

Figure 2: Dependence of the loss on the price shift relative to the liquidation threshold. Time window for the observation is 3 days

In this design, if someone borrows against collateral, even at liquidation threshold, and the price of collateral dips and bounces – no significant loss happen. For example, according to simulations using historic data for /USD since Sep 2017, if one leaves the CDP unattended for 3 days and during this time the price drop of 10% below the liquidation threshold happened – only 1% of collateral gets lost.

在这种设计中，假定有人用抵押品借款，即使是在清算阈值，抵押品的价钱下跌后反弹-也不会发生清楚的丧失。例如，依据自2017年9月以来运用ETH/USD的历史数据中止的模拟，假定放着CDP无人看守3天，在此时期，价钱下跌至低于清算价钱10%的状况发生的话，也只需1%的抵押品被丧失。

AMM for continuous liquidation/deliquidation (LLAMMA)

继续清算/无需清算的AMM (LLAMMA)

The core idea of the stablecoin design is Lending-Liquidating AMM Algorithm. The idea is that it converts between collateral (for example, ETH) and the stablecoin (let' s call it USD here). If the price of collateral is high – a user has deposits all in ETH, but as it goes lower, it converts to USD. This is very different from traditional AMM designs where one has USD on top and ETH on the bottom instead.

波动币设计的中心思想是Lending-Liquidating AMM算法。这个想法是，它在抵押品（例如ETH）和稳定币（这里权且称之为USD）之间中止转换。假定抵押品的价钱很高-用户的放款都是ETH，但当价钱降低时，它就会转换为USD稳定币。这与激进的AMM设计有很大不同，保守的AMM设计是将USD稳定币放在下面（AMM曲线上半截），ETH放在下面（AMM曲线下半截）。

The below description doesn' t serve as fully self-consistent rigorous proofs. A lot of that (especially the invariant) are obtained from dimensional considerations. More research might be required to have a full mathematical description, however the below is believed to be enough to implement in practice.

下面的描画并不能作为一个完整自洽的松散证明。很多东西（特地是不变量）都是从各种维度思索取得的。要有一个完整的数学描画，可以需求更多的研讨，但是上面的描画被以为足以支持在中实施。

This is only possible with an external price oracle. In a nutshell, if one makes a typical AMM (for example with a bonding curve being a piece of hyperbola) and ramps its "center price" from (for example) down to up, the tokens will adiabatically convert from (for example) USD to ETH while proving liquidity in both ways on the way (Fig. 3). It is somewhat similar to avoided crossing (also called Landau-Zener transition) in quantum physics (though only as an idea: mathematical description of the process could be very different). The range where the liquidity is concentrated is called band here, at the constant p_0 band has liquidity from p_{cd} to p_{cu} . We seek for $p_{cd}(p_0)$ and $p_{cu}(p_0)$ being functions of p_0 only, functions being more steep than linear and, hence, growing faster than p_0 (Fig. 4). In addition, let's define prices p_{\downarrow} and p_{\uparrow} being prices where $p_{\downarrow}(p_0) = p_0$, and $p_{\uparrow}(p_0) = p_0$, defining ends of bands in adiabatic limit (e.g. $p = p_0$).

这只需经过外部喂价才干完成。简而言之，假设一团体做了一个典型的AMM（例如，粘合曲线是一块双曲线），并将其“中心价钱”从（例如）下降到下降，代币将从（例如）USD“绝热”地转换为ETH，同时在进程中提供两种方式的流动性（图3）。这有点类似于量子物理学中的“规避交叉”（也称为Landau-Zener跃迁）（固然只是一个概念：对该进程的数学描画可以十分不同）。

流动性集合的范围在这里被称为“波段”（Band），在恒定的 p_0 波段有从 p_{cd} 到 p_{cu} 的流动性。我们寻求 $p_{cd}(p_0)$ 和 $p_{cu}(p_0)$ 只作为 p_0 的函数，函数比线性更峻峭，因此，增减速度比 p_0 快（图4）。此外，让我们把价格 p_{\downarrow} 和 p_{\uparrow} 定义为 $p_{\downarrow}(p_0) = p_0$ 和 $p_{\uparrow}(p_0) = p_0$ 的价格，定义为绝热极限中的波段两端（例如 $p = p_0$ ）。

