Digital Finance (2023) 5:643–687
https://doi.org/10.1007/s42521-023-00093-x

ORIGINAL ARTICLE

A primer on the insurability of decentralized finance (DeFi)

Felix Bekemeier[1]

Received: 24 January 2023 / Accepted: 1 August 2023 / Published online: 28 August 2023

Abstract
Decentralized finance (DeFi), a blockchain-based form of alternative financial markets, has gained significant public attention in recent months. Despite its relatively short history, DeFi offers a range of opportunities for designing and transferring digital assets. This establishes market structures that bear resemblance to traditional financial markets. Notably, the landscape of DeFi projects has expanded to include insurance protocols that offer DeFi-inherent mechanisms for hedging DeFi-specific risks, particularly those associated with smart contracts. These insurance protocols aim to provide similar value propositions as traditional insurance, namely the minimization and transfer of risks in exchange for a premium. However, it is crucial to acknowledge that most of these risk transfer protocols are strongly dependent on subjective expectations and decentralized governance structures. This article aims to develop a taxonomical understanding of DeFi insurance. Moreover, it seeks to assess the insurability of risks related to smart contracts. By doing so, this study contributes to the emerging body of knowledge surrounding DeFi insurance, paving the way for further research and analysis in this evolving field.

Keywords Decentralized finance · Decentralized insurance · Risk transfer · Smart contracts

JEL Classification G22 · G52 · O32

1 Motivation and contribution

Since the beginning of the digital century, new challenges and prospects for the insurance industry related to new technological opportunities are discussed in different contributions (O'Hare, 1994; Bernheim, 1998; Punter, 2002; van den Berghe, 1998). Blondeau (2001) provides a particularly pertinent prediction: "*We can bet*

✉ Felix Bekemeier
felix.bekemeier@unibas.ch

[1] Faculty of Business and Economics, Center for Innovative Finance, University of Basel, Peter Merian-Weg 6, 4002 Basel, Switzerland

that the Internet, for example, will be a mature technology within the next ten years and that it is changing the picture both in terms of demand and insurance risk" (Blondeau (2001), p. 151).

Today, the insurance industry faces a new challenge in the form of decentralized finance (DeFi), which introduces risks that are intangible and cannot be assessed using conventional actuarial methods. Unlike traditional insurance policies, DeFi insurance centers around digital contracts known as "smart contracts." At present, DeFi insurance is in its nascent stage, with considerable scope for further development and exploration.

Figure 1 depicts recent developments of the total value locked (TVL)[1] in DeFi and its share covered by insurance policies of Nexus Mutual (Karp & Melbardis, 2017), one of the leading protocols for smart contract insurance as of early 2022.

The level of coverage exhibited significant variability, ranging from less than 0.01% to slightly below 1.6% during 2020 and 2021. A notable downward trend can be observed, starting from the second quarter of 2021 until the beginning of 2022. In January 2022, Nexus Mutual covered approximately 0.7% of all assets locked in DeFi. One reason for the strong downward trend of the TVL coverage ratio might be the continued exponential growth of TVL relative to the risk-bearing capital provided. While the TVL was still approximately USD 17 billion in November 2020, over USD 250 billion was observed for November 2021 (Statista, 2021), depicting a growth in no way comparable to Nexus Mutuals capitalization.[2]

On May 12, 2021, Nexus Mutual recorded its peak annualized premiums in force, reaching approximately USD 33.6 million.[3] This amount corresponds to approximately 20% of the non-life gross premiums written in Nicaragua in 2020, which is the country with the lowest non-life written gross premiums globally, as illustrated in Table 1.

In comparison to the top 5 countries in terms of written non-life premiums, the premiums written by Nexus Mutual are relatively insignificant. Despite the exponential growth of insurable risk in DeFi, the contribution of DeFi insurance to the global non-life insurance market remains limited. However, an examination of historical data regarding previous exploits within various DeFi settlement layers shows the significance of potential risks. Hence, the practical importance of risk transfer within DeFi increases alike. This paper aims to start a discussion on selected aspects of DeFi insurance by combining taxonomical considerations and empirical observations, and contributes threefold to its exploration. First, it presents a brief theoretical introduction to DeFi insurance in comparison with traditional lines of insurance. Second, it outlines a taxonomical framework for an advanced understanding of currently operating insurance protocols and potentially transferrable risks associated with DeFi. Third, it discusses the inherent insurability of a subset of those risks, smart contract risks, as the empirically most prevalent DeFi risk.

[1] TVL describes the total monetary value of crypto assets deposited in a DeFi protocol or on a specific settlement layer, see DeFiLlama (2022).

[2] The dashboard of Nexustracker (2022) delivers further insights into relevant key performance indicators.

[3] According to the data of Nexustracker (2022).

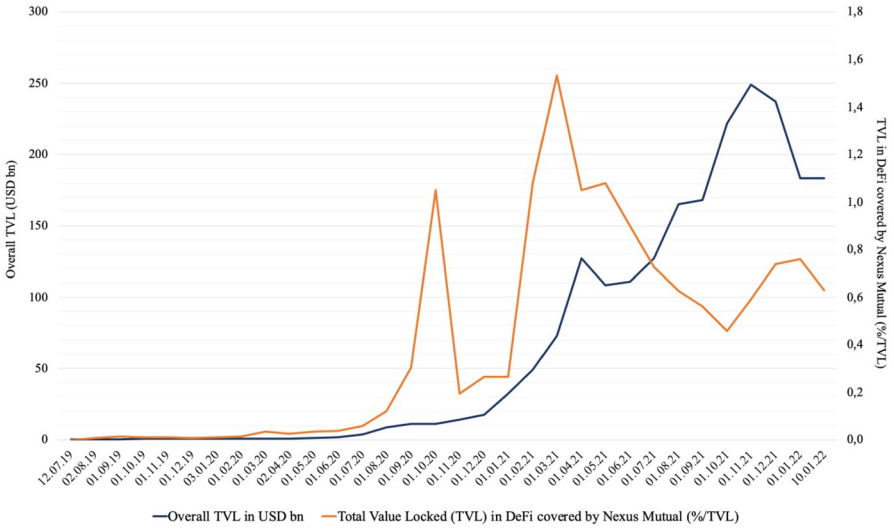

Fig. 1 Overall TVL and TVL in DeFi covered by Nexus Mutual in %/TVL (data sources: Nexustracker (2022), DeFiLlama (2022))

Table 1 Non-life insurance business written in selected OECD and non-OECD countries in 2020 (data source: OECD (2022))

Top-5	Gross premiums in USD m	Lowest-5	Gross premiums USD m
United States	1,565,690	Nicaragua	162
Germany	153,844	Bolivia	309
France	126,740	Honduras	426
Japan	91,437	El Salvador	490
Korea	86,688	Iceland	495

This study primarily concentrates on the DeFi asset category of utility tokens and the associated interaction with smart contracts, but also on payment tokens in direct connection with the settlement layers on which DeFi applications are executed. It is important to note that other asset categories such as security tokens, non-fungible tokens (NFTs), and other on-chain[4] asset types, particularly those associated with real-world commodities, which have gained significant attention in recent months, are beyond the scope of this analysis.[5]

[4] "On-chain" is commonly referred to as transactional activities that occur directly on the respective settlement layer. They are typically transparent for all network participants, and immutably stored on the blockchain. The opposite is "off-chain", which refers to activities outside the blockchain itself, typically involving external systems and processes. For further information, cf. CoinDesk (2023).

[5] Noteworthy developments can also be observed in these areas, although they are at present more likely to be served by traditional insurers with various forms of organization and degrees of decentralization. A recent example is the integration of NFT insurance into the cyber portfolio of Mitsui Sumitomo, see Cointelegraph (2022).

Following a brief introduction to related works in Sect. 2, Sect. 3 offers a focused thematic introduction that enables an in-depth discussion of DeFi insurance in subsequent sections. Section 4 presents a taxonomy that aligns with a prototypical insurance value chain and compares risk transfer in DeFi to traditional insurance lines. Section 5 delves into the examination of the general insurability of smart contract risks, in which the new taxonomy serves as a framework for this analysis. Finally, Sect. 6 concludes the study by summarizing the findings and highlighting potential areas for future research.

2 Related work

This paper is an interdisciplinary contribution at the intersection of insurance theory, computer science, and finance. Its primary objective is to address the research gap in the relatively unexplored domain of DeFi-inherently organized risk transfer facilitated through DeFi protocols. The contribution aligns with the growing body of literature dedicated to exploring DeFi, often referred to as the "lego of finance" (Popescu, 2020). Schär (2021) offers a comprehensive description of DeFi's architecture, providing valuable insights into the current market landscape and its rapid development, while also addressing the overall risk perspective. Werner et al. (2021) deliver a delineation of the DeFi ecosystem regarding different dimensions, and outline open research challenges.

First, this analysis focuses on the transferability of risks associated with smart contracts, which encompass a wide range of consumer-oriented financial applications deployed on permissionless blockchain technologies (Jensen et al., 2021). Recent years have witnessed several discussions not only on the opportunities presented by smart contracts (Chen & Bellavitis, 2020), but also on their associated risk profiles (Chang et al., 2022). Atzei et al., (2017) provide an overview of past attacks on blockchain, EVM (Ethereum Virtual Machine), and the Solidity programming language, emphasizing the discrepancy between intended behavior and actual execution of smart contracts. Furthermore, various mitigation measures, such as formal verification (Almakhour et al., 2020; Osterland & Rose, 2020; Singh et al., 2020), game-theoretic methods (Zhang et al., 2019), and multi-bot approaches (Viglianisi et al., 2020), are already analyzed in literature. The inherent capability for risk transfer within DeFi remains an important consideration, especially considering the overall systemic fragility (Lehar & Parlour, 2022) of DeFi.

Second, the risks associated with DeFi partially overlap with those of general cyber and IT risks covered in typical cyber insurance. The main findings from seminal works on IT and cyber insurance, such as Richards (1986), Biener et al. (2015), Bodin et al. (2018), Kshetri (2020), and Peters et al. (2018), help to identify the precise differentiators between these fields.

Third, considering the organizational structure, DeFi risk transfer embodies a distinct technology-driven form of decentralized insurance, as conceptualized by Feng et al. (2023), operating without the need for legal recourse or regulatory

intervention. The organizational perspective presented in this paper is not an isolated concept, but rather aligns with the notion of emerging competitive financial markets and the associated analysis of risks and opportunities (Auer et al., 2023).

Fourth, this contribution is concerned with the question of the extent to which the risks discussed can be classified as insurable in the inherently existing organizational form of insurance protocols. The discourse surrounding the insurability of risks is addressed in earlier publications (Berliner, 1982, 1985; Mehr & Cammack, 1976; Schmit, 1986). This paper extends the debate by emphasizing an overarching perspective on the insurability of smart contract risks. The discussions on insurability lie at the core of fostering a harmonized societal progress (Stahel, 2003).

Fifth, the objective of this paper is to provide a structured framework for understanding the intricacies of DeFi-related risk transfer within a specific subset of risks. It contributes to the growing body of literature addressing DeFi-inherent risk transfer, alongside works by Cousaert et al. (2021) and Nadler et al. (2022). However, it is important to distinguish this paper from contributions that discuss smart contracts as a supportive element within broader traditional insurance domains. Contributions such as those by Kar and Navin (2021), Abramowicz (2019), and Gatteschi et al. (2018) explore the integration of smart contracts in traditional insurance contexts with a wider scope.

3 Well-known principles in a different guise

Early forms of *solidarity-based risk mitigation* were prevalent in different social communities, such as trade associations and guilds, centuries ago (Swiss Re, 2017). The beginnings of modern insurance date back to the Great Fire of London in 1666 (Wuthrich, 2013). Today, insurance plays a decisive role in modern economies, facilitating the expansion of the economic possibilities of individuals and companies through better risk control and financial security, as discussed by Han et al. (2010), Liedtke (2007) and, in a solidarity-related sense, by Lehtonen and Liukko (2011). With the progressive development of monetary values and commercial activities in DeFi, risk transfer is increasingly demanded within the same domain. In line with contributions such as Schär (2021), DeFi is a collective term describing the establishment of code-based alternative financial markets based on various blockchain settlement layers. The main goal of DeFi is to reduce intermediaries in financial markets, to increase the authenticity and speed of monetary transactions, as well as to reduce frictions and improve the accessibility of financial services.

Schär (2021) depicts a comprehensive overview of all DeFi layers, including an economic perspective on the main DeFi applications and mechanisms. All individuals interacting with DeFi expose their digital assets (token) to a complex risk profile related to smart contracts. Smart contracts are a form of digital contracts deployed on a blockchain. Similar to traditional understandings, insurance and risk-hedging mechanisms in DeFi are intended to aggregate individual risks into larger liquidity pools. This increases the risk-bearing capacity of individuals and economic entities. Hence, DeFi insurance overall can be described as a well-known concept regarding purpose and economic relevance but is now hidden in a new guise in terms of the

underlying risk transfer mechanism and insurance organization. Insurance protocols focus primarily on DeFi-inherent risks, but real-world risks such as flight delays and crop losses are also made insurable on-chain, such as those provided by Etherisc (2022).

3.1 Differentiation of DeFi insurance from traditional insurance lines

To disentangle the inherent novelty of DeFi insurance, the following section compares the policy-related characteristics of two major lines of traditional insurance, which address physical and digital risks related to information technologies, with DeFi insurance. Specifically, this analysis will delve into the question of why conventional IT insurance policies or cyber insurance policies currently do not or cannot take into account the newly identified risk vectors. In addition to this product-specific dimension, the degree of technological reliance of DeFi insurance is assessed and delineated from InsurTech projects as described by Neale et al. (2020). The product-based analysis considers three dimensions: the degree of formalization, risk exposure, and risk concentration, as shown in Fig. 2.

The *degree of formalization* refers to the organizational structure of the risk transfer, specifically whether it is managed through a central entity (the insurer) or through a decentralized form of organization. *Risk exposure* depicts whether predominantly real-world risks or digital-inherent risks are insured. *Risk concentration* indicates whether a specific central entity is affected by the risk or if the risk impacts various decentralized infrastructural entities.

Compared to conventional IT insurance as described by Richards (1986), DeFi differs in all three dimensions. Richards (1986) provides a list of insurable risks related to IT infrastructure, mentioning physical exposures such as access to the computer room or physical data backups as the most common central points of failure. DeFi insurance, on the contrary, deals solely with token-based digital assets that are primarily exposed to a complex digital risk profile, mostly decoupled from any physical possessions. This leads to differences in both risk concentration and risk exposure. Regarding the degree of formalization, in most cases, it is not possible to identify a liable legal entity responsible for claims settlement, as discussed in Sect. 4. In DeFi, transactional parties interact with each other through "on-chain" smart contract ecosystems, rather than through the legally secured and standardized structures found in conventional IT insurance.

Compared to cyber insurance, in line with the understanding of Biener et al. (2015), DeFi insurance shows crucial differences in two dimensions, as will be described with reference to Table 2.

Cyber insurance incorporates the fact that physical hardware, such as computers, encounters additional digital risk profiles and digital attack vectors, following high levels of connectivity (Biener et al., 2015).

