exponential

AUGUST 2023

Assessing Risk in DeFi

THE EXPONENTIAL WHITEPAPER

Table of Contents

Introduction

Decentralized finance (DeFi) is a revolutionary movement that aims to democratize and disintermediate traditional financial services. By leveraging blockchain technology and smart contracts, DeFi enables novel ways for users to access and provide liquidity, such as staking, market making, lending, farming protocol incentives, and fee sharing from protocol earnings. These new opportunities to earn yield are native to the blockchain and thus come with their own unique risk vectors.

Managing risk is the next frontier for DeFi. To invest smarter in DeFi, one needs to understand all the risks of a particular DeFi investment. However, DeFi also faces several challenges and threats, such as highly inflationary projects, smart contract exploits, questionable decentralization, and outright fraud. These factors have raised doubts about the sustainability and security of DeFi. In this paper, we propose and establish a common framework for risk assessment in DeFi.

At Exponential, we take risk seriously. We believe that risk is not something to be avoided, but rather something to be understood and managed. Risk is hard because the devil is in the details, and any small thing can kill your investment. That's why we don't rely on intuition or gut feeling, but on rigorous analysis and research.

This is how we do it: we use a framework that asks all the relevant questions that need to be answered before investing in any DeFi project. These questions cover aspects such as governance, tokenomics, security, liquidity, smart contract design, and more. We do the research in detail, using both qualitative and quantitative methods, and we objectively quantify the chances of loss based on historical data and simulations. We also monitor the performance of our risk framework on an ongoing basis, and adjust or update our risk criteria accordingly.

We hope this will help our community look into the hard subject of risk with more confidence and clarity. We believe that by applying this framework, we can reduce the uncertainty and complexity of DeFi investing, and unlock its full potential for exponential growth.

The Exponential Approach to Risk

Before we dive into the details of our framework, we want to share our overall approach to risk in DeFi. We believe that risk is not a static or linear concept, but a dynamic and multidimensional one. Risk can come from many sources and affect many aspects of a DeFi project, and it can change over time and in response to external events. To go beyond what's obvious and try to imagine the worst (principle of max pain), we use a catch-all holistic framework that covers all the possible angles and scenarios. This way, we can anticipate and prepare for any potential risk event that may occur in DeFi.

We believe that risk is not a subjective or relative concept, but an objective and absolute one in terms of its potential impact on users. Risk is not only a matter of opinion but also a matter of fact. Risk exists objectively and can be measured and quantified, but it also depends on how users perceive and evaluate it. Risk is not something that can be ignored or dismissed, but something that must be acknowledged and addressed. As such, we need to apply a high standard of quality when evaluating risks in DeFi. We view DeFi as the infrastructure for the future of money, and we want to ensure that they are safe and reliable for everyone.

Finally, we recognize that risk is not a simple or isolated concept, but a complex and interconnected one. Risk can arise from many factors and affect many outcomes, and it can interact and amplify with other risks in unexpected ways. Therefore, we need to recognize the complexity, composability and interconnectivity of DeFi, and account for the systemic and emergent risks that may arise from the interdependencies between different DeFi protocols. We use a graphical representation of DeFi to illustrate how any risk event can propagate and affect the whole ecosystem. This way, we can avoid being blindsided by unexpected or cascading risk events that may affect the whole DeFi ecosystem.

In summary, this is the Exponential approach to risk in DeFi. We believe that by following this approach, we can better understand and manage the risks that users face in this rapidly evolving space.

The Exponential Risk Framework

Our risk framework captures the composability of DeFi. This means that we do not simply average the risks of each component in a DeFi liquidity pool, but rather compound or multiply them across the chain, protocols, assets, AND pool level. This gives a more accurate and comprehensive risk score for each pool. To achieve this composability, we estimate a probability of failure for every risk type based on its frequency and severity. These risk probabilities are proprietary to Exponential and will be reevaluated periodically. For the purposes of this paper, we have assigned a relative risk score from 1 to n for each risk type, where 1 indicates the lowest risk and n indicates the highest risk. Since the exact numerical value of the risk score is not disclosed in this paper, the 1-n scale is only for relative comparison within each risk type and not meant to be compared across different risk types. These risk types are then grouped into four main categories that form the basis of our framework.

Our framework consists of four main components: risk categories, risk types, risk scores, and risk ratings.

- The first component is the risk categories, which are the broad areas of risk that we consider in DeFi. We have identified four risk categories: chain risk, protocol risk, asset risk, and pool risk. Each category represents a different dimension of risk that can affect a DeFi investment.

- The second component is the risk types, which are the specific aspects of risk that we measure and analyze within each category. We have defined a set of risk types for each category based on our research. Each risk type captures a particular feature or characteristic of a DeFi protocol or liquidity pool that can influence its risk level. Within each risk type are risk items that relate to scoring that particular risk type (e.g. TVL and maturity are used to score Chain Maturity).

- The third component is the risk scores, which are the numerical values that we assign to each risk type based on our estimation of its probability of failure. We use both qualitative and quantitative methods to estimate the probability of failure for each risk type based on historical data and simulations. We also update our estimates periodically to reflect the latest developments and changes in DeFi.

- The fourth component is the risk ratings, which are the qualitative labels that we assign to each DeFi protocol or investment based on its overall risk score. We use a scale from A to F to rate the overall risk level of a DeFi investment based on its total risk score across all categories and factors. We also provide a breakdown of the ratings by category and factor to show the strengths and weaknesses of each DeFi pool.

Risk Categories	Risk Types	Risk Items
Blockchain	Chain Maturity	TVL, maturity
	Chain Design	# of validators, concentration of top validators, validator economics, warm-up/cool-down period
	Rollup Design	Rollup type, upgradeability, validator failure, sequencer failure
	Chain Reliability	Blockchain halts
Protocol	Protocol Code Quality	# of audits, team anonymity, # of experienced auditors, # of hacks
	Protocol Maturity	Maturity of last version, maturity of first version, TVL, governance issues, governance concentration, access controls
	Protocol Design	Oracle type, reflexivity, job types
Asset	Asset Strength	Intrinsic value or collateralization, market capitalization, centralization, stablecoin volatility
	Tokenomics	Inflation, reflexivity
Pool	Pool Design	Fee sharing, staking, yield, lending, collateral type, market making, options, insurance

Blockchain Risks

This risk category evaluates how well the blockchain is designed and implemented to provide security and functionality to its users. A secure and functional blockchain should prevent or mitigate threats such as attacks, bugs, forks, or disruptions. An insecure or dysfunctional blockchain could expose its users to risks such as losing funds, experiencing delays, facing interruptions, or losing trust. This section assigns an overall risk score to each blockchain based on its design and maturity

Chain Maturity

This risk type evaluates how battle-tested, and Lindy-proof a blockchain is. It considers the total value locked in a blockchain and how long it has been live on mainnet. A battle-tested blockchain should have survived various challenges and threats that tested its performance and security. A Lindy-proof blockchain should have a long and consistent track record of reliability and resilience. An immature blockchain could have unresolved issues or vulnerabilities that could compromise its performance and security in the future.

I. What is the total value locked for the blockchain?
This risk score shows how mature and established a blockchain is based on its total value locked (TVL). TVL is the amount of money (measured in USD value) that is locked in smart contracts or protocols on a blockchain network. It shows the demand and usage of the network, as well as the trust and confidence of the users in the network's security and functionality. A higher TVL often means a lower risk because it implies the network has a lot of users, a strong and diverse ecosystem, and a good history of delivering value and innovation. A lower TVL often equates to a higher risk because it suggests the network has fewer users, a more fragile ecosystem, and a lack of experience and reputation in the market.

Risk Score	TVL Ranking	Description
4 (most risky)	Non-top 10	The network has a low TVL and is new, unproven, or unpopular among users
3	Top 10	The network has a moderate TVL and is somewhat mature and established among users
2	Top 5	The network has a high TVL and is very mature and established among users
1 (least risky)	Top 1	The network has the highest TVL and is the most mature and established among users

II. How mature is the blockchain?

This risk score evaluates how long the blockchain has been live on mainnet without any major issues or incidents. The longer a blockchain network has been live, the more likely it has been exposed to different scenarios and stress tests and that any bugs or vulnerabilities have been fixed or mitigated. Therefore, a higher maturity score indicates a lower risk of encountering unexpected problems or failures with the network.

