Risk AMM whitepaper Draft

RAMM

February 2023

1 Problem Statement

We continually observe that risk assessment systems serve to be the primary failure mode in capital markets, and argue that its decentralized variant eliminates the problems that arise from moral hazard and incentive misalignment.

Although it is questionable whether the cyclical nature of credit markets can be completely avoided, it is mostly the liquidity providers that bear the loss from irresponsible assessments during times of excess liquidity. Prevailing decentralized systems either can't price risk and only resort to centralization(where developers act as managers) or trivial systems such as collateralized lending with liquid collateral. However, a vibrant capital market needs a method that can define and assess arbitrary forms of risk.

Thereby we present a mechanism for decentralized underwriting and instantiate several applications in the context of asset management in DeFi. We propose a general and automated system that allows it to permissionlessly instantiate capital markets and appropriately distribute value between assessors and LPs.

We draw inspiration from the various results presented in ensemble models and prediction market literature to argue that decentralization in underwriting, with an attack-resilient mechanism for aggregating private information and alligning incentives, not only exhibit values in the ethos it presents but can be strictly better than its centralized counterparts from a practical accuracy perspective.

2 Protocol Design

We propose a system that is general and simple. At a high level, the system requires 3 parties; a utilizer who *demands* liquidity, an investor who *supplies* liquidity, and managers/validators who prices the equilibrium. The protocol flow can be distilled down to the following.

A `utilizer` proposes a new investment opportunity `Instrument`. Each $\texttt{Vault}_i$ is connected and exposed to multiple $\texttt{Instrument}_{ij}$, and whether liquidity is supplied to each $\texttt{Instrument}_{ij}$ from $\texttt{Vault}_i$ will be determined by a decentralized risk-assessment module. The module primarily involves two parties; managers who wants *levered* exposure to $\texttt{Instrument}_{ij}$, and $\texttt{Vault}_i$ investors who wants *protection* from exposure to $\texttt{Instrument}_{ij}$. The summation of these two market forces determines whether $\texttt{Instrument}_{ij}$ is trusted and liquidity is provided to $\texttt{Instrument}_{ij}$ from $\texttt{Vault}_i$.

2.1 Key terms

- VT: Shorthand term for RAMM Vaults attached and exposed to multiple instruments.
- Instruments: Any risk-definable financial asset programmed to a contract. Could take the form of, but not limited to, cash flow generating assets such as debt, lending pool supply positions, volatility selling positions, AMM LP positions, or even logic that simply buys and hold financial assets.
- `longZCB`: a tokenized long position in (synthetic) bonds for an instrument. These are concentrated and junior bets on an instrument, while VT is a passive and senior investment on a pool of instruments. Managers buy them for instruments they deem to have an investable risk reward profile. They are programmed such that purchaser's collateral would be used as first loss capital. Its synthetic nature stems from its arbitrary scaling of open interest given a counterparty.
- `shortZCB`: a tokenized short position on synthetic bonds for an instrument. It's payoff is opposite to that of `longZCB` tokens.
- Reputation: A proxy of a manager's risk assessment capability. Updated at the completion of each instrument's cycle.

2.2 Protocol Agents

2.2.1 Utilizer

These are agents that request and utilize liquidity. They could take the form of strategists, borrowers, market makers, etc. They first *propose* potential instruments. By doing so, they generate a new prediction market and deploy a new instrument contract(inherited from the protocol's base class).

2.2.2 Liquidity Providers

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, and in doing so they gain passive exposure to a wide set of instruments.

While these are passive investors, they have the ability to fine-tune their exposure levels to an instrument via an AMM. They can participate in the assessment of an instrument via (only) short-selling the instrument's ZCB(by buying `shortZCB`) in the prediction market. They would do so if they don't want to be exposed to the underlying instrument while still being invested in the parent VT. After its approval, they can buy either `longZCB` or `shortZCB` from a counterparty based on their risk appetite on the instrument.

2.2.3 Managers

These agents are responsible for assessing the risk of to be added instruments by claiming a junior(leveraged, first-loss) position to the said instrument. They do so by buying `longZCB` in the instrument's prediction market during the assessment phase. Redemption prices of `longZCB` are set such that they represent leveraged exposure to an instrument and absorb all the return volatility that deviates from the proposed fixed returns.

These agents are characterized by a *reputation* score, which increases when their longZCB was profitable and decreases when it was not(the incrementing system also takes into account the manager's confidence, which can be computed from the amount purchased). The reputation system acknowledges the non-uniformity of risk/reward assessment skills and gives rise to a more equitable value distribution mechanism. A higher reputation allows a manager to acquire more leverage and get better prices when purchasing longZCB which in turn allows them to be more profitable per capital spent. Higher reputation also grants them a heavier weight when aggregating decisions in the prediction market through increased leverage and budget.

In traditional finance managers usually are rewarded with asymmetric compensations, where the convexity of reward structures allows them to undermine the risk of an instrument. In the proposed system they would instead share the same linear pay-off as that of LPs, but one that is amplified and becomes more capital efficient with their reputation.

These managers can also act as a utilizer and propose a profit-seeking endeavor by proposing an instrument(which deploys an AMM) and buying longZCB. In this instance, other managers would have to agree to the proposal by buying longZCB in the same newly deployed AMM.

2.2.4 Validators

These are randomly(weighted by each's reputation) chosen managers who act as final gatekeepers for an instrument's approval. Their primary goal is to a) identify the risk of the potential instrument at a systemic level (i.e ensure low correlation among existing instruments), b) identify any malicious behavior (such as collusion with managers and utilizers) and c) propose/approve any subsidiary actions related to an instrument(such as early resolve). These validators are required to hold/lock their VT(such that they are exposed to the pooled risk) and purchase longZCB at a discount to mark price to make an approval decision.

2.3 Fixed Term vs Perpetual Instruments

Our system classifies the universe of investable assets into two types of instruments.

- Fixed-term fixed yield(Fixed) instruments are assets that have a set maturity and a predetermined rate for the capital it uses. An example would be a fixed-term loan.
- Perpetual instruments are assets that do not have a set maturity, and where the yield/returns will always accrue before the instrument is forced to resolve. An example would be supply positions to lending pools.

