Risk Harbor V2

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 invariant detection mechanism to secure liquidity providers and stakers against smart contract risks, hacks, and attacks. Blockchain-based risk management protocols are heavily constrained by a shortage of available underwriting capital. Risk Harbor V2 solves the problem of insufficient underwriting capital 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 Uniswap. Without lenders, we would not have decentralized money markets like Compound. 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 (see table 1); while the size, scope, and severity of these loss events continues to rise exponentially.

TABLE I
VALUE LOST TO BUGS, HACKS, AND ATTACKS

Protocol	Blockchain	Value Lost
Polynetwork	Etherum, BSC, Polygon	$600 Million
PAID network	Ethereum	$180 Million
Parity	Ethereum	$160 Million
C.R.E.A.M	Ethereum	$130 Million
Easyfi	Polygon	$80 Million
Compound	Ethereum	$80 Million
BzX	BSC, Polygon	$55 Million
DAO	Ethereum	$50 Million
Uranium Finance	Binance Smart Chain	$50 Million
Alpha Finance	Ethereum	$37 Million
C.R.E.A.M	Ethereum	$36 Million
Vee Finance	Avalanche	$35 Million
Parity	Ethereum	$30 Million
C.R.E.A.M	Ethereum	$29 Million
dForce	Ethereum	$25 Million
Harvest	Ethereum	$24 Million
Pickle Finance	Ethereum	$20 Million
Indexed Finance	Ethereum	$16 Million
Meercat Finance	Binance Smart Chain	$13 Million
Thorchain	Cosmos SDK	$13 Million
Yearn	Ethereum	$11 Million
Maker	Ethereum	$9 Million
bZx	Ethereum	$8 Million
Warp	Ethereum	$8 Million
Cover	Ethereum	$4 Million
Total		$1.7 Billion

Sources [1], [2], [3], [4], [5], [6], [7] [8], [9], [10], [10], [11], [12], [13].

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 each claim, which is a major barrier to scalability. Unless governance-based protection protocols find a way to scale as fast as DeFi does, they 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 Harbor Protocol

A. Claim Tokens

Deposits in DeFi protocols are often represented by claim tokens which are minted when deposits take place and burned when the underlying capital is withdrawn. For example, USDC deposits in Compound are represented by cUSDC. Risk Harbor's automated claims assessment process checks the redeemability of claim tokens with the protocol that issued them by examining key invariants that differ from protocol to protocol. The Risk Harbor V1 whitepaper offers a more in depth explanation of this mechanism.

B. Invariant Triggered Buyout

In order to file a claim on Risk Harbor, users first transfer claim tokens to the protocol. If the claim is deemed to be valid, then those claim tokens are exchanged for the underwriting tokens. In comparison to settling claims in cash, an invariant triggered buyout has many advantages. First, it safeguards against profitable manipulation of the default detector contract. 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, an action which can drive up prices for people who actually want to use the protocol for protection.

C. Composability

Composability in DeFi has been a core contributor to its success. Risk Harbor relies heavily on this composability in its default detectors, its invariant triggered buyout mechanism, and for capital efficiency. Risk Harbor vaults are also post composable with other protocols. Risk Harbor claim tokens can be bundled together to create highly customizable risk profiles. Risk Harbor underwriting positions can be held and actively managed by yield aggregation protocols. Risk Harbor pools can be created to protect underwriting deposits in other Risk Harbor pools. Underwriting capital in a vault can be invested into other protocol's reward bearing assets. A Risk Harbor protection position can be wrapped together with a protected claim token to create a single protected token.

III. Multi Pool Vaults

Capital efficiency is critical for risk transfer markets. An overcollateralized solution such as the ones that currently exist in DeFi lending markets would not be able to function unless heavily subsidized, since underwriters could simply take on the risks themselves and earn higher rewards 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.

Risk Harbor V2 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.

IV. Automated Market Maker

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 modern portfolio 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.

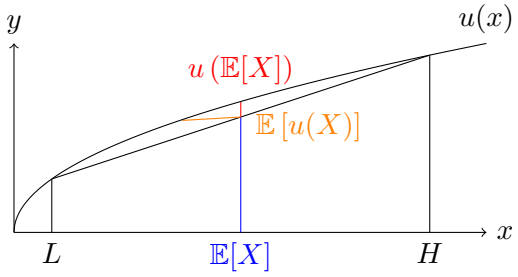

Fig. 1. Classical Model of Risk Aversion

Figure 1 depicts the classical model of a risk averse agent with a concave utility function u. Suppose the risk averse agent earns X, a random variable that can be either low, L, with probability .5 or high, H, with probability .5. How much would the risk averse agent be willing to pay to buy protection that allows him to receive H all the time? The expected benefit of this would be $(H-L)/2$, this is known as the actuarially fair price. If the agent only pays $(H-L)/2$, he will receive $u(\mathbb{E}[X])$ depicted in red. Before he paid for protection, his expected utility was $\mathbb{E}[u(X)]$ so he is strictly better off paying for the protection. But he could pay slightly more than the actuarially fair price for the protection and still be better off. Any additional premium he pays is known as the risk premium. The maximum risk premium that the agent would be willing to pay in this case is depicted as the orange line in the figure.