A common denominator of cyber insurance and DeFi insurance is related to risk exposure. Both lines cover risks induced by digital attack vectors, although the attacks on infrastructures typically protected with cyber insurance potentially entail

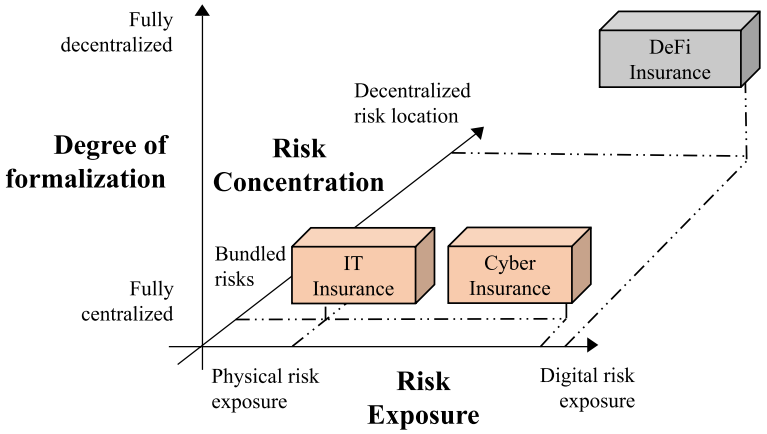

Fig. 2 Classification of digital insurance policy types

Table 2 Comparison of organizational parameters between cyber and DeFi insurance policies

	Cyber insurance	DeFi insurance
Insurable object	Hard- and software-related risks and associated processual or human components (Biener et al., 2015; Richards, 1986)	Assets stored in (self-)custodial wallets and assets operationalized through or locked in smart contracts
Premium determination	Centralized actuarial/statistical assessment by insurer (i.e., considering extreme value theory models such as in Eling and Wirfs (2019))	Decentralized premium determination (judgment-rated, prediction markets)
Policy distribution	Established insurance distribution channels and centralized marketplaces	Decentralized marketplaces facilitated through different insurance protocols

more severe secondary implications of a physical or digital nature.[6] This aspect will be further examined in Sect. 4, as it is evident that certain risks within the layer structure of DeFi are inherently encompassed within cyber policies.

A significant difference between the two lines of coverage is the degree of formalization, as well as the risk concentration. Formalization refers to "*the act of giving something a fixed structure or form by introducing rules*" (Oxford Learners Dictionary, 2023). In the context of insurance, this means above all clear insurance policy

[6] Considering a power grid controlled and protected by sophisticated IT systems as an example, where an attack via digital vectors would also have enormous physical consequences, i.e., widespread power outages.

definitions and organizational structures, as well as, if applicable, a sound regulatory framework. Some risks in DeFi could arguably be categorized within cyber insurance policies, commonly found in the portfolios of most of the world's major insurers. However, insurance against new DeFi-inherent risks is not yet broadly[7] offered by centralized insurers in the form of standardized products and, thus, mostly depends on informally organized, decentralized insurance protocols including internal and external dependencies. Risk transfer takes place in exactly the same environment in which the risks occur. For example, one of the main barriers to the replication of an existing policy line such as cyber insurance products in DeFi, or more generally for traditional insurers to offer coverage for DeFi-inherent risks, is the strong operational change required by the inherent characteristics of decentralized, public settlement layers such as Ethereum. Risk transfer for those inherent risks, on-chain, does not necessarily require (or even tolerate) a centralized insurance company, neither for premium determination nor for policy distribution.

Governance and sovereignty over insurance protocols usually require a decentralized design to be accepted by the community. This allows risk transfer at the level of protocols and, most importantly, facilitated and verified by the same cryptographic mechanisms as the insurable objects and associated interactions with smart contracts. Furthermore, the actuarial evaluation of DeFi risks poses a challenge for traditional insurers primarily in terms of the lack of historical data. Historical data are not available in sufficient length and detail. The most prevalent risk, smart contract risk, is also one of the most complex risks to be transferred, as Sect. 4.2 will outline. Overall, the result is a less formalized and decentralized market for risk transfer from the perspective of a traditional insurance understanding. Furthermore, corresponding legislation for DeFi insurance has not been established. Therefore, there is no key level of formalization either from the perspective of the risks covered or from the perspective of the controlling framework.

Risk concentration varies as well. In terms of cyber risks, mostly centralized elements, such as database systems, control systems or other risk locations at the interface between hardware and software, are insured. On the other hand, risk transfer in DeFi focuses on insuring smart contract risks within fully decentralized and public infrastructures such as the Ethereum blockchain. These infrastructures typically offer a high level of anonymity for both infrastructure and protocol users. In most cases, except for user wallets and crypto asset balances associated with their public keys or a smart contract account, no central risk location can be determined. In these scenarios, the only certainty lies in the fact that engaging with smart contracts exposes individual users to potential risks, specifically pertaining to token loss.

Finally, DeFi insurance sets itself apart from *InsurTech* ventures. Taking common definitions of InsurTech into account, DeFi insurance could be seen as a form of "disintermediary" InsurTech. Neale et al. (2020) describe a particular strategy type of InsurTech, the "*disintermediaries*", as "[…] *companies that compress the*

[7] There are isolated movements in the market, such as Chainproof as one of the first regulated smart contract insurers, among others under the backing of SOMPO and the reinsurance of MunichRe, see Bloomberg (2022). However, there are currently no substantial indications of a broad or standardized adoption of these policy offerings by traditional insurers.

distribution chain, bypassing one or more parties in the insurance transaction" (Neale et al., 2020, p. 68). The operations of decentralized insurance protocols could fall into this category by definition since DeFi protocols offer, similar to the description of Neale et al. (2020), a risk exchange for non-complex, potentially high-volume risk transfers with automatic valuation of the risks. This will be further described in Sect. 4. However, DeFi insurance also changes the fundamental nature of risk transfer and pricing in these marketplaces due to the high degree of operational and governance-related decentralization. This increases both the complexity and the lack of replicability of the offered policies, apart from the independence from centrally organized transaction parties. Therefore, DeFi could represent a further development rather than a known form of InsurTech.

Hence, from a theoretical point of view, the inherent novelties of risk transfer within DeFi, and associated insurance capabilities compared to traditional lines of insurance as well as known forms of technological innovation in insurance, are manifested by both the prevalence of new risk profiles and different operational settings and requirements.

3.2 A common fate: lack of historical data

In addition to the previously described differentiating features from established insurance lines, risk transfer and management in DeFi insurance entails a noteworthy commonality with operational risk management as categorized by Chorafas (2004). Both risk types show a crucial dependency on historical data to effectively assess and mitigate risk. As DeFi is a relatively new field, there are limited historical data points available to accurately assess risks. This lack of historical data in DeFi insurance makes it difficult to establish reliable actuarial models and pricing mechanisms, and demands alternative forms of risk and claim assessment. Analogous to DeFi insurance, a lack of comprehensive historical data has been affecting risk management related to operational risk, as described earlier by Fontnouvelle et al. (2003). Historical data are critical for operational risk management to analyze past events and understand their frequency, severity, and potential impact on business operations. While methods to mitigate the associated problems with respect to operational risk suggest, for example, the inclusion of external data (Guillen et al., 2007) or the use of (alternative) modeling such as Bayesian networks (Cowell et al., 2007), DeFi relies primarily on subjective methods and prediction-market-like structures, as presented in the following sections, especially in line with Karp and Melbardis (2017).

3.3 Market overview

DeFi protocols to date are neither regulated nor can be considered economic entities. Rather, most of the protocols available to date resemble decentralized risk marketplaces and mutual structures in various forms. Hence, those protocols might even represent a manifestation of a phenomenon termed "bancassurance" that is characterized by O'Hare (1994). At its core, it suggests a new era of competition for

insurers from non-traditional entities. In the following section, current protocols are discussed in more depth. On the one hand, we describe risk transfer products offered by current insurance "providers" in DeFi. On the other hand, we describe the commercial development of the market-leading protocol Nexus Mutual (Karp & Melbardis, 2017) using empirical data on key insurance metrics.

Table 6 in the Appendix shows a selection of currently active insurance protocols. Looking at the competitive landscape, the number of insurance protocols is rather small, whereas the range of products shows a significant level of diversity, including direct coverage, primarily against smart contract exploits, oracle[8] risks, counterparty risks, and price risks. Regarding risk assessment, almost all protocols require risk underwriters to stake protocol governance tokens or to provide dedicated liquidity for certain insurance liquidity pools. This implies that a consortium of risk underwriters, utilizing their own capital, assumes liability for the risks, thereby distributing the risks among the members. In terms of claim assessment, some protocols rely on automated forms using a combination of oracles and predefined triggers and actions, facilitated through smart contracts. Other protocols rely on centralized or decentralized subjective claim assessments. Both risk and claim assessment are described in more detail in Sect. 4.1.

Nexus Mutual has long used a hybrid model in terms of the organizational form: Nexus was a company limited by guarantee in the UK[9] with approval by the Financial Conduct Authority (Bank of England) to use the word "mutual" in the company title, but at the same time operationally managed by its members under a decentralized governance structure on a smart contract basis. In terms of liquidity and economic success of the concept, the protocol recorded strong growth towards 2021, as shown in Table 7. Currently, it operates as a DAO without any legal recourse.

Table 7 compares key economic metrics of Nexus Mutual as of December 2020 with December 2021. Denoted in the relative token amount, the protocol shows remarkable growth of both the insurance organization in terms of active cover amount (+165%), premiums (+202%), as well as of community participation, expressed by total amount staked (+216%) and staking rewards (+287%). Similarly, capital efficiency, a crucial indicator for the operational economic efficiency of the protocol, significantly increased (+45.5%). Furthermore, the P/B ratio fell by approximately 57%, indicating, from a risk perspective, a decrease in market risk exposure. The strong scaling in terms of risk mass and available cover is therefore observable as an increase in absolute profits but at the same stabilization of market risk exposure. Table 8 refers to the economic dimension related to individual cover projects. For example, Nexus Mutual has an average project size in terms of active cover of USD 7.8 million at the end of 2021, while the average premium income for these projects is USD 361,000. At the same time, the average claim amount is USD

[8] An oracle is a technical construct that enables off-chain information (e.g., weather data for specific coordinates) to be used on-chain, e.g., for utilization in smart contracts, cf. Ethereum (2023).

[9] This applied at the time of the first working draft (February 2022). In the context of the special resolution "project wartortle execution", a dissolution of the official legal status and the conversion to a decentralized autonomous organization (DAO) as a private interest foundation in Panama has been executed. Nexus Mutual now switched to a second version of the protocol (May 2023).

235,000, indicating an imbalance between the individual risks that could potentially materialize and the economic benefit. The total surplus of the protocol is on average approximately USD 950,000.

The data show remarkable capital movement related to DeFi-inherent risk transfer. However, in addition to the DeFi native offering, some protocols aim at insuring "real-world" risks on-chain without insurance intermediaries in traditional forms, such as Etherisc (2022) with crop and flight delay insurance. This creates new forms of competition in traditional insurance segments. While the latter is not the focus of this work, it shows a notable trend that traditional insurers should keep in mind. Individual projects, such as Nexus Mutual, show exponential growth rates and strong capital utilization while covering completely new risk profiles and should accordingly also be assessed from the perspective of traditional finance intermediaries.

4 A taxonomical framework for DeFi-inherent insurance

This section presents a taxonomy that organizes the fundamental elements and processes of risk transfer specific to DeFi. By considering various aspects of insurance organization and risk transfer, a comparative analysis between traditional approaches and DeFi-specific insurance concepts will be conducted. Additionally, the significance of these differences for the insurability of DeFi will be discussed in subsequent Sect. 5. Moreover, the section highlights the substantial reliance of risk transfer in DeFi on decentralized organizational roles and external dependencies for risk and claim assessment.

4.1 On the insurance organization

Prior works discuss that different organizational forms can control different internal stakeholder conflicts. Pottier and Sommer (1997) postulate that stock insurance companies are better at resolving owner-manager conflicts, whereas mutual forms are better at managing owner-policyholder conflicts. In DeFi, the governance and management of the insurance organization is, at its core, fully decentralized, both at the level of the *organizational institution* and at the level of the *settlement logic*.

First, the decentralization of the insurance institution will be described with the help of Fig. 3. It provides a comparison of the traditional insurance organization and DeFi insurance protocols as operated today based on an empirical screening of the governance structure of different insurance protocols.[10]

In traditional insurance, primarily two parties interact with each other: the insurant and the insurance company. All operational processes, such as premium determination or reimbursement decisions, are internal to the insurer and handled through centralized functions, for example, reimbursement decisions made by a claims department, as described in Olivieri and Pitacco (2011). In DeFi, the

[10] The list can be found in Table 6. Many more insurance protocols are potentially deployed and used, but most do not indicate significant usage levels (relevant TVL levels), or only aggregate existing insurance offerings. These are not explicitly listed, as the list cannot claim to be complete.

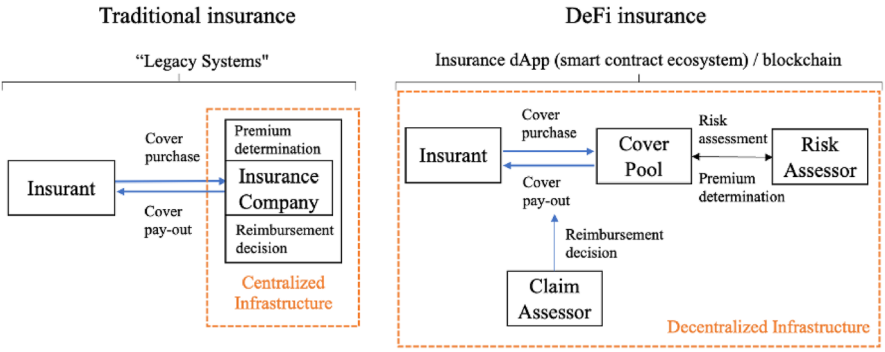

Fig. 3 Comparison of the traditional insurance organization with the organizational structure in DeFi, own figure

insurant most often obtains cover directly from a decentrally organized cover liquidity pool. Hence, operationally decisive roles are no longer centralized departments within the insurance company. Instead, consortia of claim and risk assessors, such as those described in Karp and Melbardis (2017), conduct claim and risk assessments through the lock-in (staking) of a dedicated amount of tokens in exchange for voting rights. The associated incentives and interests are initially located at the subjective level, but the roles are nevertheless partially interdependent with a 1:*N* dependency structure.

Risk assessors, as characterized by Karp and Melbardis (2017), use a set of public and private information to quantify the risk for a smart contract exploit and participate in the provision of a cover liquidity pool by staking their own capital. In return, they eventually participate in premium payments. This function is therefore most comparable to the traditional underwriting process for risks and must ensure that the required liquidity fits the risk profile of each smart contract considered for cover. Three major forms of *risk assessment* are observable throughout the protocols screened in Table 6. *Staking-based risk assessment*, in which decentralized agents with a personal capital stake carry out a risk assessment; *expert-based risk assessment*, in which dedicated experts with or without personal capital involvement carry out a risk assessment; and *model-based risk assessment*, in which insurance pricing is supplemented by objective risk models. Derivatives-based price risk-hedging options are a special case. Here, staking is first and foremost about *risk-oriented liquidity provision (LP)*, which is either specified according to an alpha factor or falls into a simple long or short logic, where the liquidity providers either bet on falling or rising prices mid- to long term but do not specifically insure underlying technical risks such as smart contract risks.

