Whitepaper Rough Draft

August 2022

1 Problem Statement

We present a mechanism for decentralized risk underwriting and instantiate an application in the context of unsecured lending and asset management.

2 Protocol Design

2.1 Glossary

- vt: Vault token inherited from the ERC4626 standard, attached to multiple *instruments*.
- ZCB: Acronym for zero coupon bond
- longZCB: a tokenized long position on ZCB
- shortZCB: a tokenized short position on ZCB
- Instruments: Any risk-definable single-sided yield-bearing position. Represented by either a `creditline` or a `stategy` contract
- Reputation: A proxy of a manager's risk assessment capability. Updated at the completion of each instrument's cycle.
- Proposal Parameters: The parameters
    1. Principal:
    2. Expected Yield: The predetermined expected payoff proposed by the utilizer; i.e total accrued interest, LP trading fees. This could take the form of either fixed or variable rates.
- Notations
    1. P: principal
    2. I: Interest in notional value

3. c: total supply of ZCB
4. R: price function of ZCB, the parameter being c
5. α: Insurance parameter in the domain $0 \leq \alpha \leq 1$. This is the only predefined parameter in the system.

2.2 Protocol Agents

2.2.1 Utilizer

These are agents that request and *utilize* liquidity. They could take the form of strategists, borrowers, etc. They *propose* potential instruments. By doing so, they generate a new prediction market. They are also responsible for the deployment of the instrument contract. They have the choice to deploy a pre-written contract(`creditline`) or their custom development(strategy).

2.2.2 Liquidity Providers (Senior LP)

These are passive vault token(vt) holders, claiming a senior(fixed-rate, protected) position to all instruments attached to vt. They mint vt to invest.

These passive vt holders can participate in the assessment of the instrument via (only)short selling in the prediction market. This allows them to hedge their exposure to the instrument in the event that it gets approved. As the prediction market's collateral is vt, their losses in vt will be offset by the increase in the exchange rate of vt/it's underlying(e.g usdc) when the instrument successfully delivers.

2.2.3 Managers (Junior LP)

These are active vault token(vt) holders, claiming a junior(variable-rate, first-loss) position to all instruments attached to vt. They are responsible for assessing the risk of added instruments. These agents a) would provide proof of humanity as a means of preventing Sybil attacks(e.g disguising as utilizers) b) holds a unique *reputation* score. The verification process is specified in the specification section.

These verified vt holders can participate in the assessment of the instrument via trading in the prediction market. If they deem the underlying instrument to have a favorable risk-reward profile they will purchase a `longZCB` to leverage up their exposure. This position is junior as, at maturity, redemption prices of the `longZCB` are set such that they absorb all the return volatility that deviates from the expected yield.

Essentially, this mechanism entails that, for a particular instrument, assessment is conducted through identifying *if there are more people willing to leverage their exposure than there are people trying to hedge their exposure.*

2.2.4 Validators

These are randomly(weighted by each's *reputation*) chosen managers whose primary goal is to a) identify the risk of the potential instrument at a systemic level (ensure low correlation among existing instruments) b)identify any malicious behavior (such as collusion with managers and utilizers). These validators are required to purchase longZCB at a discount to mark price to make an approval decision.

2.3 Protocol Flow

A high level life-cycle of an instrument is shown below

1. Proposal: A utilizer i submits a proposal to vault with the necessary parameters, and a prediction market is generated. New $\texttt{longZCB}_i$, $\texttt{shortZCB}_i$ tokens for the underlying instrument are deployed. (Each market, utilizer, tokens, instrument are all indexed with the same `marketId` i)

2. Assessment: Managers who deem that the instrument has a favorable risk-reward profile buy $\texttt{longZCB}_i$ from this newly created market. Any vt holders who deem that the instrument is too risky can choose to opt out of the potential returns by short selling the risk. When the cumulative area under the curve exceeds a threshold αP_i(sufficient net longs), `canbeApproved` returns true.

3. Approval: When `canbeApproved` the validator can approve the instrument. Liquidity will then be directed from the vault to the instrument. When !`canbeApproved` for a prolonged amount of time the market would automatically close and all participants will redeem their ZCB for their collateral.

4. Maturity: Redemption price for the ZCB tokens will be computed based on the contrast between realized returns vs expected returns from i's proposal, after which any ZCB holders can redeem from this price. (details for redemption prices in section 4). Reputation scores for the managers who participated in the assessment phase are also updated. Liquidity is withdrawn from the instrument contract back to the vault, and all additional accounting logic takes place.

3 Bonding Curve

We choose a bonding curve as the AMM for our prediction market primarily due to its versatility(can easily incorporate different curves optimized for different incentive structures), automated liquidity provision, and intuitive mathematical properties. Its detachment to a requirement of exogenous liquidity provision as is necessitated in a CP/CS invariant-based AMM allows participants to take a

long or short position without a counterparty.

