Decentralized Insurance Alternatives: Market Landscape, Opportunities and Challenges
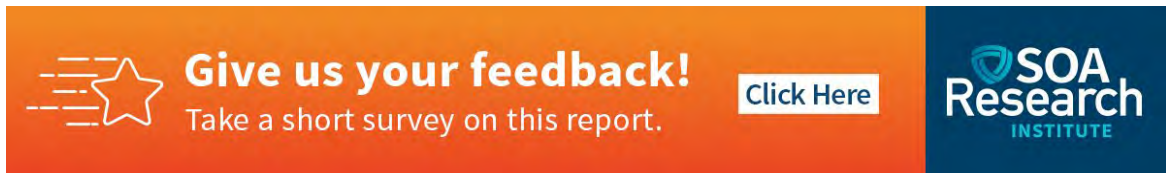
September | 2022

Actuarial
Innovation and
Technology

SOA
Research
INSTITUTE

Decentralized Insurance Alternatives: Market Landscape, Opportunities and Challenges

AUTHORS	Alvin Kwock, OneDegree	**SPONSOR**	Actuarial Innovation and Technology Strategic Research Program Steering Committee
	Erik Lie, FSA, CERA, Hailstone Lab		
	Gwen Weng, FSA, CERA, FCIA, Hailstone Lab		
	Rex Zhang, ASA, OneDegree		

Give us your feedback! Take a short survey on this report. Click Here — SOA Research Institute

CONTENTS

Decentralized Insurance Alternatives: Market Landscape, Opportunities and Challenges

Section 1: Introduction to Decentralized Insurance Alternatives

Decentralized insurance alternatives is a rapidly expanding sector of Decentralized Finance (DeFi), an emerging and growing financial ecosystem powered by blockchain technologies. Instead of aggregating risks by centralized insurance entities, these platforms enable cost-effective and scalable peer-to-peer risk sharing with new forms of decentralized business models that leverage global accessibility and transparency, self-executing smart contracts, as well as social media tools like Discord and Twitter to coordinate community decision-making to support operations.

Since these platforms operate on blockchains, financial transactions such as payments of premiums and claims and provision of capital are all settled with cryptocurrencies. Users can obtain instant quotes of premiums and buy coverages through web portals offered by the platforms. The process of purchasing a coverage is similar to performing other on-chain transactions in the DeFi ecosystem: Users need to sign transactions with their on-chain wallets to pay premiums. They would also receive any claim payments in their wallets.

The purpose of this report is to review and discuss the business models and operating designs of decentralized insurance alternatives, which may have significant implications for traditional insurance businesses, as well as the actuarial profession. Most decentralized insurance alternatives focus on developing products that cover unique risk events in the DeFi ecosystem, such as smart contract exploits and de-pegging of stablecoins. These products are the focus of this paper.

There are also other types of decentralized insurance or blockchain-based models, such as:

- Blockchain-based solution offering coverages for off-chain risks, such as parametric flight delay or weather risk. Example: Etherisc, Fizzy by AXA
- Blockchain-based solution to serve a piece of the traditional value chain, such as using smart contracts to automate claim processing or an on-chain process to manage the insurance-reinsurance or broker-reinsurance relationship (e.g. B3i, Nayms)
- Decentralized insurance model without the use of blockchain or smart contract technologies, such as P2P insurance, takaful and mutual aids.

These are not the focus of this paper.

1.1 DEFI RISKS

The DeFi ecosystem has been expanding rapidly in the past few years, growing from less than USD $1 billion in 2020 to USD $61.6 billion as of June 2022 as measured by Total Value Locked (TVL)[1], the amount of crypto asset deposited in the DeFi protocols.

With continuous innovation in product design and delivery, the potential of DeFi adoption is massive. However, the rise of DeFi is marred by security issues. Nearly 200 blockchain hacking incidents have taken place in 2021 with

---

[1] The TVL is a commonly used growth metric in DeFi.

approximately USD $7 billion in stolen funds (Cointelegraph, 2021). These hacking events have a wide range of causes including, but not limited to, the following:

- Smart contract vulnerabilities exploited by hackers to steal funds
- Manipulation of oracles to cause price feed deviation
- Attack on governance where a small group of individuals took over the protocol's governance decision-making mechanism

Another key risk faced by the DeFi ecosystem is stablecoin de-pegging. Stablecoins, especially those that are pegged to fiat (i.e., USD), play an important role for the entire DeFi ecosystem as they are widely used due to their low volatility. There are stablecoins (i.e., USDT, USDC) issued by centralized institutions, stablecoins (i.e., DAI) issued by decentralized protocol and algorithmic stablecoin (i.e., UST), for which the peg is maintained by an algorithm. Stablecoin de-pegging could happen due to a variety of risks depending on each stablecoin's design (Kalges-Mundt, Harz, Gudgeon, Liu, & Minca, 2020). A renowned example of a stablecoin de-pegging event is the UST de-pegging in May 2022, causing billions of direct and consequential losses (CoinDesk, 2022).

For these new and complex DeFi risks, experience data availability and underwriting expertise are both limited. Despite the high demand for insurance, traditional insurers hesitate to supply the relevant coverage. Decentralized insurance protocols are designed to fill the void. They provide insurance solutions to protect policyholders against the risks associated with DeFi protocols using a decentralized business model without a centralized insurer making the underwriting and claim decisions. In addition to standalone protocol risks, these platforms also started to offer more advanced and comprehensive coverages against more sophisticated events such as cross-chain exploits.

1.2 MARKET LANDSCAPE

As of June 2022, the decentralized insurance sector in DeFi has a joint total of USD $601.43[2] million in TVL. By this measure, the insurance sector is relatively small, compared to other sectors in DeFi, such as decentralized exchanges (USD $26.43 billion in TVL) and lending markets (USD $17.42 billion in TVL). The adoption of DeFi insurance is poised to grow with the rest of the DeFi ecosystem as users seek risk mitigation solutions.

The DeFi insurance sector is dominated by two protocols: Nexus Mutual, the pioneer in the space since 2018, and Armor Finance, a distributor of covers underwritten by Nexus Mutual. Combined, they make up over 80% of the insurance sector market share as measured by the TVL. The rest of the market stays fragmented, with only Unslashed Finance, InsurAce and Sherlock holding more than 4% of the market share.

---

[2] The TVL figures in this paper are also extracted from DeFi Llama, dated Aug 19th,2022. Please note that TVL figures fluctuate a lot along with high cryptocurrency price volatility.

Figure 1
MARKET SHARE OF TOP INSURANCE PROTOCOLS (IN TERMS OF TVL)

Market Share (in TVL)

Sherlock 3%
Risk Harbor 2%
Others 2%
InsurAce 3%
Unslashed Finance 5%

Armor 44%

Nexus Mutual 41%

Legend:
- Armor
- Nexus Mutual
- Unslashed Finance
- InsurAce
- Sherlock
- Risk Harbor
- Others
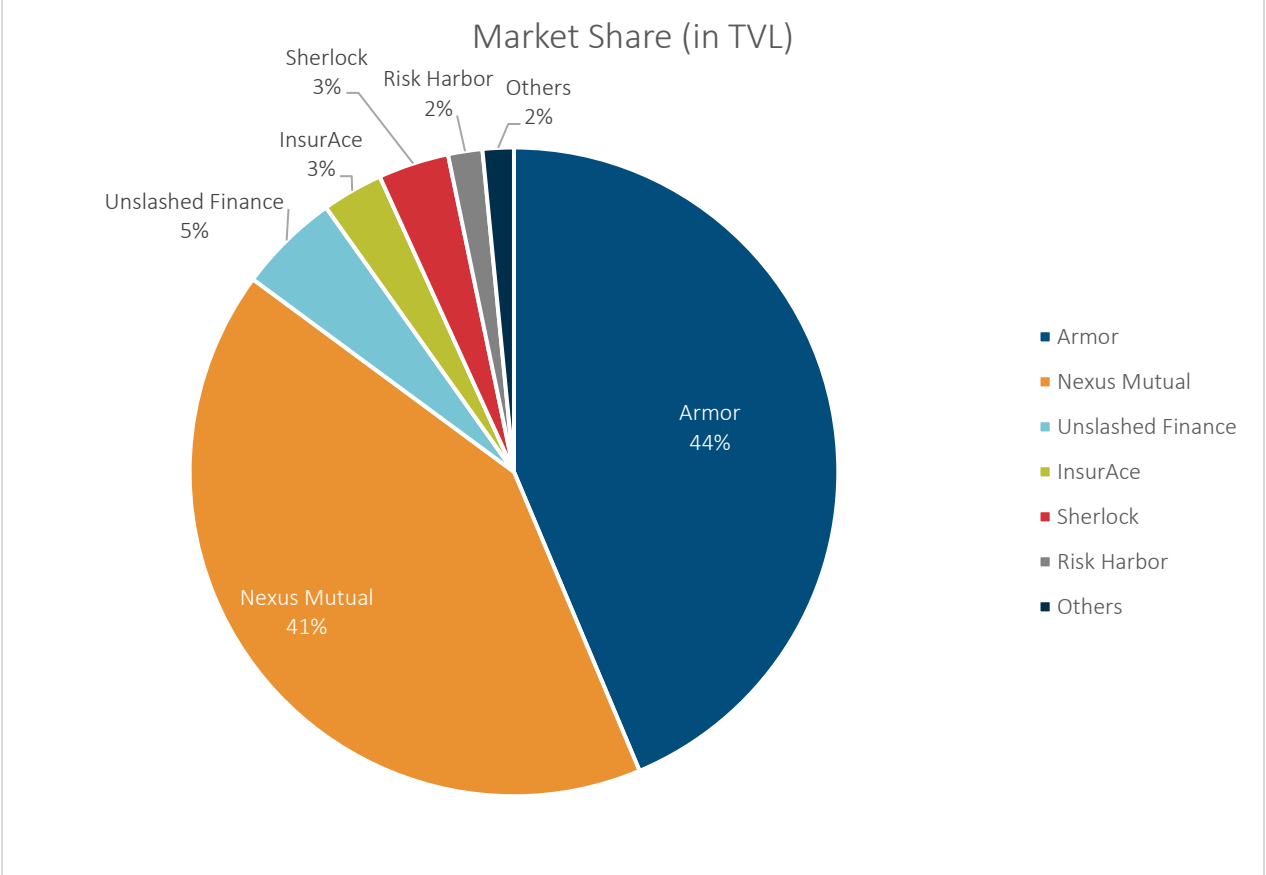
The table below shows more details of the leading protocols:

Table 1
LEADING PROTOCOLS

Protocol	Blockchain	Description	Founding Year	TVL (in Million USD)	Market Share (in TVL)	Token	Market Cap (in Million USD)
Armor[3]	Ethereum	A decentralized brokerage for coverage underwritten by Nexus Mutual	2021	262.65	43.67%	$ARMOR	1.57
Nexus Mutual	Ethereum	A decentralized alternative to insurance that covers smart contract failure and exchange hacks	2018	249.26	41.44%	$NXM	266.65
Unslashed Finance	Ethereum	Decentralized insurance for major DeFi protocols	2021	30.36	5.05%	$USF	1.12
Sherlock	Ethereum	A risk management protocol that has a decentralized smart contract security team to bring affordable coverage to DeFi.	2021	21.21	3.53%	$SHER	Not Available
InsurAce	Ethereum, Polygon, Avalanche, Binance Smart Chain	A multi-chain decentralized insurance protocol, similar to Nexus Mutual. Offer cross-chain portfolio-based covers.	2021	18.32	3.05%	$INSUR	4.59
Risk Harbor	Ethereum, Arbitrum, Terra	A risk management marketplace for decentralized finance (DeFi) that uses a completely automated, transparent, and impartial invariant detection mechanism to secure liquidity providers and stakers against smart contract risks, hacks, and attacks.	2021	10.28	1.71%	N/A	Not Available

---

[3] Armor.FI was rebranded to ease.org at the end of May 2022

Most decentralized insurance solutions operate on Ethereum as it is the largest blockchain with over 60% market share in terms of TVL across all blockchains that support smart contracts. Nexus Mutual, the largest decentralized insurance solution provider, founded in 2018, focused on its development on Ethereum. Newer solutions, such as InsurAce and Risk Harbor, launched in 2021, have expanded their footprints to other chains with growing activities. Unslashed Finance and Sherlock are different from the other protocols as they sell bulk insurance coverage to institutional players or other DeFi protocols.