Claim assessors replace centrally organized claim departments and participate in different forms of voting currently practiced throughout the major insurance protocols in Table 6. This voting determines the reimbursement decision regarding claims made by insurants. First, in *community-based voting*, the voting of several claim assessors takes place according to a predefined scheme and defined quorums. In this context, the participation condition for each claim assessor is similar to risk

underwriting. To obtain voting rights for claim assessments, a claim assessor must provide a specific number of tokens to the protocol (lock-in/staking) and receives a return or a penalty payment depending on the voting behavior. Second, in an *expert-based form*, dedicated experts review claims and propose a decision based on their expertise and information. Both forms induce a situation in which the insurant's decision to purchase cover is endogenously dependent, since the risk assessors stake determines the insurance premium, and claim assessors decide on the pay-out of a claim. Moreover, indemnity payment execution relies on technical guarantees in smart contracts instead of legal guarantees. Third, *automatic payouts* are enabled through trigger definitions and oracles that can verify if pay-out requirements for an insurance policy are fulfilled. This is mostly comparable to a parametric insurance contract. However, no distinction is made between different types of loss adjusters, such as company adjusters, adjustment bureaus, independent adjusters, or public adjusters, as Mehr and Cammack (1976) discuss related to traditional insurance organizations.

Both roles involve a significant reliance on subjective elements within the insurance organization. It is crucial that losses and risks associated with smart contracts are, at the very least, observable through a set of public information. This enables individuals to develop informed beliefs and make staking decisions based on their subjective risk expectations. The advantage of subjectivity in this context is difficult to modify. Objective on-chain data, accessible to all users, provides orientation. However, the evaluation of this information and its enrichment with off-chain data, such as discussions in online forums or media reports, remains entirely individual. Overall, a certain degree of subjectivity must be allowed to ensure the insurability of a fundamental set of risks, as will be further discussed in Sect. 5. At the same time, the organizational structure of DeFi insurance is only partially comparable to traditional understandings. Risk transfer in DeFi is accompanied by additional risk participation, requiring decentralized voting through a collective of anonymous users performing risk and claim assessment and inferring a lack of objective risk assessment due to data scarcity. Only by incorporating collective intelligence can risks be insured for which no historical information of any kind has been available to date and for which classic actuarial methods cannot be applied. To provide economically feasible cover products, the risks must be objectively observable and verifiable. Idiosyncratic risks with components of private information remain difficult to insure.

Second, the *settlement logic* of risk transfers, which consists of both the infrastructure used and the contractual settlement process, changes. In traditional insurance, the insurance policy is typically a contract between the insurer and the insured, precisely outlining terms and conditions as well as the associated coverage. The insured pays premiums in exchange for the insurers' promise to cover specified risks. In the case of a loss event, a claim is filed through an ex ante agreed upon communication channel, and the insurant provides evidence of the loss.

Regarding the *infrastructure used*, settlement takes place entirely through centralized infrastructure and legacy systems. Traditional insurance relies on centralized infrastructure, in which insurance companies act as intermediaries underwriting policies, assessing risks and managing the claims process. In particular, insurance companies typically use their own proprietary software systems or third-party insurance

platforms to manage policy administration, underwriting, claims processing and other operational aspects. DeFi insurance operates solely on decentralized blockchain platforms, in which smart contracts govern all insurance policies and related processes. Blockchain technology and smart contracts are leveraged to enable transparent, cryptographically secured, and decentralized transactions.

Regarding the *contractual settlement process*, traditional insurance mostly follows a discretionary settlement approach. Hence, the insurance company has discretion in evaluating claims through manual or (semi-)automated processes, and the settlement is typically based on policy terms, coverage limits, deductibles, and any applicable exclusions. DeFi insurance follows algorithmic settlement principles. The settlement amount in DeFi insurance is, in most cases, predefined within the insurance contract. It is based on objective parameters and data, such as the occurrence of a specific event, the data provided by oracles (external data sources), or a positive pay-out vote by a consortium of claim assessors. For any given trigger, claim evaluations and potential settlements are conducted according to the predefined rules, fully decentralized and partially automated.

In addition to the differentiating features discussed earlier, DeFi-inherent risk transfer offers comprehensive organizational benefits that require thorough assessment in terms of their relevance and applicability within the specific context. At the core of DeFi risk transfer are smart contracts as self-executing agreements governed by predefined rules and conditions (Ante, 2020). While risk transfer protocols themselves may, in certain situations, represent the risk they aim to insure against, smart contracts collectively provide a unique opportunity for cryptographically secured risk transfer that is executed as intended by all parties involved. This mitigates trust issues and simultaneously reduces transaction costs for the involved parties. The programmable nature of smart contracts enables customization to align precisely with the framework conditions of risk transfer, as described throughout this section. Furthermore, the replication of peer-to-peer insurance principles within these protocols contributes to the reduction of transaction costs. DeFi-inherent risk transfer operates without any central contracting party other than the smart contracts themselves and the governance constructs of the protocols.

In summary, users of DeFi-inherent risk transfer also benefit from enhanced transparency and auditability. All token or asset movements as well as smart contract interactions are traceable on-chain, and the outcomes are securely recorded in an immutable manner. Depending on the specific application context, this can be a crucial advantage in reinforcing trust and transparency within an insurance framework that holds significant importance. Section 5 will reevaluate the organizational advantages in regard to the insurability of DeFi-inherent risks.

4.2 On transferrable risks

The initial stage of any insurance undertaking involves the identification of risks that are insurable and financially viable for insurers to underwrite. However, in the context of DeFi, this process gains complexity through the multilayered risk profile

faced by individuals engaging with DeFi. While this paper does not delve into an exhaustive examination of all individual risks, this section offers a concise overview of the primary risks associated with DeFi. Tables 9, 10, 11, and 12 depict empirical data on past exploits in the context of major DeFi blockchains, clustered by vulnerability categories and affected layers, until December 2021. The data set also includes some of the largest DeFi hacks in history, e.g., the PolyNetwork hack from 2021, exposing over USD 611 million, and a Compound Finance vault bug, which caused a loss of approximately USD 150 million. The individual sources (see notes to Tables 9, 10, 11, and 12) provide more details for the reader on specific events.

Figure 4 proposes, based on these empirical observations, an indicative DeFi risk cluster, supplemented by theoretical considerations for each layer. Furthermore, the matrix provides insights into the current definitory coverage of each risk cluster.

The cluster "natively insurable" indicates that DeFi protocols offer a dedicated risk transfer mechanism for that particular risk. On the other hand, for risks clustered as "not natively insurable," DeFi-inherent risk transfer mechanisms are not yet offered. In the third cluster, certain risks may align with the definitions outlined in cyber insurance policies, particularly those specified in Biener et al. (2015). The fourth cluster depicts risks primarily known from traditional finance, such as liquidity and counterparty risks.

The *exogenous* dimension of risks includes environmental influences and exogenous shocks in a broader sense. Exogenous risks arise from the interactions of DeFi with the external economy, with risks including oracle risks, infrastructure risks, regulatory risks, and others. These risks are particularly prevalent when information is to be transferred between the two worlds or regulatory or legal claims are to be asserted. *Endogenous* risk factors refer to risk profiles located within different technological layers of DeFi as described by Schär (2021), whose understanding of each

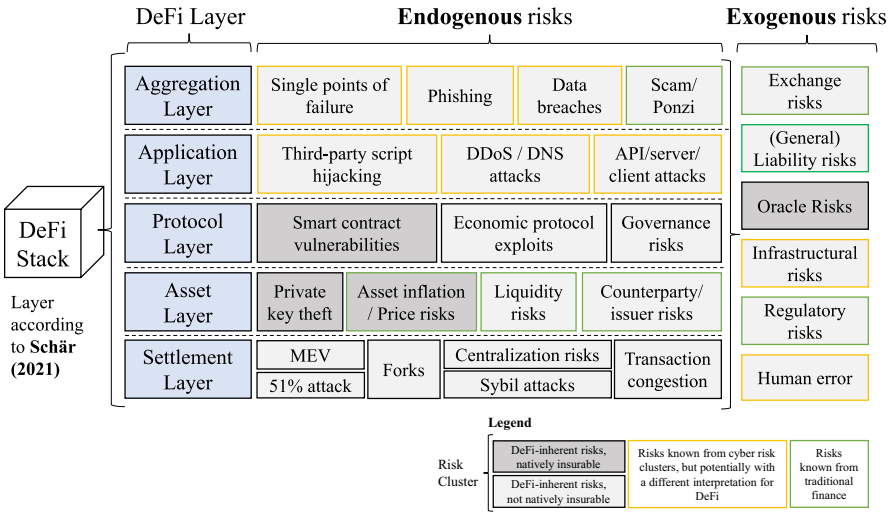

Fig. 4 Risk matrix for DeFi risks, own figure

layer is supplemented with a short discussion of layer-specific risks below. The clear distinction of risks depicted in the figure may not always be feasible in practice. However, in retrospect, incidents typically allow for the identification of a distinct root cause. In addition, it should be noted that the risks presented may have definitional overlaps with the understanding in the traditional finance literature as well as a DeFi-specific interpretation, but that the understanding of risks in Fig. 4 is based on a DeFi-specific root cause of risk manifestation.[11]

The *settlement layer* harbors various risks such as 51%[12] and sybil attacks[13] and, due to its composability structure, also has a significant impact on the functionality of the other layers. Another risk at this level is the issue of maximal extractable value (MEV),[14] a Pareto-inefficient surplus generation strategy of miners, with secondary problems such as those described by Daian et al. (2020). In addition, cross-chain[15] vulnerabilities prevail in the overall picture, which arise from cross-chain protocols connecting different settlement layers. This layer has the greatest DeFi inherency in terms of risks due to the technological characteristics of the blockchain(s) underlying DeFi. However, coverage of these risks in DeFi does not exist and would not be reasonable, as adverse events at this level would also directly affect the functioning of the insurance protocols. At the same time, none of these risks has been previously addressed in cyber insurance or in connection with financial markets in general.

The *asset layer* is primarily affected by a new risk cluster connected to asset ownership and transfer, in particular, private key[16] risks that can influence cryptographic sovereignty over DeFi assets. However, risks in interaction with the counterparties of the asset transfers (counterparty/issuer risk) or liquidity, and inflation and price risks, are also observed related to this layer. These are already familiar from traditional finance, but are manifested in DeFi with a new interpretation and new framework conditions.

[11] One example for such an overlap is the category asset inflation/price risks. The result of an asset inflation in DeFi is similar to inflation known within real economies, mainly a loss in purchasing power. However, the root cause is technically different compared to the real economy. In DeFi, inflation is often caused by a stablecoin de-peg, i.e., an event in which the value of a stablecoin develops significantly below its benchmark value. This in turn can have a root cause in the underlying smart contracts, in the counterparty risks such as the stablecoin custodian, or other factors. Furthermore, asset inflation could also occur due to oracle failures and other contract vulnerabilities.

[12] 51% attacks on a blockchain are performed by a consortium of miners, which are in control of more than 50% of the mining hash rate. They can interrupt the processing of new blocks, and thereby fundamentally intervene into the network's operation, cf. CFI (2023).

[13] Sybil attacks utilize multiple fake identities within a network to gain disproportional impact over a system or protocol, cf. Bybit (2022).

[14] Pending transactions are held in a so-called mempool until miners or validators validate the transaction and add it to the official chain. MEV includes strategies that add, exclude, or change the order of transactions to generate additional profit, cf. Daian et al. (2020).

[15] Cross-chain refers to a situation in which one blockchain network can exchange information with another blockchain in case they share similar underlying technological principles.

[16] A private key is a cryptographic component enabling a user to access their crypto assets assigned to a wallet, i.e., public key, cf., e.g., the different definitions of NIST (2023).

The *protocol layer* is one of the most important layers from an insurance perspective, harboring solely DeFi-specific risks, as this element is not found in traditional financial markets. Insurants in DeFi are always dependent on the functionality and exploit resistance of smart contracts according to the definition of Szabo (1996), either primary (for direct contract calls and interactions) or secondary (via the application or aggregation layer). Recent contributions depict in much detail the characteristics and security mechanisms of smart contracts (Ante, 2020; Atzei et al., 2017; Singh et al., 2020; Wohrer & Zdun, 2018). Overall, smart contracts represent a completely new dimension of complexity for the provision of insurance solutions. Other risks at the protocol layer include economic exploits and governance risks related to smart contracts. However, their root cause is potentially a code-based issue rather than a conceptual issue.[17]

The *application layer* is naturally influenced by common IT risks. These risks consist of third-party script hijacking with malicious code injections, distributed denial of service (DDoS) or domain name system (DNS) attacks, and general attacks on the server or on clients through application programming interfaces (APIs).

The *aggregation layer* inherently harbors risks from the application layer, which are amplified through this layer by various forms of interconnectivity. Risks on this layer include single points of failure, phishing, and data breaches as well as scam and Ponzi schemes through bundled and managed access to DeFi applications.

The risks on the aggregation and application layer show analogies to cyber risks in terms of their definitions and characteristics and are mostly not covered through DeFi-inherent insurance offerings to date. For example, protection against traditional DDoS attacks[18] falls within the spectrum of most cyber insurance policies and is not covered by any of the considered insurance protocols. Simultaneously, it becomes evident that certain aspects, specifically the protocol, asset, and settlement layers unique to blockchain, encompass new types of risks that have not yet been comprehensively addressed by existing insurance policies. While certain risks such as smart contract flaws and bugs are already considered natively insurable within the DeFi ecosystem, the insurability of risks associated with the settlement layer may not be straightforward, as the impacts of these risks are primarily observed on a transactional basis in the layers above. Exogenous risks also rarely fall within the scope of on-chain insurance protocols, with some exhibiting similar characteristics to elements of cyber insurance, while others represent residual risks such as regulatory risk. Oracles, on the other hand, are often considered since they are inherently linked to smart contracts and their behavior, allowing for a more precise definition of specific risks.

[17] A striking example is a bug in the Compound Finance lending protocol that occurred in 2021. A specific function related to a contract vault incorrectly triggered the distribution of governance tokens to wrong addresses via another vault, see CNBC (2021).

[18] In the context of DeFi, the concept of a DDoS attack can be interpreted in various ways. The traditional form of DDoS attacks, as illustrated in the figure, involves targeting specific applications on the blockchain and frontend applications connected to it. However, there are also crypto DDoS attacks that predominantly focus on the protocol layer, often referred to as transaction flooding, see, e.g., Halborn (2021).

Based on the current empirical observations presented in Tables 9, 10, 11, and 12, certain layers and types of risks emerge as notably prominent. Among the layers and blockchain networks examined, the most quantitatively significant layer in terms of losses within the analyzed networks is the protocol layer with up to 80.97% of losses for Ethereum, where smart contract vulnerabilities exhibit the highest occurrence of exploit volumes. Notably, flash loans, as elaborated by Qin et al. (2021), pose a recurring issue within this layer, accounting for significant loss shares (8.73%; 33.34%; 3.98%) in the ecosystem in almost all considered settlement layers. Furthermore, another strongly prevailing category (4.28%; 24.10%; 70.45%; 0.55%) is the loss, leakage, or theft of private keys located at the asset layer. When considering the distribution of maximum individual risks, the aforementioned risk types also hold significant relevance in assessing tail risks based on these initial data. Risk manifestations commonly associated with traditional lines of insurance, such as scams, phishing, and system-related attacks such as DDoS attacks, scams and Ponzi schemes, play a rather subordinate role.

When comparing the risk matrix depicted in Fig. 4 with the cover types offered by the providers listed in Table 6, it becomes evident that conceptually, only a part of the overall risk profile is DeFi-natively coverable to date, specifically smart contract risks, private key thefts, oracle risks, asset price risks, and counterparty risks. However, these risks account for the largest risk profiles in relative terms. Complementarily, the emphasis of current insurance protocols primarily revolves around addressing endogenous forms of risks pertaining to the asset and protocol layer. The next subsection discusses how these risks are priced.

