dYdX Safety Staking Module Review

Thomas Cintra
tncintra@gmail.com

Max Holloway *
max@xenophonlabs.com

August 2022

Abstract

A number of successful crypto projects have crumbled at the feet of unpredictable exchange insolvencies, smart contract exploits, and market downturns. dYdX developed an insurance fund, the Safety Staking Module, that acts as a backstop in case the DEX were to face such a shortfall event. As dYdX navigates uncertain financial waters, especially with the planned migration to v4, we ask an important question: "Does the Safety Staking Module provide adequate insurance for the protocol?". In this paper we define insurance power, and argue why the insurance power of the current Safety Staking Module is significantly lower than its Total Value Locked. We dive into some empirical evidence for how popular native tokens fared during exchange insolvencies, and conclude that the current iteration of the Safety Staking Module is unlikely to withstand a significant shortfall event. We then describe a modification to the Safety Staking Module that can significantly increase its insurance power with governance modifications.

*Disclosure: Reference to the `DYDX` price is necessary for this research. The authors do not own `DYDX` token, nor are they affiliated with dYdX Trading Inc. or any of its affiliates. This research was funded by the dYdX Grants Trust. Any opinions and results stated here are those of the authors, not of dYdX, its affiliates, nor the dYdX Grants Trust. This is not financial advice.

1 Introduction

The Safety Staking Module (SSM) is dYdX's token pool designed to backstop the protocol in case of a Shortfall Event (SE). 2.5% of the initial DYDX supply is gradually emitted as rewards for safety staking. The module has two stated objectives:

1. **Insurance:** Bootstrap a decentralized fund to be used in the case of insolvency or other issues with the protocol.
2. **Accountability:** Incentivize DYDX holders to govern correctly. DYDX holders risk dilutive events as the ultimate backstop and act as the governors of risk in the system.[1]

In this paper, we explore how the current implementation of the SSM approaches these objectives. Our research is organized into three parts: (1) we provide some background and data on how safety staking works, highlighting some important concerns for governance, (2) we investigate why the current design of the SSM is likely to fail on objective 1 with reference to relevant case studies, and (3) we describe a proposal to improve the SSM so it can reliably backstop dYdX.

1.1 Research Motivation

DeFi projects are susceptible to black swan events that can wipe out millions of dollars of a project's treasury in days, minutes, or seconds (think "Black Thursday" or LUNA/UST). These so-called shortfall events are always unexpected: they can occur due to smart contract vulnerabilities, missed liquidations, or contagion effects from related projects. The SSM is a crucial last resort for dYdX to be able to handle such insolvency events, but only if its insurance power can hold up in an exchange insolvency scenario. However, we argue here that dYdX's SSM provides a much less robust safety net for dYdX than previously thought.

All protocol liabilities, namely dYdX users' deposits, are denominated in USDC. In order to pay remunerations to dYdX users affected by a shortfall event, the DYDX from the safety staking module would be used to pay USDC debts. This could be at a time when DYDX's value is significantly deflated. Furthermore, dumping this amount of DYDX onto the market to pay for debts would be yet more dilutive. To encapsulate the effective resilience that dYdX's SSM has to a shortfall event, we define the following term.

Insurance Power := The USDC amount that the Safety Staking Module can be auctioned for if a Shortfall Event were to occur.

Notice that the Total Value Locked (TVL) of the SSM is not necessarily equal to its insurance power, due to potential negative price impacts to DYDX at the moment the SSM is auctioned. In

[1] When users stake their DYDX they receive newly minted stkDYDX in return. stkDYDX retains all the original governance rights as DYDX, and it entitles the stkDYDX holder to a pro-rata share of the DYDX in the staking module.

section 3 we argue how two important financial concepts, pro-cyclicality and slippage, lead us to the following conclusion.

The insurance power of a safety pool denominated in a project's native token is significantly smaller than its current TVL.

Notice this is not specific to dYdX, but applies to any insurance fund denominated in a native token such as DYDX, AAVE, SNX, BICO, etc..

Note: Most of the data and plots in this paper were taken from this Dune Analytics dashboard.

2 Background

DYDX token holders can stake their DYDX in the SSM and earn yield on their deposits. This yield is determined *pro rata* based on all stakers in the SSM. In a given epoch, stakers can request to withdraw their staked DYDX such that it is claimable at the beginning of the following epoch. This request must occur before the blackout window, which begins 14 days before the epoch end.

If dYdX suffers from a shortfall event, token-holders must wield their governance power to pass a proposal to slash the funds contained in the SSM. As detailed here, a request to slash SSM funds must go through the dYdX proposal lifecycle.

2.1 Staking Module Size

As of July 2022, roughly 38 MM DYDX is staked in the SSM. As we can see in figure 1, the amount staked in the SSM has steadily increased over time.

2.2 Staker Voting Power

In order for the SSM to act as an insurance fund, a proposal to slash funds must pass in the case of a shortfall event. A legitimate shortfall event can be defined as an event in which SSM funds are the only way for dYdX to prevent insolvency. An important question we must ask is then: who owns stkDYDX and how much voting power do they have?

Voting Power := DYDX + stkDYDX

In table 1 we provide data on DYDX holders taken from this Dune dashboard.

