CRYPTO LEADERS SINCE 2014

New Frontiers™

SPREADING THE RISK: DECENTRALIZED INSURANCE

Kent Barton

Head of Research and Development, ShapeShift

ShapeShift

This report is for educational purposes only and nothing in it should be construed as investment, legal, or tax advice. Purchasing digital assets, such as those discussed in this report, is risky, and we highly encourage you to understand the underlying technology of digital assets and cryptocurrencies specifically and contact an investment, tax, or legal professional prior to deciding to invest in such assets.

Forward

The amount of money locked in decentralized finance (DeFi) platforms has increased at a staggering rate since last summer. This type of hockey-stick growth suggests that an enduring inflection point has been reached. Now that a product/market fit appears to be established, users and their digital wealth are rushing into the ecosystem. It's exciting!

But for all of the awesomeness of DeFi, it's not for the faint of heart. These platforms are only as secure as the code that powers them. Say what you will about traditional bank accounts, but they're built on stable systems that have been around for decades—and if something does go wrong, banks can often reverse the transaction and make the user whole.

In the immutable world of crypto, there are no reversals. There's plenty of risk to go around too; while innovation happens at a breakneck pace, it doesn't always leave much time for thorough testing. And things get even crazier when you consider the compounding risk that stems from DeFi's fabulous "money lego" composability.

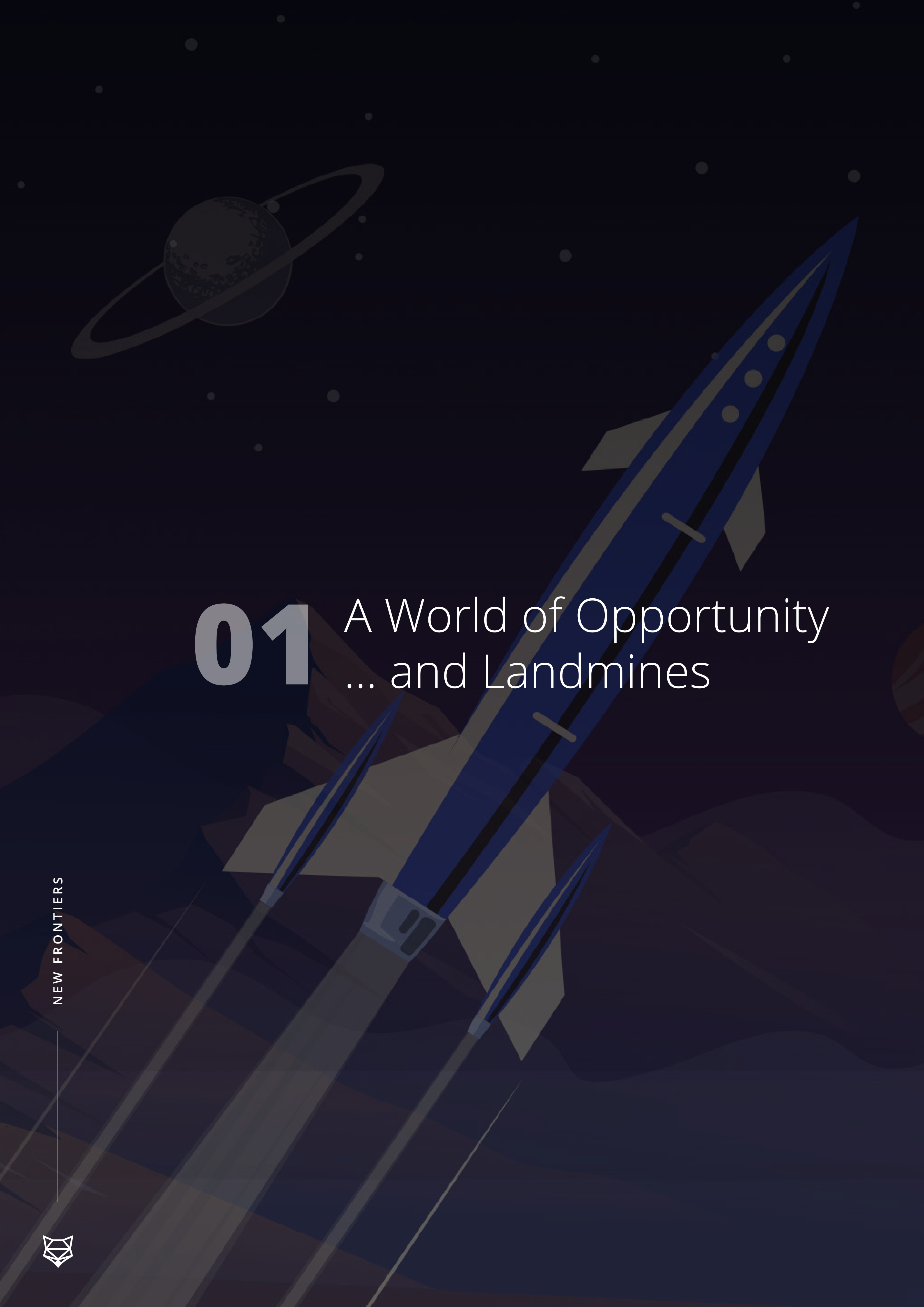
Fortunately, decentralized insurance platforms are beginning to offer crypto users a way to limit their downside exposure. In this report we'll take a look at the broad categories of risk and focus on two DApps that are providing this service: Nexus Mutual and Cover Protocol. We'll conclude with some thoughts on how this niche is likely to evolve over the next year.

