ZigZag: An Algorithmic Lending Service

zigzag.finance

Abstract. ZigZag is an algorithmic lending service premised on overcollateralization. ZigZag provides the former an instrument for hedging and adding leverage to their long positions, and enables volatility-free daily usage of digital assets for the latter. The platform has two tokens - ZIG and ZAG. ZIG is a stablecoin which users receive in return for collateralizing their digital assets.

1. Introduction

The financial system sets the goal to facilitate the well-being of the overall economy. In doing so, it performs a set of crucial functions. Mobilization of savings from economic agents with capital surplus and their further channeling to entities and individuals that seek financing, inter alia, is one of the most important objectives set before the financial system. It achieves this goal by organizing savings flow process around financial intermediation, which, in most cases, is performed by banks and credit unions.

With the renaissance of the blockchain technology, economic agents received another type of asset applicable for storing their savings which are usually referred to as “digital assets”. However, traditional financial intermediaries are barely capable of interacting with them, let alone providing lending services, primarily due to uncertainty in regulatory framework. There are several projects in the blockchain industry that aim to fill in the gap and facilitate lending of digital assets. While some of such projects utilize centralized solutions by taking digital assets in custody, others operate as DAOs with smart contracts managing lending process. ZigZag relates to the latter group. Its smart contracts utilize collateralized debt positions to issue and lend ZIG tokens in return for deposited digital assets.

According to CoinMarketCap as of the beginning of March 2019, the capitalization of digital assets was $190B with the market share of collateralized stablecoins comprising for 0.06% ($110M). Unlike regular digital assets, their supply is not algorithmically determined. Instead, it depends on the value of the collateral deposited into the corresponding smart contracts.

The competition between collateralized stablecoins experiences a significant level of fragmentation due to compatibility issues. Smart contacts, deployed on a particular blockchain, can accept only digital assets native to that network without any additional technical enhancements. The ability to collateralize digital assets of other blockchains comes at the cost of incremental development, which is expensive and time-consuming.

Currently, MakerDAO prevails in the market of collateralized stablecoins with the capitalization of issued DAI totaling to $85M. However, its domination is presently limited only to the Ethereum ecosystem since Maker DAO smart contract is deployed on Ethereum blockchain and is capable of accepting only ETH as collateral. Therefore, the demand for collateralized stablecoins in many other blockchain networks is still untapped.

ZigZag leverages MakerDao solution and alters it with a novel mechanism of dynamic adjustments to system parameters. In this way, ZigZag establishes an algorithmic lending service governed by a set of smart contracts deployed on EOS mainnet.

2. Vision

Volatility limits the use of digital assets as a source of funding. Bullish sentiment makes holders unwilling to spend or lend their coins, while bearish sentiment makes merchants unwilling to accept digital assets as payment. In this way, holders are forced to seek financing in traditional markets. ZigZag premises its lending services on its overcollateralized stablecoin - ZIG, and aims to become a reliable platform for entrepreneurs, traders, and regular consumers who want to finance their ideas, bootstrap existing projects, or fund daily consumption with their coins/tokens. With only smart contracts governing the lending process and no third parties involved, ZigZag strives to give the momentum to the emergence of algorithmic banking in the long run.

While in the initial bootstrap phase, ZigZag primarily targets traders, offering them an instrument for adding leverage to their long positions in digital assets in a transparent way. The broader use case would be, however, funding daily consumption with the funds borrowed through ZigZag platform.

3. ZigZag Overview

ZigZag is an algorithmic lending service that utilizes overcollateralization to mitigate default risk. The platform is powered by two tokens - ZIG and ZAG. ZIG and ZAG tokens are similar to other digital assets such as Bitcoin or EOS: they can be freely transferred, used as a means of payment or held as long term savings.