Notice that ***if*** all holders of DYDX and stkDYDX were to vote on a DIP to slash the safety module, stakers alone would not be able to swing the vote in their favor. However, the average DIP has been voted on with a fraction of outstanding voting power. If a DIP to slash the staking module

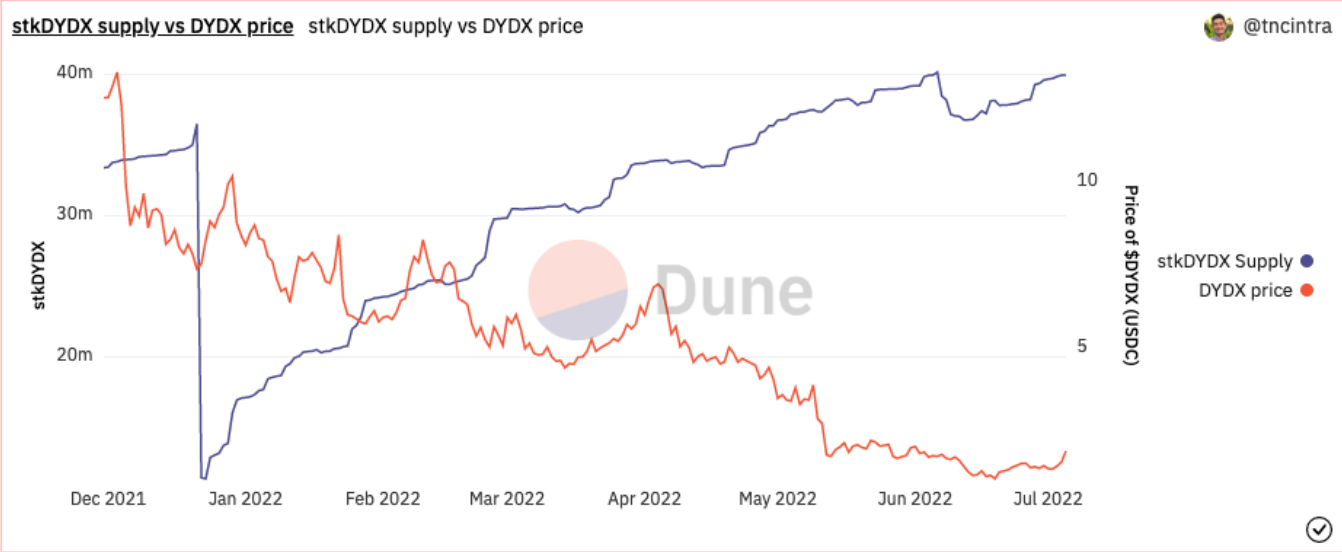

Figure 1: stkDYDX supply and price over time.

Description	**Value**
Total Voting Power	$607,270,937$
Voting Power from stakers holding >100k stkDYDX	$53,467,153$ or 8.8%
Voting Power from All stakers	$68,995,533$ or 11.4%
Average DYDX voted in DIPs	$64,810,126$
Max DYDX voted in DIPS	$141,886,514$

Table 1: Information on DIP voting and voting power, taken on July 6th, 12pm.

does not attract significantly more voter participation than the average DIP has, stakers could swing the vote in their favor. If stakers decided to veto a slashing vote ***en masse***, then this would defeat the purpose of the safety staking module.

2.3 Blackout Window

When traders stake their DYDX, they have until the 14th day of the epoch to request to withdraw their staked DYDX. It is concerning that stakers might try to withdraw their funds before they are slashed. This means that worst-case scenario, governance will only have 14 days to push a DIP to slash the SSM before any or all of the funds in the SSM are withdrawn.

The average DIP has taken roughly 8 days from creation to execution/cancellation. This does *not* take into account the amount of time the proposal spent in forum discussions and snapshot

polling, a process that could take days to weeks. For instance, DIP 3 took 18 days until the voting process was concluded and the DIP was passed.

This is a significant practical concern for governance. Increasing the blackout window could provide a better cushion in case the proposal cycle takes longer than expected, although longer lockup periods could also lead to less engagement in the SSM.

2.4 Preliminary Takeaways

Some key takeaways:

1. Stakers hold enough voting power to swing the average DIP, but there is more than enough DYDX in circulation to prevent them from doing so;
2. The average DIP takes 8 days to conclude a vote, with several days devoted to community discussion before the DIP is created. Since the blackout window is 14 days, governance risks a potentially significant amount of staked DYDX being withdrawn before the slashing DIP is passed.

3 The Insurance Power of the Safety Staking Module

We now reinforce our claim that the insurance power of the SSM is much smaller than its current TVL. To do so, we call on historical examples of DeFi projects whose native-token treasuries suffered in the face of shortfall events.

3.1 Case Studies - Token Prices and Shortfall Events

Let's explore a handful of case studies for how native token prices and auctions faired after shortfall events. These examples are meant to corroborate our claim that Insurance Power is likely to be significantly smaller than the TVL in the SSM, due both to the effects of pro-cyclicality and slippage.