Risk Score	Maturity	Description
5 (most risky)	0-6 months	The blockchain has been live for less than half a year, meaning that it has a low level of reliability and resilience. This exposes the blockchain to a high risk of instability or failure due to untested scenarios or undiscovered bugs.
4	6-12 months	The blockchain has been live for 6 to 12 months, meaning that it has a moderate level of reliability and resilience. This exposes the blockchain to a moderate risk of instability or failure due to untested scenarios or undiscovered bugs.
3	12-18 months	The blockchain has been live for 12 to 18 months, meaning that it has a high level of reliability and resilience. This reduces the risk of instability or failure due to untested scenarios or undiscovered bugs.
2	18-24 months	The blockchain has been live for 18 to 24 months, meaning that it has a very high level of reliability and resilience. This minimizes the risk of instability or failure due to untested scenarios or undiscovered bugs.
1 (least risky)	24+ months	The blockchain has been live for more than two years, meaning that it has an almost perfect level of reliability and resilience. This eliminates the risk of instability or failure due to untested scenarios or undiscovered bugs.

Chain Design

This risk type evaluates how well a blockchain is designed to ensure its reliability, stability, and resilience. It considers various factors such as the consensus mechanism, the validator economics, the network topology, and the upgrade process. A well-designed blockchain should provide a high level of security to its users by preventing or mitigating threats such as 51% attacks, double-spending, censorship, forks, bugs, hacks, or exploits. A poorly-designed blockchain could expose its users to various risks, such as losing funds, experiencing delays, facing disruptions, or losing trust.

I. How many validators secure the network?

This risk score is a measure of how vulnerable a blockchain network is to attacks by malicious validators. Validators are nodes that process transactions and create new blocks on the blockchain. They are usually rewarded with fees or tokens for their service, but they can also be penalized or slashed for misbehavior or downtime. The more validators there are, the more secure and decentralized the network is because it is harder for a single entity or a small group of validators to control the network or manipulate the transactions. A network with less than 100 validators is considered very risky as it is easy for a majority of validators to collude and compromise the network's integrity. For example, they could censor transactions, reverse transactions, double-spend tokens, or halt the network. A network with more than 10,000 validators is considered very secure as it is unlikely for a large fraction of validators to act maliciously or coordinate an attack. For example, they would need to overcome high coordination costs, reputation risks, economic incentives, and cryptographic proofs.

Risk Score	Number of Validators	Description
5 (most risky)	Less than 100	Very low security and decentralization
4	100 - 999	Low security and decentralization
3	1,000 - 4,999	Moderate security and decentralization
2	5,000 - 9,999	High security and decentralization
1 (least risky)	More than 10,000	Best in class security and decentralization

II. How concentrated are the top validators?

This risk score shows how much power the top validators have over the network based on their stake. Stake is the amount of tokens or assets that validators lock up to join the network. Top validators are the validators that have the most stake in the network and therefore have the most power to produce blocks. The percentage of blocks produced by a validator is a measure of how often they are selected to create new blocks and add them to the blockchain. The more stake they have, the more they can influence the network's decisions. If the top validators have too much stake, they can try to cheat or harm the network by changing the blockchain history or blocking transactions. This is called a 51% attack. A network with a lower risk score is more decentralized and secure from such attacks.

Risk Score	Validator Concentration (Top 5)	Description
3 (most risky)	More than half (51%) of the total stake	Top validators can do a 51% attack easily
2	More than a third (33%) of the total stake	Top validators can do a 51% attack with some difficulty
1 (least risky)	Less than a third (33%) of the total stake	Top validators cannot do a 51% attack alone

III. What percent of validator economics comes from fees?

This risk score shows how much the validators depend on inflation for their income. Inflation is when new tokens are created and given to the validators for securing the network. Transaction fees are what users pay to the validators for processing their transactions and adding them to new blocks. Inflation and transaction fees are the two main ways that validators make money. A high percentage of income from fees means that the validators are making more money from the network's activity and demand versus the issuance of new tokens. This is better for the network's security and economy in the long run because it reduces the risk of inflation lowering the tokens value over time. A low percentage of income from fees means that the validators are making more money from inflation, which could disincentivize validators from participating in the network as the price of the token drops due to inflation. Thus, sustainable economics is crucial for validator participation and decentralization.

Risk Score	TransactionFee as % of Validator Income	Description
5 (most risky)	<25%	The validators depend a lot on inflation and have low income from the network's activity and demand
4	>=25%	The validators still depend on inflation but have some income from the network's activity and demand
3	>=50%	The validators have a balanced income from inflation and the network's activity and demand
2	>=75%	The validators have a high income from the network's activity and demand and a low dependence on inflation
1 (least risky)	>=90%	The validators have a very high income from the network's activity and demand and a very low dependence on inflation

IV. Is there a warm-up or cool-down period to become a validator?

This risk score shows how well the network stops validators from cheating or running away. A warm-up period is the time a validator has to wait before they can start staking their assets and join the network. A cool-down period is the time a validator has to wait before they can stop staking their assets and leave the network. A warm-up period stops validators from joining the network only when it suits them and getting an unfair edge over other validators. A cool-down period stops validators from leaving the network suddenly and avoiding the consequences of their actions. A network with no warm-up and cool-down period is very risky because it lets validators come and go as they please, without any rules or delays. This could let them abuse the network's weaknesses or dodge the network's penalties. A network with both warm-up and cool-down periods is less risky because it makes it harder and costlier for validators to join and leave the network. This incentivizes them to not behave maliciously or carelessly.

Risk Score	Warm-up Period	Cool-down Period	Description
4 (most risky)	No	No	The validators can join and leave the network anytime, without any restrictions or delays
3	Yes	No	The validators have to wait before they can join the network, but not before they can leave it
2	No	Yes	The validators have to wait before they can leave the network, but not before they can join it
1 (least risky)	Yes	Yes	The validators have to wait before they can join and leave the network

Rollup Design

This risk type evaluates the incremental risks associated with scaling rollups built on top of a Layer 1 network like the Ethereum mainnet. Rollups are a type of Layer 2 solution that execute transactions outside of Layer 1 (i.e. Ethereum mainnet) but post transaction data on Layer 1. This allows rollups to increase transaction speed and throughput while maintaining most of the security and decentralization of the Layer 1. However, rollups also introduce some trade-offs and challenges, such as centralization, interoperability, data availability, and composability, which can compromise security to a certain extent.

I. How is the rollup's state validated?

This risk score is a measure of how much trust is needed for a rollup design. A rollup's design determines how the transactions are executed, verified, and stored on the Layer 2 network and how they are secured by the Layer 1. A higher trust requirement means that the users have to rely more on the honesty and availability of the Layer 2 operators or validators or on the validity of certain cryptographic assumptions. A lower trust requirement means that the users can verify and dispute the Layer 2 transactions by themselves or rely on the security guarantees of the Layer 1 network. A rollup design with a high trust requirement is considered very risky because it exposes the users to more potential threats, such as fraud, censorship, data loss, or invalid proofs. A rollup design with a low trust requirement is considered less risky because it protects the users from these threats by allowing them to challenge or exit the Layer 2 anytime.

Risk Score	TVL Ranking	Description
4 (most risky)	Non-top 10	The network has a low TVL and is new, unproven, or unpopular among users
3	Top 10	The network has a moderate TVL and is somewhat mature and established among users
2	Top 5	The network has a high TVL and is very mature and established among users
1 (least risky)	Top 1	The network has the highest TVL and is the most mature and established among users

II. Where is the rollup's data stored?

This risk score is a measure of how much trust is needed for a rollup design. A rollup's design determines how the transactions are executed, verified, and stored on the Layer 2 network and how they are secured by the Layer 1. A higher trust requirement means that the users have to rely more on the honesty and availability of the Layer 2 operators or validators or on the validity of certain cryptographic assumptions. A lower trust requirement means that the users can verify and dispute the Layer 2 transactions by themselves or rely on the security guarantees of the Layer 1 network. A rollup design with a high trust requirement is considered very risky because it exposes the users to more potential threats, such as fraud, censorship, data loss, or invalid proofs. A rollup design with a low trust requirement is considered less risky because it protects the users from these threats by allowing them to challenge or exit the Layer 2 anytime.

