Zephyr Protocol

The Untraceable Over-Collateralized Stablecoin

June 5, 2023

Abstract. This paper presents an exploration of the Zephyr Protocol, a privacy-oriented cryptographic coin that combines the novel algorithmic, reserve backed approach of the Djed stablecoin framework with the privacy enhancing features of Monero. Serving as an autonomous financial institution, Zephyr Protocol facilitates the buying and selling of stablecoins within a predetermined price range tied to a target price. The Zephyr Protocol relies on a reserve composed of a volatile cryptocurrency, enabling the minting and redeeming of stablecoins by users who wish to move in and out of stable value, while also storing the revenue generated from stablecoin transactions as profit for the reserve backers.

Introduction

Zephyr is a digital currency that combines the principles of privacy and stability. Grounded firmly on the proven Minimal Djed protocol, in combination with the powerful privacy preserving features of Monero, Zephyr introduces the first private, reserve backed stablecoin system. The Djed protocol, which draws inspiration from AgeUSD, is a collaborative brainchild of Emurgo, IOHK, and the Ergo Foundation and has been successfully implemented in a number of crypto projects with great success.

With Zephyr, users can mint or redeem stable (ZephUSD) and reserve (ZephRSV) coins in exchange for the base coin (ZEPH). The price for stable coins is determined by a pricing oracle and contains both a spot and moving average (MA) price. The price for reserve coins is determined using a formula based on the current reserve data.

When minting new stable/reserve coins the base coins that are exchanged (+fee) get added to the Zephyr reserve. This reserve is the collateral backing for the stablecoin holders and is ensured to be above 400% collateral at all times. In the event that collateralization falls below 400% due to price decrease, new stable coins are unable to be minted, however the reserve coin price will drop (to a min of P^{min}_{RC}) giving incentive for users to buy reserve coins at a reduced rate.

Reserve coin holders are entitled to redeem their reserve coins for the amount of equity in the reserve based on their proportion of reserve coin holdings. This means that as stable coins are minted and redeemed, the accumulated fees will build up in the reserve as profit for holders of the reserve coin. There is a maximum reserve ratio of 800% that halts the minting of new reserve coins to prevent dilution for the existing reserve coin holders.

An important part of Zephyr's design that differs from DJED, is the introduction of two reserve ratios. One for the current spot price and one for the current moving average price. This is done as DJED only uses one oracle price however Zephyr has opted to use 2 in order to eliminate any potential advantages gained via price manipulation. The details of the reserve calculations are described later in this paper.

Technical Specifications

Total Supply: 18.4 Million *(+ tail emission 0.6 ZEPH p/block)*
Block Time: 120 seconds
Assets:

- **ZEPH** (Base Currency)
- **ZephUSD** (USD Stablecoin)
- **ZephRSV** (Reserve Currency)

Mining Algorithm: RandomX proof-of-work (PoW) optimized for general-purpose CPUs to promote decentralization and egalitarian mining.
Emission Curve: Zephyr has been designed with a slightly slower emission curve compared to Monero. This design choice is aimed at rewarding early adopters by reducing their dilution over time. By slowing the initial emission, the potential inflationary impact on the price of ZEPH is lessened, benefitting the stability of the algorithmic stablecoin system.

Assets

Base coin (ZEPH)
At the core of the Zephyr Protocol lies the base currency - ZEPH. ZEPH forms the primary medium of exchange within the Zephyr ecosystem, serving as the fundamental layer linking the stablecoin (ZephUSD) and the reserve coin (ZephRSV).

ZEPH, being the native currency, has an essential role in ensuring the smooth operation of the Zephyr Protocol. Users who wish to enter the stablecoin system can do so by depositing ZEPH into the Protocol and minting ZephUSD in return. Here, the value of ZEPH serves as the underlying collateral, giving ZephUSD its stable character.

The supply of ZEPH is not affected from the minting and redeeming process of the stablecoin and reserve coin. ZEPH can only be added or removed from the reserve. The supply of ZEPH can never increase during these operations due to the reserve's function, shielding ZEPH holders from runaway inflation.

The Zephyr Protocol has been designed with a slightly slower emission curve compared to Monero. This design choice aims to reward early adopters by reducing their dilution over time. The slower initial emission mitigates the potential inflationary impact on ZEPH's price, enhancing the stability of the entire algorithmic stablecoin system. By carefully managing ZEPH's emission, Zephyr ensures the long-term sustainability and health of the ecosystem while protecting the interests of all stakeholders.

In essence, ZEPH serves as the lynchpin of the Zephyr Protocol, acting as the primary medium of exchange and the fundamental value layer.

Stable coin (ZephUSD)
Zephyr Protocol introduces ZephUSD, a truly unique stablecoin that combines the stability, efficiency, and privacy in a way not seen before in the cryptocurrency landscape. This stablecoin, while maintaining a stable value in relation to the US dollar, also inherits the powerful privacy features of Monero, making it a private stablecoin. This special characteristic sets ZephUSD apart in the crypto market by providing a level of anonymity similar to cash transactions.

This privacy-oriented stablecoin is over-collateralized by ZEPH, the base currency, and its price is determined by a pricing oracle that incorporates both spot and moving average (MA) prices. The system smoothly adjusts to market conditions, ensuring the stability of ZephUSD. Users can mint or redeem ZephUSD in exchange for ZEPH based on the oracle's current price.

Unlike traditional stablecoins that require central authorities to maintain their peg to real-world assets, ZephUSD operates in a decentralized manner, thereby eliminating the potential risks associated with centralized control. This decentralization, combined with advanced privacy features, enables users to transact freely and anonymously without the worry of volatility or surveillance.

In essence, ZephUSD is not just a stablecoin, it is a novel fusion of stability and privacy, reshaping the idea of anonymous cash transactions for the digital age. It does not aim to replace the traditional systems but strives to refine them, making them more suited for the needs of today's world. With ZephUSD, users can maintain their value stability while ensuring their transactions remain private and secure, in a system that is resistant to central control or manipulation.