3.1.1 MakerDAO

On March of 2020 MakerDAO suffered a significant shortfall event due to Ethereum mainnet congestion, high gas prices, and missed liquidations. Failure to liquidate under-collateralized positions on time led to roughly 6 MM dollars in losses to the DAO. In order to cover this deficit, MakerDAO had to cover the bulk of their losses by auctioning MKR tokens on the market (they only held roughly 500k in DAI). They ultimately sold $20,600$ MKR at an average price of roughly

$275. For context, MKR had been steadily trading at around $500 for months prior to the shortfall event. Roughly $4 million could have been saved if the DAO held more stable currencies in their treasury: perhaps by selling MKR for DAI instead of burning it and then having to mint/auction more[2].

Figure 2: MKR prices from mid-2019 to mid-2020, taken from CoinMarketCap. The red arrow indicates when the MKR auction was conducted and MKR prices briefly plummeted by over 50%.

MakerDAO had to sell MKR at approximately a 50% discount, perhaps primarily due to slippage, and partly due to the effects of pro-cyclicality.

This example was also notably used in Hasu and monetsupply's detailed article on the dangers of holding a treasury composed primarily of a project's native token. Their article highlights that token prices and token liquidity deflate after significant shortfall events, and selling large sums of the token incurs heavy slippage [3]. We quote a segment of their article that helps illustrate the vulnerability of the SSM with respect to pro-cyclicality:

" [...] Times when Defi projects urgently need liquidity can correlate with project-specific risk: for example, when a project experiences a large insolvency event due to a bug or hack and wants to make users whole, the token price tends to be depressed as well – especially if holders expect a dilution event."

[2] Black Thursday Article
[3] A New Mental Model for Defi Treasuries by Hasu and monetsupply

3.1.2 Axie Infinity

Axie Infinity, the popular NFT-based game on the Harmony blockchain, suffered a sizeable attack earlier this year. Axie Infinity lost roughly $\$600$ million due to an exploit of their Ronin Bridge (which connected Ethereum mainnet to Sky Mavis' Ronin chain). The hackers anticipated the negative impact of a hack on investor sentiment and asset-prices; the address that reportedly hacked Axie's Ronin Bridge also shorted their Axie Infinity native currency, AXS. When the Ronin network announced the exploit, AXS token tumbled to historic lows. Within a week AXS had dropped roughly 30%, and the token never recuperated [4].

Figure 3: AXS prices from February to June of this year, taken from CoinMarketCap. The left-most red arrow indicates when the hack took place, the right-most arrow indicates when the hack was uncovered and announced. AXS prices gradually crashed over the ensuing days/weeks, although Sky Mavis never conducted a large auction of AXS so no slippage is clearly observed.

Sky Mavis did not attempt to auction AXS to cover the losses suffered by its users, so we do not observe the slippage effects we saw with MakerDAO in the previous section.

[4] Axie Infinity Hack

3.1.3 Venus Protocol

Venus is a lending protocol on the Binance Smart Chain. In May 18th of 2021, a flaw in Venus' liquidation module was exploited, leading to over $70 million in losses to the protocol [5]. The attack was allegedly a result of oracle price manipulation of their governance token XVS. The token had been trading at over $100 throughout late April and early May. Within days of the exploit was uncovered, XVS plummeted below $40, an over 60% crash from the high of that month

Figure 4: XVS prices from April to June of 2021, taken from CoinMarketCap. The red arrow indicates when the oracle price manipulation took place. XVS token quickly crashed well below its pre-exploit price and never recovered.

In their post-mortem, the Venus team acknowledged that the exploit had led to further "FUD" (fear, uncertainty, distrust) in the protocol that contributed to the price depreciation of XVS token.

3.2 Reducing DYDX Exposure

These case studies corroborate the idea that a shortfall event will likely depreciate the value of DYDX token and its sale/auction could incur significant slippage. The objective of this paper is then to modify the SSM to close the gap between insurance power and TVL. Ideally we would like

[5] Venus Protocol Hack

$InsurancePower = TVL$. The most intuitive way to achieve this would be using a stablecoin-denominated safety pool.

3.3 A USDC Pool

Suppose we replace the current SSM with a USDC-denominated staking pool: users can stake USDC and earn DYDX rewards for doing so. Staking USDC instead of DYDX means that if a SE is triggered and funds are slashed, the exchange can use the staked USDC directly to pay off their deficit. In this case, insurance power is equal to the TVL. Furthermore, this would open up the possibility for anyone to stake into the pool and earn yield, not just DYDX holders. Notice the APR for staking in the SSM from DYDX rewards is currently at 13% whereas common USDC staking pools expect significantly lower returns [6]. Although staking in a safety module incurs additional risk (from slashing) compared to regular USDC staking, we could reasonably expect an increase in TVL in the SSM by attracting a new demographic of stakers.

Let's now consider the concerns regarding a USDC-denominated pool.

3.3.1 USDC Pool Drawback 1: Decreased DYDX Token Utility

Eliminating the DYDX yield opportunity decreases the utility that users can derive from owning the DYDX token. The precise effect that this change would have on demand for the token is unknown, and we do not speculate on it here. However, we can say with confidence that users who only hold the token in order to derive yield from it will no longer have an incentive to hold the token.

The relevance of this drawback depends on two factors: (1) whether token demand is important, and (2) the magnitude that token demand will change if staking rewards are removed. The first factor is dependent on community preferences, and we do not comment on it here. On the other hand, we are able to argue that the second factor is unimportant: under specific economic assumptions, the removal of yield from DYDX staking should not meaningfully change token demand.

