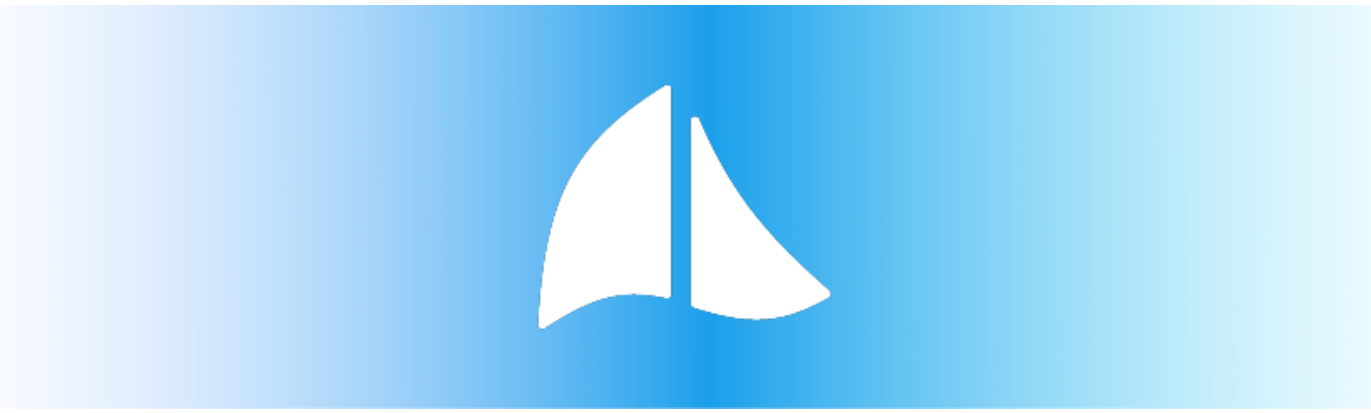
# Risk Harbor V1



Raouf Ben-Har
raouf@riskharbor.com

Drew Patel
drew@riskharbor.com

Albert Su
albert@riskharbor.com

Max Resnick
max@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.**

## I. Introduction

Today, more than $60 billion is locked in DeFi protocols and smart contracts have suffered over $375 million in losses from hacks and attacks (See table I). DeFi Liquidity providers and stakers are exposed to an enormous amount of acute risk. In traditional financial markets, market makers would use put options, credit default swaps, or other derivatives to manage this risk, but in decentralized finance (DeFi), these derivatives either do not exist or are too expensive to be used for loss-protection. Risk Harbor fills this gap by providing automated risk mitigation contracts, tailored to fit the needs of liquidity providers and stakers.

TABLE I
VALUE LOST TO BUGS, HACKS, AND ATTACKS

| Protocol | Blockchain | Value Lost |
|---|---|---|
| Parity | Ethereum | $160 Million |
| DAO | Ethereum | $50 Million |
| Uranium Finance | Binance Smart Chain | $50 Million |
| Parity | Ethereum | $30 Million |
| dForce | Ethereum | $25 Million |
| Pickle Finance | Ethereum | $20 Million |
| Yearn | Ethereum | $11 Million |
| Maker | Ethereum | $9 Million |
| bZx | Ethereum | $8 Million |
| Warp | Ethereum | $8 Million |
| Cover | Ethereum | $4 Million |
| Total | | $375 Million |

Sources [1], [2], [3], [4], [5], [6], [7].

## II. Existing Solutions

In traditional protection markets, when someone files a claim, the underwriter or claims adjuster evaluates the claim to determine its validity. This requires an element of trust between the claims adjuster and the policyholder. In the world of DeFi, however, anonymity allows users to exploit trust based systems for personal gain without fear of repercussion.

Existing risk management protocols in DeFi rely on underwriters to assess whether or not a claim is valid and if a claim should be paid out or not. But this process of allowing underwriters to vote on claim legitimacy is inherently flawed. The underwriters are the people who stand to lose most from a valid claim, therefore, they do everything in their power to ensure that a claim is invalid, regardless of the underlying merit of the claim. This is a clear conflict of interest.

In both the outside world and in DeFi, an underwriter's primary goal is to optimize profits by collecting premiums and denying as many claims as possible. As a result, many policyholders have become victims of vague and exploitative legal terms that allow underwriters to avoid paying out legitimate claims. This has led to numerous disputes between underwriters and policyholders that invariably resulted in unfair outcomes.

Put options provide a trustless but expensive alternative to governance based protection. A put option gives the option holder the option but not the obligation to sell an underlying asset for a set price at a future date. When a protocol is hacked, the protocol's token price plunges and those who own put options can exercise their right to sell that token for the previously agreed-upon price to cover their losses. This effectively makes option writers protection underwriters.