Reserve coin (ZephRSV)
The Zephyr Protocol has introduced the concept of a reserve coin, termed ZephRSV. Holders of this reserve coin function as reserve providers, depositing ZEPH into the Protocol to mint ZephRSV. The pricing structure for these reserve coins relies on a formula rooted in the current state of the reserve, thereby creating a dynamic system responsive to market fluctuations.

ZephRSV holders are strategically positioned to benefit when the base coin, ZEPH, appreciates in value, offering a form of leveraged exposure to ZEPH's potential growth. This potential profit isn't just limited to ZEPH's price appreciation, but also includes the accruing of transaction fees, which add to the reserve as more ZephUSD coins are minted and redeemed. This process not only amplifies the profit potential for ZephRSV holders but also contributes to the stability of the ZephUSD, as these transaction fees increase the value of the reserve, thereby reinforcing the over-collateralization of ZephUSD.

Yet, this process doesn't carry the risk of diluting the value held by current ZephRSV holders. The Protocol maintains a maximum reserve ratio of 800%, ensuring that the minting of new

reserve coins is halted so that the value held by existing ZephRSV holders is not diluted. This mechanism underscores the balance that the Zephyr Protocol strikes between enabling growth and maintaining stability.

In addition to these benefits, ZephRSV holders have the power to redeem their coins based on their share in the reserve's equity. This gives them a significant degree of flexibility and control, reinforcing the decentralized ethos of the Zephyr Protocol.

ZephRSV presents an enticing blend of profit-making and stability-supporting features, offering its holders a distinctive position in the Zephyr Protocol. It's not just a reserve coin but an opportunity to be part of a robust and dynamic system that aims to redefine the intersection of privacy, stability, and decentralization in the cryptocurrency world.

Privacy and Anonymity

Zephyr inherits all of Monero’s robust privacy-centric features, fortifying transactional privacy and confidentiality.

- **Ring Signatures**: Ring signatures obfuscate the origin of transactions by mixing a user's account keys with public keys from the blockchain. This cryptographic methodology ensures the user's identity remains concealed, making it impossible to isolate and trace transactions back to the user.

- **Bulletproofs**: Bulletproofs are a form of non-interactive zero-knowledge proof that Monero uses to obscure transaction amounts. While protecting privacy, Bulletproofs also reduce the size of cryptographic proofs, thereby optimizing blockchain efficiency by conserving space and improving transaction speed.

In addition to these foundational privacy features, Zephyr advances this functionality by supporting multiple, private, and anonymous assets on a single chain: ZephUSD (stable coin) and ZephRSV (reserve coin).

By maintaining the integrity of the privacy and security inherent to the Monero architecture, Zephyr ensures that users of ZephUSD and ZephRSV can transact with the assurance of complete anonymity and confidentiality.

Supply Transparency

Although the amounts in transactions are hidden, we record the amount minted/redeemed/added to reserve during conversion transactions to keep a running tally for

consensus and so each block can calculate and verify all of the reserve data. Privacy is preserved even when revealing the amount in a conversion as it is not known which outputs made up the inputs for that transaction, nor is it possible to know for an outside observer which of the outputs contain the newly minted amount or the address that controls it.

Pricing Oracle

A blockchain oracle is a system that retrieves and verifies real-world data and supplies this information to the blockchain. It acts as a bridge between the deterministic world of blockchain and the non-deterministic world outside, providing the necessary data for smart contracts to execute based on real-world events and conditions.

The pricing oracle in Zephyr operates as a key component in maintaining the stability of the system. It retrieves current market data, processes it, and provides this information to the network to use in conversion transactions.

Oracle v1
In the initial version of Zephyr's oracle, when a new block is mined, the miner makes a call to the oracle to populate a pricing record. The oracle's response is signed, and this signature is verified when the mined block is added to the chain. Other nodes in the network perform this same verification, ensuring the pricing record matches as a part of network consensus. This helps maintain the integrity and accuracy of the data provided by the oracle.

Anti-Price Manipulation Measures
Price manipulation poses a significant threat to the stability of any system tied to market data. In the case of Zephyr, it is essential to counter such potential threats. Here is a manipulation scenario without any counter-measures:

1. Zeph is priced at $1.
2. An actor mints 100 stablecoins for 100 ZEPH (mint_stable).
3. The actor then dumps the price to 50 cents.
4. The spot price drops to 50 cents and is included in the next block.
5. The actor uses redeem_stable on the 100 stablecoins to get 200 ZEPH from the reserve (200 ZEPH @ 50c = $100).
6. The actor drives the price back up to $1 and repeats the process.

To prevent such manipulation, Zephyr employs a mechanism that uses the worst price between the spot and the moving average (MA) for both pricing assets and calculating the reserve state. At all times the reserve rules must be satisfied for both the spot and moving average pricing of the reserve assets.

Oracle v2 and Future Directions
While Oracle v1 offers a robust solution for price verification and network consensus, the plan is to further improve this system with Oracle v2. Potential updates may include measures to further enhance the robustness of price data verification, minimize the potential for manipulation, and improve the overall security, decentralization, and efficiency of the oracle. More research is underway to determine the best approaches and methodologies for implementing these enhancements. The precise specifications for Oracle v2 will be shared once they are finalized.

Basic Scenarios

1: When the Base Currency (ZEPH) Price Increases
Consider Alice, a user with 100 ZEPH, looking for value stability. On the other side, we have Bob, who owns 200 ZEPH and wants to increase his holdings, betting on ZEPH's future value.

Bob becomes a Reserve Provider, depositing his 200 ZEPH into the Zephyr Protocol and minting reserve coins. These coins are redeemable for underlying ZEPH reserves at any point, as long as the reserves are above the minimum reserve ratio.

Alice, seeking stability, deposits her 100 ZEPH into the Protocol and mints 100 USD stable coins. Now, the total reserve equals 300 ZEPH. Imagine four weeks pass, and the price of ZEPH increases by 10%.

Alice, excited about the recent price spike, decides to exit stability. She redeems her 100 USD stable coins and withdraws 100 USD worth of ZEPH. With ZEPH price at $1.10, her stable coins are redeemed for 90.90 ZEPH, leaving 209.1 ZEPH in the Protocol reserves.

