opencover

# The State of DeFi Insurance Alternatives (DeFi Cover) 2023

Nexus Mutual · UNSLASHED · INSURace · SHERLOCK · ease · NEPTUNE MUTUAL

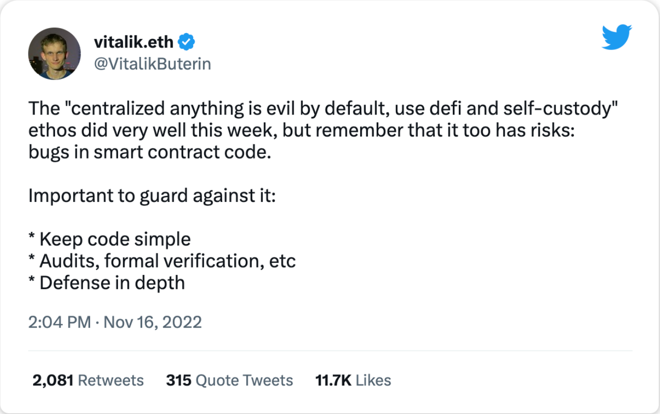
chainproof · carapace · Risk Harbor · UnoRe · solace · Amulet

OpenCoverDeFi

# Foreword

**Your keys, your coins — your risk**. In the aftermath of the dramatic CeFi events of 2022, self-custody and DeFi emerged as the ultimate solution for a safer digital asset ecosystem with usability often cited as the main barrier to adoption. With a record $3 billion lost to DeFi exploits last year, it is likely security will prove to be the fundamental bottleneck.

DeFi risk mitigation remains an open problem. Beyond individual security measures such as robust key management and transaction simulation, insurance alternatives, commonly known as DeFi cover, are the primary solution to DeFi technical and economic risks.



vitalik.eth
@VitalikButerin

The "centralized anything is evil by default, use defi and self-custody" ethos did very well this week, but remember that it too has risks: bugs in smart contract code.

Important to guard against it:

* Keep code simple
* Audits, formal verification, etc
* Defense in depth

2:04 PM · Nov 16, 2022

**2,081** Retweets **315** Quote Tweets **11.7K** Likes

In practice, DeFi cover is a rapidly emerging industry with heterogeneous approaches to risk management, governance and claim assessment. Extrapolating from the fundamental role of traditional insurance in off-chain Finance, DeFi cover is poised to play a key role in scaling and normalizing its on-chain counterpart.

We launched OpenCover in Q3 2022 to provide the standardized, unbiased industry data missing to democratize DeFi cover and contribute to make DeFi safe and accessible. Today, we could not be more excited to share unique insights from the data collected over the past 9 months, together with key insights from insiders building at the forefront of the industry.

Great things ahead,

**Jeremiah Smith** @itsJeremiahS
**OpenCover** co-founder and CEO

*Special thanks to my-co author Yohji van Weert, Will Robinson from Alliance, Richard Chen from 1confirmation, NFX and Orange DAO for the precious feedback and support.*

# Key Takeaways

- Born in 2017, the DeFi cover industry is now composed of 23+ active participants from DAO-governed protocols to regulated companies. 9 new players launched in 2022.
- Historically, DeFi cover providers focused on protocol, custody, and stablecoin depeg risks. The recent launch of new products like validator slashing, audit and credit default covers, indicate offerings are evolving in tandem with the overall ecosystem.
- At time of writing, OpenCover tracked $286m in current underwriting capital across on and off-chain pools covering $231m in risks (~0.5% of DeFi TVL). This represents over 90% of industry activity extrapolating from the size of on-chain capital pools.
- Historical data shows an all-time total of 19,839 covers sold, 552 claims and 379 payouts across leading on-chain DeFi cover providers so far. The number of covers sold since Nov. 6, 2022 grew by 85% compared to the previous 4 months. While materially driven by L2 airdrop speculation, the real figure is estimated to be ~15%. However, the total amount of active cover decreased 44% since its June 2022 peak.
- 2022 marked the industry's first large-scale stress test with $34.4m in claims paid out (out of $36.9m all-time tracked total i.e. over 90% of all payouts occurred in the last 12 months). Notable payouts: UST depeg ($22.5m paid out), FTX collapse ($4.7m paid out)
- For 2023, DeFi cover founders and builders are most excited about: cover marketplaces, scaling cover capacity and bridging the gap with traditional insurance.
- Delivering these advances at scale will likely be key for rekindling and growing institutional DeFi adoption as the lack of insurance is often cited as a key friction point.

# Table of Contents

# 1 Scope and Methodology

This report was created to answer the fundamental questions about the lesser known, but increasingly important, DeFi cover i.e. DeFi insurance alternatives industry. How big is it? Who are the main players? What are the different approaches to cover? How is adoption evolving? What (future) role does the industry play in the overall digital asset ecosystem?

To compile what we have found to be the first in-depth analysis of its kind, data was collected between June 6, 2022 and March 6, 2023 across 7 EVM compatible chains (Ethereum, Polygon, Arbitrum, Optimism, BNB Smart Chain, Astar and Avalanche).

OpenCover's data infrastructure collects on-chain events, smart contract state and transaction trace data using leading blockchain node providers such as Alchemy, Chainstack and Infura for chain coverage and resilience.

OpenCover research indicates there are at least 23 active players in the space operating fully on-chain or as off-chain regulated entities. The report's penultimate industry data section, offering a deep dive into the longitudinal evolution of underwriting capital, active cover amount and claims data was compiled from 9 of the most active cover providers. This represents over 90% of the industry's on-chain underwriting capital[1] (Nexus Mutual, Unslashed Finance, InsurAce, Chainproof, Sherlock, Neptune Mutual[2], Risk Harbor[3], InsureDAO[4] and Ease[5]).

[1] Derived from TVL analysis of providers listed on DeFiLlama (protocol TVL ≠ underwriting capital).
[2] Data collection start: December 1, 2022 following provider initial launch on mainnet.
[3] Data collection paused from 31 Dec 2022 following V2.5 launch, expected to resume with V3.
[4] Data collection start: November 14, 2022.
[5] Data collection start: Jan 25, 2023.

# 2 DeFi Cover (DeFi Insurance Alternative)

Despite insurance being a $6 trillion industry, traditional insurance providers typically only offer risk protection in a narrow area of the digital assets ecosystem: custody. Recent examples include Copper, which secured $500m of insurance for digital assets it holds in cold storage from AON through a Lloyd's of London syndicate in November 2022.

To date, DeFi-native risks such as smart contract vulnerabilities have not been insurable by traditional providers due to their novelty and complexity. This led to the creation of native solutions built from the ground up within the DeFi ecosystem. The term *DeFi insurance* is often used to describe this new type of risk protection, a more accurate term is *DeFi cover* as traditional insurance is a heavily regulated industry, and while some providers are able to offer bona fide insurance, most products are discretionary rather than contractual.

DeFi cover providers are a relatively recent development with the first provider established in 2017 (Nexus Mutual). These providers typically function as a DAO that governs an on-chain protocol that facilitates the purchase of cover, assessment of claims, and triggering of payouts. In addition to enabling mitigation of new risks, the transparency of on-chain operations and opportunity for anyone to participate are frequently highlighted as the unique value propositions of decentralized approaches to DeFi cover.

> *DeFi cover is one of the fundamental building blocks that's necessary for the next wave of capital to enter the ecosystem. Both retail users and institutions require safety nets like they enjoy in traditional finance to be comfortable participating in on-chain markets. This is a huge opportunity for the wider DeFi cover space and Nexus Mutual specifically as we work to embed our products within the ecosystem. In 2023, we will see teams building solid foundations for future DeFi adoption, with innovations setting the stage for years to come.*

**Hugh Karp** @HughKarp
Founder at **Nexus Mutual**

Despite the increasing demand for insurance in DeFi, OpenCover has only tracked $231 million of covered funds in DeFi (~0.5% of DeFi TVL) across the bulk of underwriting capital at the time of writing, a significant gap in the market.

## 2.1 Provider Overview

The DeFi cover market comprises at least 23 active players (with offerings in development, alpha/beta or ready for live purchase) with a dichotomy between centralized and decentralized providers. Decentralized providers operate fully on-chain, typically as a decentralized autonomous organization (DAO) and are designed to offer trust-minimized risk protection. Centralized providers operate as regulated entities (e.g. will require KYC/KYB) and keep a significant portion, if not all, of their operations off-chain providing a more familiar customer experience.

