TLDR

Back a stablecoin with a basket of diverse, non-correlating assets. This creates organic stability with no peg that gets more stable over time. So then you have to find a way to intrinsically set the weights of the assets such that non-correlating ones are favoured. Such a method is described here.

Or by process of elimination:

- Algo stables don't work.
- Under-collateralised produces bank-run risk.
- Over-collateralised works but does not scale. See: Maker Dai: Stable, but not scalable - Uncommon Core by Su Zhu and Hasu
- Tying stability specifically to USD does not work because it requires external oracles with unknown sustainable security and relies on centralised market venues.

Therefore we want:

- 100% collateralised.
- No pegging to a specific external asset and instead aim for organic stability.

Preamble

Two key ideas/insights:

- Stability is not unique to fiat USD or specific indexes. Stability is a relative measure which can be found without reference to fiat currencies. It is in fact created through reference to many individually volatile assets.
- Closed cycle arbitrage is necessary to scale a stablecoin while keeping it stable.

Unique selling points

- Crypto native stability without reference to any oracles or external data i.e. create a basket of many different tokens and incentivise deposits of tokens that do not correlate with the others.
- Minimal governance: only necessary to curate a whitelist of non-corrupted

collateral assets.

- Grows stronger from negative sentiment - each deposit is a short position against it.
- 100% collateralised means perfect hedge for depositors with no liquidation risk (only smart contract bug risk).
- Closed cycle arbitrage: it can scale.

Basic idea:

- The sToken supply represents shares of a basket of assets (i.e. 'fully backed').
- The shares of the basket can be represented as LP shares of a Balancer pool but importantly, you cannot trade on this pool, it is not

an AMM.

- Depositors receive an equal value of sToken based on the asset amount they deposit (100% collateralisation) similar to a single-asset

LP deposit on a Balancer pool.

- The pool has no asset-to-asset trades as would be the case on an AMM - you simply deposit and withdraw. Therefore, depositors can always withdraw at the same price they deposited

.

- Depositors set a maturity for their deposit by which time they must return their sToken or else their collateral is auctioned (liquidated).
- Therefore, collateral is only liquidated based on expiry, never based on market price

.

- All depositors are charged a fee to cover the cost of abandoned collateral.
- Portfolio weight of each asset-type is determined by the average maturity for the deposits for each asset-type.
- Deposit price for each asset is always arbed back to the market price by other deposits/withdrawals.
- Therefore, a natural distinction is made between short maturity deposits - some of which are pure arbitrage - and long maturity. It is the amount of long maturity which determines the weight for each asset-type.
- Depositors have a natural incentive to deposit assets which they are long - this results in a basket of non-corelating, competing assets.
- As more and more assets are added stability increases over time.
- Since each deposit is effectively shorting the sToken in favour of the collateral deposited, the sToken's success is based upon those who can see how it might fail - natural anti-fragility.
- Only depositors can later withdraw their collateral.

How it works

Some theory

The generalised AMM equation from Balancer represents a surface of constant value as (as described in the balancer whitepaper) (assuming arbitrage forcing the spot price back to the market price):

$V = \prod_t B_t^{W_t}$

Furthermore, the asset weights, W_t

correspond to the relative value of each asset. The deposit equation therefore yields an equal value of shares of the pool:

$P_{issued} = P_{supply} \cdot ((1+\frac{A_t}{B_t})^{W_t}-1)$

Therefore, we can simply change the pool weights (to change the relative portfolio value) based on the respective volume of deposits for each asset.

Note 1: even though asset-to-asset trades are disallowed, arbitrage can still take place through deposits and withdrawals.

Note 2: this is effectively forming an intrinsic

multi-asset oracle where any minipulation is a natural cost to the manipulator and natural gain to the next trader (same as in any AMM).

Differentiating weight change from price change

Arbitrage deposits can be differentiated from deposits where the depositor is long the asset in question by the length of maturity chosen (since maturity serves no purpose for someone simply trying the arbitrage the pool).

Therefore, we define the weight of each asset-type by $\sum m d$

where m

and d

are maturity and debt, respectively, for each deposit.

Defaults

Defaults or abandoned collateral will be common since the depositor has the option to simply keep the sToken amount rather than withdrawing their collateral. Since this will occur when the collateral is worth less than the debt, it represents a loss for the protocol. Therefore, deposit fees are charged based on the average loss. Since losses will depend on maturity,

fees are calculated based on maturity tranches.

If in the case of large loss in which average fees take a long time to recoup the surplus sToken, this would be soaked up by future collateral auctions.

Corrupt asset attack

If an asset is whitelisted where a central party can mint arbitrarily they can make arbitrarily large deposits to then mint arbitrary amounts of sToken. This attack is defended against by limiting the rate of debt-share increase for each individual asset-type. E.g. each asset could be limited to increasing its share of debt by 50% per day. This gives some time for governance to then remove the asset from the whitelist.

It is also worth bearing in mind in such a scenario the market would reduce the price of the asset before such an attack based on any public information.

Also, note that this attack poses no risk to deposit holders only sToken holders.

Arbitrage price

Unlike projects based on over-collateralised, the cRatio is 100% for this design. Importantly, this means arbitrageurs can engage in closed cycle arbitrage allowing them to profitably repeat many cycles of arbitrage. Therefore, the sToken price on secondary markets should tend towards the value of the assets backing it.

Two scenarios

- In the best case, the sToken will become stable and also enable a highly efficient lending/options market.
- In the worst case, the sToken will not be stable but would be one of the best low-risk, high-return, crypto indexes since its backed by assets others are long.

Minimal governance

GOV token Purposes:

- Main voting responsibility is to remove or add asset types from/to the whitelist.
- Optional (supply inflation based) funding proposals are also possible.

The minimal responsibility for voters means easier participation and smaller attack surface.

An additional deposit fee can be charged to depositors as a cashflow to depositors.

Note: governance does not choose assets on the basis of stability - that happens naturally via depositors. It is only necessary to choose assets that are not corrupted i.e. corruption here means central party/admin arbitrarily minting and depositing it into the asset pool.

Simple token voting is suggested here but it may be possible to use more secure governance methods in the future. E.g. Soul bound token affiliations etc.

Collaboration

Whitepaper and smart contracts have further technical details for those interested.

Seeking any feedback and potential collaborators.

Whitepaper: https://github.com/Cauldron-Labs/v1-docs/blob/main/cauldronWhitepaper.pdf

Smart contract PoC: [Revealed soon]