Baseline Risk Framework for Institutions Interacting with DeFi

Genesis Global Trading
Summer 2022

Thomas Baker

Table of Contents

Motivation

For the Defi/Lending rotation, it was necessary to fully research and comprehend the unique risks present when interns interact with DeFi protocols. A full understanding of these risks was vital to be able to evaluate Genesis' opportunities in the space. This report is the summation of the research done into specifically counterparty, KYC/AML, and operational risk. Counterparty and KYC/AML risks were investigated for higher level understanding, while operational risks were delved into deeper as they are a risk very unique to DeFi. For each risk, a way to framework to quantify and rank the risk present in any given protocol was developed as a starting point for evaluating economic opportunities.

Counterparty Risk

Definition

Counterparty risk in traditional finance is defined as "the probability that the other party in an investment, credit, or trading transaction may not fulfill its part of the deal and may default on the contractual obligations."[1] For DeFi, the issue with this definition is determining who exactly the counterparty is, as many protocols function essentially as financial intermediaries. May the protocol be held as the responsible counterparty in case of a default? There are two levels to this in DeFi – direct lending (Maple, TrueFi) and indirect lending (Aave, Compound). For direct lending, the counterparty will be defined normally as the party being lent too, while for indirect pooled lending this will be altered to be the protocol itself. For DeFi, the counterparty risk will only include the risk that the borrower/protocol fails to meet financial obligations for purely financial reasons. It is important to note that this does not include various smart contract exploits that may result in lost funds – that is defined as an operational risk for the purposes of this report.

Quantification

There are two aspects which make up the overall counterparty risk – the probability of default, and the severity of a default. The probability of default is self-explanatorily the odds that the protocol/borrower fails to meet its obligations, while the severity of default is dependent on the procedures in place to protect the lender, such as insurance. To consolidate these two risks, a NASA risk matrix[2] will be adapted and used to determine the overall counterparty risk, which will be given a score 1-10. Generally, for such a matrix, a risk of score of 1-4 is be deemed an acceptable risk, 5-7 is acceptable with mitigation, and 8+ is unacceptable – though in such a nascent industry it may be necessary to bend the rules at times.

Table 1. DeFi Counter-Party Risk Matrix

Default Probability	Default Severity				
	Catastrophic 5	Hazardous 4	Major 3	Minor 2	Negligible 1
Frequent 5	10	9	8	7	5
Occasional 4	9	8	7	6	4
Remote 3	8	7	6	4	3
Improbable 2	7	6	4	3	2
Extremely Improbable 1	5	4	3	2	1

The only way to achieve a score of 1 is if the loan is overcollateralized or there simply is no counterparty (staking, liquidity mining), so that it is impossible for the borrower to default as the position would simply be liquidated. Barring overcollateralization, the probability of default is determined simply by the basic assumption that risk corresponds to reward (though recall that this model can be adapted any number of way). The following simple scoring mechanism was made:

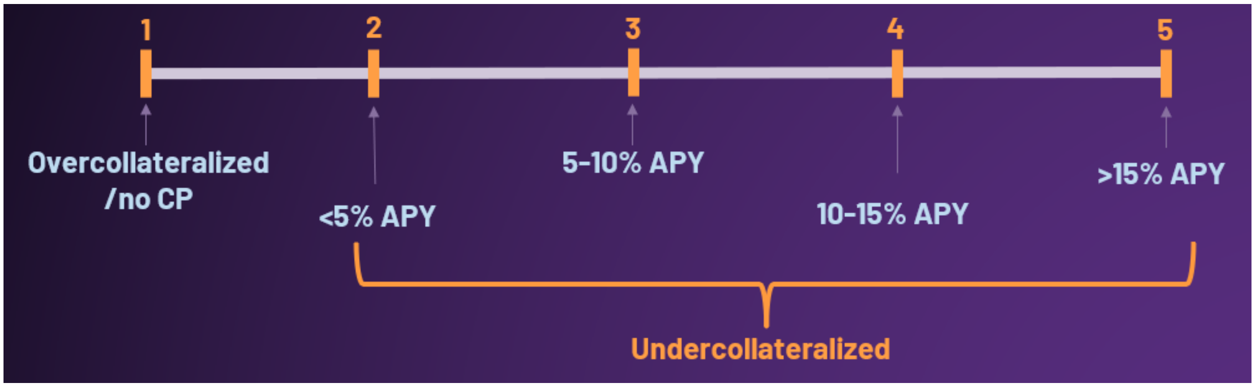

Figure 1. Counterparty default probability scorecard

As for the severity of default, this is determined by the insurance employed by the borrower, protocol, or Genesis. Unfortunately, from the lending side, the only real insurance available is via other DeFi protocols such as Nexus Mutual[3], which themselves have risks associated with usage. As such, DeFi insurance is just a notch above no insurance at all with a score of 4 (hazardous). Other than this, Genesis must rely on the protocols implementing effective insurance policies. Ideally, the protocol would be insured by a true 3rd party insurance provider, which lands it a score of just riskier than there being overcollateralization/no counterparty at all, 2 (minor). Finally, landing in the middle, are insurance policies provided by the protocols themselves, where tokens staked by retail investors act as collateral incase of a default, as is the case with Maple[4]. The summation of this is shown below.