### DeFi Cover Provider Landscape (DeFi Insurance Alternatives)

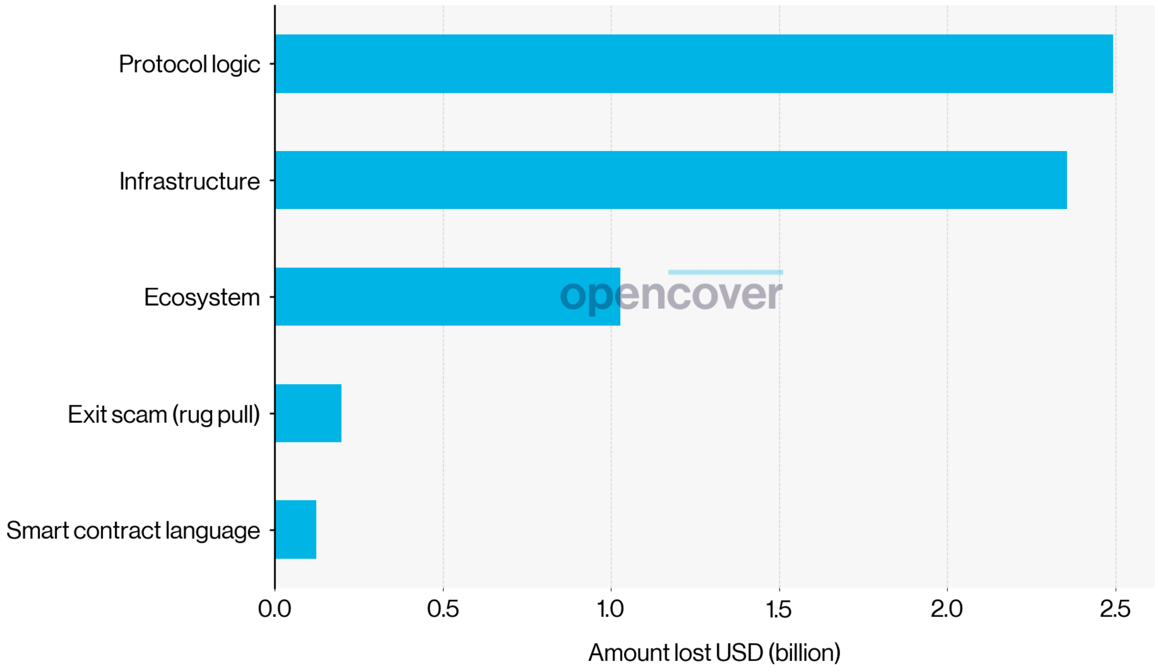
| On-chain | | | |
|---|---|---|---|
| **Community voting claims assessment** | **Parametric claims assessment** | **Optimistic oracle claims assessment** | **Expert claims assessment** |
| Nexus Mutual | Risk Harbor | UNSLASHED | UnoRe |
| INSURace | ETHERISC | SHERLOCK | InsureDAO |
| ease | Amulet | NEPTUNE MUTUAL | carapace |
| FAIRSIDE | BUMPER | **Hybrid claims assessment** | bridge.v2 |
| nimble. | solace | Amulet | CheckDot |
| | Y2K FINANCE | tidal | |
| **Off-chain - regulated** | | | |
| chainproof | ETHERISC | BREACH Crypto Shield | Evertas |

Source: OpenCover active providers as of March 2023

# 3 DeFi Risks

Since inception, DeFi users have suffered losses in excess of $6 billion due to technical and governance exploits according to DeFiLlama (this figure does not include economic failures such as the UST depeg or custodian failures such as the FTX collapse). For comparison, this figure represents over 10% of the $48 billion DeFi market cap at the time of writing.

Funds lost to DeFi exploits 2016-2023



Source: OpenCover, DeFiLlama

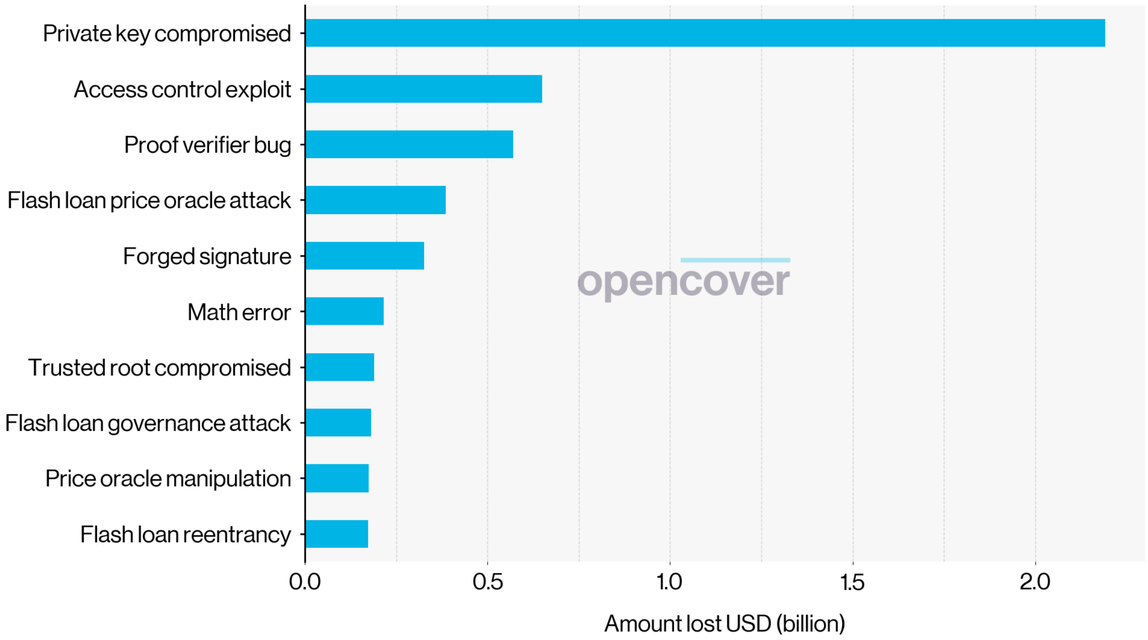
| DeFi Exploit Classification | |
|---|---|
| **Protocol logic** | Involves exploiting vulnerabilities in the logic behind a protocol. |
| **Infrastructure** | Focused on the underlying technology and physical components that support the system, such as servers, networks, and storage. |
| **Ecosystem** | Related to the wider context in which the system operates, such as the oracles, governance, and external factors. |
| **Smart contract language** | Exploiting vulnerabilities in the language used to write smart contracts. |
| **Exit scam ('rug pull')** | Intentional draining of funds, usually by the deployer themself. |

## 3.1 DeFi Exploit Attack Vectors

The most common DeFi exploit attack vectors can be divided into five categories: protocol logic, infrastructure, ecosystem, smart contract language, and exit scam (commonly referred to as 'rug pull') with the first two categories accounting for 78% of recorded fund loss ($4.84 billion).

Within the broader exploit classification, the leading attack vector is compromised private keys which led to nearly $2 billion in losses. Historically, the typical implementation of cross-chain bridges have been notoriously fragile to this type of attack with the Ronin bridge exploit standing out as the largest loss in the category with $624 million lost.

**Funds lost to DeFi exploits, top 10 attack vectors 2016-2023**



Source: OpenCover, DeFiLlama

While secure private key management remains a key challenge for the broader adoption of self-custody, compromised private keys are often due to targeted attacks or user errors such as social engineering and phishing. As such, current cover solutions typically exclude losses due to compromised private keys, historically responsible for $2.19 billion of funds lost to DeFi exploits, and focus on protecting users against risks beyond their control.

The combined historical losses of the 9 other leading DeFi attack vectors ($2.87 billion) fall into the category of protocol design flaws and technical risks that can typically be protected against through DeFi cover such as the $611 million Poly Network access control exploit.

| Top 10 DeFi Exploit Attack Vectors | | |
|---|---|---|
| **Private key compromised** | Infrastructure | Compromising the private key used to secure a system to gain access to funds. |
| **Access control exploit** | Protocol logic | A type of vulnerability that allows an attacker to gain unauthorized access to a system or smart contract. |
| **Proof verifier bug** | Protocol logic | A type of vulnerability in which an attacker can manipulate a proof verification process to trick a smart contract into executing a transaction. |
| **Flash loan price oracle attack** | Ecosystem | An attack which leverages a flash loan to manipulate the price of an asset to ultimately extract value from a protocol. |
| **Forged signature** | Protocol logic | An attack that involves forging a digital signature to gain access to a smart contract or other system. |
| **Math error** | Protocol logic | An attack that takes advantage of errors in mathematical calculations, leading to unexpected or unintended behavior in a smart contract. |
| **Trusted root compromised** | Protocol logic | Occurs when a vulnerability in a trusted component is exploited to manipulate data or gain unauthorized access to a system. |
| **Flash loan governance attack** | Ecosystem | Attempt to manipulate the decision-making processes, often through the accumulation of voting power or the exploitation of governance vulnerabilities. |
| **Price oracle manipulation** | Ecosystem | An exploit that manipulates a price oracle, leading to inaccurate price data being used in smart contract execution. |
| **Flash loan reentrancy** | Ecosystem | A type of vulnerability that allows an attacker to repeatedly call a function before the previous execution completes, allowing them to manipulate the state of the contract to their advantage. |

Losses attributed to vulnerabilities in the smart contract language or to exit scams are considerably smaller and have therefore not made it in the top 10 attack vectors.

Assuming the continued adoption of more robust private key management practices (e.g. hardware wallets, MPC, social recovery mechanisms) and growth in transaction security solutions (e.g. in-wallet transaction simulation, anti-phishing filters), it is expected that DeFi security will increasingly hinge on protecting against protocol-level and economic risks.

> *The DeFi market will undergo a narrative change this year as DeFi users demand for better security standards from protocols. DeFi users are frustrated by the unending hacks and exploits directly affecting their portfolios, and they will prefer insured protocols over others which will make adoption much faster. Overall, we think security will take the limelight and become the central focus and priority for a lot of players in the space - big or small.*

**Misbah SP** @Misbah6SP
CMO at **UnoRe**

## 3.2 DeFi Economic Risks

DeFi protocols can function as designed but lead to undesired economic outcomes despite the lack of technical exploits as in the infamous case of UST. In May 2022, the algorithmic stablecoin depegged from the dollar causing $17 billion in losses for UST holders despite its underlying on-chain peg-stabilizing mint and burn mechanism working as intended from a technical perspective. DeFi cover products, such as stablecoin depeg and pegged asset depeg cover exist to mitigate these new economic risks. Notably, some DeFi providers offer stablecoin depeg cover for asset-backed and centrally managed stablecoins such as USDC, effectively protecting against off-chain risks.

