Intent

I am proposing a series of changes to SigmaUSD.

For the sake of charity, this is a Hackathon project that is being done for fun, on my own personal time, and does not reflect the position or opinion of the Ergo Foundation.

Why Protocol Owned Equity

Stablecoins operate on decentralized systems and are not backed by a central authority, such as a central bank.

(Unless you are going to steady the lads and deploy liquidity)

One of the consequences of this is that there is no lender of last resort for these systems. In traditional financial systems, a lender of last resort is an entity that provides liquidity to the market in times of stress, such as a financial crisis, in order to stabilize the system.

The absence of a lender of last resort in the cryptocurrency space can lead to market instability and increase the risk of systemic failures.

To mitigate these risks and stabilize the system, some have proposed the idea of internalizing equity and creating a new type of lender of last resort.

In the context of SigmaUSD the central bank proposed would act as a “RESERVE OF LAST RESORT” which means that the risk of the ReserveCoin investment is partially absorbed by the protocol rather than the investor.

This could be achieved by introducing fees or taxes on transactions in the system. The revenue generated from these fees or taxes could be used to provide a backstop for the market, slowly converting the Net Reserve Risk to inside the protocol itself.

Protocol-owned equity can help to reduce the risk of investing in the currency, making it more accessible and appealing to retail investors. As such less risk and dilution are being passed on to other parties (SigRSV Holders). The “RESERVE OF LAST RESORT” would be accumulated via fees.

Users can see this as a weak type of protocol insurance that strengthens as the RoLR builds over time.

Stability vs Capital Efficiency

Stablecoins operate on decentralized systems and are not backed by a central authority, such as a central bank.

What this mean in practice is that the underlying stability mechanisms of stablecoins need to be the primary focus?

This is not the traditional system where you can build net leverage, systemic risk, get rekt, and look for a savior. That is the path the pursuit of hyper capital efficiency trends towards.

Ideally in a system with no Lender of Last Resort to step in a try to deleverage or bail out the system, the underlying hardness of the Reserve/Stability mechanism is vital to long term function and health of the subsequent economy.

Capital efficiency and leverage can and ideally should be built beyond the base stablecoin protocol in environments that isolate the systemic nature of leverage and default.

When the potential for leverage and systemic risk are baked into the base economic assumptions of a stablecoin, I believe that the cyclical nature of markets will inevitably build enough net risk in a system and lead to the potential for serious economic harm/failure/insolvency.

There may even be a use case for a type of small taxation of insurance in reference markets to stabilize an underlying RoLR in times of uncertainty, however, this is speculative and should ultimately be determined by Liquidity Providers who stake their livelihood on the net financial health and performance of stablecoin ecosystems.

A large part of the school of thought trained towards hyper capital efficiency is the base assumption that the system itself is backstopped. In Decentralized Finance this needs to become the first assumption as systemic risk and failure is terminal. That which depegs can often become some type of speculative zombie ecosystem, however, trust is often the hardest thing to recover beyond lost keys.

The focus of Reserve stability is a collective exercise in trust management. There is no central lender of last resort, therefore, collectively we need to manage our risk assumptions.

Primary Issues with the Current Implementation of SigmaUSD

1. SigRSV Risk Imbalance/Race Conditions

The ReserveCoin holders inherit all of the net protocol risks, while the reward mechanism is somewhat imbalanced.

A loss of trust or willingness to engage in the Reservecoin can lead to stagnation in the protocol.

Actors who mint SigUSD have a simpler set of assumptions as they are not subject to race conditions. The player vs. player assumptions of SigRSV positions is much more complex than a position in SigUSD.

Protocol Owned Equity is a potential solution to internalizing a part of this risk, which I believe will create a more balanced game, greater price stability, and make SigRSV a more attractive investment.

The goal is over time the Protocol Owned Equity acts as a Reserve of Last Resort.

2. Dilution From Draining

There has been significant dilution in the amount of SigRSV, which negatively affects the willingness of retail investors to assume risk.

At a Reserve Ration of 100% relative to the value of SigUSD this token is essentially worthless.