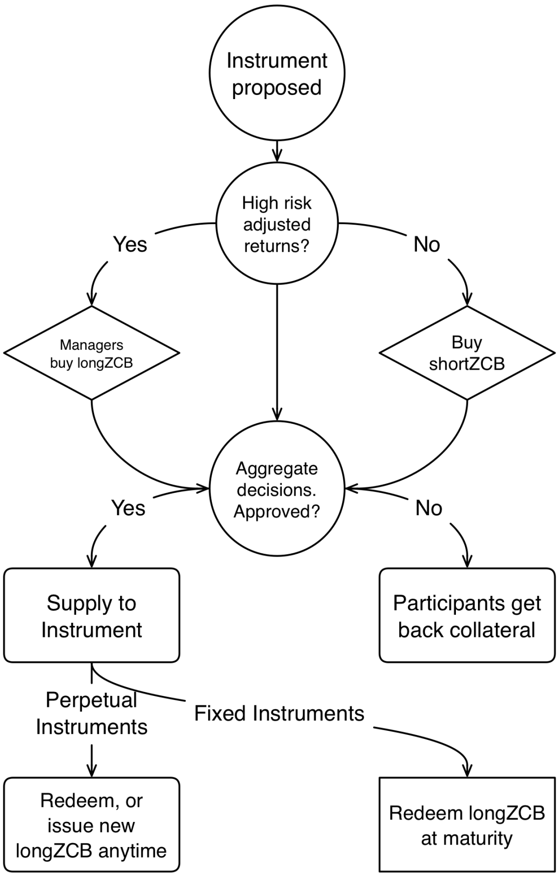
For Fixed instruments, the potential payout of longZCB is a function of the principal, the expected returns of the instrument, and its duration. For example, profitability for longZCB for a fixed-term loan would be proportional to the interest(expected return) to be paid by the borrower, and inversely proportional to the principal to be borrowed.

For perpetual instruments, the potential payout of longZCB is a function of the pro rata share of the returns generated by the underlying instrument. For example, profitability for longZCB where the instrument is a supply position in a lendingpool would be proportional to the utilization rate and the interest rate curve of the pool.

Detailed derivations of payouts are shown in section 6.

2.4 Protocol Flow

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


Instrument proposed
High risk adjusted returns?
Yes
No
Managers buy longZCB
Buy shortZCB
Aggregate decisions. Approved?
Yes
No
Supply to Instrument
Participants get back collateral
Perpetual Instruments
Fixed Instruments
Redeem, or issue new longZCB anytime
Redeem longZCB at maturity

1. Proposal: A utilizer i submits a proposal for utilizing liquidity with the necessary parameters(such as principal, expected returns, duration, etc), and deploys a contract that holds the instrument's logic and inherits from the protocol's base instrument contract. A prediction market is generated and new $\texttt{longZCB}_i$, $\texttt{shortZCB}_i$ tokens for the underlying instrument are deployed.

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 buying `shortZCB`. When the cumulative area under the AMM bonding curve(which is total `longZCB` bought - `shortZCB` bought) exceeds a threshold, `canbeApproved` returns true. During the assessment phase, the utilizer is the sole market maker by issuing `longZCB` in this prediction market.

3. Approval: When `canbeApproved` validators can finalize the instrument approval. If approved, capital will then be directed from the vault to the instrument contract.

The market will then proceed to the post-asssessment stage, where AMM liquidity provision will be amortized among traders(limit order based system). However, when `!canbeApproved` for a prolonged amount of time the market would automatically close and all participants will redeem their ZCB for their collateral.

4. Post Assessment:

   - **Fixed Instruments**: At maturity, redemption price for the ZCB tokens will be computed based on the contrast between the instrument's realized returns vs proposed returns from i, after which any `longZCB/shortZCB` holders can redeem with this price. Remaining profit from the instrument after all the ZCB holders redeemed are distributed to VT holders. Reputation scores for the managers who participated in the assessment phase are updated. Capital is withdrawn from the instrument contract back to the vault, and all additional accounting logic takes place.

   - **Perpetual Instruments** For perpetual instruments, the returns of `longZCB` are computed at a per block basis. Managers can either *mint* new `longZCB` or *redeem* their `longZCB`. Whenever they mint, capital will be supplied by the instrument's parent vault to the instrument, and whenever they redeem, capital will be withdrawn from the instrument back to the vault, and the redeemer can realize his/her profit.

3 AMM

The AMM is a key module in our system. It is responsible for a) aggregating opinions and pricing risk b) speculating or hedging on an instrument's returns and, in cases where the underlying instrument is a loan, c) extracting market driven interest rates.

An AMM instance is deployed for each instrument, which goes through two phases;

1. assessment phase: a positive sum prediction market where the utilizer is the sole `longZCB` issuer and market maker

2. post assessment phase: a zero sum prediction market where any traders can submit limit/taker orders on `longZCB` and `shortZCB`.

3.1 Assessment Phase

During the assessment phase, approval criterion is met when net `longZCB` buys(`longZCB` buys - `shortZCB` buys) exceeds some threshold(such that the total collateral accrued by the AMM is set as some fraction of the instrument's principal). Maximum net `longZCB` is capped to ensure a portion of the profit is distributed to VT holders. This phase is characterized as positive sum since `longZCB`'s profit are generated from `shortZCB`'s loss *and* returns from the instrument.

Liquidity is kept constant throughout all price ranges, and the AMM reduces to a simple bonding curve with uniform liquidity and prices set as a function of net `longZCB`(`longZCB` - `shortZCB`) issued. Under some modeling assumptions, this price can be interpreted as the aggregated subjective probability of the instrument's success.

During this phase, a vault investor(VT holder) who might be potentially exposed to the instrument but deems the instrument risk/reward profile unfavorable, can opt out from its potential returns by purchasing shortZCB. These decisions to hedge in aggregate are reflected to the net longZCB buys(longZCB buys - shortZCB buys), which in turn decreases the chance that the instrument will be approved.

Such two-sided markets aim to elicit more accurate default/profitability probability estimates from market participants.

3.2 Post Assessment Phase

During the post-assessment phase, no more ZCBs are issued from the utilizer, but liquidity provision is amortized among market participants(managers, VT holders, external speculators, etc). Anyone can submit limit orders to purchase/sell longZCB/shortZCB, where longZCB's profit equates to shortZCB's loss and vice versa. A longZCB bought and minted will necessitate a counterparty willing to either sell a longZCB or buy shortZCB, and vice versa.

During this phase VT holders who deem the instrument's risk/reward profile to be favorable can purchase longZCB as a means of amplifying his exposure to this instrument. Equally, an informed VT holder who decides to hedge against the instrument can purchase shortZCB.