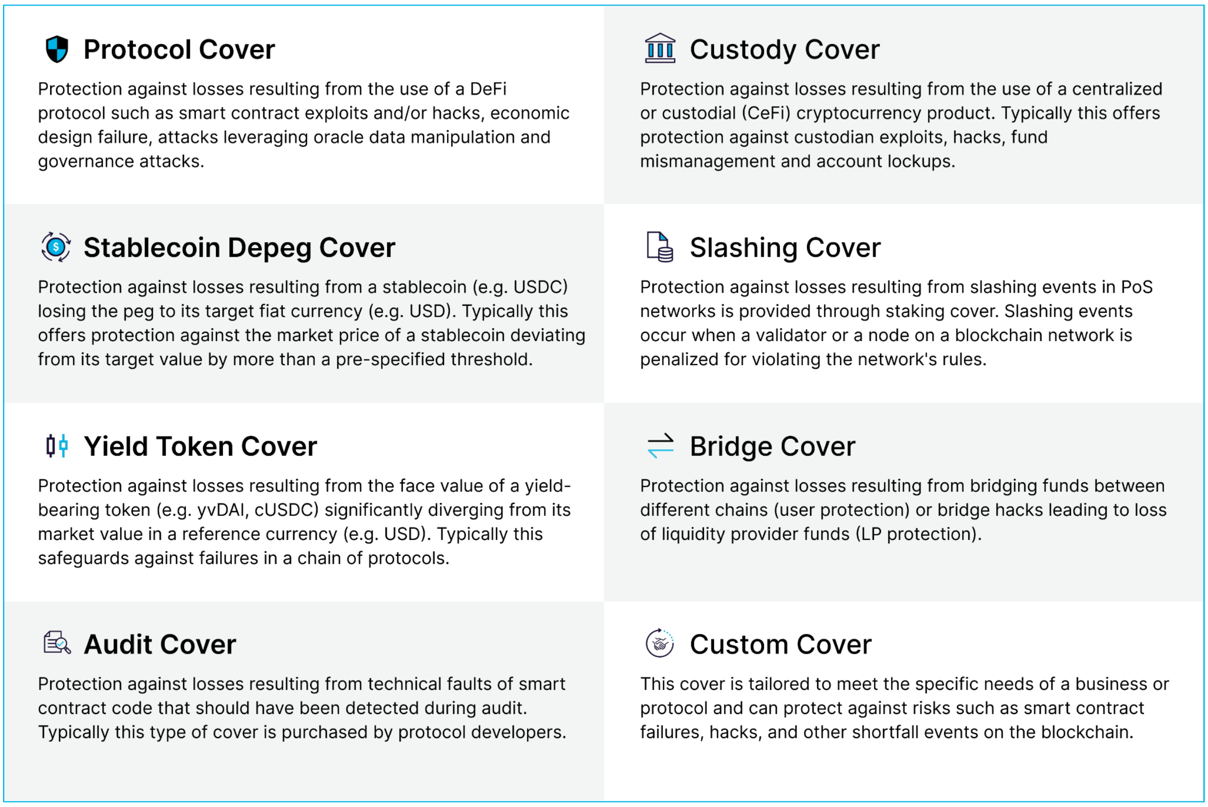
## 3.3 DeFi Cover Beyond DeFi

DeFi cover providers effectively offer specialist insurance alternatives where traditional insurance players have not yet been able to meet the demand. This includes custody cover to protect against risks associated with holding user funds in centralized finance applications (aka CeFi) such as centralized cryptocurrency exchanges. While not a DeFi risk per se, third-party custody is often part of the DeFi user experience because on and off-ramping from DeFi to the traditional financial system requires the use of centralized, custodial intermediaries. While it remains unclear whether DeFi cover providers will seek to expand and scale their cover offering for CeFi products in the short term given recent events, cover for real-world risks are actively being developed across multiple providers.

# 4 DeFi Cover Products

Eight broad categories of covers are currently offered, with each provider having their own terms and exclusions pointing to a nascent industry with standardization still in progress.

### DeFi Cover Categories



**Protocol Cover**

Protection against losses resulting from the use of a DeFi protocol such as smart contract exploits and/or hacks, economic design failure, attacks leveraging oracle data manipulation and governance attacks.

**Custody Cover**

Protection against losses resulting from the use of a centralized or custodial (CeFi) cryptocurrency product. Typically this offers protection against custodian exploits, hacks, fund mismanagement and account lockups.

**Stablecoin Depeg Cover**

Protection against losses resulting from a stablecoin (e.g. USDC) losing the peg to its target fiat currency (e.g. USD). Typically this offers protection against the market price of a stablecoin deviating from its target value by more than a pre-specified threshold.

**Slashing Cover**

Protection against losses resulting from slashing events in PoS networks is provided through staking cover. Slashing events occur when a validator or a node on a blockchain network is penalized for violating the network's rules.

**Yield Token Cover**

Protection against losses resulting from the face value of a yield-bearing token (e.g. yvDAI, cUSDC) significantly diverging from its market value in a reference currency (e.g. USD). Typically this safeguards against failures in a chain of protocols.

**Bridge Cover**

Protection against losses resulting from bridging funds between different chains (user protection) or bridge hacks leading to loss of liquidity provider funds (LP protection).

**Audit Cover**

Protection against losses resulting from technical faults of smart contract code that should have been detected during audit. Typically this type of cover is purchased by protocol developers.

**Custom Cover**

This cover is tailored to meet the specific needs of a business or protocol and can protect against risks such as smart contract failures, hacks, and other shortfall events on the blockchain.

opencover

## 4.1 Protection Types

### 4.1.1 Protocol Cover

Protocol cover protects against financial losses resulting from the use of a DeFi protocol. Covered risks are provider specific and typically protect against a combination of:

- Smart contract exploits: intentional misuses of a smart contract that allow an attacker to manipulate contract execution in their favor such as reentrancy attacks.
- Smart contract bugs: unintentional programming errors in smart contract code that result in user fund loss such as computational errors.
- Economic design failure: fundamental flaws in protocol design that leave users vulnerable to edge cases such as large amounts of capital entering and exiting the protocol in a short amount of time leveraging via flash loans.

- Oracle failures or manipulation: incorrect protocol state due to intentional or accidental disruption of a data source (oracle) used in its smart contracts.
- Governance attacks: malicious players gaining enough voting power to reshape protocol rules in their favor.

Notable protocol failures:

- The absence of a delay in proposal execution combined with the use of flash loans allowed a hacker to execute two subsequent malicious proposals on Beanstalk governance, getting away with $181 million.
- Rari Capital suffered an $80 million loss due to the lack of proper reentrancy protection.
- An oracle manipulation attack has allowed a malicious actor to steal $15 million from Inverse Finance by manipulating the price of their governance token (INV).

### 4.1.2 Stablecoin and Other Pegged Assets Depeg Cover

Stablecoin depeg cover protects against losses resulting from a stablecoin (e.g. USDT, DAI) losing its peg to a target fiat currency (e.g. USD) so that the user is unable to redeem the stablecoin for the intended amount of pegged currency. Pegged asset depeg cover works similarly for assets pegged to non-fiat currencies (e.g. Lido's stETH depegging from ETH).

Depeg covers differ across providers in terms of:

- The percentage decrease in price that qualifies as a depeg event.
- The duration of the depeg to qualify as a depeg event.
- The percentage of the token's original market price that is reimbursed.
- Whether the event qualifies for total or partial financial reimbursement.

Claims for depeg cover are typically made after the Time Weighted Average Price (TWAP) as reported by a price authority (e.g. Chainlink, Coingecko) over a predefined time frame reaches the cover policy's specified threshold.

Notable stablecoin depeg events:

- The UST stablecoin started losing its peg on May 9, 2022 and lost more than 99% of its value in the days that followed. A total of $22.5 million was paid out in claims[6].

[6] 11,629,014 USDC + 1,752,443 USDT + 5,780 ETH + 402 AVAX + 50 BNB + 27,744 MATIC, dollar equivalent computed using cryptocurrency prices at the time of payout.

- The Waves native USDN stablecoin has been depegged for 6 months at the time of writing and is currently trading at 80% below the peg.

> *I expect to see continued growth of insurance products in the market, as more and more investors seek out ways to protect their digital assets. This will be driven by the increasing popularity of DeFi platforms, the rise of new risk management tools and techniques, and the ongoing development of blockchain technology itself.*
>
> *One of the most important of these will be the emergence of bridges between traditional insurance and blockchain-based DeFi cover, which will enable higher capacities and greater flexibility in the insurance market, benefitting DeFi with higher capacity, and Traditional Insurance with higher efficiency. Another key trend I expect to see is the rise of decentralised insurance marketplaces, which will offer a wider range of coverage options and greater accessibility for users.*

**Dan Thomson** @vagrantcrypto
CMO at **InsurAce**

### 4.1.3 Yield Token Cover

Yield token cover safeguards against losses caused by the face value of a yield-bearing LP token, such as yvDAI or cUSDC, significantly deviating from its market value in a reference currency, such as DAI or USD.

The loss of value can be attributed to different kinds of shortfall events such as smart contract exploits, oracle failure, economic design, and governance attacks. Similar to stablecoin depeg cover, yield token cover also has a depeg requirement that must exceed a certain percentage of its face value for a claim to be paid.

Notable yield token depeg event:

- The yDAI v1 vault was compromised on February 4, 2021, resulting in an $11 million loss. A total of 132,160 DAI and 1,351 ETH were paid out in claims.

### 4.1.4 Custody Cover

Custody cover protects against losses that may occur for digital assets held in a custodial accounts (e.g. centrazlied exchange). Covered risks are provider specific and typically protect against:

- Theft: the custodian wallet gets hacked, leading to a loss of funds for the customers.
- Halted withdrawals: the user is prevented from accessing their funds for an extended period without prior notice from the custodian.

Custody cover varies across providers in scope, including how much of a loss is required to submit a qualifying claim and how long the user must wait after the loss of funds to submit a claim. Typically, the cover holder must be able to prove a 10% loss of funds kept with the custodian and wait more than 90 days after the shortfall event to file their claim.

Notable custody failure events:

- FTX halts all crypto withdrawals on November 8, 2022. About $8.9 billion in customer funds were stuck on the exchange. Approximately $4,795,709 in claims have been paid by Nexus Mutual and InsurAce.
- Hodlnaut suspends withdrawals on August 9, 2022, holding about $250 million in customer funds. About $1 million in claims have been paid out by Nexus Mutual to cover this event.

### 4.1.5 Bridge Cover

Currently, Bridge Cover provides protection against losses when using a bridge to transfer funds from one blockchain to another. While in high demand, OpenCover is unaware of protection against malicious depletion of liquidity pools used to bridge funds (LP protection) due to the historically risky centralized architectures of most existing bridges.

Notable bridge failure events:

- The Ronin Bridge was drained for $624 million due to the compromise of multiple private keys on March 23, 2022.