Now we can begin to formalize what we described in the first paragraph, starting with what a model of risks looks like. Let $X = (X_1, \ldots, X_n)$ be an ensemble of not necessarily independent not necessarily identically distributed random variables $X_i : \Omega \to [-1, 0]$ for some common measure space Ω. These random variables represent a model of loss events on the various pools that the vault offers protection on. For example, suppose the vault offered protection on a protocol that had a 5 percent chance 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 $0-\text{Bernoulli}(.05)$. The larger the proportion of principle lost, the lower the realization of the random variable. In the event that no funds from pool i are lost, $X_i = -1$. For ease of notation, we introduce a probabilistic modeling of the risk free asset $X_0 \equiv 1$ and include it in the ensemble $X = (X_0, \ldots, X_n)$.

Let $A = (A_1, \ldots, A_n)$ be a vector that stores the assets and liabilities of the protocol. In particular, $A_1, \ldots, A_n$ represent the purchased protection on pools $1, \ldots, n$ respectively. For ease of notation, we introduce A_0, which represents the amount of the risk free asset that the vault holds.

Whenever an underwriter deposits, A_0 will increase by the amount that they deposited. Whenever a policy is purchased from pool i, A_0 will increase by the premium amount, and A_i will increase by the notional policy size. 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.

Now we can begin to discuss the properties that we would like our AMM to satisfy. First, it should be the case that the marginal cost of protection on a particular pool is increasing in outstanding protection on that pool. Similarly, if hacks on pool i coincide at least some of the time with hacks on pool j, then the marginal price of protection on pool i should be increasing in the amount of outstanding protection on pool j. It should also be the case that the vault is more willing to pay out protection when it has more underwriting capital. In practice, this should mean that the marginal cost of protection on all pools should decrease as underwriting capital increases.

Finally, the marginal price of protection should always be at least the actuarially fair price for protection so that the vault is never making a trade that causes assets at expiry to be lower in expectation. These properties can be expressed mathematically as follows:

- (increasing in self) $\forall i$, if $A_i < A'_i$, then
$$\frac{\partial_{A_i} f}{\partial_{A_0} f}(A) < \frac{\partial_{A_i} f}{\partial_{A_0} f}(A')$$
- (increasing in non disjoint others) $\forall i, j$, if $\text{supp}(X_j)$ is not disjoint from $\text{supp}(X_i)$ and $A_j < A'_j$, then
$$\frac{\partial_{A_i} f}{\partial_{A_0} f}(A) < \frac{\partial_{A_i} f}{\partial_{A_0} f}(A')$$
- (above actuarially fair) $\forall i$ and for any A,
$$\frac{\partial_{A_i} f}{\partial_{A_0} f}(A) \geq \mathbb{E}[X_i]$$

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:

$$f_X(A) = \mathbb{E}\left[u\left(\sum_{i=0}^{n} A_i X_i\right)\right] \tag{1}$$

This can be expressed equivalently in vector notation as

$$f_X(A) = \mathbb{E}\left[u(A \cdot X)\right] \tag{2}$$

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

Proof. (increasing in self). Suppose $A_i < A'_i$. It follows that the random variable $A \cdot X$ weakly first order stochastically dominates $A' \cdot X$. From this we can see that:

$$\begin{aligned}
\frac{\partial_{A_i} f}{\partial_{A_0} f}(A) &= \frac{\partial_{A_i} \mathbb{E}[u(A \cdot X)]}{\partial_{A_0} \mathbb{E}[u(A \cdot X)]}(A) && (3)\\
&= \mathbb{E}\left[\frac{\partial_{A_i} u(A \cdot X)}{\partial_{A_0} u(A \cdot X)}(A)\right] && (4)\\
&< \mathbb{E}\left[\frac{\partial_{A_i} u(A \cdot X)}{\partial_{A_0} u(A \cdot X)}(A')\right] && (5)\\
&= \mathbb{E}\left[\frac{\partial_{A_i} u(A \cdot X)}{\partial_{A_0} u(A \cdot X)}(A')\right] && (6)\\
&= \frac{\partial_{A_i} f}{\partial_{A_0} f}(A') && (7)
\end{aligned}$$

The inequality in equation (5) is true by the weak first order stochastic domination discussed above.