Our bonding curve is designed with the following considerations

1. It should act to align the manager's economic incentives with the Senior LP. Also, the participating managers should not be allowed to easily "pool and securitize" and off-load their risk positions.

2. It should promote diversity, so as to mitigate homogeneity of opinions and variance in error.

3. It should be versatile enough to be tailored for each utilizer parameters(principal, expected yield, maturity dates) in a permissionless manner.

In light of these features, the curve $R : \mathbf{R} \mapsto \mathbf{R}$ should be a monotonically increasing function initialized with a positive y-intercept, with the maximum quantity $\hat{c}$ set such that the $R(\hat{c}) = 1$. An example of such curve is the affine function

$$R(c) = ac + b$$

with $0 \leq a, b \leq 1$. These parameters are determined analytically with the sole inputs being P_i and I_i of the instrument proposed by i. A derivation instance for the affine function is presented in section 4.

The AMM will have two tradeable units; for each utilizer i, a $\texttt{longZCB}_i$ and a $\texttt{shortZCB}_i$, (the pay-off of a $\texttt{shortZCB}_i$ token is designed to be similar to that of a credit default swap). For a fixed rate instrument, the mark/redemption price of both of these units are bounded in the range $0 \leq \text{price(ZCB)} \leq 1$, denominated in Vault Tokens(VT), and price of $\texttt{longZCB}_i$ is always equal to $1-\text{price}(\texttt{longZCB}_i)$. For example, a $\texttt{longZCB}_i$ token bought at 0.84vt per contract should be redeemable for 1vt at maturity, if the underlying instrument successfully delivers it's expected yield, and the $\texttt{shortZCB}_i$ token which could have been bought at 0.16 USD would be worth 0.(Note that the bonding curve supply is that of $\texttt{longZCB}_i$, and the $\texttt{shortZCB}_i$ token is merely a tokenized representation of debt/sell position.)

The included figure 1 provides an illustration of a curve, the initial output of the function starts at b and ends at 1. The x-axis at any given point represents the total supply of $\texttt{longZCB}_i$ minted, and the y axis its price.

The following areas represent:

- **Yellow Area**: The amount of collateral from net longs and the maximum profit for $\texttt{shortZCB}_i$ holders. Used as first loss capital.

- **Blue Area**: The maximum profit for $\texttt{longZCB}_i$ holders when the underlying instrument returns a fixed rate. For a variable rate, a *targeted* expected profit for the managers.

- **Dashed Area**: The amount of additional profit for $\texttt{longZCB}_i$ holders when the underlying instrument returns a variable rate and the instrument delivers excess returns.
- **Green Area**: Profit returned to senior LPs(passive vt holders). This profit would be distributed implicitly via increasing the exchange rate of the vt/usd.
- **Yellow + Dark Area**: P_i, the total principal for instrument i
- **Blue + Green Area** : I_i, the notional value of expected yield to be gained from the instrument.
- **Blue + Green Area + Dashed Line**: The notional value of realized returns from the instrument.
- **Total Area of Square**: $P_i + I_i$

We use the term α as a parameter that signifies a notion of the maximum management fee/ minimum insurance for the underlying instrument. A higher α would guarantee more protection for vt holders, at the expense of lowering risk/reward for managers who push up the marginal price, while decreasing profit returned to vt holders.

3.0.1 Identifying and Dealing with different management Skills

Each manager will have a varying degree of sophistication and tools at their disposal for judging the risk/reward-profile of the instrument. A prediction market with the sole purpose of efficiently aggregating opinions should take into consideration their different management capabilities, albeit not at the expense of diversity(recall that diversity is necessary for, in expectation, the grouped prediction to be more accurate than the smartest individual in the group). We do this by introducing a *reputation* system, an indicator of the manager's track record. The reputation score(rep) for managers is updated at the maturity dates for the instrument, where we present an example increment/decrement scheme in the appendix.

A reputation score system then allows us to weigh the managers through the following mechanism.

- Only those with high reputation scores can participate early in the bonding curve: This serves two purposes, a)It presents an equitable rewarding system that scales with each's skill b)The market only proceeds when the earliest managers deem the instrument worthy.
- Budget: A budget is a maximum quantity a trader can buy/sell in the prediction market. We design the budget of a manager to be an output of a monotonically increasing function of reputation. Clearly, this would serve as a direct mechanism for weighing more on those with higher scores.