However, a shortZCB buy / longZCB sell is penalized by a fee that decreases monotonically until the instrument's maturity. This is to ensure the managers can't easily transfer risk and thus be held accountable for their assessment of an instrument. If however the shortZCB buyer / longZCB seller owns and locks the instrument's parent VT, this fee is reduced by a value proportional to the amount of locked VT she owns as she would have passive exposure to the instrument that can't be removed. Details are in section 6.

4 Reputation

Managers will exhibit nonuniform management skills, and a prediction market with the sole purpose of efficiently aggregating opinions should be designed to accommodate these variabilities. Yet, the system should still be designed to encourage diversity such that the aggregated opinions are, in expectation, more accurate than that of the smartest individual in the group and mitigate information cascades(a phenomenon where the group's solution trivially converges to the opinions of a select few, even if they are incorrect).

A reputation score would characterize each manager's track record. If a manager predicts an instrument to be profitable, in the event of his correctness the system will increment his reputation score, and decrement in its complement.

A reputation score system then allows a more equitable value distribution and decision weighing scheme through the following mechanism.

- When assessment phase begins, only those with high reputation scores can participate early(where prices are lower) in the longZCB sale from the utilizer. Other managers can participate only after some reputable managers have bought longZCB: This serves two purposes, a) It presents a rewarding system that scales with one's reputation b) The market only proceeds when these reputable managers deem the instrument 'worthy', thereby providing a simple way that allows the skilled managers to filter out 'unworthy' instruments.

- Managers' leverage limit when buying longZCB scales with their reputation, which increases their capital efficiency and profitability when they are correct. (Akin to a futures margin long position, they would borrow from the vault and pay back during redemption)
- A budget is a maximum quantity a trader can buy/sell in the prediction market. We design the budget of a manager to scale with his reputation. Clearly, this would directly place more weight on those with higher reputations, while allowing them to place heavier bets. If the manager loses his reputation, this budget can decrease to 0, thereby disallowing consecutively bad decisions.

Recall that during the assessment phase AMM reduces to a simple bonding curve with uniform liquidity, and prices increase linearly with number of longZCB bought. This structure also mitigates information cascades as with more managers buying longZCB the marginal risk/reward of longZCB decreases while that of shortZCB increases, making the cost of hedges increasingly more attractive. While in a naive staking system the system is susceptible to an instance with a trivial solution where the group imitates the smartest or earliest risk-takers, an increasing price allows increased diversity and thus the inclusion of more information.

4.1 Leverage Multiplier

When buying longZCB, a manager's leverage multiplier, which scales with his reputation, determines how capital efficient his investment would be. It would also determine how much weight he has when the decisions are aggregated. (as the total amount of one's longZCB exposure determines one's total weight)

As an example, for a leverage ratio l of x, he would buy 100 underlying worth of longZCB with $\frac{100}{x}$ underlying. The extra capital is borrowed from VT. He would then pay back the debt to the vault whenever he redeems his levered longZCB position. He would have the same decision weight as purchasing with 100 underlying with just $\frac{100}{x}$. During redemption, if the longZCB with no leverage makes a y percent return, the manager will have made xy percent return.

5 Plausible Attacks

A general system may be susceptible to various attacks, and we search in its design space that prioritizes simplicity while negating plausible attacks. Below we list a non-exhaustive list and a corresponding solution for each.

5.1 Sybil

A Sybil attack is arguably the most trivial, albeit one of the most significant, attack from a manager or a utilizer. To ensure diversity, each manager has a finite budget for each instrument(which is usually much less than the instrument's principal), an utilizer can disguise as multiple managers or validators and approve an instrument via purchasing longZCB(approval criterion can be met when amount of longZCB bought is much less than the instrument's principal), which will direct the funds to the instrument contract from the vault. The system foregoes centralized KYC and implements sybil resistance through the following mechanisms

- A newly created manager identity starts with a 0 reputation score, reputation is only gained via honest and correct behavior over time, and every instrument's market requires reputable managers to go first.

- Validators, who act as final approval gate keeprs, are randomly chosen subsets of managers who are required to purchase and lock VT.

- A manager's identity instance can be only created via an identity gate. This could take the form of identity commitments exported from Web2 and generated on the frontend(i.e twitter oauth that filters accounts with less than some number of followers, implemented with a nullifier to prevent double signaling), KYC services, or other identity protocols in web3.

5.2 Maturity Payout Oracle

5.2.1 Fixed Instrument Return Oracle

The redemption price of `longZCB`(and `shortZCB`) are computed by the balance of its instrument contract at maturity. This balance is therefore the primary input to the oracle that determines the redemption price.

Each instrument contract is required to be inherited from the system's base abstract implementation, which ensures all profit and principal to be restored before the validator calls the function that officially closes the market(they are incentivized to do so since they are also purchasers of `longZCB` that need to be redeemed, which is only possible if the market is officially closed).

An attack where an adversarial utilizer(perhaps a borrower from a creditline instrument) purchase `shortZCB`, and manipulate the balance of the instrument contract is not viable as the `shortZCB` that can be bought by an address is capped by a value proportional to its balance of locked VT, which itself is exposed to the instrument and negates the profitability of such an attack(put plainly, insurance buyers need to hold what the insurance is insuring). Details are presented in section 6.

An attack where a `longZCB` buyer 'donates' to the instrument to increase its balance as to increase the redemption price of `longZCB` would not be economically rational for the attacker.

5.2.2 Uni-block attack resistant oracles

Oracles that feed in returns data of the underlying instrument serve a pivotal role in determining the redemption/issuance price of longZCB tokens. It is important that these data feeds are resistant to manipulations within a block.

Oracles for fixed term instruments: For fixed-term fixed-rate instruments, the balance of the instrument contract when they are resolved at maturity determines the redemption price of `longZCB`/`shortZCB` tokens. These can't be manipulated via flash loans as the written logic requires the redemption price to be computed at least a block after the instrument has been resolved.

Oracles for perpetual instruments `lastRate` is the last recorded exchange rate between an instrument's underlying(i.e USDC) vs its shares. For perpetual instruments, the exchange rate between the instrument's shares and its underlying reflects the socialized profit and loss of the instrument.`lastOracleRate` could be manipulated over short time frames (such as via flash loans) to display a rate that does not reflect the true returns generated by the instrument at a particular time. These limitations make the lastRate insecure as a price oracle by which to value longZCB tokens. Given that RAMM allows users to issue/redeem longZCB at this valued price, we need to ensure that the exchange rate oracle used to value can't be manipulated. As such, RAMM uses the lastOracleRate, a time linear interpolation of the lastRate and the lastOracleRate, to value longZCB tokens. The system is designed such that lastOracleRate will converge to the lastRate with sufficient time between the last recorded time and the current timestamp.