(increasing in non-disjoint support others) Suppose $A_j < A'_j$ and $\text{supp}(X_i) \cap \text{supp}(X_j) \neq \emptyset$. It follows that the random variable $A \cdot X$ weakly first order stochastically dominates $A' \cdot X$. Then, the proof proceeds identically to the proof of increasing in self.

(above actuarially fair) This property, like the one above follows directly from the strict concavity of u:

$$\begin{aligned}
\frac{\partial_{A_i} f}{\partial_{A_0} f}(A) &= \frac{\partial_{A_i} \mathbb{E}[u(A \cdot X)]}{\partial_{A_0} \mathbb{E}[u(A \cdot X)]}(A) && (8)\\
&\geq \frac{\partial_{A_i} u(\mathbb{E}[A \cdot X])}{\partial_{A_0} \mathbb{E}[u(A \cdot X)]}(A) && (9)\\
&= \frac{\partial_{A_i} u(\mathbb{E}[\sum_{i=0}^{n} A_i X_i])}{\partial_{A_0} \mathbb{E}[u(A \cdot X)]}(A) && (10)\\
&= \frac{u' \mathbb{E}[A_i]}{u'}(A) && (11)\\
&= \mathbb{E}[X_i] && (12)
\end{aligned}$$

□

A. Leverage

The only difference between the leveraged case and the unlevered case is that, in the levered case, there is a probability that the vault will have negative assets at expiry. More concretely, when the AMM is under leverage we have:

$$P\left[A \cdot X < 0\right] > 0 \tag{13}$$

In other words, there is a non 0 probability that the vault will have to pay out more in protection than it has on hand. This is not a problem, so long as the u function has been properly extended onto the negative real line. Many common concave functions do not behave well on the negative real axis (e.g $\log$). The particulars of the extension depend on the u function itself. It is useful to think of these values as penalties for a default of a certain size.

B. Price decay over time

In a vault with a fixed expiry date, protection should become less valuable as time passes since part of the hazard period has already passed. To accommodate this, we substitute $X = (X_1, \ldots, X_n)$ for the family $X_\delta = (X_{1,\delta}, \ldots, X_{n,\delta})$ where $\delta \in [0, 1]$ represents the time that has elapsed as a proportion of the vaults total lifespan. Each $X_{i,\delta}$ is the random variable X_i, conditional on the fact that δ time has passed already. This family of risk models, defines a corresponding family of constant function AMMs:

$$f(A) = \mathbb{E}\left[u(A \cdot X_\delta)\right] \tag{14}$$

Since part of the hazard region has passed, we can assume that the magnitudes of the entries in X_δ are

decreasing in δ. Hence the prices of protection should be decreasing in δ. In options markets, this type of price decay over time is represented by $\boldsymbol{\theta}$.

V. Risk Engine

If two different lending protocols, such as 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.

Together, with structural models, partitioning the space of risks into these three categories allows us to model many types of risks computationally and allows us to model correlated risk across protocols.

VI. Governance & Tokenomics

The Risk Harbor token launch date is still yet to be determined. Governance token holders will make critical macro level decisions for the protocol including but not limited to: adjusting risk parameters, whitelisting new protocols, creating new vaults, adjusting risk tolerance on vaults, levying and adjusting protocol fees. But they will not be involved in the micro level pricing and leveraging decisions. Those will be decided by the markets themselves.

References

[1] Jeff Benson. $11 million gone in yearn finance exploit, Feb 2021.

[2] Defi platform bzx sees new $8m hack from one misplaced line of code.

[3] Colin Harper. Defi exchange uranium finance loses $50m in exploit, Apr 2021.

[4] Becky Peterson. The amount of ether frozen in digital wallets is worth $162 million - which is less than initially feared, Nov 2017.

[5] Conor Maloney and Conor Maloney. Grap finance claims responsibility for $4m cover protocol hack, returns funds, Dec 2020.

[6] Kayleigh Petrie. bzx flash loan event, Feb 2020.

[7] Martin Young. Warp finance reportedly loses up to $8m in flash loan attack, Dec 2020.

[8] Andrew Asmakov. Avalanche defi platform vee finance suffers $35m hack, Sep 2021.

[9] Ryan Browne. Crypto platform hit by $600 million heist asks hacker to become its chief security advisor, Aug 2021.

[10] Catalin Cimpanu. Hacker steals $24 million from cryptocurrency service 'harvest finance', Oct 2020.

[11] Jamie Crawley. Defi project meerkat raises eyebrows with claimed $31m hack a day after launch, Mar 2021.

[12] Defi pulse: The defi leaderboard: Stats, charts and guides.

[13] Andrew Thurman. $22m drained from compound contract that was hit for $80m last week, Oct 2021.

VII. Disclaimer