

读懂 Curve Stablecoin

崔晨

从多家交易所被起诉可以看出，美国对数字资产领域的监管态度愈发严格，不会任其发展。其中对稳定币的监管要求依旧是空白，美国国会没有通过稳定币相关法律，各监管机构也没有相应的牌照管理制度。在此背景下，在 BSC 上发行的 BUSD 被纽约金融服务部叫停，USDT、USDC 这两大美元稳定币仍面临很多不确定问题，去中心化稳定币再次成为市场焦点。

去中心化稳定币指的是储备资产在链上且由协议控制的稳定币，本文介绍的 crvUSD 就是其中一种。crvUSD 由 Curve 团队设计，通过超额抵押的方式发行美元稳定币。抵押品价格下跌时，crvUSD 创新地通过特定 AMM 实现软清算，并在抵押品价格回升后通过 AMM 买回抵押品。本文将基于 crvUSD 白皮书的内容，介绍 crvUSD 的设计思路，各组件的实现方式、潜在问题，现状等。

一、crvUSD 的设计思路

（一）通用去中心化稳定币的发行规则

本文讨论的去中心化稳定币是基于数字资产超额抵押发行的，与一般意义上的算法稳定币不同，资产抵押型稳定币的发行相当于用户超额抵押借贷，抵押资产会因为价格下跌到一定水平线而被清算，以偿还系统债务。这是维持稳定币价格的基础，保证稳定币的发行背后总是有足额的资产抵押。在抵押品价格下跌过程中，协议要对抵押品及时清算以保证系统不会

出现坏账，这时需要给清算者套利空间，以快速完成清算。清算过程可能存在的问题如下：

- 1、 市场剧烈波动时产生大量待清算资产，清算者为完成套利会在市场抛售清算资产，导致更剧烈的价格波动。
- 2、 资产被清算让抵押者利益受损，尤其是在抵押资产价格回升后，抵押者的损失是难以弥补的。

（二）crvUSD 对清算过程的改进和设计思路

1、引入软清算机制

在 crvUSD 中，抵押品的清算是通过 AMM 进行的，并且是以渐进式的软清算方式，抵押品会随价格下跌逐渐清算。AMM 中的清算是可逆的，在抵押品价格上涨后，AMM 会帮助用户买回资产。

2、清算 AMM 设计思路

crvUSD 通过 LLAMMA (Lending-Liquidating AMM Algorithm) 实现软清算，为抵押资产设计了一个特殊的 AMM 池，实现在资产价格下跌时逐渐清算。LLAMMA 中的清算线有两个，分别是清算开始价格和清算终止价格。在抵押资产高于清算价格时，AMM 池中全部是抵押品。抵押品价格下跌至清算开始价格时，AMM 中的抵押品开始被卖出换成稳定币，之后在价格下跌过程中抵押品被逐渐卖出。在抵押品价格跌至清算终止价格之下时，AMM 中只剩下稳定币。

LLAMMA 的清算过程可以理解为一个“反向的 Uniswap V3”。假设 AMM 要处理的是 ETH-USD 交易对 (LLAMMA 处理的是 ETH-crvUSD 交易对，下文简称 USD)，在 Uniswap V3 中，流动性提供者 (LP) 需要设置

ETH 的价格区间。当 ETH 的价格处于区间之内时，AMM 中存在两种可以互相交易的 Token，在价格区间之外时，AMM 池中只有一种 Token，这同样是 LLAMMA 清算开始价格和结束价格的设计思路。当抵押品是 ETH 时，价格高于区间 AMM 池中全部为 ETH，在价格区间之内时 ETH 逐渐被清算为 USD，见图 1。

不同的是，在 Uniswap V3 中，ETH 价格越高，AMM 池中的 USD 的数量越多。而在 LLAMMA 中，ETH 价格越低时，AMM 池中 USD 的数量越多，因为需要卖出 ETH 用于清算。ETH 价格升高时，还可以买回 ETH 抵押资产，尽量保证用户的敞口不变。

