

A Risk Classification Framework for Decentralized Finance Protocols

September | 2022



A Risk Classification Framework for Decentralized Finance Protocols

Exploring Emerging Risks for Insurers and Reinsurers

AUTHORS Tara Chang, OneDegree


Joe Ho, Hailstone Labs

Zachary Tirrell, FSA, FIAA

Gwen Weng, FSA, CERA, FCIA, Hailstone Labs

Jo You, OneDegree


SPONSOR Actuarial Innovation and Technology
Strategic Research Program Steering
Committee



Give us your feedback!

Take a short survey on this report.

[Click Here](#)



Caveat and Disclaimer

The opinions expressed and conclusions reached by the authors are their own and do not represent any official position or opinion of the Society of Actuaries Research Institute, the Society of Actuaries or its members. The Society of Actuaries Research Institute makes no representation or warranty to the accuracy of the information.

Copyright © 2022 by the Society of Actuaries Research Institute. All rights reserved.

CONTENTS

Section 1: Introduction	4
1.1 Overview	4
1.1.1 What is the Context?	4
1.1.2 Who are the Stakeholders in DeFi?	4
1.1.3 Who is the Intended Audience of this Paper?	5
1.1.4 What are the Contributions?	5
1.2 Contents	6
1.3 Discussing Risk	6
Section 2: Narrative Review	7
2.1 Risk Taxonomy Development	7
2.2 Operational Risk	7
2.3 Cyber Risks	8
2.4 Risks to DeFi	8
2.5 DeFi Risk and Insurance	9
Section 3: Information Sources and Methodology	10
3.1 Information Sources	10
3.2 Methods of Analysis	11
Section 4: The Proposed Risk Framework	13
Section 5: Discussion of the Risk Classification Framework	16
5.1 Overview	16
5.2 Smart Contract Technical Risk	16
5.3 Economic Design Risk	19
5.4 Cybersecurity Operational Risks	22
5.5 Blockchain Infrastructure Risk	25
Section 6: Conclusions	27
Section 7: Acknowledgments	28
Section 8: References	29
Appendix A: Risk Categorization and Definitions Identified in the Review of Relevant Literature	34
Appendix B: Glossary – Commonly used DeFi Terms	37
About The Society of Actuaries Research Institute	40

A Risk Classification Framework for Decentralized Finance Protocols

Exploring Emerging Risks for Insurers and Reinsurers

Section 1: Introduction

1.1 OVERVIEW

1.1.1 WHAT IS THE CONTEXT?

Decentralized finance (DeFi) is an emerging and rapidly growing financial ecosystem with the defining feature that it is powered by blockchain technology. While traditional financial systems are a collection of institutions (e.g., banks and insurers), DeFi is an ecosystem of decentralized applications or protocols. DeFi protocols are powered by smart contracts, which are computer programs that are executed on a blockchain. Smart contracts enable business logic and contractual agreements to be executed without human intervention. In the context of DeFi, smart contracts are built and used on public blockchains, and are self-executing¹, publicly available² and composable³. The open-source nature of smart contracts requires higher assurance development practices, which are still evolving in the DeFi space. The DeFi ecosystem is still in its nascent stage with rapid technological innovations. Naturally, this emerging market is associated with a range of risks, some new and unique to DeFi, while others are risks seen in traditional financial services.

1.1.2 WHO ARE THE STAKEHOLDERS IN DEFI?

Jensen, Von Wachter, and Ross (2021) set out four agents in the DeFi environment: Users of the application (users), those who supply the capital to ensure liquidity (liquidity providers), market participants who strategically purchase and sell assets - generally to support an equilibrium (arbitrageurs), and the team that designs, implements and maintains the protocol (application designers). We highlight two additional stakeholders:

- insurers, insurance solution providers, and risk managers, who we believe will play an increasingly prominent role in the DeFi ecosystem as it matures; and
- investors and speculators (speculators) who seek profit through the purchase and sale of assets.

¹ Self-executing: The execution of smart contracts is autonomous when predetermined conditions are met.

² Publicly available: The compiled bytecode of a smart contract is on the blockchain, and the human-readable source code of a smart contract is usually also publicly available.

³ Composable: Smart contracts can communicate and interact with each other and can be used as building blocks in new applications.

Figure 1
STAKEHOLDERS IN THE DEFI ECOSYSTEM



1.1.3 WHO IS THE INTENDED AUDIENCE OF THIS PAPER?

This paper proposes a risk classification framework relevant for (re)insurers considering the risks of the DeFi environment. Consequently, the focus of this paper is on risks for DeFi protocols that could lead to economic losses that could be insurable. This framework was designed around the risks associated with the existing and emerging DeFi protocols.

As DeFi develops, so does the opportunity for traditional insurers in the DeFi ecosystem. We speculate that insurers (and reinsurers) will initially address the needs of liquidity providers interested in solutions that protect against DeFi risks, which this paper may support. Therefore, the intended audience of this paper is for traditional insurers and reinsurers interested in the DeFi market. However, it also can support other stakeholders in the DeFi ecosystem in understanding the risks from the perspective of a protocol. This research paper also aims to increase awareness within the actuarial professional community about this rapidly developing industry and its emerging risks and opportunities.

1.1.4 WHAT ARE THE CONTRIBUTIONS?

There has been limited research to support the risk management process and strategic decisions for DeFi protocols. There is no consistent risk classification even for the limited scope of risks focused on smart contracts (de Sousa Matsumura, dos Santos, Conceição, & Vijaykumar, 2021) or digital assets more generally. Among other uses, this classification framework could guide the product design, offering and underwriting practices of a new generation of insurance and risk management products for DeFi. As noted above, it also adds to the body of evidence for actuaries to increase their familiarity with the DeFi ecosystem.

1.2 CONTENTS

The structure of this paper is as follows:

- Section 2 - a narrative review of relevant topics in published literature
- Section 3 - description of the data source and methodology for our analysis of past risk events
- Section 4 - our proposed risk classification framework of DeFi protocols
- Section 5 - discussion of the risk classification framework

The narrative review in section 2 considers the development of this risk classification framework generally. This review also summarizes the existing research on the risks and risk categorization for DeFi protocols. Following this review, we have set out the following framework development principles:

- The framework should be easy to use for the end-users
- Classifications should be mutually exclusive and collectively exhaustive
- The structure should be ‘future-proofed’ to be relevant for both current and future risks
- The framework should be generic enough for adaptation by different end-users – while being supported by the granular detail for the risks that are the focus of the study in this report.

Section 3 outlines the approach to developing an incident database of risk sources and the attack methods for known economic loss events for DeFi protocols and their users. This database is also discussed in section 5. We focus on economic losses that are not related to price volatility because other financial instruments, such as derivatives, may be more suitable for managing price volatility rather than insurance. The economic losses that we are interested in are the result of a risk event, such as a hacker stealing funds from the protocol, since potential insurance policyholders are more likely to use insurance to protect themselves against these risk events. This incident database aims to highlight relevant case studies to inform a risk classification framework.

The analysis of loss events, the narrative review, and our understanding of DeFi protocols culminate in section 4 with the proposed risk classification framework for DeFi protocols for insurers and reinsurers. The discussion in this section and section 5 centers on smart contracts, blockchains, and cybersecurity operational risks in the DeFi ecosystem because we have stronger support for these risks from the analysis of the incident database. We also present a selection of other key risks that are most relevant for DeFi protocols. However, the risks in the aforementioned categories may be more relevant to insurers, given the current state of DeFi.

1.3 DISCUSSING RISK

We developed the risk categories in our framework based on the analysis above. We aligned our language about risk with ISO 31000 terminology (International Organization for Standardization, 2018), which

- defines risk as the ‘effect of uncertainty on objectives’...’usually expressed in terms of risk sources, potential events, their consequences and their likelihood’;
- considers the elements that give rise to risk as a ‘risk source’ (instead of hazards, perils, or vulnerabilities); and
- uses the term event(s) (or risk event(s)) to refer to the actualization of a risk that changes the circumstances with resultant consequences affecting objectives.

This definition allows for both upside and downside risks. However, the focus of this paper is on insurable/downside risks.

Section 2: Narrative Review

2.1 RISK TAXONOMY DEVELOPMENT

The categorization of risk may be by the source of risk or by ‘consequence, aspects or dimensions of objectives or performance’ (ISO 31010: (2019)). Published risk classifications generally present high-level risk categories aligned with standard convention and the regulatory context. Many risk taxonomies are adaptations of the categorizations set out for financial service organizations by the Basel Committee (1994) and the Global Derivatives Study Group (1993), such as Kelliher (2013), or more generic frameworks, such as Hardy (2013) and Bender & Panz (2020).

To highlight the type of approaches to risk classifications, we briefly review two broad risk categories that have been the area of focus for many institutions since the Global Financial Crisis. First, we discuss literature and learnings from risk taxonomies in operational risk in subsection 2.2. Second, we highlight the development of cyber risk classification in subsection 2.3.

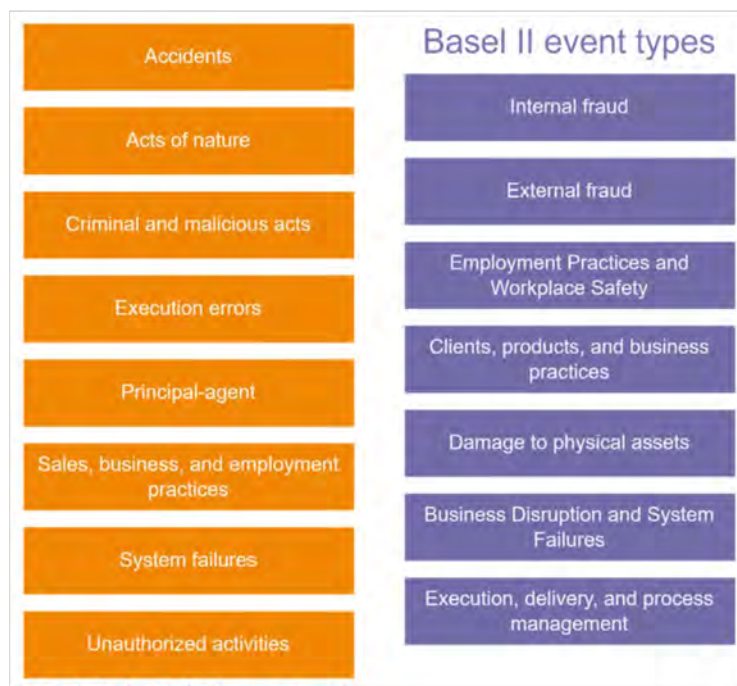
This section closes by considering the risks to DeFi in subsection 2.4 and DeFi risk and insurance in subsection 2.5.