Risk Score	Data Availability	Description
4 (most risky)	Off-chain	Data is stored off-chain
3	Off-chain with data availability committee	Data is stored off-chain but secured by a data availability committee
2	On-chain	Data is stored on-chain
1 (least risky)	N/A	Chain is not a rollup

III. Is the rollup upgradeable?

This risk score measures how upgradeable a rollup is and what restrictions are in place to prevent malicious actors from pushing critical changes. Upgradeability refers to the ability of the rollup operators or developers to modify or improve the Layer 2 smart contracts. Upgradeability can be beneficial for fixing bugs, adding features, or enhancing performance, but it can also be harmful if the upgrades are done without proper notice, consent, or oversight from the community. To manage this risk, rollups have mechanisms that limit the rollup's upgradeability, such as timelocks and multisigs. A timelock is a delay period that prevents the rollup upgrades from taking effect immediately, giving users time to review and react to any changes. A multisig is a requirement that multiple parties must sign or approve the rollup upgrades before they can be executed, ensuring that no single party can control or manipulate the rollup. Another mechanism is on-chain governance, which is a process of making decisions about the rollup upgrades through voting by token holders on the Layer 2 network.

Risk Score	Upgradeable	On-chain governance	Multisig	Timelock	Description
6 (most risky)	Yes	No	Yes (≤3 signers)	No	The rollup can be upgraded without a waiting period, and only a few people need to agree
5	Yes	No	Yes (≥4 signers)	No	The rollup can be upgraded without a waiting period, but many people need to agree
4	Yes	No	Yes (≤3 signers)	Yes	The rollup can be upgraded, but there is a waiting time and a few people need to agree
3	Yes	No	Yes (≥4 signers)	Yes	The rollup can be upgraded, but there is a waiting time and many people need to agree
2	Yes	Yes	No	Yes	The rollup can be upgraded via on-chain governance
1 (least risky)	No	N/A	N/A	N/A	The rollup cannot be upgraded at all

IV. What happens in case of validator failure?

The risk score is a measure of what mechanisms the rollup has in place in case there is a validator failure. A validator failure is a situation where the validators or operators of the rollup stop producing or verifying blocks on the Layer 2 network, either due to technical issues, malicious attacks, or economic incentives. A validator failure can cause the Layer 2 to halt, preventing the users from accessing or transferring their funds on the rollup. Some rollups have mechanisms in place that allow users to exit the rollup and recover their funds on the Layer 1 in case of a validator failure. A rollup with no mechanism is considered very risky because it means that the users have no way of escaping or recovering from a validator failure. They would be stuck on the Layer 2 and lose their funds permanently. A rollup with a mechanism for users to propose blocks after inactivity is considered less risky because it means that users can exit the rollup and recover their assets on the Layer 1 after a certain period of time without any blocks being produced on the Layer 2. This mechanism is automatic and permissionless, meaning that it does not require any human intervention or approval from the validators or operators.

Risk Score	Mechanism	Description
3 (most risky)	None	Users have no way of exiting the L2 from a validator failure
2	Escape hatch	Users have a way of leaving the L2 from a validator failure, but it requires human intervention or permission from the validators
1 (least risky)	Propose blocks after inactivity	Users have a way of leaving the L2 from a validator failure, and it does not require human intervention or permission from the validators

V. What happens in case of sequencer failure?

This risk score is a measure of what mechanisms the rollup has in place in case there is a sequencer failure. A sequencer failure is a situation where the sequencer or operator of the rollup stops ordering or batching transactions on the Layer 2 network, either due to technical issues, malicious attacks, or economic incentives. A sequencer failure can cause the Layer 2 to halt, preventing users from accessing or transferring their assets on the rollup. Some rollups have a mechanism that allows users to exit the rollup and recover their funds or assets on the Layer 1 in case of a sequencer failure. A rollup with no mechanism is considered very risky because it means that the users have no way of escaping or recovering from a sequencer failure. They would be stuck on the Layer 2 and lose their assets permanently. A rollup with a mechanism to transact using the Layer 1 is considered less risky because it means that the users can exit the rollup and recover their funds by submitting their transactions directly to the Layer 1 instead of relying on the sequencer. This mechanism is automatic and permissionless, meaning that it does not require any human intervention or approval from the sequencer or operator.

Risk Score	Mechanism	Description
3 (most risky)	None	Users have no way of getting back to L1 from a sequencer failure
2	Force exit to L1	Users have a way of getting back to L1 from a sequencer failure, but it requires them to pay a fee and wait for a period of time
1 (least risky)	Transact using L1	Users have a way of getting back to L1 from a sequencer failure, and it does not require them to pay a fee or wait for a period of time

Chain Reliability

This risk type evaluates the dependability and stability of a blockchain network. It considers factors like how many network halts have occurred on the blockchain.

I. How many network halts has the blockchain experienced within the past year?
This risk score is a measure of a blockchain's reliability by evaluating how many times the network has halted over the last 12 months. A network halt is an event that causes the blockchain to stop producing new blocks or validating transactions. A network halt can be caused by various factors, such as software bugs, hardware failures, network attacks, or consensus issues. A network halt can affect the availability, security, and performance of the blockchain and its applications. The more frequent and severe the network halts are, the higher the risk of losing data, facing delays, or experiencing disruptions, all of which can lead to principal loss during highly volatile market conditions.

Risk Score	Number of Halts	Description
3 (most risky)	More than 3	The blockchain has experienced more than three network halts in the last 12 months. This indicates a high risk of losing data, facing delays, or experiencing disruptions due to the poor reliability and stability of the network.
2	At least 1	The blockchain has experienced at least one network halt in the last 12 months. This indicates a moderate risk of losing data, facing delays, or experiencing disruptions due to the moderate reliability and stability of the network.
1 (least risky)	None	The blockchain has not experienced any network halts in the last 12 months. This indicates a low risk of losing data, facing delays, or experiencing disruptions due to the high reliability and stability of the network.

Protocol Risks

This risk category evaluates how well the protocol is coded and designed to provide security and functionality to its users. A secure and functional protocol should prevent or mitigate threats such as exploits, hacks, errors, or failures. An insecure or dysfunctional protocol could expose its users to risks such as losing funds, experiencing delays, facing interruptions, or losing trust. This section assigns an overall risk score to each protocol based on its code quality, maturity, and design.

Protocol Code Quality

This risk type evaluates how well the protocol's code is written and audited to ensure its security and functionality. It considers factors such as the number of hacks (if any), documentation, team background, and auditing.

I. How many audits of the deployed contract?
This risk score is a measure of the number of public audits performed on a protocol's core contracts. A public audit is a process of reviewing and verifying the code and design of the core contract by an independent third-party auditor. A public audit aims to identify and fix any bugs, vulnerabilities, or errors in the core contract that could compromise the security or functionality of the protocol. A public audit also provides a report that documents the findings and recommendations of the auditor, which can be accessed and reviewed by anyone. A protocol with zero audits of the deployed contract is considered very risky because it means that the core contract has not been thoroughly tested or validated by any external expert, and it could contain unknown or hidden flaws that could endanger the users' funds or assets. A protocol with two or more audits of the deployed contract is considered less risky because it means that the core contract has been extensively examined and improved by multiple external experts, and it could have a higher level of quality and reliability.

Risk Score	Number of Audits	Description
3 (most risky)	0	The core contract has not been checked or tested by any auditor
2	1	The core contract has been checked or tested by one auditor
1 (least risky)	2+	The core contract has been checked or tested by many auditors

II. Is the team anonymous?

This risk score is a measure of whether the team is anonymous or public. A team is anonymous if the identities and backgrounds of the team members are not disclosed or verified by any credible source. A team is public if the identities and backgrounds of the team members are disclosed and verified by any credible source, such as LinkedIn, Twitter, or GitHub. A team's anonymity or publicity can affect the trust and confidence of the users in the protocol. A protocol with an anonymous team is considered riskier because it means that the users have to rely more on the code and design of the protocol. An anonymous team could also have malicious intentions or hidden agendas that could harm the users or the protocol. A protocol with a public team is considered less risky because it means that the users have some information and assurance about the team's qualifications and reputation. A public team could also have more incentives and accountability to act honestly and responsibly towards the users and the protocol.

