Y2K Finance: Exotic Peg Markets

@neworderDAO (@0xdrej
@0xSami), @dcfintern, @slumdogy2k, @badquant1

July 2022

Abstract

Y2K is a crypto-native take on structured products on-chain , the protocol provides exotic peg markets which allow users to hedge, leverage, speculate and trade the different components of pegged assets. The protocol launches with 2 different products Earthquake, a 4626 vault allowing users to take risk or hedge against a potential peg deviation , and Tsunami, a liquidation wrapper and aggregator that redefines how collateral auctions for bad debt are conducted.

1 Introduction

The advent of stablecoins, token wrappers and liquid staking derivatives has offered crypto investors a delta-neutral alternative to transacting, storing value, and earning yield on passive investments. In the infancy of decentralized finance, there were only two types of stablecoins: asset-backed, and fiat-backed. These products opened the door to a new type of legitimization in the space, where market participants could take advantage of both the stability of traditional currencies and the benefits of decentralization. As the market for these pegged assets matured, however, new types of products began to appear with a variety of features, marketing themselves as stable assets - some of which are not even pegged to fiat currency.

In an environment where users are offered an innovative and experimental twist on what is allegedly the "safest" asset class in the crypto marketplace, we need to create fair markets to gauge how stable these assets really are. Market participants should be given the option to hedge, speculate, long, and short these various pegged asset architectures.

This paper introduces Y2K Finance, a novel, programmable peg exotic market. Y2K offers a wide range of market participants (including DAOs, institutional investors, and retail traders) a way of gaining exposure to the constantly-evolving pegged asset market by redefining catastrophe (CAT) bonds to a DeFi native setting. A CAT bond is a financial instrument that pays the issuer when a predefined disaster risk is realized, such as hurricanes or earthquakes, or, in this case, a depeg event.

Y2K offers users an alternative to traditional hedge vehicles like money-market borrows or DeFi insurance markets and allows risk to be transferred to a larger set of market participants with a focus on capital efficiency. Unlike traditional insurance where it is possible for the issuer to fail to pay out following a loss event, y2kTokens are over-collateralized structured products with payouts guaranteed on-chain through Chainlink price oracles.

2 How it Works

We define a risk position as a deposit of ETH in one of two types of vaults, which are implemented using the ERC4626 standard: "Premium" vaults, and "Collateral" vaults. A user can "purchase" coverage on a stablecoin depegging event by depositing to the Premium vault, and can similarly "sell" risk by depositing funds in the Collateral vault. Each pair of vaults is designed with the following properties:

- Pegged Asset: the stablecoin, token wrapper, liquid staking derivative for which risk is being traded,
- Epoch: the start and end date of the vault, and
- Strike: how far a coin's price needs to deviate from its peg in order to trigger a liquidation event.

Market participants can deposit into Y2K vaults at any time before the epoch start date, after which funds are locked for the duration of the epoch. A Chainlink oracle is used to monitor token prices, and in the event of a depegging, the contents of the collateral vault are liquidated and awarded to the coverage buyers. In the event of no depegging over the course of a vault's epoch, both premium and collateral payments are delivered to the risk sellers. It should be noted that insurance sellers receive premiums regardless of whether there was a liquidation event, and all cash-flows occur at the end of the epoch.

In an efficient market, the "yield" generated from depositing in either of these vaults should be reflective of the pegged assets risk. This means that riskier asset contracts should have a higher proportion of ETH in Premium vaults, otherwise arbitrage opportunities would present themselves. Naturally, some uncertainty arises when the vaults are empty - the first depositors have limited knowledge of how many funds there will be on the opposite side of the trade, as well as how much their position may be "diluted" as others join the same vault. In order to compensate initial depositors for this information asymmetry, they will receive rewards boosted rewards decided by a bonding curve tracking each vaults TVL, encouraging deposits in the infancy of an epoch and solving the chicken-and-egg problem that arises with most structured product markets.