2.2 OPERATIONAL RISK

Operational risks are prone to overlapping with or being embedded within ‘traditional’ risk categories. Since risk classification will affect management decisions, it is crucial to attribute the impact of operational risks. Without identifying the operational risks, they cannot be managed. From this perspective, it is necessary to take a pragmatic approach and consider operational risks from a management perspective. Toward this aim, operational risk taxonomies should consider how events can be grouped into a homogeneous class to support their management (OpRisk Advisory and Towers Perrin, 2010). Further, OpRisk Advisory and Towers Perrin set out that the development of these risks should consider not just the events but also whether the contributory factors are endogenous or exogenous and their effect.

Two categorization approaches are set out in Figure 2. While these may not reflect current or best practices, they are two thoughtful approaches for the high-level categorization of operational risks.

Figure 2
OPERATIONAL RISK CATEGORIES



OpRisk Advisory and
 Towers Perrin (2010)

2.3 CYBER RISKS

Cyber risks emanate from the use and transmission of electronic data (CRO Forum, 2016). The prevailing taxonomy was proposed in the CRO Forum (2016), which includes four groupings:

- System malfunction/issue
- Data confidentiality
- Data integrity/availability
- Malicious activity

Since it can be considered a type of operational risk, cyber risk can also be mapped to the Basel II operational risk type categories (Curti, Gerlach, Kazinnik, Lee, & Mihov, 2019). In the first instance, the categorization of cyber risks should consider the intent (intentional vs unintentional), root causes, actors, and impact type (CRO Forum, 2016).

2.4 RISKS TO DEFI

Despite the relative infancy of DeFi, there has been some consideration of the risks in the literature. The risks in DeFi are both inherited and unique. The inherited risks include those from traditional financial services, cryptocurrencies, public blockchain technology, and project risk for emerging innovative and nascent technology. The risks are also unique due to the interacting nature of the risks in this ecosystem. However, there has been limited attention from professional risk managers (although this is growing).

A summary of findings and relevant citations from our review of the relevant literature are set out in Appendix A. This review is aligned with the focus of the paper, so is primarily concerned with risk categorization and risks in DeFi that are relevant to DeFi protocols. The findings from this review have informed the development of the proposed framework contained in section 4.

2.5 DEFI RISK AND INSURANCE

Due to the growth of the DeFi ecosystem and the abundance of risks in the space, there is an increasing demand for the management and transfer of these risks both from retail investors and institutional investors. DeFi protocol users or investors can use different mitigation strategies to protect themselves and manage their risk exposure. Other than traditional portfolio management techniques, such as hedging and diversification, and performing their research and due diligence, purchasing insurance, or “covers,” is one of the most straightforward and effective ways to protect against risks associated with DeFi protocols.

However, due to complexity, variety, and limited experience data, the risks in DeFi protocols have not been widely studied. In the current market of insurance and risk solutions for DeFi risk management, it is not a prevalent practice that risks are explicitly used in the pricing and reserving process. Instead, the pricing models are often driven by factors related to the supply and the demand of the coverages. Generally speaking, the greater the supply of capital to support the coverages, the lower the demand for the coverages, and the cheaper the coverage will be for policyholders. For a review of the current landscape of existing insurance solutions, see SOA research paper “Decentralized Insurance Alternatives: Market Landscape, Opportunities and Challenges.” Additionally, there is a general reluctance from insurers and reinsurers to enter this space, perhaps due to a lack of credible experience data, underwriting expertise or contextual limitations (e.g., regulatory). This gap posts a barrier for insurers, reinsurers, and risk managers to navigate and benefit from the new emerging financial system. This paper proposes a risk classification framework, which is the first step in developing robust actuarial framework around these risks.

Section 3: Information Sources and Methodology

This section provides an overview of the information sources and methodology used in the research for developing the risk classification framework.

3.1 INFORMATION SOURCES

After the initial literature review, the first task of this research was to collect historical incidents of hacks, exploits, and other events that led to economic losses from DeFi protocols. The majority of the incidents covered in this study were gathered from SlowMist, a blockchain security firm. The data collection process is a combination of web scraping and manual processing. The data covers all the past incidents up to the year-end of 2021. We observe that many notable DeFi incidents have occurred in 2022 and will continue to occur in the future. These newer incidents are generally out of scope for this paper, but some notable developments are mentioned in the footnotes. Our intention is to set up a framework that can be applied to all past and future incidents.

For each incident, the following attributes are provided by the database and collected by the researchers: the hacked target (name of the DeFi protocol), amount of loss (could be denominated in U.S. dollars or crypto assets), attack method as assessed by SlowMist, and references. Even though the attack method is one of the available attributes, we do not directly use it in the analysis as we undertake independent assessments.

Despite collecting all the entries from the database, the research focused on the Ethereum (ETH) ecosystem and the Binance Smart Chain (BSC) ecosystem⁴. The ETH chain was launched in 2015 and DeFi activities emerged in 2017. The BSC chain was launched in September 2020. Both of these ecosystems have significant total value locked and have a significant number of protocols that could be potential attack targets (DeFi Llama, 2022). Since ETH and BSC are Ethereum Virtual Machine (EVM)-compatible, consistent analysis methods could be applied across them.

Overall, 132 incidents in the ETH ecosystem of incidents⁵ and 47 from the BSC ecosystem were collected. Incidents from Avalanche and Polygon were also reviewed, but they are excluded from the research statistics as the incidents on those chains are not distinct from the incidents on ETH and BSC.

The second task of this research was to collect multiple sources of analysis of these incidents beyond the references provided by the original database. This is desired because multiple sources may provide more comprehensive information and different perspectives. Google, a search engine, and Twitter, a social media platform, are primarily used to search. For each incident, the research team collected at least two of the types of sources below:

- News articles from news websites reporting on the incidents,
- published analysis articles from blockchain security firms, and
- analysis and commentary from well-known security researchers in the blockchain space.

Subsequently, we excluded two incidents, one due to a lack of public information and the second due to a duplicated entry.

Additional incidents were identified and included based on the knowledge of the authors. For example, six incidents of stablecoin depeg events are included. The native networks of the corresponding stablecoin protocols span across

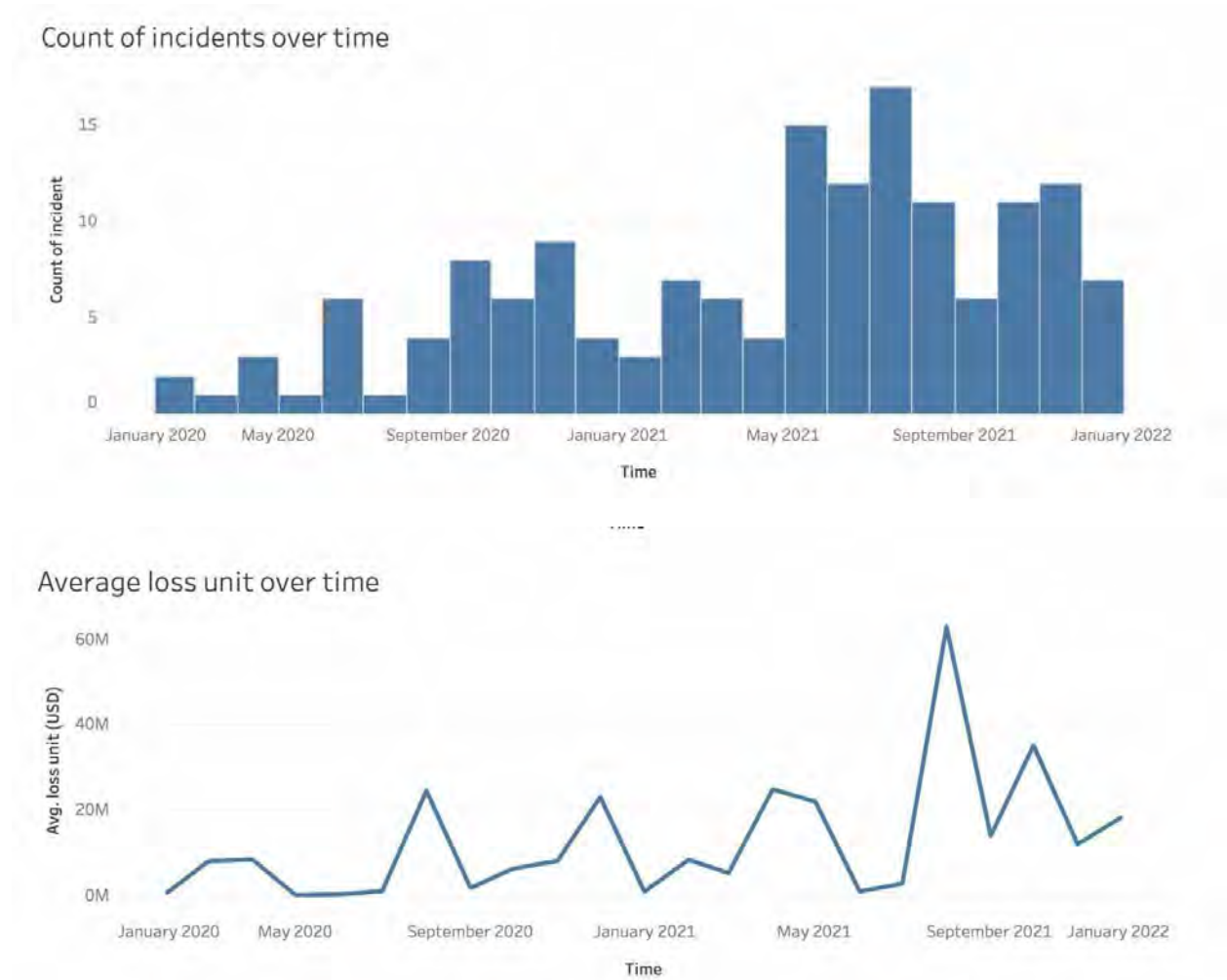
⁴ We noted that there were relevant cases labeled as "DEX" in the database that could be re-labeled as belonging to the ETH or BSC ecosystem and adjustments were made accordingly.