5.3 Gaming the system during assessment

As prices of longZCB during its sales(assessment) phase are designed to be monotonically increasing with sales, it may incentivize some to front-run future flows as the downside to this behavior is close to none(since the frontrunner can easily sell back to the bonding curve when prices are higher). However, recall that early on when the assessment phase begins only reputable managers can participate, and their reputation would only be earned if they redeem their longZCB at maturity.

It is also the case that the price of longZCB during the post-assessment phase is higher than that of the assessment phase (to incentivize managers to participate during assessment phase). After the instrument is approved, adversarial managers can decide to immediately offload the risk to other participants and realize a smaller but certain profit without bearing the instrument's risk until it matures(think subprime mortgage originators). As stated previously, this behavior is penalized as the AMM induces a selling fee(incurred to both longZCB sells and shortZCB buys) that is proportional to one's balance of locked VT and which slowly decreases to 0 until maturity.

5.4 Incentive Compatibility

Implementing the aforementioned selling fee mechanism requires all managers to act in accordance with their private information as their action space of profitable actions is limited only to purchasing longZCB and redeeming at maturity when their beliefs were accurate(although this necessitates the selling fee to be above a certain amount).

5.5 Managers' collusion with utilizers

Managers could collude with utilizers to get an instrument approved. Formal guarantees are left as future work, but the attack is prevented via the reputation mechanism(more weight is granted to more reputable managers, and reputation is gained only by being correct and honest over time), a manager's finite budget for each instrument(thereby requiring a diverse set of managers for approval), the randomness when choosing the validators(final gatekeepers), and an implementation of any of the aforementioned anti-sybil mechanism.

6 Implementation

6.1 AMM

We first briefly explain how the risk AMM is implemented, such that traders can long/short and submit limit orders.
Every proposed instrument will iterate through the following steps

1. Instrument Proposal
2. Deploy new bonding curve, its associated pool, and ZCB tokens
3. Parameter Calculation for initial bonding curve liquidity
4. Participants assess risk

6.1.1 Parameter Calculations

Fixed Term Instruments: The bonding curve implements price as a linear function of issued `longZCB`. See figure 1. The uniform liquidity constant, or the inverse slope, $\frac{1}{a}$ and the initial price b of the curve are computed from the principal and the expected returns(proposed by the utilizer) of a given instrument as input.

For a maximum net `longZCB` c, a given principal P and expected returns I, and assuming without loss of generality that the maximum price $m = 1$, we can construct the following conditions

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

Solving for a and b yields

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

When net `longZCB` is capped at αc during the assessment phase, for some $0 \leq \alpha \leq 1$, the parameters above ensure that $1 - \alpha$ fraction of the instrument's profit I is distributed to VT holders. α would then correspond to how much VT holders are willing to trade off profitability for protection.

Perpetual Instruments: The bonding curve implements price as a piecewise function of a linear function(with a positive slope) followed by a flat line. See figure 2. The `initialPrice` b, the starting price of `longZCB` in this curve, is a predetermined parameter. The uniform liquidity constant, or the inverse slope, $\frac{1}{a}$ is computed from `inceptionPrice` $\hat{b}$, `initialPrice` , and `saleAmount` $\hat{s}$. `inceptionPrice` is the price at which

The point $\hat{c}$ where the linear curve becomes a flat line is when `saleAmount` has been pulled as collateral and when the price becomes `inceptionPrice` $\hat{b}$. Noting that the area under curve until $\hat{c}$ is equal to `saleAmount` $\hat{s}$, we can construct the following conditions

- $\int_0^{\hat{c}}(ax + b)dx = \hat{s}$
- $a\hat{c} + b = \hat{b}$

solving for a yields

$$a = \frac{(\hat{b}^2 - b^2)}{2\hat{s}}$$

from the principal and the expected returns(proposed by the utilizer) of a given instrument as input.

6.1.2 Shorting

In essence, shorting can be decomposed into two sequential actions; borrowing and selling. One can combine and tokenize these two steps by setting a `maxPrice` of the underlying asset to short and allowing the shorter to only present the margin, $quantity *$ $(\texttt{maxPrice} - \texttt{curPrice})$, as initial collateral, If the asset's value exceeds `maxPrice`, the collateral presented would be irretrievable irrespective of subsequent price movements.

During the assessment period, liquidity for shorting is presented by the `longZCB` buyers. Consequently, some of the `longZCB`'s profit should be derived from `shortZCB` buyers' collateral, not just from the instrument.

Numerically, the procedure during assessment is outlined as follows

1. Shorter desires to short $\hat{x}$ unit amount of `longZCB`, thereby purchasing $\hat{x}$ unit amount of `shortZCB`. The collateral pulled out from the pool from selling $\hat{x}$ amount of `longZCB` is $\int_{c-\hat{x}}^{c}(p(x))dx$.
2. The shorter is quoted $(\texttt{maxPrice} * x) - \int_{c-\hat{x}}^{c}(p(x))dx$ amount of collateral
3. The shorter pays the quoted collateral and retrieves $\hat{x}$ unit amount of `shortZCB`. System-wise, the effect would be equivalent to selling $\hat{x}$ unit amount of `longZCB`.

When the instrument is approved, both `shortZCB` buyers and `longZCB` buyers need to find a counterparty. Liquidity would be presented from anyone via the open order system.

6.1.3 Fixed Instrument Prediction Market

An instantiation of a linear bonding curve for a fixed-term instrument is shown in the figure below. Managers buy up the curve and `shortZCB` buyers sell down the curve. The area under the curve represents collateral added/subtracted from the system during this bonding phase.

`approvalCriterion` for fixed term instruments is met when the following condition is satisfied

$$\int_0^{\hat{c}}(ax+b)dx \geq \alpha * principal$$

for total net `longZCB` bought $\hat{c}$ and where $\alpha * principal$ would be used as first loss capital.

This is illustrated in the figure above, where the area labeled yellow represents $\alpha * principal$. A higher α would necessitate more collateral presented by the managers and would give rise to a larger insurance buffer for passive investors. The area labeled green, or $principal - \alpha * principal$ represents collateral presented by the vault holders.

Profit for `longZCB` buyers : Naturally, for a redemption price R the profit allocated for all `longZCB` buyers can be decomposed into two elements; profit generated from the instrument and collateral presented by `shortZCB` buyers indexed by i, as shown below

$$R\hat{c} - \int_0^{\hat{c}}(ax+b)dx + \sum_i((R * x_i) - \int_{c_i - x_i}^{c_i}(ax+b)dx)$$

The first two terms represent the blue area in the figure above, and the latter two terms represent collateral presented by all `shortZCB` buyers.