Kent Barton

Head of Research and Development, ShapeShift

Table of Contents

01 A World of Opportunity ... and Landmines



NEW FRONTIERS

A World of Opportunity ... and Landmines

When you think about it, insurance is one of those "boring" financial primitives that we take for granted in everyday life. It's just . . . there. It's been around for several centuries. It's not new or sexy, but it helps us sleep better. And if something does go wrong, it helps ensure that an event that could produce massive financial losses is instead relegated to the "mere inconvenience" category.

When it comes to DeFi, it's also a necessary precondition for widespread institutional participation. Your average degen on "crypto Twitter" is more than willing to throw caution to the wind and ape into some new food protocol. This is hardly the case for large funds and endowments that seek a more manageable risk/reward proposition. Even for "less risky" DeFi platforms, there are plenty of potential pitfalls that may be a bridge too far for institutional money.

Thanks to crypto-based insurance, that barrier to entry is starting to fall—at least for some types of risk.

Categorizing the Landmines

Custodial Risk

From Mt. Gox to Bitfinex to Kucoin and many more, crypto history is replete with examples of centralized exchanges losing or absconding with users' funds.

While crypto is an unpredictable space, one thing is for very sure: it'll happen again.

Some exchanges aim to manage the risk of hacks through "insurance" pools such as Binance's SAFU fund. Others, like Coinbase, use external insurers to provide some degree of protection. Having "backup" funds in case something goes wrong is a workable approach for exchanges. But for users, a lot is left up in the air. Is there sufficient insurance to cover a hack of all the exchange's funds? If it's only partial, will the user need to deal with socialized losses? There's a lot of ambiguity inherent in this approach.

Not your keys, not your coins—even if the exchange claims to have full insurance. But as we'll see shortly, users who do decide to keep their tokens on certain centralized exchanges now have the option of insuring their holdings in a decentralized fashion.

Smart Contract Risk

It's an unwritten rule that any discussion of smart contract risk must begin with a mention of "the DAO incident" in 2016. Even in those early days, investors were eager to put their money in a promising new project. One re-entrancy bug later, 3.6 million ETH was drained from the contract and the Ethereum community was headed for a divisive hard fork.

Since then there have been a great many additional instances of smart contract bugs or exploits leading to lost funds—and with the proliferation of new DeFi DApps, there's no shortage of potential problems.

The good news is that smart contract risks are a very good fit for decentralized insurance. Since everything happens in a transparent fashion, it's not difficult for insurers or claims assessors to determine what happened. And if a payout does need to be made, it can happen quickly and in a semi-automated fashion.

Protocol Risk

What if an entire blockchain had a show-stopping fault? That's the type of issue we're dealing with in this category; something that impacts not just one DApp, but the entire ecosystem.

The higher-level nature of this risk arguably makes it harder to insure against, since claims could quickly spiral out of control. However, it's less likely that a well-established blockchain like Ethereum will have a protocol-level bug, relative to a smart contract running on it. Other than Nexus' coverage of the ETH 2.0 Beacon Chain contract on ETH 1.0, we're not seeing anything resembling protocol-level insurance just yet—but that could quickly change as the space evolves.

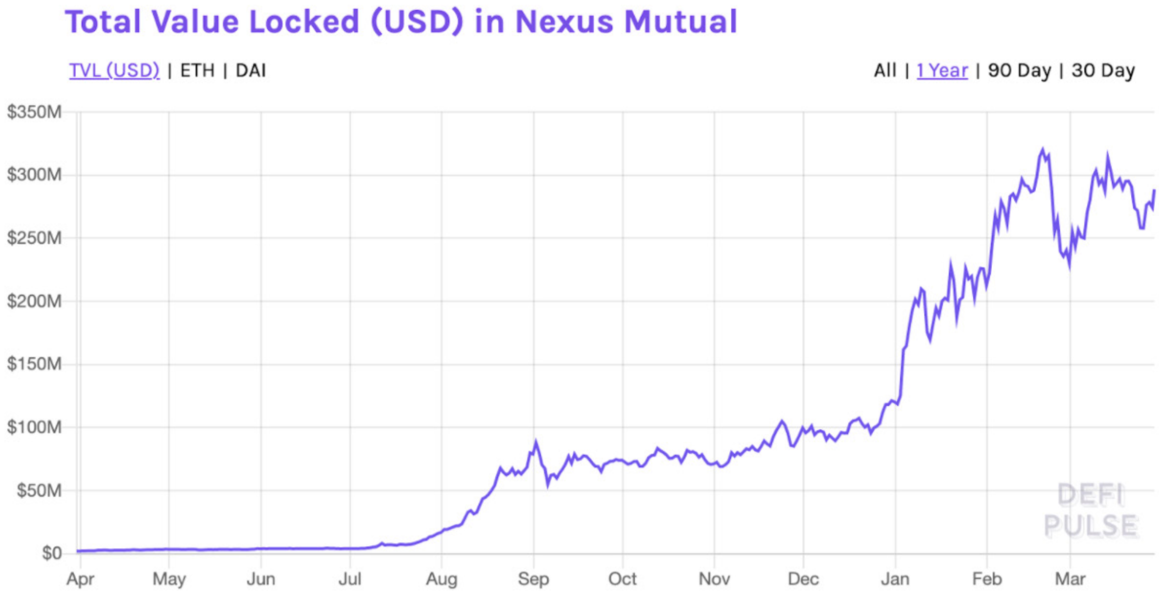
Oracle Risk

Many DApps require an oracle to feed them information from an external source or from the off-chain world. Over DeFi Summer we saw multiple cases where flash loans were used to artificially manipulate those price feeds, leading to sizable losses. This is a type of risk that's more difficult to quantify, predict, and assess for claims. As such, it's less likely to be covered by decentralized insurers.

02 Nexus Mutual

Nexus Mutual

Nexus Mutual is the largest player in the decentralized insurance space. How might one quantify "largest?" Consider the total value locked (TVL), as reported by defipulse. It's grown from under $10 million last summer to more than $200 million as of this writing.