Bob, wishing to secure his profit, redeems his reserve coins for the remaining reserves, receiving 209.1 ZEPH. Thus, Bob profits 9.1 ZEPH by providing reserves to the Protocol, while Alice, by minting her stable coins, maintains value stability.

2: When the Base Currency (ZEPH) Price Decreases
Now, let's look at the scenario where ZEPH's price drops. Assuming Alice and Bob start with the same amount of StableCoins/ReserveCoins as in the previous example, after four weeks, ZEPH's price decreases by 10%.

Alice decides to exit her StableCoins, redeeming them for 100 USD worth of ZEPH. With ZEPH price at $0.90, she receives 111.12 ZEPH for her StableCoins, leaving 188.88 ZEPH in the Protocol reserves.

Next, Bob decides to exit his ReserveCoins, receiving the remaining 188.88 ZEPH in reserves. In this situation, Bob has lost 11.12 ZEPH by providing reserves to the Protocol, while Alice, through her StableCoins, has maintained value stability in relation to USD.

In essence, the ZephRSV holders take on a leveraged position, betting on the value of ZEPH via increased adoption. This leverage is fundamental to how ZephRSV holders make a profit.

Stablecoin Solutions: A Comparative Analysis

Stablecoins are digital tokens designed to maintain a consistent value relative to an underlying asset or currency. They play a vital role in offering liquidity to cryptocurrency markets and provide a buffer against market volatility. When the stormy seas of cryptocurrency markets appear to churn, investors often seek shelter by moving their assets into stablecoins.

The Central Dilemma
Algorithmic stablecoins face a balancing act: how to best protect the base coin and the stablecoin simultaneously. These two components are equally critical, and Zephyr Protocol aims to safeguard both in the most practical manner.

The Unique Proposition of Zephyr
What distinguishes Zephyr is its protocol design, which ensures no additional ZEPH (the base coin) is ever spontaneously created, safeguarding the stability and value of the network. Instead, ZEPH's supply grows only through scheduled emission.

Zephyr Protocol
Zephyr sets a conservative minimum reserve ratio of 400%. Consequently, no stablecoin can be minted when the reserve ratio falls below this threshold. This design ensures that every ZephUSD (the stablecoin) has backing from an equivalent value of at least 400% in ZEPH. The protocol incorporates mechanisms and incentives to maintain adequate collateral supporting the circulating ZephUSD. These include transaction fees on minting and redeeming stablecoins, which contribute additional ZEPH to the reserve over time. Furthermore, the value of ZephUSD is tethered to both the spot and moving average prices of ZEPH. Any discrepancy between these prices reduces the strain on the reserve during mint and redeeming actions. In scenarios where the reserve ratio drops, users are incentivized to deposit ZEPH in exchange for ZephRSV (reserve tokens) at a discounted rate, thus bolstering the reserve. In the worst-case scenario, where reserve ratios fall below 1, the value of ZephUSD corresponds to the actual share in the reserve. Redeeming actions of ZephUSD at a reduced rate under these conditions serve to bolster the protocol reserve.as opposed to further damaging the network state.

Limitations

- **Capital Efficiency**: The mandatory 400% collateral requirement can impact capital efficiency in the model.
- **Catastrophic Events**: In extreme situations where the protocol's mechanisms and incentives are insufficient, the value of ZephUSD may be affected for users needing to redeem their tokens before additional ZEPH is added to the reserve or the value of ZEPH recovers.

- **Growth Impact**: The protocol specifies an 800% maximum reserve ratio, potentially limiting growth. This constraint, however, fosters sustainable growth by controlling the quantity of circulating ZephUSD, which overall aids in maintaining the peg.

Below we give an explanation of four notable stablecoin solutions that have entered the crypto space and against which Zephyr compares favorably in regard to economic stability and privacy.

With the exception of the Haven model, no other existing solutions currently offer a private, untraceable stablecoin.

Tether (USDT)

Tether (USDT) is one of the most well-known stablecoins, offering a 1:1 ratio with the US dollar, ostensibly maintained through reserves of real-world fiat currency. Despite its significant usage and acceptance across a variety of exchanges, Tether has faced ongoing criticism.

Pros:

- Stability: With each token supposedly backed by fiat reserves, Tether offers relative stability in the volatile crypto marketplace.
- Liquidity: Tether's acceptance across exchanges and high trading volume make it easily exchangeable and a popular pairing choice for other cryptocurrencies.
- Global Availability: Tether provides an avenue for cross-border transactions, bypassing the need for traditional banking systems.

Cons:

- Lack of Transparency: Tether has been criticized for inadequate transparency and auditing of its reserves. Despite its claims of fiat-backed reserves, there's been little verifiable evidence to confirm these claims.
- Counterparty Risk: Tether operates as a centralized entity. Therefore, users must trust Tether Limited to honor its commitments, exposing them to the risk of Tether's potential financial difficulties or regulatory issues.
- Regulatory Concerns: Regulatory scrutiny in the stablecoin market has been on the rise, with concerns over potential market manipulation, insufficient anti-money laundering controls, and overall market stability.
- It's also worth noting that Tether's reserve breakdown reveals only approximately 3% is fiat USD, with a substantial portion being "commercial paper" – essentially, debt loans to unknown entities. This structure could potentially collapse under a "run" on Tether, and the chances of a bailout from a state or international body are minimal.

Terra (UST)

The Terra network offers an algorithmic stablecoin, TerraUSD (UST), which is pegged to the U.S. dollar. The protocol is designed to maintain this peg through a system of minting and burning of its native coin, Luna.

To create UST, Luna tokens are burnt, implying that when Luna's price was high, more UST could be generated for each Luna token. This system essentially ensured that the value of UST would remain around $1 by allowing UST and Luna to be interchanged at will, adjusting for Luna's price.