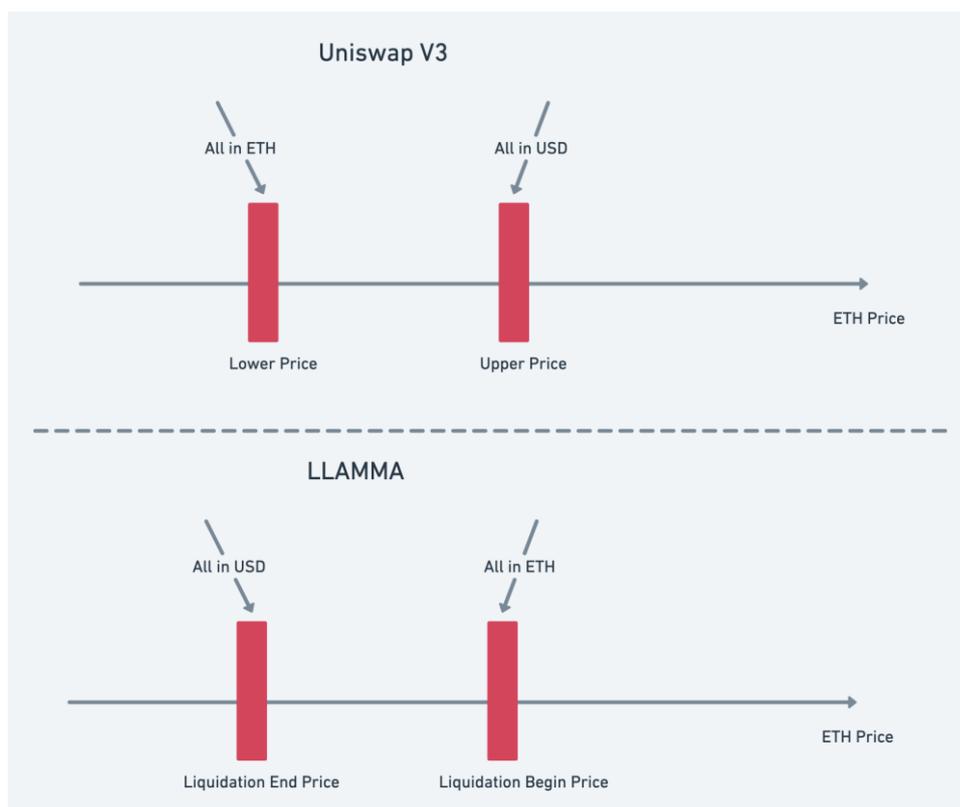


图 1: LLAMMA 实现的“反向 Uniswap V3”^[1]

图片来源: <https://paco0x.org/curve-stablecoin/>

3、LLAMMA 的定价方式

LLAMMA 之所以能够实现不同于传统 AMM ($x \cdot y = k$ 规则) 的交易

方向，是因为除了受资产池中 Token 的数量比例影响外，LLAMMA 的清算 AMM 中抵押资产定价 (p_{AMM}) 还会受外部预言机报价 p_{oracle} (p_o) 的影响。LLAMMA 需要 p_{AMM} 与 p_o 产生价格差，进而吸引套利者参与交易完成上文设定的“反向 Uniswap V3”清算机制。

例如，在外部 ETH 价格 (p_o) 下跌时，LLAMMA 需要对 ETH 进行清算。那么 p_{AMM} 要比 p_o 下跌得更多，这样才会有套利者从 AMM 中买走 ETH。这一过程与传统 AMM 正相反，因为传统 AMM 中资产的价格与外部价格无关，只与资产池中资产 X、Y 的数量有关。还是以 ETH-USD 交易对为例，当 ETH 价格变动时，传统 AMM 与 LLAMMA 实现的清算 AMM 的对比如表 1、表 2 所示。

表 1：当外部 ETH 价格下跌时，清算 AMM 与传统 AMM 的对比

外部 ETH 价格 (p_o) 下跌时	传统 AMM	清算 AMM
AMM 中 ETH 价格 (p_{AMM}) 变化	无变化，直到发生交易	比 p_o 下跌更多
套利活动	在 AMM 中出售 ETH (因为 p_{AMM} 高于 p_o)	在 AMM 中购买 ETH (因为 p_{AMM} 低于 p_o)
套利活动后 p_{AMM} 变化 (趋于 p_o)	降低	升高
AMM 中 ETH 数量变化	变多	变少

表 2：当外部 ETH 价格上涨时，清算 AMM 与传统 AMM 的对比

外部 ETH 价格 (p_o) 上涨时	传统 AMM	清算 AMM
AMM 中 ETH 价格 (p_{AMM}) 变化	无变化，直到发生交易	随 p_o 变化，且比 p_o 高
套利活动	在 AMM 中购买 ETH (因为 p_{AMM} 低于 p_o)	在 AMM 中售出 ETH (因为 p_{AMM} 高于 p_o)
套利活动后 p_{AMM} 变化 (趋于 p_o)	升高	降低
AMM 中 ETH 数量变化	变少	变多