Risk Score	Team Anonymity	Description
2 (most risky)	Anonymous	No one knows or can prove who the team is or what they have done before
1 (least risky)	Public	Everyone knows or can prove who the team is and what they have done before

III. How many experienced auditors?

This risk score is a measure of the number of experienced auditors that have reviewed the core contracts. An experienced auditor is an independent and reputable third-party auditor that has a proven track record of conducting high-quality and comprehensive audits for various protocols in the blockchain space. Some examples of experienced auditors are OpenZeppelin, Trail of Bits, and Quantstamp. A protocol with zero qualified audits is considered very risky because it means that the core contract has not been thoroughly tested or validated by any reputable expert in a recent time period, and it could contain unknown or hidden flaws that could endanger the users' funds or assets. A protocol with two or more qualified audits is considered less risky because it means that the core contract has been extensively examined and improved by multiple reputable experts in a recent time period, and it could have a higher level of quality and reliability.

Risk Score	Number of Qualified Auditors	Description
3 (most risky)	0	The core contract has not been checked by any experienced auditor
2	1	The core contract has been checked by one experienced auditor
1 (least risky)	2+	The core contract has been checked by many experienced auditors

IV. How many hacks since launch?

This risk score is a measure of the number of hacks experienced by a protocol across different versions. A hack is a malicious attack that exploits a vulnerability or flaw in the protocol's code, resulting in the loss or theft of funds or assets from the protocol or its users. A version is a specific iteration or release of the protocol's code or design, which may contain new features, improvements, or bug fixes. A protocol may have multiple versions over time, as it evolves and adapts to changing needs or demands. A protocol with two or more hacks since launch is considered very risky because it means that the protocol has a history of being compromised by attackers multiple times, and it could indicate a lack of security or quality in the protocol's code or design. A protocol with zero hacks since launch, across versions, is considered less risky, because it means that the protocol has a history of being secure and resilient against attackers, and it could indicate a high level of security or quality in the protocol's code.

Risk Score	Number of Hacks	Description
5 (most risky)	2+	The protocol has been hacked many times since launch
4	1 - unaddressed	The protocol has been hacked once since launch and has not fixed the problem
3	1 - addressed	The protocol has been hacked once since launch and has fixed the problem
2	0 in current version, but 1 - addressed in last version	The protocol has not been hacked in the current version, but was hacked once in the last version and fixed the problem
1 (least risky)	0 across versions	The protocol has not been hacked at all since launch, across versions

Protocol Maturity

This risk category evaluates how long the protocol has been running on the mainnet and how well it has performed in different scenarios. It considers factors such as the maturity of the first and latest versions, governance issues, and upgradeability.

I. What is the maturity of the latest protocol version?

This risk score evaluates how long the latest version of a protocol has been running on the mainnet without any major issues or incidents. The mainnet is the live network where real transactions and interactions take place, as opposed to testnets where developers can experiment and test their code. The longer a protocol has been on the mainnet, the more likely it is that it has been exposed to different scenarios and stress tests and that any bugs or vulnerabilities have been fixed or mitigated. Therefore, a higher maturity score indicates a lower risk of encountering unexpected problems or failures with the protocol.

Risk Score	Maturity	Description
5 (most risky)	0-3 months	The newest version of the protocol has been on the mainnet for less than 3 months
4	3-6 months	The newest version of the protocol has been on the mainnet for 3 to 6 months
3	6-9 months	The newest version of the protocol has been on the mainnet for 6 to 9 months
2	9-12 months	The newest version of the protocol has been on the mainnet for 9 to 12 months
1 (least risky)	12+ months	The newest version of the protocol has been on the mainnet for more than a year

II. What is the maturity of the first protocol version?

This risk score evaluates how long a protocol has been in existence and operating on the mainnet since its first version. The longer a protocol has been on the mainnet, the more likely it is that it has established a reputation, a community, and a track record of delivering value and innovation. The Lindy effect is a theory that states that the future life expectancy of a non-perishable thing like a technology or an idea is proportional to its current age. Therefore, a higher maturity score indicates a lower risk of the protocol becoming obsolete or irrelevant.

Risk Score	Maturity	Description
5 (most risky)	0-6 months	The protocol has been on the mainnet for less than 6 months since its first version
4	6-12 months	The protocol has been on the mainnet for 6 to 12 months since its first version
3	12-18 months	The protocol has been on the mainnet for 12 to 18 months since its first version
2	18-24 months	The protocol has been on the mainnet for 18 to 24 months since its first version
1 (least risky)	24+ months	The protocol has been on the mainnet for more than two years since its first version

III. What is the total value locked for the protocol?

This risk score evaluates how much trust and confidence a protocol has earned from users based on how much capital they have deposited into it. Total value locked (TVL) is a metric that measures the amount of assets that are locked in a protocol's smart contracts. TVL can indicate the popularity, utility, and profitability of a protocol, as well as its resilience to market fluctuations and security incidents. The higher the TVL of a protocol, the lower the risk of it being abandoned or exploited.

Risk Score	TVL Rank	Description
5 (most risky)	Bottom 80%	The protocol has a low TVL and is not very popular or trusted by users
4	Top 20%	The protocol has a moderate TVL and is somewhat popular or trusted by users
3	Top 10%	The protocol has a high TVL and is very popular or trusted by users
2	Top 5%	The protocol has a very high TVL and is extremely popular or trusted by users
1 (least risky)	Top 1%	The protocol has the highest TVL and is the most popular or trusted by users

IV. Are there any governance issues?

This risk score evaluates how well the protocol's governance system works and how it handles any issues or disputes that may arise. Governance is the process of making decisions and implementing changes to a protocol, and it can involve different stakeholders such as developers, users, token holders, or third parties. Governance can be formal or informal, centralized or decentralized, on-chain or off-chain, depending on the design and goals of the protocol. However, governance can also face various challenges or problems, such as low participation, high concentration, lack of transparency, misalignment of incentives, or conflicts of interest. Therefore, the fewer and less severe the governance issues are, the lower the risk of the protocol being dysfunctional or unfair. However, this score does not guarantee that a protocol is always democratic or efficient, as governance can also evolve or adapt over time. We define the severity of governance issues based on the impact of the issue on the protocol's security, performance, functionality, or fairness.

Some examples of governance issues are:

- Low: Timelock contract shorter than 3 years that grants core team members tokens
- Medium: Unintended release of tokens from the staking or liquidity mining contracts
- Critical: Has the team been involved in public scandals (personally or in a professional capacity) such as self-dealing, conflict of interests or about their background?

Risk Score	Description
5 (most risky)	Multiple Critical issues
4	At least 1 issue of Critical severity
3	At least 1 issue of Medium severity but none higher
2	At least 1 issue of Low severity but none higher
1 (least risky)	No other governance issues

V. How concentrated are governance holders?

This risk score evaluates how decentralized and diverse the protocol's governance holders are. Governance holders are the entities that own or control the governance token of a protocol, which gives them the right to vote on proposals or changes that affect the protocol. Governance tokens can be distributed or sold in various ways, such as airdrops, liquidity mining, public sales, or private sales. However, governance tokens can also be concentrated or hoarded by a few holders, such as founders, investors, whales, or insiders. This can create a power imbalance or a conflict of interest in the governance process and can undermine the legitimacy and security of the protocol. Therefore, the more holders that collectively own 51% of the governance token, the lower the risk of the protocol being dominated or captured by a few parties.

Risk Score	Governance Concentration (>51% voting power)	Description
5 (most risky)	5 or less holders	The protocol is highly centralized and vulnerable to capture by a few parties
4	6 to 20 holders	The protocol is moderately centralized and susceptible to influence by a small group of parties
3	21 to 50 holders	The protocol is somewhat decentralized and diverse, but still has room for improvement
2	50 to 100 holders	The protocol is fairly decentralized and diverse, but may face challenges in coordination or representation.
1 (least risky)	More than 100 holders or N/A	The protocol is very decentralized and diverse or does not use a governance token

VI. How can the protocol be upgraded?

This risk score evaluates how decentralized and secure the protocol's governance and upgrade process is. A protocol can be upgraded by changing its smart contract code or parameters to add new features, fix bugs, or improve performance. However, the ability to upgrade a protocol also implies the ability to change its rules or logic, which can affect the users and their funds. Therefore, the more transparent, participatory, and immutable the upgrade process is, the lower the risk of it being abused or compromised.

