Whitepaper Draft

Jeongwon Park

November 2022

1 Problem Statement

We continually observe that risk assessment systems serve to be the primary mode of failure in capital markets, and argue that its decentralized variant eliminates the failure modes 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 LPs 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. 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 an application 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. From a bird's eye view the system 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 skew in 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: Vault 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 `creditline` or `stategy`, or a contract that simply buys and hold non cash flow financial assets.
- `longZCB`: a tokenized long position on synthetic (zero coupon-like) 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. They are programmed such that purchaser's collateral would be used as first loss capital. It's 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 value is 1- value of `longZCB`
- 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 simple exposure to complex strategies

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(buy `shortZCB`) in the prediction market. This allows them to hedge their exposure to the instrument if it is approved. After its approval, they can buy either `longZCB` or `shortZCB` 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 (ensure low correlation among existing instruments) and b) identify any malicious behavior (such as collusion with managers and utilizers). 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 Protocol Flow

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

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 `longZCB`$_i$, `shortZCB`$_i$ tokens for the underlying instrument are deployed.

2. Assessment: Managers who deem that the instrument has a favorable risk-reward profile buy `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, liquidity 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. 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 the instrument's realized returns vs proposed returns from i, after which any `longZCB`/`shortZCB` holders can redeem with this price. 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.

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 the case for credit-line instruments, 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 linear function of net `longZCB`. 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.

We argue that such two-sided markets aim to elicit more accurate default 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. Since a `longZCB` bought will necessitate a counterparty willing to either sell a `longZCB` or buy `shortZCB`, this phase allows arbitrary total notional value of open interest, allowing anyone to profit from the instrument's profitability.

During this phase VT holders who deem the instrument's risk/reward profile to be favorable can purchase `longZCB` as a means of amplifying her 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 on an instrument. If however the `shortZCB` buyer / `longZCB` seller owns locked 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.

3.3 AMM implementation

Our implementation of AMM is inspired by Uniswap V3, and is a generic module that can be used to trade any derivatives with a bounded price range. Key features include limit orders, passive(concentrated) liquidity provision, and long/short functionalities. The trades will be denominated in the underlying asset of VT, and traders will be able to trade `longZCB`/asset or `shortZCB`/asset(liquidity is not fragmented as both long/short are tradeable in a single AMM).

To a trader, the experience will be on par with the experience of trading futures with expiry dates.

The price of `longZCB` and `shortZCB` always add up to 1. This holds true even at maturity, where the redemption price of `shortZCB` will be 1 - redemption price of `longZCB`.

The AMM can be thought of as a permissionless market for predicting the returns of any investable asset. Its oracle is based on functions with inputs solely from on-chain states and, under some constraints(as shown later), will be difficult to manipulate.

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 after 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.

5 Plausible Attacks and Problems

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) or other identity protocols in web3.

5.2 Maturity Payout 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).

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.

5.3 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 Manager's collusion with utilizers

Managers could collude with utilizers to get an instrument approved. Formal guarantees are left as future work, but currently the attack is prevented via the reputation mechanism(more weight on 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), and the randomness when choosing the validators(final gatekeepers).

6 Use Cases

We specifically designed our system to be a general asset management infrastructure that leverages its existing managers for a wide set of instrument classes. Since an AMM/instrument pair can be deployed by anyone, a prediction market for an arbitrary investment's returns can be used to make a collective decision on whether the investment is worth funding.

Moreover, a vault instance(where a new VT is deployed) can be created for different instrument classes. Below we present some examples.

6.1 CreditLine

A straightforward example would be a creditline instrument that facilitates uncollateralized lending from the protocol to a utilizer. A utilizer would be a borrower, a `longZCB` would represent a bond, a `shortZCB` would represent a credit default swap, and managers would represent credit underwriters. VT holders would represent passive investors who have invested in a senior tranche of a bundle of loans, but through the AMM they would have the option to hedge a loan they deem too risky, or be more exposed to a loan they deem less risky.

In this example, the AMM during assessment can also be used to derive market driven interest-rates.

6.2 Options Vault

In this instance, a vault would take form of a decentralized options vault that sells volatility at each predetermined time interval.

Every week, a utilizer could propose a suite of n different delta options OTC buys, which would create n markets that corresponsds to each of the strikes. These utilizers would generally be a market maker who are incentivized to purchase options without slippage while hedging via an external exchange, and capture a spread(by proposing a discounted implied volatility). Each created market will be associated with a different strike price a week from the point of market creation. Managers will then buy `longZCB` from the prediction market with the strike price they deem are less risky, and the most funded strike price will be funded by the vault.

VT holders would represent passive investors with protected exposure for the weekly options short. They can hedge a strike price they deem too risky, or increase exposure to a strike price they deem less risky.

6.3 Liquidation Free Leverage Trading

A utilizer can submit a proposal for an instrument contract that purchase, say, ETH from the open market. The decentralized set of managers will decide if the potential reward is worth the risk, and approve it if they deem it so. Since `longZCB` is tokenized leveraged exposure to the underlying instrument where the PnL is realized only at maturity, the managers and utilizers will be able to purchase ETH with liquidation free leverage that lasts until maturity.