Source: Defipulse.com, Nexus Mutual, https://defipulse.com/nexus-mutual.

Clearly they're doing something right . . . but the success didn't happen overnight.

The Nexus Vision

Nexus Mutual is the creation of Hugh Karp, a crypto enthusiast who had prior extensive experience in the traditional insurance industry. Combining both areas of expertise, he rolled out Nexus at the EthCC hackathon in 2018. The premise for Nexus was simple, yet powerful: create a pool of funds that can be used to pay claims on smart contract bugs and exploits.

There's an important distinction here: as you can glean from its name, Nexus is a "mutual" entity whereby members are the ones who stand to profit from underwriting claims and taking out policies. In a traditional insurance company, policyholders don't directly profit from these arrangements; profits instead accrue to shares of the company.

The mutual sharing of risk and profit undergirds the fundamental economics of Nexus. Interestingly, these fundamentals are codified both at the legal level—the organization is incorporated as a "discretionary mutual," thereby eliminating any obligations for members to directly pay claims—and of course at the on-chain level. The latter is facilitated by Nexus's smart contract code and its own token, NXM.

How It Works

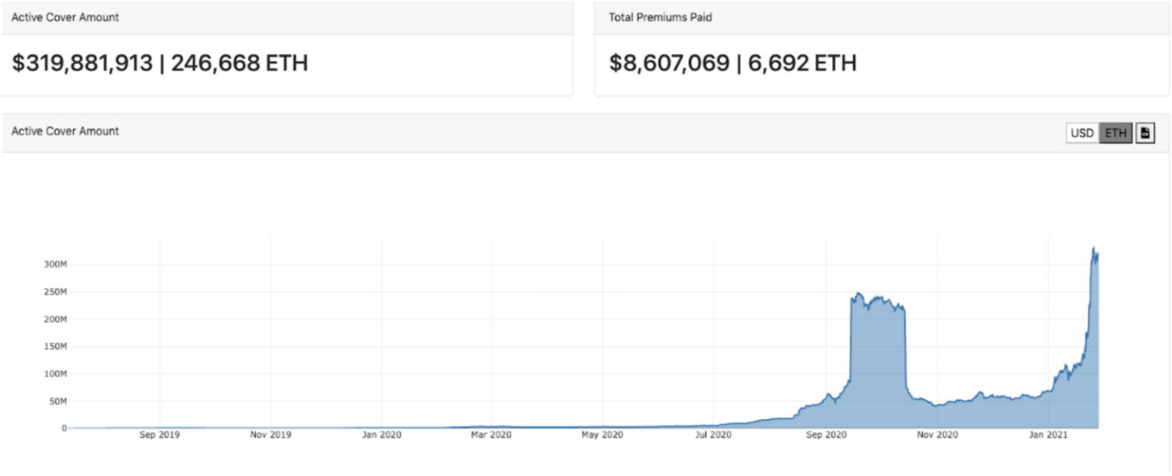
There are three types of players in the Nexus world: risk assessors, claim assessors, and policyholders. The common economic thread binding these actors is NXM.

Like most DeFi tokens, NXM provides holders with a say in the platform's decentralized governance. However, things get much more interesting thanks to its additional attributes; NXM can also be used to purchase coverage, assess risk, and assess claims. The token provides an elegant way to incentivize the latter two functions.

The going rate for NXM is derived from a bonding curve that aligns price with the total funds locked in the DApp. Crucially, this model also includes a Minimum Capital Requirement (MCR), which ensures (within a reasonable amount of certainty) that Nexus is always sufficiently capitalized to meet its obligations. That addresses one of the main risks with this type of arrangement: Nexus simply not having enough funds to back its claims.

Although NXM can be bought and sold only on the platform, there's a wrapped ERC20 (WNXM) available for trading on various exchanges. In practice, both of these tokens have been closely mirroring the price of ETH in recent months. That's to be expected, since the Nexus capital pool consists primarily of ETH.

The mechanics of how this all works get pretty deep. For further learning, the white paper and FAQ are a good place to start. Suffice it to say, the system's functionality has been proven out by Nexus's track record; it's been live for over a year and is currently providing users with around $320 million in coverage:



Active Cover Amount

$319,881,913 | 246,668 ETH

Total Premiums Paid

$8,607,069 | 6,692 ETH

Active Cover Amount

Source: Nexus Mutual Tracker, https://nexustracker.io/.

