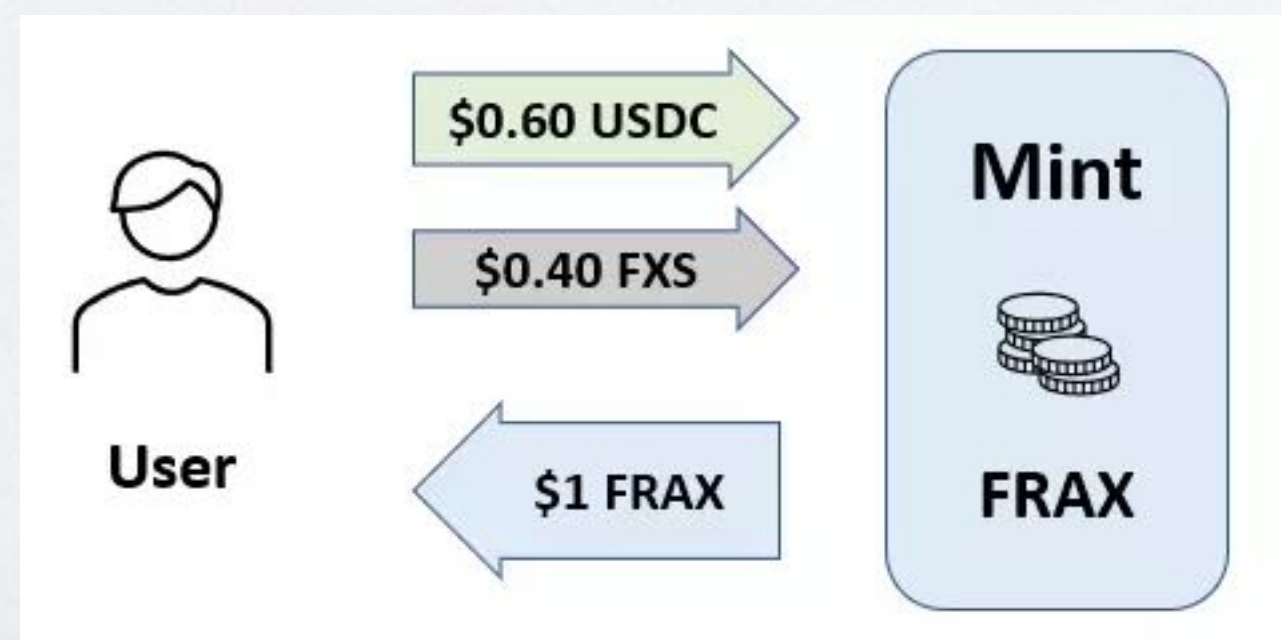




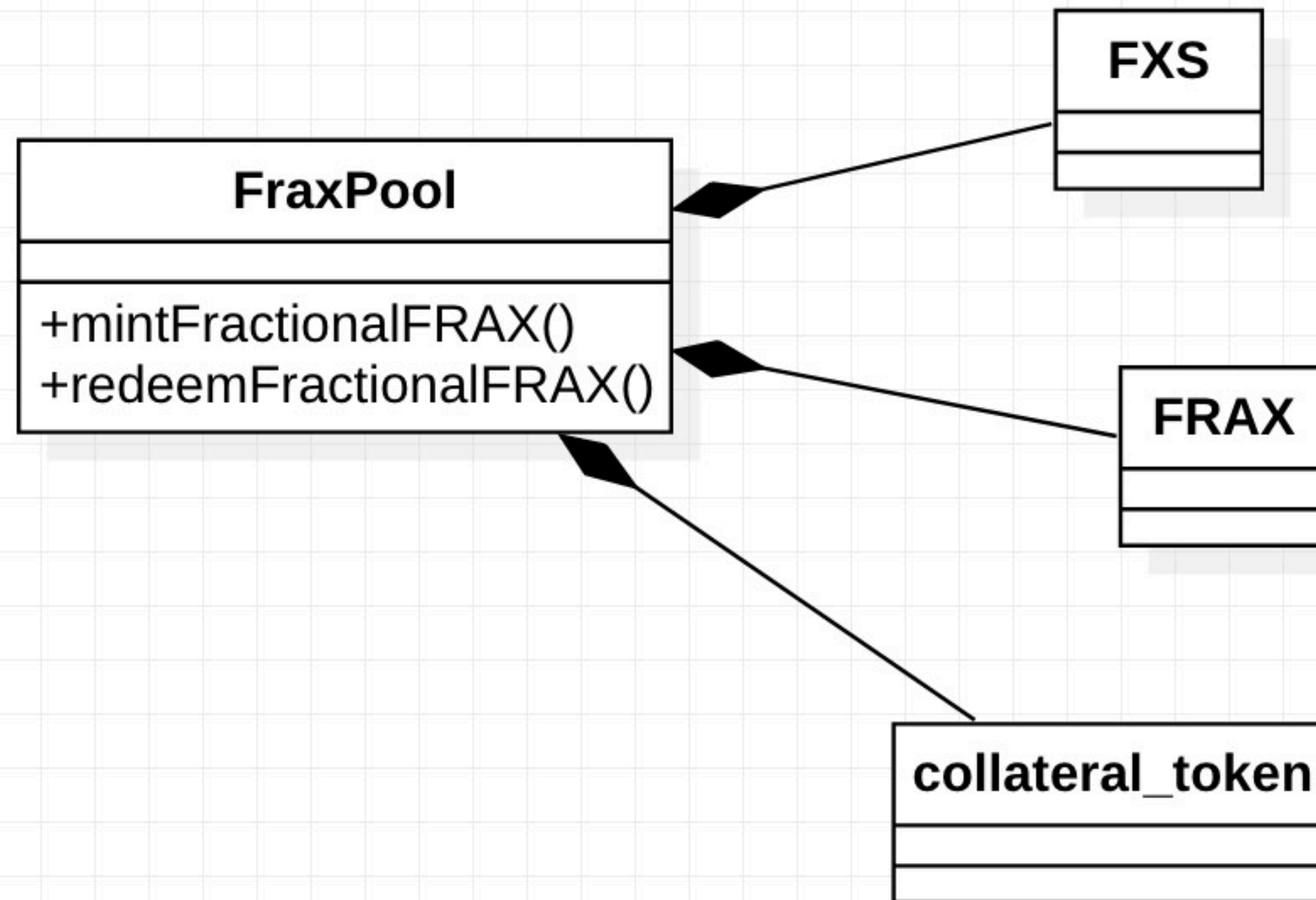


# Frax

- 纯算法稳定币，在早期缺乏信心时，容易进入螺旋死亡，FRAX采用渐进式实现算法稳定。
- 部分抵押，引入套利模式：
  - 当  $FRAX < \$1$ （外部价格），套利者会购买FRAX（外部），并以 FRAX 去赎回 USDC 和 FXS，并通过出售FXS获利(下右图)。对 FRAX 的购买需求将让汇率恢复。
  - 当  $FRAX > \$1$ （外部价格）：套利者将通过USDC和FXS去创建FRAX（系统内），并卖出FRAX而获利（外部），卖出压力将促使汇率恢复。



# Frax





# LUNA / UST

- LUNA 是 Terra 的生态治理代币；UST 则是锚定美元稳定币，1 UST 锚定1美元。
- UST 通过消耗 Luna 来铸造，销毁 UST 则赎回 Luna
- Luna 支撑 UST 价值且吸收UST的波动性。

