Risk Harbor Ozone

Max Resnick
max@riskharbor.com

Raouf Ben-Har
raouf@riskharbor.com

Drew Patel
drew@riskharbor.com

Atul Bipin
atul@riskharbor.com

***Abstract*—Risk Harbor is a risk management marketplace for decentralized finance (DeFi) that utilizes a completely automated, transparent, and impartial claims process to protect liquidity providers and stakers against smart contract risks, hacks, and attacks. Risk Harbor V1 introduced a protocol for automated risk transfer financial derivatives adjudicated by smart contracts. Risk management protocols are heavily constrained by the lack of available underwriting capital. Risk Harbor solves the problem of insufficient underwriting capital by using vaults. Vaults hold capital that can be used to provide protection on many protocols simultaneously. Alongside vaults, we developed an Automated Market Maker (AMM) tailored to risk management marketplaces. The AMM understands risk programmatically and prices protection accordingly. The AMM also allows the vault to enter leveraged positions, which is the fundamental pillar of generating competitive rewards for users providing capital.**

I. Introduction

Decentralized Finance (DeFi) protocols rely on deposits from users to function properly. Without liquidity providers, we would not have decentralized exchanges like Terraswap. Without lenders, we would not have decentralized money markets like Mars. Whenever users deposit funds into a protocol, there is a non-negligible risk that those funds may be lost. Over 1 billion dollars has already been lost to hacks, bugs, and attacks; while the size, scope, and severity of these loss events continues to rise exponentially.

These risks are not unique to DeFi; depositors in traditional finance also face deposit risk. But in traditional finance, there are systems in place that protect depositors from the risks associated with their deposits. For depositors in US banks, the Federal Deposit Insurance Corporation (FDIC) protects deposits up to 250,000 \$. Other solutions exist for deposits over 250,000 \$. Lenders in traditional finance have access to a robust market for risk transfer financial derivatives that allow them to offset default risks. However, analogous structures do not exist in DeFi yet.

The first attempts at blockchain-based decentralized protection relied on governance to assess claims. This introduced a major conflict of interest: those who held governance tokens were often the very same actors who were underwriters in the protocol. Therefore, those who decided on the validity of claims were deciding whether to give away their own money to cover the losses. In other words, they had every incentive to deny claims, regardless of their validity. Truly decentralized protection requires properly aligned incentives. This means that evaluating a claim must either be done by a party whose only interest in the matter is to evaluate the claim correctly, or the evaluating party must be eliminated entirely. Additionally, governance-based protection requires subjective agents to manually vote on the validity of a claim, which is simply not scalable. Since governance-based protection cannot scale at the same rate that DeFi does, it will ultimately become obsolete.

Risk Harbor V1 demonstrated that subjective agents could be completely eliminated from the claims assessment process, replaced by parametric smart contracts designed specifically for detecting default events. We found that by checking key invariants on-chain, we were able to identify whether a protocol was hacked or not in a completely objective and codified manner. This process is much faster than governance-based claims assessments, and notably eliminates the perverse incentives that can arise when governance token holders also have major shares of underwriting capital in the protocol. Moreover, parametric protection can accommodate volume at scale.

II. Risk Management on Terra

A. UST

Uncertainty about the stability of UST has prevented cautious investors from reaping the bountiful rewards available in the Terra ecosystem. Providing protection against a UST depeg event will serve a dual purpose. First, it will enable risk averse investors to enter the ecosystem, protected by Risk Harbor Terra. Second, it will stabilize the price of UST itself by preventing cascading loss of confidence in the stablecoin. By accumulating a pool of stablecoins and primitives such as Wrapped BTC and Wrapped ETH, Risk Harbor Terra will be a buyer of last resort for UST in the event of a depeg.

B. Anchor

Competitive, stable yields on Anchor have attracted a large number of depositors. Many of these depositors would have liked to purchase protection but supply of underwriting capital was not nearly enough to keep up with demand.

The unmet demand for Anchor protection must be met as soon as possible. Making protection available, natively on Terra, will usher in a new wave of users to the ecosystem who were previously kept away by uncertainty about the security of their deposits. Moreover, it will strengthen Anchor protocol and the broader Terra ecosystem by preventing cascading loss of confidence in the protocol.