4.3 On actuarial methods and premium determination

According to Borch (1985), an insurance premium must fulfill two main purposes. First, there must be *adequate compensation* for the insurer's acceptance of the transferred risk. Second, it must be *acceptable* to the insured. Hickman and Miller (1970) discuss early criticisms of insurance premium determination methods and provide related theoretical considerations. Tapiero and Jacque (1987) provide a formal link between insurance premiums and the expected cost of ruin in mutual insurance settings, which is helpful for assessing the fairness of premiums in a hybrid mutual insurance setting. Nendel et al. (2021) discuss the structure of premium principles in a general setting with model uncertainty.

Figure 5 compares the pricing structure for both lines of insurance, traditional and DeFi-based, starting with the traditional understanding according to Olivieri and Pitacco (2011).

In traditional (centralized) insurance markets, exogenous factors such as the statistical basis, the interest rate, and the profit and loss expectations of the insurer are, among other factors, used to determine an appropriate premium using ex ante defined formulas. Together with this determination, the market situation and

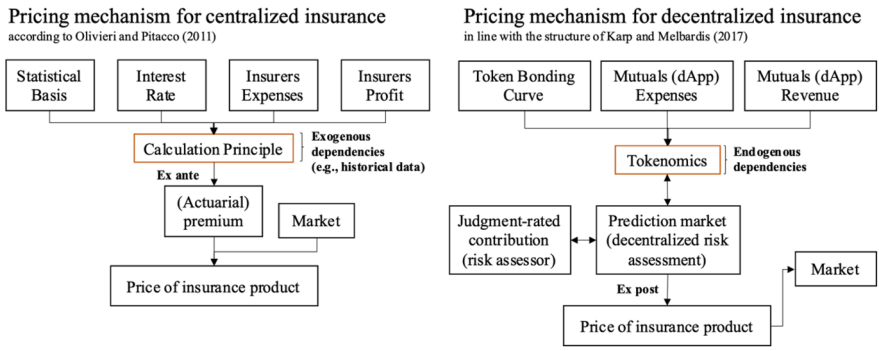

Fig. 5 Comparative analysis of the pricing mechanisms, own figure

demand-related metrics, i.e., competition and price sensitivity of customers, the cover premium is determined. Through this objective approach, fair premiums can be calculated, considering objective and historical data.

Pricing for decentralized insurance offerings follows a different approach, depending on the form of risk assessment described in Sect. 4.1. The model-based form of risk assessment closely resembles the traditional mechanism as described by Olivieri and Pitacco (2011) with a calculation principle defined exogenously and ex ante by the model. For staking-based and expert-based risk assessment, the pricing of the insurance contract is mostly determined endogenously and ex post via prediction markets for smart contract security, facilitated by risk assessors, or through a consortium of experts. The aim is to involve individual agents with relevant knowledge in the subjective risk analysis to determine an optimal premium, despite the scarcity of historical data and objective actuarial metrics.

Hence, the insurance premium for each offered smart contract cover is a judgment-based outcome, with the market which is a price taker and demand for insurance services being regulated through a token bonding curve at the protocol level. Karp and Melbardis (2017) provide a practical example for the endogenization of premium determination. The pricing mechanism of protocol version 1 (V1) can be found in the code repository of Nexus Mutual.[19] The cover price P_{β,T_i} for an individual insurant β with coverage amount $I_{\beta,T_i} > 0$ for a duration of $\Delta t > 0$ is given in a generalized form by

$$P_{\beta,T_i}\left(\sum_{\alpha=1}^{n} L_{\alpha,T_i}\right) = R_{T_i} \times (1+\delta) \times I_{\beta,T_i} \times \Delta t$$

$$\text{with} R_{T_i} = \max\left(\text{SRCL}, 1 - \left(\frac{\sum_{\alpha=1}^{n} L_{\alpha,T_i}}{\pi}\right)^{\frac{1}{b}}\right).$$

[19] The code repository of Nexus Mutual is available via https://github.com/NexusMutual.

Table 3 Variable characteristics in Nexus Mutual derived from NexusMutual Gitbook (2022)

Variable	Definition	Dependency type	Determination
P_{β,T_i}	Price of smart contract cover	Endogenous	Ex post
π	Low risk cost limit	Exogenous (defined in contract)	Ex ante
SRCL	Staked risk cost low	Exogenous (defined in contract)	Ex ante
δ	Surplus margin (loading factor)	Exogenous (defined in contract)	Ex ante
b	Bonding curve elasticity	Exogenous (defined in contract)	Ex ante
I_{β,T_i}	Insured token amount of agent β in for protocol T_i	Exogenous (chosen by insurant)	Ex post
L_{α,T_i}	Individual stakes by risk assessor α on cover liquidity pool related to insurable protocol T_i	Endogenous (supply and demand of risk capital)	Ex post

The staking factor $R_{T_i} > 0$ determines the premium via the (net) aggregate staking amount $\sum_{\alpha=1}^{n} L_{\alpha,T_i} \in \mathbb{R}$ provided by $n \in \mathbb{N}$ risk assessors for a specific insurable protocol T_i. $\delta > 0$ depicts a surplus margin. The actual premium is restricted to an ex ante defined interval. *SRCL* defines the lower bound ("*staked_risk_cost_low*" in the concept of Karp and Melbardis (2017)) of the risk factor which independently holds for sufficient stakes provided. Furthermore, the shape and elasticity of the bonding curve are determined through elasticity factor $b > 0$ and the low risk cost limit $\pi > 0$, the influence of which are explained in more detail below. Table 3 delivers more details on each variable.

The variables show differences regarding endogeneity and exogeneity, as well as their temporal determination ex ante and ex post protocol deployment. Initially, exogenous variables, which remain unaffected throughout the risk transfer process, are specified. Those variables, characterized by their static nature, are defined ex ante, i.e., before or upon deployment of the insurance protocol. Typically, modifications to these variables require decentralized governance decisions involving a specific quantity of governance token holders. This reflects the necessity of community-based decision-making for any truly decentralized insurance protocol. Conversely, endogenous variables, such as the risk factor, staking amount contributed by risk assessors and the cover premium, are established incrementally during the risk transfer process through the supply and demand of risk capital, and mostly ex post of the protocol deployment.[20] Only their provisioning rules and effects are specified ex ante within the smart contract structures. Now, we take a look at further dynamics of the premium determination. For a situation in which the risk factor has reached the lower bound, hence $SRCL \geq 1 - \left(\frac{\sum_{\alpha=1}^{n} L_{\alpha,T_i}}{\pi}\right)^{\frac{1}{b}}$, we obtain

[20] An exception from this categorical coherence is the insured token amount, which is determined within each request by a potential insurant ex post of the protocol deployment.

$$\frac{\partial P_{\beta,T_i}\left(\sum_{\alpha=1}^{n} L_{\alpha,T_i}\right)}{\partial\left(\sum_{\alpha=1}^{n} L_{\alpha,T_i}\right)} = 0.$$

For the following analysis, we particularly focus on the behavior of R_{T_i} within its ex ante defined interval; hence, we assume $\text{SRCL} < 1 - \left(\frac{\sum_{\alpha=1}^{n} L_{\alpha,T_i}}{\pi}\right)^{\frac{1}{b}}$. The first derivative for this interval is given as

$$\frac{\partial P_{\beta,T_i}\left(\sum_{\alpha=1}^{n} L_{\alpha,T_i}\right)}{\partial\left(\sum_{\alpha=1}^{n} L_{\alpha,T_i}\right)} = -\frac{(1+\delta)\times I_{\beta,T_i}\times \Delta t\times\left(\frac{\sum_{\alpha=1}^{n} L_{\alpha,T_i}}{\pi}\right)^{\frac{1}{b}}}{b\times\left(\sum_{\alpha=1}^{n} L_{\alpha,T_i}\right)} \leq 0.$$

Theoretically speaking, the more secure the risk assessors classify a smart contract, the more risk capital L_{α,T_i} is provided for risk underwriting. This lowers the price P_{β,T_i} depending on the elasticity b and the low risk cost limit π.[21] Figure 6 highlights the relevance of π in shaping the transition of dynamic premium determination towards the low-risk premium range.

We obtain the following cross partial derivative:

$$\frac{\partial^2 P_{\beta,T_i}\left(\sum_{\alpha=1}^{n} L_{\alpha,T_i}\right)}{\partial\left(\sum_{\alpha=1}^{n} L_{\alpha,T_i}\right)\partial\pi} = \frac{(1+\delta)\times I_{\beta,T_i}\times \Delta t\times\left(\frac{\sum_{\alpha=1}^{n} L_{\alpha,T_i}}{\pi}\right)^{\frac{1}{b}}}{b^2\times\left(\sum_{\alpha=1}^{n} L_{\alpha,T_i}\right)\times\pi}.$$

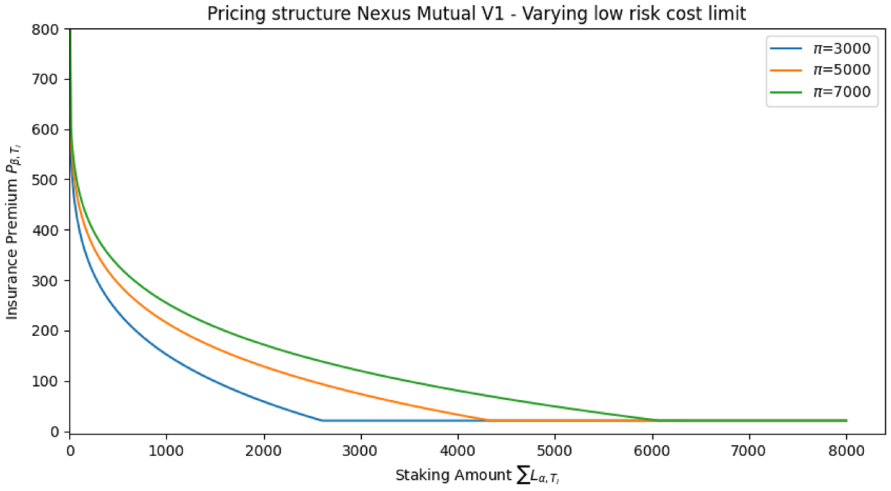

Fig. 6 Pricing structure of Nexus Mutual V1 under varying risk thresholds for $\delta = 0.05, b = 7, I_{\beta,T_i} = 1000$, $\text{SRCL} = 0.02$

[21] Note that the low risk threshold was usually much higher in practice (for Nexus V1 around 50,000 NXM), and we lowered the threshold for our illustrative example.

As the low risk cost limit increases, there is a corresponding decrease in the cross partial derivative with respect to π for all $\sum_{\alpha=1}^{n} L_{\alpha,T_i} > 0$. Furthermore, the larger π the larger the premium for each level of $\sum_{\alpha=1}^{n} L_{\alpha,T_i}$ as well as the interval of direct dependence of the premium on the staking amount until the SRCL lower bound has been reached. This result is in line with the lower relative change for increasing $\sum_{\alpha=1}^{n} L_{\alpha,T_i}$.

Figure 7 shows the dependence of the price curve under varying elasticity factor b. The corresponding cross partial derivative is given by

$$\frac{\partial^2 P_{\beta,T_i}\left(\sum_{\alpha=1}^{n} L_{\alpha,T_i}\right)}{\partial\left(\sum_{\alpha=1}^{n} L_{\alpha,T_i}\right)\partial b} = \frac{(1+\delta)\times I_{\beta,T_i}\times \Delta t\times \left(\frac{\sum_{\alpha=1}^{n} L_{\alpha,T_i}}{\pi}\right)^{\frac{1}{b}}\times\left(b+\log\left(\frac{\sum_{\alpha=1}^{n} L_{\alpha,T_i}}{\pi}\right)\right)}{b^3\sum_{\alpha=1}^{n} L_{\alpha,T_i}}.$$

The elasticity factor b exhibits a negative effect on the relative price change as the parameter $\sum_{\alpha=1}^{n} L_{\alpha,T_i}$ undergoes variation, as well as on the premium for each fixed level of $\sum_{\alpha=1}^{n} L_{\alpha,T_i}$. With an increasing elasticity factor, changes in the staking amount exert diminishing relative effects compared to the scenario without such changes. This is true as long as

$$\frac{(1+\delta)\cdot I_{\beta,T_i}\times \Delta t\times \left(\frac{\sum_{\alpha=1}^{n} L_{\alpha,T_i}}{\pi}\right)^{\frac{1}{b}}\times\left(b+\log\left(\frac{\sum_{\alpha=1}^{n} L_{\alpha,T_i}}{\pi}\right)\right)}{b^3\sum_{\alpha=1}^{n} L_{\alpha,T_i}} > 0,$$

which is the case for

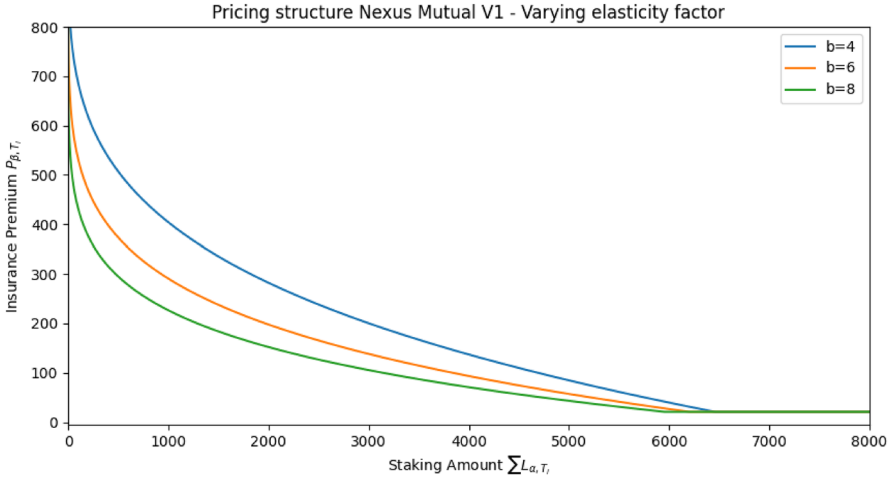

Fig. 7 Pricing structure of Nexus Mutual V1 under varying elasticity factor, $\delta = 0.05, \pi = 7000, I_{\beta,T_i} = 1000$, SRCL = 0.02

$$\sum_{\alpha=1}^{n} L_{\alpha,T_i} > e^{-b} \times \pi \; \forall \; \delta > -1, \pi > 0, b > 0, I_{\beta,T_i} > 0.$$

The interval for which this condition holds changes with varying b and low risk cost limit π. In general, if the risk assessors are not convinced of the safety of a smart contract, a cover will not be offered, or only with a significant risk premium due to particularly low capital provisioning.

This example prototypically reflects the transition from ex ante defined insurance premiums determined by actuarial methods and historical data to pricing via subjective beliefs and the associated staking of risk capital. In turn, this pricing method depicts a prediction market for risk valuation with different endogenous dependencies. Last, it should be considered that the staking amount L_{α,T_i} could entail different inherent definitions. For example, protocols such as Nexus Mutual[22] introduce a net factor that considers pending staking withdrawals, and hence, dynamizes staked capital and its endogenous dependencies further.

4.4 On operational administration of transferred risks

Finally, the operational level of risk transfer, as depicted in Fig. 8, will be compared between traditional lines of insurance and DeFi.