Figure 3: Behavior of an "AMM with an external price source". External price p_{center} determines a price around which liquidity is formed. AMM supports liquidity concentrated from prices p_{cd} to p_{cu} , p_{cd}

We start from a number of bands where, similarly to Uniswap3, hyperbolic shape of the bonding curve is preserved by adding virtual balances. Let say, the amount of USD is x , and the amount of ETH is y , therefore the "amplified" constant-product invariant would be:

我们从一些波段末尾，与Uniswap3相似，经过增加“虚拟余额”，保管了粘合曲

线的双曲外形。比如说，USD的数量是 x ，ETH的数量是 y ，因此"增强的"常数-产品不变性将是：

We also can denote $x_0 \equiv x + f$ and $y_0 \equiv y + g$ so that the invariant can be written as a familiar $I = x_0 y_0$. However, f and g do not stay constant: they change with the external price oracle (and so does the invariant I , so it is only the invariant while the oracle price p_0 is unchanged). At a given p_0 , f and g are constant across the band. As mentioned before, we denote p_{\uparrow} as the top price of the band and p_{\downarrow} as the bottom price of the band. We define A (a measure of concentration of liquidity) in such a way that:

我们也可以表示 $x_0 \equiv x + f$ 和 $y_0 \equiv y + g$ ，这样不变式就能够写干练习的 $I = x_0 y_0$ 。但是， f 和 g 并不是坚持不变的：它们随着外部预言机价格的变化而变化（不变量 I 也是如此，所以它只是在预言机价格 p_0 不变时的不变量）。在给定的 p_0 下， f 和 g 在整个波段内是不变的。如前所述，我们把 p_{\uparrow} 表示为波段的顶部价格， p_{\downarrow} 表示为波段的底部价格。我们对 A （权衡活动性集合度的手段）的定义是这样的：

The property we are looking for is such that higher price p_0 should lead to even higher price at the same balances, so that the current market price (which will, on average, follow p_0) is lower than that, and the band will trade towards being all in ETH (and the opposite is also true for the other direction). It is possible to find many ways to satisfy that but we need one:

我们正在寻觅的属性是这样的：更高的价格 p_0 应当招致在相同的余额下更高的价格，因此，以后的市场价格（平均来说，将跟随 p_0 ）低于这个价格，并且波段将朝着局部为ETH的方向买卖（而另一个方向也是如此）。能够找到很多方法来满意，但我们需求这样一个：

where y_0 is a p_0 -dependent measure of deposits in the current band, denominated in ETH, defined in such a way that when current price p , p_{\uparrow} and p_0 are equal to each other, then $y = y_0$ and $x = 0$ (see the point at $p_0 = p_{\uparrow}$ on Fig. 4). Then if we substitute y at that moment:

其中 y_0 是一个与 p_0 相关的权衡以后波段放款的手段，以ETH为单位，其定义是：当以后价格 p 、 p_{\uparrow} 和 p_0 相互相等时，则 $y = y_0$ ， $x = 0$ （见图4上 $p_0 = p_{\uparrow}$ 的点）。那么，假设我们把那一刻的 y 交流掉：

Price is equal to dx_0 / dy_0 which then for a constant-product invariant is:

价格等于 dx_0 / dy_0 ，那么关于一个恒定的产品不变量来说，就是：

One can substitute situations where $p_0 = p^\uparrow$ or $p_0 = p^\downarrow$ with $x=0$ or $y=0$ correspondingly to verify that the above formulas are self-consistent.

我们能够用 $x=0$ 或 $y=0$ 来替代 $p_0 = p^\uparrow$ 或 $p_0 = p^\downarrow$ 的状况，以考证上述公式是自洽的。

Typically for a band, we know p^\uparrow and, hence, p^\downarrow , p_0 , constant A , and also x and y (current deposits in the band). To calculate everything, we need to find y_0 . It can be found by solving the quadratic equation for the invariant:

一般关于一个波段，我们知道 p^\uparrow ，因此也知道 p^\downarrow 、 p_0 、常数 A ，还有 x 和 y （波段中的当前放款）。为了计算剩下的一切，我们需求找到 y_0 。它可以经过处置不变量的二次方程来找到：

which turns into the quadratic equation against y_0 :

这就变成了针对 y_0 的二次方程：

In the smart contract, we solve this quadratic equation in `get_y0` function.