C. Mirror

Peg protection on Mirror assets would allow risk averse traders to set up trusted, protected, foreign currency and stock exchanges using synthetic assets. Liquidation protection could protect synthetic asset minters from flash volatility risks and oracle manipulation risk.

III. Risk Harbor Protocol

A. Credit Default Swaps

In order to file a claim on Risk Harbor, users first transfer credit tokens to the protocol. If the claim is deemed to be valid, then those credit tokens are swapped for the underwriting tokens. This financial derivative is known as a Credit Default Swap. The use of a Credit Defualt Swap as opposed to a simple payout has many security advantages for the protocol. First, it safeguards against profitable manipulation of the invariant. Even an adversary who had complete control over the default detector could not make a profit without the underlying protocol having been hacked. Second, it ensures that policyholders must actually be able to procure distressed assets to file claims, which makes it more difficult for opportunistic actors to use the protocol as a vehicle for price speculation, which can drive up prices for people who actually want to use the protocol for protection.

B. Initial Deployment for Terra

The first iteration of Risk Harbor Terra will begin with protection for Anchor protocol. The default detector will be an implementation of the default detector already deployed on Ethereum mainnet for the Risk Harbor Anchor pool. The anchor vault will not have leverage initially since it will only be covering one protocol. The payout mechanism will be a credit default swap, meaning users will exchange distressed aUST for UST during the automated claims process.

The remainder of this paper details future plans for Risk Harbor Terra

IV. Multi Pool Vaults

Capital efficiency is critical for risk transfer markets. An overcollateralized solution such as the ones that exist in lending markets would not be able to function unless heavily subsidized, since underwriters could simply take on the risks themselves and earn higher yields rather than underwrite the risk for others. This means that the same underwriting capital must be used to simultaneously underwrite risk on many different protocols. The limitation of this approach is that when all the pools are hacked simultaneously, the vault is unable to pay out all of its obligations. The severity of this limitation depends on the independence of the risks in each of the protocols that the vault has outstanding protection on. When risks are independent, the probability of vault default events is much lower than the probability of individual default events; however, this does not hold when one protocol failure cascades and causes others to fail as well.

In the near future, Risk Harbor will rely on a vault architecture that concentrates capital in a central vault, allowing it to be used to underwrite a wide range of protocols. Default detector contracts will be stored separately. The vault will call the appropriate default detector contract whenever a claim is filed and pay out if the default detector returns true, meaning the underlying protocol has suffered a loss event.

V. Automated Market Maker (AMM)

Our research team developed a risk aware automated market maker tailored specifically to risk transfer financial derivative markets. It relies on classical models of risk averse agents from microeconomic theory. In particular, it acts like an expected utility maximizing agent with a concave utility function would act, given some model of the risks associated with the various protocols that it offers to sell protection on.

Let $X = \{X_1, \ldots, X_n\}$ be an ensemble of not necessarily independent not necessarily identically distributed random variables $X_i : \Omega \to [0, 1]$ for some common measure space Ω. These Random variables represent the loss events on the various pools. For example, suppose the vault offered protection on a protocol that had a 5 percent probability of being hacked and losing all of the deposited money and otherwise the funds were safe. Then the random variable X_i corresponding to that pool would be distributed according to bernouli$(.5)$. The larger the proportion of principle lost, the higher the realization of the random variable. In the event that no funds from pool i are lost, $X_i = 0$.

Let $A = \{A_0, \ldots, A_1\}$ be a vector that stores the assets and liabilities of the protocol. In particular, let A_0 be the cash on hand which is defined as the total deposited underwriting capital plus the premiums paid minus the amount of capital paid out to fund valid claims. Let $A_1, \ldots, A_n$ be the outstanding protection amount on pools $1, \ldots, n$ respectively.

Whenever an underwriter deposits, A_0 will increase by the amount that they deposited. Whenever a policy is purchased, A_0 will increase by the premium amount, and A_i will increase by the notional policy size where i is the pool that the protection was purchased for. Whenever a claim is paid out, A_i will decrease by the size of the claim and A_0 will decrease by the size of the payout.