Suppose, to the contrary, that there are many stakers who stake due to the DYDX yield that they receive, and that removing that yield would cause them to un-stake. If we assume they are rational and display risk-aversion in the form of Markowitz-like portfolio management, then the only reason they would buy DYDX to stake, while not being willing to buy DYDX to hold when not staking, is because the staking yield increases their expected returns enough to justify their expected portfolio volatility, while the expected returns of DYDX token alone is not enough to

[6] DefiRate USDC

justify its expected portfolio volatility [7] [8]. However, if we look at the historic volatility of the DYDX token, (or any volatile crypto-asset for that matter,) the investor's expectation of returns on the asset must be sizeable in order to justify the token's price volatility. If investors require high expected returns, in the order of hundreds of percentage points, then offering yield on the token that increases expected returns by 10% will likely not be relevant in the investor's decision to invest. That is, in the Markowitz portfolio optimization that the investor conducts, whereby traders minimize volatility for a given threshold of returns, there is some threshold of expected returns that must be met to justify the asset's downside risk; for volatile crypto assets, this threshold expected return must be very high, in the order of hundreds of percentage points, in order to justify investing in crypto rather than leveraging up on other lower-volatility investments; therefore, if an investor is willing to buy DYDX token and stake it, it is likely due to an expectation of multi-hundred percentage returns on DYDX, not on staking yields.

It is important to reiterate that this argument relies heavily on the assumption that investors use a Markowitz-like portfolio optimization. We believe this is a fair assumption, since Markowitz's work on Modern Portfolio Theory dominates to this day.

Furthermore, this analysis does not take into account alternative ways of receiving staking yield without assuming exposure to the underlying DYDX volatility. This can be achieved by staking borrowed DYDX, or by simultaneously shorting DYDX perps while providing DYDX spot assets to the safety staking module. Under these scenarios, it is possible for spot prices to increase (due to higher demand for spot assets) while DYDX interest rates increase and DYDX perp funding rates get more negative. There is some evidence that this behavior may occur in reality, and by eliminating DYDX staking yields, those who buy DYDX spot and short it elsewhere would stop performing that trade.

While eliminating DYDX staking yields would lower the demand for DYDX spot token, it would by an equal amount increase long-demand for DYDX derivatives. Currently, the staking module "crowds out" those who would buy and hold the spot asset without staking module, since they can effectively "buy" DYDX perps at a discount.

We are doubtful that DYDX's safety staking module meaningfully increases token utility.

3.3.2 USDC Pool Drawback 2: Decreased Governance Accountability

A USDC pool would be primarily an insurance service that they dYdX treasury pays for, similar to auditing services or the dYdX grants program. Paying for an insurance service is a legitimate method for insuring the protocol, but it removes the guarantee that stakers (insurers) are DYDX token-holders with some voting power in the protocol. Holders of stkDYDX have a dual incentive

[7] Markowitz Model
[8] Modern Portfolio Theory

to govern the protocol correctly: they are exposed to DYDX, and in the case of a shortfall event, they can lose their stake. Therefore, stkDYDX holders have an incentive to prioritize security as a governance tenant. The idea behind this drawback is the following: if there is no longer a significant stkDYDX voting power component, then governance may have a weakened incentive to treat security as a top governance priority, and if the protocol experiences a shortfall event, then users can exteralize the cost to the insurers in the USDC safety-staking pool, rather than the protocol bearing responsibility.

In practice, this drawback is likely unwarranted, due to implicit incentives for DYDX token governance to prioritize security. Deprioritizing security can lead to ruin of the dYdX protocol, which would clearly lead to the ruin of the dYdX token governance. For this drawback to be warranted, one would need to hold the belief that the dYdX safety staking module is an important component for dYdX's governance decision making on security topics, which we believe is false.

Furthermore, we can cross-reference how many stkDYDX holders have casted a vote on a DIP, and we find that fewer than 10% of stakers have participated in on-chain governance (figure 5). Furthermore, there have been no on-chain DIPs relating to shortfall events since the creation of the safety staking module (aside from the vote regarding issues with the safety staking module itself). The staking module has clearly not contributed much in the way of encouraging DYDX holders to foster better security against shortfall events, and thus we find that this is potential concern on a USDC pool is illegitimate.

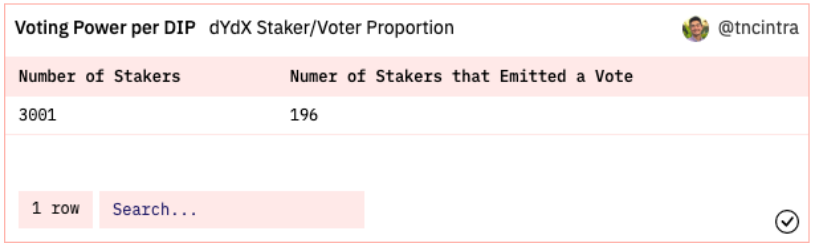

Figure 5: Dune query for how many stakers have voted on any DIP.