- The Harmony Bridge was drained due to a private key compromise, leading to a loss of $100 million.

### 4.1.6 Audit Cover

Unlike the cover types above, audit cover is directly purchased by protocols developers, rather than protocol end users, to protect a protocol against vulnerabilities undetected during audit. It is typically offered by auditors as a form of paid warranty on their service. By purchasing audit cover, protocols are effectively bearing the cost of protecting users against losses due to smart contract bugs up to the cover amount.

> *Ultimately, the goal is to protect as many end users as possible and Sherlock is excited to see more collaboration in the DeFi cover space in 2023. Working together to diversify risks across different capital pools is the path to covering the maximum amount of TVL and Sherlock expects the approach it pioneered, combining audits with cover, to become industry norm in the next 12-24 months.*

**Jack Sanford** @jack__sanford
Co-founder at **Sherlock Protocol**

Notable Audit failure events:

- The Euler protocol was drained of $197m using a vulnerability in account health checks that went undetected 8 months despite multiple audits.
- Solidity Finance failed to detect a vulnerability in Elephant Money's pricing system, which was subsequently exploited in a flash loan attack, resulting in a loss of $22m.
- An attacker exploited a vulnerability in Crema Finance's owner validation process to steal $8.8m in excess LP fees. Although the auditors Sec3 and Slowmist identified the vulnerability of the swap method, it went undetected in the claim method.
- The auditing firm Armor labs failed to detect an oracle manipulation attack vector that resulted in a loss of $13.4m for Deus DAO.

### 4.1.7 Slashing Cover

Slashing cover protects against funds lost due to slashing on a proof-of-stake (PoS) blockchain, and is offered to professional validators. Slashing refers to the penalty imposed on validators (stakers) who break the rules of the PoS consensus mechanism, such as double-signing or failing to reach consensus. The penalty results in a reduction of the staked assets which can lead to substantial losses for stakers.

Causes of slashing events include:

- Misconfiguration of validator nodes.
- Presence of bugs or unknown issues in validator client software.
- Downtime due to external factors such as network outages.
- External exploits of vulnerabilities in the software exposed by the node operator.

While there were no notable slashing events thus far, routine validator slashing occurs relatively regularly.

### 4.1.8 Custom Cover

Custom Cover is akin to specialist insurance in a traditional setting. With DeFi risks being new and complex, protocol and application developers sometimes seek cover tailored to their specific operations unavailable on the open market. For instance, this could be to protect against failures in a chain of third party protocols or wrapper on-chain code on the backend of a dApp.

OpenCover expects that the demand for Custom Cover will grow significantly starting this year, as DeFi and the associated cover infrastructure, e.g. cover marketplaces, mature.

# Comparison of Leading DeFi Cover Providers

| | Org. Type | Claims process | Contracts | Investors | Cover provided | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Protocol | Pegged asset | Yield Token | Custody | Audit | Bridge | Slashing |
| Nexus Mutual | DAO | Community vote | Open source | 1confirmation, Blockchain Capital, Placeholder + 6 others | ✓ | | ✓ | ✓ | | | ✓ |
| UNSLASHED | DAO | Optimistic oracle | Open source | Lemniscap, Chainlayer, P2P capital + 4 others | ✓ | ✓ | | ✓ | | | |
| INSURace | DAO | Community vote | Partially open source | ParaFi, Hashkey, DeFiance Capital, 10 others | ✓ | ✓ | | ✓ | | | |
| Risk Harbor | Private Co. | Parametric | Closed source | Coinbase, Bain Capital, Pantera, + 7 others | | ✓ | ✓ | | | ✓ | |
| SHERLOCK | DAO | Optimistic oracle | Open source | Alliance, CoinFund, Archetype | | | | | ✓ | | |
| chainproof | Private Co. (Regulated) | Expert panel | Off-chain | Undisclosed | ✓ | | | | ✓ | | ✓ |
| NEPTUNE MUTUAL | Association | Optimistic oracle | Open source | Fenbushi Capital, Coinbase Ventures, GBV Capital+ 30 others | ✓ | | | ✓ | | | |
| InsureDAO | DAO | Expert panel | Open source | NGC Ventures, OSAZ, LD Capital, + unknown number of others | ✓ | | | | ✓ | | |
| ease | DAO | Community vote | Open source | Collider Ventures, Delphi Ventures, DeFiance Capital+unknown others | ✓ | ✓ | ✓ | | | | |

opencover

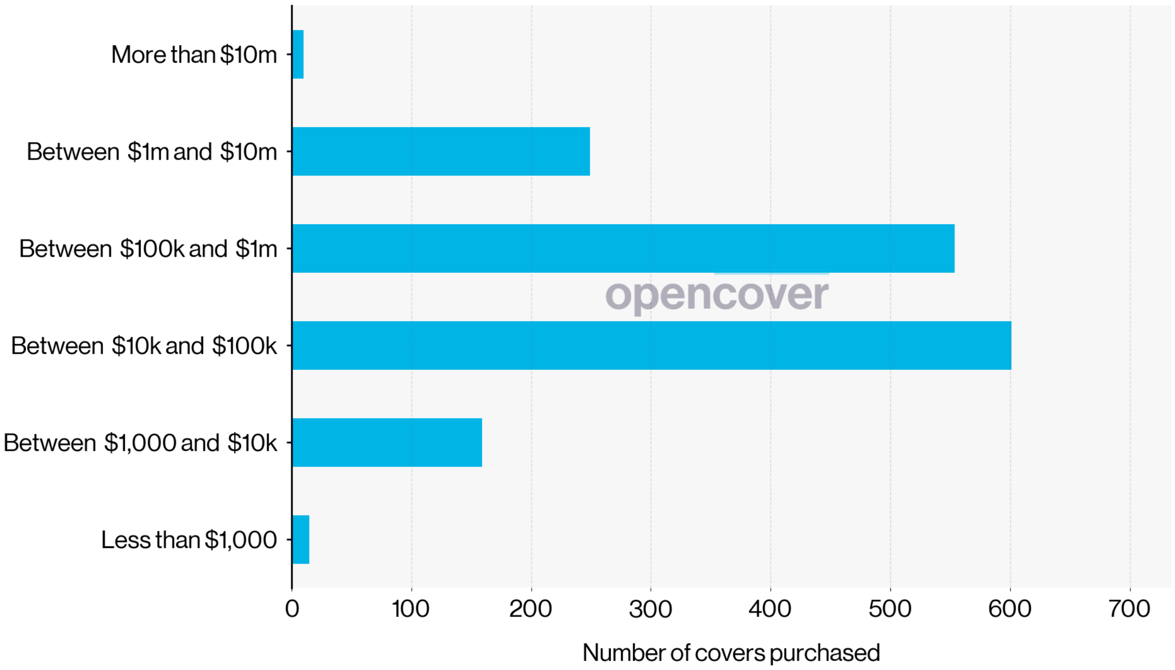
## 4.2 Cover Buyer Profiles

To better understand recent DeFi cover buyer profiles, data was compiled from all 2022 Nexus Mutual cover purchases on Ethereum and all 2022 InsurAce cover purchases on Polygon and BSC where transaction costs are typically 10 to 100x lower.

For Nexus Mutual, the median and mean cover amounts purchased in 2022 hover around $100,000 and $750,000 respectively indicating that sophisticated DeFi users are the primary cover purchasers with little retail activity (cover amount above $10,000 in roughly 90% of purchases). This is likely due to the higher cover purchase transaction costs on Ethereum compared to other chains (~500,000 gas on Nexus Mutual V1 or ~$40 at a 40 Gwei gas price and ETH at $1,600).

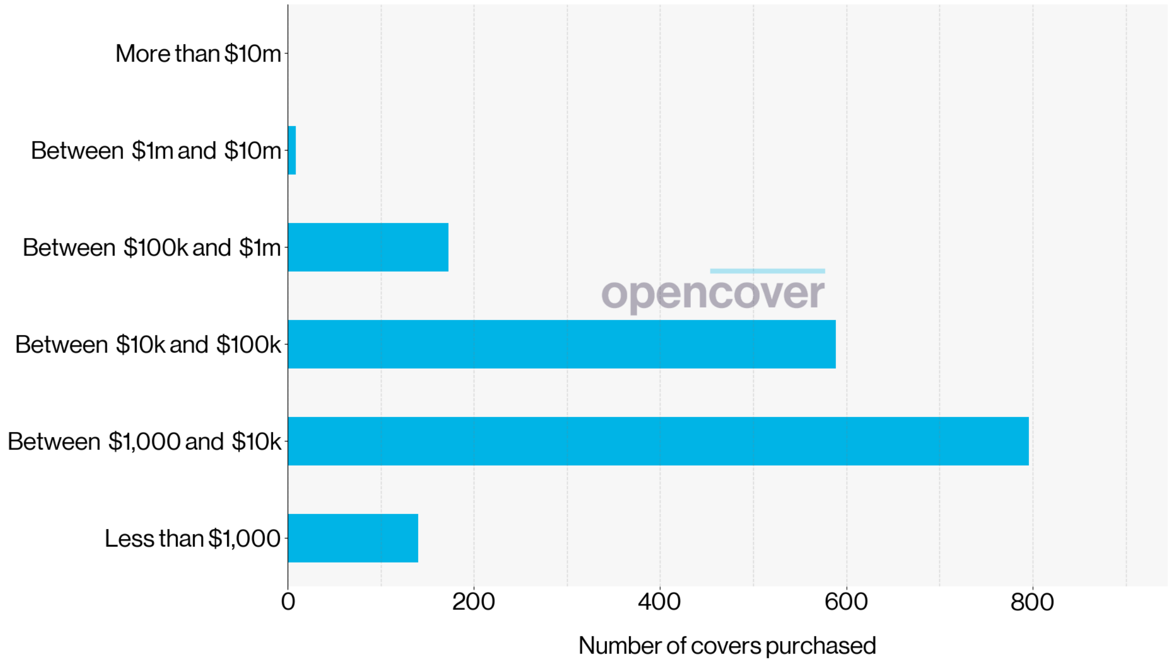
The InsurAce cover purchase data on Polygon and BSC show that approximately 50% of purchases were for cover amounts below $10,000 in 2022 indicating more retail adoption on lower cost chains. In 2022, the median and mean cover amounts purchased were around $9,000 and $52,000 on Polygon, and $10,000 and $50,000 on BSC.