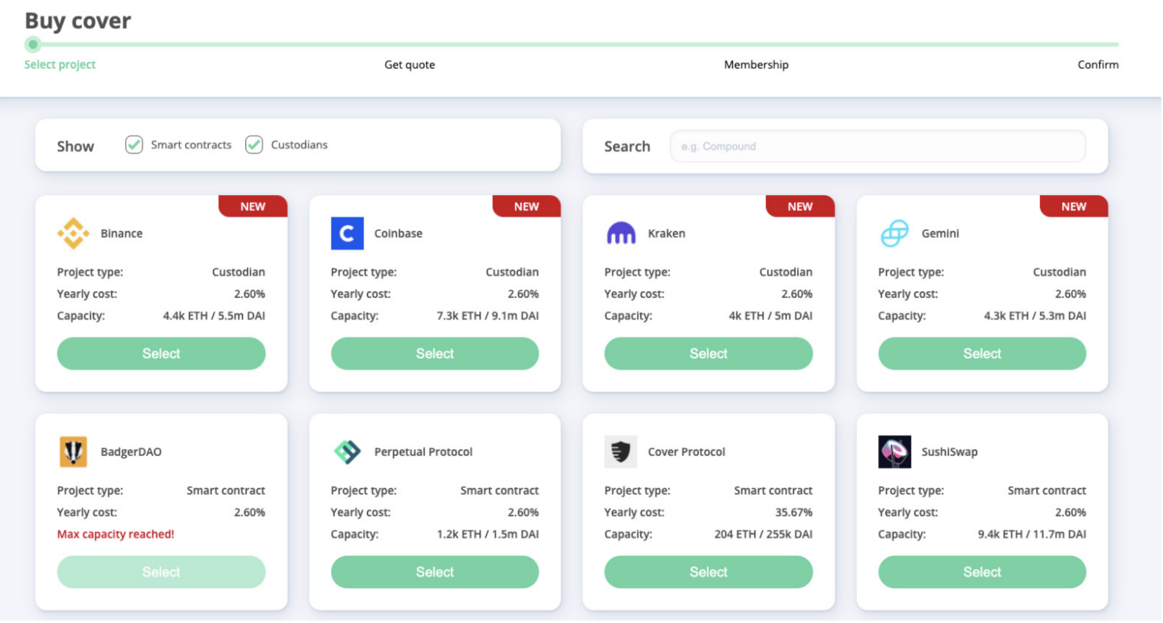
The project hit an important milestone in February 2020 when it paid out its first claim, related to an exploit of bZx. While claims assessors initially denied the claim because it appeared that oracle manipulation was the primary culprit, subsequent evidence showed that a smart contract bug was responsible for the loss of funds.

Nexus in Action

Occasionally in crypto, you have those magical moments where you realize you suddenly have newfound powers to do something cool. Nexus is one of those moments. Upon visiting the site, you'll see two primary options—one to supply cover, and one to purchase coverage. (Note that in order to participate or purchase NXM, you'll need to KYC your account and pay a small mutual membership fee.) Upon seeing the list of covered projects, the implication is immediately clear: you can purchase peace of mind and sleep easier at night.

Sure, all the usual suspects are here, from Uniswap to Balancer and SushiSwap. However, there's also coverage of many lesser-used projects and long-tail food tokens. Interestingly, you can even buy cover for Cover Protocol, which we'll cover next. Insurance Inception!

One interesting aspect of Nexus is that they've broadened their scope beyond smart contract coverage to include custodial exchanges. Should you choose to keep your digital wealth on a centralized exchange, you can mitigate some of that risk using Nexus. (Here at ShapeShift we strongly recommend buying a hardware wallet and avoiding those risks altogether.)



Binance
Project type: Custodian
Yearly cost: 2.60%
Capacity: 4.4k ETH / 5.5m DAI

Coinbase
Project type: Custodian
Yearly cost: 2.60%
Capacity: 7.3k ETH / 9.1m DAI

Kraken
Project type: Custodian
Yearly cost: 2.60%
Capacity: 4k ETH / 5m DAI

Gemini
Project type: Custodian
Yearly cost: 2.60%
Capacity: 4.3k ETH / 5.3m DAI

BadgerDAO
Project type: Smart contract
Yearly cost: 2.60%
Max capacity reached!

Perpetual Protocol
Project type: Smart contract
Yearly cost: 2.60%
Capacity: 1.2k ETH / 1.5m DAI

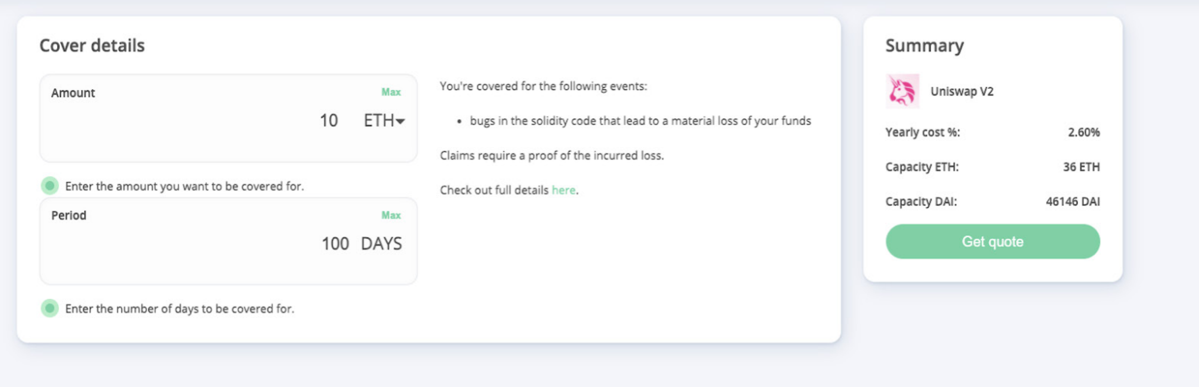
Cover Protocol
Project type: Smart contract
Yearly cost: 35.67%
Capacity: 204 ETH / 255k DAI

SushiSwap
Project type: Smart contract
Yearly cost: 2.60%
Capacity: 9.4k ETH / 11.7m DAI

Source: Nexus mutual, https://app.nexusmutual.io/cover/buy/select-project.

"But good ser, how much will it cost to purchase coverage before I ape into my next DeFi adventure?"

One can easily answer that question on the following screen. While costs vary with perceived risk, coverage is generally affordable and "feels right' for the various DApps that are presented. That's no accident; NXM risk assessors are economically incentivized to act as accurate actuaries.



Cover details

Amount
10 ETH
Enter the amount you want to be covered for.

Period
100 DAYS
Enter the number of days to be covered for.

You're covered for the following events:

- bugs in the solidity code that lead to a material loss of your funds

Claims require a proof of the incurred loss.

Check out full details here.