However, when UST's value began to significantly deviate from its $1 peg, the protocol's response led to a catastrophic outcome. In an effort to stabilize UST, the protocol significantly increased the supply of Luna tokens. This increase in supply, however, caused Luna's price to plummet as a result of hyper-inflation and investors rushing to sell their holdings.

This scenario highlights some critical issues:

- **Extreme Volatility**: The sudden and *extreme* depreciation in Luna's value demonstrated the risk of volatile and severe price movements in the system. Luna lost about 98% of its market value overnight, falling close to $0.
- **Instability**: The algorithmic model, intended to keep UST's value around $1, failed under stress, leading to a loss of its peg to the U.S. dollar.
- **Rush to Exit**: When UST lost its peg and Luna's value started to crash, a rush to exit ensued as investors sought to minimize their losses. This rush further exacerbated the downward pressure on Luna's price.
- **Uncontrollable Inflation**: The protocol's response mechanism caused a vast increase in Luna's supply, leading to rampant inflation that further devalued the token.

Zephyr Protocol, based on the Djed/AgeUSD model, does not face these issues due to the built-in stability mechanism and a fixed supply of its base coin, ZEPH.

Haven (XHV)

Haven Protocol offers its stablecoin (xUSD), backed by its native cryptocurrency (XHV), but the implementation has faced some challenges. Initially, the technical design of Haven ensured that 1 xUSD was equal to 1 USD worth of Haven at any time. While technically effective, this model did not protect the value of the base currency, XHV.

- **Unlimited Minting Mechanism**: By design, the supply of the stablecoin and XHV is limitless and isn't tied to the underlying network value. This mismatch has led to an imbalance where the amount of xUSD in circulation today exceeds Haven's market cap, a discrepancy that has grown over time.
- **Security Breaches**: Haven has suffered multiple security breaches, leading to unauthorized xUSD minting.
- **Volatility Risk**: The protocol's design is set to protect the stablecoin's value at any cost. However, this can be detrimental to the base currency, potentially causing a drop in confidence and leading to a slow death or "death spiral."

- **VBS**: The advent of Vault Backed Securities (VBS) addressed some of these issues but at the cost of xUSD's peg. It introduced a need for long-term collateral locking and thus introduced an opportunity cost for users limiting adoption. Any attempt to ease VBS could result in more xUSD being redeemed for XHV, potentially decreasing XHV's price and leading to a similar problem. VBS in its current state has also made it impractical to arbitrage xUSD on exchanges to help repeg.
- **Non-inflationary Peg**: Haven offers a BTC xAsset, allowing users to switch between xUSD and xBTC and mint more xUSD when trades are favorable. This process does not involve any buying or subsequent burning of XHV. However, even under optimal conditions, any increase in BTC's price would lead to base coin holders bearing the cost of these gains. This highlights the importance of pegging to an inflationary asset like fiat currency for a stablecoin protocol. The inflation inherent in such pegs theoretically eases pressure on the supporting network.

MakerDAO (DAI)
MakerDAO is a decentralized autonomous organization on the Ethereum blockchain, which manages and controls the DAI stablecoin. It's one of the oldest and most well-known DeFi projects in the cryptocurrency space.

The DAI stablecoin is soft-pegged to the U.S. dollar and is backed by collateralized debt positions (CDPs), now referred to as Vaults in the Maker system. Users can deposit Ether or other approved tokens into a Vault and generate DAI against this collateral. The collateral-to-debt ratio is always maintained above a specific minimum to ensure the system's solvency.

If the value of the collateral falls below this threshold, the Vault is automatically liquidated, with the collateral being sold off to cover the debt and maintain DAI's stability. The system also includes a governance token (MKR) used for voting on system parameters and decisions.

Zephyr Protocol, based on the Djed model, follows a different approach. Instead of using CDPs/Vaults, Zephyr Protocol maintains stability through an in-protocol reserve. This reserve, consisting of the native coin (ZEPH), is used to back the issuance of the stablecoin and ensure its peg to the U.S. dollar with minimum reserve requirements of 400%.

In conclusion, while each stablecoin solution has its unique features and advantages, they all carry significant risks and drawbacks. Zephyr Protocol, with its emphasis on protecting the value of the base currency and stablecoin, presents a promising alternative in this space.

Zephyr Symbol Definitions

Symbol	Definition
spot	Base coin Spot Price
MA	Base coin Moving Average Price
P^{spot}_{SC}	Stable coin spot price
P^{MA}_{SC}	Stable coin MA price
P^{spot}_{RC}	Reserve coin spot price
P^{MA}_{RC}	Reserve coin MA price
P_{SC}	Stable coin Price
P_{RC}	Reserve coin Price
P^{min}_{RC}	Minimum Price of Reserve Coin
R	Total Reserves
r	Reserve Ratio (spot)
r_ma	Reserve Ratio (MA)
E_{spot}	Equity (spot)
E_{MA}	Equity (MA)
Nsc	Number of Stable coins
Nrc	Number of Reserve Coins