In anticipation of the bullish market, traders strive to add leverage to their long positions, and regular users are unwilling to fund their daily consumption with accumulated digital assets. ZigZag allows the former to magnify their gains and the latter to consume without selling off their holdings by engaging in collateralized debt positions (CDPs). CDPs can be created by depositing digital assets into the service's smart contract, which issues and transfers ZIGs in return. Borrowers subsequently can either convert their ZIGs into fiat currencies or buy with them more digital assets, thus, leveraging their long positions. CDPs continue indefinitely and have no maturity date, which makes them similar to perpetual loans.

Borrowers pay a daily fixed interest charged in ZIGs which we will refer to as APR. Its rate is determined at the inception of the CDP by ZigZag algorithms depending on the market conditions. The system always quotes annualized APR, but the interest is accrued on a daily basis.

As said, ZigZag premises its lending service on overcollateralization. For $1.7 of the value of deposited digital assets, borrowers receive 1 ZIG worth 1 USD. The proportion of the dollar value of the collateral to the number of ZIGs issued is called the collateralization ratio (CR). The ratio is calculated separately for each CDP and, thus, is specific to each borrower. At the inception of the CDP, CR is set to 1.7. Later on, with appreciation (depreciation) of the collateralized digital asset's relative to USD and decrease (increase) of the accrued interest, the CR may increase (decrease). Should CR be above 1.7, a borrower can claim more ZIG tokens, thus decreasing the ratio. When CR fluctuates between 1.2 and 1.7, no more ZIGs can be claimed. Should CR fall below 1.2, the smart contract liquidates CDP by selling the collateral. If the case, the borrower gets charged the liquidation penalty of 13%.

4. Stakeholders

We anticipate five distinct groups of ZigZag stakeholders to evolve: (i) borrowers with immediate liquidity needs, (ii) borrowers with hedging intent, (iii) borrowers with trading intent, (iv) arbitrageurs and market makers, (v) contributors. They will have a direct impact on ZIG exchange rate, so we account for their behaviour and interests in calculating ZigZag system parameters and conducting scenario analysis.

Borrowers with immediate liquidity needs. Borrowers overcollateralize their debt positions by depositing digital assets to ZigZag smart contract in excess to the value of ZIGs they receive in return. The overcollateralization secures intrinsic value of the issued ZIGs and ensures stability of ZIG/USD exchange rate. Thus, borrowers obtain liquidity on demand without selling their assets.

Borrowers with hedging intent. Some borrowers may utilize ZIG tokens to hedge their digital assets against decrease in prices. The portion of the hedged long position is inversely related to CR. By default, users can hedge up to 59% of their digital asset holdings against depreciation.

Borrowers with trading intent. Borrowers may also engage in CDPs to obtain leverage for their trading strategies. For that one has to convert ZIG proceeds from collateralization back to the digital asset used to initiate a CDP. For example, given CR is 1.7, a borrower receives ZIG tokens worth 59% of the value of deposited EOS and converts it back into EOS. Then, s/he initiates a new CDP and repeats the described procedure again. Theoretically, one can repeat the process an unlimited number of times, however, with each next cycle the amount of received ZIG tokens diminishes. Given the default CR of 1.7, the cumulative leverage approaches 43% as depicted in the Figure 1.

Figure 1. CDP Leverage

Iteration	**ZIG Received**	**EOS Collateralized**
1	58.82	**100**
2	34.60	58.82
3	20.35	34.60
4	11.97	20.35
5	7.04	11.97
6	4.14	7.04
7	2.44	4.14
8	1.43	2.44
9	0.84	1.43
10	0.50	0.84
Total	**142.77**	

Arbitrageurs and market makers. The deviation of USD/ZIG exchange rate from the target creates an arbitrage opportunity. Arbitrageurs tend to exploit it by purchasing ZIG tokens when the price falls below 1 USD/ZIG and selling them when the price fluctuates above the target exchange rate. Rational arbitrageurs will trade at the edges of the allowed exchange rate target zone and bet on the price movements that tend towards the target exchange rate, thus, accelerating reversion of the exchange rate to its target. Being the end buyer of ZIG tokens, the ZigZag system will intervene in the market by using its Liquidity and Stabilization Fund to buyback tokens when sellers dominate the market and issue more of them by engaging in interest-free CDPs in case buyers prevail. The trading activity of market makers will facilitate high liquidity and low bid/ask spreads.