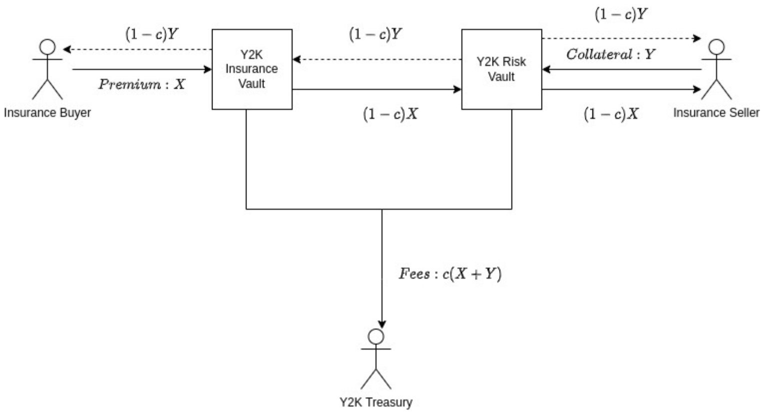


Figure 1: Cashflow diagram

3 Payout Calculations

This section outlines the methodology via which payouts are calculated for either side of the transaction. We define the following variables:

- B_i is the premium paid by each user hedging,
- S_j is the collateral posted by each user seeking risk,
- N_B is the number of hedge buyers,
- N_S is the number of risk sellers, and
- c is the trading fee taken by the protocol.

In the event of no depegging event,

- Each buyer i pays B_i, and does not receive anything
- Each seller j receives $\frac{S_j}{\sum_{k\in N_S} S_k} \sum_{k\in N_B} B_k(1-c)$, in addition to the return of their collateral.

In the event of a depegging event,

- Each buyer i net receives $\frac{(1-c)B_i}{\sum_{k\in N_B} B_k} \sum_{k\in N_S} S_k - B_i$
- Each seller j net pays $S_j - \frac{(1-c)S_j}{\sum_{k\in N_S} S_k} \sum_{k\in N_B} B_k$.

3.1 A Numerical Example

We let $B_1 = 1, B_2 = 3, S_1 = 150, S_2 = 200, S_3 = 50, c = 0.005$. It is clear that, before accounting for trading fees, the yield in this scenario for a single epoch is 1%.

In the event of no depegging event,

- Buyer 1 pays 1 ETH,
- Buyer 2 pays 3 ETH,
- Seller 1 receives $1.5 \times 99.5\%$ ETH,
- Seller 2 receives $2 \times 99.5\%$ ETH, and
- Seller 3 receives $0.5 \times 99.5\%$ ETH.

In the event of a depegging event,

- Buyer 1 pays 1 ETH and receives 100 ETH, leaving him with $(100 \times 99.5\% - 1)$ ETH,
- Buyer 2 pays 3 ETH and receives 300 ETH, leaving him with $(300 \times 99.5\% - 3)$ ETH,
- Seller 1 receives 1.5 ETH and pays 150 ETH, leaving him with $(-150 + 1.5 \times 99.5\%)$ ETH,
- Seller 2 receives 2 ETH and pays 200 ETH, leaving him with $(-200 + 2 \times 99.5\%)$ ETH, and
- Seller 3 receives 0.5 ETH and pays 50 ETH, leaving him with $(-50 + 0.5 \times 99.5\%)$ ETH.

4 A Methodology for Determining Strikes

Y2K Finance aims to eventually expand to provide insurance markets for various different pegged asset markets. Here we provide a sample methodology for determining strike prices, which someone may seek to use when creating new Y2K vaults. At genesis, Y2K epochs will assigned on a per-month basis; that is to say, there will be a July epoch, August epoch, September epoch, etc. This is subject to change according to protocol governance votes.

The methodology presented below is for a stablecoin pegged to 1 USD. In this framework, we assign three strikes to each stablecoin:

- K_1 is the riskiest strike, which is expected to be breached every 3 months.
- K_2 is a “medium risk” strike, which is defined as being breached every 18 months.
- K_3 is a “low risk” strike, which denotes black swan events. These are the lowest yielding but provide protection against events that are unexpected to ever occur over the lifetime of a stablecoin.