在智能合约中，我们在`get_y0`函数中处置这个二次方程。

While oracle price p_0 stays constant, the AMM works in a normal way, e.g. sells ETH when going up / buys ETH when going down. By simply substituting $x=0$ for the "current down" price p_{cd} or $y=0$ for the "current up" price p_{cu} values into the equation of the invariant respectively, it is possible to show that AMM prices at the current value of p_0 and the current value of p^\uparrow are:

在预言机价格 p_0 坚持不变的状况下，AMM以一般的方式义务，例如，下跌时卖出ETH/下跌时买入ETH。经过冗杂地将 $x=0$ 交流为"当前下跌"的价格 p_{cd} 或 $y=0$ 交流为"当前下跌"的价格 p_{cu} 值区分代入不变量方程，就可以说明在 p_0 的当前值和 p^\uparrow 的当前值下的AMM价格是：

Another practically important question is: if price changes up or down so slowly that the oracle price p_0 is fully capable to follow it adiabatically, what amount y^\uparrow of ETH (if the price goes up) or x^\downarrow of USD (if the price goes down) will the band end up with, given current values x and y and that we

start also at $p=p_0$. While it's not an immediately trivial mathematical problem to solve, numeric computations showed a pretty simple answer:

另一个主要的实际效果是：假设价格的变化如此缓慢，致使于预言机价格 p_0 完好能够“绝热地”（在一个波段内）跟随它，那么在给定当前值 x 和 y ，并且我们也从 $p=p_0$ 末尾的状况下，这个波段最终会取得 $y\uparrow$ 的ETH（假设价格下跌）或 $x\downarrow$ 的USD（假如价格下跌）。固然这不是一个立刻可以处置的数学效果，但数字计算显现了一个相当冗杂的答案：

We will use these results when evaluating safety of the loan as well as the potential losses of the AMM.

在评价借贷的性以及AMM的潜在丧失时，我们将运用这些结果。

Now we have a description of one band. We split all the price space into bands which touch each other with prices $p\downarrow$ and $p\uparrow$ so that if we set a base price p_{base} and have a band number n :

往常我们有了对一个波段的描绘。我们把一切的价格空间分红若干波段，这些波段的价格 $p\downarrow$ 和 $p\uparrow$ 相互接触，因此，如果我们设定一个基础价格 p_{base} ，并有一个波段号 n ：

It is possible to prove that the solution of Eq. 7 and Eq. 5 for any band gives:

关于任何一个波段，可以证明公式7和公式5的解都可以失掉：

which shows that there are no gaps between the bands.

这标明波段之间没有空隙。

Trades occur while preserving the invariant from Eq. 1, however the current price inside the AMM shifts when the price p_0 : it goes up when p_0 goes down and vice versa cubically, as can be seen from Eq. 8.

买卖发生的同时保管了公式1的不变性，但是，当价格为 p_0 时，AMM外部的当前价格会发生变化：当 p_0 下降时，它就会下降，反之亦然（立方系数），从公式8可以看出。

LLAMMA vs Stablecoin

Stablecoin is a CDP where one borrows stablecoin against a volatile collateral (cryptocurrency, for example, against ETH). The collateral is loaded into LLAMMA in such a price range (such bands) that if price of collateral goes down relatively slowly, the ETH gets converted into enough stablecoin to cover closing the CDP (which can happen via a self-liquidation, or via an external liquidation if the coverage is too close to dangerous limits, or not close at all while waiting for the price bounce).