Section 2: Decentralized Insurance Models

This section discusses the existing designs of the major decentralized insurance protocols from the following aspects:

- Product Design
- Underwriting and Pricing
- Claim Assessment
- Legal and Compliance
- Distribution Model
- Governance
- Capital Modeling and Management

2.1 MODEL OVERVIEW

Decentralized insurance protocols have many of the same characteristics as many other decentralized financial protocols:

PERMISSIONLESS

Everyone can take part in decentralized insurance as long as they have access to blockchains. There is no need to go through a lengthy registration process. The users just need to open an on-chain wallet and connect to the protocol to use their products and services. Just like the other DeFi protocols, a decentralized insurance protocol usually does not collect users' personal information to perform Anti-Money Laundering or Know Your Client (AML/KYC) checks. One notable exception is Nexus Mutual, which does need AML/KYC since its inception in 2018. It is, however, moving towards removing it based on a governance proposal (BraveNewDeFi, 2021).

DISINTERMEDIATION

Disintermediation happens both externally and internally. External disintermediation refers to the fact that the distribution of insurance coverage in the decentralized insurance model does not rely on any central intermediaries such as a broker or agent. They are now based more on member-to-member word-of-mouth or partnership with other protocols to build a user base and gain traction. Internal disintermediation refers to the removal of layers and layers of managerial roles to coordinate efforts across functions in a traditional insurance company. Decentralized insurance's operation and coordination efforts can be largely done by the self-motivating community and the orchestration is done by smart contracts and readily available polling tools that support community voting (i.e., Snapshot).

COMPOSABILITY

Decentralized insurance alternatives can interact with other DeFi protocols easily through smart contracts, which are like open APIs (Ethereum Org, n.d.). Developers can easily call other smart contracts to build additional functionality and extend what's possible. Therefore, a decentralized insurance protocol can leverage other decentralized services to perform key functions such as claim arbitration or investment.

DECENTRALIZATION

Governance processes and decision-making in decentralized insurance protocols are set up to be run by its members, instead of a centralized entity. Membership is proved by holding the protocol's governance token to participate in governance processes, such as voting and online discussion. Participants are only represented by their unique wallet address and are, therefore, anonymous. However, like other DeFi protocols, full decentralization can

be illusory (Aramonte, Huang, & Schrimpf, 2021). Centralization can be observed in key strategic decision-making, especially at an early stage of protocol development, in which a core team helps to develop and determine the strategic direction for the protocol. There are also unique elements of centralization found in decentralized insurance alternatives' operation aspects, such as pricing, which we will discuss in subsequent sections.

TRANSPARENCY AND IMMUTABILITY

Just like the rest of DeFi, all transactions can be viewed by anyone and cannot be changed once included in the blockchain. Such transparency is especially valuable in an insurance model because of the importance of trust needed in insurance transactions.

UNREGULATED AND NON-LICENSED

Decentralized insurance alternatives are not regulated as insurance providers yet. Their operations do not require any license or regulatory approval. Therefore, they can launch with much smaller capital investments, at a much faster pace, and with a global reach. There are also no regulatory constraints on product design, pricing, or operations, which typically results in a hotbed of both vigorous innovations and risky activities. However, it is questionable whether such an unregulated state will persist for a long time as regulators are calling for DeFi laws and regulations.

2.2 PRODUCT DESIGN

We can categorize decentralized insurance protocol's product offerings into two types: reimbursement and parametric. A reimbursement product relies on an insured to suffer the loss first and make a claim actively from the policy issuers. Claimants are often required to provide incident proof to support their claims. Parametric-type products leverage third-party data sources to detect trigger events. The claim process is coded in a smart contract such that when a pre-defined trigger event happens, claims are automatically paid out to the beneficiary's wallet. Benefit payout design decides a protocol's claim process design, which we will discuss in the 'Claim Assessment' section. In this section, we will also share some statistics on the covers provided by the key players, such as Nexus Mutual and InsurAce, to demonstrate their popularity.

REIMBURSEMENT PRODUCTS

Reimbursement products pay claims to reimburse the policyholder's financial losses caused by the covered incidents up to a specified limit. The claim amount differs case by case depending on the assessment result on the size of the loss. Compared to traditional products, reimbursement products offered by decentralized insurance protocols are simpler. Usually, they have only one overall plan limit, often referred to as the cover amount. Customers specify their desired cover amount when buying the coverage.

The benefit limits or event limits are set up in a simple way. Usually, the coverage only has a cover amount that is equivalent to the maximum possible payout. A protocol may, however, limit the maximum number of false or rejected claims that a user can submit. An example is Nexus Mutual's claim submission requiring a deposit of the protocol token, NXM, for claim submission, which will be burnt upon claim rejection. Coverage will also end if two of the policyholders' claims are rejected.

There are a variety of forms of reimbursement products. In the section below, we provide a brief explanation of each product offered by key players (Nexus Mutual and InsurAce) in this category to help readers develop a basic understanding.

- Smart contract/Protocol cover

  A smart contract cover protects policyholders against financial loss due to malicious exploits or unintended use of a smart contract of the covered protocol. Both Nexus Mutual and InsurAce have offered smart contract covers since the start of their service. In April 2021, Nexus Mutual launched "protocol covers," extending the coverage to protocol economic design failure, severe oracle failure, and governance attacks based on community governance proposal #131[4].

- Custodian / Custody cover

  Both Nexus Mutual and InsurAce offer custody cover to protect the policyholders against loss due to hacking of centralized exchanges and custodians, such as Binance, Gemini, and Coinbase. The coverage kicks in when a user loses more than 10% of their fund safekept by the covered custodian. Coverage will also kick in when the covered custodian's withdrawal facility is suspended for more than 90 days.

- Stablecoin de-pegging cover

  InsurAce provides stablecoin de-pegging coverage to protect policyholders against stablecoins (USDC, USDT, and UST[5]) moving off-peg from the 1:1 exchange rate with USD based on a time-weighted average price calculated using market data. The coverage kicks in only when the time-weighted exchange rate drops below a certain threshold. For example, for the UST de-peg cover, the threshold is USD $0.88. Nexus Mutual does not offer any cover dedicated only to covering stablecoin de-peg events. However, their yield-bearing token covers do provide relevant coverage. This is explained in the next section.

- Yield-bearing token cover

  Nexus Mutual provides yield-bearing token cover that protects the policyholders against any losses causing a yield-bearing token to de-peg from its market value of more than 10% for a continuous period of four hours or more.

  Yield-bearing tokens are tokenized proof of deposit users receive in return for depositing crypto assets into yield-framing strategies provided by DeFi protocols to earn returns. Yield farming refers to the process of using DeFi protocols to maximize returns. Some farming strategies may involve multiple protocols leveraging the composability of DeFi smart contracts. For example, a user can borrow cryptocurrency from a lending protocol and supply liquidity to a decentralized exchange to earn yields. There are protocols that automate these strategies using smart contracts. A user can deposit into these smart contracts to benefit from the automation and save gas fees. Corresponding yield-bearing tokens would be given to the user as a proof of deposit. This proof can be used to redeem the assets in the future.

---

[4] The Nexus Mutual proposal 131 (Nexus Mutual, 2021) has not only extended coverage to include oracle, economic and governance attacks, but also a couple of other changes on the coverage scope and terms (e.g., expanding coverage to chains other than Ethereum). It is passed with a 100% approval vote from both members and advisory board voting.

[5] As of Jun 26, 2022, according to coinmarketcap, USDT has the largest market cap at USD $67 billion. USDC is the 2nd largest stablecoin with a market cap of USD $56 billion. UST is de-pegged and no longer a legit stablecoin. Its market cap shrunk to USD $100 million.

Certain risk events can cause the value of the yield-bearing token to drop unexpectedly; for example, a malicious exploit of the smart contract running the yield farming strategy. The key difference between a yield-bearing token cover and a protocol cover is the scope of coverage. A protocol cover includes one specific protocol's risks. Yield-bearing token coverage may encompass multiple protocols, as well as any associated risks in one contract.

This can be better explained through a concrete example. 'Convex3CRV' is a yield-bearing token users get as a proof of deposit of stablecoins (UST, DAI and/or USDT) into the Convex3CRV staking pool. This staking pool further channels assets to a 3CRV liquidity pool on another DeFi platform named Curve Finance to earn yields. A graphical explanation of the yield-generating strategy is below:
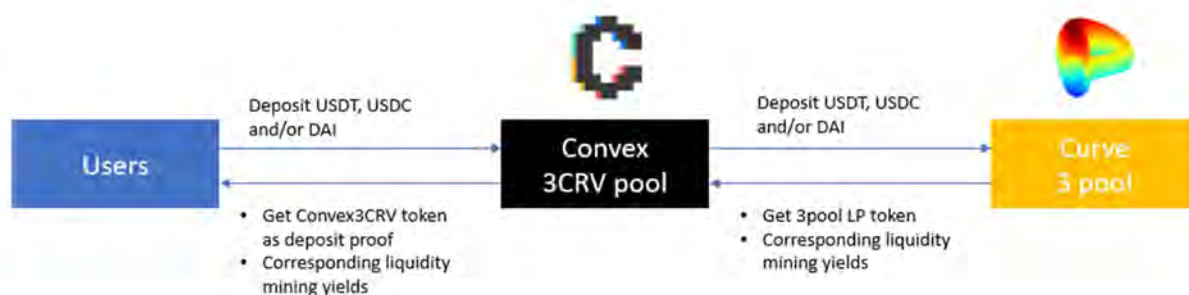
Graphical Illustration: Convex3CRV yield farming

Several risk events can cause 'Convex3CRV' to lose its peg:
1. Convex protocol gets hacked
2. Curve protocol gets hacked
3. Stablecoin USDC / USDT / DAI loses its peg

If one buys a protocol cover for Convex, cover holders get reimbursement only when event 1 above happens. After a yield token cover for the Convex3CRV is purchased, cover holders get reimbursed if any of the above risk events happen. In summary, you may consider yield-bearing token cover all-in-one protection for any protocol or stablecoin de-pegging risk the underlying yield-farming strategy is exposed to. The product saves users the hassle of buying several protocols and stablecoin covers.

One thing to note is Nexus Mutual only provides such coverage for a specified list of yield-bearing tokens issued on the three biggest DeFi protocols: Curve, Convex, and Yearn Finance. These are the leading protocols in terms of TVL in their respective sectors. They are perceived to have greater security and a limited number of incidents in the past.

To cover risks across protocols, InsurAce offers a different solution named "bundled cover." It is a bundled offering of smart contract covers over multiple protocols. However, the coverage is limited to losses due to smart contract vulnerabilities.

We have provided links to the detailed policy wording from Nexus Mutual and InsurAce in Appendix A for further reference.