We assume that price deviations from \$1 are independent and identically distributed random variables,

$$X_i \equiv X(s_i) = |s_i - 1| \times 10^4$$

where s_i is the stable coin price at a given time t_i. It is well known that in times of mass decollateralization spirals, these variables become correlated and the i.i.d. assumption above does not hold. We deal with this by assuming that the discrete time series of stablecoin prices is sampled from a "continuous" (block-by-block) series $\hat{S}$,

$$s_i = \{\hat{s_j} \in \hat{S} | \max_{\hat{s_j} \in \hat{S}} X_i\}$$

where we assume that any correlation spirals happen within each interval $\Delta t = t_i - t_{i-1}$.

Each strike $K_{k \in \{1,2,3\}}$ has an associated rate r_k, which is defined as the probability that the strike is breached within a given Δt. The rate is calculated using an indicator function from the discrete time series $S = \cup s_i$, as

$$r_k = \sum_{i=1}^{n} \frac{1_{X_i > K_k}}{n}$$

and can be used in a binomial distribution to find the probability P_k of a particular strike being breached within a given month:

$$P_k = (1 - r_k)^{d \times f}$$

where f is the sampling frequency and d is the number of days in a given epoch.

The equation above is then solved for each r_k on the interval $(0, 1) \in \mathbb{R}$ given the desired values of P_k. This can be done using a variety of root finding algorithms. Once r_k is determined, the set of all X_i can be iterated through for varying strikes until an appropriate K is found.

For the cases K_1 and K_2, each P_k, respectively, is $\frac{1}{3}$ and $\frac{1}{18}$.

5 Example Pricing Model

In this section an example is provided for someone who may wish to build a pricing model for a given stablecoin contract. It is important to note that this is not a definitive pricing model, and is only being provided for illustrative purposes. Individual market participants looking to build arbitrage models for these contracts are encouraged to use realistic assumptions that are directly relevant to the particular stablecoin's dynamics.

We will include the effect of trading fees on risk-neutral pricing, which we will denote with the variable c.

Using ϕ_k to denote the proportion of hedge purchased for a given strike in a given epoch, the return for "selling" risk can be shown as

$$APR_k = 12 \times \left(\frac{1-c}{1-\phi_k} \right),$$

and in order for a no-arbitrage environment, we must have the relation

$$P_k = \frac{\phi_k}{1-c}.$$

It should be noted that although the APR for selling risk may seem quite high, there is always a probability P_k of the seller's entire position being liquidated.

In order to determine P_k, we must first understand the distribution of the random variable X. For this analysis, we consider the stablecoin DAI and use a time series of hourly prices on Bitfinex ranging from 1-Jan-2021 to 26-Apr-2022. This time series can be found in Figure 2.

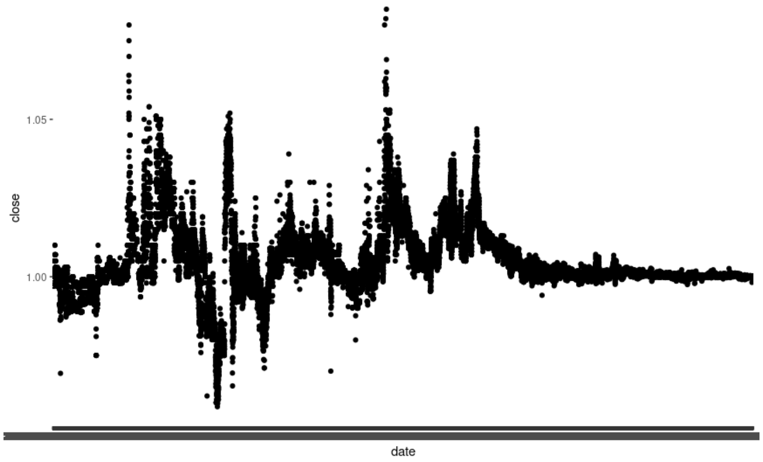


Figure 2: DAI Deviations

A cleaner way to look at this data is to denote it using the deviations X_i described in the previous section. This is seen in Figure 3.

Visually, from Figure 3, it is evident that these price movements follow a distribution that exhibits some sort of exponential decay. This is also intuitively perceived due to the nature of the stablecoin's mechanics continuously forcing its price to be as close to the peg as possible. What we aim to understand further is the behaviour of the distribution in the tail, as this is the area of concern when it comes to strike prices being breached.

The two distributions above are fitted using maximum likelihood estimates, and it is evident from the Q-Q plot in Figure 4 that the Weibull distribution massively over-estimates tail events. The figure below gives a closer look at the gamma distribution fit.