⁵ Excluding one incident which was mislabeled and did not occur on ETH.

ETH, Avalanche, Polygon and Terra. There are also two vulnerability reports on potential price manipulation on ETH, and two cases of base network malfunctions on Evmos and Solana.

While not the focus of this study, we observed increasing frequency and severity of events over time. This is consistent with the growth that the DeFi ecosystem has experienced from 2020 up until the end of 2021.

Figure 3
DEFI INCIDENTS OVER TIME



3.2 METHODS OF ANALYSIS

With the compiled data, we reviewed the sources for each incident and extracted several variables, including, but not limited to:

- basic information, including the DeFi protocols impacted, date of the incident, and the amount of loss denominated in cryptocurrencies and U.S. dollar, if applicable,
- whether the impact was cross-chain,
- whether the incident was malicious, meaning that the incident was initiated by an ill-intended attacker with the goal of personal gain and financial or reputational harm to the victim,
- the root cause, or the most prominent and impactful factor leading to the compromise, according to our risk identification framework, which is a tree-like model that branches out into the risk taxonomy.

In this report, we did not summarize all the information we collected, rather, we focused on the information useful for risk classification.

During our analysis, we first categorized incidents based on whether the incident was related to the smart contracts developed and deployed by the protocol, as they provide the primary functions of DeFi protocols. If an incident was related to a protocol's smart contracts, we then determined if the issue was primarily due to technical vulnerabilities in the smart contracts or any faulty economic design embedded in the smart contracts. Some incidents were not directly related to the protocol's own smart contracts. Amongst those incidents, some were pertinent to the blockchain network powering DeFi protocols. Those vulnerabilities could apply to any generic protocol. The rest of the incidents that were specific to the protocol are related to cybersecurity and operational issues, with further categorizations based on the Basel II event types.

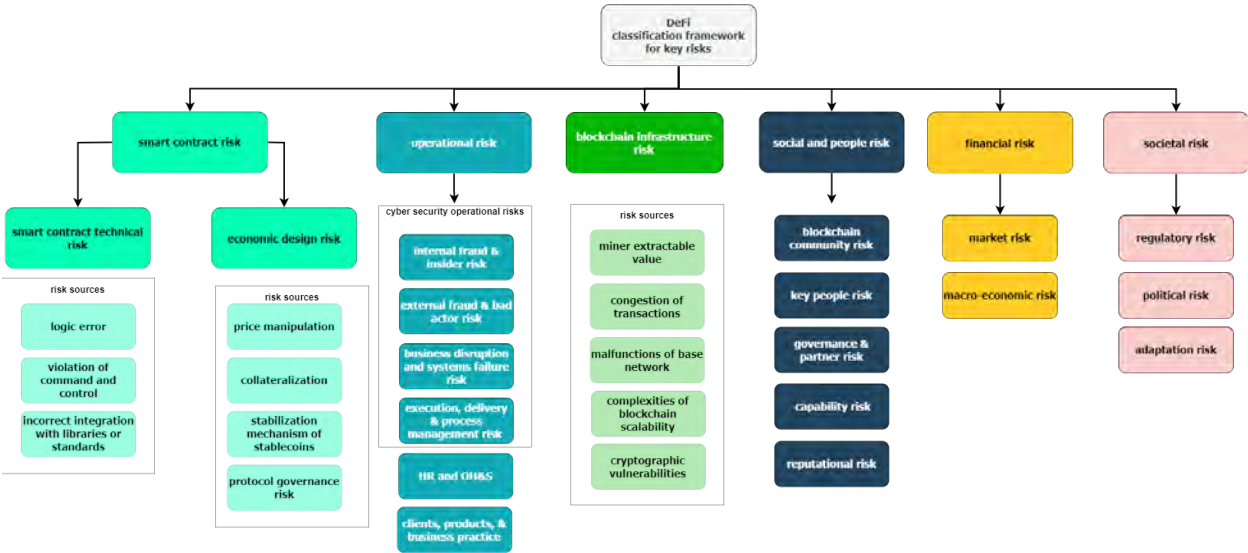
Our analysis was focused on the risk sources that enabled the realization of the risk events in our incidents database. However, there was one notable exception. The existence of funding mechanisms for potential attacks (e.g., "flash loan attacks") is a single risk source that cannot lead to a risk event in isolation, so we did not solely focus on that risk source (i.e., the funding mechanism does not contribute to the other risk source that is being exploited).

To study the incidents beyond using the sources discussed in section 3.1, we consulted existing frameworks for cybersecurity analysis, such as the CIA triad model and the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework built by the MITRE Corporation. However, we did not share all the details of our analysis due to the limited scope of the paper.

Section 4: The Proposed Risk Framework

We propose a generic risk classification framework for DeFi protocols in Figure 3. While a selection of subcategories is presented, this taxonomy is not exhaustive at the subcategory or risk level.

Figure 4
 DEFI: CLASSIFICATION FRAMEWORK FOR KEY RISKS



The focus of this report is on the risks set out in Table 1, which were developed based on our research on the incident database. There may be gaps in areas outside of this focus due to a lack of formally collected experience data. Also, because our paper’s primary goal is to provide information for insurance purposes, we focused on economic losses associated with the risks set out in Table 1.

Table 1
CATEGORIES OF RISK BASED ON INCIDENT DATABASE

Risk Category (RC)	Definition	Risk Sources	Case Count from Incident Database ⁶
Smart contract risk – Smart contract technical risk	The risk of a defect or an error in the code causing the contract to operate in ways unexpected by the developers.	<ul style="list-style-type: none"> ● Logic error ● Violation of command and control ● Incorrect integration with libraries or standards 	85
Smart contract risk – Economic design risk	The risk of a design fault in a protocol’s resource allocation mechanism or incentive structure that causes it to be vulnerable to exploitation or unforeseen market conditions.	<ul style="list-style-type: none"> ● Price manipulation ● Collateralization failures ● Dysfunctional stabilization mechanism of stablecoins ● Protocol governance 	48
Cybersecurity operational risk	The risk of deficient cybersecurity controls or faulty operational procedures, including the exploitation of human factors and system vulnerabilities.	<ul style="list-style-type: none"> ● Internal fraud ● External fraud ● Business disruption and system failures ● Execution, delivery and process management 	50
Blockchain infrastructure risk	The risk of negative externalities, inefficiencies and malfunctions associated with the blockchain settlement layer and scaling solutions.	<ul style="list-style-type: none"> ● Maximal Extractable Value (MEV) ● Congestion of transactions on-chain ● Malfunctions of base networks ● Complexities of blockchain scalability ● Cryptographic vulnerabilities 	4

In addition to the risks in Table 1, we have also proposed high-level categories of social and people risk, financial risk, and societal risk. These additional risks reflect some of the unique nature of the DeFi industry. For example, blockchain community risk is carved out from reputation risk because of the importance of this risk. Many DeFi

⁶ The case statistics are based on the classification of the primary risk source we identified. In some cases, there are multiple risk sources at play and we discuss the interaction between them in subsection 4.5.

protocols employ individuals to engage with the DeFi community and actively manage this risk. As noted above, the subcategories serve as a starting point for considering risks beyond those in Table 1. We define these additional risks:

- Operational risk
 - HR and OH&S – the risks associated with HR practices and operational health and safety.
 - Clients, products, and business practices – ‘Unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product’⁷.
- Social and people risk
 - Blockchain and community risk – the risks associated with the perception of established blockchain communities and individuals.
 - Key people risk – a subcategory of risk concerned with the performance (e.g., due to capability, focus, or execution) or departure of significant individuals in the organization as it affects retained knowledge, relationships, or available skills. A small team of application designers in a DeFi protocol elevates this risk.
 - Governance and partner risk – the risk that the association of those with an ownership stake in or partner status with a DeFi protocol affects its reputation or financial performance.
 - Capability risk – the risk associated with the skills of those involved in the DeFi protocol, including the development team, community engagement, or leadership team.
 - Reputational risk – the risk that the DeFi protocol is impacted or suffers a loss from negative opinions among stakeholders or the general public, often due to actions of the entity or associated persons.
- Financial risk
 - Market risk – the risks associated with market price changes affecting the operations or viability of the DeFi protocol. This could include the contagion effect where the success and failure of one token could have wide-ranging impacts across multiple protocols that integrate the token.
 - Macroeconomic risk – the risks associated with business cycles, inflation, or other macroeconomic factors.
- Societal risk
 - Regulatory risk – the risk of regulatory scrutiny, regulation that impacts the protocol or its reputation.
 - Political risks – the risks associated with changes in the political environment that affect the DeFi protocol.
 - Adaptation risk – the risks of societal views negatively affecting adaptation.

⁷ [Sound Practices for the Management and Supervision of Operational Risk \(bis.org\)](https://www.bis.org/publ/pract/pract.htm)

Section 5: Discussion of the Risk Classification Framework

5.1 OVERVIEW

Due to the unique dependency of DeFi protocols on smart contracts and blockchains, we proposed the top-level risk categories to be:

- Smart contract risk - with two key subcategories of ‘smart contract technical risk’ and ‘economic design risk’
- Operational risk, with a focus on cyber security operational risks
- Blockchain infrastructure risk
- Financial risk
- Social and people risk
- Societal risk

The first four categories are considered in greater depth in the remainder of this section.