PARAMETRIC PRODUCTS

Parametric insurance is a data-driven insurance product with pre-specified payouts paid automatically when a trigger event happens. In decentralized parametric insurance, insurance terms are coded into smart contracts, which pay claims automatically upon events triggered by data feeds from oracles or through algorithmic checking. The smart contract's self-executing property makes it a perfect technology to support such use cases, with terms and conditions coded and agreed upon instead of paper policy wording, while using cryptocurrencies for instant settlement.

An example of parametric DeFi insurance products is the yield-bearing token de-pegging cover offered by Risk Harbor. The protocol detects hacking events through checking invariants on-chain. An example of such an invariant is to check if the redemption rate for these yield-bearing tokens is dropping, or the Underlying-To-Claim-Ratio (Ben-Har, Patel, Su, & Resnick, 2021). The exact checking mechanism, however, differs by each covered protocol. Risk Harbor claims to have built a specific detector smart contract[6] for each protocol to help check the associated invariants to see if any hacking events happen. Any event confirmation will trigger automatic claim payout to the cover holders in USDC, a stablecoin.

However, parametric DeFi insurance development is limited due to a lack of reliable data sources. The development of a parametric product requires the presence of a reliable data oracle that can constantly feed the most real-time data stream to the smart contract. The data provided needs to be granular enough to support the trigger event identification and corresponding terms coded in the contract. Presently, on-chain data oracles are insufficient in terms of the number of oracles available and the types of data they provide, primarily cryptocurrency market prices and limited real-world information on flight delays, weather, and election outcomes.

---

[6] For more details, please refer to the section on Covered and Non-Covered Invariants under Risk Harbor docs (Risk Harbor,, 2021)

COVER STATISTICS

A key merit of decentralized insurance alternatives is transparency. All transactions can be viewed on blockchain. Nexus Mutual and InsurAce and, in addition, provide easily accessible data and dashboards. Below, we provide a sample of their cover statistics.

Figure 2
NEXUS MUTUAL WRITTEN PREMIUM (IN USD) BY QUARTER
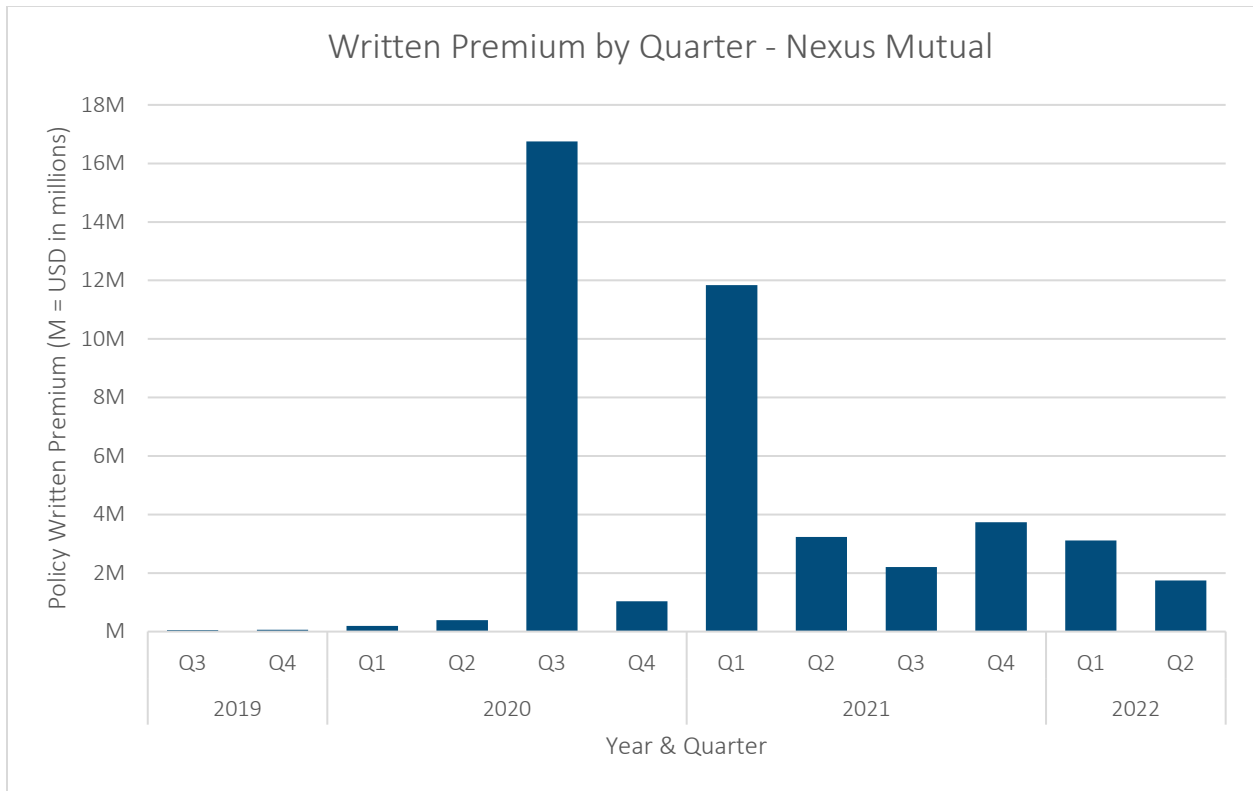
Figure 3
NEXUS MUTUAL PORTFOLIO SPLIT (SINCE 2021 OCT 21)

Portfolio Split - Nexus Mutual

- Custodian
- Protocol
- Yield Token
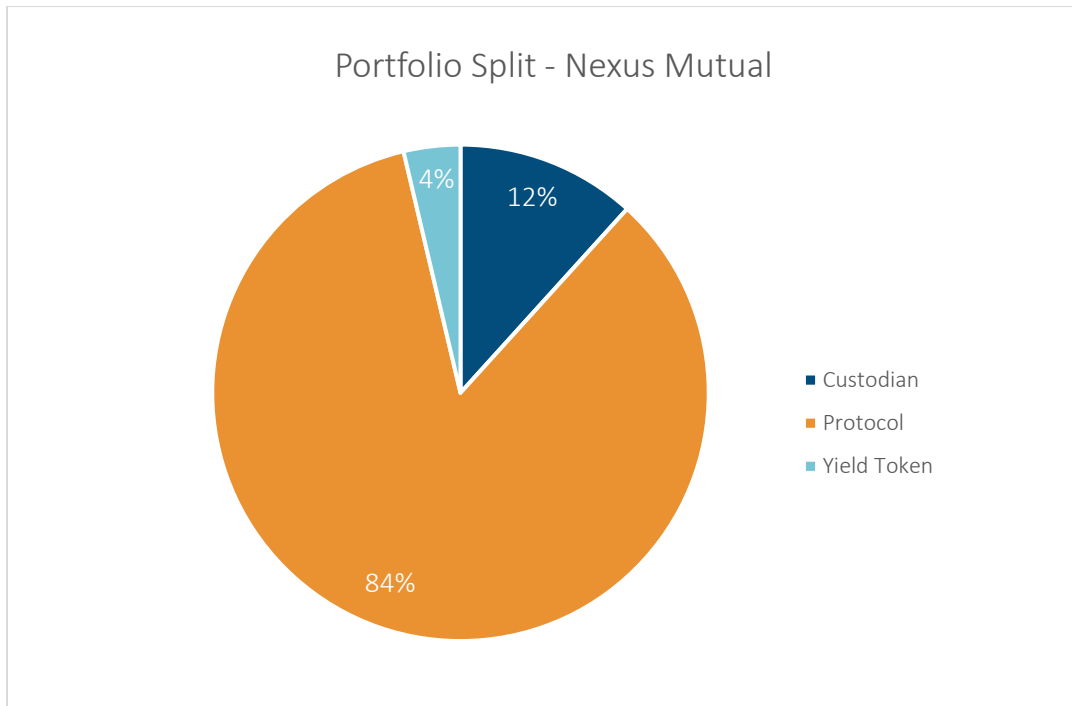
Figure 4
INSURACE WRITTEN PREMIUM (IN USD) BY QUARTER

Premium in USD by Quarter - InsurAce

Figure 5
INSURACE PORTFOLIO SPLIT BY COVER TYPE

Portofolio Split by Cover Type - InsurAce

- Bundled Cover
- Custodian Risk
- Smart Contract Vulnerability
- Stablecoin De-Peg Risk

Following are several observations from the above charts:

- Nexus Mutual's written premium has been dropping since 2021, while InsurAce's premium is rising. This may be because new insurance protocols (e.g., InsurAce, Risk Harbor) are taking market shares from existing protocols (e.g., Nexus Mutual), as they can provide more economic incentives by distributing governance tokens to users.
- A majority of both Nexus Mutual and InsurAce's portfolios is on protocol risks. Eighty-four percent of Nexus Mutual's portfolio is in protocol cover and 69% of InsurAce's portfolio is in smart contract cover.
- Yield token coverage only constitutes 4% of the portfolio in Nexus Mutual, while bundled covers occupy 20% of InsurAce's portfolio. It may be the case that the yield token coverages are too complex to appeal to most users.

