

TL;DR

Introducing the Correlated-asset price oracle, an adapter smart contract introducing extra upper price protections for assets highly correlated with an underlying, like LSTs (Liquid Staking Tokens) or stablecoins.

Context

On the Aave protocol, the pricing of assets is done in different ways: some feeds are coming directly from the Chainlink network and its algorithms, others combine multiple Chainlink feeds into one, and a last type combines some Chainlink and/or on-chain data to get a final price.

The most representative case of the last group of feeds using on-chain data is the price oracles for LSTs listed in Aave, like wstETH, stMATIC, or sAVAX. In these cases, the method of calculation is usually considering the price of the underlying, and multiplying by some type of exchange rate between the LST and the underlying. For example, for wstETH, the price is high-level calculated as the price of ETH in USD * exchange rate between stETH and ETH

(assuming a 1:1 peg between ETH and stETH).

This approach for pricing is sound, as it reduces important price manipulation risks. However, there have been different discussions in the community surrounding the topic, and there is even the Killswitch project being developed in order to apply protective measures whenever the price of an LST based on the exchange rate deviates too much from a secondary market.

However, there is another protection that could be applied based on a clear principle: for certain type of assets, the price should never be above a certain threshold that can be defined with pretty high certainty in advance.

Correlated-asset price oracle

Let's take wstETH as a high-level (not considering aspects like compounding) illustrative example to explain the new mechanism.

For the last 1-2 years, the yearly growth of wstETH's exchange rate has fluctuated in the range of 3-5%. What that means is that at any point of time during that period, if you supplied 1 ETH into wstETH, after 1 year you would have between 3-5% on top of the 1 ETH.

Consequently, we can say that the price of wstETH has increased at an average rate of 3-5% yearly.

So the follow-up question is, can we say that the price of wstETH has a maximum increase over a period X of time? The answer is, kind of.

The Aave protocol prices its assets in USD, so for example it expects the price of wstETH in USD for its internal calculation. It is not totally straightforward to set an upper limit for that price, as wstETH (and ETH) is a volatile asset that could increase (and decrease) radically in price in a short period of time. However, we can set an upper limit on how much the correlation with the underlying can probabilistically change over X period of time. Naively, we could say that in the previous example, a number close to 5% is a good reference for the maximum growth of wstETH in ETH terms.

Our Correlated-asset price oracle solution is based on the previous idea and works the following way:

- For each eligible asset we will apply a custom price adapter (Correlated-asset price oracle).
- Each custom adapter will have the following configurable parameters in relation with the new functionality:
- A ratio provider smart contract

, to read the current exchange rate or any other correlation ratio between the asset priced and a reference. For example, the stETH contract itself in the case of wstETH, and its function `getPooledEthByShares()`

.

- A `ratioReference`

, which is the value of the ratio used as reference to calculate the growth from. For example, a valid value could be the exchange rate of wstETH/stETH two weeks prior, or a fixed value in the case of an stable-coin pegged to the USD.

- A `ratioReferenceTime`

, which is the timestamp of when the `ratioReference`

was set, to be used to calculate the growth from then.

- A maxYearlyRatioGrowthPercent

, to be defined as the maximum yearly percentage growth to be accepted as “correct” by the system. For example, a value of 6% for wstETH.

- A ratio provider smart contract

, to read the current exchange rate or any other correlation ratio between the asset priced and a reference. For example, the stETH contract itself in the case of wstETH, and its function getPooledEthByShares()

.

- A ratioReference

, which is the value of the ratio used as reference to calculate the growth from. For example, a valid value could be the exchange rate of wstETH/stETH two weeks prior, or a fixed value in the case of an stable-coin pegged to the USD.

- A ratioReferenceTime

, which is the timestamp of when the ratioReference

was set, to be used to calculate the growth from then.

- A maxYearlyRatioGrowthPercent

, to be defined as the maximum yearly percentage growth to be accepted as “correct” by the system. For example, a value of 6% for wstETH.