3.3.3 Takeaways

We maintain that the SSM is an insurance service, and modifying the SSM to only contain USDC provides the best insurance power against a shortfall event. Furthermore, we believe removing the staking incentive will likely have little effect on demand for the DYDX token, however we concede that our reasoning relies on risk-aversion and Markowitz-like portfolio optimization assumptions which cannot be easily verified. This demonstrates a potential trade-off between insurance power and DYDX spot token utility. In the next section, we discuss a way to tune this tradeoff by composing the staking pool of a combination of USDC and DYDX.

3.4 Balancer Liquidity Pools

Enter Balancer Liquidity Pools. Balancer is an AMM platform that enables the creation of self-balancing weighted portfolios with automated price discovery [9]. Balancer pools define a value function that determines the price of swapping any two assets within the pool. These value functions, coupled with a swap fee, encourage arbitrageurs to quickly and consistently re-balance the pool such that each asset represents a constant share of value in the pool. Here, we analyze how Aave utilizes Balancer pools in their safety module implementation, and we show how dYdX could implement a similar safety module tuned to its specific needs.

3.4.1 Aave's Safety Module

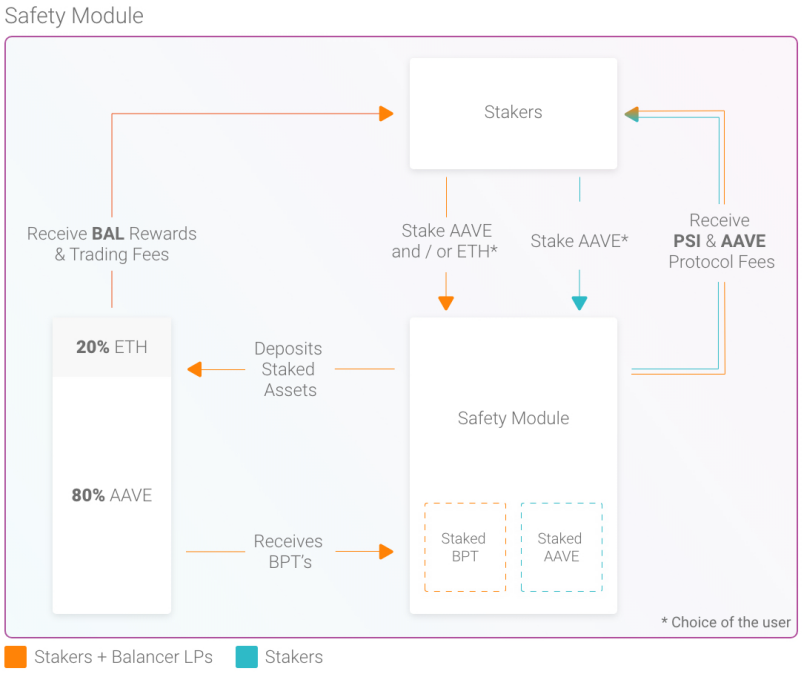

Figure 6: Infographic of Aave's Safety Module using an AAVE/ETH 80/20 Balancer pool. Notice that Aave has both a regular SM (exactly the same as dYdX's) as well as a Balancer pool.

For an illustration for how Balancer weighted pools can serve as safety staking modules, refer to figure 6, taken from Aave's safety module. Aave manages two safety modules, one exactly the same as dYdX's and the other hosted on a Balancer pool. Their Balancer safety staking module works as follows: a user provides some combination of AAVE and ETH into an 80/20 AAVE/WETH Balancer pool and an AAVE Balancer Pool Token (ABPT) is minted to their address. They can then

[9] For a more detailed guide to what Balancer is and how it works, please refer to their whitepaper

stake their ABPT in Aave's staking pool and receive a stkABPT token in return, for which they are rewarded both with AAVE and BAL tokens.

This introduces an intermediate step in the staking process. Instead of staking directly into a DYDX pool, users would stake some combination of DYDX and another token in a Balancer pool, receive a DBPT token in return that they can then stake in dYdX's Safety Staking Module, and earn rewards on it. If a shortfall event occurs, DBPT tokens staked in the Safety Staking Module would be slashed by governance.

Aave allows users to stake a combination of AAVE and ETH into a Balancer weighted pool where 80% of the pool consists of AAVE and 20% of the pool consists of ETH. This uneven weighting maintains a high exposure to AAVE such that stakers can still primarily stake and earn on their AAVE deposits. According to Aave's docs, the primary benefit of using a Balancer weighted pool instead of simply staking AAVE is as follows:

"The Safety Module solves the issues with traditional staking systems and market liquidity: tokens with locking/reward schemes tend to suffer from low market liquidity and extreme volatility when high percentages of the total supply are being locked. With the ability of contributing to the safety module not only by locking AAVE, but also by contributing with liquidity into an AMM, stakers create a trustless and decentralized market with deep liquidity for trading AAVE against ETH." [10]

Hence, a Balancer pool both backstops the protocol and improves liquidity on AAVE despite having it be theoretically "locked up". Furthermore, unlike a USDC pool it maintains the utility of the native token, allowing token-holders to passively earn yield on their token keeping them liable for shortfall events in the protocol. ETH seems to have been chosen as the secondary token in this pool because a large portion of Aave's liabilities are denominated in ETH, and ETH is a highly liquid token that is common in DeFi token pairs.