Given the pivotal role of smart contracts in DeFi protocols, risks endogenous to smart contracts developed by the protocols are a key focus of our study. We decompose smart contract risks into two broad categories:

Smart contract technical risk is the risk of a defect or an error in the code causing the contract to operate in ways unexpected by the developers. Technical vulnerabilities are caused by technical code design and implementation of smart contracts. For example, an attacker could create excessive assets with certain exploited functionalities of a protocol. The smart contract technical risk and its risk sources are discussed in subsection 5.2.

Economic design risk is the risk of a design fault in a protocol’s resource allocation mechanism or incentive structure that causes it to be vulnerable to exploitation or unforeseen market conditions. For example, this risk could materialize with an attacker taking advantage of loopholes in governance voting rules to seize control of the protocol’s treasury. Some malicious attacks were only successful because of a combination of both technical and economic design vulnerabilities. The economic design risk and risk sources are discussed in subsection 5.3.

We also highlight risks exogenous to smart contracts developed by the protocols in two broad categories:

Cybersecurity operational risk is the risk of deficient cybersecurity controls or faulty operational procedures, including the exploitation of human factors and system vulnerabilities. Such incidents may be caused by unintentional issues, such as human errors or system failures, or they can be malicious, such as attacks from hackers. Cybersecurity operational risks are exogenous to smart contracts developed by the protocols, but may include processes that interact with the development, deployment, and management of contracts. This is discussed further in subsection 5.4.

Blockchain infrastructure risk concerns the negative externalities, inefficiencies and malfunctions associated with the lower layer that DeFi applications are built upon. These issues can lead to varying degrees of economic loss, ranging from unfair pricing and transaction delay for users to settlement-layer level exploits. This risk is discussed further in subsection 5.5.

5.2 SMART CONTRACT TECHNICAL RISK

Smart contract technical risk is the most prominent risk category based on the number of incidents in the incident database. In many of the incidents we analyzed, the economic losses were a result of malicious external attacks. An external attacker exploits one or multiple technical vulnerabilities to manipulate the behavior of a protocol’s smart

contracts to drain the protocol's economic resources. Also, due to the composability characteristic of DeFi protocols, a single exploit could lead to cascading effects, as seen in the ChainSwap exploit_(ChainSwap, 2021), and the impact on other protocols, such as Umbrella Network (2021), and DAOVentures (2021).

Our analysis finds smart contract technical risk to manifest in three main ways.

Table 2
RISK SOURCES OF SMART CONTRACT TECHNICAL RISK

Risk Source	Description
Logic error	Loopholes in the smart contract that cause the contract to operate incorrectly or produce unintended behavior
Violation of command and control	Improper access management that allows users to perform unauthorized actions
Incorrect integration with libraries or standards	Misuse of external libraries and standards that cause the contract to perform unintended actions

Logic Error

Logic errors are a risk source arising from loopholes in the technical model design or implementation of a smart contract that causes the contract to operate incorrectly or produce unintended behavior. A large portion of DeFi incidents are a result of the execution of malicious codes that exploit logic errors. These logic errors may allow attackers to manipulate the contract's behavior and obtain economic resources at the expense of the protocol and its users. In some cases, even in the absence of an attacker or a beneficiary, logic errors can lead to code malfunction and irrecoverable losses (see, for example, Hegic (Hegic, 2020) and TBTC (TBTC, 2020)).

Some errors are surprisingly simple and could be identified and mitigated during code testing. Some DeFi projects were pieced together from existing codes from other DeFi protocols without adequate examination, resulting in vulnerabilities. Even if secure coding principles are followed and thorough testing is done, it is difficult to guarantee bug-free implementation⁸ of smart contracts without formal verification methods⁹.

Based on our analysis of past incidents, we found a few common errors that enabled the attacks:

- Unsafe math operations
- Inconsistency in code structure
- Missing validation in user-supplied values
- Improper error handling

Logic errors can be highly complex and manifest in unexpected ways, so the above list is only a starting point.

Unsafe math operations could manifest in multiple ways, such as mishandling of boundary conditions and inappropriate use of complex functions. For example, rounding errors occur when a value is rounded off to a certain degree of precision, resulting in a difference from the actual value. Overflow and underflow errors occur when an

⁸ The difficulty also varies depending on development programming languages and the design of the underlying infrastructure of blockchains. The details are out of the scope of this paper.

⁹ Formal verification methods use mathematical proofs to validate smart contracts.

arithmetic operation causes the resulting value to exceed the maximum or minimum value a type can store. An attacker may exploit these limitations to inappropriately accumulate funds or bypass/circumvent the intended operation of the code (for example, BeautyChain (SECBIT, 2020), Alpha Homora (Halborn, 2021), and ValueDefi (ValueDefi, 2021)). Some tools, such as vetting libraries, can identify some of these errors.

Inconsistency in code structure refers to issues relating to how components (parameters, functions, etc.) of smart contracts interact and work together (for example, the THORChain hack (Halborn, 2021)). Inconsistency in code structure can cause minor operational glitches or total failures during user interactions. Sometimes, the inconsistency is introduced during contract upgrades when some components are changed without proper considerations given to the rest of a contract (see, for example, PercentFinance (2020)).

Missing validation in user-supplied values can expose a protocol to unexpected exploits or malfunction. This issue is pertinent to the inappropriate use of variables and functions, which often involves false inputs that can pass through validations. As a principle of secure coding, developers should always be cautious when it comes to user-supplied data. Specifically, the code must implement multiple layers of validation by strictly sanitizing the received information in each component. The lack of such scrutiny may allow an attacker to manipulate the contract and steal funds (for example, Origin Protocol (OriginProtocol, 2020) and PickleFinance (Halborn, 2020)).

Improper error handling occurs when an execution error is not processed appropriately. Smart contracts can experience errors during execution. In some cases, existing protocols do not explicitly define how errors should be processed, thus the error handling mechanism varies across the implementation. For instance, the ERC-20 standard does not mandate if a failed token transfer should result in a reversion or a returned 'False' value, thus both are considered valid outcomes. Hence, developers are responsible for weighing both options, implementing the logic accordingly, and maintaining consistency throughout the program (ForceDAO, 2021).

Violation of Command and Control

Violation of command and control are implementation errors in the security designs of smart contracts. It is crucial to define and control who can do what action. Otherwise, anyone would be able to perform critical operations and potentially compromise the protocol. Failure to secure critical and sensitive functions is equivalent to inviting attackers to enjoy escalated privilege and, in some cases, administrative permissions, which may lead attackers to:

- modify the parameters of a contract (e.g., (ChainSwap, 2021)),
- drain funds (e.g., (VetherAsset, 2020)), or
- claim ownership of a contract (e.g., Parity Wallet (Openzeppelin, 2017)).

Notably, contract initialization is a common attack angle (for example, DODO (Halborn, 2021), Value DeFi (SlowMist, 2021), DAO Maker (Coinfirm, 2021)).

Command and control management is particularly critical for protocols that handle cross-chain transactions. Weaknesses can be the starting point of sophisticated attacks, such as ChainSwap (ChainSwap, 2021) and PolyNetwork (Kudelskisecurity, 2021).

Incorrect Integration with Libraries or Standards

When leveraging existing libraries and standards, incorrect integration can lead to exploitable interactions. The complexity of DeFi is ever-increasing due to technological innovation and the composability of DeFi. Several token standards have been established over time, such as ERC-20 and ERC-777. Each token standard is designed with various features to support diverse application requirements. These advanced qualities could become pitfalls for many developers, as seen in cases of reentrancy attacks involving the ERC-777 standard (for example, Uniswap (Peckshield, 2020), Lendf.Me (ImToken, 2020)). There are also cases where developers misused existing libraries or

mis-integrated functions from other protocols (e.g., Rari Capital (Pitimanaaree, 2021)¹⁰). A developer should consider the potential pitfalls that advanced features present when identifying the desirable properties of integrable libraries or standards.

5.3 ECONOMIC DESIGN RISK

A DeFi protocol's economic design is its resource allocation mechanism and incentive structure. Resource allocation mechanisms refer to any rules and procedures determining the pricing and allocation of crypto assets. For example, a decentralized exchange determines the price and amount of assets involved in a trade with some mathematical functions. Alternatively, a lending protocol determines the value of loans available to a user based on the user's collateral amount. The incentive structure of a DeFi protocol is the economic incentive provided to users to achieve its goals, such as scalability of liquidity sizes, maintenance of target price pegs and balances of governance power.

Accordingly, economic design risks are risks that cause intentional exploits or market conditions to disrupt resource allocation mechanisms or incentive structures. Intentional exploits are often flaws of the economic design that allow opportunities for an economically equipped adversary to manipulate in such a way as to profit inappropriately at the contract's expense. On the other hand, unanticipated market conditions, such as exceedingly volatile price movements, may undermine the robustness and maintenance of protocols' economic designs.

Economic design risks identified here are not explicitly covered in current cyberattack frameworks, which can be further extended to incorporate them. The high-level attack stages of ATT&CK framework are also applicable to economic design-oriented attacks. For example, the funding mechanisms for launching attacks can be classified under resource development in ATT&CK.

¹⁰ For this case, we believe the main risk source is economic design but integration with an external protocol played a role.

Based on our analysis, economic design risk has manifested in four main ways as follows.

Table 3
RISK SOURCES OF ECONOMIC DESIGN RISK

Risk Source	Description
Price manipulation	Pricing model designs adopted by protocols may contain loopholes that allow distortion of exchange rates and mispricing of assets
Collateralization failures	Collateral systems adopted by protocols may lead to depletion of collateral reserves or even bank-run-like crises during adverse market conditions
Dysfunctional stabilization mechanism of stablecoins	Stablecoin protocols may fail to maintain stablecoins' ideal price pegs due to dysfunctional stabilization mechanisms
Protocol governance	Any protocol can be controlled by a minority of stakeholders, who may gain benefits from making protocol updates at the expense of the majority of stakeholders

Price Manipulation

We define pricing models as all models and methods that determine or gauge the value of assets. Pricing models have been one of the most common exploit targets in the DeFi space. We define price manipulation as a risk source associated with loopholes in pricing model designs that allow a distortion of exchange rates and mispricing of assets.