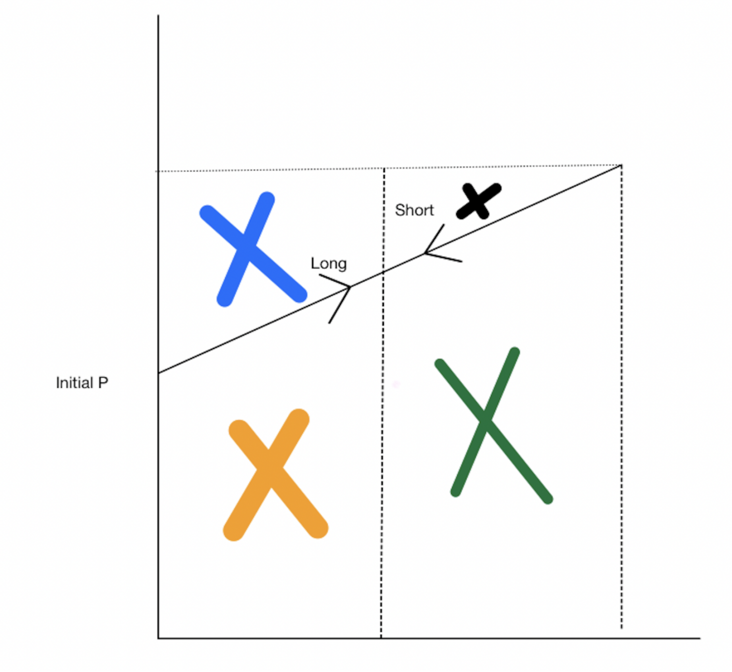


Figure 1: Y axis denotes price of `longZCB` and X axis denotes amount of `longZCB` minted.

Profit for vault holders: Profit for vault holders is the remaining value after the `longZCB` holders redeem for the redemption price R.

$$totalProfitFromInstrment - (R\hat{c} - \int_0^{\hat{c}} (ax+b)dx)$$

which is represented as the black area in the relevant figure.

6.1.4 Perpetual Instrument Prediction Market

Bonding curves for perpetual instruments is a piecewise function, where a linear curve is followed by a flat curve when a certain amount of `longZCB` is bought. The price at which the flat curve begins is the `inceptionPrice` of the value of the junior tranche of the instrument; it is the price at which new `longZCB` will be minted at the instance the instrument is approved and supplied.

For perpetual instruments, as managers will be able to issue and buy `longZCB` after the assessment phase, such a curve was implemented as a means to incentivize managers to participate before approval when `longZCB` is at a discount to `inceptionPrice`.

The bonding curve formula is the following

$$p(x) = \begin{cases} ax+b, & \text{if } x \leq C \\ \texttt{inceptionPrice}, & \text{otherwise} \end{cases}$$

where C represents the point where price becomes equal to the `inceptionPrice`, or equivalently the total amount of `longZCB` sold at a discount.

`approvalCriterion` for perpetual instruments is met when the following condition is satisfied

$$quantity\ \texttt{longZCB} - quantity\ \texttt{shortZCB} \geq C$$

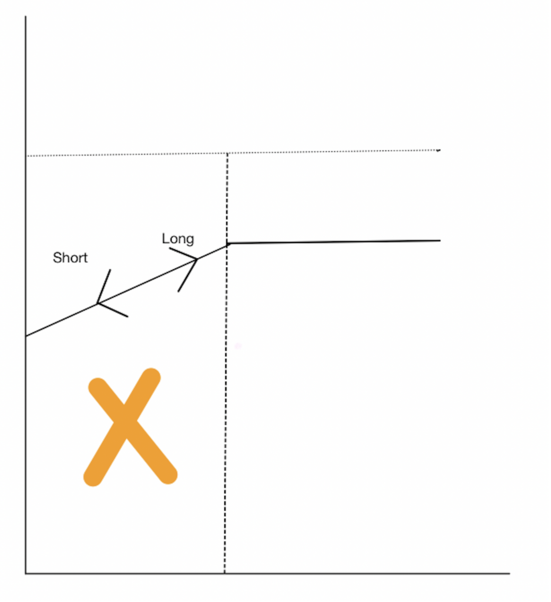


Figure 2: Y axis denotes price of `longZCB` and X axis denotes amount of `longZCB` minted.

6.1.5 Open Orders

The order system is a mechanism that serves to amortize liquidity provision for `longZCB` and `shortZCB` markets if the instrument has been approved. A potential `shortZCB/longZCB` buyer would submit an order with the following parameters. The order would be queued and can be filled by a price and orderId basis.

- bool isLong
- uint256 price
- uint256 amount
- uint256 orderId
- address owner

6.2 Fixed Instruments details

6.2.1 How to extract interest rates

For instruments that involve loans, the AMM can extract interest rates that are implied by the managers' number of `longZCB` bought.

When a borrower proposes a principal P and a desired interest rate I, the AMM's initial parameters would be constructed following steps outlined in section 6.1.1. Noting that the maximum price of `longZCB` is $m = 1$, we can then construct an adjusted interest rate $\hat{I}$ and the adjusted principal $\hat{P}$ as a function of net `longZCB` multipled by some constant, $\hat{c} = constant * net$. The constant terms signifies how much leverage `longZCB` would incur as a junior tranche of the loan. Adjusted principal will be less or equal to the proposed principal and adjusted interest will be greater or equal to the proposed interest.

$$\hat{P} = \int_0^{\hat{c}} p(c)dc$$

$$\hat{I} = \hat{c} - \int_0^{\hat{c}} p(c)dc$$

Intuitively, more managers buying `longZCB` results in a greater $\hat{c}$, which means the borrower can borrow more principal with lower interest rates. When $\hat{c}$ is equal to the maximum `longZCB` that can be issued, $\hat{P}, \hat{I}$ would equal to the proposed principal and interest rate proposed by the borrower.

6.2.2 Redemption Price(Fixed return Instruments)

For Instruments with fixed yields and a predetermined maturity date, the protocol can determine the payout for `longZCB` holders by its redemption price. Computing redemption prices for `longZCB` takes into account the following observations.