**Nexus Mutual cover protection amount distribution 2022**



Source: OpenCover

### InsurAce cover protection amount distribution BSC and Polygon 2022



Source: OpenCover

While wallet labeling services did not give a comprehensive view on the identity of large cover buyers, a sample of these sophisticated users indicated profiles such as DAOs and protocol development teams, as well as market makers, hedge funds and high-net-worth individuals.

> *From the perspective of a regulated insurer for Web3 we see institutions are more careful when choosing which projects they deploy capital in, as opposed to aping in obscure projects because they promise a high APY. Institutions are demanding proper security audits from their projects of interest as well as regulated crypto insurance that is backed and reinsured by traditional insurance players. In the past few months, we have seen this as an increasing trend and we're hoping that this will lead to mass adoption of Web3 by offering consumers more confidence in the products offered by this industry.*

**Sebastian Banescu** @banescusebi
CEO at **Chainproof**

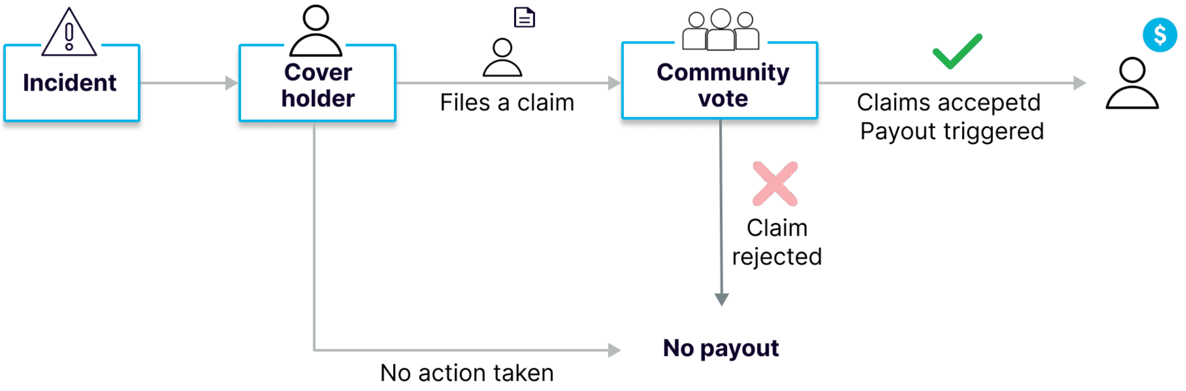
# 5 Cover Mechanics

DeFi cover providers typically differentiate themselves across 3 dimensions: their claims assessment process, risk management and the source of underwriting capital.

## 5.1 Claims Assessment

Claims assessment is the process used to determine the validity of claims submitted by cover holders. These can be categorized into: community vote, parametric, optimistic oracle, expert panel and hybrid. It is important to note that while the claims assessment process for given providers might fall into the same category, the way in which incentives are aligned between claimants and claims assessors typically differ.

### 5.1.1 Community Vote Claims Assessment

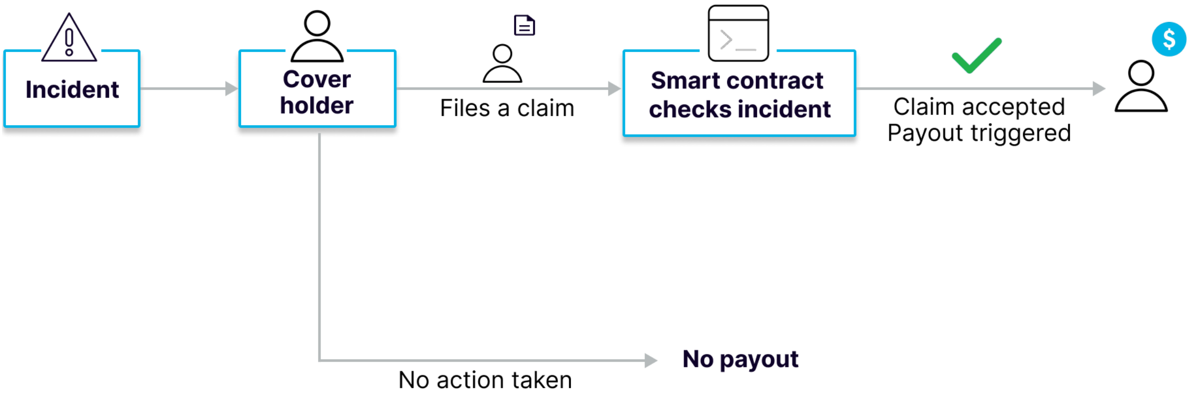


A community vote based claims assessment process typically involves DAO community members who hold protocol governance tokens. While some claims assessment processes include the publication of an internal opinion before voting starts (e.g. advisory board recommendation), community voters ultimately determine at their discretion whether a submitted claim, or group of claims, should be paid out following the associated cover policy wording.

This is akin to traditional discretionary mutuals, but unlike the time-proven model, community members are pseudonymous. For this reason, on-chain voting mechanisms to determine claim validity are designed to incentivize a community to pay out valid claims while making it prohibitively expensive to rig votes. This is typically done by rewarding participation in claim assessment to diversify the voter base and penalizing voters who vote not to pay out claims determined valid by the majority.

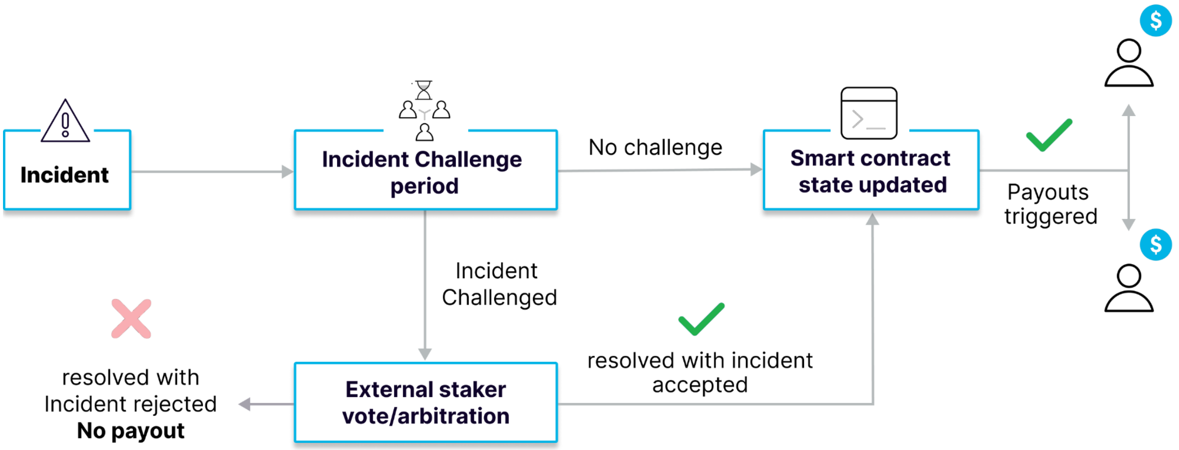
OpenCover data indicates that claim payouts using a community vote approach typically occur within 6–16 calendar days from submission. In case cover holders are dissatisfied with the outcome, providers typically allow resubmission of claims with added evidence.

### 5.1.2 Parametric Claims Assessment



A parametric cover assessment process allows affected cover holders to claim payouts automatically when a predetermined on-chain condition is met as reported by an oracle (e.g. Chainlink). Unlike a community vote claims assessment, cover holders do not have to submit proofs of loss or wait for the result of a vote so that payouts of covered incidents can happen within blocks of the trigger condition. So far, parametric approaches have mostly been used for depeg cover as the payout condition can be measured objectively.

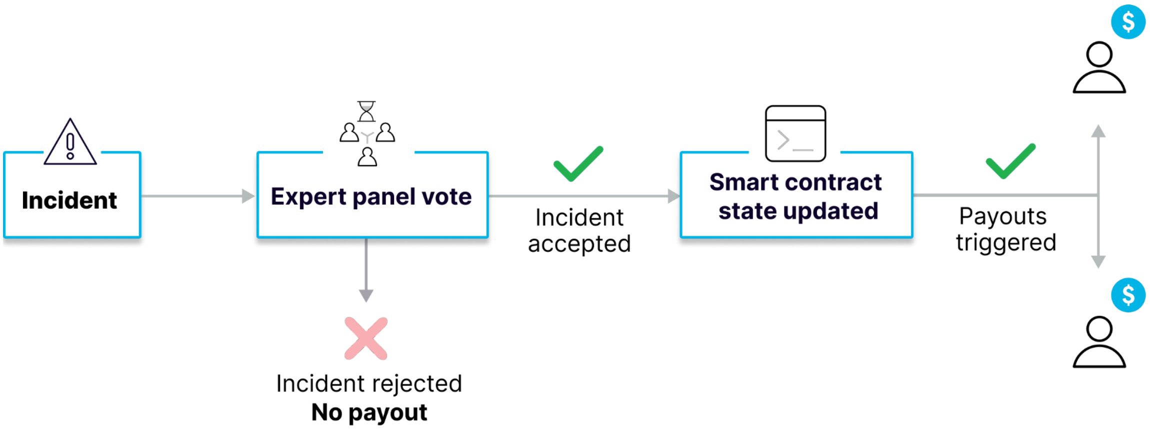
### 5.1.3 Optimistic Oracle Claims Assessment


Incident
Incident Challenge period
No challenge
Smart contract state updated
Payouts triggered
$
$
Incident Challenged
External staker vote/arbitration
resolved with incident accepted
resolved with Incident rejected
No payout

An optimistic oracle claim assessment process combines mechanics of community vote and parametric approaches by including some human supervision in the claims process without relying on a cohesive community. In this approach claims are accepted as valid unless disputed by any one party during a given timeframe.