- By using the previous parameters, on each price query, the adapter will do the following calculation:
- First, it will calculate an upper ratio limit at the maximum growth expected, normalised to the time passed.
- Fetch the current ratio for the ratio provider smart contract, e.g. the current wstETH/stETH exchange rate.
- With all the data available, two options:
- If the current ratio is above the max ratio calculated, the price returned will be based on the max ratio, ignoring the current.
- If the current ratio is below the max ratio, the price returned will be based on the current ratio.
- If the current ratio is above the max ratio calculated, the price returned will be based on the max ratio, ignoring the current.
- If the current ratio is below the max ratio, the price returned will be based on the current ratio.
- First, it will calculate an upper ratio limit at the maximum growth expected, normalised to the time passed.
- Fetch the current ratio for the ratio provider smart contract, e.g. the current wstETH/stETH exchange rate.
- With all the data available, two options:
- If the current ratio is above the max ratio calculated, the price returned will be based on the max ratio, ignoring the current.
- If the current ratio is below the max ratio, the price returned will be based on the current ratio.
- If the current ratio is above the max ratio calculated, the price returned will be based on the max ratio, ignoring the current.
- If the current ratio is below the max ratio, the price returned will be based on the current ratio.

The high-level implications of this mechanism are the following:

- If the price of a correlated asset is above a pre-calculated maximum proportion with the reference, the system will circuit-break and return the price based on the maximum growth allowed.
- This protects against any kind of unexpected inflation of the asset.
- To not cause false positives mispricing down the asset, the system should be maintained in the following way:
- The maxYearlyRatioGrowthPercent

should be set with a certain margin based on the volatility of the growth rate of the correlated asset. This is perfectly fine, because the Aave protocol has extra protections with its risk parameters configuration.

In the previous example of wstETH, if the historic fluctuation of growth is on the range 3-5%, it is recommended to set a value in the order of 6-8%.

- Periodically, the ratioReference

should be updated. The rationale of this is that growth rate naturally changes over time, and there can be periods where maybe the rate is 5%, and next one is 3%.

The update frequency should be defined based on historic data and coordinated with the risk providers of the community, but with the type of quality assets listed on Aave, monthly or bi-monthly updates should be enough.

- The maxYearlyRatioGrowthPercent

should be set with a certain margin based on the volatility of the growth rate of the correlated asset. This is perfectly fine, because the Aave protocol has extra protections with its risk parameters configuration.

In the previous example of wstETH, if the historic fluctuation of growth is on the range 3-5%, it is recommended to set a value in the order of 6-8%.

- Periodically, the ratioReference

should be updated. The rationale of this is that growth rate naturally changes over time, and there can be periods where maybe the rate is 5%, and next one is 3%.

The update frequency should be defined based on historic data and coordinated with the risk providers of the community, but with the type of quality assets listed on Aave, monthly or bi-monthly updates should be enough.

- This is a biased mechanism: for certain assets, we consider there can't be any rational reason for their price to increase radically in comparison with a reference. Therefore, we think it is legitimate for the Aave protocol to consider that anomaly as an event to simply ignore.
- This system should be complemented with others being worked on, like Killswitch, as whenever the custom adapter will be returning the max accepted price instead of using the current ratio, extra actions could be applied risk-wise in the system (e.g. freezing, LTV 0, etc).
- Changes on the configurable parameters of the system post-deployment (ratioReference, ratioTimestamp and maxYearlyRatioGrowthPercent mainly) are to be done via governance to start with, as for having non-governance parties, extra validations would need to be evaluated and introduced, which we think can be done later.
- To start with, our intention is to apply this solution to all assets with a clear reference, so mainly all stable-coins and LSTs listed on all Aave instances.

Next steps

We welcome the feedback from the community on the new proposed system, and after some discussion, we will proceed with an ARFC Snapshot.

If that Snapshot is positive, after the security procedures are finished, we will proceed with the activation of the Correlated-asset price oracle on all the applicable assets.

Props to [0xaddi](#) for our discussions on the topic and highlighting the importance of extra protections on some assets to apply this solution on.