1. `longZCB` holders claim a junior tranche position, which entails that they absorb volatility that deviates from the fixed predetermined rate.
2. Since the bonding curve allows shorting via purchasing `shortZCB` with a fixed collateral amount(and this is simply an abstraction of the borrowing and selling process), the collateral presented by the short sellers(which is default set at m per ZCB borrowed) may not be enough to fully compensate the lender when the underlying instrument generates a return greater than the fixed predetermined rate.

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 (either positive or negative) return in relation to the expected yield, and the number of bought `shortZCB`, respectively. Consequently, the redemption price for a `shortZCB` token is $\max(1 - \omega_i, 0)$.

We can quickly verify the redemption price with some algebra. Precisely, we show the system will remain solvent after paying all the longs and shorts.

We need to show that

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

where ValueIn, the combined value of total collateral in the system and profit from the underlying instrument, can be represented as $V_{in} =$ Collateral from longZCB + Profit from Instrument + Collateral from shortZCB + Collateral stored from short sells

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

Where for ValueOut, the total redeemed value by both `longZCB` and `shortZCB` traders, can be represented as $V_{out} =$ 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 $\lambda_i \leq 0$

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

6.2.3 Prediction market manipulation prevention with shortZCB cap

A plausible attack scenario is an instance where an actor buys shortZCB and manipulates the outcome of the market to alter the redemption price of shortZCB in his favor(such as not repaying the loan for a credit-line instrument). To prevent such attacks, the system necessitates the buyer to hold and lock the instrument's parent vault. By doing so, the actor's profit from shortZCB will be offset by their loss from holding the vault.

The system decides how much shortZCB quantity Q_s can be bought for a given actor's locked vault shares s_i. Given that we want the profit generated by shortZCB to roughly equal the negation of the vault's socialized loss(and vice versa), we can use the redemption price computations from the previous section to derive the following relationship

$$Q_s(-\frac{\lambda}{c} - 1 + P_s) = -\frac{s_i(\lambda + \hat{P}c)}{\sum_j s}$$

where λ denotes the profit(or loss) generated by the instrument, c is the total supply of longZCB, P_s is the average price of longZCB at which the buyer bought shortZCB, $\hat{P}$ is the average price of total bought longZCB by all participants. The term $\sum_j$ is a summation of shares of all participants, which also represents the total circulating supply of vault shares. Rearranging we have

$$Q_s = \frac{s_i(\lambda + \hat{P}c)}{\sum_j s(-\frac{\lambda}{c} - 1 + P_s)}$$

However, since λ which denotes the profit(or loss) generated by the instrument after approval and can't be known when shortZCB is being bought, we insert $\hat{\lambda}$ as a parameter, the maximum loss guaranteed to be hedged, instead to determine $\hat{Q_s}$, which is the quantity of shortZCB that is guaranteed to offset the loss $\hat{\lambda}$ generated by the instrument.

6.3 Payouts for Perpetual Instruments

When the underlying instrument does not have a maturity date and incurs variable yield, longZCB tokens cannot be redeemed from redemption prices computed as in the previous section as the return of the instrument is unpredictable when the instrument is being proposed. The protocol instead utilizes a continuous pricing mechanism for the

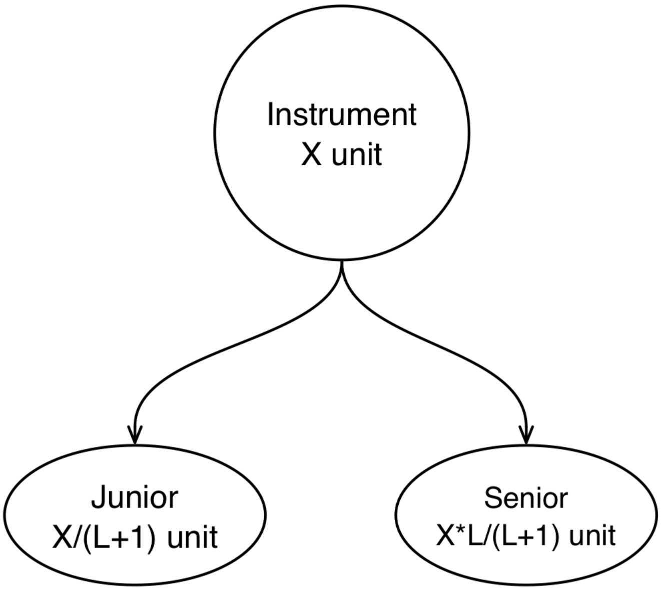


Figure 3: X unit of instrument always breaks down into X

junior tranche(tokenized as `longZCB`) and senior tranche(capital in the vault), based on the `promisedReturn` R_f of the senior tranche.

`promisedReturn` can either be a dynamic or a fixed parameter of the tranching module that represents a per-second compounding rate of the senior tranche. For example, for a 10 percent fixed APR for the seniors, its fixed `promisedReturn` equivalent is 1.0000000031. When the `promisedReturn` is dynamic, it is a function of a certain parameter(i.e utilization rate of a lending pool, as with a higher utilization rate it makes sense to allocate a higher `promisedReturn` for senior tranche holders and vice versa).

Normally, `promisedReturn` would be set lower than the expected real returns R_r of the instrument, such that the junior tranche would incur greater profit with these real returns. Greater profit comes at a cost of providing first loss capital.

At a high level, the protocol uses a general tranching module that splits any asset's(Instrument) volatility into tokens with a senior(VT) and junior(`longZCB`) claim. These senior/junior tokens will be continuously priced, where the input to the pricing function will be given by the exchange rate oracle feeds of the asset in the Instrument denominated in it's underlying, and time that has elapsed since the tranche has been incepted. See figure 3 for illustration.

As shown in figure 3, X unit of shares of an instrument will always split to $\frac{X}{L+1}$ junior tranche tokens and $\frac{XL}{L+1}$ senior tranche tokens for some leverage factor $L \geq 1$. Junior and senior tokens are constantly priced as p_{ju} and p_{su} respectively. For the exchange rate of instrument shares versus its underlying R, XR represents the total amount of underlying represented by X unit shares of the instrument. this allows us to form the supply invariant principle

$$XR = \frac{p_{ju}X}{(L+1)} + \frac{p_{su}XL}{(L+1)}$$

which states that the returns of the instrument is not related to the supply of `longZCB` tokens, and p_{ju} is solely a function of R, Lp_{su} as is shown

$$R = \frac{p_{ju}}{(L+1)} + \frac{p_{su}L}{(L+1)}$$

6.3.1 Notations

An Instrument, where its total value denominated in `underlying` is always quantifiable by an exchange rate oracle, can have its value separated into a senior and a junior token, by a fixed ratio $0 \leq w \leq 1$, such that the invariant $(1-w)$ senior + w junior = 1 Instrument always holds. If w is 0.3, for example, 1 Instrument will always split to 0.7senior and 0.3junior. Equivalently, the protocol will only accept $(1-w)$ senior + w junior when redeeming for 1 Instrument. w would be pre-determined parameter for each tranche, and would characterize the degree of leverage junior incurs. Note that the leverage factor $L = \frac{1-w}{w}$, which will be used interchangeably.