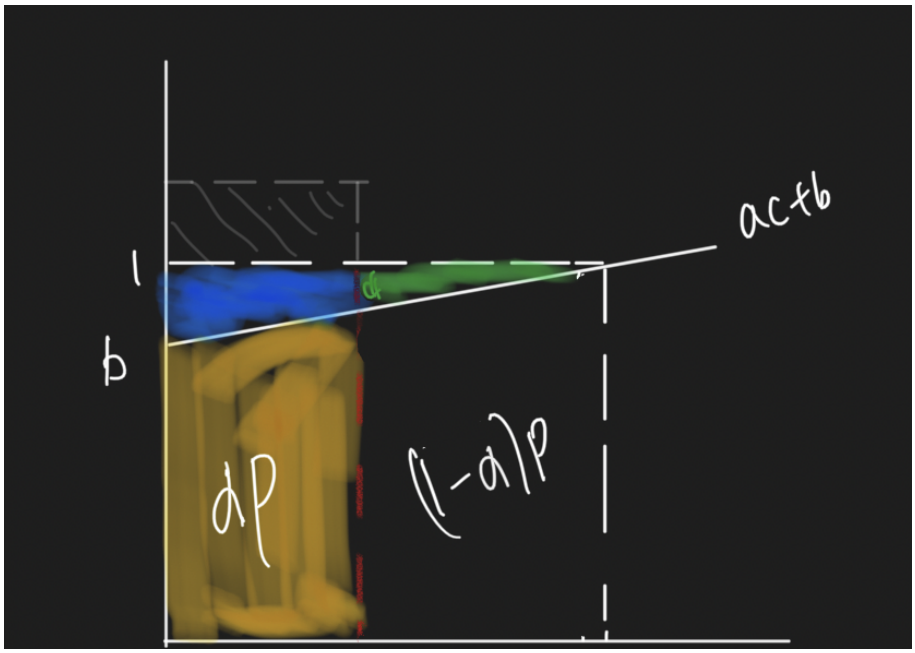

Figure 1: An example Bonding Curve for a given instrument. As with all other bonding curves X-axis measures supply and Y-axis measures price. Traders *buy up* the curve and *sell down* the curve

3.0.2 Market Phases

Assessment Phase: An assessment phase ascribes a period where only the managers are allowed to purchase $\texttt{longZCB}_i$(Recall that managers are anti-sybil verified entities, as we want the market to reflect many opinions when approving risky instruments), This phase begins whenever a new instrument is proposed by the utilizer, and is separated into two phases; a period where only those with a reputation score above a threshold can participate followed by a period where all managers can participate. Whereas these anti-sybil restrictions are set for $\texttt{longZCB}_i$ buys, any VT can purchase $\texttt{shortZCB}_i$ tokens to hedge their exposure. Assessment period ends when the validator either approves the market or when the market is denied. `approvalCriterion` is met when net $\texttt{longZCB}_i$ collateral is larger than the αP.

Post Assessment Phase: After the assessment phase, anyone can trade in the market if the instrument is approved, with the following conditions;

- Upper/Lower bound on the supply of $\texttt{longZCB}_i$: Setting the upper bound is equivalent to setting the minimum profit for passive vt holders. The lower bound is set to ensure minimum insurance in outcomes that results in principal loss.
- Selling Fee: The selling fee is set to a) disincentivize immediate risk sharing/transfer from the managers and b) incentivize potential short-sellers to short during the assessment phase. Selling Fee will taper off and converge to 0 as the underlying instrument approaches maturity.

3.0.3 Difference between a constant price ZCB

An increasing bonding curve as opposed to a constant curve(note that the risk assessment system in Nexus Mutual can be seen as an anti-protection market with a constant bonding curve) provides the following benefits:

1. Mitigates information cascades: With more managers buying $\texttt{longZCB}_i$ the marginal cost of $\texttt{longZCB}_i$ increases while that of $\texttt{shortZCB}_i$ decreases, making the cost of hedges increasingly more attractive. While in a constant bonding curve the system is susceptible to an instance with a trivial solution where the group imitates the smartest/earliest risk-takers, an increasing function allows increased diversity and thus the inclusion of more information.
2. Rewarding System: Allowing managers with higher reputation to buy at a discount is an equitable mechanism that transfers value to those with skills from those yet to prove themselves.
3. Short-Selling functionalities: Allowing shorting ZCBs allow any vt holder to hedge the precise amount of exposure they would incur as a shareholder when the instrument is approved. Along with extra diversity, this allows

LPs to voice out disagreements on the risk-reward profile of the underlying investment, and opt out of the risk.

3.0.4 Vaults

Vault Token(vt) is the base unit for all the ZCB markets. Essentially, a VT represents a senior tranche position, and buying $\texttt{longZCB}_i$ for each instrument with VT is equivalent to swapping a senior position to a junior position and levering up the yield. At maturity, these $\texttt{longZCB}_i$ will either be redeemed with more or less VT. This is more capital efficient than using exogenous collateral for insurance, as it functions solely from the transfer of value between participants.

