Curve stablecoin design

Michael Egorov, Curve Finance

May 15, 2022

Overview

The design of the stablecoin has few concepts: lending-liquidating amm algorithm (LLAMMA), PegKeeper, Monetary Policy are the most important ones. But the main idea is in LLAMMA: replacing liquidations with a special-purpose AMM.

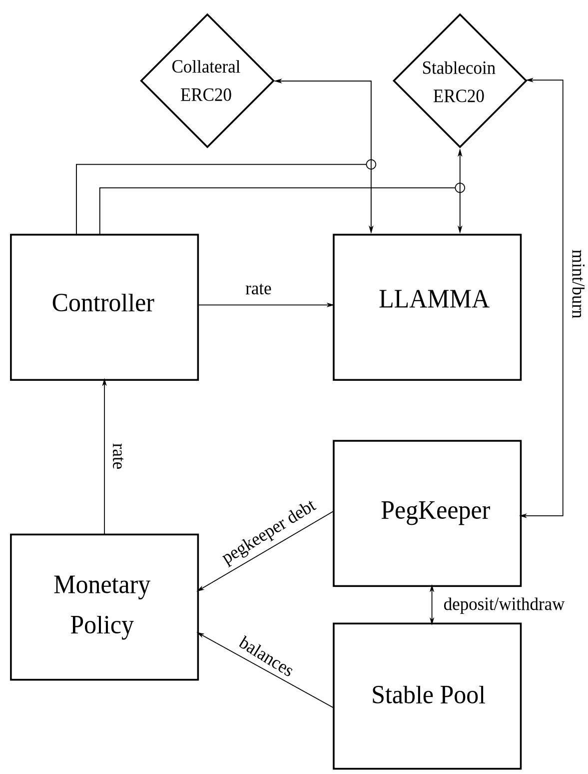

Figure 1: Overall schematic

AMM for continuous liquidation/deliquidation (LLAMMA)

The core idea of the stablecoin design is Lenging-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.

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

This is only possible with an external price oracle. In a nutshell, if one makes an typical AMM (for example with a bonding curve being a piece of hyperbola) and ramps its "center price" from up to down, the tokens will adiabatically convert from one to another while proving liquidity in both ways on the way. It is somewhat similar to avoided crossing in quantum physics (though only as an idea: mathematical description of the process could be very different).

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:

$$I = (x + f)(y + g). \tag{1}$$

We also can denote $x' \equiv x + f$ and $y' \equiv y + g$ so that the invariant can be written as a familiar $I = x'y'$.

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_o is unchanged). At a given p_o, f and g are constant across the band. Let's denote $p_\uparrow$ as the top price of the band and $p_\downarrow$as the bottom price of the band. We define A in such a way that:

$$\frac{p_\downarrow}{p_\uparrow} = \frac{A-1}{A}. \tag{2}$$

The property we are looking for is such that higher price $p_o$should lead to even higher price at the same balances, so that the current market price (which will converge to p_o) is lower than that, and the band will trade towards being all in USD (and the opposite is also true for the other direction). As an example, this property is satisfied when:

$$f=\frac{p_o^2}{p_\uparrow}Ay_0, \qquad g=\frac{p_\uparrow}{p_o}\left(A-1\right)y_0, \tag{3}$$

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_o are equal to each other, then $y=y_0$ and (by definition of $p_\uparrow$) $x=0$. Then if we substitute y at that moment:

$$I=p_oA^2y_0^2. \tag{4}$$

Price is equal to dx'/dy' which then for a constant-product invariant is:

$$p=\frac{dx'}{dy'}=\frac{x'}{y'}=\frac{f+x}{g+y}. \tag{5}$$

One can substitute situations where $p_o=p_\uparrow$ or $p_o=p_\downarrow$ with $x=0$ or $y=0$ correspndingly to verify that the above formulas are self-consistent.

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

$$\left(\frac{p_o^2}{p_\uparrow}Ay_0+x\right)\left(\frac{p_\uparrow}{p_o}\left(A-1\right)y_0+y\right)=p_oA^2y_0^2, \tag{6}$$

which turns into the quadratic equation against y_o:

$$p_oAy_0^2-y_0\left(\frac{p_\uparrow}{p_o}\left(A-1\right)x+\frac{p_o^2}{p_\uparrow}Ay\right)-xy=0. \tag{7}$$

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

While oracle price p_o stays constant, the AMM works in a normal way, e.g. low ETH on the top / low USD on the bottom. 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_o and the current value of $p_\uparrow$ are:

$$p_{cd}=\frac{p_o^3}{p_\uparrow^2}, \qquad p_{cu}=\frac{p_o^3}{p_\downarrow^2}. \tag{8}$$

Another practically important question is: if price changes up or down so slowly that the oracle price p_o 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 $p=p_o$. While it's not an immediately trivial mathematical problem to solve, numeric computations showed a pretty simple answer:

$$y_\uparrow=y+\frac{x}{\sqrt{p_\uparrow p}}, \tag{9}$$

$$x_\downarrow=x+y\sqrt{p_\downarrow p}. \tag{10}$$

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

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:

$$p_{\uparrow}(n) = \left(\frac{A-1}{A}\right)^{n} p_{base}, \qquad p_{\downarrow}(n) = \left(\frac{A-1}{A}\right)^{n+1} p_{base}. \tag{11}$$

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

$$p\left(x=0, y>0, n\right) = p_{cd}\left(n\right) = p_{cu}\left(n-1\right), \tag{12}$$

$$p\left(x>0, y=0, n\right) = p_{cu}\left(n\right) = p_{cd}\left(n+1\right), \tag{13}$$

which shows that there are no gaps between the bands.

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

Automatic Stabilizer

Automatic Monetary Policy