The pricing mechanisms backing automatic market makers (AMMs) have been a common source of DeFi exploits. In a typical AMM, liquidity providers supply two or more tokens in a pool, and the exchange rates between the tokens are derived from a liquidity-based formula such as the constant product function. That means the exchange rate of a token pair is usually determined by the token's relative liquidity in a pool. With sufficient capital, a user can significantly reduce the price of token A relative to token B by swapping a large amount of token A into token B. This action results in a pool with an excess of liquidity of token A relative to token B, which causes prices to deviate from market prices. In other words, large trading orders generally induce high price slippage in AMM, causing the AMM exchange rates to deviate from the market prices. Since DeFi protocols tend to interact with AMMs in various ways, the manipulatable AMMs have made them prone to attacks.

Most exploits require substantial capital to impose distortions on the prices or valuation of assets. Attackers usually borrow the required capital to launch their exploits. Flash loans are frequently leveraged as a major funding mechanism to manipulate the exchange rates on the AMM pools and other pricing models. They allow borrowers to make transactions with the borrowed funds in an instant and uncollateralized manner. Attackers may not possess sufficiently ample capital that can create huge imbalances in the AMM pools and, thus, flash loans facilitate the implementation of such exploits. Attackers also occasionally utilize leveraged lending as a funding mechanism, as it enables users to borrow assets that are multiple times the principal and execute trade orders with them.

There have been two major exploit types regarding AMM manipulation. One type exploits the AMM-based oracles. A vast amount of DeFi protocols rely on price quotes supplied by AMMs to gauge the value of assets and, thus,

attackers can create and profit from mispricings of asset values. Representative cases of this type include xToken (Cohen, 2021), Yearn Finance (Yearn Finance, 2021) and Harvest Finance (Harvest Finance, 2020). Another type takes arbitrage profits directly from the abnormal exchange rates on AMMs, as seen in the cases of Fei Protocol (OpenZeppelin, 2021), bZx (Kistner, 2020), and Balancer Protocol (McDonald, 2020). Pricing models other than AMM may also entail loopholes in asset valuations and, hence, room for exploits (e.g., Eminence Finance (The Defiant, 2020)).

Collateralization Failures

Many protocols rely on collateralization to ensure that their debts or issued tokens are backed by sufficient assets. Other than the pricing models' vulnerabilities, extreme and unfavorable market conditions can lead to failures of collateral systems. Lending and stablecoin protocols tend to back their issued debts with other crypto assets as collateral. Protocols generally require borrowers or stablecoin issuers to deposit collateral at a certain ratio in return for loans or stablecoins.

The collateralization ratio is measured by the collateral value to debt value, i.e.,:

$$\text{collateralization ratio} = \frac{\text{collateralized assets}}{\text{debt value}}$$

If this ratio falls below a predetermined threshold (as a result of decreasing collateral value and/or increasing debt value), the borrower or issuer needs to add enough collateral to meet the requirement or the debt position needs to be liquidated, i.e., the collateral is sold (often at a discount) to repurchase the corresponding assets to restore the collateralization ratio. Over-collateralization is commonly adopted by protocols to replace third-party custodians with decentralized operations. It requires the collateral value to outweigh debt issuance so that the issued debts are backed by sufficient collateral value even if the collateral price plunges during market turmoil. Despite this seemingly solid safety net, some protocols experience substantial drawdowns of collateral. The drawdowns may be exacerbated if the liquidation process leads to further sales when the purchasers of the discounted collateralized assets immediately sell the assets.

Under some unfavorable market conditions, the deleveraging process, similar to margin calls in traditional finance, could further aggravate the current price trends and undermine or even deplete the collateral reserves, creating a liquidation feedback effect. Such liquidation incidents may further develop into typical bank-run-like crises, in which a majority of users lose their confidence and pull their funds out of the protocols, depleting the protocols' reserves and resulting in systematic insolvency. A more serious impact is that the bank-run-like crises could be contagious among similar assets and protocols. The lack of confidence in one single asset or protocol could trigger runs on those with similar risk profiles and characteristics.

Stabilization Mechanism of Stablecoins

Stablecoin protocols¹¹ generally adopt certain stabilizing mechanisms that aim at anchoring the peg to fiat currencies and reducing the peg volatility. The majority of stablecoins are backed by collaterals, such as off-chain reserves (e.g., USDC, USDT), on-chain crypto assets (e.g., LUSD), or commodity-based (e.g., PAXG). Some other stablecoins are not fully backed by collaterals (e.g., UST, FRAX). Collateral-backed stablecoin protocols mainly incentivize traders to execute arbitrage trades between an external market (i.e., a market outside the protocol) and the internal market (i.e., within the protocol) such that any deviating rate can be pushed back to the target peg. Still, it is apparent that stablecoins usually trade at premiums or discounts against their target rates and some even lose their pegs. The failures can arise from collateralization (e.g., IRON (Iron Finance, 2021), arbitrage mechanisms (e.g., IRON (Kuznetsov, 2021)) and algorithmic adjustments¹² (e.g., Dynamic Set Dollar (Thurman, 2020)).

Protocol Governance Risks

Protocol governance stands for the structures and mechanisms by which a protocol determines and updates the protocol operations. Many protocols operate by community votes, e.g., how assets should be allocated. In particular, the governance parameters serve as terms and constraints directing and governing the participants' activities within the system. A governance risk would include if a small group of users (or a single user) controls a high enough share of tokens to alter the protocol at the expense of the majority of stakeholders. This risk is illustrated by Gudgeon, et al. (2020), and is seen in the incident of True Seigniorage Dollar (True Seigniorage Dollar, 2021).

Interactions between Technical and Economic Design Risks

Technical and economic design vulnerabilities may coexist and interact at the protocol level. This is similar to hurricane damage that can be caused by the wind and water. The existence of technical loopholes may allow a user to maliciously magnify the shortcomings of certain resource allocation mechanisms or incentive structures. As identified in the incident database, most of these cases involve price manipulation. Representative cases include Yearn Finance (Yearn Finance, 2021) and MonoX (MonoX Team, 2021).

5.4 CYBERSECURITY OPERATIONAL RISKS

Cybersecurity operational risks are well studied in existing literature, as discussed in section 2. In the DeFi ecosystem, even though the execution of the applications is decentralized on blockchains, the development and maintenance of applications are usually not decentralized¹³. This leaves room for attack vectors similar to those targeting centralized entities. In our research, we identified incidents in this category and classified them according to the well-developed Basel II operational risks event types. The meanings of "internal" and "external" could vary by protocols depending on their level of decentralization. The risk sources are summarized in the following table. Other risk event types from Basel II that are not included in the table (e.g., ET3) were not covered by our incident database.

¹¹ The discussion here revolves around non-custodial stablecoins, which operate on the blockchain network in a decentralized manner.

¹² Also, see the UST (Terra USD) crash in 2022 (Sandor & Genç, 2022).

¹³ Some protocols (i.e., Liquity protocol) have decentralized front-end development.

Table 4
CYBERSECURITY OPERATIONAL RISK SOURCES

Internal Fraud (ET1)	External Fraud (ET2)	Business Disruption and System Failures (ET6)	Execution, Delivery and Process Management (ET7)
<ul style="list-style-type: none"> ● Fraudulent scheme 	<ul style="list-style-type: none"> ● Social Engineering ● Intrusion ● Third-party service vulnerabilities 	<ul style="list-style-type: none"> ● Denial-of-service (DoS) ● Hardware or software service failures ● Centralized oracle failures 	<ul style="list-style-type: none"> ● Poor management of private keys ● Improper process setup or execution ● Governance process risk

Internal Fraud (ET1)

In the DeFi ecosystem, internal fraud is committed by an insider with sensitive knowledge of a DeFi protocol's inner operations. The most common form of internal fraud is fraudulent schemes or scams, which may be planned at different stages of a protocol. For instance, developers could set up a protocol as a fraudulent scheme from the very beginning. Alternatively, individuals may commit internal fraud after the project has gained substantial profit. Key contributors may decide to abandon the project and run away with users' funds, an action often referred to as a 'rug pull.'

Internal fraud is one of the most prominent risk sources and, according to Chainalysis' 2022 Crypto Crime Report, accounts for a loss of more than \$2.8B from victims in 2021 (see, for example, AnubisDAO_(Cryptoslate, 2021), Eleven Finance (Peckshield, 2021)).

External Fraud (ET2)

External frauds are activities committed by a third party that target the customers, employees, and systems of a DeFi protocol. This includes:

- Social engineering and malware
- Intrusion
- Third-party dependency

Social engineering and malware refer to cases where an attacker attempts to trick the victim into acting to the attacker's advantage, such as making fraudulent transactions, submitting sensitive information, or downloading malware. Several incidents followed the same pattern: the attacker created phishing sites to imitate legitimate services, then lured victims to authorize the malicious sites to transfer, swap, or migrate funds for them. Some incidents involved the purchase of online advertisement, so the phishing sites would precede the legitimate services in the search results (e.g., Bondly Finance_(Halborn, 2021)).

The intrusion of a DeFi protocol's or key contributors' system often targets the private keys and other administrative rights used to manage a protocol. This can be done via the direct hacking of private systems or via exploitation of vulnerabilities in external-facing services or the infrastructure. Once an attacker obtains access to the private keys or other administrative rights, they effectively gain full control over the wallet or smart contracts and can drain funds from them, for example, BadgerDAO_(Halborn, 2021), Phoenix Finance (PhoenixFinance, 2021), and BXH_(Forkast, 2021).

Third-party service vulnerabilities refer to the exploitation of or attacks on the third-party services that a DeFi protocol may rely on for daily operations. This includes a plethora of applications, including hardware devices (servers, routers, etc.), software packages (code libraries, antivirus, office software, program management, etc.), cloud platforms (AWS, Azure, GCP, etc.), and external service providers (DNS, etc.). When these upstream services are tightly embedded in a protocol's operations, they become part of the attack surface that hackers target. Vulnerabilities in the supply chain thus become the downstream clients' weaknesses (e.g., PancakeSwap (Pancakeswap, 2021)).