There is a proposal in the Djed paper for Debt to Equity Swaps. While that may appear as a potential solution to protocol-level insolvency, I believe that there are much better ways of potentially mitigating that risk that maintain trust. Personally, I think this would lead to a loss of confidence in the protocol and a reduced willingness of retail investors to interact with the ReserveCoin.

We are already seeing some negative sentiment around SigRSV. The greater value of over-collateralization is trust. However, if the actors that are inheriting the risk side of the trade do not trust the position this model will fail.

3. Whale Reserve Draining Attacks

A malicious user who can foresee how the exchange rate will evolve, perhaps because of an excessive oracle delay or active price manipulation, can perform sequences of actions that will drain the bank's reserves.

There is currently no mechanism to prevent whale abuse. Defi is ultimately a PVP game. However, when I protocol does not have restrictions in minting PVP transforms to player vs. protocol.

The Reserve Draining attacks are feasible for a very small subset of users. This gives this subset of users the potential to have disproportionate power and the potential ability to manipulate the protocol.

So long as this vector of attack is open, there is an open question of trust. The long-term viability of SigRSV is questionable, and the protocol itself is potentially at risk.

The Reserve of Last Resort (ReserveCoin Protocol Owned Equity)

The shift in the design proposed is a path towards creating a protocol-owned Reserve of Last Resort (RoLR). The long term goal is to create a protocol backing that could offset and internalize as much liability in the stablecoin in the event as possible.

In a healthy market, the RoLR will accumulate continuously, collecting a portion of fees in parallel with the reserve fees. This RoLR will rebalance the initial risks SigRSV holders inherit from interacting with the protocol and acts to absorb the dilution from losing positions.

Much of this SIP proposal will be centered around shifting AgeUSD in this direction, the benefits, and potential stabilization mechanisms that can be used in an attempt to create a stablecoin with greater inherent resilience.

RoLR- An Ungoverned Stability Mechanism

There are some important key assumptions that need to be clearly communicated and designed with Protocol Owned Equity.

1. This Reserve should have no Internal Governance. This is effectively an Autonomous Reserve. Governance and investment of this reserve is subject to human risk. This should be mitigated.

2. The value of the Reserve is the stability mechanism it offers to the ecosystem. The reserve is acting as a type of collective good or fund for the overall health and well-being of the protocol.

Adding Dual Mint

Currently, there is no option for Mint SigUSD when the Reserve Ratio is beneath 400%.

Dual Minting 50% ReserveCoin and 50% SigUSD should always be an option that comes with a reduced fee.

I would propose that the dual mint fee be less than the mint fees in optimal fee conditions.

Dual Mint allows any user to quickly become an LP for the stablecoin framework at a lower cost burden. Dual Mint should not negatively impact the Reserve Ratio and should offer a small incentive for the PoE fund.

The low fee will encourage liquidity on reference markets, as slippage can be arbitraged with minimal risk. This market is both a tool for stability and market efficiency.

Reference Market Stability Fee and Expanding the Reserve Ratio

Debt to Equity Swaps leave a bad taste in my mouth. The idea of backing an insolvent asset by printing another insolvent asset is the type of financial yoga we should keep out of the core functionality of a stablecoin.

On top of protocol-enforced RoLR fees, it makes sense to create a small fee in reference markets that feed into the RoLR. This can be viewed as similar to a type of protocol insurance mechanism to underwrite the stability of the protocol in the event of failure.

The benefit of this mechanism in the model I am proposing is that activity in the reference market continually expands the reserve, which in turn expands the potential amount of stablecoins that can be minted.

Currently, the AgeUSD framework has a Reserve Ratio. The updated framework will require a secondary RoLR Ratio.

This is the % of the overall Reserve Ratio that is held by the protocol. Upon update, this RoLR Ratio will be an indicator of risk assumed by the protocol.

The RoLR will not be able to sell SigRSV rather it will use fees, protocol enforced, and perhaps reference market enforced to accumulate SigRSV.