5. ZIG Stablecoin

ZigZag resilience revolves around the stability of USD/ZIG exchange rate. Though short-term deviations are inevitable, the reversion to the target exchange rate in the long run is crucial to the platform's stability. The system tolerates fluctuations around the target exchange rate of 1 USD/ZIG within the protocol-defined range. Its width constantly adjusts in conformity with the market conditions (e.g., volatility, trading volume). We intentionally do not disclose the formula that we use to calculate the price range in order to prevent Soros-style attacks. Gaps in demand for ZIG and its supply are the primary cause of temporary exchange rate fluctuations. The long-term instability is only possible should the market participants lose confidence in the ability of the platform's stabilization mechanism to maintain the exchange rate at its target or individual collateralization rates fall. To bridge short-term gaps between demand and supply of ZIG token, ZigZag utilizes a set of instruments such as market making, market interventions as well as adjustments to system parameters.

Market making. ZigZag has a dedicated Market Making Bot which fills order books with liquidity using the holdings of the Liquidity and Stabilization Fund. The Market Making Bot operates in an adaptive price band with the deviation of +/-3% from the target price. Given the abnormal level of volatility, hedging costs rise and the band may be widened to +/-5%.

Market interventions. ZigZag platform engages in open market interventions using the Liquidity and Stabilization Fund to quickly mitigate imbalances in demand and supply. Should the demand for ZIG tokens exceed their supply, the system collateralizes a portion of its reserves to create interest-free CDPs, thus, increasing the amount of ZIG in circulation. Conversely, to mitigate the downward pressure of the excessive ZIG supply on the exchange rate, the platform conducts buyouts of ZIG tokens, again, using reserves of the Fund. Unlike Maker, ZigZag has no requirements for mandatory buyouts of ZIG tokens issued by defaulted CDPs. Such tokens remain in free float until the system intervenes in the market to decrease ZIG supply.

Adjustments to system parameters. Such system parameters as APR and CR influence both demand for and supply of ZIG tokens, thus, having a direct impact on USD/ZIG exchange rate. APR is essentially the price that borrowers pay for holding a CDP. High APR indicates expensive credit which less borrowers can afford. As a result, the aggregate amount of collateralized digital assets across the platform falls and system generates fewer ZIG tokens. CR, the system's second parameter, impacts the level of the potential leverage that borrowers can obtain. The higher the ratio is, the less ZIG tokens users receive per dollar of collateral value. Therefore, high CR limits the leverage that borrowers can create as described in section 4. Thus, both APR and CR are inversely related to ZIG supply. ZigZag recalculates optimal APR and CR on a daily basis and proposes ZAG holders to vote for the adjustments. The detailed description of the calculations that platform uses to derive at optimal CR and APR is provided in section 7 of this Whitepaper.

The combination of the outlined instruments creates a complex framework for ZIG exchange rate stabilization. However, its use will differ depending on the stage of the platform development:

1. Upon ZigZag launch, the demand for ZIG tokens prevails. At the same time, the amount of created CDPs and collateralized digital assets is low which limits ZIG supply and drives ZIG appreciation. Let bid-ask quotes equal 1.01-1.03 USD/ZIG. To fulfill demand, the system creates CDPs utilizing its Liquidity and Stabilization Fund and immediately sells generated ZIG tokens at 1.01 USD/ZIG, thus, increasing ZIG in circulation and replenishing reserves of the Fund. The Market Making Bot operates within the range of 0.97-1.03 USD/ZIG and provides constant liquidity to other market participants. Should bid-ask quotes be lower (higher) than the lower (upper) band of the price range, the bot remains inactive and ZigZag intervenes in the market by buying (selling) ZIG tokens.
2. After ZigZag reaches the state of equilibrium, the platform only utilizes Market Making Bot to bridge short-term gaps between demand and supply. At this stage the Bot operates with the proceeds from its trading activity mitigating the necessity to utilize Fund reserves.
3. In case sellers dominate the market, USD/ZIG exchange rate falls. To create an upward pressure on the exchange rate, ZigZag closes its CDPs and engages in market interventions buying out ZIG tokens. As a result, ZIG in circulation decreases and exchange rate reverts back to the target.

6. Use Cases

ZigZag is primarily a lending service, however, its use cases are not limited to borrowing only and include hedging as well as marginal trading.

Borrowing. Alice works for a small research company and has 500 EOS in savings that are worth 4000 USD at the spot market rate of 8 USD/EOS. Alice is bullish on EOS and wants to hold it. However, her laptop was stolen a day ago. She needs 882 USD to buy a new one as soon as possible to be able to finish her assignments that are due in 10 days. Alice decides to fund the purchase of a new laptop with ZigZag. ZigZag has APR set to 3% and CR to 1.7.

1. She uses ZigZag mobile app to create a CDP and deposits 187.5 EOS worth 1,500 USD.
2. Given CR of 1.7, she receives 882 ZIG that can be converted into 882 USD in return for deposited EOS that is worth 1,500 USD.

3. Alice goes online and finds a merchant who accepts ZIG tokens as payment. She buys a laptop and successfully finishes her tasks by the deadline.
4. Each day ZigZag credits Alice interest expense of 0.0081% on the amount of received ZIG tokens.
5. Five days after the deadline (15 days after CDP inception), Alice receives her paycheck which she uses to close CDP. For that she repays accrued interest of 1.07 ZIG (15*0.081) and principal of 882 ZIG.

Hedging. After 2018 Bob decided to cease using Buy and Hold strategy and started active trading to better manage his risk and return. He usually holds his positions open from several days up to several weeks. ZigZag has APR set to 3% and CR to 1.7.

1. Bob spends 8,000 USD to purchase 1,000 EOS as he expects a sustained EOS appreciation relative to fiat currencies. However, he decides to hedge against downside risk.
2. A few days prior to EOS purchase, Alice, Bob's friend, met him at a cafe. She was very positive about her recent experience with ZigZag lending services, so Bob decided to learn more about the platform. After carrying out a research, he came to a conclusion that overcollateralization enables hedging. So, immediately after EOS purchase Bob deposits 1,000 EOS into ZigZag smart contract and receives 4,706 ZIG (8,000 USD / 1.7) tokens. Now 58% of his long EOS position is hedged.
3. Contrary to Bob's expectations, EOS depreciates against USD sharply in one day, and now USD/EOS exchange rate is 5.65 USD/EOS. Bob's CR is now 1.2 (5,650/4,706). ZigZag app sends Bob an alert asking to collateralize more EOS in order to improve his CR. However, Bob decides not to purchase more EOS.
4. The next day, USD/EOS exchange rate drops even more to 4 USD/EOS. However, ZigZag liquidated Bob's CDP when his CR fell below 1.2. Bob converts his ZIG tokens into dollars and receives 4,706 USD. Had Bob not hedged his long position, it would be worth 4000 USD instead.

Margin trading. Bob discusses his hedging strategy with Clara. She is a more risk tolerant person and often engages in margin trading. She believes that she can use overcollateralization to leverage her long positions in EOS. ZigZag has APR set to 3% and CR to 1.7.

1. Clara creates a CDP and collaterizes EOS worth 100 USD receiving 58 ZIG tokens in return.
2. She converts her ZIG tokens in EOS and creates another CDP.
3. She repeats the process a number of times and increases her initial position by 43% so that now she has EOS worth 143 USD.