Summary

Uniswap V2

Yearly cost %:	2.60%
Capacity ETH:	36 ETH
Capacity DAI:	46146 DAI

Source: Nexus mutual, https://app.nexusmutual.io/cover/buy/select-project.

Building on the runaway success of liquidity mining during DeFi Summer, Nexus added an additional option in September: Shield Mining. This arrangement cleverly incentivizes NXM stakers to provide coverage for specific DApps by rewarding them with the project's native token. While this approach necessitates higher inflation from DApp-specific tokens, it looks like a good way to bootstrap early usage while also growing the coverage pool—and in turn, possibly making the incentivized DApp more attractive to less risk-averse users.

Risks

Nexus, like most platforms, has a few risks of its own. The platform could wind up being insufficiently capitalized to pay out claims, especially in the event of a cascading failure or smart contract bug that leads to the loss of funds across several DApps. In practice, this is made less likely by the Minimum Capital Requirement outlined above.

The DApp's smart contracts could also have their own problems. Solidity audits ostensibly have minimized those risks, and the DApp's track record of protecting millions of dollars also bodes well for the platform's ongoing security. With every passing week their Lindy-ness gets a bit stronger.

Finally, there's the scenario where an attacker could take out cover on a DApp prior to exploiting it and thereby maximize their "earnings." There's currently no easy way around this. However, the KYC requirement could dissuade some attackers from implementing this approach. Additionally, the MCR would likely prevent any related losses from deep-sixing the overall project.

03 Cover Protocol

NEW FRONTIERS

Cover Protocol

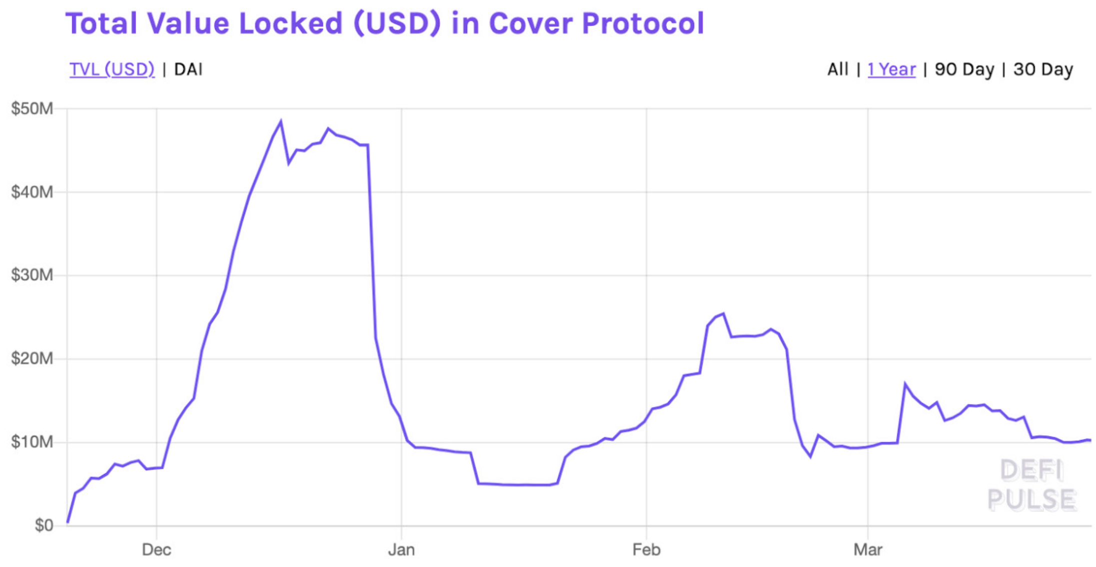
Cover is a more recent entrant to the decentralized insurance space, having launched last November.

This platform presents an interesting contrast to Nexus. The most notable difference is that coverage is provided via ERC20 “CLAIM” tokens. Separate token types are minted for each DApp and coverage expiry date. This presents an interesting scenario where a DEX could facilitate trading these ERC20s against other insurance projects, opening the door to arbitrage possibilities. CLAIM tokens could also be locked as collateral in all manner of crypto lending applications. (Similar to Nexus, Cover also offers Shield Mining.)

Another difference is the straight-outta-DeFi foundations of the project. One gets the sense that it was built by DeFi users, for DeFi users. The spirit of decentralization is embraced as well; there is no KYC with Cover, and the team includes multiple pseudonymous contributors.

Cover is such a DeFi-native project that yearn decided to acquire the platform in late November. This has led to a bifurcated experience where users can get down and dirty on Cover’s platform page, or enjoy a more streamlined experience in yearn.

Cover’s current TVL is also much smaller than Nexus, owing to a precipitous decline in late December. We’ll explain the reason for that decline shortly:



Source: Defipulse.com, https://defipulse.com/cover-protocol.