In the common understanding of insurance, as described in Olivieri and Pitacco (2011), individual risks are initially transferred to insurers, which are considered risk pools from a risk transfer perspective. Since some risks are too large or too difficult to quantify to be covered by a single insurer, secondary and alternative

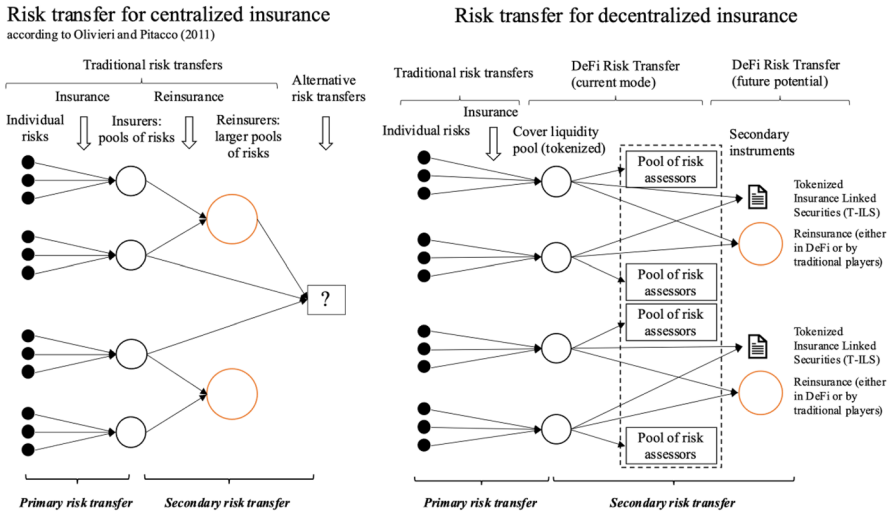

Fig. 8 Operational risk transfer mechanisms in comparison

[22] In 2023, the pricing mechanism has been upgraded to V2. More details can be found on the project homepage via https://nexusmutual.io/.

risk transfers, such as the availability of reinsurance or insurance-linked securities (ILS), can facilitate the transfer by involving further entities with higher risk-bearing capacities or by distributing the risks to other market participants with different risk preferences.

In DeFi, primary risk transfer follows a traditional approach. Initially, individual risks are pooled in various cover liquidity pools. However, a cover liquidity pool does not represent a single liable entity within the risk transfer structure. The risk-bearing capacity of the liquidity pool is solely provided by risk assessors who delegate their personal token capital for risk assessment through staking. The primary transfer structure to the cover liquidity pool shares similarities with risk transfer to a special purpose vehicle (SPV), where the SPV holds capital from a diverse set of investors and issues instruments similar to cat bonds to those investors.

The secondary transfer takes place from the cover liquidity pools to risk assessors. The insurant transfers risk primarily to the cover liquidity pool, which itself has no inherent risk-bearing capacity, and the risk assessors in turn support the cover liquidity pool through an aggregation of individual risk-bearing capacities and not exclusively for an individual risk as the counterparty. In principle, this is most comparable to the ownership concept of a traditional insurance mutual, such as that described by Albrecht and Huggenberger (2017), Cass et al. (1996) and Talonen (2016), but with key differences in the guarantee and structure of risk-bearing capacity. Practically, one can compare this approach to, e.g., Lloyds of London, where different underwriters provide risk capital for specified risk profiles and subsequently underwrite risks, whereby risk assessors are comparable to underwriters, but with no central organizational structure keeping in mind the arguments from Sect. 4.1. Reinsurance or tokenized ILS could also be an option for DeFi insurance to increase risk-bearing capacities while maintaining high capital efficiency. In summary, the operational administration of risks in DeFi insurance is not fundamentally different from traditional lines, but the operational "responsibilities" differ considerably in some aspects from the traditional understanding.

5 Discussion on insurability

This section follows up on the comparison in Sect. 4 and aims to start a discussion on the insurability of smart contract risks as the most prevalent risk class in DeFi. The discussion aligns with the classification of insurability according to Biener et al. (2015) citing Berliner (1982), considering additional insurability factors such as described by Schmit (1986) citing different secondary sources, as well as Mehr and Cammack (1976). Table 4 presents an overview of the insurability criteria discussed in the following.

A1 (Large number of similar exposure units)—The relevance of this criterion results from the law of large numbers (LLN) and the applicability of the central limit theorem (CLT) as described by Le Cam (1986). However, empirical observations on this in relation to DeFi insurance are difficult to obtain. A first approximation is provided by historical data on Nexus Mutuals operations. Utilizing information from Table 8, one can obtain a rough estimate for the number of theoretical individual risks by estimating total cover amounts per project and comparing them with

Table 4 Aggregated list of insurability criteria

Actuarial (A)	A1. Large number of similar exposure units A2. Independence among exposure units A3. Calculable expected loss in monetary values A4. Loss: definite (time, place, amount, cause), accidental/random, large A5. Limited risk of catastrophically large losses ("maximum possible loss") A6. Controllable exposure to information asymmetry/moral hazard
Market (M)	M7. Affordable premium M8. Cover limits M9. Economic feasibility (feasible business case)
Societal (S)	S10. Insurance in line with public policy S11. Insurance in line with legal framework(s)

Table 5 Indications on individual risk units for Nexus Mutual

Mean active cover amount per project	7,829,237 USD
Mean claim amount	235,773 USD
Average cover-to-claim ratio	~33.2

average claim sizes, i.e., realized risks, as shown for 2021. As shown in Table 5, this ratio infers that approximately 33.2 individual risks have been aggregated on average in a cover liquidity pool of Nexus Mutual. However, this represents only a particularly rough approximation and not a reliable forecast, which would require greater data availability and a longer data time span.

While further empirical investigation is needed as different protocols accumulate more historical data, it appears that the number of exposure units currently pooled in insurance protocols is relatively small or that at least risks that become imminent could affect a disproportionately large part of the risk pools. There could be two primary reasons for this. First, insurance in DeFi still has a low adoption rate, as discussed in Sect. 1. Second, conservative capital efficiency necessitates a disproportionately high collateral requirement to scale cover offerings. The convergence towards the applicability of the Central Limit Theorem (CLT) and the associated benefits in risk management within the insurance protocol inevitably involves a substantial capital commitment that is currently missing. Simultaneously, further scaling in terms of risk pooling solely for homogeneous risks may not always be desirable. In the event of a smart contract exploit, all risks within a pool are inevitably exposed to potentially similar loss likelihoods. As the number of insured risks increases, the potential loss that the entire protocol may need to settle increases alike. Therefore, achieving further scaling necessitates risk diversification through the aggregation of different risks, such as different smart contracts or risk categories, within a cover liquidity pool. Whether small sample sizes are finally sufficient for the applicability of CLT and, consequently, provide a better understanding of the average expected loss is a strongly subjective discussion, with the underlying discussion on necessary sample sizes being as old as CLT itself. Canals and Canals (2019) cite various secondary sources that postulate a sample size of 25–30 to approximate the validity of the CLT. However, authors such as Chang et al. (2006) cast early doubt on

those sample size requirements. If these values are taken as a benchmark, at least Nexus Mutual would have a good chance of ensuring actual insurability regarding this criterion. However, particularly considering the following criterion A2, the structure of the risk aggregation and the size of individual risks raises doubts as to whether this criterion can be fully met at the current level. Furthermore, one should only carefully exploit LLN and CLT if the involved risks are not too heavy tailed, which requires further observations and analysis in the case of DeFi insurance.

A2 (Independence among exposure units)—As Biener et al. (2015) summarize, this condition is closely related to the LLN and CLT. The authors describe a violation of the condition for cyber risks, and a similar situation prevails for smart contract risks. While users purchasing coverage for the interaction with a specific smart contract are presumably independent of each other, i.e., the behavior of insurant A is not highly correlated with effects on insurant B, elements that can cause a potential loss overlap are inherent dependencies in each cover liquidity pool and similarity factors between different protocols. Cover liquidity pools often group identical risks, such as insurance of individual users in interaction with a specific lending protocol. In turn, this also infers that in the event of a loss in one protocol, all risks in the cover liquidity pool are potentially realizable because all users access and rely on the same code base. Furthermore, cross-protocol correlations cannot be ruled out at the current state of knowledge, e.g., code similarity factors due to protocol forks.[23] This inevitably leads to a contradiction with one of the most important conceptual hypotheses in DeFi insurance: independence of risks. The liquidity and risk management of each protocol should therefore maintain operations of different mixed cover pools to achieve a higher level of independence in the overall risk profile and to ensure adequate fulfillment of this insurability criterion, given the high level of DeFi composability in practice, as described by Schär (2021) and Popescu (2020). If achieving risk diversification and a mix of risks is not feasible, it is advisable to conduct ex ante checks for code similarity factors and consult additional audits. These measures help to assess the risk associated with dependencies between risks within and across the liquidity pools, and hence to increase the insurability of smart contract risks within a specific cover liquidity constellation.

A3 (Calculable expected loss in monetary values)—In the context of this criterion, Schmit (1986) mentions two potential dimensions of indefiniteness influencing the calculability of expected losses: knowledge of the risk and knowledge of the (monetary) consequence. For smart contracts, it is almost impossible to determine ex ante which potential combinations of code flaws could lead to which exploits or how severe the consequences would be. The use of ex post information on possible vulnerabilities is also limited in a dynamic risk environment such as DeFi. The main reason for this, as with other code development projects, is that a bug fix does not necessarily promise immunity against similar future bugs, as demonstrated by the Parity MultiSig hack(s).[24] However, interactions with token and smart contracts potentially always have direct or indirect monetary consequences as a result of a bug. As stated in Sect. 3.2, the scarcity of data must be compensated by manual or

[23] Forks are redeployments of the code of another protocol, usually with slight modifications.

[24] The second exploit was facilitated by a bug in a multi-signature contract and was similar to a previous multi-sig hack related to Parity, cf. Petrov (2017).

alternative analyses of DeFi-inherent risks to enable feasible risk transfer. The gap created by the lack of historical experience with DeFi protocols inevitably leads to a situation in which either all risks must be assessed in aggregate form or the actual coverage must be limited to marginal subsets of risks, e.g., usage of specific code components. In those cases, the application of actuarial methods based on other information values could deliver reliable estimates. If the former option is adopted, this strongly impacts premiums (see M7).

What can be defined by the empirical observations to date, however, are general risk vectors of smart contracts, which are addressed, among others, by Atzei et al., (2017) and Sayeed et al. (2020). The probability of loss and the loss consequence are nonetheless more difficult to assess due to the high diversity of risks, as shown in Fig. 4. Hence, only the (maximum) consequence of a smart contract risk can be delimited: Only as much can be lost as was used by the individual in the interaction with the contract (see also criterion A5). Therefore, the insurability of smart contract risks remains dependent on individual underwriting by risk assessors or through secondary risk transfer mechanisms described in Sect. 4.4. Provided that data availability changes and sufficient data on smart contract vulnerabilities and associated losses have been collected, the use of proper statistical models to estimate expected losses would be desirable. First and foremost, Monte Carlo simulations could be used for a more precise assessment of the expected risks in each cover liquidity pool. Furthermore, the use of machine learning and artificial intelligence methods, combined with code-based knowledge of the potential behavior of a smart contract, could also benefit insurability with regard to A3.

A4 (Loss: definite (time, place, amount, cause), accidental/random, large)— These attributes are frequently addressed by different authors and depict an essential dimension in assessing insurability. The first characteristic is fulfilled regarding DeFi risks. Through transparent on-chain data, the exact time (in block time and in real time), transfer amounts and affected wallet IDs (places) can be identified. Furthermore, general smart contract vulnerabilities can also usually be analyzed ex post, delivering reasonable causes for an exploit.

The second characteristic is a double-edged sword with regard to smart contract risks. First, the general occurrence of smart contract risk seems to be subject to a high degree randomness, as numerous factors that cannot be controlled ex ante can independently lead to exploits. The agent has no control over the behavior of a deployed smart contract, or similar to Mehr and Cammack (1976), the risk is beyond the control of the individual. On the other hand, randomness (see also A1 and A2) within the portfolio of risks is to some extent undermined by the operational setup of most insurance protocols. Pooling similar risks, or categories of protocols, entails strong correlation and a correspondingly low degree of randomness within a cover liquidity pool. If something happens to a specific contract, it is likely that many or all users of the contract will be affected. Accordingly, all risks transferred to the cover liquidity pool will be at risk of realization. Randomness can therefore be assumed at the level of individual losses but not at the level of cover liquidity pools.

The third criterion follows a highly subjective assessment. The exploits observed so far provide an indication of whether smart contract risks are large enough in line with

Mehr and Cammack (1976). The average ETH holding per address without the top 50 addresses has been ~1.59 ETH (ConsenSys, 2018). The average amount at risk in a hack or malfunction according to the data used for Tables 9, 10, 11, and 12 is over 8500 ETH, a factor of over 5300 compared to average individual holdings, illustrating the significance of the amounts lost in single exploits so far. Since protocols in particular often hold large amounts of user funds, these aggregate risks can certainly be described as large enough to be considered for insurance. Henceforth, it can be stated that this dimension of insurability is fulfilled with restrictive assumptions regarding the underlying cause of exploits and malfunctions, as well as operational setups due to high cover pool internal correlations.

A5 (Limited risk of catastrophically large losses)—This criterion includes various interpretations of risk limits that an insurance policy can internalize. Berliner (1982) describes a maximum possible loss (MPL), referring to both a subjective and an objective component. The objective component depicts the maximum risk that can occur within a risk profile, which can be determined recursively as depicted in Tables 9, 10, 11, and 12. The subjective component looks at the risk that an insurance company needs to cover in the event of risk manifestation. Current insurance options are protected by the cover limit selected by the insurant and implemented in the protocol-specific liquidity requirements or cover availability factors (see M8). Accordingly, even a large loss does not directly endanger the protocols' overall liquidity. In the case of large exploits, however, depending on the specific insurance protocol, claims within one cover liquidity pool may only be settled on a pro rata basis. This would be comparable, for example, to the pro rata settlement of creditors' claims in the event of a company's insolvency. Often, this correlation can also be observed indirectly via the price development of protocol-specific governance tokens, which indicate the value of an internal clearing unit of the insurance protocol. In summary, a MPL can be objectively defined, whereas the subjective interpretation in the sense of Berliner (1982) inevitably infers partial insurability rather than actual full insurability considering a low degree of randomness within each cover liquidity pool (see A2 and A4).

A6 (Controllable exposure to information asymmetry/moral hazard)—This criterion considers the behavior of the insurant under information asymmetry and the insurer's control over it. Under certain circumstances, the insurant obtains insurance not only to cover actual risks but also to obtain protection other than against losses. Smart contract cover is affected by moral hazard as well, and the discussion of this criterion is one of the most challenging. Berliner (1982) lists three main categories of risk potentially susceptible to moral hazard, as described below:

Category 1

Risk category consisting of "natural risks" in which the occurrence and the amount of losses are independent of the will of any human beings. *Example: Hurricanes, hail*

Category 2

Risk category consisting of risks which are dependent on human beings, in the occurrence of which, however, no one has an interest. *Example: Motor third-party liability*

Category 3

Risk category consisting of risks which are dependent on human beings, some of whom may have an interest in the occurrence of a loss event. *Example: Fidelity insurance, disability insurance*
(Berliner, 1982, p. 72)

Category 1 is less susceptible to moral hazard overall and in DeFi insurance, as the insured individual cannot influence the probability of smart contract risks occurring. Whereas Category 2 is generally affected by moral hazard, in DeFi, there is little incentive to exert harmful influence since the occurrence of the risk is, in most cases, not in the interest of the individual. Category 3 is directly susceptible to moral hazard in DeFi, as the insured individual can and would influence the risk through individual behavior related to protocol usage and the disclosure of private information on possible weaknesses.