4 Specifications

4.0.1 Initial Curve Parameters

1. Linear Curves: Noting the following three conditions

- $\int_0^c R(c)dc = \frac{ac^2}{2} + bc = P$
- $c = P + I$
- $c = \frac{1-b}{a}$

Solving for a and b yields

$$b = \frac{2P}{P+I} - 1, a = \frac{1-b}{P+I}$$

4.0.2 Shorting

We provide shorting functionalities with an ERC20 representation of the debt+sell position. A user looking to hedge/speculate will mint $\texttt{shortZCB}_i$ tokens with price 1− price of $\texttt{longZCB}_i$. These short tokens would be eligible for redemption at maturity.

4.0.3 Redemption Price

The redemption price for a ZCB is determined from the following observations

1. Bond holders claim a junior tranche position, which entails that they are required to primarily pay out the senior fixed rates if the realized yield is lower than the fixed rate.

2. Since the bonding curve AMM allows shorting through borrowing and selling down the curve, the collateral presented by the short sellers(which is default set at 1USD per zcb borrowed) may not be enough to fully compensate the lender when the underlying instrument is holding a variable yield position and the realized yield is higher than the expected yield.

We thus arrive at the following zcb redemption price ω_i for instrument i at maturity;

$$\omega_i = \begin{cases} 1 + \frac{\lambda_i}{\hat{c}+c_s}, & \text{if } \lambda_i > 0 \\ \max((1 + \frac{\lambda_i}{\hat{c}}), 0), & \text{otherwise} \end{cases}$$

where λ_i and c_s denotes the excess (either positive or negative) variable return in relation to the expected yield, and the number of short-sold zcb, respectively.

Consequently, the redemption price for a short-ZCB token(an ERC-20 representation of the debt/sell position) is $\max(1 - \omega_i, 0)$.

4.0.4 Solvency Proof

Although the above redemption price can be derived solely from intuition we support it with some algebra for added confidence. Precisely, we show the system will remain solvent after paying all the longs and shorts. We need to show that

$$\text{ValueIn} := V_{in} = V_{out} := \text{ValueOut}$$

where ValueIn, the combined value of total collateral and profit from underlying instrument

V_{in} = Long Collateral+Profit from Instrument+Short Collateral+Sells stored in shortZCB

$$= (\alpha P) + (C - \alpha P + \lambda) + (C_s R_s) + ((1 - R_s)C_s)$$
$$= \lambda + C + C_s$$

Where for ValueOut, the total redeemed value

V_{out} = LongZCB Redemption Price$*$LongZCB Supply+shortZCB Redemption Price$*$ShortZCB Supply

$$= \omega_i C_l + \max(1 - \omega_i, 0)C_s$$
$$= \omega_i(C_s + C) + \max(1 - \omega_i, 0)C_s$$

Realizing that $C = C_l - C_s$. Now when $\lambda_i > 0$ we have $\omega \geq 1$ and thus substituting the predefined redemption weights

$$V_{out} = (1 + \frac{\lambda_i}{C + C_s})(C_s + C) + 0 = C_s + C + \lambda_i = V_{in}$$

and when $\lambda_i \leq 0$

$$V_{out} = (1 + \frac{\lambda_i}{C})(C_s + C) + (1 - (1 + \frac{\lambda_i}{C}))C_s = C_s + C + \lambda_i = V_{in}$$

4.1 Mangers' Beliefs and Reputation

We henceforth denote p_j as the subjective probability of survival for the instrument of concern by manager j.

4.1.1 Deriving Individual Implied Probability of Survival

We consider a simple model where each ZCB is redeemable for 1USD if the underlying instrument succeeds to deliver its promised yield or 0 otherwise(in the case of default). Under the assumption of risk neutrality each managers j's expected log utility can be modeled as follows:

$$\mathbf{E}[U] = p_j log(a_j + (1 - R_j)x_j) + (1 - p_j)(a_j - R_j x_j)$$

where $R_j := \frac{\int_{c_j}^{c_{j+1}} R(c)dc}{c_{j+1} - c_j}$ is the average price for trader j's paid to increment total supply from c_j to c_{j+1}. First order conditions allows us to represent the *implied probability* of j as follows:

$$p_j = \frac{x_j}{a_j} R_j(1 - R_j) + R_j$$

We can then compute, for each managers, the subjective probability of survival for every instrument.

4.1.2 Reputation and Budget

Each manager is associated with his reputation score ρ_j, stored in a non-transferable NFT. When a manager j participates in the assessment phase of instrument i, his reputation score will be updated at maturity of i, based on the actual outcome and his confidence in the outcome.

At each maturity manager j 's reputation will be updated as the following. Using the same definitions, If correct:

$$\rho_j += \frac{x_j R_j}{a_j}(1 - R_j)x_j R_j$$

If incorrect:

$$\rho_j -= \frac{x_j R_j}{a_j}(R_j)x_j R_j$$

Budget a_j is the output of a monotononically increasing function of ρ_j, as a means of weighing managers with higher reputation more.