4. The next day, after EOS market exchange rate increases by 10%, she closes her CDP and earns 14.3% return on invested EOS.

7. ZigZag Parameters

In this section we consider fundamental parameters of ZigZag perpetual lending service, such as accrued debt obligation, value of collateral, leverage and liquidation ratios. Furthermore, we provide formulae for their calculation and develop mathematical justification of CR and APR optimal values accordingly to market conditions.

Accrued debt obligation. The calculation of an accrued debt obligation for a perpetual CDP is performed using the following formula:

$$D_n = -\delta_{n-1} + (1 + r_n)D_{n-1} \tag{7.1}$$

where D_n and D_{n-1} — debt sizes at the moment of the accrual, n and $n-1$, δ_{n-1} — sum of payouts in the period between the moments of accruals n and $n-1$. If $D \leq 0$, then the loan is cleared off in full. The lendee receives their remaining balance $|D_n|$, if $D_n < 0$. The assessments are performed in equal timespans, which are provisionally enumerated with integers starting at 0. The moment 0 is for the moment of lending.

Value of collateral. Value estimation of the collateral is performed based on the USD/EOS exchange rate, collected from the oracles. The change in collateral value is calculated as follows:

$$r = \frac{P_n - P_{n-1}}{P_{n-1}} \tag{7.2}$$

where P_n and P_{n-1} — USD/EOS exchange rate at the moment of the debt recalculation. It is also known as RoC (rate of change) — a technical indicator, which belongs to oscillators.

Leverage ratio and liquidation ratio. Assume there are two assets with different profitabilities r_1 and r_2, where $r_1 > r_2$. Hence, a risk-free profit is possible by means of arbitration. To do so, it is required:

1. To long the more profitable asset r_1
2. To short the less profitable asset r_2

Let $S_1 = S_2 = S$ — assets' price in the moment of position creation. By the moment of position closure, the net profit will be equal to:

$$\Delta S = (1 + r_1)S - (1 + r_2)S = (r_1 - r_2)S > 0. \tag{7.3}$$

This way, the profit can be reached even with the decreasing profitability $0 > r_1 > r_2$. If n time has elapsed by the moment of closure, the profit can be calculated as follows:

$$\Delta S_n = S_n\left(\left(\frac{r_1 - r_2}{1 + r_1}\right)^n - 1\right) > 0. \tag{7.4}$$

Obviously, the difference in the asset profitability will tend to zero, and once it is reached, the price will stop changing, indicating full exploitation of the arbitrage opportunity. That being said, consider two scenarios.

Scenario 1. Assume that RoC for ZIG is $r_1 = 0$, RoC EOS is $r_2 < 0$, and APR is $i > 0$. Rational traders short EOS and go long ZIG by either selling EOS and buying ZIG, or collateralizing EOS and getting ZIG in return. The minimal cost of the first option is $1 \pm \sqrt{\sigma}100\%$ USD, where σ denotes volatility. The ZigZag system will perform it automatically, when possible. The second option is to get a ZIG loan and not to pay it off, having the depreciable EOS as a collateral.

That being said, it is required to find lending terms, which make the arbitrage using the second option impossible or disadvantageous.

Suppose the collateral amount at the starting moment equals S_0, and the loan price — D_0, which is also equal to the debt size at the starting moment. Also assume that r_2 and i remain unchanged. The collateral value at the moment n will be equal to $S_n = (1 + r_2)^n S_0$. Assume the loan has not been paid off $\delta_k = 0,\ \forall k = \overline{0, n}$. Then the debt will equal to $D_n = (1 + i)^n D_0$.