How It Works

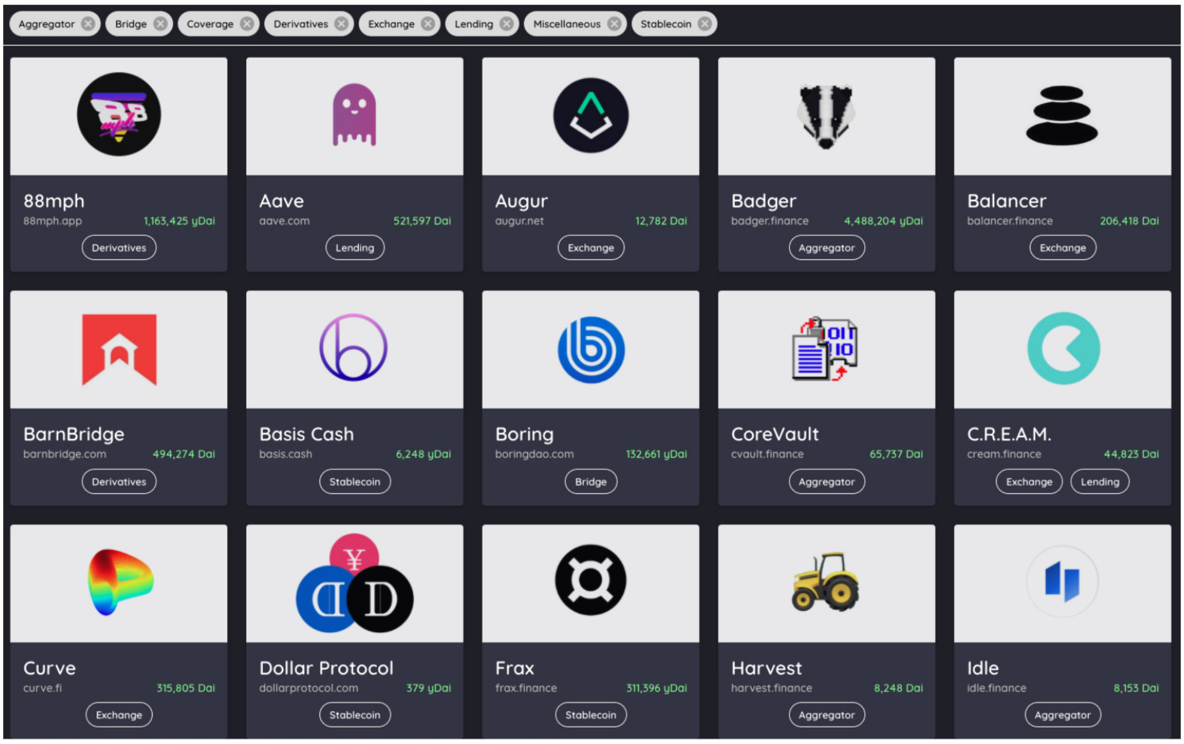
Unlike Nexus's bonding-curve approach, Cover employs a floating-rate open market for each of its CLAIM and NOCLAIM tokens. Market makers deposit collateral for a specific platform and expiry, then receive both CLAIM and NOCLAIM tokens in return. From there, they can earn a premium by selling those tokens, or they can add liquidity to one of the insurance markets.

Users seeking insurance can purchase CLAIM tokens, which expire at $1.00 (or 1 DAI, to be more specific) if a covered incident occurs. The tokenomics behind Cover's approach, while differing from the familiar bonding-curve process, work nicely in the context of the three primary actors in the Cover ecosystem: Market Makers, Coverage Providers, and Coverage Seekers.

Cover in Action

Relative to Nexus, Cover's user flow is more complicated. (If you'd like a deeper dive, Andre Cronje provided a granular explanation of the process.)

At a high level, though, the marketplace for projects is similar to Nexus. Users can choose what they'd like coverage on ...



88mph
88mph.app 1,163,425 yDai
Derivatives

Aave
aave.com 521,597 Dai
Lending

Augur
augur.net 12,782 Dai
Exchange

Badger
badger.finance 4,488,204 yDai
Aggregator

Balancer
balancer.finance 206,418 Dai
Exchange

BarnBridge
barnbridge.com 494,274 Dai
Derivatives

Basis Cash
basis.cash 6,248 yDai
Stablecoin

Boring
boringdao.com 132,661 yDai
Bridge

CoreVault
cvault.finance 65,737 Dai
Aggregator

C.R.E.A.M.
cream.finance 44,823 Dai
Exchange Lending

Curve
curve.fi 315,805 Dai
Exchange

Dollar Protocol
dollarprotocol.com 379 yDai
Stablecoin

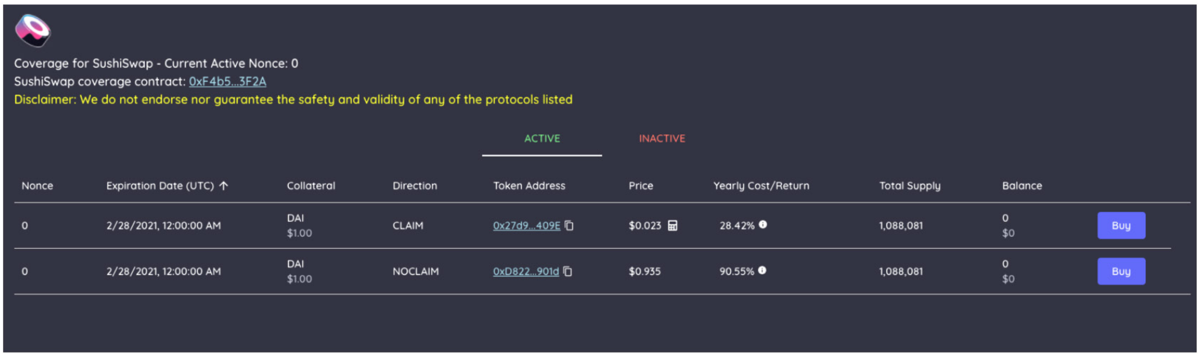
Frax
frax.finance 311,396 yDai
Stablecoin

Harvest
harvest.finance 8,248 Dai
Aggregator

Idle
idle.finance 8,153 Dai
Aggregator

Source: Coverprotocol.com, https://www.coverprotocol.com/

… then view the details of the coverage and the associated cost to purchase the relevant CLAIM tokens:



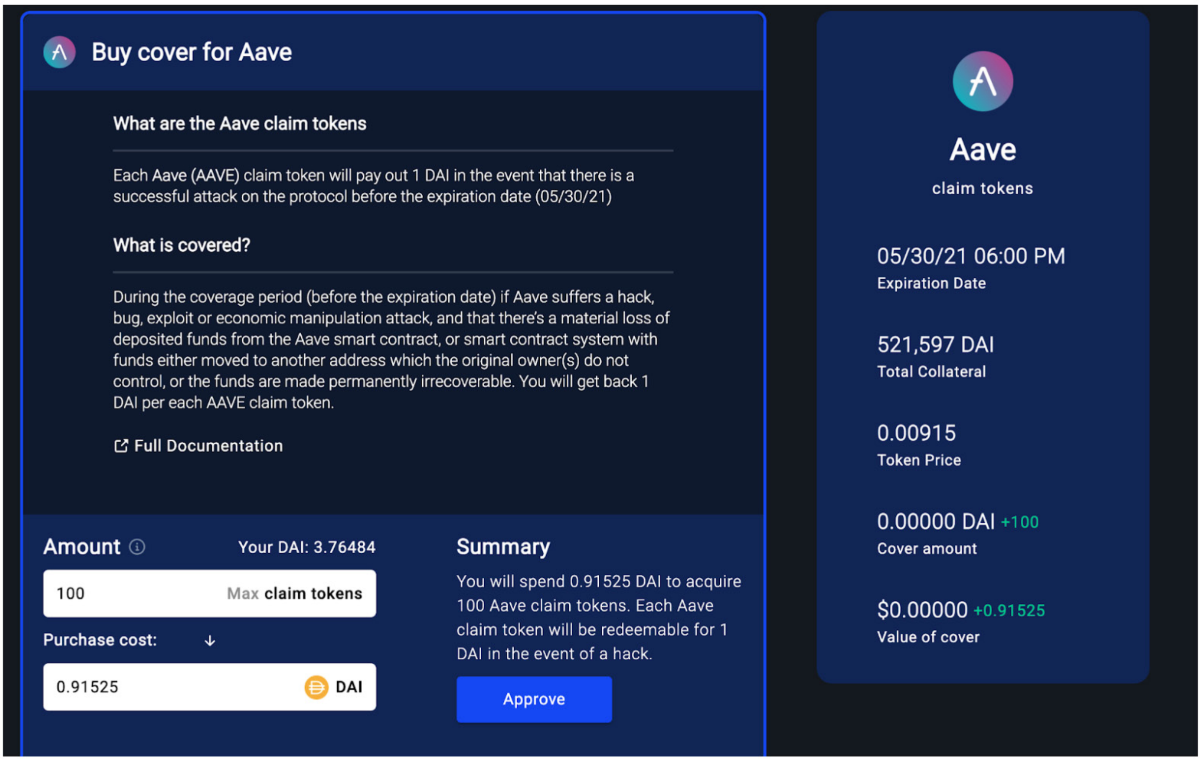
Coverage for SushiSwap - Current Active Nonce: 0
SushiSwap coverage contract: 0xF4b5...3F2A
Disclaimer: We do not endorse nor guarantee the safety and validity of any of the protocols listed

Nonce	Expiration Date (UTC) ↑	Collateral	Direction	Token Address	Price	Yearly Cost/Return	Total Supply	Balance	
0	2/28/2021, 12:00:00 AM	DAI $1.00	CLAIM	0x27d9...409E	$0.023	28.42%	1,088,081	0 $0	Buy
0	2/28/2021, 12:00:00 AM	DAI $1.00	NOCLAIM	0xD822...901d	$0.935	90.55%	1,088,081	0 $0	Buy

Source: Coverprotocol.com, https://www.coverprotocol.com/

One challenge with Cover Protocol is that it takes many steps to secure coverage through the platform. In addition to UX friction, this may be cost-prohibitive for some users since many of those steps involve an on-chain transaction—not a fun proposition when gas prices seem to be at permanently elevated levels. Look for Cover to streamline this UX over time, and possibly even integrate the DApp in one of the emerging layer-2 platforms.

In terms of the yearn integration, things are already moving quickly along those lines. Available under "COVER" on the yearn interface, there are over 20 DApps to choose from. Pick one, and you'll be greeted with a very simple interface for purchasing or selling CLAIM tokens. Here, we see a big advantage of the ERC20 approach; while more complex actions happen on the actual Cover platform, yearn is facilitating much more streamlined buying and selling of coverage. For users who want to quickly and easily purchase insurance on one of the listed DApps, yearn's interface is the way to go:



Buy cover for Aave

What are the Aave claim tokens

Each Aave (AAVE) claim token will pay out 1 DAI in the event that there is a successful attack on the protocol before the expiration date (05/30/21)

What is covered?

During the coverage period (before the expiration date) if Aave suffers a hack, bug, exploit or economic manipulation attack, and that there's a material loss of deposited funds from the Aave smart contract, or smart contract system with funds either moved to another address which the original owner(s) do not control, or the funds are made permanently irrecoverable. You will get back 1 DAI per each AAVE claim token.

Amount — Your DAI: 3.76484
100 — Max claim tokens
Purchase cost: ↓
0.91525 DAI

Summary

You will spend 0.91525 DAI to acquire 100 Aave claim tokens. Each Aave claim token will be redeemable for 1 DAI in the event of a hack.