Risk Score	Upgrade Process	Description
5 (most risky)	EOA (Externally Owned Account) wallet	The protocol can be upgraded by one person or account that has full control over the smart contract
4	Multisig wallet	The protocol can be upgraded by a group of people or accounts that have shared control over the smart contract
3	DAO vote	The protocol can be upgraded by the members of a decentralized organization that have voting rights over the smart contract
2	Fully immutable with on-chain voting for parameter updates	The protocol's core contracts cannot be upgraded at all, but there are certain parameters that can be updated via governance
1 (least risky)	Fully immutable	The protocol cannot be upgraded at all, and the smart contract code and settings are fixed

VII. What multisig configuration does the protocol use?

This risk score evaluates how secure and decentralized the protocol's multisig configuration is. A multisig is a type of smart contract that requires multiple signatures or approvals from different parties to execute a transaction or function. A multisig can be used to control the funds, governance, or upgradeability of a protocol and can prevent single points of failure or malicious actions. However, the security of a multisig depends on how many signers are required and who they are. Therefore, the more signers a multisig requires, the lower the risk of it being compromised or corrupted.

Risk Score	Multisig Configuration	Description
3 (most risky)	1 signer (or EOA)	The protocol can be controlled by just one person or account that has full access to the smart contract
2	<4 signers	The protocol can be controlled by a small group of people or accounts that have shared access to the smart contract
1 (least risky)	>4 signers	The protocol control is distributed amongst a large group of people or accounts that have shared access to the smart contract

VIII. What timelock configuration does the protocol use?

This risk score evaluates how safe and transparent the protocol's timelock configuration is. A timelock is a feature that delays the execution of a transaction or function for a certain period of time after it has been approved. A timelock can be used to protect the funds, governance, or upgradeability of a protocol, and can give users time to react or exit if they disagree with a proposed change. However, the safety and transparency of a timelock depend on how long the delay is and how well it is documented. Therefore, the longer the timelock and the better the documentation, the lower the risk of it being exploited or misused.

Risk Score	Timelock Configuration	Description
3 (most risky)	No timelock (or no documentation)	The protocol can be changed without any delay or transparency
2	<48hrs	The protocol can be changed with a short delay and minimal transparency
1 (least risky)	>=48hrs	The protocol can be changed with a long delay and high transparency

Protocol Design

The Protocol Design section evaluates how well the protocol's architecture and features meet its goals and user needs. It considers factors such as the type of oracle (if applicable), convex relationships, and the protocol's job type.

I. What type of oracle is used?

This risk score evaluates the type of oracle the protocol relies on for its core services. An oracle is a third-party service that connects smart contracts with external data sources. Oracles can use different methods to calculate the average price of an asset over a period of time, such as TWAP, VWAP, or Multiple Feeds.

- **TWAP** (time-weighted average price) is calculated by summing prices at multiple points across a set period and then dividing this total by the total number of price points. TWAP is simple to calculate and can protect against flash loan attacks, but it can be inaccurate if the market is volatile or illiquid.
- **VWAP** (volume-weighted average price) is calculated by multiplying each price by its corresponding volume and then dividing the sum by the total volume. VWAP can reflect the true market price better than TWAP, but it can be more complex to calculate and more vulnerable to manipulation by large trades.
- **Multiple Feeds** refer to using data from multiple sources or aggregators to calculate the average price of an asset. An oracle with Multiple Feeds can increase the reliability and security of the price data, but it can also introduce more latency and complexity in the oracle mechanism.

Risk Score	Oracle Type	Description
6 (most risky)	No TWAP or Multiple Feeds or no documentation	The protocol uses oracles that do not have TWAP or Multiple Feeds or does not say what type of oracle it uses
5	Only TWAP	The protocol uses oracles that only have TWAP
4	Only TWAP (geometric mean)	The protocol uses oracles that only have TWAP (geometric mean), which is more accurate than regular TWAP
3	Only Multiple Feeds	The protocol uses oracles that only have Multiple Feeds
2	Both VWAP and Multiple Feeds	The protocol depends on oracles that have both VWAP and Multiple Feeds, which is more accurate and reliable than other types
1 (least risky)	No oracles needed	The protocol does not depend on any oracles

II. Does the protocol have any convex relationships?

This risk score evaluates how reflexive or circular the protocol's tokenomics are. Tokenomics ("token economics") is the study of how tokens are designed, distributed, and used within a protocol or ecosystem. Tokens can have various functions and incentives, such as governance, utility, reward, or speculation. However, tokens can also create feedback loops or convex relationships, where the price of the token affects the behavior of the users, which in turn affects the price of the token. This can lead to positive or negative spirals, where the token price either increases or decreases exponentially. This can create instability, volatility, or manipulation risks for the protocol and its users. Therefore, the less reflexive or circular the tokenomics are, the lower the risk of the protocol being unsustainable.

Risk Score	Convexity	Description
4 (most risky)	High	The protocol's purpose is selling its own token and the token has no use other than speculation. The token price is highly dependent on demand and supply, which can be easily manipulated or affected by external factors.
3	Moderate	The protocol has a purpose and uses its token in a reflexive way. The token price affects the utility or reward of the token, which influences the user behavior and demand for the token.
2	Low	The protocol has a purpose and uses its token in a reflexive way but there are mechanisms to stop reflexivity. The token price affects the utility or reward of the token, but there are caps, floors, burns, locks, or other features that limit the feedback loop and stabilize the token price.
1 (least risky)	None	The protocol has non-reflexive tokenomics. The token price does not affect the utility or reward of the token, and there are no feedback loops or circular dependencies in the tokenomics.

III. What job type does the protocol fall under?

This risk score evaluates how complex and risky the protocol's job type is. A job type is the main function or service that a protocol provides to its users or the ecosystem. Different job types have different levels of difficulty, regulation, and competition, which can affect the security and profitability of the protocol and its users. Therefore, the more complex and risky the job type is, the higher the risk of the protocol being hacked, exploited, or outperformed.

Risk Score	Job Type*	Description
8 (most risky)	Insurance	The protocol provides coverage for losses or damages caused by unforeseen events or risks. The protocol faces high complexity, as well as potential fraud or undercollateralization issues. The protocol also needs to maintain sufficient reserves and liquidity to pay out claims.
7	Bridge	The protocol enables cross-chain interoperability and asset transfers between different blockchains. The protocol faces high technical challenges and security risks, as well as potential network congestion or compatibility issues. The protocol also needs to ensure trustless and decentralized bridging mechanisms.
6	Options	The protocol enables users to buy or sell the right to trade an underlying asset at a predetermined price and time. The protocol faces high volatility and competition, as well as potential liquidity or oracle issues. The protocol also needs to ensure fair and efficient pricing and settlement mechanisms.
5	Derivatives	The protocol enables users to trade contracts that derive their value from an underlying asset or index. The protocol faces high leverage and complexity, as well as potential manipulation or liquidation issues. The protocol also needs to ensure accurate and timely margin and risk management mechanisms.
4	Market Making	The protocol enables users to provide liquidity and facilitate trading for various assets or pairs. The protocol faces high capital and competition, as well as potential slippage or impermanent loss risks. The protocol also needs to ensure optimal fee and reward mechanisms.
3	CDPs & Lending	The protocol enables users to create collateralized debt positions (CDPs) or lend and borrow various assets. The protocol faces high demand, as well as potential overcollateralization or liquidation issues. The protocol also needs to ensure stable and attractive interest rate mechanisms.

2	Yield	The protocol enables users to earn passive income by staking or farming various assets or tokens. The protocol has low complexity but may have potential inflation or sustainability issues. The protocol also needs to ensure consistent and diversified yield sources and strategies.
1 (least risky)	Staking	The protocol enables users to stake their native tokens to secure the network and earn rewards. The protocol faces low risk and regulation but may have potential lockup or opportunity cost issues. The protocol also needs to ensure fair and transparent staking mechanisms and policies.