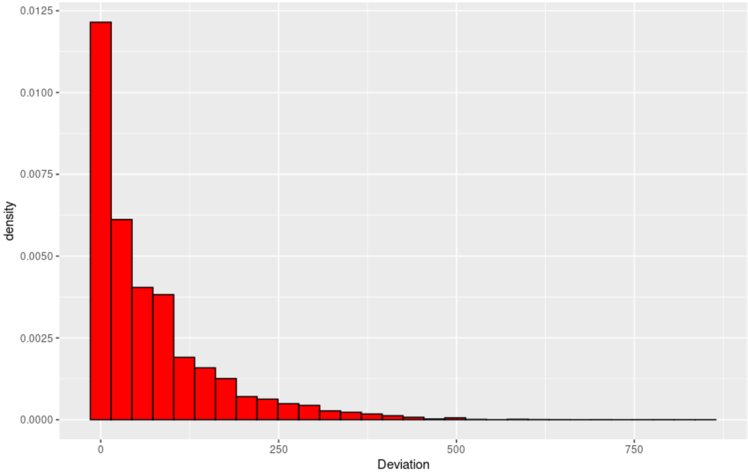


Figure 3: Distribution of DAI Deviations

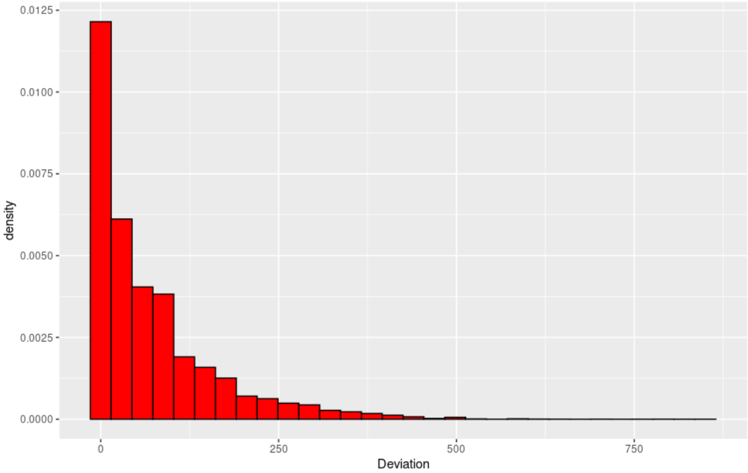
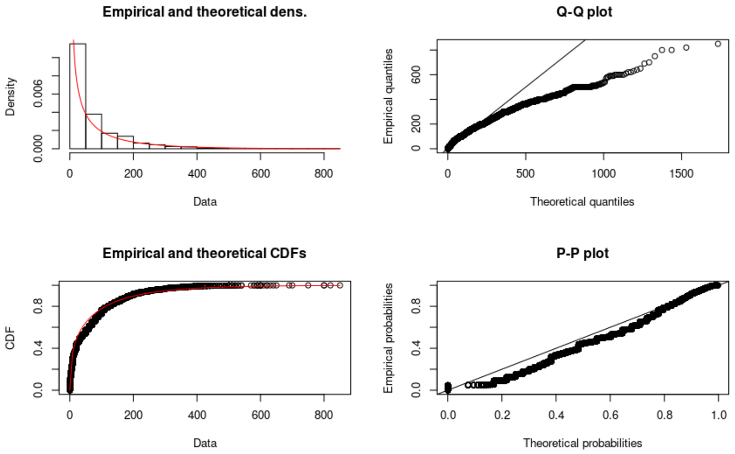


Figure 4: Goodness of fit for Weibull and gamma distributions

It can be seen that the CDF in Figure 5 fits the data quite well. All that's left now is to measure the uncertainty in its parameters. This can be done using a parametric bootstrapping technique, which yields the following results:

```
Parametric bootstrap medians and 95% percentile CI
Median        2.5%       97.5%
shape 0.357186307 0.352383384 0.360546837
rate  0.005059954 0.004985465 0.005147282
```

The CDF will be denoted as follows:


Empirical and theoretical dens.