Moral hazard in DeFi insurance primarily arises between the insurant and other protocol participants, with the consequences passed on directly to the claim assessor and indirectly to the risk assessor. The claim assessor must verify whether the insured is telling the truth based on his own information, while providing tokens to obtain claim assessment rights. The risk assessor is indirectly involved since fraud on the part of the insured with a pay-out vote by the claim assessor reduces the risk assessor's staked capital.

The moral hazard problem is most pronounced in a situation in which a user acts as both risk and claim assessor. This is possible given weak identities, as they occur in the case of public keys in DeFi and if the user is providing risk capital for both roles. In this situation, the claim assessor would be strongly incentivized to protect his risk assessment stake by voting against the pay-out. At the same time, the informative value of on-chain data is objectively equal to all parties involved. However, not all parties have the same possibility to use or interpret the information.

Moreover, information asymmetries related to the functionality and behavior of deployed contracts open up a second dimension of moral hazard between the insured and the smart contract itself, even though in most cases, no legal, liable entity can be established around the smart contract to react actively to this issue. If a smart contract has been published open-source, it can be easily converted to EVM bytecode and compared to the actual deployed code to verify the correct code deployment. The reverse case is much more complicated.

The underlying problem with the second case is to understand the true nature of smart contracts despite potential discrepancies between publicly available smart contract code and its deployed version, a problem particularly related to the Ethereum settlement layer. First, the dimension and extent of this problem should be addressed. According to Li et al. (2020), less than one percent of smart contracts deployed to date are "open-source", i.e., are available with accessible and readable source code. While the authors are solely referring to the number of etherscan.com verified contracts, the total number of open-source deployed contracts through repositories such as GitHub is probably larger. In addition, the consideration of TVL in the relationship between open-source contracts and unverifiable contracts should be considered. If 99% of the TVL is locked on a settlement layer in open-source deployed and verifiable contracts and only 1% in a protocol with a hidden code, then the problem dimension is certainly different than in the opposite situation. Nonetheless, a significant residual risk persists regarding the true behavior and nature of contracts in a substantial share of active protocols. Only the EVM bytecode is transparent and visible to everyone, providing limited insight. To gain a comprehensive understanding of the remaining contracts, appropriate decompiling tools must

be utilized to decompile the EVM bytecode, although these tools frequently generate errors. Theoretically, decompiling the EVM bytecode allows for a rough understanding of how the contract operates. However, variable names are not preserved during decompiling, and while rough dependencies between variables can still be discerned, it becomes challenging to reconstruct the overall picture and behavior within a protocol containing numerous individual codes. As a result, the EVM bytecode offers limited assistance in reducing information asymmetries, unless substantial advancements are made in the decompiling tools market. Additionally, "dry runs" could reveal whether expected execution and state changes occur within a specific protocol, making the behavior observable but not unequivocally documented. A noteworthy concern applies to any open-source smart contract code, even if the full code base is available. The availability of the entire code does not guarantee a comprehensive understanding of the contract's behavior and true nature. If the code is convoluted or extensively written in assembler language, the public information available to mitigate information asymmetry is relatively limited. In addition, smart contract data could be inaccessible for some parties due to high access costs (e.g., through the requirement to operate a full node).

In conclusion, information asymmetry cannot be completely mitigated in both of the described constellations, neither between insurant and the insurable object (smart contract) nor between insurant and insurer (protocol). Accordingly, a residual risk remains for each insurance protocol or insurer. Hence, the fundamental requirement for the insurability of smart contract risks is that they are published as open-source, ensuring the best possible fulfillment of this criterion. However, due to the governance and incentivization challenges inherent in DeFi insurance protocols, a complete inherent mitigation of moral hazard remains challenging.

M7 (Affordable premium)—Due to the mechanisms of the price bonding curve explained in the previous section, premiums of more than 50% of the insured sum have been observed in the past, e.g., with cover for the "Trader Joe" protocol offered at an annual premium of 53.88% for cover purchased via Nexus Mutual on February 10, 2022. In the traditional argumentation, this would be equivalent to a fair premium definition in which the insurer expects with sufficient certainty the loss of approximately half of the hedged assets. This seems relatively high compared to the vast majority of insurance categories in traditional lines. Insurance is not always obtained at such high rates, but the pricing mechanism ultimately serves to protect the liquidity pool itself, hence impacting the affordability for insurants.

At the same time, the metrics cannot be directly compared with traditional insurance lines, since the risk assessment and premium determination differ, as described in Sect. 4. Hence, the validity of this criterion for DeFi insurance is limited by the endogeneity of premium determination, considering solely the cover amount, in combination with a lack of centralized control as described before.

M8 (Cover limits)—This criterion, described in particular by Berliner (1982), is concerned with the establishment of liability limits within the insurance policy. Under certain circumstances, cover limits can shift a risk from the uninsurable to the insurable area, as described in the geometric model of Berliner (1982). First, the general cover limit in a parametric insurance policy as offered in most insurance protocols in DeFi is determined by the initial sum insured. No more is paid out than

agreed upon in the contract; hence, no tail risks above the cover amount need to be considered by the insurer in this setting, although the protocol must consider the proportional liquidity requirement in portfolios with similar risks. In addition, some protocols introduced proof-of-loss methods to objectively verify the loss. At the same time, only as much insurance cover is provided as enabled by the protocol economics based on the amount of risk capital provided. Hence, there is an ex ante limit on the potentially obtainable insurance coverage and an ex post limit on compensation in the event of a loss. The criterion is therefore met in the vast majority of cases.

M9 (Economic feasibility (feasible business case))—Schmit (1986) describes economic feasibility as an aggregate of various other prerequisites of insurance, in particular characteristics of loss distributions, moral hazard, and the occurrence of catastrophic losses. First, a feasible business case related to the transfer of smart contract risks is hampered by the scarcity of historical data. The premium determination is based on the previously described risk assessment, with additional consideration of a margin as described in Sect. 4.3. Thus, the profit expectation can only be controlled based on predictions and not based on historical knowledge, with the latter promising a more reliable and precise assessment and supposedly a higher economic feasibility. Whether the criterion is met always additionally depends on the specific design of the insurance protocol. An unstable economic model behind the protocol will show significant drawbacks, even in a flawless smart contract. However, there is one decisive advantage of decentrally managed insurance protocols over traditional insurance businesses. The economic model of the insurance protocol is implicitly defined in terms of key metrics ex ante in unforgeable smart contract structures and accordingly can be kept constant in the defined efficacy and profitability areas during operations. The disadvantage in turn is the inflexibility and lack of foresight for the overall economic model. The degree to which this criterion is met is therefore influenced not only by the risk itself but also by the specific type of risk transfer. With regard to this criterion, it should also be considered that in many DeFi (insurance) projects, the idea of avoiding centralized profits is at the forefront. Accordingly, the closest definition of profit in DeFi would be the avoidance of individual damages at the lowest possible opportunity cost for protocol users.

S10 (Insurance in line with public policy)—Regarding this criterion, Berliner (1982) lists five subcriteria. No speculative entrepreneurial risks are to be covered, nor any risks where there is no need for insurance. In addition, the insurance of trivial losses should be avoided, and the high costs from one line of business should not be passed on to other lines of business wherever possible. Furthermore, it must be taken into account that external circumstances can jeopardize insurability, which applies under a ceteris paribus assumption.

Currently, DeFi is more of an entrepreneurial venture, since dApps and smart contract protocols in general are neither a recognized nor widely used concept in our societies. However, these are by no means risks for which there is no need for insurance, since partial or total loss of crypto assets by or in interaction with a protocol does not seem to be bearable by the insurant without additional burden. This is therefore not a trivial risk according to the definition of Berliner (1982). With regard to risk pool (cost) sharing with other lines of business, it can currently be assumed that DeFi insurance complies with the authors' definition, with one operational

restriction. The reason for this was described earlier in Sects. 4.1 and 4.3. Premium determination for one cover is fundamentally independent of the risks in other insurance pools, and therefore costs will not be shared throughout. However, for governance token concepts, the fiat quoted market price of the governance token shows a holistic dependence on the overall coverage demand captured by the insurance protocol, which creates an indirect dependency on all other cover products offered within the same protocol. Finally, a certain dependence of smart contract risks on external circumstances can be identified, which may lead to non-insurability under certain circumstances. First, it cannot be excluded that tokenized assets are used for illegal purposes related to the real economy, as a report for the European Parliament depicts (European Parliament, 2018). In addition, new inherent criminal activities in DeFi emerge, as Wronka (2023) shows, which may be spurred by the securitization of assets or smart contract interactions through insurance. However, societal laws effectively exclude the coverage of criminal activities in any form of financial transaction. Hence, at least theoretically, claim assessors can deny claims on the same regulatory basis as in traditional insurance contracts, and risk assessors can avoid covering protocols related to illegal activities. In contrast, since DeFi is currently not subject to regulation, a responsible government body in the sense of Berliner (1982) cannot be used to validate this criterion (see also criterion S11). Overall, this criterion is therefore not comprehensively fulfilled in line with the understanding of Berliner (1982) but also does not show any fundamental contradictions to insurability.

S11 (Insurance in line with legal framework(s))—While the previous criteria require a subjective or multidimensional quantitative interpretation, this criterion is an objective, binary criterion, as Berliner (1982) states. This criterion requires a legal framework within which the insurance company and the cover product are organized. With respect to DeFi, this criterion cannot be fully assessed because insurance activities in DeFi have not yet been subject to any form of regulation. Accordingly, ceteris paribus, the offer does not violate any applicable law. Nevertheless, governance tokens in particular, in their capacity as tokens with monetary value or exchange tradability, could be subject to more extensive regulation in some jurisdictions. However, this primarily concerns their properties as exchange and transfer assets. The actual risk transfer provided by the insurance protocol is not affected.

Overall, the insurability of smart contract risks within the framework of established definitions cannot be determined conclusively. With regard to the actuarial dimension, the high correlation of risks through potential code similarity factors, as well as a limited number of exposure units aggregable in current protocols, represents a limitation to insurability. This can be partially compensated by the inherent technological and organizational advantages of DeFi, for example, through ex ante clearly defined incentivization and decentralized governance mechanisms to incentivize risk capital provisioning. At the same time, the determination of fair and reasonable premiums is hampered by the lack of historical data, although smart contract risks can at least be assessed ex post. Moral hazard is also considered to be a major problem between insurant and other insurance protocol users, as well as the protocol to be covered. The market dimension speaks in favor of the insurability of smart contract risks. Clearly defined ex ante cover limits and parametric processing allow a precise definition of the liability limits and associated maximum liquidity requirements, and

the interaction between the risk to be insured and the on-chain processing of the risk transfer also provides enough design options for feasible business cases. A major limitation is the premium determination, which tends to deliver premiums higher than in traditional lines of insurance due to the pricing mechanism based on subjective expectations rather than historical data and which will not always match the individual risk premium tolerance. The societal dimension of smart contract risks shows no principal inconsistencies with insurability, yet difficulties arise due to the young history of DeFi as well as the lack of assignment to a legal and societal framework, which leaves some related questions unanswered. Overall, DeFi insurance replicates many of the insurability challenges that have already been discussed with regard to cyber insurance, such as difficulties in comparison to other risk classes (Eling & Wirfs, 2019), missing modeling methods, change risk and accumulation risks that are impossible to quantify (Eling & Schnell, 2016).

Finally, it should be noted that the insurability of smart contract risks in the aggregate view also depends in particular on the precise design of an insurance protocol and on how the weaknesses identified in this paper with regard to the operational, actuarial, or procedural treatment of smart contract risks and related risk categories are dealt with. While smart contracts and DeFi present some entirely new challenges related to risk transfer, the new infrastructure also offers inherent advantages in turning weaknesses back into strengths, such as the possibility of enabling transparent, decentralized governance for the insurance organization.

6 Conclusion

DeFi-inherent risk transfer differs significantly from traditional lines of insurance. This is not limited to the risk clusters to be insured but also includes the organization of risk transfer. This paper suggests a taxonomy to classify current DeFi insurance protocols and their differences from traditional lines of insurance and discusses the insurability of smart contract risks as one of the most important and inherent risk clusters in DeFi.

First, DeFi insurance exhibits crucial differences from traditional lines of insurance in three dimensions: (A) the inherent complexity of risks to be transferred caused by the composability of the underlying technological infrastructure, including new risks observed in particular to DeFi's settlement and protocol layer, (B) a more difficult and subjective actuarial judgment of risks, especially smart contract risks, through prediction-market-like structures, and (C) new operational circumstances, in particular including decentralized governance structures instead of centralized organizational forms.

Second, analyzing the insurability of smart contract risks in line with established insurability criteria depicts an overall miscellaneous result. Many DeFi protocols exhibit significant similarities and interdependencies due to a high level of DeFi composability, leading to potential correlations in transferable risks. Consequently, this poses challenges for actuarial assessments and the establishment of reasonable insurance premiums. However, DeFi-inherent risk transfer mechanisms have the

potential to address these limitations through new infrastructural and organizational capabilities in the form of different protocols.

Third, it is important to note that while traditional insurance has a long-established infrastructure and well-defined, legacy-driven processes, DeFi insurance is still in its early stages of development. Depending on the specific setup of DeFi risk transfer, insurance protocols face challenges such as ensuring the reliability of oracles, handling complex claims scenarios and systematic events, reducing subjective dependencies, and eventually managing regulatory compliance in case of exogenous restrictions. As the technology matures and these challenges are addressed, risk transfer in DeFi has the potential to provide more transparent and efficient contractual settlement processes compared to established forms of insurance organizations. However, one should keep the, to date, non-mitigatable, risk in mind, that insurance protocols themselves are exposed to the same risks (e.g., smart contract exploits) as the protocols that are to be covered through these projects.

In addition to DeFi-inherent insurance, traditional insurers and reinsurers can explore diverse commercial opportunities to engage in DeFi risk transfer. However, applying the organizational structures and methods of centralized insurers to DeFi may not be promising, as it could result in the transfer of outdated inefficiencies and frictions to DeFi projects. Feasible opportunities may arise in terms of liquidity provision for insurance protocols, potentially as reinsurers for large-scale and tail risks. The risk-bearing capacity of decentralized insurance projects is currently still very limited, and further scalability is heavily dependent on collective beliefs and a critical threshold of individuals participating in a project. Traditional insurers, with their reputation and established legacy, could potentially take on a leading role in providing additional risk transfer capacity through liquidity provision in different projects. Hence, insurers are advised to cultivate expertise in DeFi and develop robust IT infrastructures to effectively engage with blockchain technologies, thereby securing substantial market shares in the future insurance landscape.

The topic offers diverse further research potential. Further analyses could include a more detailed analysis of the consequences of asymmetric information on decentralized insurance marketplaces, the role and design of reinsurance in and for DeFi risks, as well as a more quantitative framework around the discussion on general insurability, currently limited through data scarcity. Furthermore, DeFi risk transfer could additionally benefit from behavioral economic considerations, helping to analyze which control mechanisms and types of policies could enforce the right incentivization in decentralized governance. In addition, it would be worthwhile to explore how risk management and assessment methods from traditional areas affected by similar actuarial challenges, such as operational risk, could also be used for DeFi risk transfer, e.g., methods from extreme value theory.