Claims undisputed during the timeframe, or disputed but resolved as valid, are made automatically payable similarly to a parametric claims assessment. Economic incentives are used to make it prohibitively expensive to dispute valid claims. This semi-automated approach can result in a faster claims assessment compared to a community vote. OpenCover data indicates that valid claim payouts using a hybrid claims assessment typically takes 3–8 calendar days from the associated incident occurring.

### 5.1.4 Expert Panel Claims Assessment



An expert panel claims assessment process relies on a predetermined group of experts to determine whether a (group) claim is valid. Typically, the panel is composed of security and legal experts as well as protocol core contributors and community representatives where applicable. Members of the panel may be internal to the company/protocol or external for neutrality. A common practice is to leverage a multisig contract which requires a majority vote (signatures) to either approve or reject an incident and triggers the corresponding payout. OpenCover data indicates that valid claim payouts using an expert panel claims assessment typically takes 3–14 calendar days from the associated incident occurring.

### 5.1.5 Hybrid Claims Assessment

A hybrid claims assessment process combines elements from other claims assessment approaches methods. For instance, a claim may first undergo a community vote and then be evaluated by an expert panel for review before payout. Alternatively, the claim may be evaluated by an expert panel and if there is a dispute, it can be resolved by an optimistic oracle. The time it takes for a valid claim to be paid under a hybrid regime can vary depending on the combination of assessment methods.

> *The vast majority of digital assets are unprotected. Compare this with insurance adoption in TradFi and you can easily see that the DeFi insurance space has huge potential to grow and contribute to better protection for users in the DeFi, CeFi, and Metaverse ecosystems.*
>
> *In a word, the challenge for DeFi Insurance is 'scale'. DeFi insurance protocols that have been designed to scale, both in terms of their appeal to liquidity providers and in terms of their effectiveness at paying out policyholders after an incident (i.e., quickly and reliably), should look forward to rapid growth.*

**Edward Ryal** @edward_ryall
Co-founder at **Neptune Mutual**

## 5.2 Risk Management

Traditional insurance providers can be benchmarked using their loss ratio, the ratio of losses (paid insurance claims and adjustment expenses) to premiums earned. In the realm of DeFi cover, loss ratios are generally driven by the risks providers choose to cover and the associated pricing.

### 5.2.1 Cover Selection

Cover listing opportunities and requests by third-party protocols/companies are typically evaluated by a predetermined panel of experts overseeing a cover provider's listing process. For instance, providers usually include the following in their analysis when deciding whether to offer cover for a given protocol:

- Total Value Locked (TVL) and historical protocol usage.
- Whether protocol contracts are open source and software development best practices are being followed.

- Recency of smart contract audits and quality of the auditors.
- The team's publicness and background.

### 5.2.2 Cover Pricing

Pricing risk is still a major challenge for DeFi cover providers given the novelty of the risks as well as the relative lack of historical incident and claim data (OpenCover has tracked approximately 500 claims across a 90% sample of the on-chain providers since the first provider going live on mainnet in May 2019).

While the industry is still in price discovery mode, the typical approach is to leverage supply and demand (low capacity cover becomes increasingly expensive to incentivize underwriting capital providers to supply more capital) and/or an internal risk model. For instance, Nexus Mutual V2 uses a dutch auction mechanism together with a cover price floor (target price) to determine the current cover fee based on demand while Risk Harbor combines demand with an internal risk model taking into account the expected loss of the cover product in relation to their entire cover portfolio to set cover fees. Notably Ease, foregoes a pricing model entirely by equally sharing risk (payouts) across all cover holders in case of an incident.

> *Insurance is one of the most important parts of traditional finance and it is no different in decentralized finance. The cover industry is likely the single biggest sleeping giant in all of DeFi. Within the next few years, DeFi will gain in popularity among non-crypto retail and traditional institutional investors. Therefore, the number of risk-averse participants will explode and demand coverage to match.*
>
> *Now that the industry has discovered better methods of distribution and ways to increase coverage capacity we will experience exponential growth. Ease offers the most practical way to scale coverage, while being a user-friendly and economical entry point for newcomers.*

**Robert Forster** @RobertMCForster
Co-founder and CEO at **Ease**

## 5.3 Underwriting Capital

A DeFi cover provider's underwriting capital pool refers to the funds available to pay out valid claims. This capital pool is typically composed of:

- Cover purchase fees paid by cover holders (premiums in traditional insurance).
- Institutional and retail investments where investors provide underwriting capital in exchange for a share of cover purchase fees (with the risk of a net loss depending on the value of claims paid out over the investment period).
- Returns from investment of funds in the underwriting capital pool.

Depending on the provider, underwriting capital is kept in free-floating cryptocurrencies such as ETH, stablecoins (or fiat for regulated providers) or a combination of both.

The total amount covered by DeFi cover providers at any given time, i.e. active cover amount, is designed to be greater than the size of their underwriting capital pool with the leverage parameters varying across providers. In the last 9 months, the mean daily leverage ratio of active cover amount to underwriting capital was 1.07x across providers tracked by OpenCover.

> *I expect a convergence of cover this year with providers operating at full tilt on all chains. By 2024 users should be able to get as much cover as they need on the chain they desire for the correct asset and risk.*

**Rupert Barksfield** @met4be4r
Project Lead at **Amulet**

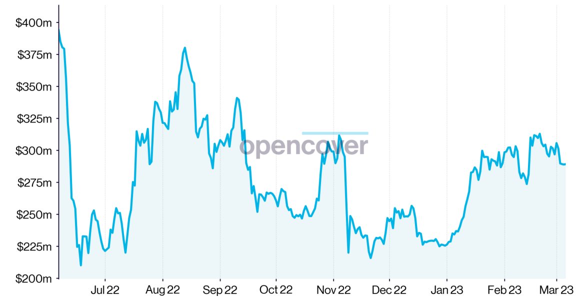
# 6 Industry Data June 2022 to March 2023

We sampled data for 9 leading DeFi cover providers[7], representing over 90% of the industry's on-chain underwriting capital, to benchmark industry dynamics in the last 9 months. The analysis focuses on underwriting capital value, active cover amount, covers sold, claims and payouts data as a proxy for industry adoption and maturity.

## 6.1 Value of Underwriting Capital

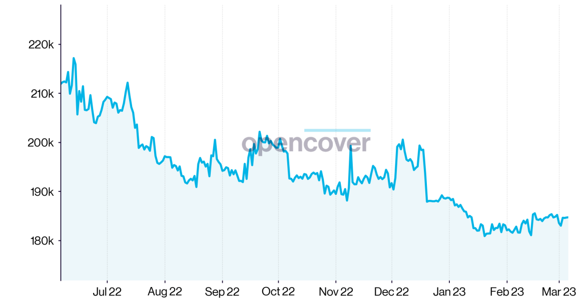
The value of a DeFi cover provider's underwriting capital pool is effectively the amount of liquidity backing active covers. It is similar to the popular Total Value Locked (TVL) metric used to compare DeFi protocols but not always equal, as raw TVL can include protocol treasury for decentralized providers for instance.

USD total value of underwriting capital across DeFi cover providers



Source: OpenCover

ETH total value of underwriting capital across DeFi cover providers



Source: OpenCover

At the time of writing, the total value of underwriting capital pools tracked by OpenCover amounts to $286 million (186k ETH) with a low of $210 million and high of $394 million in the last 9 months. The current value is 26% lower than the period maximum in USD terms.

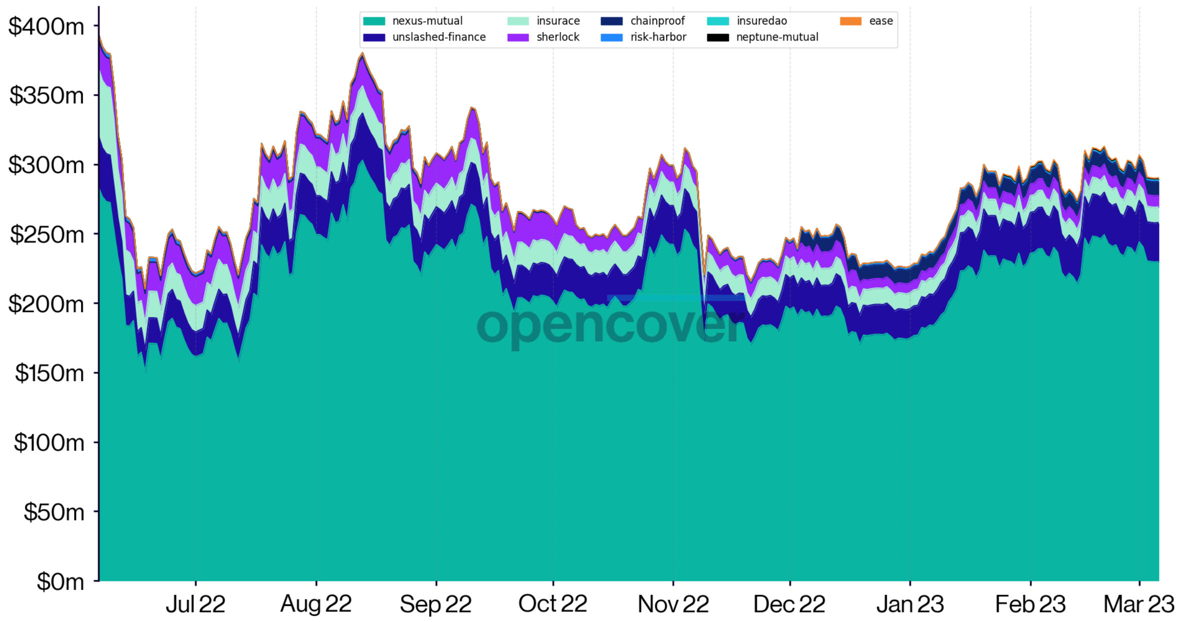
The same analysis with ETH as base currency, which minimizes changes in capital pool value resulting from fluctuations in free-floating cryptocurrency exchanges rates, indicates the current total value of underwriting capital pools is close to the 9-month minimum of 181k ETH but only 14% lower than the period maximum of 217k ETH.