Business Disruption and System Failures (ET6)

Business disruption can arise from several factors, including hardware and software failures, attacks by a third party, unintentional incidents from providers, or deliberate damage orchestrated by an insider. Other than the blockchain infrastructure, which due to its high importance is categorized as a higher level risk (see subsection 5.5), there are other off-chain risk sources for business disruption and system failures. For example, DeFi protocols often utilize cloud platforms to deploy their services, reducing the probability and frequency of protocol-specific system failures, but the cloud platforms themselves could fail. A common form of business disruption is the Denial of Service (DoS) attack, which is when an attacker sends an abnormal amount of traffic that exceeds the victim's capacity. Eventually, the victim is overwhelmed, causing services to respond at an unusable speed or even stop functioning. In the context of DeFi, the DoS attack can impact the front-end of a protocol (e.g., My DeFi Pet (bitcoiner.tv, 2021)), or cause congestions on-chain, which are discussed in subsection 5.5.

We also categorized central oracle failures as a source of risk in this category. For centralized data providers, data accuracy is subject to centralized controls and management (see, for example, Compound_(Decrypt, 2020) and Synthetix_(Synthetix, 2019)).

Execution, Delivery and Process Management (ET7)

Business execution is a recognized risk category causing financial loss due to inferior execution of internal processes. This may include ill-designed procedures, human errors, or any form of improper management of assets. Within the DeFi ecosystem, this risk source can manifest in many ways, and we will discuss three types below. First, private keys could be poorly managed resulting in a loss or leak of the keys, where attackers somehow obtain access to the private keys without necessarily intruding a system (e.g., PAID Network_(Halborn, 2021)). Difficulty of private key management is exacerbated by the lack of security precautions, such as multisig wallets¹⁴. Second, the setup and execution of contract-relevant processes may lack sufficient control or be improper, such as in the case of OlympusDAO_(Theblock, 2021). Third, limitations in governance procedures could cause delays in solving technical problems, as observed in the unfolding of the COMP token accrual bug (Cryptonews, 2021).

¹⁴ Multisig wallets require more than one private key.

5.5 BLOCKCHAIN INFRASTRUCTURE RISK

Blockchain infrastructure risks could result in issues related to data availability, execution and the settlement of transactions on blockchains due to limitations in the design of blockchains. These include:

- Maximal Extractable Value
- Congestion of transactions
- Malfunction of the base networks
- Complexities of blockchain scalability
- Cryptographic vulnerabilities

Maximal (or Miner) Extractable Value

First introduced by (Daian, et al., 2020), MEV refers to the economic value that can be extracted by miners or validators¹⁵ at the expense of other users through prioritizing, injecting or censoring transactions. From a broader perspective, such value can be shared between miners/validators and other traders who target such MEV opportunities. MEV materializes on DeFi applications through the application of various strategies, such as displacement attacks, sandwich attacks and suppression attacks (Eskandari, Moosavi, & Clark, 2019). These MEV-extracting activities cause unfavorable conditions for other users, such as relatively unfavorable pricing or delays in execution (e.g., Alpha Finance (Punyanermitdee, 2021)). With the growth of cross-chain transactions, MEV opportunities can also arise across multiple blockchain networks. For instance, the prices for the same token pair on liquidity pools at different blockchain networks can vary, rendering cross-chain arbitrage profitable. The above negative externalities can, thus, apply in cross-chain settings (Obadia, Salles, Sankar, & Chitra, 2021).

Congestion of Transactions

The negative externalities brought on by network congestion to DeFi can vary by scale and impact. Network congestion can trigger relatively mild consequences, such as higher transaction fees and delay in transactions afforded by users. For example, in the Chainlink incident (Dalton, 2020), some malicious actors spammed the nodes with excessive requests to raise the transaction fees. This could further result in protocol-level failure under some abnormal congestion levels or tumultuous market conditions (e.g., MakerDAO (Blocknative, 2020)).

Malfunctions of Base Network

There is vast literature studying the validity and consistency of different distributed consensus protocols, which constitute the foundations of modern blockchain networks (Shi, 2020). Different consensus protocols are theoretically robust given certain assumptions, such as asynchronous networks and the bounds on the number of malicious validators. However, there is no guarantee that the necessary assumptions will occur in practice. Also, since most public blockchains are still in the experimental stages for stability and scalability, they remain susceptible to pitfalls, such as network instability¹⁶, failure in upgrades¹⁷, or consensus-layer security risks. These network-level malfunctions jeopardize on-chain financial activities.

¹⁵ Miners are contributors on the blockchain that provide proof-of-work validations for new blocks, while validators are usually referred to as contributors that provide proof-of-stake validations.

¹⁶ e.g., [Solana \(01/22/2022\)](#) (Ossinger, 2022)

¹⁷ e.g., [Evmos \(03/07/2022\)](#) (Khosla, Küllmer, Abbey, Barcevic, & Gautam, 2022)

Complexities of Blockchain Scalability

Scaling a blockchain refers to the improvement of a blockchain's capability of executing and storing transactions. To improve scalability, different blockchains have taken on different approaches. Most notably, Ethereum has decided on a roll-up¹⁸ centric roadmap that promotes the separation of data availability and execution (Buterin, A rollup-centric ethereum roadmap, 2020). Discussions of scaling risks and approaches to solving them are outside of the scope of this report. However, the challenges are similar to many new technologies, such as having the potential for malfunctions in the code and onboarding new users, but also may require high computational power and result in further centralization. These risks apply to all DeFi protocols that adopt the technologies.

Cryptographic Vulnerabilities

The emergence of quantum computing may threaten the encryption technology adopted by blockchains, thus undermining the security of the blockchain ecosystems, including the applications built on top of them. For example, the Shor's algorithm can be applied to crack the Elliptic Curve Cryptography (EEC) that is commonly adopted for the creation of pairs of public key and private key (Guo & Yu, 2022). These security issues are worth in-depth discussions, but they are beyond the scope of this report.

¹⁸ Rollups perform transaction execution outside layer 1 and then the data is posted to layer 1 where consensus is reached (Ethereum Foundation, 2022).

Section 6: Conclusions

Decentralized finance (DeFi) is an emerging financial system built on blockchains with unique risks and opportunities. We have proposed a risk classification framework to help the (re)insurance and risk management communities to develop an understanding of the risks associated with DeFi protocols. In addition, we hope that this study will encourage more actuaries and researchers to participate in the DeFi ecosystem and enhance the risk management practice in this space.



Give us your feedback!

Take a short survey on this report.

[Click Here](#)

 **SOA**
Research
INSTITUTE

Section 7: Acknowledgments

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

Project Oversight Group members:

Stephen Chan, PhD

Jeffrey Chu, PhD

Runhuan Feng, FSA, CERA

Petar Jevtic, PhD

Douglas W. Oliver, ASA, MAAA, ACAS

Franck Pralas, AQ

Jared Pranievicz, FSA, MBA, PhD

Geu Roo Yang, ASA

Yifan Zhang, FSA, MAAA

At the Society of Actuaries Research Institute:

Korrel Crawford, Senior Research Administrator

Alice Locatelli, Senior Director of Digital Strategy

David Schraub, FSA, MAAA, Senior Practice Research Actuary

Section 8: References

- bitcoiner.tv. (2021, September 15). Retrieved from https://bitcoiner.tv/video-my-defi-pet-ddos-attack-bisw_7e520fd89.html
- Blocknative. (2020). Evidence of mempool manipulation on Black Thursday: Hammerbots, mempool compression, and spontaneous stuck transactions. Retrieved from <https://www.blocknative.com/blog/mempool-forensics>
- Buterin, V. (2013). *Ethereum Whitepaper*. Retrieved from Ethereum: <https://ethereum.org/en/whitepaper/>
- Buterin, V. (2020). A rollup-centric ethereum roadmap. Retrieved from <https://ethereum-magicians.org/t/a-rollup-centric-ethereum-roadmap/4698>
- Buterin, V. (2021). An incomplete guide to rollups. Retrieved from <https://vitalik.ca/general/2021/01/05/rollup.html>
- Buterin, V. (2021). Endgame. Retrieved from <https://vitalik.ca/general/2021/12/06/endgame.html>
- Chainswap. (2021, July 11). Retrieved from <https://chain-swap.medium.com/chainswap-exploit-11-july-2021-post-mortem-6e4e346e5a32>
- Cohen, M. J. (2021). Initial report on xBNTa, xSNXa exploit. Retrieved from <https://medium.com/xtoken/initial-report-on-xbnta-xsnxa-exploit-d6e784387f8e>
- Coinfirm. (2021, September 3). Retrieved from <https://www.coinfirm.com/blog/dao-maker-hack/>
- CRO Forum. (2016). *CRO Forum Concept Paper on a proposed categorization methodology for cyber risk*.
- Cryptoslate. (2021, October 29). Retrieved from <https://cryptoslate.com/police-forces-jump-into-anubisdao-saga-after-60-million-rug/>
- Curti, F., Gerlach, J., Kazinnik, S., Lee, M., & Mihov, A. (2019). *Cyber risk definition and classification for financial risk management*. Federal Reserve Bank of St Louis.
- Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., . . . Juels, A. (2020). Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. Retrieved from <https://arxiv.org/abs/1904.05234>
- Dalton, M. (2020). Chainlink endures spam attack: Congestion, high fees. Retrieved from <https://cryptobriefing.com/chainlink-endures-spam-attack-congestion-high-fees/>
- DAOVentures. (2021, July 11). Retrieved from <https://daoventuresco.medium.com/the-day-after-chainswap-exploit-our-action-plan-4a53a75a0c26>
- de Sousa Matsumura, G., dos Santos, L., Conceição, A., & Vijaykumar, N. (2021). Vulnerabilities and Open Issues of Smart Contracts: A Systematic Mapping. *The International Conference on Computational Science and Its Applications*.
- Decrypt. (2020, November 26). Retrieved from <https://decrypt.co/49657/oracle-exploit-sees-100-million-liquidated-on-compound>