2.3 UNDERWRITING AND PRICING

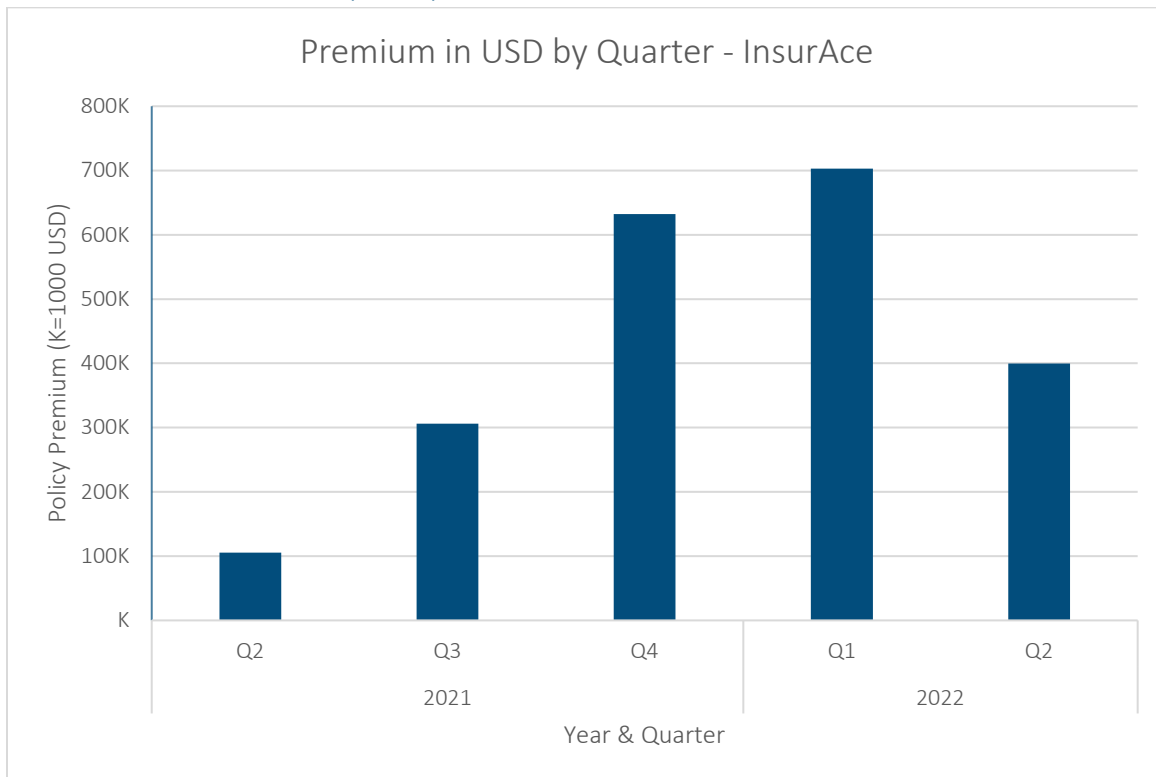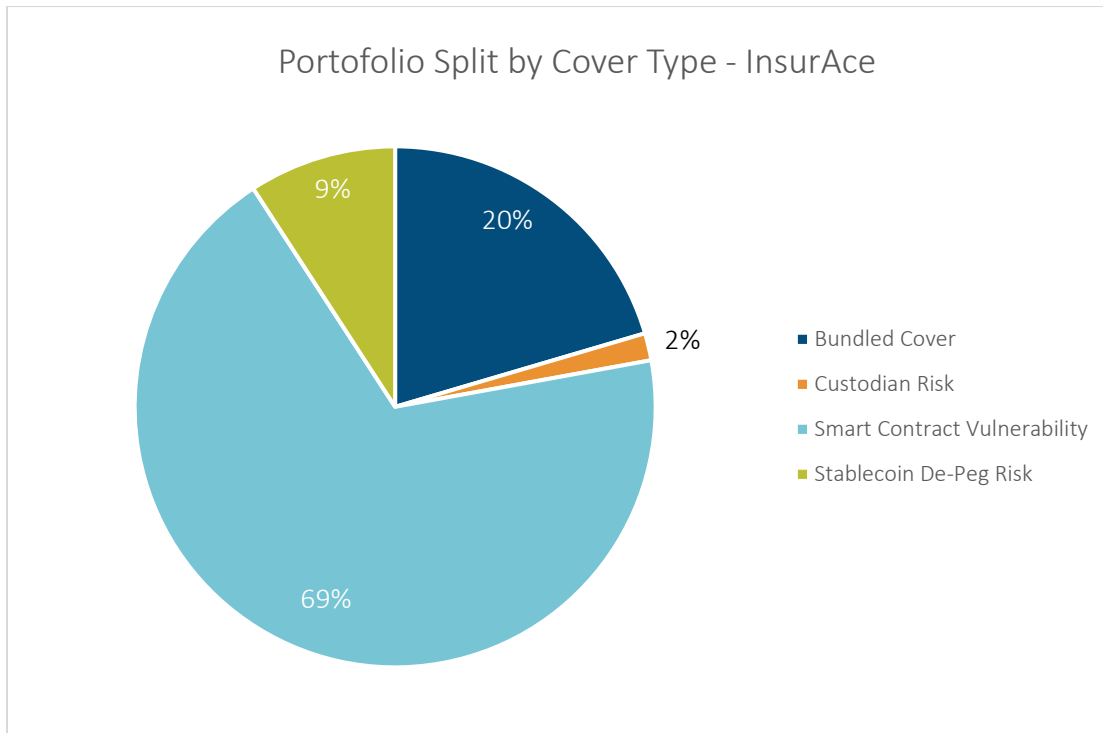By the design of their operating structure, decentralized insurance alternatives' pricing and underwriting activities are not performed by hired professionals, such as underwriters or actuaries, in a centralized manner. Instead, risk assessment is crowdsourced to individual participants.

The protocols establish a risk pool for each cover to fund the claim payout. Risk capital providers are expected to deposit funds into risk pools with a higher return relative to the level of risk. Therefore, the resulting capital allocation indicates their risk assessment. The pricing of a cover is not only determined by the amount of risk capital in the corresponding pool, but also by how many members are buying the coverage. This becomes essentially a prediction market in which people trade the outcomes of events based on their own forecast of the probability of the underlying risk event. Arguably, this can serve to forecast the true probabilities.

We take a deeper dive into this idea through Nexus Mutual's pricing methodology[7]. Nexus Mutual establishes one risk pool for each protocol, custodian, or yield-bearing token covered. Risk capital providers can stake their NXM to different pools to serve as the risk capital and earn the premium income.

The pricing formula used is as below:

$$Cover\ Price = Risk\ Cost\ \times\ (1 + Surplus\ Margin) \times \frac{Cover\ Period}{365.25} \times Cover\ Amount$$

In the formula above, the cover price is the final premium. A cover period is the length of the policy period selected by a user in terms of days. The cover amount is the policy limit input by the user. Risk cost is determined by the formula below:

$$Risk\ Cost = 1 - \left(\frac{Net\ Staked\ NXM}{Low\ risk\ cost\ limit}\right)^{\frac{1}{7}}$$

$with$:

$$Risk\ Cost\ Low\ Bound: 2\%$$
$$Risk\ Cost\ High\ Bound: 100\%$$

for which the bounds are arbitrarily set. In addition, the low-risk cost limit is also an arbitrarily set minimum amount of NXM (50,000) required to reach a low-risk cost at 2%. How such a number is set is not explicitly informed.

We can see that the only variable in the above formula is the amount of net staked NXM, which is equivalent to the total staked NXM in the risk pool net of the pending withdrawals. The larger the net staked NXM indicates a more favorable risk assessment by the risk capital providers, therefore resulting in a more favorable risk cost and lower premium for a specific risk pool. You may find in the screenshot below, the resulting risk premium varies drastically across risk pools, from 2.6% to 130%:

---

[7] Details of Nexus Mutual's pricing methodology are disclosed in the Nexus Mutual Gitbook Cover Pricing section (Nexus Mutual, Nexus Mutual Gitbook, 2018), which is public information.
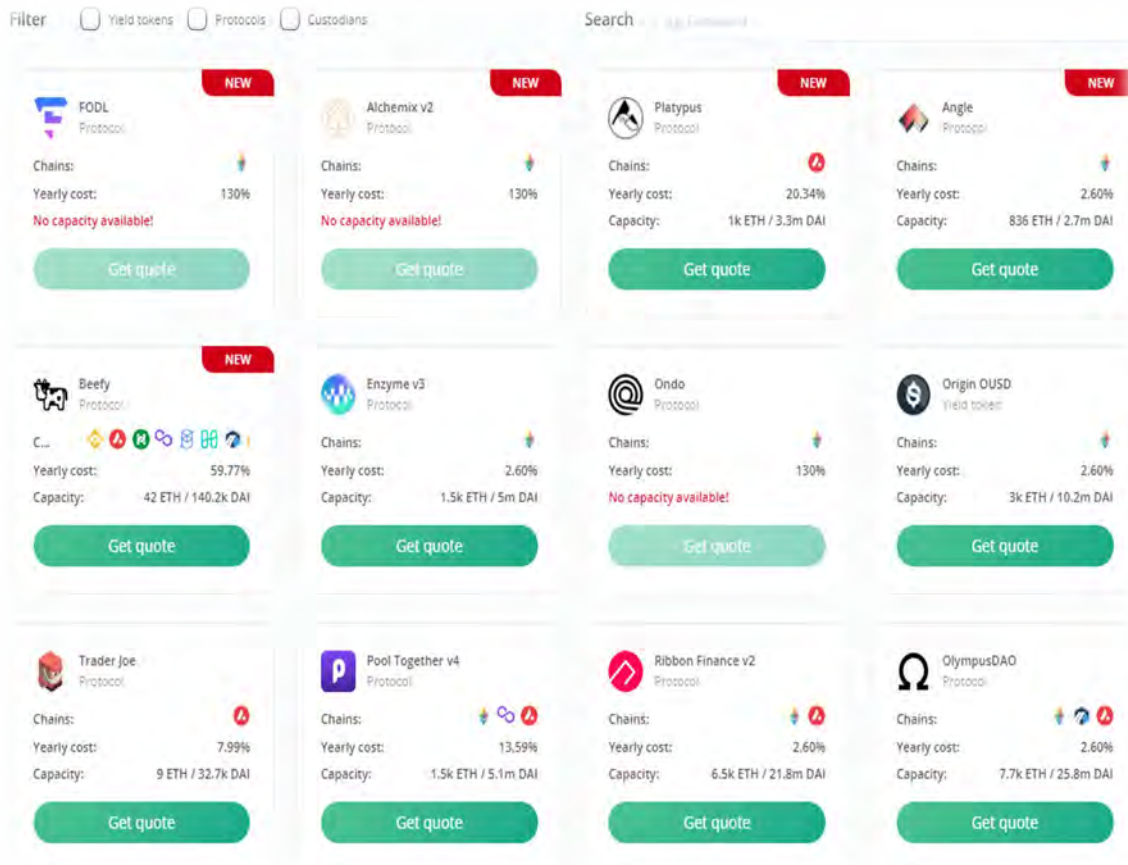
Cap screen: Nexus Mutual Buy Cover Interface

InsurAce claims to have taken one step further to use actuarial risk and loss-driven pricing models. Such a model can ideally provide a better price in the risk characteristics of the DeFi protocols compared to Nexus Mutual's. However, when we look deeper into the pricing methodology disclosed by InsurAce[8], we find that the actual premium is determined by:

1. Arbitrarily assigned minimum and maximum prices (3X the minimum price) without clearly defined methodology on how these values are determined
2. Market supply and demand for the cover that determines how the actual premium shifts between a minimum price and a maximum price[9]

In conclusion, both Nexus Mutual and InsurAce's underwriting and pricing are done through crowdsourcing individual participants' risk assessments, which is reflected by the supply (i.e., risk capital allocation) and the demand of the coverage. It functions like a risk prediction market. However, it's important to note that both protocols arbitrarily set minimum and maximum pricing levels, which makes the pricing not entirely determined by

---

[8] Details of the InsurAce pricing model can be found in the InsurAce Gitbook Pricing Models section (InsurAce, InsurAce Documentation, 2021).
[9] This is stated clearly in the section 'Dynamic Pricing" under the InsurAce Gitbook Pricing Models section. (InsurAce, InsurAce Documentation, 2021).

market demand and supply. The methodology to set these arbitrary price caps and floors is not explicitly disclosed by either protocol.

2.4 CLAIM ASSESSMENT

Decentralized insurance alternatives generally have three forms of claim assessment design: governance-based, parametric, and third-party voting.

GOVERNANCE-BASED CLAIM MECHANISM

Major protocols offering reimbursement products such as Nexus Mutual and InsurAce are implementing the governance-based design. In a governance-based design, a claim decision is made through voting either by the whole community or by a selected group of individuals within the community, who are usually referred to as the claim assessors.

Membership within the community is proven by holding the protocol token in a user's wallet. For example, for Nexus Mutual, NXM holders are eligible to vote in claim decisions. Token holders are not equivalent to policyholders as someone can hold the token without any active policies. For instance, the risk capital providers who join the capital pool also earn NXM tokens. Therefore, even though some decentralized insurance alternatives market themselves as 'Mutual,' their models are not equivalent to mutual insurance where policyholders are the sole or a majority of the members with voting power.

There are several key considerations for governance-based claim mechanism design:

Claim Investigation: DeFi incidents often require in-depth investigations of incident details, including assessment of on-chain data, to determine the nature of the incident and whether a specific claimant's wallet is affected. Ideally, there shall be a group of community members with sufficient expertise to conduct the investigation and provide sufficient information for the community to vote. In practice, a core development team behind the protocol often takes up the role of investigation under the name of Advisory Board and provides an investigation summary to the community before the voting starts. Both Nexus Mutual and InsurAce have Advisory Boards to help with claim investigation.