[*]: Note that this risk score is based on a general assessment of the job type and does not reflect the specific risks of each protocol within the same job type. We have developed more granular risk frameworks for CDPs & Lending and Bridge protocols (will be published soon). For the other job types, we are still working on building out the detailed risk frameworks and will update this table accordingly.

Asset Risks

This risk category evaluates how the asset is valued or its underlying backing to provide stability and growth to its holders. A stable and growing asset should reflect the demand and supply of the protocol and its users. An unstable or declining asset could expose its holders to risks such as losing value, facing volatility, experiencing dilution, or losing utility. This section assigns an overall risk score to each asset based on its strength and tokenomics.

Asset Strength

This risk type evaluates how well the asset's price and market cap reflects the value and potential of the protocol and its users. It considers factors such as the demand and supply of the asset, collateralization levels, market cap, centralization, and volatility.

I. Does the asset have intrinsic value or is it fully collateralized?

This risk score evaluates how well the asset's value is backed or supported by an intrinsic use case. An asset can have intrinsic value, which means that it derives its value from its own properties or utility, such as being a native token of a blockchain or a protocol. Alternatively, an asset can be collateralized, which means that it derives its value from being backed or redeemable by another asset, such as a synthetic token or a stablecoin. However, collateralization can also involve risks, such as over-issuance, under-collateralization, liquidation, or insolvency. Therefore, the more intrinsic or over-collateralized the asset is, the lower the risk of it losing its value or becoming worthless.

Risk Score	Collateralization	Description
5 (most risky)	Under-collateralized by less than 100%	Asset does not have enough backing to cover the full value of the asset in case of redemption or liquidation. This exposes the asset to high volatility and default risk.
4	Might be undercollateralized	Asset has uncertainty about the level of backing or the quality of the collateral. This exposes the asset to moderate volatility and default risk.
3	Fully collateralized above 100%	Asset has enough backing to cover the full value of the asset in case of redemption or liquidation. This reduces the volatility and default risk of the asset.
2	Intrinsic value as native protocol token	Asset derives its value from its own properties or utility, such as being used for transactions, governance, or staking on a protocol layer that provides a specific service or functionality on top of a blockchain network. This makes the asset independent of any backing or collateral.
1 (least risky)	Intrinsic value as native blockchain token	Asset derives its value from its own properties or utility, such as being used for transactions, governance, or staking on a blockchain network. This makes the asset independent of any backing or collateral and also increases its demand and utility.

II. What is the asset's market capitalization?

This score evaluates how large and established the asset's market is based on its total market capitalization. Market cap is a metric that measures the total value of all the circulating supply of an asset. It is calculated by multiplying the current price of the asset by the number of units in circulation. Market cap can indicate the popularity, demand, and liquidity of an asset, as well as its potential for growth or decline. In general, the higher the market cap of an asset, the lower the risk of it being illiquid or unstable.

Risk Score	Market Cap	Description
3 (most risky)	Less than $1 billion USD	Asset has a small market cap, meaning that it has a low level of adoption, recognition, and liquidity. This exposes the asset to high volatility and price manipulation.
2	Between $1 billion and $10 billion USD	Asset has a medium market cap, meaning that it has a moderate level of adoption, recognition, and liquidity. This exposes the asset to moderate volatility and price manipulation.
1 (least risky)	More than $10 billion USD	Asset has a large market cap, meaning that it has a high level of adoption, recognition, and liquidity. This reduces the volatility and price manipulation of the asset.

III. Does the asset have any centralized dependencies?

This score evaluates how decentralized and independent the asset is from any centralized entities or intermediaries. An asset can have centralized dependencies, which means that it relies on or interacts with third-party services or platforms that are not controlled by the asset's users or community. For example, an asset can depend on a centralized custodian for storage. Centralized dependencies can also introduce risks around censorship, manipulation, confiscation, or shutdown. Therefore, the fewer centralized dependencies the asset has, the lower the risk of it being affected or disrupted by external factors.

Risk Score	Number of Dependencies	Description
4 (most risky)	3+ centralized entities	Asset has a high level of centralization, meaning that it has a low level of autonomy, security, and resilience. This exposes the asset to a high risk of interference, disruption, or loss by third parties.
3	2 centralized entities	Asset has a moderate level of centralization, meaning that it has a moderate level of autonomy, security, and resilience. This exposes the asset to a moderate risk of interference, disruption, or loss by third parties.
2	1 centralized entity	Asset has a low level of centralization, meaning that it has a high level of autonomy, security, and resilience. However, it still has some exposure to the risk of interference, disruption, or loss by a third party.
1 (least risky)	None	Asset has a high level of decentralization, meaning that it has a high level of autonomy, security, and resilience. It does not have any exposure to the risk of interference, disruption, or loss by third parties.

IV. If the asset is a stablecoin, how closely does it follow its peg?

This score evaluates how stable and consistent the asset's price is relative to its target value. A stablecoin is a type of asset that aims to maintain a stable value by pegging itself to another asset, such as a fiat currency, a commodity, or a basket of assets. A stablecoin can use different mechanisms to achieve its peg, such as collateralization, algorithmic adjustment, or hybrid models. However, stablecoins can also face various challenges or shocks that can cause their price to deviate from their peg, such as market fluctuations, supply and demand imbalances, regulatory actions, or technical issues. Therefore, the smaller the deviation from the peg, the lower the risk of the asset losing its stability or utility.

Risk Score	Peg Deviation	Description
5 (most risky)	>100bps	Asset has a high level of deviation from its peg, meaning that it has a low level of stability and consistency. This exposes the asset to high volatility and inefficiency.
4	≤100 bps	Asset has a moderate level of deviation from its peg, meaning that it has a moderate level of stability and consistency. This exposes the asset to moderate volatility and inefficiency.
3	≤50 bps	Asset has a low level of deviation from its peg, meaning that it has a high level of stability and consistency. This reduces the volatility and inefficiency of the asset.
2	≤20 bps	Asset has a very low level of deviation from its peg, meaning that it has a very high level of stability and consistency. This minimizes the volatility and inefficiency of the asset.
1 (least risky)	≤10 bps	Asset has a negligible level of deviation from its peg, meaning that it has an almost perfect level of stability and consistency. This eliminates the volatility and inefficiency of the asset.

Asset Tokenomics

This risk type evaluates how the asset's token design aligns with the incentives and interests of the protocol and its users. Currently, It only considers factors about the asset's inflation rate and convex relationships (if any).

I. Is the asset inflationary?

This risk score evaluates how the asset's supply affects its value over time. An asset can have a fixed or a variable supply, depending on how it is created, distributed, and destroyed. An asset with a fixed supply has a predetermined or capped number of units that will ever exist, such as Bitcoin. An asset with a variable supply has an unlimited or uncapped number of units that can be created or destroyed, such as Ether. An asset with a variable supply can also have a burn mechanism, which means that some units are permanently removed from circulation under certain conditions, such as transaction fees or network activity. However, the supply of an asset can also influence its price, demand, and scarcity. Therefore, the more limited or predictable the supply of an asset is, the lower the risk of it losing its value or purchasing power due to inflation.

Risk Score	Inflation	Description
3 (most risky)	Infinite supply	Asset has an infinite supply, meaning that there is no limit to how many units can be created. This exposes the asset to high inflation and dilution.
2	Infinite supply with burn mechanism	Asset has an infinite supply with a burn mechanism, meaning that some units are destroyed under certain conditions. This reduces the inflation and dilution of the asset.
1 (least risky)	Supply capped	Asset has a supply cap, meaning that there is a limit to how many units will ever exist. This protects the asset from inflation and dilution.