总的来说，LLAMMA 是通过调整 AMM 内部价格，以实现在价格波

动时，抵押品的数量变化，最终 AMM 内的价格会趋于外部价格，此过程可以分为两步：

- (1) 外部预言机价格变化引起内部价格变化： p_o 升高或降低时， p_{AMM} 要升高或降低得更多，进而形成吸引套利者交易的价差。
- (2) 套利者活动引起 AMM 池抵押品数量变化：在第一步形成价差后，套利者会进行交易，使 p_{AMM} 趋于 p_o ，实现 LLAMMA 需要的交易方向。

二、实现 crvUSD 功能的组件

下图是 crvUSD 实现的具体方式，主要分为 LLAMMA、Controller、PegKeeper、Monetary Policy 几个组件。LLAMMA 指的是实现抵押资产清算的机制，Controller 负责分配抵押资产到清算 AMM 中，计算相应的清算价格，PegKeeper 通过参与 Curve V1 中的交易，维持 crvUSD 的价格稳定，Monetary Policy 负责调整 crvUSD 的借款利率，下文将详细介绍各组件的实现方式和潜在的问题。

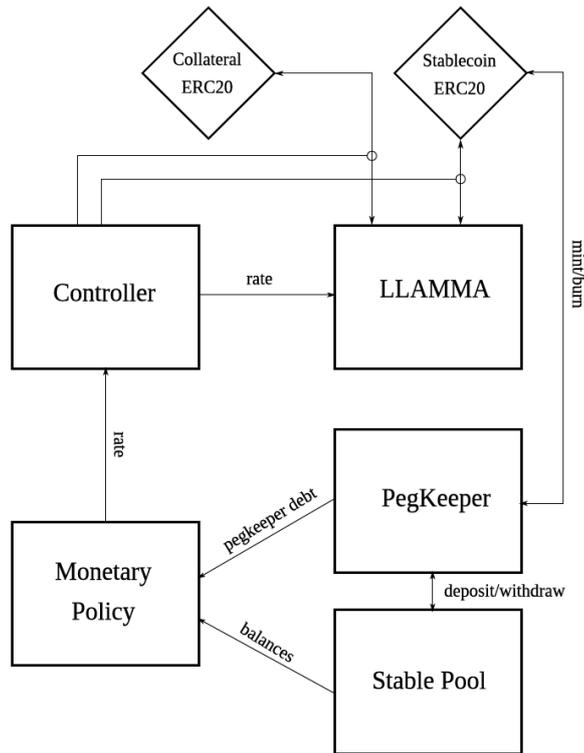


图 2: Curve Stablecoin 的主要组件^[2]

资料来源: <https://github.com/curvefi/curve-stablecoin/blob/master/doc/curve-stablecoin.pdf>

(一) LLAMMA

1、清算 Range 与 Band: p_{\uparrow} 和 p_{\downarrow} 的确定

当用户设置抵押资产数量和稳定币借款数量时,系统会通过 Controller 组件计算出抵押资产的清算范围,把抵押资产的流动性分配到相应的 Range 中。Range 是外部价格区间,代表清算开始和结束的范围,将在后文 Controller 部分详细介绍。

Range 会分为多个 Band, Band 代表最小的流动性区间,对应固定的外部价格。Band 有自己编号,挑选 Range 区间就是将流动性放入一组连续的 Band 中。实际中的清算和交易活动是根据当时的外部价格,发生在具体的 Band 中。