Over time the equity of the protocol will become a dominant reserve shareholder in SigRSV.

New Proposed Reserve Range and Fee Distribution

In the new model, I propose we expand the Reserve Range (Currently 400%-800%) to 400%-1600%

Rather than a flat fee across the Reserve Range, I propose a 3-tiered fee mechanism, plus the dual mint option.

Tier 1
RR 400-799%

T1 Fee Distribution
1.75% Reserve Fee
.5% PoE Fee
2.25% Total Mint Fee

Tier 2
RR 800-1199%

T2 Fee Distribution
.75% Reserve Fee
.25% PoE Fee
1% Total Mint Fee

Tier 3
RR 1200-1600%

T3 Fee Distribution
.25% Reserve Fee
.25% PoE Fee
0.5% Total Mint Fee

Dual Mint
RR 100-1200%

DM Fee Distribution
0% Reserve Fee
.25% PoE Fee
0.25% Total Mint Fee

Mitigating Whale Attacks

One proposed way to mitigate whale attacks is to incur a cost on moving the reserve ratio percent. This, however, may be offset by a whale interacting with the protocol from multiple wallets. Assuming a sophisticated adversary, this type of whale defense is most likely useless.

Unfortunately, it appears the more efficient and robust way to prevent Whale Draining attacks is a type of capital control regarding the new amount of SigUSD that can be minted in an oracle Epoch. This, however, should not impact the redemption of SigUSD.

The Reserve Ratio can be used as the limiting factor, an example a specific % adjustment however, this is somewhat controversial, and proposing an actual percentage is something I would need to think about. Consensus matters here and would probably be different than my rough opinion anyway.

This is a mechanism of creating protocol enforced minting limits per epoch as a means to avoid whale attacks.

One thing to remember is that as the RoLR grows, if successful in theory, the % adjustments may represent a more significant net value.

Some net adjustment limitations would mitigate short-term draining attacks.

Reserve Draining Higher Tiers

We have to assume that in the lower fee environment (Reserve 800+), the incentive to attempt to drain the reserve is more attractive, as the attack is lower cost.

However, with substantial reserves, limited mints per epoch, and the result of a portion of economic activity going into the RoLR. This lower fee environment may stimulate stablecoin activity and lead to a period of more rapid RoLR accumulation.

Fiat Peg Or Backing, Long Term Risk

Personally I have always believed that over the longer term the systemic risks of censorship and regulatory capture that fiat pegged stablecoins create are not worth their efficiency gains. The dollar is probably a shitcoin.

It is not a popular opinion. More can be read regarding my personal opinion here.

https://curiaregiscrypto.medium.com/sigmausd-vs-the-competition-e70b23fe37a3

Economies are complex. Beyond price correlations in assets you have social, political, environmental, micro and macro economic pressures, the market is made up of a combination of factors, each exerting either upward or downward pressure on prices. Keeping this in mind stability is a illusion.

Personally I think that the issue should be approached from the perspective of store of value vs stability.

In the short term I think that single commodity stablecoins such as gold, silver, lumber, oil, etc are a positive first step forward. While they “may” experience more volatility than fiat currencies they are less prone to censorship. Private partnerships allowing physical delivery, with the traditional framework of premiums over spot etc could potentially be built.

There has been a variety of research regarding currency/commodity baskets to offset volatility. Currencies will always pose some regulatory risk, so it may be best to avoid these long term.

What would a store of value look like, what would a basket comprise of, and how build that type of complex system long term are open questions.

Personally I support moving away from fiat pegs towards commodity peg as a move towards the creation of a more mature decentralized store of value.

Oracle Delays and Smoothing

Just as stability is an illusion I am under the belief that the concept of a “true” market price feed is an illusion. There has been some criticism that the SigUSD oracle “lies” as it does not update in real time and has a smoothing component to offset volatility and prevent whale attacks.

As a mechanism to create predictability and security, I feel this approach has been effective. The net goal is to prevent MEV that is designed to drain the protocol.

Data availability is not equal. When you have different time thresholds to receive and send data market data is somewhat subjective truth anyway.