3.4.2 A dYdX Safety Module of Balancer Pool Tokens

Let us now consider a dYdX-specific implementation of Aave's safety module. In this implementation, the dYdX safety staking module would only accept deposits of a 20/80 DYDX/USDC Balancer pool token.

3.4.3 Balancer Pool Benefit 1: DYDX Token Liquidity

According to Etherscan, the majority of DYDX token liquidity is held on Uniswap v2, Uniswap v3, and Sushiswap. If we aggregate on-chain data for Uniswap v2, Uniswap v3, and Sushiswap, DYDX token has about $\$1.2$M in liquidity as of July 14th 2022. Furthermore, Uniswap estimates

[10] Aave Docs

that swapping 10000 DYDX for ETH incurs a price impact (slippage) of almost 10% [11]. Note that liquidity for DYDX token on Uniswap used to be orders of magnitude higher and has rapidly decreased since the airdrop in September of last year.

Although AAVE has considerably higher liquidity/TVL than DYDX, fluctuating around $\$10$ M across Uniswap v2, v3, and Sushiswap, its liquidity on the Balancer AAVE/WETH pool is considerably higher at over $\$89$ M (taken on July 14th). It seems clear that the Balancer pool has provided significant on-chain liquidity for traders to swap AAVE and ETH, despite AAVE/ETH pools already existing on other AMMs. The reason, as described in the docs, is that Balancer provides liquidity using the staked tokens, which would otherwise be locked up in a staking pool.

Developing a DYDX pool on Balancer could provide a drastic improvement to DYDX on-chain liquidity. Improving liquidity makes it easier for DYDX to be used as collateral on decentralized lending protocols by improving on-chain price oracles.

3.4.4 Balancer Pool Benefit 2: Insurance Power

Although incorporating a non-Aave coin is a step toward improving shortfall-event coverage, the improvements to insurance power by denominating 20% of the pool's TVL as ETH is still insufficient. Notice that a high exposure to AAVE means that large price movements against AAVE reflect incredibly large movements against the TVL of the pool. Let p_A be the price of the native token (DYDX) and w_A be the its weight, then the change in TVL before and after a price-shock is:

$$\Delta TVL = \Delta p_A^{w_A} \tag{1}$$

We plot this equation in figure 7, assuming the other token in the pool stays constant in value.

AAVE Weight	95%	50%	25%
20%	54%	85%	95%
50%	22%	70%	90%
80%	9%	57%	83%

Table 2: Summary of insurance power at different AAVE weights and price shocks. For example, if AAVE represents 20% of the Balancer pool and drops in price by 95% then the Balancer pool will retain 54% of its TVL whereas if it represents 80% of the pool then the pool will only retain 9% of its TVL.

If AAVE were to crash by 95% after a Shortfall Event, then the Balancer pool will lose 91% of its value. We argue that this high exposure to AAVE means their Balancer pool barely improves the

[11] DYDX/ETH Swap

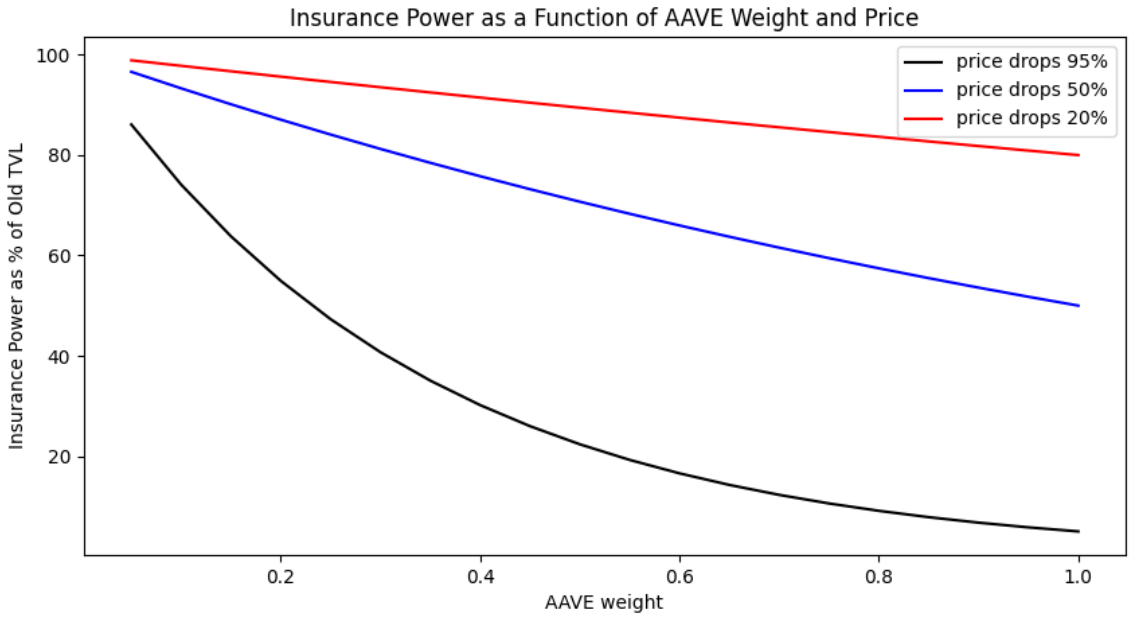

Figure 7: Insurance Power of the Balancer pool as a function of AAVE weight and price. For example, if AAVE is auctioned at 95% of its pre-shortfall-event price, and AAVE weight it 80%, then the insurance power of the Balancer pool is only 9% of its pre-shortfall-event TVL, whereas a weight of 20% retains 54% of the TVL as insurance power.

insurance power of their SM, and this begets a reduction of AAVE's weight in the Balancer pool. In table 2, we tabulate how different native token weights affect the final TVL of the pool after some negative price movement. By allocating a weight of only 20% to the native token, even a 95% crash to the token still retains more than 50% of the TVL in the pool.

