Insurance as a Market Design Tool in DeFi

Abhimanyu Nag • 4 Apr 2026

Special thanks to friends at Catalysis Labs whose reviews were very helpful in writing this up. Thanks to Ming from Gauntlet for his insightful observations and Srisht Fateh Singh from UToronto for raising a point that made me think

> Why do you not have your crypto in a Morpho vault or something? What did you say? You don't care about crypto? You don't think it's safe? You think it's too risky and it's a fad? AI will take over anyway? But look at all that yield™ just waiting for you to..okay never mind I understand

Above is probably an average conversation on the street. The problem of large scale adoption of DeFi is nothing new but at this point sounds too old. More than 560 million people globally owned crypto in 2024, yet DeFi activity is low, with regulators estimating roughly 54 million DeFi users worldwide and much lower regular engagement. Even where there is capital, usage is still not mainstream. Morpho, for example, scaled from institutional demand to more than $9 billion in deposits by July 2025. Unfortunately this means that vault adoption today still belongs mostly to experienced onchain users, not ordinary people like you and me.

Insurance as an incentive tool

Picture this. You have USDC lying around. USDC vaults exist on Morpho. You can easily put some of your (hard earned hopefully through onchain degeneracy) USDC to say the Gauntlet USDC Prime Vault and earn some of that nice 3.72% yield on your deposit. Sounds good right?

You will say "Are you crazy? Don't you remember what happened a few days ago? All this vault business is too risky and I am not getting into it. I am happy where I am."

I will then say "But what if you were insured against this? What if you would be covered for your losses (if any ever) in return for a small slice of your cake (a few basis points off your APY)?"

You will stop the conversation and probably call me a scammer/ insurance maxi and just some guy from academia who doesn't understand how the real world works.

Formally though…

Attacks are multidimensional. It is very difficult to think through all kinds of attack vectors that can come from both endogenous and exogenous sources. We cannot secure everything and that is understandable. We can however try to power through it. Designing a financial market has its quirks and not every game is zero sum and if you were wondering where the math is and if it even makes sense to continue to read on my rambling through this, let me produce a short formal proof for why it makes sense.

Let there be an insurance agency called I. I covers the full extremities of losses that arise from say a vault V. Let the loss distribution of Vault V be $\mathcal{L}$ where $L_{(1)} < L_{(2)} < \cdots < L_{(n)}$ are n ordered samples from $\mathcal{L}$ and $\max(\mathcal{L}) = L_{(n)}$. I covers the entire loss distribution for premium p which is a fraction of user's APY and formally $p = c \cdot APY$ and $c \in (0, 1)$.

Incentive alignment for users

Let us look at the payoffs for a potential user who wants to deposit their initial assets of value D into Morpho. They have a few choices

- Deposit into uncovered vault. Get full APY and at the same time face losses from $\mathcal{L}$
- Deposit into covered vault. Get a part of APY but never have losses (never?).

Let $q \in [0, 1]$ denote the probability of a loss event, and let L denote the expected realized loss in the bad state. We compare net payoffs relative to simply holding the asset.

Under the payoff matrix

User action	No loss state	Loss state
Uncovered vault	$APY \cdot D$	$APY \cdot D - L$
Covered vault	$(1-c) \cdot APY \cdot D$	$(1-c) \cdot APY \cdot D$

the expected payoff from the uncovered vault is

$$\mathbb{E}[\Pi_U] = (1-q)\, APY \cdot D + q(APY \cdot D - L) = APY \cdot D - qL,$$

whereas the expected payoff from the covered vault is

$$\mathbb{E}[\Pi_C] = (1-c)\, APY \cdot D.$$

Hence the depositor prefers the covered vault if and only if

$$(1 - c) \cdot APY \cdot D \geq APY \cdot D - qL,$$

which is equivalent to

$$c \cdot APY \cdot D \leq qL.$$

Thus, insurance increases adoption whenever the premium paid through sacrificed yield is no greater than the depositor's expected loss avoided. That is the point that will focus on incentive compatibility for user adoption (institutional adoption, retail adoption what have you).

> This way of analysing the payoffs, as rightly pointed out by Ming, misses the nuances of insurance pool aggregation since there is an implicit assumption that both user and insurer payoffs are linearly related to the APY. However this analysis was merely a demonstration of a case rather than a full fledged model which is why I am foregoing rigor for communication.

Insurance in this way becomes a market design tool and not merely just some gimmick. It will enforce economics over engineering as a security tool. While the engineers figure attacks out, this will keep the people coming and staying in the money.

As vault curators begin to bake security into the yield itself, the question changes from 'Is it safe?' to 'Is the premium worth the peace of mind?' What about when the APY is so small that any haircut on top of it breaks the user's incentive to even consider taking insurance? even if it is a few bps? Maybe other incentives help in that case such as a high risk high reward curation strategy on top of premiums?

I know what you're thinking. You'll say "Abhi, your previous blog was about how insurance is bad and keep it out of reach of anyone", and yeah you're right. As I said, insurance is a market design tool and you can use it to design both adversarial and safe markets. Do what you will with it. I guess I am on a mission to figure out where the line is.

I am helping Catalysis Labs build this and community feedback is the moat. Reach out and check out our work on vault insurance and covered lending markets if this interests you.

I have been Abhimanyu Nag