Zephyr Formulas

Formula	Description
P^{spot}_{SC} = $\frac{1}{spot}$ *(if r >= 1 or Nsc = 0)*; $\frac{R}{Nsc}$ *otherwise*	Stable coin spot price is the spot price in terms of ZEPH if the Reserve Ratio is >=1 or there are no stable coins. Otherwise use Reserves / number of stable coins
P^{MA}_{SC} = $\frac{1}{MA}$ *(if r_ma >= 1 or Nsc = 0)*; $\frac{R}{Nsc}$ *otherwise*	Stable coin moving average (MA) price is the MA price in terms of ZEPH if the Reserve Ratio is >=1 or there are no stable coins. Otherwise use Reserves / number of stable coins
P_{SC} = $max(P^{spot}_{SC}, P^{MA}_{SC})$ *If mint_stable*; $min(P^{spot}_{SC}, P^{MA}_{SC})$ *If redeem_stable*	Stable coin price depends on the transaction type and either the minimum or maximum of P^{spot}_{SC} and P^{MA}_{SC}
$E_{spot} = R - \frac{Nsc}{spot}$	Equity (spot) is the Total Reserves minus (Number of stable coins / spot).
$E_{MA} = R - \frac{Nsc}{MA}$	Equity (MA) is the Total Reserves minus (Number of stable coins / MA).
$P^{min}_{RC} = 0.5$	Minimum reserve coin price of is set to 0.5.
P^{spot}_{RC} = $max(\frac{E_{spot}}{Nrc}, P^{min}_{RC})$ *if Nrc > 0*; P^{min}_{RC} otherwise	Reserve coin spot price is the max of Equity (spot) / number of reserve coins (Nrc) and the minimum price of reserve coin, if Nrc is greater than 0. Otherwise use the minimum reserve coin price.
P^{MA}_{RC} = $max(\frac{E_{MA}}{Nrc}, P^{min}_{RC})$ if Nrc > 0; P^{min}_{RC} otherwise	Reserve coin MA price is the max of Equity (calculated using the MA price) / number of reserve coins (Nrc) and the minimum price of reserve coin, if Nrc is greater than 0. Otherwise use the minimum reserve coin price.
P_{RC} = $max(P^{spot}_{RC}, P^{MA}_{RC})$ *If mint_reserve*; $min(P^{spot}_{RC}, P^{MA}_{RC})$ *If redeem_reserve*	Reserve coin price depends on the transaction type and either the minimum or maximum of P^{spot}_{RC} and P^{MA}_{RC}
$r = \frac{R * spot}{Nsc}$	Reserve Ratio (spot) is the Reserves times spot price, divided by the number of stablecoins.
$r\_ma = \frac{R * MA}{Nsc}$	Reserve Ratio (MA) is the Reserves times the MA, divided by the number of stablecoins.

Protocol Actions

Mint Stable

Convert Zeph into ZephUSD

Allowed when r and r_ma are ABOVE 4.0 before and after the action.

Redeem Stable

Convert ZephUSD into Zeph

Always allowed. If reserves are not sufficient to cover existing stablecoin holders then they receive rate $\frac{R}{Nsc}$

Mint Reserve

Convert Zeph into ZephRSV

Allowed when r and r_ma are BELOW 8.0 before and after the action.

Redeem Reserve

Convert ZephRSV into Zeph

Allowed when r and r_ma are ABOVE 4.0 before and after the action unless the number of stablecoins is 0 before and after in which case you can always redeem reserve coins.

Zephyr Protocol Scenario Exploration

In the following section we will go over various scenarios to have a practical look on how the protocol can be affected by market conditions and how actions performed on the network contribute to the network state.

A Github repository is available which was used to simulate these examples and will be updated and expanded on over time. Feel free to define your own scenarios.

This also serves as an approachable overview of Zephyr Protocol in an abstracted form to better understand the core functions, calculations and rules that govern the protocol.

https://github.com/ZephyrProtocol/pyzeph

Scenario 1 (excl/ tx fees)

Lets go over all actions and their effects starting from when the protocol is initialized.
Note that figures provided are often rounded for readability purposes

1. Initialization after Hardfork

Initial Network State:

Price: spot: $2.00
MA: $1.50

Reserve: 0 ZEPH
$0 (spot) $0 (ma)
Ratio: (inf,inf)

Nsc: 0
Nrc: 0

2. Mint 2000 reserve coins for 1000 ZEPH at price P^{min}_{RC}

Because no reserve coins currently exist, this action is allowed in order to initialize the reserve and uses this formula

$$RC\_Received = ZEPH\_Deposited \,/\, PminRC$$
$$RC\_Received = 1000 \,/\, 0.5 = 2000$$

Updated Network State:

Price: spot: $2.00
Ma: $1.50

Reserve: 1000 ZEPH
$2000 (spot) $1500 (MA)
Ratio: (inf, inf)

Nsc: 0
Nrc: 2000

3. Mint stable coins from 300 ZEPH at the max of P^{spot}_{SC} and P^{MA}_{SC}.
This action is allowed because the resulting Reserve Ratios will be above the minimum and below the maximum.
Mint_stable uses the max of P^{spot}_{SC} and P^{MA}_{SC}. The 300 ZEPH is added to the reserve.

$$P_{SC} = max(P^{spot}_{SC}, P^{MA}_{SC})$$
$$P_{SC} = max(0.5, 0.666) = 0.666$$

$$SC\_Received = (stables\_redeemed / P_{SC}) * (1 - Fee)$$
$$SC\_Received = (300 / 0.666) * (1 - 0.02) = 441\ ZephUSD$$

Updated Network State:
Price: spot: $2.00
MA: $1.50

Reserve: 1300ZEPH
$2600 (spot) $1950 (MA)
Ratio: (5.89, 4.42)

Nsc: 441
Nrc: 2000

4. Mint reserve coins from 200 ZEPH at the $max(P^{spot}_{RC}, P^{MA}_{RC})$
First we need to calculate the total Equity at the spot and and MA prices

$$E_{spot} = R - \frac{N_{sc}}{spot}$$
$$E_{spot} = 1300\ ZEPH - \frac{441}{2} = \$1079.5$$

$$E_{MA} = R - \frac{N_{sc}}{MA}$$
$$E_{MA} = 1300\ ZEPH - \frac{441}{1.5} = \$1006$$

Now we can calculate the ZephRSV prices. Because Nsc > 0 we can use these functions

$$P^{spot}_{RC} = max(E_{spot}/N_{rc}, P^{min}_{rc})$$
$$P^{spot}_{Rc} = max(1079/2000, 0.5) = 0.539\ ZEPH$$

$$P^{MA}_{RC} = max(E_{MA}/N_{rc}, P^{min}_{rc})$$
$$P^{MA}_{Rc} = max(1006/2000, 0.5) = 0.503\ ZEPH$$

$$P_{RC} = max(P^{spot}_{RC}, P^{MA}_{RC})$$
$$P_{RC} = max(0.539, 0.503) = 0.539$$

We have calculated the price of ZephRSV. We now can determine how much ZephRSV will be received when minting from 200 ZEPH. This action is allowed as the resulting reserve ratio will be < 8

$$RC\_Received = (ZEPH\_amount / P_{RC})$$
$$RC\_Received = (200 / 0.539) = 370.54\ ZephRSV$$

Updated Network State:

Price ZEPH:	spot: $2.00
	MA: $1.50
Price ZephUSD:	spot: 0.5
	MA: 0.66
Price ZephRSV:	spot: 0.539
	MA: 0.508
Reserve:	1500ZEPH
	$3000 (spot) $2250 (MA)
	Ratio: (6.8, 5.1)
Nsc:	441
Nrc:	2370.54

Note how minting more reserve coins in this example doesn't decrease the value of the ZephRSV price as the equity has increased by the added 200 ZEPH. Reserve ratios have increased.