稳定币是一种CDP，人们以不稳定的抵押品（加密货币，例如ETH）来借入稳定币。抵押品被加载到LLAMMA的价格范围内（这样的波段），如果抵押品的价格下降相对缓慢，ETH被转换成足够的稳定币来掩盖封锁CDP（这可以经过自我清算发生，大约经过外部清算，如果抵押率太接近风险的限制，大约基本不封锁，同时等候价格反弹）。

When a user deposits collateral and borrows a stablecoin, the LLAMMA smart contract calculates the bands where to locate the collateral. When the price of the collateral changes, it starts getting converted to the stablecoin. When the system is "underwater", user already has enough USD to cover the loan. The amount of stablecoins which can be obtained can be calculated using a public `get_x_down` method. If it gives values too close to the liquidation thresholds – an external liquidator can be involved (typically shouldn't happen within a few days or even weeks after the collateral price went down and sideways, or even will not happen ever if collateral price never goes up or goes back up relatively quickly). A health method returns a ratio of `get_x_down` to debt plus the value increase in collateral when the price is well above "liquidation".

当用户取出抵押品并借入一个稳定币时，LLAMMA智能合约会计算出抵押品所在的波段。当抵押品的价格变化时，它末尾被转换为稳定币。当系统处于"水下"时，用户曾经有足够的USD来支付放款。可以取得的稳定币数量可以通过一个公共的`get_x_down`方法来计算。如果它给出的数值过于接近清算阈值—外部清算人可以参与进来（一般不应当在抵押品价格下跌和横盘后的几天甚至几周内发生，甚至如果抵押品价格从未下跌或相对较快公开降，则永世不会发生）。当价格远高于"清算"时，一个安康的方法会前往`get_x_down`与债务的比率，再加上抵押品的价值增加。

When a stablecoin charges interest, this should be reflected in the AMM,

too. This is done by adjusting all the grid of prices. So, when a stablecoin charges interest rate r , all the grid of prices in the AMM shifts upwards with the same rate r which is done via a `base_price` multiplier. So, the multiplier goes up over time as long as the charged rate is positive.

当一个稳定币收取利息时，这应当反映在AMM中。也要反映进去。这是通过调整价格的一切网格来完成的。因此，当一个稳定币收取利率 r 时，AMM中的一切价格格都会向上移动，与相同的利率 r ，这是通过一个基础价格乘数完成的。所以，只需收取的利率是正的，乘数会随着时间的推移而下降。

When we calculate `get_x_down` or `get_y_up`, we are first looking for the amounts of stablecoin and collateral $x?$ and $y?$ if current price moves to the current price p_0 . Then we look at how much stablecoin or collateral we get if p_0 adiabatically changes to either the lowest price of the lowest band, or the highest price of the highest band respectively. This way, we can get a measure of how much stablecoin we will which is not dependent on the current instantaneous price, which is important for sandwich attack resistance.

当我们计算`get_x_down`或`get_y_up`时，我们首先要找的是如果当前价格移动到当前价格 p_0 的稳定币和抵押品 $x?$ 和 $y?$ 的数量。然后我们看一下，如果 p_0 绝热地变化到最低区间的最廉价格，或最高区间的最廉价格，我们区分失掉几稳定币或抵押品。这样，我们就可以失掉一个权衡我们将获得几稳定币的规范，它不依赖于当前的瞬时价格，这对夹层攻击的阻力很主要。****

It is important to point out that the LLAMMA uses p_0 defined as ETH/USD price as a price source, and our stablecoin could be traded under the peg (p_s

1). If p_s

p_0 .

需求指出的是，LLAMMA运用定义为ETH/USD价格的 p_0 作为价格根源，我们的稳定币可以在挂钩之下 (p_s1) 停止买卖。如果 $p_s p_0$ 。

In adiabatic approximation, $p = p_0 / p_s$, and all the collateral

stablecoin conversion would happen at a higher oracle price / as if oracle price was lower and equal to:

在绝热近似中， $p = p_o / p_s$ ，一切抵押品

稳定币的转换将发生在较高的预言机价格上/就像预言机价格较低且等于：

At this price, the amount of stablecoins obtained at conversion is higher by factor of $1/p_s$ (if p_s