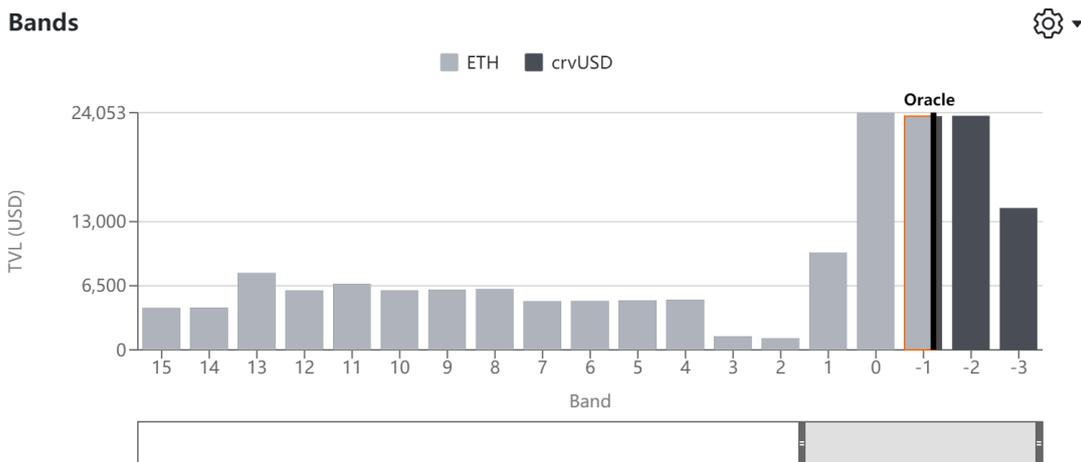


图 3: AMM 中的 Bands

p_{\uparrow} 和 p_{\downarrow} 分别代表 Band 外部价格的上下界， p_{\uparrow} 代表清算开始的价格， p_{\downarrow} 代表清算结束的价格。Band 中的上下界组成等比数列，乘以设定的基础价格 (p_{base})，Band 的上下界价格可以表示为：

$$p_{\uparrow}(n) = \left(\frac{A-1}{A}\right)^n p_{base} \quad (1)$$

$$p_{\downarrow}(n) = \left(\frac{A-1}{A}\right)^{n+1} p_{base} \quad (2)$$

2、 p_{cd} 、 p_{cu} 与 p_o 的关系

只讨论一个 Band 内的交易时，LLAMMA 中 AMM 要实现的 Token 种类变化与 p_o 关系如下图所示：当 p_o 处于 p_{\downarrow} 到 p_{\uparrow} 之间时，AMM 中有两种 Token，在 p_{\downarrow} 和 p_{\uparrow} 之外只有一种 Token。

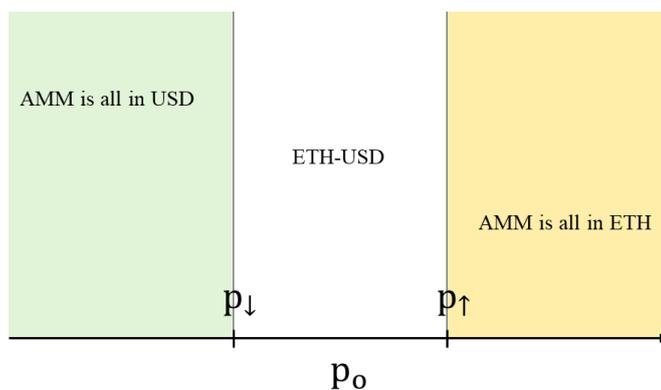


图 4: AMM 中 Token 种类与外部价格的关系

这意味着 p_o 等于 p_{\uparrow} 时，AMM 中资产应该全部为 ETH， p_o 等于 p_{\downarrow} 时，AMM 中资产应该全部为 USD。因此证明了即使 p_o 不变，AMM 中也会存在 ETH 价格的上下界，分别是 p_{cu} ($p_{current_up}$)和 p_{cd} ($p_{current_down}$)。

p_{cu} 和 p_{cd} 还可以这样理解：

上一章节提到了 LLAMMA 实现清算的两个步骤，代表了 AMM 中 ETH 价格 p_{AMM} 会受到两方面影响，引起不同的交易活动。

- (1) p_{AMM} 随 p_o 变化且形成与 p_o 的价差(变化幅度比 p_o 大)，进而吸引套利者，使 p_{AMM} 接近 p_o 。
- (2) 当 p_o 不变时， p_{AMM} 的定价逻辑与传统 AMM 相同，即套利者用 Δx_{USD} 换 Δy_{ETH} 时，会引起资产 Y 价格(p_{AMM})升高，反之亦然。

LLAMMA 要实现在某一 p_o 时，AMM 池中全部为 ETH 或 USD 的效果，就意味着在 p_o 不变时（步骤 2），AMM 的 ETH-USD 交易对存在流动性价格区间 $[p_{cd}, p_{cu}]$ 。其中， p_{cu} 代表 ETH 的价格上限，此时 AMM 中全部为 USD， p_{cd} 代表 ETH 的价格下限，此时 AMM 中全部为 ETH。