5. Redeem 200 ZephRSV

First we need to calculate the total Equity at the spot and MA prices as shown above to determine the ZephRSV Price. For the redeem_reserve function we use these functions:

$$P_{RC} = min(P^{spot}_{RC}, P^{MA}_{RC})$$
$$P_{RC} = min(0.539, 0.508) = 0.508$$
$$ZEPH\_Received = RC\_amount * P_{RC}$$
$$ZEPH\_Received = 200 * 0.508 = 101.74\ ZEPH$$

Updated Network State:

Price ZEPH:	spot: $2.00
	MA: $1.50
Price ZephUSD:	spot: 0.5
	MA: 0.66
Price ZephRSV:	spot: 0.542
	MA: 0.508
Reserve:	1398.25ZEPH
	$2796.50 (spot) $2097.37 (MA)
	Ratio: (6.34, 4.75)
Nsc:	441
Nrc:	2170.54

6. Redeem 250 ZephUSD

The redeem_stable action is always permitted. Because the reserve ratio is > 1 we can fulfill this action.

redeem_stable means that the price of the stable coin in ZEPH used is the max between the spot and ma, which means the amount of ZEPH will be calculated using the higher SC price - 2%

Firstly we need to determine the stable price in ZEPH for both the spot price and MA. Because the reserve ratios are > 1 we can simply use $\frac{1}{spot}$ and $\frac{1}{MA}$ respectively

$$P^{spot}_{SC} = \frac{1}{spot}$$
$$P^{spot}_{SC} = \frac{1}{2.0} = 0.5\ ZEPH$$
$$P^{MA}_{SC} = \frac{1}{1.5} = 0.66..\ ZEPH$$

Now we can determine the amount of ZEPH to be received:

$$ZEPH\_Received = stables\_redeemed\ /\ max(P^{spot}_{SC}, P^{MA}_{SC}) * (1 - fee)$$
$$ZEPH\_Received = 250\ /\ max(0.5, 0.66..) * (1 - 0.02) = 122.5\ ZEPH$$

We can determine the value received like so:

$$Value\_Received = ZEPH\_Received * max(Spot, MA)$$
$$Value\_Received = 122.5\,ZEPH * \$2 = \$245$$

Updated Network State:

Price ZEPH:	spot: $2.00
	MA: $1.50
Price ZephUSD:	spot: 0.5
	MA: 0.66
Price ZephRSV:	spot: 0.543
	MA: 0.529
Reserve:	1275.75 ZEPH
	$2551.50 (spot) $1913.62 (MA)
	Ratio: (13.35, 10.01)
Nsc:	191.0
Nrc:	2170.54

The reserve is extremely healthy now as seen by the reserve ratios. It's important to note that because the reserve ratios are > 8, no more ZEPH can be added to the reserve by means of mint_reserve in order to not dilute the current ZephRSV holders. More ZEPH can be added if stables are minted.

7. Redeem remaining 191 ZephUSD

$$ZEPH\_Received = stables\_redeemed / max(P^{spot}_{SC}, P^{MA}_{SC}) * (1 - fee)$$
$$ZEPH\_Received = 191 / max(0.5, 0.66..) * (1 - 0.02) = 93.59\,ZEPH$$

We can determine the value received like so:

$$Value\_Received = ZEPH\_Received * max(Spot, MA)$$
$$Value\_Received = 93.59\,ZEPH * \$2 = \$187.18$$

Updated Network State:

Price ZEPH:	spot: $2.00
	MA: $1.50
Price ZephUSD:	spot: 0.5
	MA: 0.66
Price ZephRSV:	spot: 0.544
	MA: 0.544

Reserve:	1182.16 ZEPH $2364.32 (spot) $1773.24 (MA) Ratio: (inf, inf)
Nsc:	0
Nrc:	2170.54

8. Redeem remaining 2170.54 ZephRSV

To finish off the scenario let's redeem the remaining Reserve coins. Each ZephUSD is a share of the total ZEPH reserves (1182.16)

$$P_{RC} = min(P^{spot}_{RC}, P^{MA}_{RC})$$
$$P_{RC} = min(0.544, 0.544) = 0.544$$
$$ZEPH\_Received = RC\_amount * P_{RC}$$
$$ZEPH\_Received = 2170.54 * 0.544 = 1182.16\ ZEPH$$

Conclusion

Scenario 1 has given us an in-depth perspective into how the interaction of various actions - minting and redeeming stable and reserve coins - impact the state of the Zephyr Network. From the initial hardfork and network initialization, to numerous transactions involving ZephUSD and ZephRSV, we've observed how each action recalibrates the system and impacts the reserve ratios and pricing of the native tokens.

One major takeaway is how Zephyr Protocol ensures that the system is kept within the healthy range for reserve ratios through the use of the various transaction rules and price calculations. For instance, minting more reserve coins doesn't decrease the value of ZephRSV as the equity increases simultaneously with the addition of ZEPH to the reserve. This effectively increases the reserve ratio, contributing to the overall health of the system.

The redeem_stable function also played a key role in maintaining system stability, given that it is always permitted and the fact that the reserve ratio is maintained above 1, allowing for the action to be fulfilled in full. We will look at the worst case situations in Scenario 2 in order to outline what happens in extreme market conditions

Scenario 2

Let's consider a situation where the spot price of ZEPH dramatically drops. What happens when stables are redeemed?