Furthermore, we know that ETH is not a particularly stable asset relative to a stablecoin like USDC, and the price of an ERC-20 token like DYDX or AAVE might be correlated with the price of ETH. Consider that Aave is a lending protocol with most of its activity on the Ethereum blockchain, so problems with Ethereum network may drive problems with Aave. Furthermore, Aave is one of the biggest and more pronounced protocols on Ethereum, so Shortfall Events that are detrimental to Aave might also be detrimental to Ethereum and therefore ETH. While creating a market for swapping ETH and AAVE is beneficial for a protocol that has many ETH liabilities, this is not the case for dYdX.

We conclude that the secondary token for dYdX's Safety Staking Module should be a stable currency such as USDC (not ETH), drastically improving the insurance power of the module and

hedging the module against volatile price movements.

3.4.5 Balancer Pool Drawback 1: Added Dependency

Although Balancer is by now a well-vetted protocol that has hosted billions of dollars of liquidity, it still creates an added dependency to the dYdX governance stack. This makes dYdX governance increasingly complex and increases composability risk in dYdX governance.

3.4.6 Balancer Pool Drawback 2: Voting Power Calculation

Currently, the dYdX safety staking module allows stakers to use their stkDYDX amount for governance voting. Voting power is calculated by finding the user's amount of stkDYDX at the time of the voting snapshot, and this calculation exploits the fact that the underling DYDX balance of a stkDYDX position only updates when a user interacts with the staking contract via a deposit or withdraw.

On the other hand, if we wanted to grant voting power to stakers in a balancer pool token staking pool, we would need to modify the voting power calculations to find the DYDX balance underlying DYDX/USDC balancer pool token staked by the user. This calculation requires access to the balancer pool balances at a specific block, which would likely need to be implemented with an ERC20 Snapshot-like logic. If these values are snapshotted at each staking pool interaction, then they can be used to approximate the underlying amount of DYDX underlying a position at a given time.

While this approximation of DYDX balances is possible, its accuracy degrades if the staking pool is not updated frequently. Furthermore, bugs in the voting power calculations could be extremely high-impact; if there were a vulnerability allowing attackers to claim they have heightened voting power, then all of the governance-guarded funds could be put at risk.

We can avoid smart contract issues by allotting no voting power to a balancer safety staking module. However, this has the obvious drawback that users must choose between staking their DYDX or using it to vote.

3.4.7 Takeaways

Balancer pools are a compromise between the various features of the Safety Staking Module. This has two main benefits over the existing module: it greatly increases the insurance power of the safety staking module, and it increases the liquidity of the DYDX token. However, it requires dYdX governance to depend on Balancer, which introduces potential additional smart contract risk. Furthermore, if we want to retain governance voting power with this solution, it will re-

quire modifications to the security-critical voting power calculation, and even then there is no currently known way to make a precise voting power calculation.

4 Proposal: A USDC Safety Staking Module

Here we describe what we believe will provide the best financial security for the protocol and its community. Establishing good insurance and risk-management practices is **essential to keeping the protocol healthy and keeping users safe from potential insolvencies**. We propose the following.

1. Fork and modify the SSM smart contract, changing the deposit token address to be USDC (`0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48`) rather than DYDX. This can be done by passing USDC address as an address to the safety staking module's constructor.
2. Deprecate the current SSM by diverting *all* DYDX staking rewards to the new USDC-denominated safety staking module. Although stakers in the old SSM will no longer have an incentive to keep their DYDX there, no action will be required to remove their DYDX from it.

4.1 Changes to Other Modules

The safety staking module currently has downstream dependencies in other locations: it allows traders to lower their fee tier; it increases trader and LP rewards scores; it is used to calculate voting power; and it boosts affiliate program rewards. We propose that, upon the migration of emissions from the original SSM to the new SSM, we remove the staking module from LP rewards, and trading rewards. It is the decision of dYdX Trading Inc. regarding their use of staking module in the fee tier calculation and the affiliate program rewards formula.

Importantly, we do not plan to make any modifications to the smart contract that calculates voting power. The voting power calculation currently points to the DYDX-denominated SSM, and we do not plan to update the voting power calculation to point to the new SSM. It will still be possible for depositors in the old SSM to use their deposit's voting power, however we do not expect many stakers to keep their DYDX in the module, since the DYDX in the old SSM module will no longer be earning yield.

4.2 Discussion

We anticipate push-back from the community by halting emissions to the DYDX-only safety staking module. We believe this change makes the most sense for insurance against downfall events.

However, if this is unpalatable to community members, there is potential for a compromise: letting both the new and old SSM coexist, and splitting a portion of rewards between each of the modules.