The leverage is calculated as $\gamma_1 = \frac{S_0}{D_0}$. Should the collateral value fall (or not grow), a moment n_1 will take place, when the collateral value becomes equal to the debt size:

$$1 = \frac{S_{n_1}}{D_{n_1}} = \left(\frac{1+r_2}{1+i}\right)^{n_1} \frac{S_0}{D_0} = \left(\frac{1+r_2}{1+i}\right)^{n\,1} \gamma_1 \tag{7.5}$$

where

$$\gamma_1 = \left(\frac{1+i}{1+r_2}\right)^{n_1}. \tag{7.6}$$

In the same way the liquidation ratio is determined as:

$$1 = \frac{S_{n_1}}{D_{n_1}} = \left(\frac{1+r_2}{1+i}\right)^{n_1 - n_2} \frac{S_{n_2}}{D_{n_2}} = \left(\frac{1+r_2}{1+i}\right)^{n_1 - n_2} \gamma_2 \tag{7.7}$$

where

$$\gamma_2 = \left(\frac{1+i}{1+r_2}\right)^{n_1 - n_2} \tag{7.8}$$

where $n_1 - n_2$ is derived using the liquidation relative cost $\frac{\Delta S}{S}$ given the exchange rate falls:

$$n_1 - n_2 = \frac{ln(\frac{\Delta S}{S})}{ln(1+r_2)}. \tag{7.9}$$

Parameter n_1 is determined statistically, based on the reliability of the RoC EOS forecast.

Scenario 2. Suppose that RoC ZIG $r_1 = 0$, and RoC EOS is $r_2 > i > 0$. In this case, the trader will short ZIG and long EOS. Assume that using the leverage, the trader will increase the size of their collateral. They can do it without the fear of liquidation, as the value of collateral S is growing faster than the debt size D. By selling ZIG on market, the trader will buy EOS and deposit it, while increasing the demand for EOS. Supposing all traders do so, in such a case, the ZigZag system will have to increase the offer. Thus, the part of the collateral's value increase will represent the shortfall in profits of the system. This can be resolved by increasing the leverage and changing the interest. The dependance of the leverage on r_2 and i as well as the ultimate value of collateral for given γ_1 should be found:

$$S_1 = D_0 = \frac{S_0}{\gamma_1} \tag{7.10}$$

$$D_n = \frac{S_n}{\gamma_1} = \frac{D_{n-1}}{\gamma_1} = \ldots = \frac{D_0}{\gamma_1^n}. \tag{7.11}$$

Then all debt is:

$$D = D_0 + D_1 + D_2 + \ldots = D_0 + \frac{D_0}{\gamma_1} + \frac{D_0}{\gamma_1^2} + \ldots = D_0 + \frac{D_0}{\gamma_1 - 1}. \tag{7.12}$$

The value of $\frac{D_0}{\gamma_1 - 1}$ represents the price of EOS purchased on the market, presumably, from the ZigZag system. Then γ_1 can be determined from the relation:

$$\frac{D_0}{\gamma_1 - 1}(1 + r_2)^{n_1} = D_0(1 + i)^{n_1} \tag{7.13}$$

-where the collateral value at the moment n_1 is on the left side, and on the right - the accrued debt size. Then γ_1 can be calculated as follows:

$$\gamma_1 = 1 + \left(\frac{1+r_2}{1+i}\right)^{n_1}. \tag{7.14}$$

The moment of time n_1 is determined statistically, based on the reliability of the RoC EOS forecast. As the calculations show in the article "Equilibrium Infrastructure: Collateral Adjustment Mechanisms
", the minimal leverage should be at 170%, and the minimal liquidation ratio for EOS is at 120%.

APR. To calculate an optimal leverage, consider the difference between the collateral value and the debt size and call it a liquidation reserve:

$$\Pi = NP_E - D \tag{7.15}$$

where P_E is EOS price, NP_E is collateral value denominated in USD, and N — amount of EOS. Assume that the price is random and adherent to the following stochastic differential equation (SDE):

$$dP_E = P_E \mu_E(t)\,dt + P_E \sigma_E(t)\,dW \tag{7.16}$$

where μ_E is a relative drift rate, σ_E — volatility, and W is Wiener random process. If μ_E and σ_E are time-independent, distribution P_E is log-normal. This assumption is frequently used in finance mathematics, including the development of Black-Scholes formula.