Appendix

See Tables 6, 7, 8, 9, 10, 11 and 12.

Table 6 Selected DeFi insurance protocols, offering as of 23/12/2022, own aggregation from different sources

Project	Category	Proto-col	Risk Assessment/ Underwriting	Claim assessment	Type	Products	Link
Nexus Mutual	Mutual insurance	ETH	Staking	Community	N	SCI, CP	https://nexusmutual.io/
Nsure	Open risk marketplace	ETH, MATIC, DOT	Staking	Community	N, NN	SCI	https://nsure.network/
cozy.finance	Protection market	ETH	Staking	Automated	N	SCI, AI, Other	https://cozy.finance/
Tidal Finance	Insurance platform	ETH	Staking	Expert	N	SCI	https://tidal.finance/
Etherisc	Insurance platform	ETH	Staking, Expert	Automated, Expert	NN	CP, Other	https://etherisc.com/
Opyn	Derivatives-based price-risk hedging	ETH	Risk-oriented LP, Model	Automated	N	AI	https://opyn.co/
Unslashed Finance	Insurance platform	ETH	Staking	Expert	N	SCI, PKT, AI, CP, OR, Other	https://unslashed.finance/
Union	Insurance platform	ETH	Staking, Model	Automated, Community	N	SCI, AI, OR, Other	https://www.unn.finance/
Hegic	Derivatives-based price-risk hedging	ETH	Risk-oriented LP, Model	Automated	N	AI	https://www.hegic.co/
Risk Harbor	Open risk marketplace	ETH	Staking, Model	Automated	N	SCI, Other	https://www.riskharbor.com/
InsurAce	Insurance platform	ETH	Staking	Community,Expert	N	SCI, CP, AI, Other	https://www.insurace.io/
Bridge Mutual	Insurance platform	ETH	Staking, Model	Community	N	SCI, CP, AI	https://bridgemutual.io/

Protocols: *ETH* ethereum blockchain, *MATIC* Polygon blockchain, *DOT* polkadot blockchain

Types: *N* DeFi-native offering, *NN* non-DeFi-native offering

Products: *SCI* smart contract insurance, *PKT* private key theft, *AI* asset inflation/price risk, *CP* counterparty/issuer risk (e.g., risks related to custodial activities), *OR* Oracle risks, *Other* insurance against specific other on-chain and off-chain risk profiles (more information available on individual protocols homepage), or protocols with flexible trigger definition

Disclaimer The availability, usefulness and reputation of protocols in DeFi can change quickly and dynamically into each direction. The table represents a selection of the most widely used insurance protocols at the end of December 2022. To determine the current status of the project, the homepage should be consulted and community discussions should be actively followed

Table 7 Descriptive statistics of liquidity- and performance-related parameters, Nexus Mutual, commercially rounded, data as of April 2021 and December 2021

	December 2020			December 2021			Relative growth
	Amount	Monetary equivalent	Token equivalent	Amount	Monetary equivalent	Token equivalent	
Active cover amount		$58,412,817	99,033 ETH		$646,408,047	163,561 ETH	+165%
No. of supported protocols	#57			#83			+146%
Annualized Premiums In-Force		$1,469,071	2419 ETH		$19,271,763	4876 ETH	+202%
Total no. of claims[a]	#68			#105			+154%
Whereas "Yes"-Vote	#3			#24			
Whereas "No"-Vote	#62			#81			
Whereas "Pending"	#3						
Capital pool size		$96,534,468	163,294 ETH		$606,272,624	154,624 ETH	−5.3%
MCR			162,425 ETH			162,425 ETH	+0%
Capital efficiency ratio	60.61%			106.15%			+45.5%
MCR%	100.53%			95.19%			−5.3%
Total amount staked[a]		$98,990,778	4,300,776 NXM		$1,241,751,154	9,282,308 NXM	+216%
Total staking reward[a]		$1,008,125	44,445 NXM		$16,652,992	127,568 NXM	+287%
Price-to-book (P/B) ratio	1.6			0.69			−57%
NXM price[b]		$22.99	0.0388 ETH		$130.49	0.0333 ETH	+567%
NXM supply	N/A		6,730,791 NXM		N/A	6,893,953 NXM	+2.4%
NXM market cap[b]		$154,739,121	261,750 ETH		$899,578,366	229,429 ETH	+581%
Unique addresses	#2933			#3963			+135%

MCR minimum capital requirement

Variables and explanations: *Annualized Premiums In-Force* total premium payment over the next 12 months based on the assumption that the active insurancecontracts remain in force over this time, *Capital pool size* size of the risk capital pool custodied by the insurance protocol, *MCR (minimum capital requirement)* minimum amount of funds the mutual needs to be very confident it can pay all claims (NexusMutual Gitbook, 2022), *Capital efficiency ratio* Efficiency of use of locked collateral (optimal ~ 100%, calculated as active cover amount divided by capital pool size), *MCR%* ratio of capital pool size and MCR, *Total amount staked* total of all assets pledged as collateral, *Total staking reward* total of all staking rewards paid out, *NXM price* NXM price based on the continuous token model. The NXM price depends on how the mutual is performing financially, *NXM supply* NXM tokens in circulation (controlled by the token model), *NXM Market Cap* Current market capitalization in terms of NXM tokens in circulation, *Unique addresses* Number of unique public keys interacting with the insurance protocol

[a]Considering all events from 10/2019 to 12/2020, respectively, 12/2021

[b]Relative growth calculated via market price (data sources: NexusTracker (2022), CoinGecko (2022))

Table 8 Descriptive statistics of claim-specific parameters and staking, Nexus Mutual, commercially rounded, data as of 23/12/2021

	Mean		Std. dev		Min		Max	
	Token	USD	Token	USD	Token	USD	Token	USD
ETH active cover amount per project	1988	7,829,237	4230	16,661,090	1	3939	25,535	100,580,145
ETH premiums paid per project	92	361,209	132	520,867	0	0	714	2,811,081
Claim amount[a]	–	235,773	–	480,101	–	10	–	1,969,475
ETH Monthly surplus[a]	393	949,198	298	400,663	155	553,636	1340	1,730,556

Supplementary explanations: *ETH active cover amount per project* current risk mass in relation to a smart contract risk pool (for example, insurance pool to Aave), *ETH premiums paid per project* premiums paid in relation to a smart contract risk pool, *Monthly surplus of insurance mutual* free capital after deduction of all operating expenses (governance) and claim payments, *Claim amount* loss amount (individual risks)

[a]Considering all events from 01/2021 to 12/2021 (data source: NexusTracker (2022))

Table 9 DeFi ecosystem exploits ethereum up to December 2021 (data source: own aggregation from different sources)

Ethereum ecosystem parameters and exploits (values in USD)				
Launch/Genesis Block Creation:				July 2015
TVL as of 31/12/2021:				95,220,000,000
Categorical overview of all past exploits				
Vulnerability category and layer	Count	Total category risk	% of total risk	Maximum single risk
Settlement layer				
Transaction congestion attack	1	3,883,999	0.12	3,883,999
Sybil attack	1	2,500,000	0.08	2,500,000
Sandwich attack	1	167,000	0.01	167,000
Asset layer				
Private key lost or stolen	3	133,320,974	4.28	102,820,974
Hot wallet exploit	1	5,700,000	0.18	5,700,000
Protocol layer: smart contract vulnerabilities				
Loophole exploit	14	171,684,000	5.51	68,800,000
Modified keeper	1	613,062,100	19.66	613,062,100
Issues with pricing mechanism	2	16,015,000	0.51	16,000,000
Problems with initial contract settings	1	80,000,000	2.57	80,000,000
Re-entrancy attack	5	87,059,616	2.79	60,000,000
Unauthenticated initialization	1	4,000,000	0.13	4,000,000
Unverified functions	1	135,229	0.00	135,229
Function exploit	1	500,000	0.02	500,000
Flash loan attack	19	272,253,128	8.73	130,000,000
Fake token attack	1	1,300,000	0.04	1,300,000
Infinite minting	2	9,386,549	0.30	8,186,549
Overflow attack	3	1,140,000,000	36.56	1,000,000,000
Backdoor function	1	200,000	0.01	200,000
Business logic error	1	100,000	0.00	100,000
Governance attack	1	30,000,000	0.96	30,000,000
No further details	27	99,094,897	3.18	25,000,000
Application and aggregation layer				
Scam/Ponzi	7	18,689,000	0.60	12,000,000
Malicious code injection	1	7,095,340	0.23	7,095,340
Phishing	1	100,000	0.00	100,000
Spam attacks	1	335,000	0.01	335,000
Exogenous risks				
Human error	1	12,000,000	0.38	12,000,000
Oracle attack	5	30,080,050	0.96	25,000,000
Other				
Bypassing of security mechanisms	6	218,500,000	7.01	160,000,000
No specification on method	14	161,306,845	5.17	120,000,000
Sum	124	3,118,468,727	–	–

Table 9 (continued)

The data stems from empirical research under consideration of (Hacked Slowmist, 2021), and includes exploits up to December 31, 2021, in 309 data points, not considering whether funds have been recovered at any point. Instead, the first identified loss amount has been counted towards each category risk. Each data collection period starts at the genesis block creation of the corresponding settlement layer. In addition to the information in the database, all exploits have been validated and complemented by other publicly available sources, such as the database entries of the Quadriga Initiative (2022). The classification of events into vulnerability categories is based on a subjective analysis of all available information on each exploit. There are occasional cases in which potential attack vectors became public but in which no assets were lost at time of the observation. These have been accounted towards total counts, but not to loss amounts. The total category loss is an aggregation of all individual events in each category. Maximum single risks depict the most severe loss event in each category. Furthermore, the conversion from the nominal token amount to USD was undertaken with the daily FX rate at the reporting date of the underlying exploit. Cross-chain vulnerabilities not included. TVL Data retrieved from DeFiLlama (2022)

Table 10 DeFi ecosystem exploits BSC up to December 2021 (data source: own aggregation from different sources)

Binance smart chain (BSC) ecosystem parameters and exploits (values in USD)				
Launch/Genesis Block Creation:				September 2020
TVL as of 31/12/2021:				11,980,000,000
Categorical overview of all past exploits				
Vulnerability category and layer	Count	Total category risk	% of total risk	Maximum single risk
Asset layer				
Private key leak	3	195,735,482	24.10	139,195,315
Liquidity issue	1	145,000,000	17.85	145,000,000
Protocol layer: smart contract vulnerabilities				
Re-entrancy attack	1	125,000	0.02	125,000
Economic exploit	2	1,830,000	0.23	1,500,000
Issues with pricing mechanism	1	550,000	0.07	550,000
Flash loan attack	21	270,844,365	33.34	200,000,000
Contract loophole	2	50,300,000	6.19	50,000,000
No further details	8	66,424,000	8.18	30,000,000
Application and aggregation layer				
Scam/Ponzi	13	72,692,400	8.95	32,000,000
Exogenous risks				
Oracle attack	3	8,646,599	1.06	8,000,000
Other				
No specification on method	1	170,000	0.02	170,000
Sum	56	812,317,846	–	–

See legend in Table 9

Table 11 DeFi ecosystem exploits polygon up to December 2021 (data source: own aggregation from different sources)

Polygon ecosystem parameters and exploits (values in USD)				
Launch/Genesis Block Creation:				October 2017
TVL as of 31/12/2021:				5,060,000,000
Categorical overview of all past exploits:				
Vulnerability category and layer	Count	Total category risk	% of total risk	Maximum single risk
Asset layer				
Private key leaked or stolen	2	46,995,000	70.45	46,900,000
Protocol layer: smart contract vulnerabilities				
Flash loan attack	2	2,652,462	3.98	2,402,462
Deflationary minting	1	250,000	0.37	250,000
Re-entrancy attack	1	500,000	0.75	500,000
Application and aggregation layer				
Scam/Ponzi	5	16,312,704	24.45	13,000,000
Sum	11	66,710,166		–

See legend in Table 9

Table 12 DeFi ecosystem exploits EOS up to December 2021 (data source: own aggregation from different sources)

EOS ecosystem parameters and exploits (values in USD)				
Launch/Genesis Block Creation:				June 2018
TVL as of 31/12/2021:				112,670,000
Categorical overview of all past exploits:				
Vulnerability category and layer	Count	Total category risk	% of total risk	Maximum single risk
Settlement layer				
Transaction congestion attack	27	46,726	0.14	16,520
Rollback attack—transaction rollback	16	801,234	2.35	530,000
Asset layer				
Private key leak	3	176,700	0.52	163,000
Private key lost or stolen	1	9650	0.03	9650
Protocol layer: smart contract vulnerabilities				
Fake token attack	10	752,920	2.21	375,000
Re-entrancy attack	2	13,730,000	40.26	13,400,000
Transfer error	4	196,000	0.57	188,500
Contract loophole	1	25,000	0.07	25,000
Overflow attack	2	5,520,000	16.19	5,000,000
No further details	6	856,527	2.51	750,000
Application and aggregation layer				
Scam/Ponzi	2	3,768,838	11.05	2,468,838
Exogenous risks				
Human error	1	7500	0.02	7500
Other				
Bypassing of security mechanisms	1	100,000	0.29	100,000
No specification on method	14	8,113,710	23.79	7,942,000
Sum	113	34,104,805	–	–

See legend in Table 9

Acknowledgements The author would like to thank Matthias Nadler for helpful feedback and insightful discussions, as well as two anonymous reviewers for their valuable comments and enriching suggestions for the further development of this work.

Author contributions 1 as the main author is solely responsible for the manuscript.

Funding Open access funding provided by University of Basel.

Data availability The datasets generated and analyzed during the study are available from the corresponding author on reasonable request.

Declarations

Conflict of interest The authors state that there is no conflict of interest and that no financial or nonfinan-

cial interests are directly or indirectly related to the work submitted for publication.

References

Abramowicz, M. B. (2019). Blockchain-based insurance. *Blockchain and the constitution of a new financial order: legal and political challenges (Ioannis Lianos et al. eds., 2019, Forthcoming)*. GWU Law School public law research paper no. 2019-12. https://ssrn.com/abstract=3366603.

Albrecht, P., & Huggenberger, M. (2017). The fundamental theorem of mutual insurance. *Insurance: Mathematics and Economics, 75*, 180–188. https://doi.org/10.1016/j.insmatheco.2017.06.002

Almakhour, M., Sliman, L., Samhat, A. E., & Mellouk, A. (2020). Verification of smart contracts: A survey. *Pervasive and Mobile Computing, 67*, 101227. https://doi.org/10.1016/j.pmcj.2020.101227

Ante, L. (2020). Smart contracts on the blockchain—A bibliometric analysis and review. *Telematics and Informatics*. https://doi.org/10.1016/j.tele.2020.101519

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on ethereum smart contracts SoK. In In Maffei, M., & Ryan, M. (Eds.), *Principles of security and trust: 6th international conference, post 2017, held as part of the European joint conferences on theory and practice of software, ETAPS 2017, Uppsala, Sweden, April 22–29, 2017, Proceedings. Lecture notes in computer science*. (Vol. 10204, pp. 164–86). Springer. https://doi.org/10.1007/978-3-662-54455-6_8.

Auer, R., Haslhofer, B., Kitzler, S., Saggese, P., & Victor, F. (2023). The technology of decentralized finance (DeFi). *BIS Working Papers* no. 1066. https://www.bis.org/publ/work1066.htm.

Berliner, B. (1982). *Limits of insurability of risks*. Prentice-Hall Inc.