II. Does the asset have a reflexive design?

This risk score evaluates how the asset's price affects its utility or demand and vice versa. Reflexivity is a phenomenon where the price of an asset influences the behavior of its users, which in turn influences the price of the asset. This can create positive or negative feedback loops, where the price and the utility or demand of the asset either reinforce or undermine each other. For example, an asset that has a governance function can become more valuable as its price increases because it gives more voting power or influence to its holders, which can attract more users or demand. Conversely, an asset that has a utility function can become less valuable as its price decreases because it reduces its usefulness or functionality for its users, which can deter more users or demand. Additionally, an asset can also be influenced by a sister asset, where the two assets' values are tied to each other based on certain arbitrage opportunities. For example, a stablecoin that is partially backed by another token can affect the price and demand of both assets. Therefore, the less reflexive the asset is, the lower the risk of it being affected by negative feedback loops or death spirals.

Risk Score	Reflexivity	Description
3 (most risky)	Concerning reflexivity	Asset has a high level of interdependence between its price and its utility or demand. This exposes the asset to a high risk of instability or collapse due to feedback loops or spirals.
2	Non-concerning reflexivity	Asset has a moderate level of interdependence between its price and its utility or demand. This exposes the asset to a moderate risk of instability or collapse due to feedback loops or spirals.
1 (least risky)	Non-detected/existing reflexivity	Asset has a low or negligible level of interdependence between its price and its utility or demand. This protects the asset from instability or collapse due to feedback loops or spirals.

Pool Risks

This risk category evaluates how the pool is managed and its underlying strategies that users are exposed to. This section assigns an overall risk score to each pool based on its design.

Pool Design

This risk type assesses how the pool is designed to provide liquidity and generate yield for its users. It considers various factors such as the pool type, the yield strategy, the collateralization ratio, the leverage level, and the collateral quality. A well-designed pool should provide a high level of liquidity and yield to its users. A poorly-designed pool could expose its users to various risks, such as liquidation, impermanent loss, volatility, or low returns. This section assigns a risk impact score to each pool based on its design and performance in these aspects.

I. Does the pool have any fee-sharing mechanisms?

This risk score evaluates the risk of a fee-sharing pool where users have to deposit an asset as collateral to start receiving protocol-generated fees. Fee-sharing pools are pools that distribute a portion of the fees collected by the protocol to the users who provide liquidity or stake their assets. Fee-sharing pools can provide an additional source of income for the users, but they also expose them to volatility risks. Therefore, the less risky or volatile the collateral asset is, the lower the risk of losing value or fees due to fee sharing.

Risk Score	Fee-sharing Type	Description
3 (most risky)	Fee-sharing with native token	Asset has a high level of volatility, meaning that its price can fluctuate significantly due to market forces or protocol events. This exposes the asset to a high risk of losing value due to price changes.
2	Fee sharing with crypto assets (e.g., BTC, ETH)	Asset has a moderate level of volatility, meaning that its price can fluctuate moderately due to market forces or network events. This exposes the asset to a moderate risk of losing value due to price changes.
1 (least risky)	Fee sharing with stablecoin	Asset has a low level of volatility, meaning that its price is relatively stable due to its peg or backing. This reduces the risk of losing value due to price changes.

II. Does the pool require staking an asset to secure a network?

This risk score evaluates the risk of a staking pool where users deposit an asset as collateral to secure a network. The risk depends on whether the pool has a slashing mechanism or not. Slashing is a penalty that reduces the stake of a validator if they act maliciously or fail to perform their duties. Slashing increases the risk of losing funds but also increases the security and reliability of the network.

Risk Score	Staking Type	Description
2 (most risky)	Slashing	The pool has a slashing mechanism that can reduce the stake of a validator if they misbehave or underperform. This increases the risk of losing funds.
1 (least risky)	No slashing	The pool does not have a slashing mechanism that can reduce the stake of a validator. This lowers the risk of losing funds.

III. Is the pool managed by a yield optimizer?

This risk score evaluates the risk of a pool that is managed by a yield optimizer. A yield optimizer is a smart contract that automatically allocates funds to different protocols or strategies to maximize returns. The risk depends on the complexity and number of strategies involved, as well as the need for off-chain computations. The more complex and numerous the strategies are, the higher the risk of errors, failures, or exploits. The need for off-chain computations also increases the risk of manipulation, delay, or interruption.

Risk Score	Yield Strategy	Description
3 (most risky)	6+ strategies or requires off-chain computations	The pool involves a high complexity yield strategy, which increases the risk of errors, failures, or exploits due to the high number of interactions. The off-chain computations also increase the risk of manipulation, delay, or interruption due to the reliance on external data sources or services.
2	3-5 strategies or requires off-chain computations	The pool involves a medium complexity yield strategy, which increases the risk of errors, failures, or exploits due to the moderate number of interactions. The off-chain computations also increase the risk of manipulation, delay, or interruption due to the reliance on external data sources or services.
1 (least risky)	1-2 dependencies or simple rebalancing	This pool involves a low complexity yield strategy, which lowers the risk of errors, failures, or exploits due to the low number of interactions. The simple rebalancing also does not require off-chain computations and reduces the risk of manipulation, delay, or interruption.

IV. Does the pool have exposure to any lending strategies?

This risk score evaluates the risk of a pool that has exposure to any lending strategies. A collateralized asset is an asset that is backed by another asset as a guarantee of repayment. Leverage is the use of borrowed funds to increase the potential return on an investment. The risk depends on the level of collateralization and leverage involved, as well as the volatility and liquidity of the assets. The lower the collateralization and the higher the leverage, the higher the risk of liquidation, insolvency, or principal loss.

Risk Score	Lending Strategy	Description
4 (most risky)	Recursive leverage (>2x)	The pool involves a lending strategy that uses leverage recursively, meaning that it borrows funds to lend them again and repeats the process. This greatly increases the risk of liquidation, insolvency, or loss due to the high exposure and complexity of the strategy.
3	Leverage (>1x)	The pool involves a lending strategy that uses leverage, meaning it borrows funds to increase returns. This increases the risk of liquidation, insolvency, or loss due to the high exposure and complexity of the strategy.
2	Low collateralized positions	The pool involves a lending strategy that uses low collateralized positions, meaning that it lends funds with a low ratio of collateral to loan value. This increases the risk of liquidation, insolvency, or loss due to the low security and stability of the positions.
1 (least risky)	Overcollateralized position	The pool involves a lending strategy that uses overcollateralized positions, meaning that it lends funds with a high ratio of collateral to loan value. This lowers the risk of liquidation, insolvency, or loss due to the high security and stability of the positions.

V. Does the pool have exposure to any collateralized assets?

This risk score evaluates the risk of a pool that has exposure to any collateralized assets. A collateralized asset is an asset that is backed by another asset as a guarantee of repayment. The risk depends on the type and quality of the collateral asset, as well as its liquidity and volatility. The lower the quality and liquidity and the higher the volatility of the collateral asset are, the higher the risk of loss or facing liquidations.

Risk Score	Collateralization	Description
6 (most risky)	Long-tail assets	The pool is collateralized by long-tail assets that have low demand, low liquidity, and high volatility. This increases the risk of losing value, facing liquidation, or experiencing delays due to the poor market conditions and price fluctuations of these assets.
5	Liquidity Provider (LP) tokens	The pool is collateralized by LP tokens that represent a share of a liquidity pool. This increases the risk of losing value, facing liquidation, or experiencing delays due to the lack of available price oracles to price the LP tokens. A price oracle is a service that provides reliable and up-to-date price information for an asset. Without a price oracle, the LP tokens may be under- or over-valued in the lending market, which makes them more vulnerable to exploitation by arbitrageurs or attackers.
4	Native protocol token OR Algo-stablecoins OR Liquid Staking Derivatives (LSDs) from Watch Out-rated protocols	The pool is collateralized by one of these types of assets: - Native protocol token: a token that is issued by a specific protocol. - Algo-stablecoin: a token that is algorithmically pegged to a stable asset such as USD. - Liquid Staking Derivative (Watch Out rating): a token that represents a staked asset in a blockchain network. These types of assets increase the risk of losing value, facing liquidation, or experiencing delays due to their high volatility, low liquidity, and high dependency on the performance and security of their underlying protocols.