Curve Stablecoin 白皮书给出图 5 说明 LLAMMA 机制下 p_o 与 p_{AMM} 的关系。其中紫线的斜率为 1，代表由于套利者存在， p_{AMM} 会向 p_o 收敛。 p_{AMM} 只有在 p_{cd} 和 p_{cu} 之间时，才会同时有 ETH-USD 交易对的流动性。在 p_o 等于 p_{\uparrow} 时， p_{AMM} 等于 p_{cd} ，此时 AMM 中全部为储备资产 ETH。随着 p_o 下跌，清算发生，直到 p_o 等于 p_{\downarrow} 时， p_{AMM} 等于 p_{cu} ，此时 AMM 中全部为用户债务 USD。

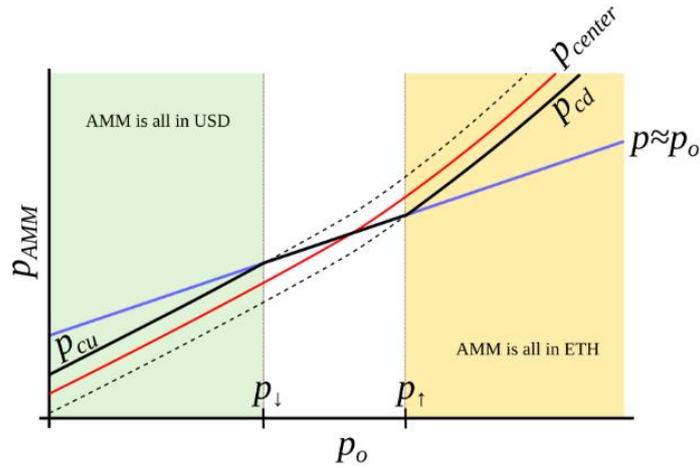


图 5: Curve Stablecoin 的 LLaMMA 实现思路^[2]

资料来源: <https://github.com/curvefi/curve-stablecoin/blob/master/doc/curve-stablecoin.pdf>

对于 crvUSD 来说, 只有找到 p_{cd} 、 p_{cu} 与 p_o 的关系, 才能得到 AMM 中的内部价格区间。由图 5 可知, p_{cu} 、 p_{cd} 上涨、下跌的幅度比 p_o (斜率为 1) 大, 且 $p_o = p_{\downarrow}$ 时, p_{cu} 过 $(p_{\downarrow}, p_{\downarrow})$ 点, $p_o = p_{\uparrow}$ 时, p_{cd} 过 $(p_{\uparrow}, p_{\uparrow})$ 点, 理论上无数条线满足要求, 例如: ^[3]

$$p_{cd} = \frac{p_o^{n+1}}{p_{\uparrow}^n}, \quad p_{cu} = \frac{p_o^{m+1}}{p_{\downarrow}^m} \quad (3)$$

Curve Stablecoin 白皮书选择了 $n=m=2$:

$$p_{cd} = \frac{p_o^3}{p_{\uparrow}^2}, \quad p_{cu} = \frac{p_o^3}{p_{\downarrow}^2} \quad (4)$$

3、LLAMMA 中的 AMM 兑换公式

上文提到, 在 p_o 不变的情况下, AMM 存在价格区间 $[p_{cd}, p_{cu}]$, 图 6 可以抽象理解这一概念, 即 p_{AMM} 只有在 p_{cd} 和 p_{cu} 之间时, 才会同时有 ETH-USD 交易对的流动性。