This indicates a slight decrease in underwriting capacity although less pronounced than the dollar value could lead to believe. The breakdown of underwriting capital on a per-provider

[7] Nexus Mutual, Unslashed Finance, InsurAce, Chainproof, Sherlock, Neptune Mutual, InsureDAO, Risk Harbor and Ease

basis indicates that Nexus Mutual held its historical dominance throughout the period with a dominance hovering around 80% of total underwriting capital.

Total value of underwriting capital across DeFi cover providers

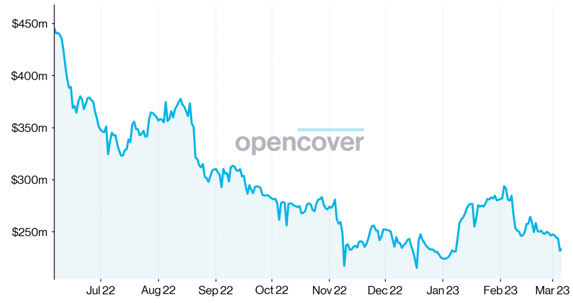


Source: OpenCover

## 6.2 Active Cover Amount (ACA)

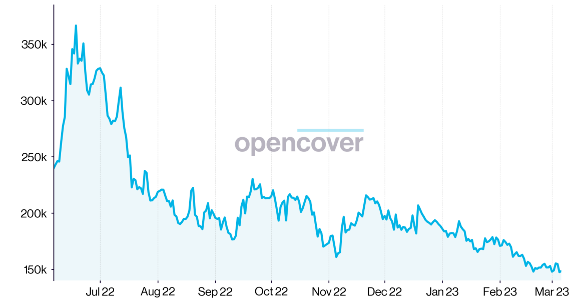
Active Cover Amount (ACA) denotes the total value a provider is liable for at any given time. In other words, the amount to be paid out to active cover holders if they all entered a claims process and all claims were determined to be valid. The cross-provider ACA stands at $231 million or 151k ETH at the time of writing, representing merely 0.5% of the $48 billion locked in DeFi. In the last 9 months, the ACA fluctuated between $220 million and $450 million or 150k and 370k in ETH terms.

USD total value of active cover amount across DeFi cover providers



Source: OpenCover

ETH total value of active cover amount across DeFi cover providers



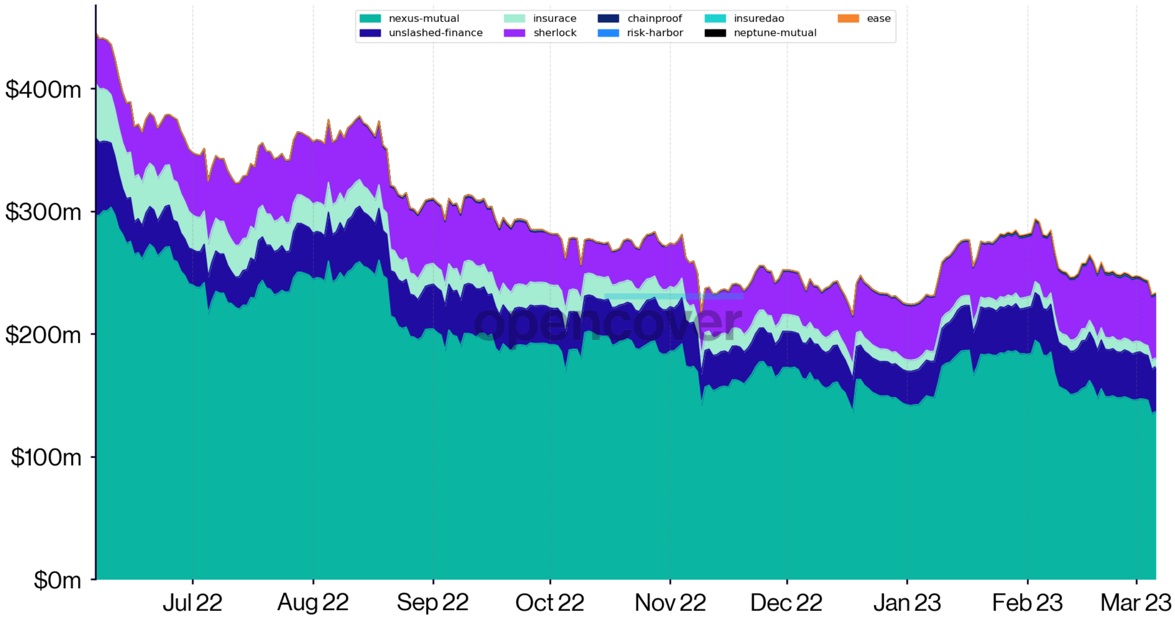
Source: OpenCover

The cross-provider ACA is a proxy for cover adoption and in this case both the USD and ETH denominated charts show the same trend, a declining trend in active cover amount in the last 9 months down 44% and 58% in USD and ETH terms respectively from their June maxima over the period.

This declining trend is due to the expiration of previously held covers together with a decrease in the purchase of new covers in line with the overall decrease in DeFi activity in the last 9 months (DeFi TVL dropped approximately 37% between June 2022 and March 2023). The USD denominated ACA increase around the turn of the year is attributed to the January cryptocurrency rally while the overall disproportionate decrease in total active cover amount is hypothesized to come from larger cover purchasers e.g. institutions withdrawing from DeFi following recent events.

The breakdown of the total ACA on a per-provider basis shows that Nexus Mutual underwrote approximately 65% of the active cover amount on the period with Sherlock and Unslashed following with 15% and 12% respectively.

### Total Active Cover Amount across DeFi cover providers

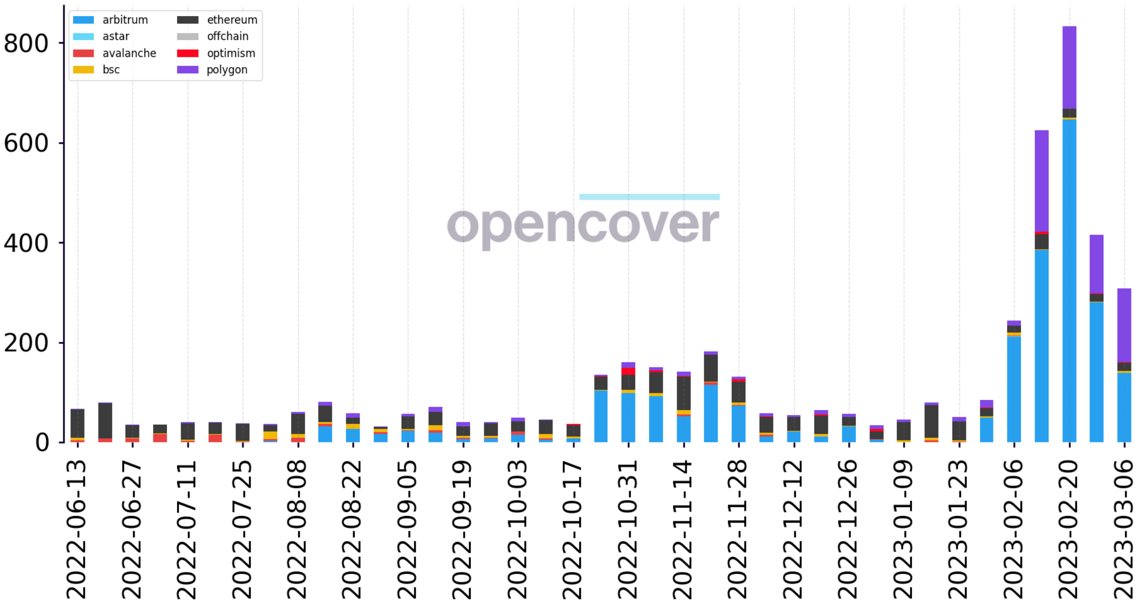


Source: OpenCover

## 6.3 Covers Sold

OpenCover recorded 19,839 all-time cover purchases across tracked providers, of which 3,434 have been purchased in the last 9 months. While the data shows an increase in the number of cover purchases immediately before and after the FTX collapse (+302% covers sold compared to previous month) as well as starting February 5, 2023 (+382% covers sold compared to previous month), the decrease in overall active cover amount points to more, but smaller, covers being purchased recently.

**Weekly number of covers sold across DeFi cover providers**



Source: OpenCover

Specifically, the number of covers sold since Nov. 6, 2022 grew by 85% compared to the previous 4 months with the growth significantly driven by L2 airdrop speculation (e.g. Arbitrum) and incentives. Discounting outlier cover purchases on Layer 2, the effective growth figure is estimated at around 15%.

## 6.4 Cover Claims and Payouts

2022 was the first-time large-scale stress test for cover providers with unprecedented events like the UST depeg and the FTX collapse leading to a record amount of respectively $22,529,978 and $4,795,709 being paid out to cover holders.