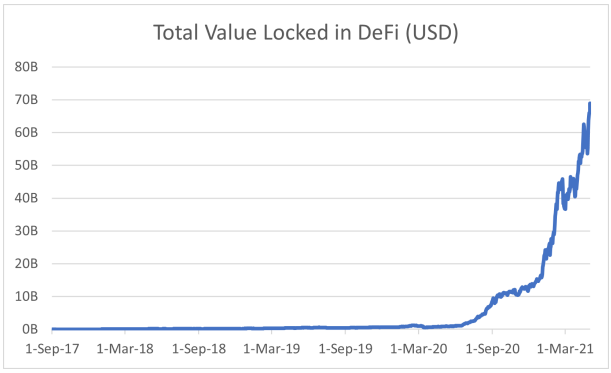



Fig. 1. Total Value locked in DeFi (2017-2021) [8]

However, option writers are exposed not only to hacks but also to the high volatility of most crypto assets. Thus, the option must be priced to prevent profitable speculation on the volatility of the underlying asset. As a result, options are not only too risky and expensive but are not a viable long-term solution for risk management.

## III. Risk Harbor Protocol

Risk Harbor is a risk management marketplace which allows users to purchase protection that objectively evaluates and automatically pays out in the event of a hack or exploit on a protected contract. Instead of buying overpriced put options or other derivatives, users can purchase protection on Risk Harbor that shields them from individually selected risks. In other words, users on Risk Harbor, only pay for what they need.

Protection will be underwritten by other users, known as underwriters, who will also partake in and help build parametric protection. Underwriters will have the ability to create a variety of unique protection pools with custom parameters such as: `premium`, `protected_events`, `loss_threshold`, `underlying-to-protected`, and `pricing_asset`. Underwriters also have the opportunity to join existing pools created by other underwriters.

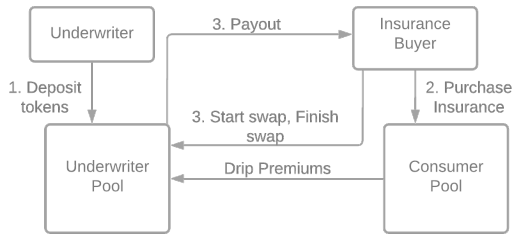



Fig. 2. Protection Pool

When users want to purchase protection, the total premium is paid upfront and then a proportional amount is added to the underwriters' pool every block. An underwriter can withdraw their initial capital in addition to premiums accrued at any time, as long as their withdrawal maintains the minimum capital requirement of the pool.

Risk Harbor delivers value through its permissionless nature and objective claim evaluation engine. Risk Harbor is available to all users and does not require Know Your Customer (KYC), so DeFi newcomers can purchase protection without having to jump through legal hoops. For DeFi power-users and institutions, Risk Harbor allows the purchase and sale of curated invariant triggered buyouts.

## IV. Invariant Detection Mechanism

Smart contracts exist in an observable finite state. Defining what constitutes a payout event is equivalent to figuring out how different variables will change in an event of a hack or attack. If all the tokens are stolen from a contract, the balance of the contract will fall but claims tokens will not therefore, the Underlying-To-Claim Ratio will decrease. If that contract was a lending pool, then the claim token's redemption rate will go from $R$ to 0. If the contract is paused, then the paused variable is set to true.

$$\text{Underlying-To-Claim-Ratio} = \frac{\text{UnderlyingTokens}}{\text{ClaimTokens}} \quad (1)$$

Take for example Compound's USDC pool which gives depositors USDC claim tokens (cUSDC) proportional to the USDC they deposit into the pool. If Compound were hacked and all its USDC was stolen, the balance of cUSDC in the contract would drop to 0. A Risk Harbor policyholder could then begin the three-step claims process to cover their loss. First, they would approve the transfer of the claimToken to the Risk Harbor Claim contract. Then they would call `startSwap` followed by `finishSwap`. Users are required to wait at least one block after calling `startSwap` before calling `finishSwap` to prevent flash loan attacks. Risk Harbor contracts are able to check the redeemability of the claimToken without actually redeeming it. If the redeemability is below the defaultRatio threshold and as long as residual checks (such as Compound being paused or having a liquidity crisis) aren't at play, the user is paid out. The claimsTokens are then transferred to the underwriters fulfilling the last part of the invariant triggered buyout. If the cUSDC token holders were paid restitution in the future, the underwriters would be the recipients of it since they would hold the claim tokens. Claims