Aave
claim tokens

05/30/21 06:00 PM
Expiration Date

521,597 DAI
Total Collateral

0.00915
Token Price

0.00000 DAI +100
Cover amount

$0.00000 +0.91525
Value of cover

Source: Coverprotocol.com, https://www.coverprotocol.com/

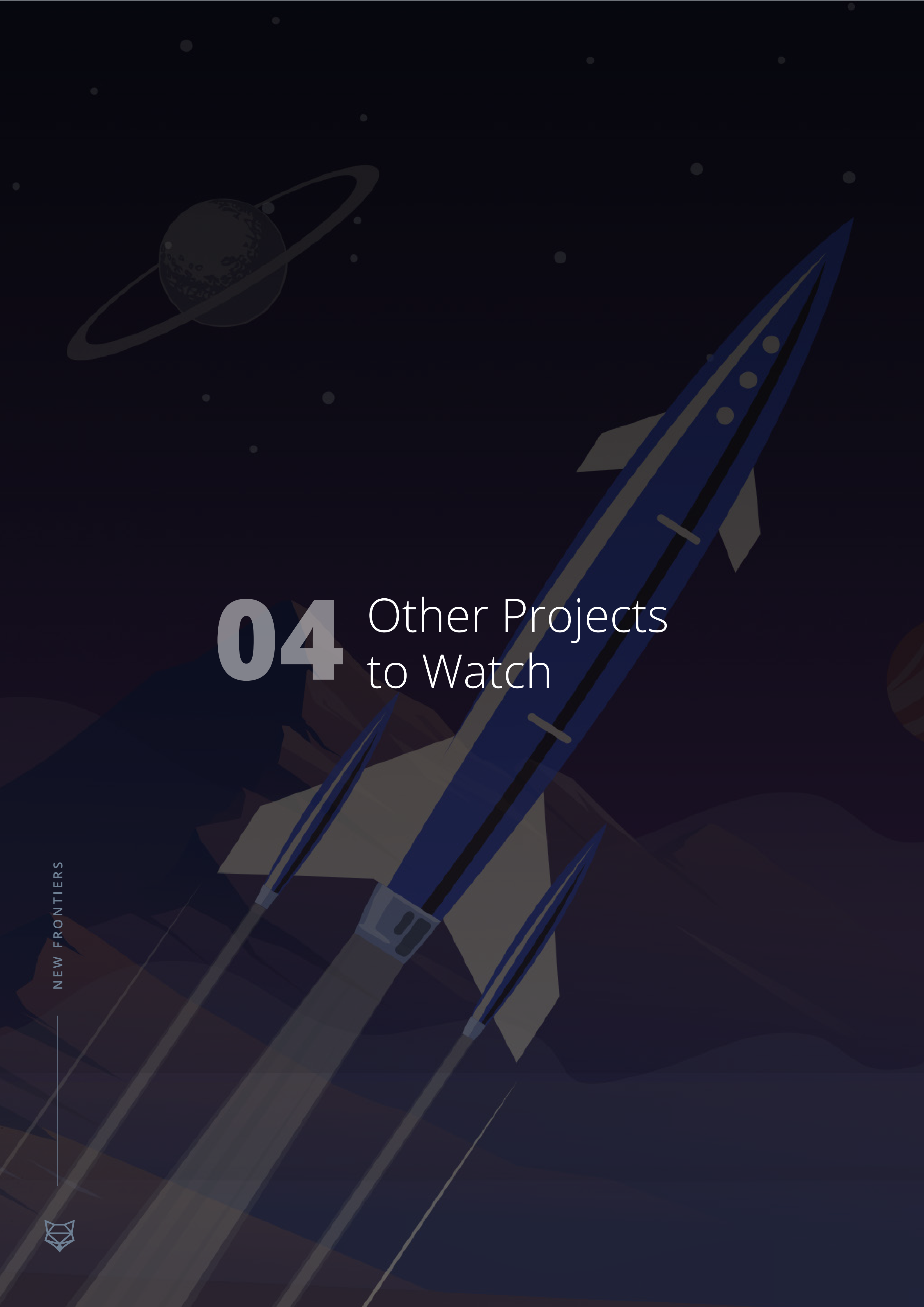
Risks

In the prior section, we mentioned how Nexus itself could be vulnerable to smart contract exploits.

That risk applies to Cover Protocol as well—a point that was driven home in December when an attacker triggered an infinite-inflation function, leading to a loss of more than 4,000 ETH.

While a loss of this magnitude could be the death knell for some projects, the attacker fortunately turned out to be a whitehat, and all funds were returned. Only in crypto.

Suffice it to say, Cover survived the hack and appears to be in a stronger position thanks to its merger with yearn. The DApp may have benefited from anti-fragility, having addressed the exploits, and it's also likely to benefit from yearn's resources with respect to future smart contract updates and audits.



04 Other Projects to Watch

Other Projects to Watch

Etherisc

The O.G. of the Ethereum-based insurance space, Etherisc has been around since 2016. That's like 25 years in ETH time!

Etherisc initially grabbed a lot of attention for offering flight insurance to Devcon attendees. Since then it's broadened its scope with designs for crop insurance, hurricane insurance, crypto-based loans, and more.

As explained in this video, the platform uses oracle data from Chainlink as the foundation for its insurance products. The key distinction here is that, rather than focusing solely on the smart contract and crypto space, this oracle-based approach could be leveraged to provide coverage for all manner of "real-world" events—some that may not be offered by traditional insurers.

Opyn

Opyn does not offer insurance per se. However, it does provide the ability to hedge the risk of holding various assets. For instance, last year the project implemented a partnership with Compound, whereby users could hedge the risk of holding COMP by purchasing Put options on the asset. (For the uninitiated, Puts generally increase in price when the underlying asset declines, thereby offering a hedge against holding the asset).

05 Key Takeaways

Key Takeaways

In my prior report on staking derivatives, I noted just how early that niche is and how much more room there is for innovation and evolution. That's also the case with decentralized insurance.

Over the coming year, look for more variety in the types of coverage offered as Nexus and others branch out from focusing primarily on smart contract risks.

More market data should make the "actuarial" process easier for those thinking about coverage oracle hacks and other economically incentivized exploits. And as DeFi continues to grow, look for increased economic efficiencies and competing projects to emerge, likely leading to better pricing for coverage.