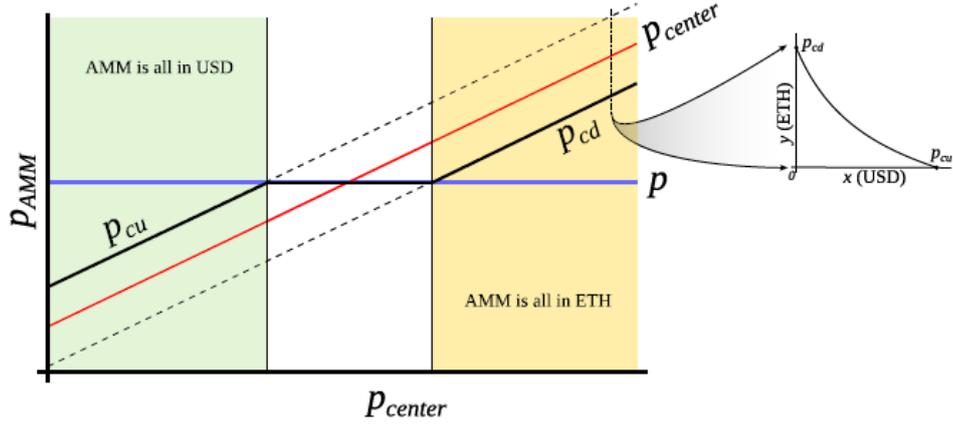


图 6: 在价格区间 p_{cd} - p_{cu} 发生类似 Uniswap V3 的交易

图 7 是 p_o 不变情况下 LLAMMA 中的 AMM 与 Uniswap V3 的对比，
这两者的交易逻辑是一样的。[3]

已知 Uniswap V3 的恒定乘积公式：

$$\left(x + \frac{L}{\sqrt{p_b}}\right)(y + L\sqrt{p_a}) = L^2 \quad (5)$$

可以得出 LLAMMA 中的 AMM 交易公式

$$\left(x + \sqrt{I}\sqrt{p_{cd}}\right)\left(y + \frac{\sqrt{I}}{\sqrt{p_{cu}}}\right) = I \quad (6)$$

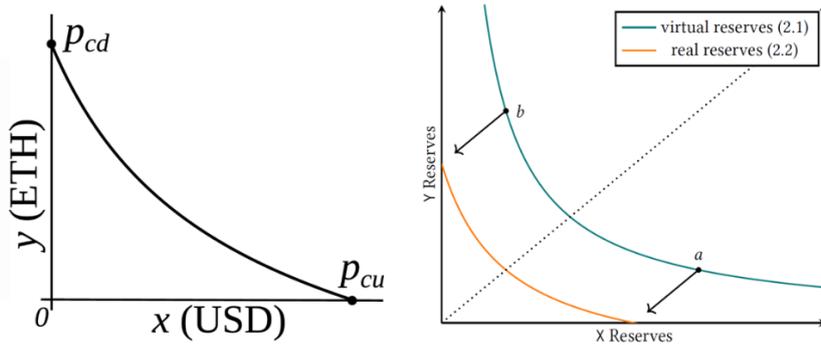


图 7: 在 p_o 不变情况下的 LLAMMA (左) 与 Uniswap V3 (右)

根据公式 (1) (2) (4) (6)，代入图 7 中特殊点 $(0, y_0)$ ，此时 $p_{\uparrow} = p_o$ ，
可得 $I = p_o A^2 y_0^2$ ，最终得到 AMM 的公式：

$$\left(\frac{p_o^2}{p_{\uparrow}} A y_0 + x\right)\left(\frac{p_{\uparrow}}{p_o} (A - 1) y_0 + y\right) = p_o A^2 y_0^2 \quad (7)$$

其中， y_0 指的是在 Band 里的资产全部转化为 ETH 时，ETH 的数量。

4、小结

LLAMMA 通过调整 AMM 内价格与实际价格的差异，吸引交易者套利，进而实现资产价格下跌且数量减少的清算效果。可以看出，在 AMM 中存在两个价格区间：

- (1) p_l-p_r ：LLAMMA 进行软清算的区间，由外部价格确定。通过套利在区间内完成资产数量变化。
- (2) $p_{cd}-p_{cu}$ ：LLAMMA 内部 AMM 的价格区间， p_{AMM} 、 p_{cd} 、 p_{cu} 都受 p_0 影响。在 p_0 不变的情况下， p_{AMM} 只受 AMM 中资产数量比例的影响。

在 LLAMMA 中，用户的抵押资产作为 AMM 的 LP，在 p_l-p_r 区间内发生软清算，ETH 价格下跌后会被逐渐卖成 crvUSD，ETH 价格上涨后还可以通过 AMM 逐渐买回 ETH 抵押品。由于 LLAMMA 中的价格变化有利于套利者，ETH 下跌并上涨到原价格后，AMM 无法买回原有数量的 ETH，造成了 LP 的永久亏损。尤其是在外部价格剧烈变化时，AMM 形成的价差更大，LP 的损失更多。LLAMMA 中的手续费收入难以弥补这种亏损，但相较于其他借贷协议实施的强制清算方式，软清算机制可以挽回不可逆清算造成的损失。