Initial Network State:

Price: spot: $2.00
MA: $1.50

Reserve: 1000 ZEPH
$2000 (spot) $1500 (MA)
Raito: (4.0,3.0)

Nsc: 500
Nrc: 1000

In this initial network state, the reserves are healthy, although importantly the minting of more stables right now will be disallowed as the ma reserve ratio is < 4.

Redeeming stables is always allowed, and in this case this would not be an issue.

1. Redeem 100 Stables

redeem_stable means that the price of the stable coin in ZEPH used is the max between the spot and ma, which means the amount of ZEPH will be calculated using the higher SC price - 2%

Firstly we need to determine the stable price in ZEPH for both the spot price and MA. Because the reserve ratios are > 1 we can simply use $\frac{1}{spot}$ and $\frac{1}{MA}$ respectively

$$P^{spot}_{SC} = \frac{1}{spot}$$

$$P^{spot}_{SC} = \frac{1}{2.0} = 0.5\ ZEPH$$

$$P^{MA}_{SC} = \frac{1}{MA}$$

$$P^{MA}_{SC} = \frac{1}{1.5} = 0.66..\ ZEPH$$

Now we can determine the amount of ZEPH to be received:

$$ZEPH\_Received = stables\_redeemed\ /\ max(P^{spot}_{SC}, P^{MA}_{SC})\ *\ (1 - fee)$$

$$ZEPH\_Received = 100\ /\ max(0.5,\ 0.66..)\ *\ (1 - 0.02) = 49\ ZEPH$$

We can determine the value received like so:

$$Value\_Received = ZEPH\_Received * max(Spot, MA)$$
$$Value\_Received = 49\,ZEPH * \$2 = \$98$$

You can see how the amount of ZEPH received and the calculated value received is tied to both the spot and MA prices. In practical terms, this example shows that when the spot price > ma price

Updated Network State:

Price ZEPH:	spot: $2.00
	MA: $1.50
Price ZephUSD:	spot: 0.5
	MA: 0.66
Price ZephRSV:	spot: 0.751
	MA: 0.683
Reserve:	951 ZEPH
	$1902 (spot) $1426.50 (MA)
	Ratio: (4.755, 3.56)
Nsc:	400
Nrc:	1000

Notice how the reserve ratio has improved.

2. Spot price drops significantly $2.00 -> 0.30c *(85% decrease)*

In this extreme example, the spot price of ZEPH drops by 85% Importantly, the MA price is unaffected.

Updated Network State:

Price ZEPH:	spot: $0.30
	MA: $1.50
Price ZephUSD:	spot: 2.37
	MA: 0.66
Price ZephRSV:	spot: 0.5
	MA: 0.684
Reserve:	951 ZEPH

$285.30 (spot) $1426.50 (MA)
Ratio: (0.713, 3.56)

Nsc: 400
Nrc: 1000

3. Redeem 100 stables

In the next step, the stable coin owner attempts to redeem 100 stable coins. However, the system is in a state where the spot reserve ratio is less than 1, indicating that there aren't enough reserves to fully cover the redemption. But because the value calculations will use the MA value for the reserve, this action will be satisfied in full with respect to the MA price.

$$ZEPH\_Received = stables\_redeemed \,/\, max(P^{spot}_{SC}, P^{MA}_{SC}) * (1 - fee)$$
$$ZEPH\_Received = 100 / max(2.37, 0.66) * (1 - 0.02) = 56.33\ ZEPH$$

We can determine the value received like so:

$$Value\_Received = ZEPH\_Received * max(Spot, MA)$$
$$Value\_Received = 56.33\ ZEPH * \$1.50 = \$98$$

Updated Network State:
Price ZEPH: spot: $0.30
MA: $1.50
Price ZephUSD: spot: 2.95
MA: 0.66
Price ZephRSV: spot: 0.5
MA: 0.685

Reserve: 885.66 ZEPH
$265.70 (spot) $1328.5 (MA)
Ratio: (0.885, 4.428)

Nsc: 300
Nrc: 1000

Importantly, due to this transaction, the reserve ratios have improved.

4. MA price falls to match spot price at 30c

Updated Network State:

Price ZEPH:	spot: $0.30
	MA: $0.30
Price ZephUSD:	spot: 2.95
	MA: 2.95
Price ZephRSV:	spot: 0.5
	MA: 0.5
Reserve:	885.66 ZEPH
	$265.70 (spot) $265.70 (MA)
	Ratio: (0.885, 0.885)
Nsc:	300
Nrc:	1000

This now outlines the “worst case scenario” for the protocol. Now there isn’t sufficient reserves to cover the number of stable coins

4. Redeem 275 stables when reserve ratios are less than 1

Because the reserve ratios are less than 1, we need to use a different calculation for determining the SC prices.

Spot and ma prices are identical in this situation.

$$P_{SC} = \frac{R}{N_{SC}}$$

$$P_{SC} = \frac{885.66}{300} = 2.95\ ZEPH$$

Now we can determine the amount of ZEPH to be received:

$$ZEPH\_Received = stables\_redeemed\ /\ P_{SC} * (1 - fee)$$

$$ZEPH\_Received = 275 * 2.95 * (1 - 0.02) = 795.623\ ZEPH$$

We can determine the value received like so:

$$Value\_Received = ZEPH\_Received * max(Spot, MA)$$

$$Value\_Received = 795.623\ ZEPH * \$0.30 = \$238.69$$

We can see how this user redeemed at a loss of ($275 - $238.69) $36.31- including fees.

Updated Network State:

Price ZEPH:	spot: $0.30
	MA: $0.30

Price ZephUSD:	spot: 2.95
	MA: 2.95
Price ZephRSV:	spot: 0.5
	MA: 0.5
Reserve:	90.04 ZEPH
	$27.01 (spot) $27.01 (MA)
	Ratio: (1.08, 1.08)
Nsc:	25
Nrc:	1000

Importantly, due to this transaction, the reserve ratios have improved. Both reserve ratios have improved to > 1

Conclusion:

In this particular situation, we have observed how a dramatic decrease in the spot price of ZEPH, along with the redemption of stable coins, affects the network's reserve and its functioning. Importantly, despite an 85% drop in the spot price, the network was still able to redeem all the stable coins, although some were not redeemed at a reduced value.