The Delay and Smoothing in my opinion create a greater balance between sophisticated traders and individual investors. I also think having the oracle epoch delayed in alignment with the assumptions of finality in settlement (which is delayed by a few blocks) makes sense.

Defi protocols may want to keep this concept of finality in settlement in mind in Defi protocols rather than focusing on just block inclusion.

Dynamic Fees

Dynamic fees are a potential way to create economic incentives to drive markets towards equilibrium.

Dynamic fees can be programmed within a smart contract based on internal parameters. This can be used to target optimal economic outcomes based on internal framework assumptions.

Dynamic fees can also be programmed as means to try to gauge and adapt to external risk. While this solution is more mature and resembles traditional credit markets ability to dynamically adjust to risk, it cannot be done without adding points of potential manipulation and failure.

The most mature would be some combination however this currently is something I would discourage due to sophistication and security concerns.

Personally I think KISS (keep it simple stupid) is the best approach as a means to mitigate points of potential exploit and failure.

Governance

I am not a fan of governance. I would like to shift this type of protocol towards an immutable framework.

It eliminates both regulatory and human related governance risks.

Governance adds fragility especially when there is a connection to fiat liability.

Reserve of Last Resort - Re-Emission and Crypto Economic Security

A Reserve of Last Resort is a potential path towards internalizing the risk of SigRSV within the protocol.

I would propose two additional features to a Reserve of Last Resort

The first is that value not simply be burned. An outstanding question exists regarding the long term crypto economic security of blockchains.

Cryptocurrencies with a capped emission supply, it should be a goal to recycle value back to miners. This creates a type of tail emission driven by economic conditions, vs just updating the tokenomics.

I would propose the Reserve of Last Resort be structured as a type of remission contract.

Fees are paid into this contract as discussed above. (Reserve of Last Resort)

This emission contract could be initiated at a certain blockheight.

I think with the recent change in emissions it should activate when the blockrewards hit 3 ERG. (BH 1,756,800)

The emissions should be dependent on the health of the Reserve Ratio.

I would propose that the Reserve of Last Resort/Emission Contract checks and if the Reserve ratio is above 800%.

This payout should occur at the start of each oracle update. Rewards may be paid out that block or could be transferred to a smoothing contract that equalizes storage rent, and other potential subsidies across multiple blocks.

Re-Emission and Offsetting Dilution

So far we have discussed a potential way to internalize the risk of SigRSV, and a mechanism to use the Reserve of Last Resort as a way to increase the long term economic health of the protocol via miner subsidy

The second feature to explore is a mechanism to offset dilution.

Currently the only way to maintain % share of ownership is to continually buy SigRSV.

One potential way to offset dilution is to slowly redistribute SigRSV from the emission contract back to the SigRSV holders.

This is somewhat similar to the concept proposed in Djed however the conditions are reversed.

One instance of Djed proposes debt/equity swaps to try to stabilize a broken/bankrupt protocol. This would reward SigRSV holders from the Reserve of Last Resort, when the backing is in a healthy range vs use unbacked debt to subsidize a failed SigUSD position.

Another option would be to take a portion of the remission SigRSV (when the contract is 800% and burn a portion).

An open question to discuss if this is how aggressive the re emission to miners should be and how aggressive the SigRSV burn or redistribution would be.

SigmaUSD Community Ideas/Proposals/Discussions From the Community

1) oracle without delays. No smoothing.
2) faster oracle price update when large deviation.
3) transaction limits.
4) dynamic fees.
5) delayed locked settlement.
6) stability fee for holding sigusd.
7) auctions for purchases of rsv.
8) Protocol controlled equity.
9) unrestricted sale of rsv.
10) invest reserve.
11) add charts. (Up to UI provider)
12) zero governance.
13) different peg or backing. Different instantiation.
14) liquidity pools across deployments. External dependence.
15) UI improvement. Up to UI provider.

16) debt to equity swap.
17) treasury and ui fees.
18) integrations.
19) simultaneous mint/redeem.
20) non-matching lock
21) zero equity