Desirable qualities for a risk management marketplace AMM:

- (increasing in self) $\forall i$, if $A'_i < A''_i$, then $\frac{\frac{\partial f}{\partial C}}{\frac{\partial f}{\partial A_i}}(C, A', X) < \frac{\frac{\partial f}{\partial C}}{\frac{\partial f}{\partial A_i}}(C, A'', X)$
- (increasing in non disjoint others) $\forall i, j$, if supp(X_j) is not disjoint from supp(X_i) and $A'_j < A''_j$, then $\frac{\frac{\partial f}{\partial C}}{\frac{\partial f}{\partial A_i}}(C, A', X) < \frac{\frac{\partial f}{\partial C}}{\frac{\partial f}{\partial A_i}}(C, A'', X)$
- (decreasing in underwriting capital)$\forall i$, if $C' < C''$, then $\frac{\frac{\partial f}{\partial C}}{\frac{\partial f}{\partial A_i}}(C', A, X) < \frac{\frac{\partial f}{\partial C}}{\frac{\partial f}{\partial A_i}}(C'', A, X)$
- (above actuarial fair) $\forall i, C, A, X$, $\frac{\frac{\partial f}{\partial C}}{\frac{\partial f}{\partial A_i}}(C, A, X) > E[X_i]$
- (able to enter leverage) $\sum_{i=1}^n A_i$ can exceed C.

Let $u : \mathbb{R}_+ \to \mathbb{R}_+$ be a monotonically increasing concave function. Then the market maker is a constant function market maker with function:

$$f(C, A, X) = E[u(C - \sum_{i=1}^{n} A_i X_i)] \tag{1}$$

This can be expressed equivalently in vector notation as

$$f(C, A, X) = E[u(C - A \cdot X] \tag{2}$$

Theorem V.1. *The AMM defined in equation (1) satisfies properties 1-4*

Proof. See Risk Harbor V2 whitepaper □

The AMM will arrive in Risk Harbor Terra V2. More details about the AMM are forthcoming in the Risk Harbor V2 whitepaper.

VI. Risk Engine

If two different lending protocols, Compound and AAVE, exist on the same network, how likely is it that a cascading deflationary spiral on Compound will result in a cascading deflationary spiral on AAVE? These types of questions are extremely important for managing leveraged vaults that provide protection on many protocols. As part of Risk Harbor's research efforts, we have invested significant time into building generalized models of risk across ensembles of DeFi protocols. Others have produced valuable reports on the risks involved with individual protocols; however, little work has been conducted on how these individual protocol risks correlate with each-other. Our approach utilizes structural modeling and dependency graphs to incorporate information about systemic dependencies and cross-protocol cascading failure into our risk models.

Alongside our work on cross-protocol dependencies, we developed a useful partitioning of the types of risks that can result in loss events on DeFi protocols. We defined 3 broad categories of risk: contract, governance, and structural.

Contract risk refers to misspecified smart contracts, improperly permissioned functions, and generally all of the kinds of risks that can be caught in a properly conducted smart contract security review.

Governance risk refers to the risks associated with the owners of the contracts. This can be an individual wallet, a multisig vault, or even a fully fledged DAO. The most common types of governance risk are rug pulls, and stolen keys.

Structural risk refers to loss events where code operates as intended and can occur without malicious actors taking control of the contracts themselves. Common examples include oracle failure, flash loan attacks, deflationary spirals, and impermanent loss.

VII. Governance & Tokenomics

The Risk Harbor token will launch after the launch of Risk Harbor Terra V1. Governance token holders will make critical macro level decisions for the protocol but will not be involved in the micro level pricing and leveraging decisions. Those will be decided by the markets themselves. These decisions will include but are not limited to:

1) Adjusting risk parameters
2) Whitelisting protocols
3) Creating new vaults
4) Adjusting risk tolerance on vaults
5) Levying and adjusting protocol fees

VIII. Disclaimer

This paper is for general information purposes only. It does not constitute investment advice or a recommendation or solicitation to buy or sell any investment and should not be used in the evaluation of the merits of making any investment decision. It should not be relied upon for accounting, legal or tax advice or investment recommendations. This paper reflects current opinions of the authors and is not made on behalf of Risk Harbor or their affiliates and does not necessarily reflect the opinions of Risk Harbor, their affiliates or individuals associated with them. The opinions reflected herein are subject to change without being updated.