6.4 Assessment system as a module

Any entity can delegate the underwriting and structuring process to a set of (reputable)managers from the protocol by creating a new vault. These entities can be DAOs that want risk assessment/structuring for their treasuries(denominated in a single numeraire) that need management by a non-centralized entity, or anyone who wants prediction markets, management, or tranching for niche instrument classes.

Vault creators can specify their investment mandate through parameters at vault creation. This includes the class of instruments they want exposure to. They can also specify the parameters of each vault. An example would be the amount of bond issued to managers or the amount of leverage each manager can take, which will correspond to how much risk the vault creator is willing to withstand(since more `longZCB` purchased by managers equates to more first loss capital, but at a cost of less returns distributed to VT holders).

7 Appendix

7.1 AMM

We first briefly explain how the AMM is implemented, such that traders can long/short, submit limit orders, and provide passive liquidity. We then show how the redemption prices of ZCB tokens and the AMM parameters during the assessment phase are computed.

7.1.1 Uniswap V3 as a Granular Bonding Curve (GBC)

Granularity in this context refers to the divisibility of the price space into distinct ticks. A linear bonding curve follows the following price rule of asset x as a function of quantity y bought. In a GBC, for a given price range(tick) i the price of asset x denominated in y, p_{xy}, follows the general form

$$(p_{xy})^n = ay_i + b$$

for some parameters a, b. The slope a can be thought of as the inverse value of liquidity L. It can be shown that UniV3's curve for a given tick follows the same form, where $n = 1/2$.

$$(p_{xy})^{\frac{1}{2}} = \frac{1}{L}y_i + \frac{y_0}{L}$$

where y_0 is the virtual reserves offset parameter, which serves to constrain the price space to lie in the range of the underlying tick instead of 0 and infinity. $\frac{y_0}{L}$ is a constant that represents the initial (powered)price $(p_{xy})^n$ when the tick is first crossed, or equivalently when $y_i = 0$.

A linear price rule exhibits the desirable property of sum preservation when working with liquidity provision math (when adding/subtracting liquidity). For a given $L = \sum_i L_i$ it holds that

$$\int_\alpha^\beta (\frac{1}{L}y + b)dy = \sum_i \int_\alpha^\beta (\frac{1}{L_i}y + b)dy$$

$$L\Delta p^n = \sum_i L_i \Delta p^n$$

This property signifies that, for a price range(such as a tick), any amount of liquidity provided by individual i would be pro-rata claimable given the total liquidity supplied in the range. This allows us to construct useful extensions.

Under this GBC framework, we can instead set $n = 1$ for a useful construction of the bonding curve such that swapOut quantities are represented as an area under a linear curve. For a given tick i with prices in the range between p_i and p_{i+1} a price rule is set

$$p_{xy} = ay_i + b$$

such that the area under the curve equates to the swapOut quantity of x_i for swapIn quantity of y_i.

$$\Delta x_i = \int_{p_i}^{p_{i+1}} (\frac{1}{L}y_i + b)dy$$

Consequently, when Δx_i value updates to $\hat{\Delta x_i}$ by adding or removing liquidity, L_i would be updated to $\hat{L_i}$ such that the difference in liquidity is a multiple of the difference in bids/asks by some constant

$$\hat{\Delta x_i} - \Delta x_i = \text{constant}(\hat{L_i} - L_i)$$

It follows then that the process of adding/reducing limit orders on tick i is equivalent to adding to/subtracting from L_i by a proportional amount.

7.1.2 OneTimeLiquidity

`OneTimeLiquidity` refers to non-recyclable liquidity that has the *fillable* property of a limit order. The sum preservation quantity allows a given tick to be composed of both `OneTimeLiquidity` and passive liqudity.

Each tick i indexes $\texttt{OneTimeLiquidity}_i$ and ΔL_i. $\texttt{OneTimeLiquidity}_i$ is added or subtracted to passive liquidity ΔL_i when a user submits or removes limit orders to i. When the price crosses to a new tick $i+1$ or $i-1$, it is *depleted*, and set to 0.

7.1.3 Shorts

For a linear price rule, recall that we can interpret areas under the curve as swapIn quantity and its corresponding change in the x-axis as swapOut quantity. When the price of the asset to be traded(`longZCB`) is bounded by $maxPrice := m$, this allows us to construct a price rule for `shortZCB` s, summed over ticks i, where each i is bounded by p_i, p_{i+1}. For a given s to be swapped out, the required amount of numeraire y to be swapped in is

$$ms - \sum_i \int_{p_i}^{p_{i+1}} (\frac{1}{L_i} y_i + b) dy$$

where the sum is iterated until all s has been filled(as each tick i has a fixed amount of s that can be sold, which depends on L_i)

7.1.4 Assessment Phase

During the assessment phase, $L_i = L$ for all reachable i. The uniform liquidity constant $L = \frac{1}{a}$ and the initial price of the bonding 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.

7.1.5 Post-Assessment

After assessment, default L_i is set to 0, and can be added (or subtracted) by providing (or removing) liquidity to tick i.

7.1.6 Redemption Price

Computing redemption price for `longZCB` takes into account the following observations.

1. Bond holders claim a junior tranche position, which entails that they are required absorb volatility that deviates from the fixed 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 is holding a variable return position(in the case where the realized return could be higher than the expected return).

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 bought `shortZCB`, respectively.

Consequently, the redemption price for a `shortZCB` token is $\max(1 - \omega_i, 0)$.

7.2 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.