6.3.2 Pricing

The pricing model should a) ensure that the return profiles of both `junior` and `senior` lie in the construct of which they are defined, i.e that seniors have the primary claims to returns(`promisedReturn`) while juniors absorb volatility and b) ensure that every supply of `junior` and `senior` can redeem for `underlying` under this computed value.

In light of these considerations, we present the following pricing mechanism. For a given Instrument, a `senior` would have a fixed return profile R_f(determined when tranche begins), such that it's value at time t, as denominated by the `underlying` of Instrument would be defined by the following formula. When `promisedReturn` (R_f) is constant:

$$P_{su}^t = I(R_f)^t$$

and when `promisedReturn` (R_f) is variable:

$$P_{su}^t = I \prod_{i=1}^{t} R_{fi}$$

while its pair `junior`'s price would be defined as the pro rata share of the remaining assets after all circulating `senior` at t, has redeemed for P_{su}^t.

$$P_{ju}^t = \frac{A_t - (P_{su}^t S_{s_t})}{S_{j_t}}$$

S_{s_t} and S_{j_t} respectively denotes the circulating supply of `senior` and `junior` at time t. When t = 0(when tranche is initialized),

$$I := P_{su}^0 = P_{ju}^0$$

$A_t := I(S_j + S_s)\prod_{i=1}^{t} R_{ri} = I(S_j + S_s)P_{vu_t}$ denotes the value of the total assets of both the senior and junior's share of the Instrument at time t denominated in `underlying`. R_{ri} is the return incurred by the Instrument (only)at timestep i. (Without loss of generality we subsequently set $I = 1$).

Using the previously defined ratio invariant we have $S_j = \frac{w}{1-w} S_s$, and making no other assumption other than the fact that the total underlying asset A_t held by the Instrument at a given point is simply $(S_j + S_s)P_{vu_t}$, where P_{vu_t} is the price of Instrument denominated in `underlying` at time t, substituting allows us to also express P^t_{ju} as

$$P^t_{ju} = \frac{w}{1-w}(\frac{\prod_{i=1}^t R_{ri}}{w} - P^t_{su})$$

This representation of P^t_{ju} eliminates its dependency of either S_j and S_s, allowing the pricing to be agnostic to supply, and is solely a function of the returns accumulated until timestep t. This property ensures the system will stay solvent and be time agnostic under arbitrary inflow and outflow of capital. All minters and redeemers of `junior` and `senior` tokens would be guaranteed their pro rata share regardless of their time of entry t (thus its perpetual nature). However, **this assumes that the system always mints and redeems $\frac{w}{1-w}$ junior for every 1 senior minted/redeemed**. So it is necessary for a user who wants a `senior(junior)` token to mint both `senior` and `junior`, and find a suitable counterparty that would hold `junior(senior)`.

One can see that P^t_{ju} will increase faster than P^t_{su} only during times where $R_{r_t} \geq R_f$. So it is the potential `junior` holder's best interest to buy when he thinks $R_{r_t} \geq R_f$ for the forseeable future.

We can also easily verify that under this pricing rule, all traders who enter at time t can realize their profit at another time $t+n$ by showing that the sum of profits for seniors and juniors over n timesteps, normalized by the ratio coefficient w, equate to the sum of a single Instrument over n timesteps. For a single `senior` and `junior` token, their profit($\hat{P}$) from timestep t to $t+n$ can be expressed as

$$\hat{P}_s := (R_f)^{t+n} - (R_f)^t$$

$$\hat{P}_j := \frac{w}{1-w}(\frac{\prod_{i=1}^{t+n} R_{ri}}{w} - (R_f)^{t+n} - \frac{\prod_{i=1}^{t} R_{ri}}{w} + (R_f)^t)$$

Since $\frac{1}{w}$ Instrument always splits to 1 senior and $\frac{1-w}{w}$ junior,

$$\hat{P}_s + \frac{1-w}{w}\hat{P}_j = \frac{\prod_{i=1}^{t+n} R_{ri} - \prod_{i=1}^{t} R_{ri}}{w}$$

which is precisely the profit for $\frac{1}{w}$ Instrument over n timesteps starting from timestep t.

6.3.3 Pricing with dynamic `promisedReturn`

It may be ideal for some instruments to have the `promsiedReturn` coefficient R^t_f as a function of a certain variable U. For example, when the underlying instrument is a lending pool then having a constant R_f entails that `longZCB` holders incur a loss not only during defaults, but also when the pool is not utilized enough. It also means the senior tranche investors(vault investors) gain yield without anyone utilizing the pool.

Under this circumstance, it may be constructive for $R^t_f(U_t)$ to be a function of the utilization rate U of the lending pool instrument. The pricing formula would not change, except that R_f here would be time-dependent. Rearranging equations and recalling that $L := \frac{1-w}{w}$ we have the following representation of the price of `longZCB` as a function of time

$$P^t_{ju} = (L+1)\prod_{i=1}^{t} R^i_r - L\prod_{i=1}^{t} R^i_f(U_t)$$

6.3.4 Post Assessment Issue and Redeeming

In this section, we outline the processes of the following post-approval functions for perpetual instruments, and how the pricing rule is applied in this setting.

Issue `longzcb`: After an instrument is approved, whenever Q_l amount of `longZCB` is issued, the collateral used to issue(let us denote this $Q_l * P_{ju}^t$) + some amount of collateral(senior shares) from the vault is supplied to the instrument. Newly issued `longZCB` will accrue value as the underlying instrument accrues yield.

Recall that the system necessitates LQ_l senior shares issued for every Q_l junior(longZCB) tokens issued. The total amount of capital supplied to an instrument by purchasing Q_l `longZCB` is

$$\begin{aligned} &Q_l * P_{ju}^t + LQ_l * P_{su}^t \\ &= Q_l * ((L+1)\prod_{i=1}^{t} R_{ri} - L\prod_{i=1}^{t} R_{fi}) + LQ_l\prod_{i=1}^{t} R_{fi} \\ &= Q_l(L+1)\prod_{i=1}^{t} R_{ri} \end{aligned}$$

$Q_l * P_{ju}^t$ is the junior tranche capital supplied by the issuer, $LQ_l * P_{su}^t$ is the senior tranche capital supplied by the vault.