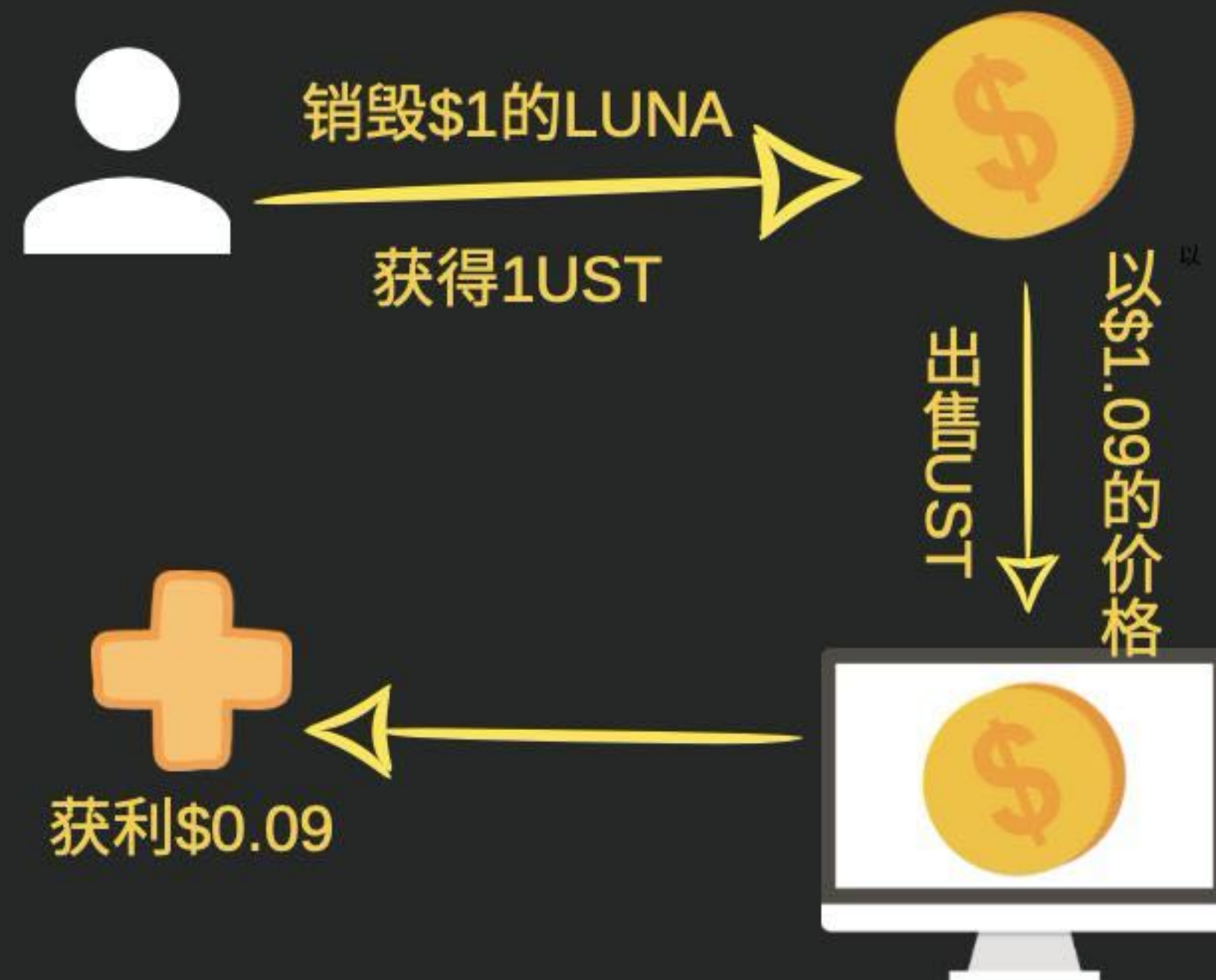




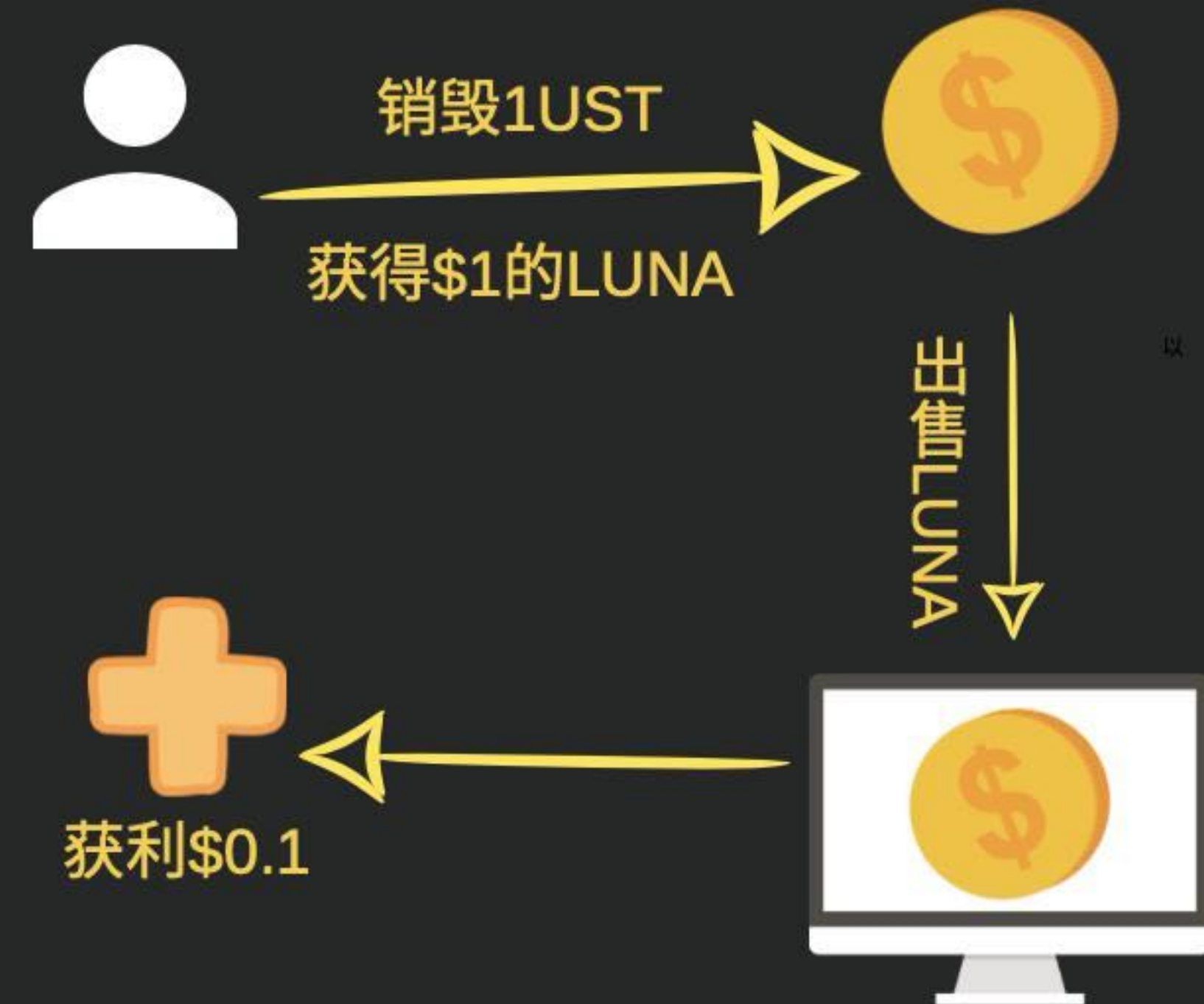
# 套利 -> 稳定

## 用户怎么套利

当UST价格 > \$1 (如\$1.1)



当UST价格 < \$1 (如\$0.9)





# LUNA

- 为了让UST和LUNA有更多的应用场景，LUNA 推出了一个稳定币年化 20% 的 Anchor 平台（旁氏吸储）
  - 通常稳定币收益 5% 已经不错。
- UST 的需求陡增，Luna 通缩，导致LUNA币也一路高歌猛进， 市场高达前 5，TVL 等数据漂亮
- 随着 Anchor 采用扩大， UST 利息支出越大越大，在抽调 UST 流动性时，被精准狙击猛烈砸盘（\$8500 万卖单导致 UST 脱锚），配合消息，让市场恐慌。
  - 市场恐慌时，不会再有人购买 UST 去销毁套利，而持有者直接卖出或销毁，进入死亡螺旋：
  - 用户销毁UST换LUNA → LUNA供给增加 → LUNA价格下跌
  - LUNA价格下跌 → 1 UST兑换的LUNA数量增加（LUNA 指数级增发） → UST价格进一步下跌



# 作业

- 设计一个通缩的 Token (ERC20) , 用来理解 rebase 型 Token 的实现原理:
  - 发行量每一年在上一年基础上下降 1%
  - rebase 方法进行通缩
  - balanceOf() 反应通缩后的余额。

<https://decert.me/quests/2d4df0b6-17dc-4e5b-8f3a-728ed855e292>