- DeFi Llama. (2022). *Total Value Locked All Chains*. Retrieved from DeFi Llama: <https://defillama.com/chains>
- Eskandari, S., Moosavi, S., & Clark, J. (2019). Sok: Transparent dishonesty: front-running attacks on blockchain. *The International Conference on Financial Cryptography and Data Security*.
- Ethereum Foundation. (2022, July). *Scaling*. Retrieved from Ethereum.org: <https://ethereum.org/en/developers/docs/scaling/#:~:text=on%20layer%202.-,Rollups,secured%20by%20native%20Ethereum%20security.>
- Ethereum Foundation. (2022). *Scaling*. Retrieved from Ethereum.org: <https://ethereum.org/en/developers/docs/scaling/#:~:text=on%20layer%202.-,Rollups,secured%20by%20native%20Ethereum%20security.>
- Fei Protocol. (2021, May 02). Retrieved from openzeppelin: <https://blog.openzeppelin.com/fei-post-mortem/>
- Fernau, O. (2022). Arbitrum goes down citing sequencer problems. Retrieved from <https://thedefiant.io/arbitrum-outage-2/>
- ForceDAO. (2021, April 04). Retrieved from <https://www.financemagnates.com/cryptocurrency/news/forcedao-exploited-for-367k-after-launch-due-to-engineering-oversight/>
- Forkast. (2021, October 29). Retrieved from forkast: <https://forkast.news/bxh-exploit-estimated-139m-admin-key-leakage/>
- Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain: Research and Applications*, 3(2). doi:<https://doi.org/10.1016/j.bcr.2022.100067>
- Halborn. (2020, November 22). Retrieved from <https://halborn.com/explained-the-defi-protocol-pickle-finance-hack-nov-2020-2/>
- Halborn. (2021, March 05). Retrieved from <https://halborn.com/explained-the-paid-network-hack-march-2021/>
- Halborn. (2021, December 02). Retrieved from <https://halborn.com/explained-the-badgerdao-hack-december-2021/>
- Halborn. (2021, March 09). Retrieved from <https://halborn.com/explained-the-dodo-dex-hack-march-2021/>
- Halborn. (2021, February 13). Retrieved from <https://halborn.com/explained-the-alpha-homora-defi-hack-feb-2021/>
- Halborn. (2021, July 14). Retrieved from <https://halborn.com/explained-the-bondly-finance-hack-july-2021/>
- Harvest Finance. (2020). Harvest flashloan economic attack post-mortem. Retrieved from <https://medium.com/harvest-finance/harvest-flashloan-economic-attack-post-mortem-3cf900d65217>
- Harvey, C. R., Ramachandran, A., & Santoro, J. (2021). *DeFi and the Future of Finance*. John Wiley & Sons.
- Hegic. (2020, April 25). Retrieved from <https://twitter.com/HegicOptions/status/1254276134344314883>
- ImToken. (2020, April 19). Retrieved from <https://medium.com/imtoken/about-recent-uniswap-and-lendf-me-reentrancy-attacks-7cebe834cb3>
- International Organization for Standardization. (2018). *ISO 31000:2018. Risk Management – Guidelines*. Retrieved from <https://www.iso.org/standard/65694.html>

- Iron Finance. (2021). Iron Finance Post-Mortem 17 June 2021. Retrieved from <https://ironfinance.medium.com/iron-finance-post-mortem-17-june-2021-6a4e9ccf23f5>
- Jensen, J. R., Von Wachter, V., & Ross, O. (2021). An Introduction to Decentralized Finance (DeFi). *Complex Systems Informatics and Modeling Quarterly*(26), 46-54. doi:10.7250/csimq.2021-26.03.
- Kelliher, P. (2013). A common risk classification system for the Actuarial Profession. *British Actuarial Journal* .
- Khosla, A., Küllmer, F. K., Abbey, J., Barcevic, M., & Gautam, P. (2022). Evmos V2 upgrade incident. Retrieved from <https://github.com/evmos/mainnet/blob/main/incidents/postmortem-1.md>
- Kistner, K. J. (2020). Post-Mortem. Retrieved from <https://bx.network/blog/postmortem-ethdenver>
- Kudelskisecurity. (2021, August 10). Retrieved from kudelskisecurity: <https://research.kudelskisecurity.com/2021/08/12/the-poly-network-hack-explained/>
- Kuznetsov, I. (2021). Analysis of the TITAN fall. Retrieved from <https://jeiwan.net/posts/analysis-titan-fall/>
- McDonald, M. (2020). Incident with non-standard ERC20 deflationary tokens. Retrieved from <https://medium.com/balancer-protocol/incident-with-non-standard-erc20-deflationary-tokens-95a0f6d46dea>
- Meegan, X. (2020). Identifying key non-financial risks in decentralized finance on Ethereum blockchain. *10.13140/RG.2.2.27175.57769*.
- MonoX Team. (2021). Exploit: Post mortem. Retrieved from <https://medium.com/monoswap/exploit-post-mortem-33921a779b43>
- My DeFi Pet. (2021, September 15). Retrieved from bitcoiner.tv: https://bitcoiner.tv/video-my-defi-pet-ddos-attack-bisw_7e520fd89.html
- Obadia, A., Salles, A., Sankar, L., & Chitra, T. (2021). Unity is strength: A formalization of cross-domain maximal extractable value. Retrieved from https://www.researchgate.net/publication/356746648_Unity_is_Strength_A_Formalization_of_Cross-Domain_Maximal_Extractable_Value
- Openzeppelin. (2017, July 20). Retrieved from <https://blog.openzeppelin.com/on-the-parity-wallet-multisig-hack-405a8c12e8f7/>
- OpenZeppelin. (2021). FEI post mortem. Retrieved from <https://blog.openzeppelin.com/fei-post-mortem/>
- OpRisk Advisory and Towers Perrin. (2010). *A New Approach for Managing Operational Risk: Addressing the Issues Underlying the 2008 Global Financial Crisis*. Sponsored by Joint Risk Management, Section Society of Actuaries, Canadian Institute of Actuaries & Casualty Actuarial Society.
- OriginProtocol. (2020, November 17). Retrieved from <https://blog.originprotocol.com/what-weve-changed-since-the-ousd-attack-5894f2bd77cf>
- Ossinger, J. (2022). Solana suffers network instability in brutal week for crypto. Retrieved from <https://www.bloomberg.com/news/articles/2022-01-23/solana-suffers-network-instability-during-brutal-week-for-crypto>

- Pancakeswap. (2021, March 15). Retrieved from <https://medium.com/pancakeswap/dns-incident-recap-36a183a2aee6>
- Peckshield. (2020, April 18). Retrieved from <https://peckshield.medium.com/uniswap-lendf-me-hacks-root-cause-and-loss-analysis-50f3263dcc09>
- Peckshield. (2021, June 22). Retrieved from <https://peckshield.medium.com/eleven-finance-incident-root-cause-analysis-123b5675fa76>
- PercentFinance. (2020, April 11). Retrieved from <https://percent-finance.medium.com/percent-finance-incident-post-mortem-d4e419cf35ab>
- Phoenix Finance. (2021, May 17). Retrieved from <https://medium.com/phoenix-finance/finnexus-statement-regarding-the-may-2021-hack-d69e1b7617dc>
- PhoenixFinance. (2021, May 17). Retrieved from <https://medium.com/phoenix-finance/finnexus-statement-regarding-the-may-2021-hack-d69e1b7617dc>
- Pitimanaaree, N. (2021, May 08). Retrieved from <https://nipunp.medium.com/5-8-21-rari-capital-exploit-timeline-analysis-8beda31cbc1a>
- Prewett, K. W., Prescott, G. L., & Phillips, K. (2020). Blockchain adoption is inevitable—Barriers and risks remain. *Journal of Corporate accounting & finance*, 31(2), 21-28.
- Punyaneramtdee, T. (2021). MEV bots & Uniswap implicit assumptions. Retrieved from <https://blog.alphaventuredao.io/mev-bots-uniswap-implicit-assumptions/>
- Sandor, K., & Genç, E. (2022). The fall of Terra: A Timeline of the meteoric rise and crash of UST and LUNA. Retrieved from <https://www.coindesk.com/learn/the-fall-of-terra-a-timeline-of-the-meteoric-rise-and-crash-of-ust-and-luna/>
- Schär, F. (2021). *Decentralized finance: On blockchain-and smart contract-based financial markets*. Federal Reserve Bank of St. Louis.
- SECBIT. (2020, April 25). Retrieved from <https://medium.com/secbit-media/a-disastrous-vulnerability-found-in-smart-contracts-of-beautychain-bec-dbf24ddbc30e>
- Shi, E. (2020). *Foundations of distributed consensus and blockchains*. Retrieved from <https://www.distributedconsensus.net/>
- SlowMist. (2021, May 05). Retrieved from SlowMist: <https://slowmist.medium.com/slowmist-value-defi-vswap-module-hack-analysis-64e8909ef6a2>
- Synthetix. (2019, June 25). Retrieved from <https://blog.synthetix.io/response-to-oracle-incident/>
- TBTC. (2020, June 18). Retrieved from <https://twitter.com/HegicOptions/status/1254276134344314883>
- The Defiant. (2020). Eminence Finance Exploit Leads to 'Degen' Soul Searching. Retrieved from <https://decrypt.co/43292/eminence-finance-exploit-leads-to-degen-soul-searching>
- Theblock. (2021, November 23). Retrieved from theblock: <https://www.theblock.co/post/125170/olympusdao-mistake-lets-user-spend-50000-to-buy-1-43-million-in-ohm>