Assume that the explicit debt formula is unknown, and the debt depends on the time elapsed from the moment of CDP creation and the collateral value $D = D(P_E, t)$. Using the Ito lemma, find dD:

$$dD = \frac{\partial D}{\partial t}dt + \frac{\partial D}{\partial P_E}dP_E + \frac{\partial^2 D}{\partial P_E^2}\frac{(dP_E)^2}{2}\,. \tag{7.17}$$

As it follows from the SDE theory:

$$(dP_E)^2 = P_E^2 \sigma_E^2 dt \tag{7.18}$$

hence

$$dD = \left(\frac{\partial D}{\partial t} + P_E \mu_E \frac{\partial D}{\partial P_E} + \frac{P_E^2 \sigma_E^2}{2}\frac{\partial^2 D}{\partial P_E^2}\right)dt + P_E \sigma_E \frac{\partial D}{\partial P_E} dW\,. \tag{7.19}$$

Assume that the liquidation reserve is decreasing with the speed, proportional to its volume:

$$d\Pi = -\alpha \Pi dt \tag{7.20}$$

where α — constant, the reciprocal value $\frac{1}{\alpha}$ is the indicative time of decreasing of the reserve e times, i.e. approximately for 63%. We may then write the formula for an optimal debt size upon the condition of absence of volatility of the reserve Π. Also, asume N is insignificantly dependent on P_E:

$$d\Pi = N dP_E - dD\,. \tag{7.21}$$

Then, by combining formulae (7.19), (7.20) and (7.21) together, we get:

$$\left(NP_E \mu_E - \frac{\partial D}{\partial t} - P_E \mu_E \frac{\partial D}{\partial P_E} - \frac{P_E^2 \sigma_E^2}{2}\frac{\partial^2 D}{\partial P_E^2}\right)dt + P_E \sigma_E \left(N - \frac{\partial D}{\partial P_E}\right)dW = -\alpha\,(NP_E - D)\,dt\,. \tag{7.22}$$

The absence of volatility means that:

$$N = \frac{\partial D}{\partial P_E}\,. \tag{7.23}$$

Using equation (7.23), we can calculate optimal debt size:

$$\frac{\partial D}{\partial t} + \frac{P_E^2 \sigma_E^2}{2} \frac{\partial^2 D}{\partial P_E^2} = \alpha P_E \frac{\partial D}{\partial P_E} - \alpha D . \tag{7.24}$$

The primary term of the equation (7.24) in partial fluxions is $D(P_E, 0) = 1$. The equation is solved numerically for the known dependance σ_E based on the historical volatility, where the optimal r can be found:

$$D = e^{rt} \Rightarrow r = \frac{lnD}{t} . \tag{7.25}$$

For an edge case occurring when $\sigma_E = const$ and the liquidation event, the solution can be achieved explicitly. Assume that the liquidation event takes place once 37% of reserve is left. It corresponds with the timeframe $\frac{1}{\alpha}$. Substituting $\frac{1}{\alpha} - t$ for τ and lnP_E for x, the final form of the equation becomes:

$$\frac{\partial D}{\partial \tau} = \frac{\sigma_E^2}{2} \frac{\partial^2 D}{\partial x} - \alpha \frac{\partial D}{\partial x} + \alpha D . \tag{7.26}$$

The solution can be sought as $D = Uexp\left(\frac{xa^2}{2} + at\left(\frac{a}{\sigma_E^2} - 1\right)\right)$. Then the problem reduces to the form:

$$\frac{\partial U}{\partial \tau} = \frac{\sigma_E^2}{2} \frac{\partial^2 U}{\partial x} \tag{7.27}$$

$$U(x, 0) = e^{-\frac{xa^2}{2}} . \tag{7.28}$$

Its solution is as follows:

$$U(x, t) = \frac{1}{\sigma_E^2 \sqrt{\pi(\frac{1}{a} - t)}} \int_{-\infty}^{+\infty} e^{-\frac{(x-s)^2}{2\sigma_E^2(\frac{1}{a}-t)} - \frac{sa^2}{2}} ds . \tag{7.29}$$