The higher the leverage factor L, the more capital supplied per Q_l.

Redeem `longZCB`: `longZCB` can be redeemed from the protocol whenever there is available liquidity to withdraw from the instrument.

Amount withdrawn from the instrument is computed as in issuance. For every Q_l `longZCB` redeemed, LQ_l senior shares are also redeemed, where the total redeemed collateral from the instrument is $Q_l * P_{ju}^t + LQ_l * P_{su}^t = Q_l(L+1)\prod_{i=1}^{t} R_{ri}$. $Q_l * P_{ju}^t$ is the collateral returned to the redeemer, and $LQ_l * P_{su}^t$ is the collateral returned to the vault.

Issue `shortZCB`: After the assessment phase, `shortZCB` can only be issued via an order matching system; when another manager is willing to issue the same quantity of `longZCB`. Collateral presented by the `shortZCB` issuer is $Q_s * (\texttt{maxPrice} - P_{ju}^t)$. Profit for `shortZCB` is derived from the loss of `longZCB` and vice versa, where it is computed as $Q_s * (P_{ju}^{t+1} - P_{ju}^t)$.

Redeem `shortZCB`: When `shortZCB` is being redeemed, it's counterparty `longZCB`'s future profit or loss is no longer backed by any capital. As the system is exposed to more net `longZCB`, redeeming Q_s `shortZCB` has the same effect as issuing Q_l `longZCB`, where $Q_s(L+1)\prod_{i=1}^{t} R_{ri}$ capital is supplied to the instrument, using withhold funds presented by `longZCB` buyers when the order was matched.

6.3.5 longZCB Returns

To observe the behavior of longZCB's profitability as a function of R_{ri}, we derive the derivative of $\log P_{ju}$ with respect to time. Assuming an infinitesimal compounding interval,

$$\log P_{ju}^t = \log\frac{1}{w} + \int(\log R_r^t - \log R_f^t)dt$$

$$\frac{d\log P_{ju}^t}{dt} = \log R_r^t - \log R_f^t$$

It is clear that longZCB is only profitable during intervals where $R_r^t \geq R_f^t$

Figure 2 illustrates this intuition. The straight increasing linear function is P_{su}, or the valued price of the senior tranche. While P_{su} increases predictably and monotonically, P_{ju} starts decreasing when R_r is less than R_f, and increases when R_r is greater than R_f.

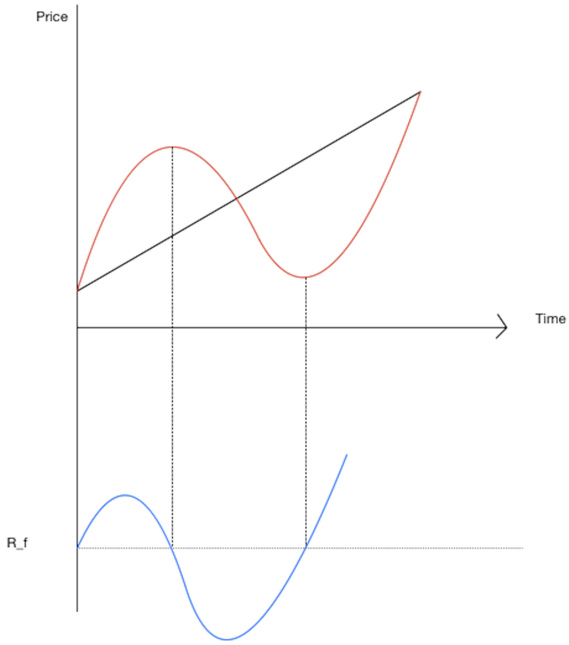


Figure 4: Red line denotes P_{ju} and green line denotes R_r

When $R_r^t \leq R_f^t$ for a prolonged time, it may be the case that $(L+1)\prod_{i=1}^t R_r^i \leq L\prod_{i=1}^t R_f^i(U_t)$. This is when the collateral backing the junior tranche is *depleted*, and the next loss would be burdened by the senior tranche.

6.3.6 Applying the pricing scheme

Here we illustrate how the perpetual tranching module can be applied in RAMM. longZCB will represent junior tokens and capital in VT will represent senior tokens, and the aforementioned pricing model applies.

Let's have an Instrument be a supply position to a lending pool, akin to minting cETH.

1. A utilizer will propose a set of collateral and an interest rate curve for the lending pool. Tranche parameters such as R_f and w are predetermined.

2. Managers will decide whether the collateral the lending pool accepts is liquid enough for the given interest rate curve. They will buy longZCB of this cETH if they deem so.

3. If there is sufficient longZCB bought, the protocol will supply capital to the lending pool. However, for every longZCB bought, $\frac{1-w}{w}$ multiplied amount of the collective collateral used to buy longZCB will be supplied by VT.

4. Even after the lending pool is approved and supplied with capital, managers can buy longZCB at the price P^t_{ju} at time t. When doing so, he will automatically supply $\frac{1-w}{w}$ multipled amount of their provided capital from VT to cETH.

5. Instead of redeeming longZCB at maturity, managers will be able to redeem longZCB with the price P^t_{ju} at time t. When they redeem, they also withdraw $\frac{1-w}{w}$ multipled amount of their redeemed collateral from cETH back to VT.

6. longZCB buyers will only be profitable if $R_{r_t} \geq R_f$ on average during their exposure to it.

6.4 Reputation Updates

We henceforth denote p_j as the subjective probability of success for an instrument of concern by manager j. We use this p_j to update the reputation scores of managers who participated in the assessment.

We first show that we can compute p_j for every instrument as a function of the manager's longZCB purchase quantity and his trading budget a_j. The trading budget restricts the manager's maximum purchase quantity and increases with his reputation.

We only consider a simple model(detailed models aren't really necessary for the purpose of the system) where each longZCB is redeemable for $m = 1$ if the underlying instrument succeeds to deliver its promised yield or 0 otherwise(in the case of default). Denote c_j as net longZCB bought before the manager j has started trading, and c_{j+1} the same quantity after j has traded. 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 paid to increment net longZCB from c_j to c_{j+1}. First-order conditions allow us to represent the implied probability of a fractional kelly optimal j as follows:

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

We can then perform brier score updates for the reputation score from this p_j, based on the binary outcome of whether or not the redemption price ω was greater or equal to 1.