Non technical specification draft

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.

Prevailing decentralized systems either can't price risk and only resort to centralization or triviality such as collateralized lending. However, a vibrant capital market needs a system that can define and assess any arbitrary 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` will propose a new 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: Tokenized 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 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. Its synthetic nature is stmes from its necessity for a counterparty(`shortZCB` buyers, `longZCB` sellers) to fulfill its demand.
- `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 the prediction market AMM. They can participate in the assessment of an instrument via (only)short selling the instrument's ZCB in the prediction market. This allows them to hedge their exposure to the instrument if it is approved. After its approval they can purchase either `longZCB` or `shortZCB` based on their risk appetite on the said 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 absorb all the return volatility that deviates from the prescribed fixed returns.

These agents would go through an anti sybil verification process and is characterized by a *reputation* score, which increases when their `longZCB` was profitable and decreases when it was not.

Reputation system exists to acknowledge the non uniformity of risk/reward assessment skills which gives rise to a more equitable value distribution mechanism. A higher reputation allows a manager to acquire more leverage 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.

In traditional finance managers usually embrace asymmetric pay-off, where the convex reward structures allows them to undermine the risk of an instrument. In the proposed system they would instead share the same linear pay-off structures as that of LPs, but one that is amplified and improves with their reputation.

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) and b) identify any malicious behavior (such as collusion with managers and utilizers). These validators are required to purchase, stake, and lock their VT and purchase `longZCB`(such that they are exposed to the risk pool) 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 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 bonding curve(`longZCB` bought - `shortZCB` bought) exceeds a threshold, `canbeApproved` returns true. During the assessment phase, the utilizer is the sole ZCB market maker by issuing bonds in the prediction market AMM.

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 expected returns from i's proposal, 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. Liquidity 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(`shortZCB` buyer) 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(set as some fraction of the instrument's principal). Maximum net `longZCB` that can be accrued 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`.

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 profit for `longZCB` defines `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 amplifyiing her exposure to this instrument. Equally, an informed VT holder who decides to hedge against the instrument can purchase `shortZCB`, enabling customizability and non-uniform exposure to different investment opportunities.

However, a `shortZCB` buy / `longZCB` sell is penalized by a fee that decreases monotonically until 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 synthetic 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 expirary 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`.

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 cascade(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.

- Only those with high reputation scores can participate early(where prices are lower) in the `longZCB` sale from the utilizer: 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)
- Budget: 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 her reputation. Clearly, this would directly place more weight for those with higher reputations, while allowing them to place heavier bets.

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 when negating plausible attacks. Below we list a non-exhaustive list and a corresponding solution for each.

5.1 Sybil

Sybil attacks 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 and every instrument's market requires the reputable manager 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 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).

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 it's balance of locked VT(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 almost designed to be monotically increasing, it may incentivize some to frontrun 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 market is initialized 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 post-assessment phase is higher than that of assessment phase (as 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 mortgages originators). As stated previously, this behaviour is penalized as the AMM induces a selling fee(incured 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.

5.5 Manager's collusion with utilizers

This attack is prevented via the reputation mechanism, a manager's finite budget for each instrument(thereby requiring a diverse set of managers for approval), and the randomness when choosing the validators.

5.6 Frontrunning Instrument Profit

Another trivial attack would be minting VT just before an instrument successfully matures, which allows the minter to realize profit without bearing risk. This can be mitigated(to some extent) by inducing a withdrawal fee.

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. A vault instance(and a new VT deployed) can be created for different instrument classes. Below we present some examples.

6.1 CreditLine

A straightforward example would be a creditline instrument. 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 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 who 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 risk underwriting/structuring process to a set of (reputable)managers from the protocol by creating a new vault. These entities can be DAOs that wants to delegate the risk assessment/structuring for their treasuries that need management to a non-centralized entity, or someone who wants prediction markets, risk assessment, or tranching for niche instrument classes.