Fair & Just Voting: Despite the discretionary nature of governance voting, it is critical that voting results shall be fair and based on the ground truth, or the protocol risks losing its credibility. Therefore, protocols need to carefully design their voting mechanism to incentivize just voting and penalize unjust ones. For example, Nexus Mutual requires token holders to stake NXM tokens for a period to become a claim assessor. The staking requirement prevents the scenario of a member joining the voting right after making a claim. Voting against the majority will result in the claim assessor's staked token being locked for a longer period of time. Any fraudulent voting found is subject to burning of the staked NXM tokens by the Advisory Board.

To ensure fairness, it is also important to avoid voting weight domination by a single party who holds a large sum of tokens. To incentivize participation, protocols offer either tokens or premium and claim fee sharing with the claim assessors. Claim assessors can only vote during a defined voting window for each claim, usually[10] ranging from 36 to 72 hours after the claim voting starts. There are other mechanisms in place to prevent voting weight domination.

---

[10] For Nexus Mutual, the voting window lasts for a minimum of 36 hours (Nexus Mutual, Nexus Mutual Gitbook, 2018) and it ends on the earliest of:
-    Voting stakes >= 10x the cover amount
-    After 72 hours have passed
For InsurAce, the default voting window is 36 hours, subject to an extension to 72 hours if no consensus is reached (InsurAce, InsurAce Documentation, 2021)

Nexus Mutual requires a majority voting of over 70% to confirm the claim decision and the total voting weight needs to be over five times the cover amount. For example, if the cover amount is USD $1000, the staked NXM token value for voting shall exceed USD $5000 or the voting result won't be considered valid. InsurAce requires 75% of the eligible claim assessors to vote for the result to be considered valid, and voting weight of a single party is capped at 5% of the total votes.

OTHER CLAIM MECHANISMS

The governance-based design is sometimes criticized because of a fundamental misalignment of interests between token holders who vote for the claims and claimants who may suffer the financial loss. When an incident happens, only a small portion of the policyholder is affected. Therefore, we can expect that most token holders, such as the other policyholders and risk capital providers' interests, will be voting to deny the claim to avoid any payouts. There are also potential behavioral issues associated with the claim reward design that incentivizes the community to vote along with the majority instead of relying on their own judgement.

Adding to that, the process itself is heavily reliant on the manual voting effort from the token holder on the platforms. The problem of voting fatigue will arise when the voters are faced with many claims, which could lead to diminishing voting rates due to a lack of incentives for token stakers to vote. Lastly, some doubt that the governance-based claim mechanism is, in essence, centralized as the Advisory Board can hugely influence the claim decision. In that regard, new solutions have arisen to automate the claims assessment process via smart contracts.

Risk Harbor is using a parametric claim design. It argues that the parametric claim mechanism is not based on any community voting that is subject to bias and conflicting interests (Max Resnick, 2021). All the terms and conditions are coded on the smart contracts and, upon event detected, claims can be paid out automatically. Even the developers of the protocol cannot stop the payment.

Another alternative is to use a third-party voting system instead of relying on a community with conflicting interests. Unslashed Finance is the first decentralized insurance alternative leveraged on Kleros[11], a decentralized dispute resolution protocol, to help with the claim decision. Unslashed Finance argues that, since the Kleros community is independent, they can review claim evidence and policy documents in a truly fair and unbiased fashion. However, this requires trust in the third party and reduces the level of decentralization in the claim process.

---

[11] More details about the collaboration between Unslashed Finance and Kleros can be found in the Unslashed Finance Gitbook Unbiased Claim Assessment Section (Unslashed Finance,, 2021)

CLAIM STATISTICS

We analyzed claim statistics provided by Nexus Mutual from 2019 to June 2022 to assess DeFi insurance's profitability and whether the governance-based claim mechanism is working well.

Below is the portfolio loss ratio since 2019:

Year	Written Premium (in USD)	Reported Claim (in USD)	Paid Claim (in USD)	Paid Loss Ratio
2019	40,293	312,662	29,994	74.44%
2020	6,451,665	5,783,524	2,715,087	42.08%
2021	9,862,267	2,677,348	520,661	5.28%
2022 (Jan – Jun)	3,971,767	5,876,823	5,045,085	127.02%
Total	20,325,992	14,650,357	8,310,826	

The paid loss ratio showed significant volatility year over year. There are two potential reasons:

- It is common for a fast-growing block of business without much loss history
- DeFi risk claims have relatively low frequency but very high severity. Since 2019, there have been only five incidents resulting in claim payouts. The average size of the claim payout per incident was USD $1.66 million. In 2022, all the claim payouts have been a result of a single incident, the Rari Capital Fuse Market Exploit[12].

Key claim count statistics are as below:

Statistics	Count
Total no. of reported claim	119
Total no. of valid claim	68
Total no. of invalid claim	51
Total no. of accepted claim	29
Total no. of denied claim	39

---

[12] More details about the Rari Capital Fuse Market Exploit's associated claim and claim detection can be found in the Nexus Mutual Gitbook Claim History Rari Capital Fuse Market Exploit (30/04/2022) section (Nexus Mutual, Nexus Mutual Gitbook, 2018).

The total number of reported claims has been 119 since the start of 2019, out of which only 68 claims were valid ones. The others were deemed invalid for the following reasons:

- Twenty-two claims were clearly fraudulent. They were made immediately after the policy was purchased.
- Twenty-two claims were not associated with a hacking event.
- Five claims were test claims filed by members to test out the claim process.
- Two claims were filed with missing information.

The 68 valid claims resulted from 15 incidents, out of which only five were covered under a Nexus Mutual policy. Claim incident details and rejection reasons can be found in Appendix B: Nexus Mutual Claim Incident Details.

2.5 LEGAL AND COMPLIANCE

American insurers in the first half of the twentieth century argued that governments had no right to interfere with their business. Their arrangements were private, the concern only of themselves and their customers. The authorities disagreed. The insurance industry, courts at the time decreed, "…is peculiarly affected with the public interest" (IRMI, n.d.). This means that insurance is so important to the smooth running of commerce and society that governments feel obliged to step in.

This resulted in two major areas of regulatory scrutiny: licensing – that is, who can offer insurance – and capital and reserve controls – what value of assets an insurance company must maintain to cover potential claims.

These regulations, variants of which are in place across the world, present a major barrier to entry to the insurance sector. Not only must a new insurance company raise significant capital, but it must also have the full suite of expertise, processes and safeguards that are preconditions to receiving a license in any major jurisdiction.

To avoid all this, decentralized protocols tend to argue (to the extent they publish any information on their regulatory considerations) that they are not, in fact, offering insurance at all.

The starting point for such arguments is to look at the definition of insurance. This, of course, varies across jurisdictions, particularly in the U.S. where insurance is primarily regulated by states and not the federal government. The English common law test, known as the "Prudential Test"[13], is the basis for the definition of insurance in several major jurisdictions and can be expressed as follows:

> 'A contract where one party (the insurer) agrees, in return for a consideration (the premium), to indemnify or provide a benefit to the other party (the insured) if any uncertain and adverse event occurs.'

One method for protocols to claim that they are not offering insurance and are, therefore, not subject to insurance regulation is to assert that they are not even entering into contracts in the first place. This is the approach taken by parametric insurance protocols such as Etherisc. In such protocols, users stake funds into a smart contract. The smart contract automatically pays out upon the occurrence of an objectively verifiable event (for example, a delayed flight or a drought).

---

[13] From the case in which it was first applied, Prudential Insurance Company v Commissioners of Inland Revenue [1904] 2 KB 658 (Prudential Insurance Co v Inland Revenue Commissioners: 1904, 1904)

While smart contracts can be "contracts" in the legal sense, this is not necessarily the case. In common law jurisdictions such as the U.S., various elements must be present before a legally binding contract is created, including offer, acceptance and consideration. In parametric insurance, it is possible to argue that the interaction by a user with a computer program (the smart contract) does not satisfy these requirements. That is, the user has not created legal relations with any other party, whether it's the developer or the risk capital providers. Etherisc describes this arrangement as a "technical guarantee" as distinct from a "legal guarantee."

We are not aware if this approach has been tested in any courts or received public blessing from a regulator. It seems likely that, were parametric insurance to reach any scale in the future, regulators would challenge this argument.

A second approach with a more established legal basis is taken by other decentralized protocols, such as Nexus Mutual. Instead of being regulated as insurers, they structure themselves as "discretionary mutuals." In jurisdictions where this concept exists, such as the UK, discretionary mutuals are recognized as falling outside insurance regulation. The key facet, similar to the parametric argument, is that participants have no legally enforceable right to receive a payout. Unlike the parametric "technical guarantee," in the mutual structure, claims are paid at the discretion of the mutual members. This lends itself quite naturally to DeFi where community voting may be used to determine whether to approve a claim.

A major downside to this approach is that a protocol must satisfy users that its community can be trusted to pay out as expected despite not necessarily being incentivized to do so. It seems likely that, if more robust alternatives existed at scale, then these would be preferred by users, especially within a DeFi community that values "trustless" as a core principle.

It appears, therefore, that DeFi protocols wishing to achieve success in the insurance space may have to accept, like the traditional insurers one hundred years ago, that DeFi insurance is also peculiarly affected with the public interest. To offer true insurance solutions where risks are properly costed, capital adequately reserved and claims predictable and enforceable, protocols cannot avoid being regulated in some shape or form. It would seem to be the right time for DeFi participants to work with regulators to find a sensible solution to manage the public interest, while still benefiting from the huge opportunities for innovation offered by DeFi.

2.6 DISTRIBUTION MODEL

Traditional insurers use intermediaries such as agents, brokers, online aggregators, and e-commerce platforms to distribute their products. Decentralized insurance alternatives depend entirely on online direct channels. They leverage social media marketing heavily to get more traction on platforms like Twitter, Discord, Telegram, Medium, and Reddit. It is also important to get key opinion leaders (KOLs) in DeFi ecosystems to buy in and help advertise the platform. This usually involves a promise of a share of the advisor tokens to the KOLs.

Another typical strategy is to form partnerships with other DeFi protocols. This can be in the form of B2B direct sales of insurance cover to a protocol. For example, Unslashed Finance sells cover directly to Lido[14] a liquid staking solution, covering up to 400,000 ETH. An example of B2B2C is the partnership between the insurance platforms and Beefy, a cross-chain yield optimizer. The Beefy platform advertises Nexus Mutual and InsurAce platforms' coverages

[14] More details can be found under the Example and Case Studies section in the Unslashed Finance documentation (Unslashed Finance,, 2021).

for Beefy's yield-bearing tokens using a button with a referral link. Upon a successful purchase, both Beefy and the user can get rewards.

There are also DeFi protocols that are built to distribute decentralized insurance solutions. Armor offers coverages underwritten by Nexus Mutual, as well as allowing existing Nexus Mutual policyholders to tokenize coverage as NFTs for resale. This design aims at removing the KYC requirement. Armor also introduced a smart cover system that can provide a 'pay-as-you-use' insurance experience for the users. The system automatically tracks user funds across various protocols in real-time and automatically adjusts coverage amounts and subject protocol. This enables premium streaming by seconds instead of an upfront premium payment, as well as ensuring that cover is always relevant and adequate for the policyholder. This is a prime example of distribution innovation made possible by the composability of DeFi, which provides a much better insurance experience to the users. It is, perhaps, one of the key reasons why Armor has the largest TVL in the insurance sector.

2.7 GOVERNANCE

Traditional insurers are run by centralized management teams. In DeFi, Decentralized Autonomous Organizations (DAO), an alternative to traditional corporate forms, are used as the governance structure by many DeFi protocols, including decentralized insurance protocols like Nexus Mutual and Unslashed Finance. DAOs are organizations on blockchains that enable decentralized control and decision-making by their members. This structure allows owners of tokens of the DAO to make decentralized decisions through voting and execute the decisions using smart contracts. These votes may set the pricing parameters, and allocate capital to investment strategies or high-level organization decisions.