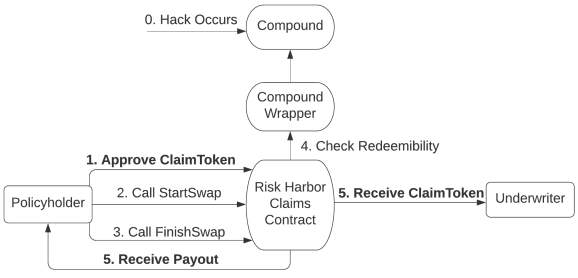



Fig. 3. Claims Process

wrappers are custom-designed for specific protocols to capture

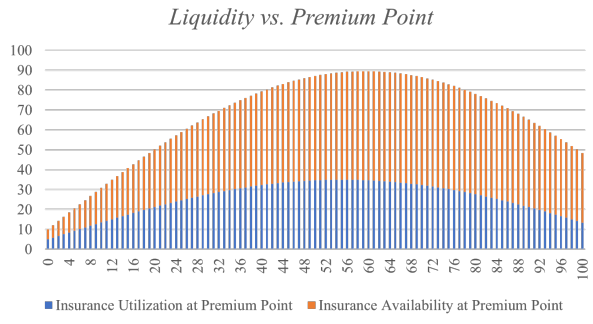



Fig. 4. Premiums vs Utilization

the nuances and risks that each implementation presents. In general, the differences between wrappers for two protocols in the same sector like Compound and Aave are miniscule. The differences between wrappers for different sectors, like DEXs and Lending Pools, are significant.

## V. False claim attacks

Policyholders filing false claims that the protocol deems as legitimate is a potential risk. To mitigate this risk, we utilize a copay to economically dissuade false claims. A copay is the percentage of loss that the policyholder must bear. The copay is applied to the payout calculation in the `finishSwap` function. For example, if a user files a false positive claim on their cUSDC in Compound with a 5% copay, they would be paid

$$(1 - .05)T < T \tag{2}$$

USDC. Where $T$ is the number of protected claim tokens. But, they could instead use their claim tokens to release $T$ USDC from compound without the copay. Therefore there is no incentive to file false claims.

## VI. Pricing

Underwriters may perceive the risk of a single protocol differently. This means underwriters will demand a wide range of premiums instead of one single premium. Since premiums are denoted in percentages, it is possible to create a dynamic pricing curve which retains gas efficiency since only 99 elements [1,100] are needed to create the price curve. At each percentage point, both the available liquidity and utilized liquidity are stored. As capital is added and removed at a specific premium point, total liquidity changes. As protection is sold at a specific price point, utilized liquidity increases. If a user attempts to buy a large amount of protection that exceeds the available liquidity in the cheapest premium slot, an algorithm will break up the order into smaller pieces that are optimally allocated across multiple premium points.

Underwriters will prefer providing liquidity to highly utilized pools where premiums are highest because more of the deposited capital is in use. This funnels capital towards the most in demand pools.

## VII. Composability

Composability allows for the creation of complex protection products and allows underwriters to limit their losses. In DeFi, capital always flows towards activities with high yields. This forces protocols to perpetually compete amongst each other for capital. If Compound offers depositors of USDC 8% in rewards, Risk Harbor must provide >8% in rewards alongside a risk premium to bring capital over. If an underwriter assumes all the risk of the protected protocol and is given only a fraction of the yield generated, they could just invest in the protocol itself instead of protecting it. This leads to less underwriting capital and higher premiums.

To mitigate this, Risk Harbor allows underwriters to underwrite with an array of tokens including claim tokens such as cUSDC and Uniswap LP. As a result, previously idle tokens can earn additional yield as underwriting capital. This increases capital inflow and decreases premiums.

Allowing underwriters to limit their losses is another advantage of composability. By purchasing re-protection, underwriters can limit their payouts to a certain range and offload critical losses to other underwriters. This feature will be rolled out in later versions of the protocol.

## VIII. Tokenomics and Governance

### A. Governance

Alongside all normal functions of governance, RH token holders will be able to vote on which protocols to protect and which protocols to stop protecting.

### B. Dev mining

Developers will be rewarded in tokens for creating wrappers for the protocols that governance votes to include.

### C. Pool Creation

To incentivize the creation of high quality pools and to reduce liquidity fragmentation, pool creators will have to stake a certain amount of RH tokens. If the pool becomes popular, their stake will be released, and they will be given additional tokens for creating a popular pool.

### D. Liquidity Mining

To incentivize early underwriters, there will be early liquidity mining rewards.

### E. Long-term Incentives

There are two mechanisms which incentivize long term participation. First, Risk Harbor will leverage Liquidity Mining - similar to the early rewards but over a longer period of time. Second, DEX liquidity providers will be allowed to underwrite with their RH LP tokens in a long-dated protection pool that protects the Risk Harbor protocol.

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


## IX. 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.