Q-Q plot

Empirical and theoretical CDFs

P-P plot

Figure 5: Summary of gamma distribution fit

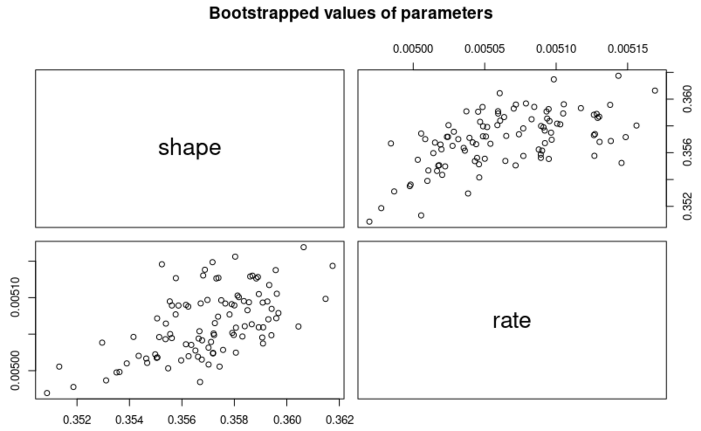

Bootstrapped values of parameters

Figure 6: Bootstrapping of gamma distribution parameters

$$\Psi(K) = P(X_i \leq K) = \frac{1}{\Gamma(\alpha)}\gamma\left(\alpha, \frac{K}{\theta}\right),$$

where α and θ^{-1} the shape and rate parameters of the gamma distribution, respectively.

Recall from the previous section that P_k represents the probability of a strike being breached in a given month. We now define the rate at which strikes being breached occurs monthly as follows:

$$\lambda(K) = (1 - \Psi(K))\frac{d}{\Delta t}$$

and P_k can be found with a Poisson distribution:

$$P_k = 1 - e^{-\lambda}.$$

6 Wildfire - Semi-Fungible Token Exchange

Y2K Finance includes a novel central limit orderbook on Arbitrum for trading depeg positions after the deposit period before an epoch ends. These positions are traded as semi-fungible tokens that are redeemable for a fraction of the deposits from the collateral vault in case of a depegging. This allows traders to speculate and profit on depegging sentiment in a secondary market without needing to lock in their positions. Tokenizing vault positions also gives initial depositors the option to take profits or stop out of positions.

7 Roadmap

The protocol will launch in seven markets: DAI, USDC, FEI, MIM, stETH*, wBTC and FRAX. Shortly after launch, use-cases and functionality will be expanded to the following niches:

- Multichain stablecoins
- Rebasing mechanisms to prevent position dilution in each vault
- CDOs
- Peg arbitrage vaults
- Ability to lend semi-fungible risk tokens (for leverage and short-selling)
- Auto-compounding of Y2K hedge deposits

In addition to the main product Y2K product (branded under the name "Earthquake"), the product suite will be extended to include "Tsunami", which aims to move further down the supply chain of pegged asset markets. This product will take advantage and ownership of the debt that backs many of these assets.

Tsunami adopts a GLP-like product where collateral is pooled from various liquidity providers into a host liquidity pool, which provides users with a mechanism for aggregation of debt positions in multiple lending agreements. These aggregated agreements will be represented by Collateral-Debt Obligation ("CDO") NFT tokens.

Users who provide liquidity to the CDO NFT have exclusive access to the liquidation bot, where in the event of a leveraged position being liquidated, the yield generated by the liquidation event is passed on to them and is added to the yield they are already earning. With Tsunami, the host liquidity pool itself represents a dedicated loan underwriter that monitors, facilitates, and liquidates loan positions.

When collateral nears liquidation, the protocol uses ETH from the y2kTOKENS as a backstop to make sure collateralization always remains above 110%. While the y2kTOKEN backstop capital is deployed, the user's CDO NFT enters an auction house, where the CDO pool liquidated them privately in a sealed bid, off chain collateral repossession.

If the user cannot post the necessary collateral, the position will be liquidated by the protocol; however, since the position is routed through a private vault separate from the public mempool, a part of the profit from the liquidation event will be returned to the user; this attracts them to borrow from Y2K and not from the providers directly. CDOs will be in the form of NFT (ERC-1155 tokens), allowing positions to be easily transferred between different addresses and maintaining composability with other agreements.