A DAO governance process typically involves a few stages, depending on the nature and the complexity of the proposals:

- **Ideation and discussions**: If community members (not necessarily members of the DAO, it could be users) come up with an idea that would benefit the protocol, they would discuss the idea with the rest of the community on Discord and forums.
- **Proposal**: Community members will draft a proposal if the idea is worth pursuing based on initial community inputs.
- **Signal voting**: Members of the DAO will vote based on their holdings of the governance token to signal whether they support or oppose the proposal. Snapshot, a voting platform, is often used for this purpose.
- **On-chain voting**: If on-chain proposals are involved, on-chain voting is often used to finalize the results,. Most popularly on Tally. On-chain voting is more costly due to transaction fees; however, the results are fully on-chain and can be used for execution.
- **Execution**: The results of on-chain votes can be executed using smart contracts written ahead of time for the proposals.

The DAO structure encourages users and community members to learn and contribute to the protocols and boosts community participation and collaboration. Research Blockchain Solutions for Agency Problems in Corporate Governance (Kaal, Blockchain Solutions for Agency Problems in Corporate Governance, 2019) have shown that smart contracts have the potential to solve some of the agency problems in corporate governance. Smart contracts can cost-effectively verify, monitor, and enforce the negotiation and performance of a contract between principal and agent, or remove the agents as intermediaries. DAO provides a different way to govern by changing traditional hierarchical relationships and focusing instead on executions and outcomes. On the other hand, DAO also comes with its own issues. For example, it is questionable whether governance is still efficient and effective if the decision-making power is spread too thin. Also, under a DAO structure, no individual or groups of individuals can be held

accountable, and it is not clear whether that is in the best interest of the participants (Morrison, Mazey, & Wingreen, 2020).

2.8 CAPITAL MODELING AND MANAGEMENT

As of July 2022, no government agency supervises and regulates the activities of DeFi protocols in a way where traditional financial institutions and insurance companies are regulated. Therefore, there are no externally imposed minimum capital tests for DeFi protocols. Some DeFi protocols, therefore, design their own capital framework to calculate what they must hold to cover potential losses. As such, DeFi protocols are self-regulated, while being monitored by their community members. However, this approach may not instill trust in users as much as traditional regulations, especially if the capital framework design and calculations are not totally transparent.

Leading protocols such as Nexus Mutual and InsurAce built their own capital framework based on concepts used by the Solvency II capital framework, developed by the European Insurance and Occupational Pensions Authority ("EIOPA"). Underlying the capital framework of Solvency II is an economic risk-based approach to assess the "overall solvency" of the undertaking of insurance. There are a few tiers of capital requirements under Solvency II, which are Solvency Capital Requirement (SCR) and Minimum Capital Requirement (MCR), which aim to act as the "soft" and "hard" floors for minimum available capital liquidity to be met under different probability bounds. The DeFi protocols also use similar language and concepts to describe their own minimum capital requirements, however, they don't explain all the details that would allow one to recreate their models. Also, since the calculation is not mandated by external parties, the capital framework design is not standardized across protocols.

The calculation of capital requirements at both Nexus Mutual and InsurAce and other platforms is carried out off-chain by centralized teams due to the complexity and associated high transaction costs if the capital requirements were to be calculated on-chain frequently. For example, at Nexus Mutual, the minimum capital requirement is calculated as the maximum of a floor and a function of the cover amount. The function of the cover amount is a simplified representation of capital requirements calculated off-chain. The opaqueness of the capital requirements calculation could lead to trust issues as the process is not transparent nor real-time for the public.

Unlike traditional insurers and reinsurers who provide capital or source capital in a centralized manner, assets for required and excess capital are provided by stakers in a decentralized manner directly on the insurance platforms. The DeFi protocols designed some mechanisms to manage liquidity risks; for example, Nexus Mutual links the token price of NXM with the amount of capital and disallows the exchange of NXM for ETH when the minimum capital is below a threshold. InsurAce imposes a lock-up period of 30 days after the unstaking of capital.

The management of capital is critical to ensuring solvency and improving capital efficiency. Nexus Mutual uses a decentralized pool structure where capital pools are separated for different products. Funds can only be deployed into a single capital pool that serves to cover a single protocol. As a result, capital providers are likely exposed to larger protocol-specific risks.

To improve capital efficiency and increase the diversification of underlying protocol risks, mutual-fund-like investment products have been designed for capital providers to endow their funds to form a portfolio and cover the coverage for different insurance protocols. This type of model is designed for insurers to underwrite and provide coverage for multiple protocols.

There are concerns about whether this approach will be vulnerable to systemic risks, specifically, when multiple protocols suffer from large losses at the same time, whether the underlying capital would be sufficient to cover the losses. To mitigate this, several protocols have adopted similar approaches to the issue - reducing the systematic risk by increasing diversification.

- Unslashed Finance curated a "Spartan Bucket" that covered products across centralized exchanges, wallets, DeFi protocols, oracles, and peg-related token protections. Each of the products is only given 5% maximum exposure, and its wide variety of selections can further reduce the systematic risks that are assumed under the portfolio.

- Risk Harbor centralized all the invested funds into one central vault such that it could maximize capital efficiency by underwriting different protocols from one capital pool. The platform estimates the correlations of potential default events across different protocols and optimizes the selection of the protocol based on those correlations.

InsurAce follows a similar model as the "Spartan Bucket" by Unslashed Finance, but it offers more varieties in terms of investment and coverage. InsureAce allows stakers to put funds into a staking pool with different types of stablecoins such as DAI, USDC, USDT, etc. Users who staked in the funds will receive an LP token in the end and enjoy rewards emitted by $INSUR, which is the platform's governance token. This creates a simplified journey where users can participate in liquidity mining, but the funds endowed will be leveraged to back on numerous offerings that are being provided on the platform.

Section 3: Opportunities and Challenges

Decentralized insurance alternatives are an integral part for the DeFi ecosystem by providing coverage for key risks. While they are growing fast along with the ecosystem, they are also facing several key challenges.

3.1 OPPORTUNITIES

THE RISE IN DEMAND FOR DEFI INSURANCE

DeFi is a fast-growing space with more and more capital pooled into it. This also means that the addressable market size and demand for DeFi insurance coverage are growing fast. This is especially vigorous when institutions start to invest in DeFi. A prerequisite for making such investments is to have adequate insurance coverage to hedge against disastrous losses due to smart contract vulnerabilities and stablecoin risks. So far, no traditional insurers are meeting the demand due to the knowledge gap and DeFi's risky and unregulated nature.

HUGE POTENTIAL FOR DECENTRALIZED INSURANCE PROJECTS

Insurance is an indispensable part of any well-established financial system. The DeFi community is expecting more and better insurance protocols to help the ecosystem pool, transfer, and manage risks. The decentralized insurance sector is still relatively small compared to the decentralized exchange and lending sectors. As the DeFi ecosystems expand and attract larger and more sophisticated users, the need for risk management is poised to grow and so is the decentralized insurance sector.

INSURE EMERGING RISKS AND SUPPORT INSURANCE PROGRAMS ON A GLOBAL SCALE

Traditional insurers hesitate to cover emerging risks like cybersecurity, climate, and technological risks caused by AI, robotics, DeFi, etc. These emerging risks have limited loss history and are ever-evolving. Therefore, it is difficult for underwriters and actuaries to estimate future losses based on past experience.

Some emerging risks, such as the climate risks, are also on a global scale. Other risks, such as cybersecurity and DeFi risks, are also challenging with their contagious nature – when a claim event happens, it could result in a cascading failure in the ecosystem that causes a great number of claims. Covering such risks often requires multiple insurers, reinsurers, and public institutions to work together and run insurance or disaster recovery programs to manage the claims and spread the risk costs. These programs usually incur high coordination and operation costs due to the large number of claims and involvement of multiple stakeholders.

Decentralized insurance models, with their global reach and blockchain-based infrastructure, present a new solution to cover emerging risks on a global scale. For emerging risk, a key role they can play is to serve as a risk exchange or prediction market that channels crypto capital with a high risk appetite to fund the risks that cannot be easily quantified. Blockchain provides transparency and traceability, which is the key to maintaining trust across multiple stakeholders (e.g., insurers, reinsurers, public institutions, and policyholders). Cryptocurrencies provide a cost-efficient settlement option for premium and claim settlement agnostic of the geographical location. Smart contracts can be used to automate operations and reduce the coordination needed between multiple parties.

There are already several pilot programs running to test out the idea for a decentralized insurance model to cover emerging risks:
- Lemonade, the listed digital insurer in the U.S., works with Hannover Re, Avalanche and Chainlink to provide parametric weather insurance for farmers in Africa.
- Deloitte has formed a strategic alliance with Avalanche to build a new disaster recovery platform that uses blockchain to help state and local governments more easily and timely demonstrate eligibility of federal emergency funding when a disaster strikes a community.

ADDRESSABLE MARKET SIZE AND COST EFFICIENCY ENABLES PRODUCT INNOVATIONS FOR NICHE MARKET NEED

Traditional insurers have a long product development cycle and associated costs. Serving niche market needs isn't a priority as most of them may not provide sufficient premium size to cover the allocated operation costs. Even if such coverage exists, it is usually expensive and unaffordable. Examples of such insurance products (Wikipedia, n.d.) include medical insurance for people with severe pre-existing conditions, temporary event insurance, body-part insurance, or alien abduction insurance.

We believe decentralized insurance can foster potential solutions for such niche market needs. First, because of their global reach, they can theoretically pool together a bigger risk facility to share the risks among all participants compared to any local direct insurers. The unit cost can be lower because of the bigger pool across the globe. Secondly, due to disintermediation and automation enabled by smart contracts, the operating costs allocated to individual products can also be lower.

There are also studies and examples of blockchain-based decentralized P2P insurance models that can be a potential solution for niche market insurance needs. A group of authors from Arizona State University demonstrated a fast deployment of a decentralized P2P insurance model to gain operational efficiencies and launch new products (Boyle, Pesic, Jevtic, & Boscovic, 2021). Teambrella, a bitcoin-based peer-to-peer insurance marketplace, created pilot groups in Peru, the Netherlands, Germany, and Argentina (Ankitha Shetty, 2022) to cover niche categories like pets and cycling.

COMMUNITY-BASED MODEL TO IMPROVE ENGAGEMENT AND ENABLE INNOVATION CROWDSOURCING

Decentralized insurance alternatives' community-based governance and token economy can engage customers better. Active participation leads to a deeper sense of belonging, ownership, and loyalty.

Policyholders, risk capital providers, and developers have more aligned economic interests. As they are all protocol token holders, they all want the protocol to succeed. Token holding incentivizes them to participate more actively in protocol development and operations, such as voting to help with operational decision-making.

This model also enables innovation crowdsourcing by engaging the community to generate ideas and co-create solutions together. Token holders are provided with tools and procedures to make governance proposals and discuss with each other in Discord and forums. They also provide feedback to the development team to help improve the products and shape the product roadmaps together. Nexus Mutual has a specific board named "Potential Protocol Changes" for members to propose and discuss potential changes, such as new products, investment strategies and governance settings, etc. InsurAce's community designed a claim bounty program that invited all community members to help assess claims related to a UST de-pegging event (InsurAce, UST De-Peg Claims Bounty, 2022).

3.2 CHALLENGES

LACK OF DATA AND UNDERSTANDING OF DeFI RISKS

There is still a general lack of understanding of DeFi risks and the magnitude of the potential losses they can cause.