(二) Controller

1、抵押品的清算价格区间

LLAMMA 中 AMM 的流动性的添加和移除是由 Controller 控制的，与债务的创建和取消相关。用户在抵押 ETH 创建债务时，ETH 会由 Controller 分配给 AMM 中的价格区间，即 Range。Range 是一组连续 Band，宽度指

的是包含 **Band** 的个数，用户可在 4-50 个之间调整。

ETH 价格下跌至最大 **Band** 的外部价格上限 p_{\uparrow} 时，开始清算。ETH 价格下跌至最小 **Band** 的外部价格下限 p_{\downarrow} 时，所有抵押 ETH 都被清算为 **crvUSD**。**Range** 的宽度代表流动性的集中度，会影响用户资产清算的开始和结束价格，包含的 **Band** 越多清算开始的价格越高，清算结束的价格也越低。**Band** 越少代表流动性越集中，清算开始的价格越低。

用户需要提供 ETH 资产数量、创建 **crvUSD** 债务量和 **Band** 数量三个参数，由 **Controller** 计算保证用户抵押资产全部清算后的 **crvUSD** 数量大于债务量后，帮用户创建债务并向对应的 **Range** 中添加 ETH。用户偿还债务撤出 ETH 抵押品也是由 **Controller** 负责。

2、最大 LTV 与清算

根据公式 (7)，假设在 p_0 在缓慢变化的情况下，**Controller** 能够计算出一个 **Band** 中，清算全部 ETH 最多能换出 **crvUSD** 的量 (x_{\downarrow})。对于用户来说，最多借出的 **crvUSD** 需要在 x_{\downarrow} 基础上打折扣 (**loan_discount**)，才能得到 **Band** 内可以实现的最大 LTV (**Loan To Value**，贷款价值比)。在 **Curve** 中，**loan_discount** 和 LTV 可以通过治理更改，目前各抵押品在 **Band** 中的 LTV 在 89%左右。

用户在整个 **Range** 内的最大 LTV 要小于 **Band** 的最大 LTV，因为每个 **Band** 对应 ETH 定价的不同会让相同数量 ETH 清算出的 **crvUSD** 数量不同。尤其是当 **Range** 包含的 **Band** 数量越多时，**Range** 内最大 LTV 越小。相反当 **Range** 越窄，包含的 **Band** 数量越少时，能实现的最大 **crvUSD** 借款量越多，因为可以得到较集中的清算。

用户抵押资产和债务的关系可以计算出债务的健康值，当健康值低到一定程度时（与 `liquidation_discount` 值有关，一般为 6%），会触发软清算。而当市场剧烈变化时（ p_0 突然下跌），**Controller** 计算出用户资产全部被软清算为 **crvUSD** 也不够偿还债务时（健康值为负），则触发硬清算。硬清算模式与其他协议的清算过程相似，用户的 **ETH** 直接出售，上涨后不会被 **AMM** 买回。

3、小结

LLAMMA 和 **Controller** 两者配合在一起，组成了 **Curve Stablecoin** 最具创新性的部分，并且具有广泛应用于借贷协议的潜质。软清算机制可以降低用户资产被一次性清算的风险，由于渐进式地清算机制，清算可以在抵押品价格较高的位置发生，所以 **crvUSD** 可以实现比其他借贷协议更高的 **LTV**。

过早清算的代价是抵押品在出售过程中会因套利者的存在而受到损失，虽然相对于其他借贷协议的一次性清算机制而言抵押品已经得到保护，但用户依然需要调整自己的债务，避免抵押资产处于清算区间。

清算的起始价格也与用户设置的 **Band** 数量有关，如果 **Band** 数量多，清算价格区间大，就会导致抵押资产价格下跌时过早清算。但如果 **Band** 数量少，清算价格区间小，抵押资产的市场价格快速下跌时，可能导致软清算机制失效，触发硬清算。

（三）**PegKeeper**

1、**crvUSD** 在 **Curve V1** 池（**Stable Pool**）中的稳定机制

crvUSD 在 **Curve V1** 中有四个池，分别是与 **USDC**、**USDT**、**TUSD**、

USDP 组成的交易对，这些是普通的 Curve 池，用户可以不受限地添加和撤出流动性，在这四个池中会分别形成 crvUSD 的价格 p_s 。当 p_s 大于 1 时，代表市场对 crvUSD 的需求让池中资产比例失衡，PegKeeper 会直接铸造 crvUSD 添加到池中，铸造 crvUSD 的债务上限由治理决定。与之相反的是当 p_s 小于 1 时，PegKeeper 会移除池中的 crvUSD 数量并销毁，上限为之前 PegKeeper 铸造的 crvUSD 总量。