4.3 Risks

Although we aimed to minimize smart contract modifications in this proposal, there is still risk with the changes posed. Our proposed changes do not modify any smart contracts other than the DYDX token allocator (which has been done before with minimal, safe code changes), and they do not require more than a single code line change in order to create the new safety staking module. Of course, we still encourage readers to do their own research, and we do not guarantee the security of the implementation.

5 Conclusion

DeFi projects have historically disregarded risk-capital management, and dYdX should not repeat risk management sins of the past. In this paper, we review why the current Safety Staking Module does not provide adequate risk capital for dYdX, and therefore is not a robust insurance mechanism for the protocol. We examine why denominating the Safety Staking Module entirely in DYDX provides insufficient insurance.

We propose simple, yet impactful modifications to the safety staking module which will drastically improve the insurance power of the module by utilizing USDC as the staking asset.

5.1 Next Steps

Pending approval from the dYdX community, Xenophon Labs will create a safety staking module, and then will follow the steps outlined in the Proposal Lifecycle to redirect emissions from the old safety staking module to the new one.

6 Appendix

6.1 Calculating Balancer LP TVL wrt. Changing DYDX Price

Here we perform some basic algebra to model how changing the token price of one asset in a Balancer LP affects the TVL of the entire pool [12]. Since dYdX's Balancer pool is some combination of DYDX and USDC, let's simplify the problem to a 2-asset pool where one asset is stable. A Balancer pool is built upon a surface defined by a value function V:

$$V = \prod_t B_t^{w_t}$$

Where B_t defines the balance of token t in the pool, and w_t defines its weight. Suppose we are considering this value function before and after some change to the price of the non-stable asset. Let these times be time i for initial and f for final. Using just two assets, A and B, we can rewrite this value function at time i:

$$V_i = A_i^{w_A} \times B_i^{w_B}$$

Where A_i defines the balance of asset A at time the initial (pre-change) time i. Suppose there are negligible fees for trading in this pool so arbitraguers will always correct the share of value of each asset in the pool (this is functionally the case for most Balancer pools). This implies that the value function is constant over time, so:

$$V_i = V_f$$

$$A_i^{w_A} \times B_i^{w_B} = A_f^{w_A} \times B_f^{w_B} \tag{2}$$

Notice that the weights w_A and w_B can be expressed as the share of value each asset has in the pool, determined by the balance and price of the assets:

$$w_A = \frac{A_i p_A}{A_i p_A + B_i p_B}$$

[12] We derive some of the math behind this medium article, written by the founder and CEO of Balancer, Fernando Martinelli

Where p_A and p_B denote the prices of the assets at time i. Let asset A be our non-stable asset and let its price p_A incur a delta of δ (ie. the price of A at time f is δp_A). Then for the share of value of each asset to remain constant it must be that:

$$\frac{A_i p_A}{A_i p_A + B_i p_B} = \frac{\delta A_f p_A}{\delta A_f p_A + B_f p_B}$$

Where each side of this equation represents the share of value of asset A at times i and f respectively. Multiplying out the denominators and rearranging we obtain the following ratio:

$$\frac{\delta A_f}{A_i} = \frac{B_f}{B_i} \tag{3}$$

From equation 2 we know:

$$\frac{A_i^{w_A}}{A_f^{w_A}} = \frac{B_f^{w_B}}{B_i^{w_B}} \tag{4}$$

We can rewrite these as:

$$\frac{A_f}{A_i} = (\frac{B_f}{B_i})^{-\frac{w_B}{w_A}} \tag{5}$$

$$\frac{B_f}{B_i} = (\frac{A_i}{A_f})^{\frac{w_A}{w_B}} \tag{6}$$

We plug equation 5 into equation 3 and obtain:

$$A_f = \delta^{-w_B} A_i \tag{7}$$

This gives us the final balance of asset A in terms of its price change, weights, and initial balance. We perform a similar substitution and find the final balance for asset B:

$$B_f = \delta^{w_A} B_i \tag{8}$$

This basically tells us that if price moves against A then $\delta < 1$ so $\delta^{-w_B} > 1$, meaning its balance increases to make up for the value deficit. This is exactly how Balancer pools rebalance, and we could extrapolate this for a mix of more than two non-stable assets. Ultimately:

$$TVL_i = A_i p_A + B_i p_B$$

$$TVL_f = \delta A_f p_A + B_i p_B$$

Substituting in equations 7 and 8 we get:

$$TVL_f = \delta^{w_A} TVL_i \tag{9}$$

Or equivalently:

$$\Delta TVL = \Delta p_A^{w_A} \tag{10}$$

Hence, **The percentage change in TVL for a Balancer LP using one stable and one non-stable token is equal to the percentage change in the price of the non-stable token to the power of its weight.**

7 Works Cited

All the relevant links we reference in this paper.

1. Introduction on treasury management by Hasu and Monetsupply
2. Delphi Digital's proposal to overhaul Aave's Safety Module
3. Aave Safety Module
4. Balancer white paper
5. Dune Dashboard
6. Calculating TVL in Balancer LP from token prices
7. Safety module address
8. TVL volatility in Balancer by increasing fees
9. Alpha-Homora exploit and settlement.