This is first due to the short history of cryptocurrency and DeFi. The first cryptocurreny, Bitcoin, was introduced in 2008 and DeFi became popular only in 2020. Experience data in terms of incidents and claims are still limited. It is also difficult to estimate future experience using past incidents given the rapid changes in the ecosystem and technology.

Secondly, these are highly correlated risks that may cause a maximum probable loss not absorbable by risk capital. Protocol risks are correlated as they are sitting on the same blockchain infrastructure. Any blockchain failure may impact multiple protocols, if not all, at the same time. Smart contract risks can be contagious in nature as many of them communicate with each other during their course of execution (Jevtic & Lanchier, 2021). If one contract fails, the impact may cascade to other contracts and spread further. Stablecoin de-pegging is also a type of systemic risk as stablecoins are cornerstone assets in the DeFi ecosystem. Many protocols are using stablecoins to back up their tokens and many investors are using stablecoins as collateral for borrowing. A stablecoin de-pegging may cause widespread default.

A perfect example to illustrate the systemic DeFi risk is the UST de-pegging incident and the resulting collapse of the entire Terra blockchain and DeFi ecosystem in May 2022, causing billions of assets to vanish in a matter of days. Two decentralized insurance protocols were impacted:

- Risk Harbor runs on several blockchains, including Terra. After the incident, the protocol's TVL dropped over 70%, from USD $9.5 million to USD $2.8 million.
- InsurAce provides UST de-pegging coverage. It sold 234 covers with a total cover amount of more than USD $22 million. The incident resulted in a claim payment of approximately USD $12.5 million (InsurAce, UST De-peg Advisory Board Report, 2022), which was one-fourth of the total risk capital in its staking pool.

Insurers benefit from diversification by underwriting many policies that cover risks with low or no correlation so that a single incident won't impact the whole portfolio's profitability. Decentralized insurance alternatives may face highly concentrated and correlated risks that would cause a drastic loss in black swan events, such as a major blockchain failure or a major stablecoin de-pegging. This would cause a significant loss for crypto risk capital providers and could potentially result in the protocol's own failure.

BARRIER TO ADOPTION IS HIGH FOR THE AVERAGE USER

Decentralized insurance applications are not easily accessible by everyone. A participant is generally tech-savvy and has both knowledge in insurance and DeFi. Like other DeFi protocols, decentralized insurance alternatives don't have a customer service team to assist users 24/7. They heavily rely on the user to figure out problems themselves or seek help from other members on social media platforms such as Twitter, Discord and Telegram. There is no guarantee of an answer or a helping hand.

LOW ENTRY BARRIERS FOR POTENTIAL COMPETITORS

Insurance is a strictly regulated industry. It has a high entry barrier because of the long licensing process and significant initial capital requirement.

In the world of decentralized insurance, the story is different. It is unregulated and without any initial capital requirement. Moreover, all the data and smart contracts that control governance and operations are publicly accessible once launched on the blockchain. Therefore, it is much easier for potential competitors to get into the

space, leveraging on what the existing players have built. It is common to see new projects forking[15] smart contracts from existing protocols and quickly launching their services. Existing protocols may face fierce competition from new protocols that offer a significant amount of governance tokens to incentivize users.

HIGH SECURITY RISKS

Decentralized insurance protocols are not immune to hacks. In 2020, a decentralized insurance protocol named Cover Protocol (Kevin Reynolds, 2020) was hacked and 4,350 ethers were stolen by a white-hat hacker, who later returned the assets. This, however, hurt the protocol's reputation and it shut down eventually (Decrypt, 2021). Another incident was a targeted attack on Nexus Mutual's CEO's wallet, who lost his NXM tokens worth USD $8 million (Godbole, 2020).

HIGH REGULATORY UNCERTAINTY

It is uncertain how regulators may step up their measures to regulate decentralized insurance. We can, perhaps, get a glimpse of how governments treat cryptocurrencies and DeFi.

When it comes to cryptocurrencies, different countries take drastically different approaches (Buchholz, 2022). Countries like China, Egypt and Iraq impose an outright ban on all crypto activities. The U.S., European countries and other typically developed countries are applying laws to regulate cryptocurrencies. However, most of them have not proposed a clear regulatory framework. Only a handful of small countries, such as El Salvador, embrace cryptocurrencies in full.

There is no doubt that the regulators have their eyes on DeFi, especially after the Terra UST de-pegging incident. The International Organization of Securities Commissions, a global umbrella organization for securities regulators, warns that DeFi contains myriad hidden conflicts and risks and warrants closer regulator attention (Financial Times, 2022). There are also worries that a new proposal by the U.S. Securities and Exchange Commission (Ligon, 2022) to expand the definition of a security dealer to include automated and algorithmic trading technology to execute trades and provide liquidity in the market will bring most DeFi protocols under SEC regulatory scrutiny.

We expect that decentralized insurance alternatives may face similar uncertainties down the road when they grow further. We also expect that discussions around how to regulate these alternatives may take even longer as it is literally a 'regulatory platypus' that does not fit easily into any regulatory umbrella.

---

[15] Copying with ad-hoc adjustments

Decentralized insurance alternatives face several key challenges when expanding into the major lines of business (LOBs) in insurance, such as life, health, motor, home, etc.:

- **Lack of oracle and data privacy issue**: There is no credible and open-source data oracle to provide risk event data for these LOBs. Centralized institutions such as governments and insurers are holding data privacy as it is sensitive customer data.

- **Regulation**: Expanding into these LOBs will inevitably invite regulator attention as they are closely associated with fundamental public interests. It's most certainly guaranteed a licensing need and regulatory oversight for any insurance model to cover such risks.

- **Product complexity**: Community-based DeFi models require the members to self-learn and self-help. Most members don't have the expertise to thoroughly understand complicated insurance products and participate in the product design and operation processes.

- **Contract complexity:** Insurance products in major lines of business usually have complex design and terms in the operation process to support their underwriting, policy administration and claim management. It is complicated to code all the business logic within smart contracts. Due to the complexity of smart contracts, the development and quality assurance costs could be high.

Section 4: Looking into the Future

Decentralized insurance is still in its infancy compared to the traditional insurance industry. However, we should not overlook the innovations and unique value propositions they can bring and their potential to disrupt the insurance industry. In this section, we summarize our key findings and discuss our thoughts on whether decentralized insurance alternatives are going to disrupt traditional insurance. We will also touch on how an actuary can prepare for it.

4.1 IS DECENTRALIZED INSURANCE GOING TO DISRUPT TRADITIONAL INSURANCE?

Decentralized insurance alternatives use blockchain-based insurance and risk-pooling models to share and transfer risks. It has the merits of transparency inherited from blockchain technology, better customer engagement backed by a token economy, a global reach of customers and crypto-based risk capital, as well as intermediary-free distribution. It is also more cost-efficient due to operation automation by smart contracts, as well as blockchain-enabled fast payment and settlement. However, they are also facing significant challenges in terms of security, a shortage of data and understanding of the risks, limitations in offering expansion to cater to average users, and regulatory uncertainty. It is, therefore, challenging, if not impossible, for decentralized insurance models to expand into and disrupt major lines of businesses in the traditional insurance sector such as life, health, motor, and home.

We believe in a probable future with decentralized insurance alternatives and traditional insurance running in parallel, each providing coverage in their strong suits. They won't be competing. Rather, decentralized insurance may play a complementary role to provide innovative products that cover underinsured segments, such as emerging risks and niche insurance needs.

Decentralized insurance alternatives and traditional insurance should also learn from each other. We believe traditional insurers can leverage smart contracts and blockchain technologies, the same as their decentralized counterparts, to channel information and support transactions and settlements, thereby significantly improving their operational efficiency and unshackling themselves from legacy systems and manual workflows. Regulatory barriers may exist if a public permissionless blockchain and cryptocurrency is used. To move fast now, traditional insurers can leverage on private blockchain technologies, such as Hyperledger, to build private chain for information sharing, data verification and internal settlements to improve operation efficiency.

Decentralized insurance can learn from its traditional counterparts in areas like risk management and operational governance. They can also invite traditional insurance professionals, such as underwriters, actuaries and claim adjudicators, to participate in their community to help drive better decisions in product design, risk and claim assessment, so that collective intelligence and true decentralization can be achieved instead of over-reliance on the capability of their Advisory Board.

4.2 HOW CAN AN ACTUARY PREPARE FOR IT?

Despite its many challenges and risks, the potential of decentralized insurance is significant. Actuaries have the relevant knowledge and skills to contribute to decentralized insurance alternatives in areas like product design, protocol economic design, claim process design, and risk assessment, as well as capital management practice. There are questionable practices in these areas that call for new actuarial thinking and tools to help make the protocol and product more financially sound and safe.

To get started, an actuary should first develop a basic understanding of DeFi. There are a lot of resources available online and the SOA's report on Decentralized Finance for Actuaries could be a good start (Lie, Weng, & Tse, 2022). Beyond learning about the basics, it's best to give DeFi and DeFi insurance protocols a try: Try out DeFi protocols, purchase a cover, join a decentralized insurance protocol's Discord channel and participate in their community discussions.

Section 5: Acknowledgments

The researchers' deepest gratitude goes to those without whose efforts this project could not have come to fruition: the Project Oversight Group and others for their diligent work overseeing questionnaire development, analyzing and discussing respondent answers, and reviewing and editing this report for accuracy and relevance.

Project Oversight Group members:

Stephen Chan, PhD

Jeffrey Chu, PhD

Runhuan Feng, FSA, CERA

Petar Jevtic, PhD

Douglas W. Oliver, ASA, MAAA, ACAS

Franck Pralas, AQ

Jared Praniewicz, FSA, MBA, PhD

Geu Roo Yang, ASA

Yifan Zhang, FSA, MAAA

At the Society of Actuaries Research Institute:

Korrel Crawford, Senior Research Administrator

Alice Locatelli, Senior Director of Digital Strategy

David Schraub, FSA, MAAA, Senior Practice Research Actuary

Section 6: References

(Please note that not all the claims within this introductory paper have references clearly specified in this section as the authors tried to strike a balance between adding more references to support the claims and a timely publication of paper.)

Ankitha Shetty, A. D. (2022). Block Chain Application in Insurance Services: A Systematic Review of the Evidence. *SAGE Journals*. Retrieved from https://journals.sagepub.com/doi/full/10.1177/21582440221079877

Aramonte, S., Huang, W., & Schrimpf, A. (2021). *DeFi risks and the decentralised illusion.* BIS Quarterly Review.

Ben-Har, R., Patel, D., Su, A., & Resnick, M. (2021, Jun 5). *Risk Harbor V1.* Retrieved from Github - Risk Harbor Whitepaper: https://github.com/Risk-Harbor/RiskHarbor-Whitepaper/blob/main/Risk%20Harbor%20Core%20V1%20Whitepaper.pdf

Boyle, E., Pesic, S., Jevtic, P., & Boscovic, D. (2021). *Peer-to-Peer Insurance: Blockchain Implications.* Society of Actuaries.

BraveNewDeFi. (2021, December). *Operation Wartortle Next Steps: Draft Execution Proposal*. Retrieved from Nexus Mutual Forum: https://forum.nexusmutual.io/t/operation-wartortle-next-steps-draft-execution-proposal/746

Buchholz, K. (2022, May 18). *Where the World Regulates Cryptocurrency*. Retrieved from Statista: https://www.statista.com/chart/27069/cryptocurrency-regulation-world-map/

CoinDesk. (2022, May 15). *The Collapse of UST and LUNA Was Devastating, but There Is Still Hope for Crypto*. Retrieved from CoinDesk: https://www.coindesk.com/markets/2022/05/15/the-collapse-of-terra-was-devastating-but-there-is-still-hope-for-crypto/#:~:text=The%20short%20of%20it%20is,billion%20of%20value%20was%20lost.