Berliner, B. (1985). Large risks and limits of insurability. *The Geneva Papers on Risk and Insurance, 10*(37), 313–329.

Bernheim, A. (1998). Challenges in insurance markets. *The Geneva Papers on Risk and Insurance. Issues and Practice, 23*(89), 479–489.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance. Issues and Practice, 40*(1), 131–158.

Blondeau, J. (2001). Insurance and reinsurance at the dawn of the 21st century. *The Geneva Papers on Risk and Insurance. Issues and Practice, 26*(2), 145–155.

Bloomberg. (2022). *Chainproof launches as the world's first regulated smart contract insurance provider*. Retrieved May 21, 2023, from https://www.bloomberg.com/press-releases/2022-07-06/chainproof-launches-as-the-world-s-first-regulated-smart-contract-insurance-provider.

Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy, 37*(6), 527–544. https://doi.org/10.1016/j.jaccpubpol.2018.10.004

Borch, K. H. (1985). A theory of insurance premiums. *The Geneva Papers on Risk and Insurance, 10*(36), 192–208.

Bybit. (2022). *Sybil attack: What it is & the threats it poses to blockchains*. Retrieved May 22, 2023 from https://learn.bybit.com/blockchain/what-is-a-sybil-attack/.

Canals, C., & Canals, A. (2019). When is N large enough? Looking for the right sample size to estimate proportions. *Journal of Statistical Computation and Simulation, 89*(10), 1887–1898. https://doi.org/10.1080/00949655.2019.1602125

Cass, D., Chichilnisky, G., & Wu, H. (1996). Individual risk and mutual insurance. *Econometrica, 64*(2), 333. https://doi.org/10.2307/2171785

CFI. (2023). *What is a 51% attack?* Retrieved May 22, 2023, from https://corporatefinanceinstitute.com/resources/cryptocurrency/what-is-a-51-attack/.

Chang, H., Huang, K., & Wu, C. (2006). Determination of sample size in using central limit theorem for Weibull distribution. *International Journal of Information and Management Sciences, 17*(3). https://www.semanticscholar.org/paper/Determination-of-sample-size-in-using-central-limit-Chang-Huang/1d0b81b851c17acfa4bc6c946d0d9f6e25438bbe.

Chang, T., Ho, J., Tirrell, Z., Weng, G., & You, J. (2022). *A risk classification framework for decentralized finance protocols*. Retrieved May 25, 2023, from https://www.soa.org/4aa5bb/globalassets/assets/files/resources/research-report/2022/decentralized-finance-protocols.pdf.

Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights, 13*, e00151. https://doi.org/10.1016/j.jbvi.2019.e00151

Chorafas, D. N. (2004). Operational risk control business opportunity and challenges for the insurance industry. *The Geneva Papers on Risk and Insurance. Issues and Practice, 29*(1), 87–101.

CNBC. (2021). *Bug puts $162 million up for grabs, says founder of DeFi platform compound*. Retrieved May 29, 2023, from https://www.cnbc.com/2021/10/03/162-million-up-for-grabs-after-bug-in-defi-protocol-compound-.html.

CoinDesk. (2023). *On-chain vs. off-chain transactions: What's the difference?* Retrieved May 20, 2023, from https://www.coindesk.com/learn/on-chain-vs-off-chain-transactions-whats-the-difference/.

CoinGecko. (2022). *Nexus mutual price chart (NXM)*. Retrieved April 02, 2022, from https://www.coingecko.com/en/coins/nexus-mutual.

Cointelegraph. (2022). *HARTi and Mitsui Sumitomo roll out NFT insurance coverage for claims*. Retrieved May 22, 2023, from https://cointelegraph.com/news/harti-and-mitsui-sumitomo-roll-out-nft-insurance-coverage-for-claims.

ConsenSys. (2018). *Ethereum by the numbers*. Retrieved December 19, 2021, from https://media.consensys.net/ethereum-by-the-numbers-3520f44565a9.

Cousaert, S., Vadgama, N., & Xu, J., (2021). *Token-based insurance solutions on blockchain*. https://arxiv.org/pdf/2109.07902.

Cowell, R. G., Verrall, R. J., & Yoon, Y. K. (2007). Modeling operational risk with Bayesian networks. *The Journal of Risk and Insurance, 74*(4), 795–827.

Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2020). Flash boys 2.0: frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *2020 IEEE symposium on security and privacy (SP)* (pp. 910–27).

DeFiLlama. (2022). *Total value locked all chains*. Retrieved March 13, 2022, from https://defillama.com/chains.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *JRF, 17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research, 272*(3), 1109–1119. https://doi.org/10.1016/j.ejor.2018.07.021

Ethereum. (2023). *Ethereum developer docs—Oracles*. Retrieved June 02, 2023, from https://ethereum.org/en/developers/docs/oracles/.

Etherisc. (2022). *Homepage and "white paper 2.0"*. Retrieved May 19, 2023, from https://etherisc.com/#products.

European Parliament. (2018). *Virtual currencies and terrorist financing: assessing the risks and evaluating response*. STUDY for the TERR Committee, Directorate General for Internal Policies of the Union. Retrieved November 23, 2021, from https://www.europarl.europa.eu/thinktank/de/document/IPOL_STU(2018)604970.

Feng, R., Liu, M., & Zhang, N. (2023). A unified theory of decentralized insurance. *SSRN*. https://doi.org/10.2139/ssrn.4374502

Fontnouvelle, P., Jesus-Rueff, V., Jordan, J. S., & Rosengren, E. S. (2003). *Using loss data to quantify operational risk*. Last modified April 2003. https://ssrn.com/abstract=395083.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet, 10*(2), 20. https://doi.org/10.3390/fi10020020

Guillen, M., Gustafsson, J., Nielsen, J. P., & Pritchard, P. (2007). Using external data in operational risk. *The Geneva Papers on Risk and Insurance. Issues and Practice, 32*(2), 178–189. https://doi.org/10.1057/palgrave.gpp.2510129

Hacked Slowmist. (2021). Blockchain and DeFi hack database. Retrieved February 20, 2022, from https://hacked.slowmist.io/en/.
Halborn. (2021). *How blockchain DDoS attacks work*. Retrieved May 20, 2023 from https://www.halborn.com/blog/post/how-blockchain-ddos-attacks-work.
Han, L., Li, D., Moshirian, F., & Tian, Y. (2010). Insurance development and economic growth. *The Geneva Papers on Risk and Insurance. Issues and Practice, 35*(2), 183–199.
Hickman, J. C., & Miller, R. B. (1970). Insurance premiums and decision analysis. *The Journal of Risk and Insurance, 37*(4), 567. https://doi.org/10.2307/251065
Jensen, J. R., Von Wachter, V., & Ross, O. (2021). An introduction to decentralized finance (DeFi). *CSIMQ*. https://doi.org/10.7250/csimq.2021-26.03
Kar, A. K., & Navin, L. (2021). Diffusion of blockchain in insurance industry: An analysis through the review of academic and trade literature. *Telematics and Informatics, 58*, 101532. https://doi.org/10.1016/j.tele.2020.101532
Karp, H., & Melbardis, R. (2017). *Nexus mutual whitepaper: A peer-to-peer discretionary mutual on the ethereum blockchain*. Retrieved March 10, 2021, from https://nexusmutual.io/assets/docs/nmx_white_paperv2_3.pdf.
Kshetri, N. (2020). The evolution of cyber-insurance industry and market: An institutional analysis. *Telecommunications Policy, 44*(8), 102007. https://doi.org/10.1016/j.telpol.2020.102007
Le Cam, L. (1986). The central limit theorem around 1935. *Statistical Science, 1*(1), 78–91.
Lehar, A., & Parlour, C. A. (2022). Systemic fragility in decentralized markets. *SSRN*. https://doi.org/10.2139/ssrn.4164833
Lehtonen, T., & Liukko, J. (2011). The forms and limits of insurance solidarity. *Journal of Business Ethics, 103*, 33–44.
Li, X., Chen, T., Luo, X., Zhang, T., Yu, L., & Xu, Z. (2020). STAN: Towards describing bytecodes of smart contract. In *Proceedings of the 20th IEEE international conference on software quality, reliability and security (QRS)*. https://arxiv.org/pdf/2007.09696.
Liedtke, P. M. (2007). What's insurance to a modern economy? *The Geneva Papers on Risk and Insurance. Issues and Practice, 32*(2), 211–221.
Mehr, R. I., & Cammack, E. (1976). *Principles of insurance. Irwin series in insurance and economic security*. R. D. Irwin.
Nadler, M., Bekemeier, F., & Schär, F. (2022). DeFi risk transfer: Towards a fully decentralized insurance protocol. In *2023 IEEE international conference on blockchain and cryptocurrency (ICBC)* (pp. 1–9). Dubai, United Arab Emirates, 2023. https://doi.org/10.1109/ICBC56567.2023.10174937.
Neale, F. R., Drake, P. P., & Konstantopoulos, T. (2020). InsurTech and the disruption of the insurance industry. *Journal of Insurance Issues, 43*(2), 64–96.
Nendel, M., Riedel, F., & Schmeck, M. D. (2021). A decomposition of general premium principles into risk and deviation. *Insurance: Mathematics and Economics, 100*, 193–209. https://doi.org/10.1016/j.insmatheco.2021.05.006
NexusMutual Gitbook. (2022). *Glossary & appendices*. Retrieved September 17, 2022, from https://nexusmutual.gitbook.io/docs/welcome/glossary-and-appendices#defined-terms.
NexusTracker. (2022). *Nexus mutual tracker*. Retrieved March 04, 2022, from https://nexustracker.io/.
NIST. (2023). *Information technology laboratory—Computer security resource center glossary, definition of "private key"*. Retrieved June 08, 2023 from https://csrc.nist.gov/glossary/term/private_key.
OECD Stat. (2022). *Insurance indicators*. Retrieved February 10, 2022, from https://stats.oecd.org/Index.aspx?DataSetCode=INSIND.
O'Hare, D. (1994). The need for insurers to change. *The Geneva Papers on Risk and Insurance. Issues and Practice, 19*(72), 357–364.
Olivieri, A., & Pitacco, E. (2011). *Introduction to insurance mathematics: Technical and financial features of risk transfers*. Springer. https://doi.org/10.1007/978-3-642-16029-5
Osterland, T., & Rose, T. (2020). Model checking smart contracts for ethereum. *Pervasive and Mobile Computing, 63*, 101129. https://doi.org/10.1016/j.pmcj.2020.101129
Oxford Learners Dictionary. (2023). *Definition of "formalization" noun from the Oxford Advanced Learners Dictionary*. Retrieved May 20, 2023, from https://www.oxfordlearnersdictionaries.com/definition/english/formalization.
Peters, G., Shevchenko, P. V., & Cohen, R. (2018). Understanding cyber-risk and cyber-insurance. *Macquarie University Faculty of Business & Economics Research Paper*. https://ssrn.com/abstract=3200166.

Petrov, S. (2017). *Another parity wallet hack explained*. Retrieved November 23, 2021, from https://medium.com/@Pr0Ger/another-parity-wallet-hack-explained-847ca46a2e1c.

Popescu, A. (2020). Decentralized finance (Defi)—The Lego of finance. *Social Sciences and Education Research Review, 7*(1), 321–348.

Pottier, S. W., & Sommer, D. W. (1997). Agency theory and life insurer ownership structure. *The Journal of Risk and Insurance, 64*(3), 529. https://doi.org/10.2307/253763

Punter, A. (2002). Reinventing re/insurance for the twenty-first century. *The Geneva Papers on Risk and Insurance. Issues and Practice, 27*(1), 102–112.

Qin, K., Zhou, L., Livshits, B., & Gervais, A. (2021). Attacking the DeFi ecosystem with flash loans for fun and profit. *Lecture notes in computer science book series, LNSC* (Vol. 12674, pp. 3–32). Springer. https://doi.org/10.1007/978-3-662-64322-8_1

Quadriga Initiative. (2022). *A community-based, not-for-profit crypto watchdog & fraud recovery platform*. Retrieved February 25, 2022, from https://www.quadrigainitiative.com/index.php.

Richards, R. M. (1986). Insuring computer risks. *Computers & Security, 5*(3), 207–210. https://doi.org/10.1016/0167-4048(86)90012-X

Sayeed, S., Marco-Gisbert, H., & Caira, T. (2020). Smart contract: Attacks and protections. *IEEE Access, 8*(99), 24416–24427. https://doi.org/10.1109/ACCESS.2020.2970495

Schär, F. (2021). Decentralized finance: On Blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis review, second quarter 2021* (pp. 153–74). https://doi.org/10.20955/r.103.153-74.

Schmit, J. T. (1986). A new view of the requisites of insurability. *The Journal of Risk and Insurance, 53*(2), 320. https://doi.org/10.2307/252380

Singh, A., Parizi, R. M., Zhang, Q., Choo, K. R., & Dehghantanha, A. (2020). Blockchain smart contracts formalization: approaches and challenges to address vulnerabilities. *Computers & Security, 88*, 101654. https://doi.org/10.1016/j.cose.2019.101654

Stahel, W. R. (2003). The role of insurability and insurance. *The Geneva Papers on Risk and Insurance. Issues and Practice, 28*(3), 374–381.

Statista. (2021). *Total value locked (TVL) in multiple DeFi blockchains from May 2020 to November 2021*. Retrieved January 21, 2022, from https://www.statista.com/statistics/1272181/defi-tvl-in-multiple-blockchains/.

Swiss Re. (2017). *A history of insurance*. Retrieved November 10, 2021, from https://www.swissre.com/dam/jcr:638f00a0-71b9-4d8e-a960-dddaf9ba57cb/150_history_of_insurance.pdf.

Szabo, N. (1996). *Smart contracts: Building blocks for digital markets*. Retrieved January 04, 2022, from https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

Talonen, A. (2016). Systematic literature review of research on mutual insurance companies. *Journal of Co-Operative Organization and Management, 4*(2), 53–65. https://doi.org/10.1016/j.jcom.2016.09.003

Tapiero, C. S., & Jacque, L. (1987). The expected cost of ruin and insurance premiums in mutual insurance. *The Journal of Risk and Insurance, 54*(3), 594. https://doi.org/10.2307/253370

Van den Berghe, L. (1998). Shaping the future for the insurance sector. *The Geneva Papers on Risk and Insurance. Issues and Practice, 23*(89), 506–518.

Viglianisi, E., Ceccato, M., & Tonella, P. (2020). A federated society of bots for smart contract testing. *Journal of Systems and Software, 168*, 110647. https://doi.org/10.1016/j.jss.2020.110647

Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2021). SoK: Decentralized finance (DeFi). https://arxiv.org/pdf/2101.08778.

Wohrer, M., & Zdun, U. (2018). Smart contracts: Security patterns in the ethereum ecosystem and solidity. *International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 2018*, 2–8.

Wronka, C. (2023). Financial crime in the decentralized finance ecosystem: New challenges for compliance. *Journal of Financial Crime, 30*(1), 97–113. https://doi.org/10.1108/JFC-09-2021-0218

Wuthrich, M. V. (2013). *Non-life insurance: Mathematics & statistics*. Last modified February 22. https://ssrn.com/abstract=2319328.

Zhang, L., Wang, Y., Li, F., Hu, Y., & Au, M. H. (2019). A game-theoretic method based on Q-learning to invalidate criminal smart contracts. *Information Sciences, 498*, 144–153. https://doi.org/10.1016/j.ins.2019.05.061