PegKeeper 代表 crvUSD 中无抵押发行的部分，只能将铸造出的 crvUSD 添加到指定的四个 Curve V1 池中，移除的也是这些池中的流动性。平衡池中代币数量是控制 crvUSD 价格稳定最直接的方式，PegKeeper 和 LLAMMA 相对独立，LLAMMA 在清算机制上保证了所有用户创建的 crvUSD 债务都是有超额资产抵押的。

2、小结

PegKeeper 通过铸造和销毁 crvUSD，控制 crvUSD 在池中的流通量来维持 crvUSD 价格稳定，整个过程相当于在 crvUSD 价格高时卖 crvUSD 给 Pool，价格低时在 Pool 中买 crvUSD，PegKeeper 在流动池中的套利收入源自其他 LP 的无常损失。

如果在只在 Curve 交易场所内，依靠 Curve V1 池由 PegKeeper 维持市场上全部流通的 crvUSD 的价格稳定是比较困难的，这需要足够的流动性。PegKeeper 在添加流动性时有债务上限，而撤出流动性的上限只与 PegKeeper 已经创建的债务有关。

（四）Monetary Policy

Monetary Policy 在系统中负责调整 crvUSD 的借款利率，其作用为降

低利率鼓励用户借款或提高利率抑制用户债务规模。借款利率的计算公式如下，主要受 crvUSD 的价格和 PegKeeper 债务占全部债务的比例影响：

$$rate = rate_0 * e^{\left(-\frac{p-1}{sigma}\right)} * e^{\left(-\frac{peg_keeper_debt}{total_debt*peg_keeper_target_fraction}\right)} \quad (8)$$

其中，当 crvUSD 的价格高于 1 时，借款利率会降低，鼓励用户借款向市场中增加供应。当 crvUSD 价格低于 1 时，借款利率会增加以减少供应，鼓励用户偿还借款。

当 PegKeeper 的债务占全部债务的比例越大时，也就是 PegKeeper 铸造的 crvUSD 的数量较多，代表 PegKeeper 未来销毁 crvUSD 的上限较高，有足够能力在 crvUSD 价格小于 1 时进行调整，借款利率会下降。反之 PegKeeper 的比例降低，借款利率会上升。

三、crvUSD 的现状

crvUSD 在 2023 年 5 月 17 日上线 UI，最先开放的是 wsteth 和 sfrxeth 这两种抵押品，也是目前已创建债务量最大的两种抵押品。截至 7 月 6 日，crvUSD 上线的四种抵押品分别是 wstETH、sfrxETH、WBTC、ETH，债务上限分别是 1.5 亿、1 千万、2 亿、2 亿枚 crvUSD。可以看出，Curve 不仅为 LSD 产品提供交易场所，还为 LSD 提供应用场景。除了 LSD 之外，未来 crvUSD 添加的抵押品也是市场关注的方向，例如 Curve 中的 LP Token。

crvUSD 上线后，Curve 交易池开启了 CRV 的挖矿活动，最高收益率保持在 10% 以上，但 Curve 中没有 crvUSD-DAI 的交易池。crvUSD 作为去中心化稳定币，与 DAI 是竞争关系。crvUSD 集成了 DeFi 中的 AMM、借贷、稳定币模块，专注于开发内部产品互操作性。不仅是 Curve，其他 DeFi 协议也有类似的产品布局。

最后，crvUSD 也给 Curve 未来带来潜在收益，这包括：给 Curve LP Token 提供应用场景、LLAMMA 模块的管理费、PegKeeper 套利收入、借款利息收入等。

参考资料：

[1] 《Curve Stablecoin 非权威解读》

<https://paco0x.org/curve-stablecoin/>

[2] 《Curve stablecoin designx》

<https://github.com/curvefi/curve-stablecoin/blob/master/doc/curve-stablecoin.pdf>

[3] 《From Uniswap v3 to crvUSD LLAMMA》

<https://www.curve.wiki/post/from-uniswap-v3-to-crvusd-llamma-%E8%8B%B1%E6%96%87%E7%89%88>

（审核：邹传伟）