Cointelegraph. (2021). Cointelegraph Consulting: Recounting 2021's biggest DeFi hacking incidents. *Cointelegraph*. Retrieved from https://cointelegraph.com/news/cointelegraph-consulting-recounting-2021-s-biggest-defi-hacking-incidents

Decrypt. (2021, September 5). *DeFi Insurance Protocol Cover Shuts Down, Token Value Plummets*. Retrieved from Decrypt: https://decrypt.co/80262/defi-insurance-protocol-cover-shuts-down-token-value-plummets

Ethereum Org. (n.d.). *Introduction to Smart Contract*. Retrieved from Ethereum Doc: https://ethereum.org/en/developers/docs/smart-contracts/#composability

Financial Times. (2022, March 23). *DeFi projects rife with hidden risks, global regulatory body warns*. Retrieved from Financial Times: https://www.ft.com/content/b0c581c8-96b2-4c34-abcc-5189d7283891

Godbole, O. (2020, Dec 14). *CEO of DeFi Insurer Nexus Mutual Hacked for $8M in NXM Tokens*. Retrieved from CoinDesk: https://www.coindesk.com/markets/2020/12/14/ceo-of-defi-insurer-nexus-mutual-hacked-for-8m-in-nxm-tokens/

InsurAce. (2021). *InsurAce Documentation.* Retrieved from InsurAce: https://docs.insurace.io/landing-page/

InsurAce. (2022, Jun 2). *UST De-peg Advisory Board Report*. Retrieved from InsurAce Blog: https://www.insurace.io/blog/?p=3059

InsurAce. (2022, Jun 6). *UST De-Peg Claims Bounty*. Retrieved from InsurAce Blog: https://www.insurace.io/blog/?p=3081

IRMI. (n.d.). *Insurance is affected with a public interest*. Retrieved from IRMI: https://www.irmi.com/articles/expert-commentary/insurance-is-affected-with-a-public-interest#:~:text=%22Affected%20with%20a%20public%20interest%22%20deals%20with%20how%20the%20insurance,Twain%20called%20the%20Gilded%20Age.

Jevtic, P., & Lanchier, N. (2021). *Probabilistic Framework For Loss Distribution.* Retrieved from https://arxiv.org/pdf/2101.08964v1.pdf

Kaal, W. A. (2019). Blockchain Solutions for Agency Problems in Corporate Governance. *SSRN*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3373393

Kaal, W. A. (2019). *Blockchain Solutions for Agency Problems in Corporate Governance.* World Scientific Publishers.

Kalges-Mundt, A., Harz, D., Gudgeon, L., Liu, J.-Y., & Minca, A. (2020). *Stablecoins 2.0: Economic Foundations and Risk-based Models.* Retrieved from https://arxiv.org/pdf/2006.12388.pdf

Kevin Reynolds, D. P. (2020, Dec 28). *Cover Protocol Attack Perpetrated by 'White Hat,' Funds Returned, Hacker Claims*. Retrieved from CoinDesk: https://www.coindesk.com/markets/2020/12/28/cover-protocol-attack-perpetrated-by-white-hat-funds-returned-hacker-claims/

Lie, J., Weng, G. Y., & Tse, W. (2022). *Decentralized Finance for Actuaries.* SOA Research Institute.

Ligon, C. (2022, March 29). *The SEC's New Proposal to Redefine 'Dealer' Could Spell Bad News for DeFi*. Retrieved from CoinDesk: https://www.coindesk.com/policy/2022/03/28/the-secs-new-proposal-to-redefine-dealer-could-spell-bad-news-for-defi/

Llama, D. (n.d.). *Insurance TVL Ranking*. Retrieved from DeFi Llama: https://defillama.com/protocols/Insurance

Max Resnick, R. B.-H. (2021). *Risk Harbor Whitepaper v2.* Retrieved from Github Risk Harbor Whitpaper: https://github.com/Risk-Harbor/RiskHarbor-Whitepaper/blob/main/Risk%20Harbor%20Core%20V2%20Whitepaper.pdf

Morrison, R., Mazey, N. C., & Wingreen, S. C. (2020). *The DAO Controversy: The Case for a New Species of Corporate Governance?* Frontiers.

Mutual, N. (2021, Apr 26). *131. Protocol Cover*. Retrieved from Nexus Mutual Proposal: https://app.nexusmutual.io/governance/view?proposalId=131

Nexus Mutual. (2018). *Nexus Mutual Gitbook.* Retrieved from Nexus Mutual: https://nexusmutual.gitbook.io/docs/

Nexus Mutual. (2021, Apr 26). *131. Protocol Cover*. Retrieved from Nexus Mutual Proposal: https://app.nexusmutual.io/governance/view?proposalId=131

Prudential Insurance Co v Inland Revenue Commissioners: 1904, 2 KB 658 (England and Wales 1904).

Risk Harbor,. (2021). *Risk Harbor Learn.* Retrieved from Risk Harbor: https://docs.riskharbor.com/

Unslashed Finance,. (2021). *Unslashed Finance Documentation.* Retrieved from Unslashed Finance: https://documentation.unslashed.finance/

Wikipedia. (n.d.). *Niche Insurance*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Niche_insurance

Appendix A: Policy Wordings

Cover Type	Nexus Mutual	InsurAce
Smart Contract Cover	Protocol Cover: Link	Smart Contract Cover: Link
Custody Cover	Custody Cover: Link	Custodian Risk Cover: Link
Stablecoin De-pegging Cover	Nil	UST De-pegging Cover: Link USDT De-Pegging Cover: Link MIM De-Pegging Cover: Link
Yield Bearing Token Cover	Yield Token Cover: Link	Nil

Appendix B: Nexus Mutual Claim Incident Details

ID	Event Name	Claim Count	Total Reported Claim	Total Paid Claim	Event Adjudication	Rejection Reason	Reference
1	bZx flashloan event	5	120,194.76	40,210	Covered		Link
2	MakerDAO Black Thursday	17	1,032,720	0	Not Covered	Does not cover liquidation event caused by market crash	Link
3	Uniswap imBTC ERC-777 issue	1	38,086	0	Not Covered	Public known bug is excluded	Link
4	Balancer Deflationary Token	1	19,043	0	Not Covered	Protocol already reimbursed the loss	Link
5	Yearn Deployer Incident	2	519,879	0	Not Covered	The hack did not happen to the Yearn Finance smart contract	Link
6	Yearn yDAI hack	19	3,427,225	2,704,870	Covered		Link
7	Prysm Beacon Nodes Stoppage	1	999.8	0	Not Covered	No clear information	Link
8	Bancor Withdrawal Issue	1	60,938.24	0	Not Covered	Impermanent loss isn't a smart contract issue, therefore, not covered	Link
9	Loss of User Wallet Access	1	79,984	0	Not Covered	User's own private key compromised is excluded	Link
10	Cream V1 Economic Exploit	8	1,198,296.24	206,146	Covered		Link
11	BadgerDAO FE Hack	1	190432	0	Not Covered	Front end exploit is not covered	Link
12	Abracadabra Incident	1	299940	0	Not Covered	Identified as not a smart contract issue	Link
13	Rari Capital Fust Market Exploit	4	5,145,064	5,045,085	Covered		Link
14	Anchor UST De-pegging Loss	4	429,914	0	Not Covered	Protocol cover does not cover stablecoin de-pegging	Link
15	Perpetual Protocol Design Failure	2	314,515	314,515	Covered		Link

Appendix C: Glossary – Commonly Used DeFi Terms

Arbitrum	A Layer 2 solution project designed and developed by Offchain Labs to enhance Ethereum's speed and scalability.
Avalanche	A Layer 1 decentralized, open-source proof of stake blockchain with smart contract functionality.
Binance Smart Chain (BSC)	A layer 1 blockchain that runs parallel to Binance's premier blockchain, Binance Chain (BC).
Composability	The ability for DeFi applications to communicate with and build upon each other.
DAI	A decentralized stablecoin cryptocurrency maintained and regulated by MakerDAO.
Decentralized Autonomous Organization (DAO)	Organizations where governance token holders discuss proposals and vote to reach collective decisions.
Decentralized Exchange (DEX)	DeFi applications that allow cryptocurrency trading without an intermediary.
Decentralized Finance (DeFi)	An emerging financial system built on public and permissionless blockchains using smart contracts.
Ethereum	A decentralized blockchain that first introduced smart contract functionality, with its native cryptocurrency, Ether, currently having the second-largest market capitalization among all cryptocurrencies as of Dec 2021.
Gas	Computation and transaction fees are paid by the transactor to be burned or to compensate miners and validators who help secure the network.
Layer 1 (L1)	A underlying main blockchain architecture.
Layer 2 (L2)	An overlaying network that lies on top of Layer 1, the underlying blockchain.
Liquidity mining / Yield farming	Providing liquidity for DeFi protocols for reward tokens, from a sharing of transaction fees or protocol equity tokens.
Liquidity Provider Tokens (LP Tokens)	ERC-20 Tokens that act as receipts for depositing cryptocurrencies into a smart contract that can be redeemed or used elsewhere.
Permissionless Blockchain	Also known as trustless or public blockchains, which allow everyone to participate.
Polygon	A Layer 2 or sidechain solution running alongside with the Ethereum blockchain.
Stablecoin	A cryptocurrency where its price is designed to peg to a cryptocurrency, fiat money or to exchange traded

commodities.

Stablecoin De-pegging	Refers to the phenomenon of a stablecoin's market price deviating from its intended peg, such as a cryptocurrency or fiat money.
Terra	A layer 1 blockchain and payment platform for algorithmic stablecoin UST.
USDC	A stablecoin pegged to USD managed by a consortium called Centre, founded by Circle.
USDT	A stablecoin pegged to USD launched by the company, Tether Limited Inc., in 2014.
UST	A stablecoin built on the Terra blockchain and created by South Korea's Terraform Labs.
Yield-Bearing Tokens	Tokens where the holders are entitled to yields, usually LP tokens.

About The Society of Actuaries Research Institute

Serving as the research arm of the Society of Actuaries (SOA), the SOA Research Institute provides objective, data-driven research bringing together tried and true practices and future-focused approaches to address societal challenges and your business needs. The Institute provides trusted knowledge, extensive experience and new technologies to help effectively identify, predict and manage risks.

Representing the thousands of actuaries who help conduct critical research, the SOA Research Institute provides clarity and solutions on risks and societal challenges. The Institute connects actuaries, academics, employers, the insurance industry, regulators, research partners, foundations and research institutions, sponsors and non-governmental organizations, building an effective network which provides support, knowledge and expertise regarding the management of risk to benefit the industry and the public.

Managed by experienced actuaries and research experts from a broad range of industries, the SOA Research Institute creates, funds, develops and distributes research to elevate actuaries as leaders in measuring and managing risk. These efforts include studies, essay collections, webcasts, research papers, survey reports, and original research on topics impacting society.

Harnessing its peer-reviewed research, leading-edge technologies, new data tools and innovative practices, the Institute seeks to understand the underlying causes of risk and the possible outcomes. The Institute develops objective research spanning a variety of topics with its strategic research programs: aging and retirement; actuarial innovation and technology; mortality and longevity; diversity, equity and inclusion; health care cost trends; and catastrophe and climate risk. The Institute has a large volume of topical research available, including an expanding collection of international and market-specific research, experience studies, models and timely research.

Society of Actuaries Research Institute
475 N. Martingale Road, Suite 600
Schaumburg, Illinois 60173
www.SOA.org