Finally, the optimal APR is as follows:

$$i = \alpha\left(\frac{a}{\sigma_E^2} - 1\right) + \frac{x\alpha^2}{2t} + \frac{1}{t} ln \frac{1}{\sigma_E^2 \sqrt{\frac{1}{\alpha} - t}} \int_{-\infty}^{+\infty} e^{-\frac{(x-s)^2}{2\sigma_E^2(\frac{1}{a}-t)} - \frac{sa^2}{2}} ds . \tag{7.30}$$

8. Risks and Attacks

Soros-style attacks. This type of attack is a speculative effort aiming to significantly destabilize exchange rate of an asset that is freely traded on the market. A malicious agent can create a downward pressure on ZIG by engaging in a CPD and immediately shorting ZIG proceeds. At the moment of CDP initiation and subsequent attack, the collateral is locked in ZigZag smart contract so that the system cannot use it as a liquidity source for exchange rate stabilization. As a result, the rate deviates from its target towards the lower bound of the allowed range of the exchange rate fluctuation threatening to breach it. If the attacker succeeds, s/he can buy underpriced ZIG then.

To prevent this type of attack, the system, as a ZIG buyer of last resort, intervenes in the market using its Liquidity and Stabilization Fund. We are developing a mathematical model to derive the sufficient amount of liquidity necessary to maintain market exchange rate close to its target at a given amount of free floating ZIG tokens.

Exchange rate fluctuations of collateralized assets. Upon the system launch EOS will be the only digital asset accepted by ZigZag as collateral. Therefore, the majority of transactions will be EOS/ZIG denominated. In base case scenario the overcollateralization of EOS guarantees stability of ZIG token as it supplies funds for ZIG buybacks. If a long-term decline in EOS price takes place, a series of liquidation events may occur. If the case, a harmful cascading effect will result in accumulation of cheap EOS in the Fund. Overcollateralization allows to mitigates this risk except for the situations when sharp drops in EOS price or any other type of black swan events occur. As a result, system balance may become negative, since the rapidly depreciating EOS reserves will not be enough to cover ZIG buybacks at 1 USD/ZIG. Moreover, EOS depreciation relative to USD may cause an increased demand for ZIG driven primarily by new market participants.

To mitigate this risk we develop a model for hedging the Fund dynamically with the instruments available on the market.

Attack of the oracles. The necessity to rely on oracles in receiving USD/EOS benchmark exchange rate serves as a potential vector of attack. A malicious agent can manipulate EOS price on the exchanges which ZigZag oracles refer to and impact ZigZag parameters. The mismatch between the economic reality and the state of ZigZag system creates an opportunity to earn riskless profit for an attacker. The entry points may differ, the vector, however, remains the same.

To ensure that oracles receive actual market data we use a number of mechanisms including but limited to: diversification of independent centralized and decentralized data feeds, statistical test of legitimacy of the obtained exchange rates and discrete reassessments of the reference price so that temporary deviations do not trigger stabilization mechanisms.

Miscellaneous manipulations. Market participants are usually skeptical about the ability of the system that governs the stablecoin to maintain a stable exchange rate and mitigate any manipulations. The risk of manipulation is particularly high in the early stages of its development when liquidity is low and the project has not earned the trust of market participants. At this time any deviation of the market exchange rate from its target causes crisis of confidence and drives contraction in demand for the stablecoin regardless of its reasons. ZigZag team mitigates this risk by accumulating enough liquidity in the Fund through fundraising and agreements with liquidity service providers.