Initially, the ZEPH reserve was at 1000 ZEPH. After redeeming all the stable coins, the remaining ZEPH reserve is 484.54. In this specific scenario, the reserve still retains 48.45% of its initial ZEPH reserve value and is not fully depleted. There are still 484.54 ZEPH in the reserve, valued at $145.36 at the current spot and MA prices.

The changes in the reserve ratio throughout these operations indicate that the system has self-balancing mechanisms to adjust to market volatility. In this case, after the initial spot price drop, the reserve ratio was less than 1, indicating that the reserves were not sufficient to cover all the stable coins. However, the mechanisms in place to protect the system allowed for a significant improvement in the reserve ratios as stables were redeemed.

Scenario 3

In this scenario, we delve into the strategies employed by ZephRSV holders as they seek to optimize their positions by betting on the ZEPH's value. It's worth mentioning that even in the absence of an upward price movement of the base currency, the value of ZephRSV can still appreciate. This is primarily driven by the growth of the ZEPH reserve, which results from transaction fees collected from minting and redeeming stables, and from more users contributing ZEPH to the reserve pool. Consequently, reserve providers have the potential to profit even in a stagnant market, thanks to the protocol's continued utilization by its user base.

1. Mint 2000 reserve coins for 1000 ZEPH at price P^{min}_{RC}

Because no reserve coins currently exist, this action is allowed in order to initialize the reserve and uses this formula. For simplicity we will imply that the ZephRSV returned in this transaction will represent all holders.

$$RC\_Received = ZEPH\_Deposited / PminRC$$
$$RC\_Received = 1000 / 0.5 = 2000$$

Updated Network State:

Price: spot: $2.00
Ma: $1.80

Reserve: 1000 ZEPH
$2000 (spot) $1500 (MA)
Ratio: (inf, inf)

Nsc: 0
Nrc: 2000

2. Mint stable coins from 300 ZEPH at the max of P^{spot}_{SC} and P^{MA}_{SC}.

This action is allowed because the resulting Reserve Ratios will be above the minimum and below the maximum.

Mint_stable uses the max of P^{spot}_{SC} and P^{MA}_{SC}. The 300 ZEPH is added to the reserve.

$$P_{SC} = max(P^{spot}_{SC}, P^{MA}_{SC})$$
$$P_{SC} = max(0.5, 0.55) = 0.555$$

$$SC\_Received = (ZEPH\_Amount / P_{SC}) * (1 - Fee)$$
$$SC\_Received = (300 / 0.666) * (1 - 0.02) = 529.2\ ZephUSD$$

Updated Network State:

Price ZEPH:	spot: $2.00
	MA: $1.80
Price ZephUSD:	spot: 0.5
	MA: 0.55
Price ZephRSV:	spot: 0.5177
	MA: 0.503
Reserve:	1300 ZEPH
	$2600 (spot) $2340 (MA)
	Ratio: (4.9, 4.4)
Nsc:	529.2
Nrc:	2000

3. The price of ZEPH increases to $3

Updated Network State:

Price ZEPH:	spot: $3.00
	MA: $2.50
Price ZephUSD:	spot: 0.33
	MA: 0.4
Price ZephRSV:	spot: 0.561
	MA: 0.544
Reserve:	1300 ZEPH
	$3900 (spot) $3250 (MA)
	Ratio: (7.36, 6.141)
Nsc:	529.2
Nrc:	2000

4. More stables are minted from 100 ZEPH at this higher price

$$P_{SC} = max(P^{spot}_{SC}, P^{MA}_{SC})$$
$$P_{SC} = max(0.33, 0.4) = 0.4$$

$$SC\_Received = (ZEPH\_Amount / P_{SC}) * (1 - Fee)$$
$$SC\_Received = (100 / 0.666) * (1 - 0.02) = 245\ ZephUSD$$

Updated Network State:

Price ZEPH:	spot: $3.00
	MA: $2.50
Price ZephUSD:	spot: 0.33
	MA: 0.4
Price ZephRSV:	spot: 0.57
	MA: 0.545
Reserve:	1400 ZEPH
	$4200 (spot) $3500 (MA)
	Ratio: (5.42, 4.52)
Nsc:	774.2
Nrc:	2000

5. All stables are redeemed (774.2 ZephUSD)

$$ZEPH\_Received = stables\_redeemed \,/\, max(P^{spot}_{SC}, P^{MA}_{SC}) * (1 - fee)$$
$$ZEPH\_Received = 774.2 / max(0.33, 0.4) * (1 - 0.02) = 252.9\, ZEPH$$

We can determine the value received like so:

$$Value\_Received = ZEPH\_Received * max(Spot, MA)$$
$$Value\_Received = 252.9\, ZEPH * \$3 = \$758.72$$

Updated Network State:

Price ZEPH:	spot: $3.00
	MA: $2.50
Price ZephUSD:	spot: 0.33
	MA: 0.4
Price ZephRSV:	spot: 0.573
	MA: 0.573
Reserve:	1147.09 ZEPH
	$3441.28 (spot) $2867.73 (MA)
	Ratio: (inf, inf)
Nsc:	0
Nrc:	2000

5. All Reserve coins are redeemed (2000)

$$P_{RC} = min(P^{spot}_{RC}, P^{MA}_{RC})$$

$$P_{RC} = min(0.573, 0.573) = 0.573$$

$$ZEPH\_Received = RC\_amount * P_{RC}$$

$$ZEPH\_Received = 2000 * 0.573 = 1147.09\ ZEPH$$

Conclusion

These scenarios provide a valuable perspective on the resilience of the network. Even in adverse market conditions, the system's design allows for stable coin redemptions, while also maintaining a substantial amount of the reserve. This demonstrates the robustness of the protocol and its ability to adapt to severe price fluctuations, ensuring the sustainable operation of the network even in turbulent market conditions.