在这个价格下，转换时取得的稳定币的数量要高出 $1/p_s$ 的系数（如果 p_s

It is less desirable to have $p_s >$

1 for prolonged times, and for that we will use the stabilizer (see next)

在长时间内， $p_s >$

1是不太梦想的，为此我们将使用稳定器（见下一章节）。

Automatic Stabilizer and Monetary Policy

自动稳定器和货币政策

When $p_s >$

1 (for example, because of the increased demand for stablecoin), there is peg-keeping reserve formed by an asymmetric deposit into a stableswap Curve pool between the stablecoin and a redeemable reference coin or LP token. Once $p_s >$

1, the PegKeeper contract is allowed to mint uncollateralized stablecoin and (only!) deposit it to the stableswap pool single-sided in such a way that the final price after this is still no less than 1. When p_s

当 $p_s >$

1时（例如，由于对稳定币的需求增加），就会有锚定的贮藏，由稳定币和可赎回的参考币或LP代币之间的不对称放款到stableswap Curve池形成。一旦 $p_s >$

1, PegKeeper合约被允许铸造无抵押的稳定币, 并且只将其单边取出stableswap池, 这样做之后的最终价格依然不低于1。当 p_s

These actions cause price p_s to quickly depreciate when it's higher than 1 and appreciate if lower than 1 because asymmetric deposits and withdrawals change the price. Even though the mint is uncollateralized, the stablecoin appears to be implicitly collateralized by liquidity in the stablecoin pool. The whole mint/burn cycle appears, at the end, to be profitable while providing stability.

这些行为招致价格 p_s 高于1时快速升值, 低于1时升值, 由于不对称的存款和提款改动了价格。即使这局部“铸币”是没有抵押的, 但稳定币似乎是由稳定币池中的活动性隐性抵押支持的。整个铸币/熄灭周期在最后似乎是有益可图的, 同时提供了稳定性。

Let's denote the amount of stablecoin minted to the stabilizer (debt) as dst and the function which calculates necessary amount of redeemable USD to buy the stablecoin in a stableswap AMM get_dx as $fdx()$. Then, in order to keep reserves not very large, we use the "slow" mechanism of stabilization via varying the borrow r :

让我们把铸造给稳定器(债务)的稳定币数量表示为 dst , 把计算在stableswap AMM get_dx 中置办稳定币所需的可赎回USD数量的函数表示为 $fdx()$ 。然后, 为了保持“贮藏”不是十分大, 我们通过改动借款 r 来使用“缓慢”的稳定机制。

where h is the change in p_s at which the rate r changes by factor of 2 (higher p_s leads to lower r). The amount of stabilizer debt dst will equilibrate at different value depending on the rate at $p_s=1$ r_0 . Therefore, we can (instead of setting manually) be reducing r_0 while $dst/supply$ is larger than some target number (for example, 5%) (thereby incentivizing borrowers to borrow-and-dump the stablecoin, decreasing its price and forcing the system to burn the dst) or increasing if it's lower (thereby incentivizing borrowers to return loans and pushing p_s up, forcing the system to increase the debt dst and the stabilizer deposits).

其中 h 是 p_s 的变化, 速率 r 的变化为2倍(p_s 越高, r 越低)。稳定器债务 dst 的数量将依据 $p_s=1$ r_0 的速率在不同的值上平衡。因此, 我们可以(而不是手动设置)在 $dst/supply$ 大于某个目的数字(例如5%)时添加 r_0 (从而鼓舞借款人借入并抛出稳定币, 降低其价格并唆使系统熄灭 dst), 大概在它较低时增加(从而鼓舞借款人

归还存款并促进ps下降，唆使系统增加债权dst和稳定器存款)。

Conclusion / 总结

The presented mechanisms can, hopefully, solve the riskiness of liquidations for stablecoin-making and borrowing purposes. In addition, stabilizer and automatic monetary policy mechanisms can help with peg-keeping without the need of keeping overly big PSMs.

希冀所提出的机制能够处置为制造稳定币和借贷手腕而停止清算的风险性。此外，稳定器和自动货币政策机制可以辅佐保持价格锚定，而不需求保持过大的PSM (Peg Stability Module 锚定稳定性模块)。