- Thurman, A. (2020). Dynamic Set Dollar faces ‘massive test’ as stablecoin falls as low as \$0.27. Retrieved from <https://cointelegraph.com/news/dynamic-set-dollar-faces-massive-test-as-stablecoin-falls-as-low-as-27>
- True Seigniorage Dollar. (2021). A malicious attacker has just utilized \$TSD DAO to mint 11.8 billion tokens to his own account and sold all. Retrieved from <https://twitter.com/TrueSeigniorage/status/1370956726489415683>
- Umbrella Network. (2021, July 11). Retrieved from <https://medium.com/umbrella-network/an-important-message-to-the-community-about-the-chainswap-hack-e2603de5f0e6>
- Ushida, R., & Angel, J. (2021). Regulatory Considerations on Centralized Aspects of DeFi Managed by DAOs. In *Lecture Notes in Computer Science vol 12676*. Springer, Berlin, Heidelberg.
- ValueDefi. (2021, May 05). Retrieved from <https://medium.com/valuedefi/vstake-pool-incident-post-mortem-4550407c9714>
- VetherAsset. (2020, June 19). Retrieved from <https://medium.com/vether-asset/vether-contract-upgrade-c2cf62b9aee2>
- Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2021). SoK: Decentralized Finance (DeFi). *Cryptography and Security (cs.CR); General Economics (econ.GN)*, arXiv:2101.08778 [cs.CR].
- xToken. (2021, May 13). Retrieved from <https://medium.com/xtoken/initial-report-on-xbnta-xsnxa-exploit-d6e784387f8e>
- Yearn Finance. (2021, February 04). Retrieved from <https://github.com/yearn/yearn-security/blob/master/disclosures/2021-02-04.md>

Appendix A: Risk Categorization and Definitions Identified in the Review of Relevant Literature

Table 5
RISK CATEGORIZATION AND IDENTIFICATION

Risk Category	Definition
Smart contract vulnerability or execution	<p>“a logic error in the code or an economic exploit in which an attacker can withdraw funds from the platform beyond the intended functionality” (Harvey, Ramachandran, & Santoro, 2021)</p> <p>(Werner, et al., 2021) provides subcategories of reentrancy, integer manipulation, logical bugs, single transaction attacks (due to governance attacks or sandwich attacks), and transaction ordering attacks.</p> <p>(Meegan, 2020) sets out reentrancy, unhandled exceptions, integer manipulation, transaction ordering, timestamp dependence, and upgradeable smart contract vulnerabilities.</p>
Operational security or centrality risk	The risk of central point failures, e.g., risks resulting from DeFi protocols’ use of admin keys (or the potential misuse) (Meegan, 2020) (Schär, 2021)
Dependencies (also termed as ‘interoperability and systemic risk’, or ‘composability risks’)	The risks associated with interacting and tightly connected protocols across the DeFi system. (Werner, et al., 2021) (Meegan, 2020) (Schär, 2021) (Jensen, Von Wachter, & Ross, 2021)
Design risk	Potentially a subcategory of smart contract vulnerability or dependencies. The risk is that a flaw in the design of a DeFi protocol causes an irreparable vulnerability, potentially due to dependencies. (Meegan, 2020)
Oracle risk	Risks associated with the reliance of protocols on accurate data (e.g., secure and tamper-resistant) (Werner, et al., 2021) (Meegan, 2020) (Schär, 2021) (Harvey, Ramachandran, & Santoro, 2021)
Anonymity and privacy (including illicit activities)	The risks due to anonymity, semi-anonymity and re-identification of agents (Werner, et al., 2021) (Schär, 2021) (Prewett, Prescott, & Phillips, 2020)
Scalability risk	The risk associated with network congestion due to the need for decentralized validation of all on-chain transactions (Meegan, 2020) (Harvey, Ramachandran, & Santoro, 2021) (Schär, 2021)
Economic (incentive or security) risks	The exploitation of the incentive structure to non-atomically realize a profit at the expense of others. (Meegan, 2020)

Risk Category	Definition
	(Werner, et al., 2021) provides subcategories of over-collateralization as security, threats from miner extractable value, governance extractable value, and market/oracle manipulation.
Governance risk	The risks associated with DeFi protocols including those governed by autonomous and smart contracts and those governed by DAOs (and therefore the distribution of governance tokens) (Harvey, Ramachandran, & Santoro, 2021) (Jensen, Von Wachter, & Ross, 2021) (Werner, et al., 2021) (Ushida & Angel, 2021)
DEX risk	The risks associated with decentralized exchanges, including AMMs, CFMM, and order-book exchanges (Harvey, Ramachandran, & Santoro, 2021)
Custodial risk	The risks associated with custody over a wallet (Harvey, Ramachandran, & Santoro, 2021) (Prewett, Prescott, & Phillips, 2020)
Environmental	The risks associated with the impact of work consensus activities on energy consumption (Harvey, Ramachandran, & Santoro, 2021)
Regulatory and compliance risks	The risks associated with (increasing) regulatory scrutiny, including the uncertain legal status of DAOs (Prewett, Prescott, & Phillips, 2020) (Harvey, Ramachandran, & Santoro, 2021) (Ushida & Angel, 2021) (Meegan, 2020)
Capability (including financial literacy) risk	The risks associated with the development team having insufficient expertise in finance or other key areas of training (Prewett, Prescott, & Phillips, 2020)
Finality risk	The risks of forks in blockchains creating multiple chains (Meegan, 2020)
Disclosure risk	The risk that a platform fails to disclose risks, e.g., the full output of auditing reports (Meegan, 2020)
Vendor risk	Risks associated with reliance on an external vendor (Prewett, Prescott, & Phillips, 2020)
Contractual risk	Risks associated with contracts defining and managing the relationship between blockchain administrators and participating nodes (Prewett, Prescott, & Phillips, 2020)

Risk Category	Definition
Emerging risks	The DeFi ecosystem is growing, and inherently risky, so emerging risks will be identified and can quickly become material. (Meegan, 2020)

Appendix B: Glossary – Commonly used DeFi Terms

Airdrop	Free tokens distributed by protocols for marketing purposes, with or without criteria to claim.
Automated Market Maker	A tool enabling automated trading without matching buyers and sellers by aggregating liquidity into a pool that traders trade against.
Bonds	Short-term vested protocol tokens sold at discount in exchange for LP tokens. Introduced by Olympus DAO.
Burning	The process of removing a token out of circulating supplies. Usually achieved by sending the token to a special address with an unobtainable private key, removing access to the token.
Composability	The ability for DeFi applications to communicate with and build upon each other.
Consensus	Agreement on a state of the blockchain in a network with multiple participants, or the mechanism to reach it.
Custodial stablecoins	Stablecoins whose value pegging mechanism is based on reserve assets held off-chain by the issuer of the stablecoin tokens.
Decentralized Autonomous Organization (DAO)	Organizations where governance token holders discuss proposals and vote to reach collective decisions.
Decentralized Exchange (DEX)	DeFi applications that allow cryptocurrency trading without an intermediary.
Decentralized Finance (DeFi)	An emerging financial system built on public and permissionless blockchains using smart contracts.
Delegators	Blockchain participants who delegate their cryptocurrencies as the equity rights to validators to ensure the integrity of transactions, thus earning a share of the fees without the need to invest in computational resources.
ERC-20	A smart contract technical standard on the Ethereum network for creating assets. Later adopted by other blockchains such as Binance Smart Chain and Avalanche.
Ethereum	A decentralized blockchain that first introduced smart contract functionality, with its native cryptocurrency Ether currently having the second largest market capitalization among all cryptocurrencies as of December 2021.
Flash loan	Smart contract enabled loan that is borrowed and repaid within the same transaction on a blockchain without collateral.
GameFi	An industry focusing on the gamification of monetary policies in play-to-earn games built on top of blockchains.
Gas	Computation and transaction fees paid by the transactor to be burned or to compensate miners and validators who help secure the network.
Governance tokens	Tokens that carry governance rights for a specific protocol. Usually these

	rights are realized by on-chain votes related to protocol decisions.
Initial Coin Offering (ICO)	The act of seeking money by creating a new token to raise funds.
Initial DEX offering (IDO)	The act of launching a new token on decentralized exchanges for trading.
Interest-bearing tokens	Tokens where the holders are entitled to interest, usually LP tokens.
Interoperability	The ability to move assets between different blockchains.
Liquidity mining / Yield farming	Providing liquidity for DeFi protocols for reward tokens, from a sharing of transaction fees or protocol equity tokens.
Liquidity Provider Tokens (LP Tokens)	Tokens that act as receipts for depositing cryptocurrencies into a smart contract that can be redeemed or used elsewhere.
Non-custodial stablecoin	Stablecoin whose value pegging mechanism is provided by a smart contract.
Non-fungible tokens (NFTs)	Tokens representing ownership of distinct digital valuables.
On-chain / Off-chain	Whether information or transactions are situated inside (on-chain) or outside (off-chain) the blockchain records.
Oracles	Services relaying off-chain information to on-chain applications, or services collecting information from applications to be used elsewhere.
Permissionless blockchains	Blockchains that are “shared by all network users, updated by miners (and validators), monitored by everyone, and owned and controlled by no one.” (Swan, M. 2015. <i>Blockchain: Blueprint for a New Economy.</i>)
Private keys	Secret information used to verify the ownership of cryptographic assets.
Protocols	An application or a group of applications built on blockchains.
Scalability trilemma	The theory that it is difficult for a blockchain to achieve scalability, security and decentralization, also known as the blockchain trilemma.
Slippage	The value lost in trading with automated market makers due to price movements from the trade itself.
Smart contracts	Systems which automatically move digital assets according to arbitrary pre-specified rules. (Buterin, Ethereum Whitepaper, 2013)
Stablecoins	Tokens whose value is pegged to fiat currencies.
Tokens	Value-storing digital records of equities, utilities, or other functions enabled by smart contracts. Loosely interchangeable with “coins” in blockchain contexts and “cryptocurrencies.”
Tokenomics	The study of the economics of crypto tokens.
Total value locked (TVL)	A measure of protocol size by the amount of capital deposited into the protocol’s smart contracts.

Validators	Blockchain participants who are responsible for verifying the integrity of transactions.
Web3	A new generation of the Internet that decentralized the online ecosystem based on blockchain with token-based economics.
Yield Aggregators	Decentralized apps that pool tokens from different users to perform yield farming transactions in a batch to save time and gas fee costs.



Give us your feedback!

Take a short survey on this report.

[Click Here](#)

 **SOA**
Research
INSTITUTE

About The Society of Actuaries Research Institute

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

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

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

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

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