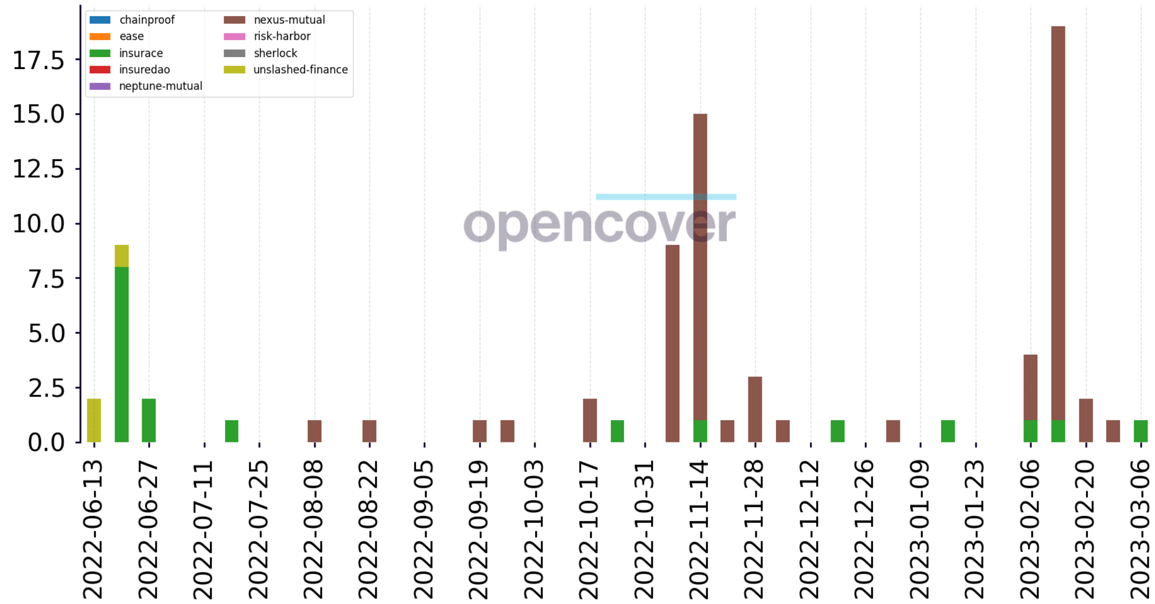
To date, OpenCover has tracked an all-time total of 552 claims filed of which 379 were paid out, totaling an aggregate dollar equivalent payout of $36,995,317 across Nexus Mutual, InsurAce, Unslashed Finance and Risk Harbor[8].

| Provider | Claims | Payouts | Payout amounts | Payout events |
|---|---|---|---|---|
| **Nexus Mutual** | 178 | 71 | $14,252,715<br>2,721 ETH + 12,326,858 DAI | bZx v1, Yearn Finance, CREAM v1,  Rari Capital, Perpetual Protocol, Bancor v3, Hodlnaut, FTX, BlockFi |
| **InsurAce** | 221 | 163 | $11,673,931<br>9,281,992 USDC + 1,753,403 USDT + 88,114 BUSD + 358 ETH + 287 BNB + 27,744 MATIC + 402 AVAX | Elephant Money, UST Depeg, FTX |
| **Unslashed Finance** | 102 | 94 | $8,641,044<br>5,429 ETH | UST Depeg, USDN Depeg |
| **Risk Harbor** | 51 | 51 | $2,427,627<br>78,443 av3CRV + 2,349,183 USDC | UST Depeg, OneUNI Depeg |

Zooming in on the last 9 months, there were 80 new claims, and 234 payouts. The reason for the higher number of payouts compared to claims is due to a large number of claims filed in the weeks before June getting paid out at once, as seen below.

[8] Excludes $197m Euler exploit of March 13, 2023, claims are being assessed at the time of writing.

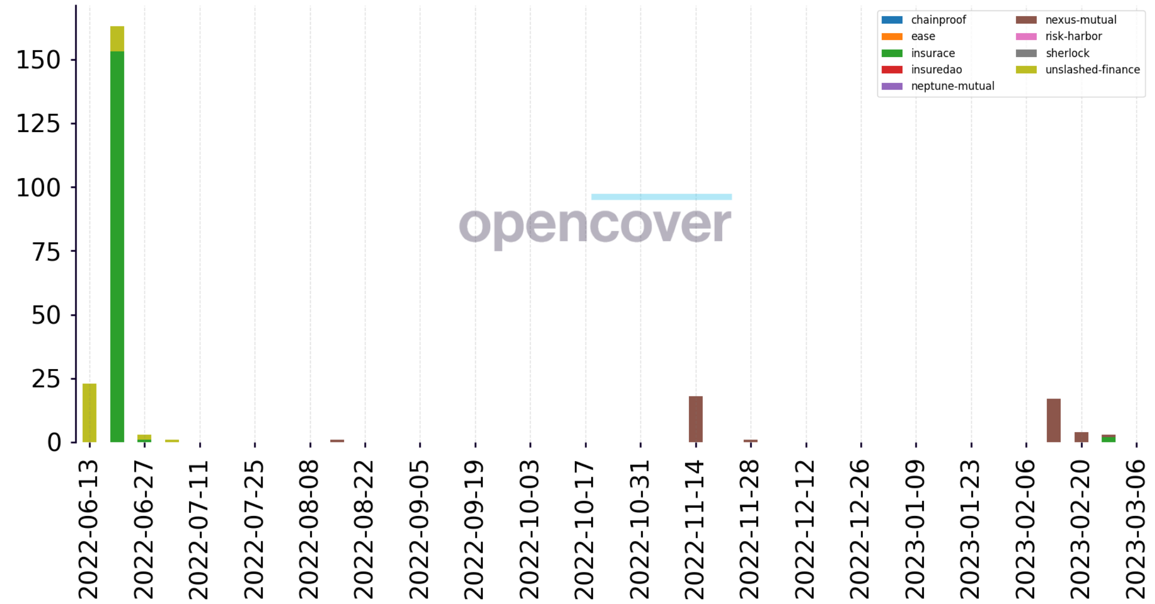
## Weekly number of claims filed across DeFi cover providers



Source: OpenCover

In the last 9 months, only three of the eight providers received claims (Nexus Mutual, InsurAce, Unslashed), these were mainly associated with the UST depeg, Hodlnaut and FTX halting withdrawals.

## Weekly number of claims paid out across DeFi cover providers



Source: OpenCover

# 7 Future Outlook

As the DeFi narrative is increasingly focusing on security, the lack of scalable DeFi cover options is a fundamental bottleneck for both retail and institutional DeFi adoption. While 2022 marked the DeFi cover industry's first stress test with 90% of all-time claim payouts occurring in the last 12 months, there is undeniable momentum from established and emergent players to tackle current challenges and seize new opportunities.

> *Unlike many predicted, during the past bull market DeFi insurance wasn't able to scale and satisfy demand. With many challenges yet to be solved, such as improving underwriting risk-reward ratios and claim processes, Solace is excited to see, and contribute, the new generation of protocol improvements this year.*

**Nikita Buzov** @0xNIKITA
Founder at **Solace**

Many established players are currently focused on protocol upgrades (e.g. Nexus Mutual V2, InsurAce V2, Risk Harbor V3) introducing new mechanisms such as marketplaces aiming to scale capacity and distribution, streamline user experience as well as share risk more effectively — laying the foundation for bridges to traditional insurance.

> *This year will be about building critical infrastructure components that make the industry more resilient to future extreme events and continue to attract traditional capital. At Carapace, we've decided to lead the charge on credit risk management — on-chain undercollateralized lending needs mature risk management solutions, data transparency and credit scoring tools to reach its full potential.*

**Rohit Sabnis** @RohitSabnis
Founder & CEO at **Carapace**

Emergent players such as Carapace, Neptune Mutual and Chainproof are exploring new DeFi opportunities such as credit default cover for on-chain undercollateralized lending, validator slashing cover with the shift to PoS blockchains and audit cover which is seemingly poised to become the norm as the ecosystem becomes increasingly security conscious.

Ultimately, scaling these innovations to a meaningful size will depend on the robustness of DeFi risk assessment frameworks — of which there are currently very few; building resilient cover protocols — for which blockchains are a evident choice of infrastructure; and devising large scale risk sharing networks akin to traditional insurance — which will likely prove to be equally challenging and vital for the DeFi (cover) industry to thrive.

# 8 Glossary

### DeFi cover

DeFi cover (sometimes informally referred to as DeFi insurance) is a catch-all term for products that protect against decentralized finance's unique risks such as protocol hacks or a stablecoin peg loss. *Traditional insurance, such as FDIC insurance, protects against financial losses that result from custodian mismanagement, while decentralized finance inherently protects against custodian risks because users retain sole control of their funds and transactions happen on public distributed ledgers (blockchains). As a result, the main risks in DeFi unique and DeFi cover products were developed to protect against these.*

### DeFi cover provider

A DeFi cover provider is typically itself a DeFi protocol but can also be a company. The former often use smart contracts to automate the process of providing coverage, and typically allow users to purchase coverage directly from the protocol through a user interface (UI). DeFi cover protocols usually operate as a DAO, meaning the service is governed by holders of the associated protocol token(s).

### DeFi cover policy

A DeFi cover policy is a document or statement that outlines the payout conditions for a given cover product. Unlike traditional insurance, cover policies are typically not legally binding and can involve community voting as part of claim assessment.

### Claim

A claim is a request for payment made by a cover policyholder in the event that a covered event occurs, such as a smart contract exploit. A claim typically includes information about the event and any supporting documentation such as proof of asset ownership and/or proof of loss.

### Claim assessment

Claim assessment refers to the process of determining the outcome of a claim made by a cover holder. This typically involves a review of information submitted by the cover holder and other evidence to determine whether the claim is valid or not following the cover policy. The claim outcome is the final decision made after the assessment process is complete. In simple terms, it is the decision of whether to approve or reject a claim.

### Claim payout

When a claim is determined to be valid via a claim assessment process, the claim payout is the final sum received by a cover holder from the DeFi cover provider. The payout currency depends on the cover policy.

### Capital pool

A DeFi cover provider's capital pool refers to the asset owned by the provider used to pay out valid claims.

### KYC

Know Your Customer (KYC) refers to the process of collecting and verifying certain identifying information about cover purchasers such as name and government ID. Some cover providers require KYC before you can make use of their services.

### Total Value Locked (TVL)

Total Value Locked (TVL) denotes the total value of funds owned by a cover provider to underwrite covers. It is effectively the amount of liquidity backing active covers. TVL is typically held as a mix of stablecoins and free-floating cryptocurrencies with TVL size often used as a proxy for cover provider adoption.

### Active Cover Amount (ACA)

A DeFi cover provider's Active Cover Amount (ACA) is the total amount currently covered by the protocol. In other words, if all of the active covers were to be claimed and the claims were determined to be valid, the ACA represents the total amount of funds that the protocol would have to pay out to cover holders.

### Covers sold

The total number of covers that a given DeFi cover provider sold since inception.

### Claims

The total number of claims received by a DeFi cover provider since inception.

### Payouts

The total number of claims paid out by a DeFi cover provider since inception.