Risk Score	Collateralization	Description
3	Highly traded assets OR LSDs from Average-rated protocols	The pool is collateralized by one of these types of assets: - Highly traded asset: an asset that has high demand, high liquidity, and low volatility in the market. - Liquid Staking Derivative (Average rating): a token that represents a staked asset in a blockchain network. These types of assets lower the risk of losing value, facing liquidation, or experiencing delays due to their good market conditions and price stability. However, they still have some exposure to the performance and security of their underlying protocols.
2	Native chain tokens OR LSDs from Good or Best-rated protocols	The pool is collateralized by one of these types of assets: - Native chain token: a token that is native to and is used for network payments on a specific blockchain. - Liquid Staking Derivative (Good or Best rating): a token that represents a staked asset in a blockchain network. These types of assets lower the risk of losing value, facing liquidation, or experiencing delays due to their high demand, high liquidity, and high security in the market. They also have less exposure to the performance and security of their underlying protocols.
1 (least risky)	Highly liquid, on-chain assets OR fully redeemable stablecoins	The pool is collateralized by one of these types of assets: - Highly liquid, on-chain asset: an asset that has high demand, high liquidity, and low volatility. - Fully redeemable stablecoin: a token that is fully backed by and redeemable for a stable asset such as USD. These types of assets lower the risk of losing value, facing liquidation, or experiencing delays due to their excellent market conditions and price stability. They also have minimal exposure to the performance and security of their underlying protocols.

VI. Does the pool have exposure to market making?

This risk score evaluates the risk of a pool that has exposure to decentralized exchanges (DEXs). A DEX is a smart contract that provides liquidity and price discovery for a pair of assets. The key risk evaluated here is the divergence loss or impermanent loss risk, which is the loss of value that occurs when the price ratio of the assets in the pool diverges from the initial ratio. The more volatile and divergent the assets are, the higher the risk of divergence loss.

Risk Score	Market Making Type	Description
4 (most risky)	Volatile-USD pools	Volatile-USD pools consist of a pair of assets where one is volatile (such as BTC), and the other is stable (such as USDC). This increases the risk of divergence loss due to the high volatility and potential divergence of the volatile asset.
3	Volatile-Volatile pools	Volatile-volatile pools consist of a pair of assets where both are volatile (such as BTC-ETH). This increases the risk of divergence loss due to the high volatility and potential divergence of both assets.
2	Stable pools	Stable pools consist of a pair of assets where both are stable (such as two stablecoins). This lowers the risk of divergence loss due to the low volatility and minimal divergence of both assets.
1 (least risky)	Central limit order book (CLOB)	Central limit order book (CLOB) systems provide liquidity for a pair of assets where buyers and sellers can place orders at different prices. This eliminates the risk of divergence loss due to the ability to adjust the price and quantity of the orders according to market conditions.

VII. Does the pool have exposure to options?

This risk score evaluates the risk of a pool that has exposure to decentralized options. An option is a contract that gives the buyer the right, but not the obligation, to buy or sell an underlying asset at a specified price and time. A decentralized option is an option that is issued and traded on a blockchain network. The risk depends on the type and complexity of the option strategy involved, as well as the volatility and liquidity of the underlying asset. The more complex and risky the option strategy is, the higher the risk of loss.

Risk Score	Options Strategy	Description
3 (most risky)	Advanced option strategies (e.g. straddles)	Advanced option strategy, such as straddles, involves buying or selling both a call and a put option with the same strike price and expiration date. This increases the risk of losing value due to the high cost and complexity of the strategy, as well as the high volatility and uncertainty of the underlying asset.
2	Secured put vaults	Secured put vaults consist of selling put options and holding enough stable collateral to buy the underlying asset if the option is exercised. This lowers the risk of losing value due to the premium received from selling the option and the security of having enough collateral. However, there is still some risk of losing value if the underlying asset drops significantly below the strike price.
1 (least risky)	Covered call vaults	Covered call vaults consist of selling call options and holding enough of the underlying asset to sell it if the option is exercised. This lowers the risk of losing value due to the premium received from selling the option and the security of having enough of the underlying asset. However, there is still some risk of missing out on potential gains if the underlying asset rises significantly above the strike price.

VIII. Does the pool offer any insurance services?

This risk score evaluates the risk of a pool that insures some users at the expense of others. An insurance service is a service that provides protection against losses or damages in exchange for a fee or premium. A pool that offers insurance services divides its users into two groups: the insured and the insurers. The insured pays a premium to the pool and receive compensation if a loss or damage occurs. The insurers provide capital to the pool and receive a portion of the premium as a reward. The risk depends on the type and position of the insurance service involved, as well as the probability and severity of the loss or damage. The higher the position and reward of the insurance service are, the higher the risk of losing capital or facing liquidation.

Risk Score	Insurance Strategy	Description
4 (most risky)	Junior tranche	The junior tranche provides capital to the pool and receives a high portion of the premium as a reward. However, it also bears the highest risk of losing capital or facing liquidation if a loss or damage occurs, as it is the first to absorb the losses.
3	Mezzanine tranche	The mezzanine tranche provides capital to the pool and receives a moderate portion of the premium as a reward. However, it also bears a moderate risk of losing capital or facing liquidation if a loss or damage occurs, as it is the second to absorb the losses after the junior tranche.
2	Senior tranche	The senior tranche provides capital to the pool and receives a low portion of the premium as a reward. However, it also bears a low risk of losing capital or facing liquidation if a loss or damage occurs, as it is the last to absorb the losses after the junior and mezzanine tranches.
1 (least risky)	Insurance fund	The pool uses an insurance fund, which is a separate pool that provides protection to another pool in exchange for a fee or premium. Protocols that offer built-in insurance or users who pay for third-party insurance are protected against all cases covered under the insurance policy.

Conclusions

In this paper, we present our risk framework for DeFi, which is based on our overall approach to risk in this space. Our approach is to view risk as a dynamic and complex concept that requires a holistic and rigorous analysis. We have developed a framework that covers all the possible sources and outcomes of risk in DeFi, and that quantifies and evaluates risk in an objective and consistent manner. Our framework consists of four main components: risk categories, risk types, risk scores, and risk ratings.

We have explained each component of our framework in detail and provided examples of how we apply them to different DeFi investments. We have also discussed the limitations and challenges of our framework and suggested some directions for future research and improvement.

Our goal is to provide a comprehensive and objective tool for risk assessment in DeFi that can help various stakeholders make better and smarter decisions in this fast-growing and ever-changing domain. We believe that our framework can have several benefits and implications for the DeFi ecosystem:

- For investors, our framework can help them diversify their portfolio and optimize their risk-return trade-off in DeFi. By using our risk framework, investors can compare and select the best DeFi pools based on their risk appetite and preferences.
- For developers, our framework can help them improve their protocol design and security practices in DeFi. By using our risk framework, developers can identify and address the potential risks and vulnerabilities of their protocols. They can also use our framework to communicate and demonstrate the security and reliability of their protocols to their users and investors.
- For regulators, our framework can help them understand and monitor the risks and opportunities of DeFi. By using our risk framework, regulators can gain a comprehensive and objective overview of the DeFi landscape and its main challenges and threats. They can also use our framework to develop and implement appropriate and effective regulations and policies for DeFi that balance innovation and consumer protection.
- For researchers, our framework can help them identify and explore new areas of research and innovation in DeFi. By using our risk framework, researchers can discover new problems and solutions in DeFi that require further investigation and development. They can also use our framework to test and validate their hypotheses and findings in DeFi.

For the DeFi community as a whole, our framework can help foster a more collaborative and transparent culture of risk management in DeFi. By using our framework as a common standard for risk assessment in DeFi, we can promote more trust, accountability, and cooperation among different stakeholders in DeFi.

We hope that our framework can contribute to the development and adoption of DeFi as a more secure, transparent, and efficient alternative to traditional finance. We invite feedback from the DeFi community on our framework and look forward to collaborating with other interested parties to improve it further.

References

1. https://tokenbrice.xyz/money-markets-risk/
2. https://li.fi/knowledge-hub/trust-is-a-spectrum/
3. https://blog.connext.network/the-interoperability-trilemma-657c2cf69f17
4. https://l2beat.com/bridges/tvl
5. https://lambert-guillaume.medium.com/uniswap-v3-lp-tokens-as-perpetual-put-and-call-options-5b66219db827
6. https://smartcontentpublication.medium.com/twap-oracles-vs-chainlink-price-feeds-a-comparative-analysis-8155a3483cbd