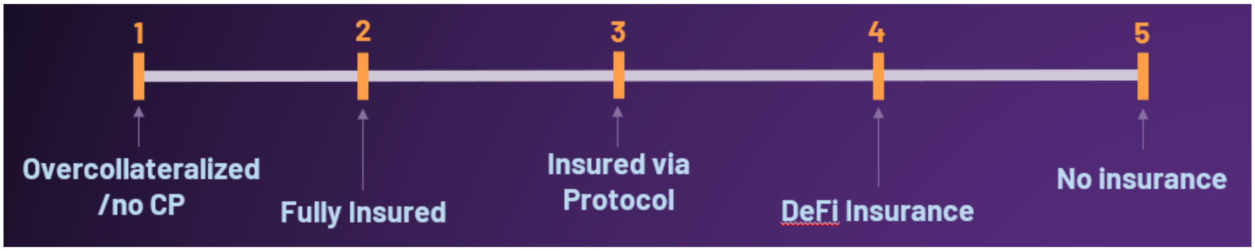

Figure 2. Counterparty default severity scorecard.

Mitigation

Unfortunately, there are little to no ways to mitigate counterparty risk in the DeFi space other than plain avoidance. DeFi insurance may be considered some small form of mitigation, but can only provide relatively small covers. Unless the protocol itself has made a deal with an insurance provider as stated previously, it is next to impossible as of now to get insurance coverage on a DeFi loan – institutions still see the space as simply too risky. Until either DeFi insurance grows or centralized insurance becomes more comfortable with DeFi, the opportunities available to mitigate counterparty risk in the space will remain few and far between.

Looking Forward

A major differentiator between DeFi and TradFi loans is how the protocol itself is not regulated as a financial intermediary. If a loan is defaulted on, there is no precedent of what/who to sue, and as of now is impossible. In traditional finance, the counterparty is cut and dry and can be legally pursued to fulfill its financial obligations. The only way DeFi could reach this point would be through further regulation, however this is a delicate balance, as beginning to regulate smart contracts as financial intermediaries would stifle innovation in the space and inevitably centralize it. The way the CFTC/SEC begins to approach DeFi regulations will be a turning point for the space in the coming years – whether by expanding adoption by improving the safety of investments, or becoming choke point at which innovation is halted.

KYC/AML Risk

Definition

KYC/AML risk in DeFi will be kept essentially the same as it would for traditional finance. Due diligence must be done on any party borrowing from Genesis else the firm risks fines for lending to bad actors. However, there is an important distinction between the final landing spot of the money and who Genesis itself is facing. For example, in a traditional Compound pool, anyone may borrow directly from this pool in an entirely permissionless manner, therefore directly lending into this pool would put Genesis at great KYC/AML risk as no due diligence can be done and the firm is directly facing the borrowers. Compound Treasury obscures this and allows Genesis to lend into the protocol as the firm is only directly facing Compound Treasury itself, allowing proper due diligence to be done.

Quantification

The best way to define KYC/AML risk is to define the level at which the due diligence is being done, and how much that party can be trusted with doing the job properly. These are broken-down into 5 main segments: no counter-party (therefore no KYC/AML diligence must be done), Genesis due diligence, protocol-level due diligence, token-level due diligence, and fully permissionless. As will be explained in further detail, it is important to remember that these are generalizations, and this model will have to inevitably be twisted and changed to fit with the nuances in this new space.

Starting with the riskiest is a fully permissionless protocol, such as Aave or Compound. Participants in these protocols have to undergo absolutely no checks before borrowing or lending money – aside from whether or not they meet funding requirements. Not only is no due diligence done, as of now there is no possible way for due diligence to be done if anyone wanted. The wallets remain pseudonymous, so while on-chain identity may be pinpointed, it is impossible to check the person behind the address, and for these reasons a fully permissionless protocol clearly presents the highest KYC/AML risk.

The next two levels where due diligence may take place are at the protocol-level and at the token-level, both of which are largely theoretical as of now. Token-level (or blockchain level) means that anyone wanting to get tokens native to a blockchain – such as ETH on Ethereum – would have to be KYC/AML checked first. This ensures that not just certain participants in certain protocols, but any active wallet on the chain is deemed whitelisted. Possible ways to achieve this will be looked into further in the Looking Forward section, but what is important for quantifying risk is that at the time of this report token-level due diligence is much much looser than protocol-level due diligence and is therefore considered a higher risk to KYC/AML of Genesis.

Protocol-level due diligence has already been experimented with and done successfully by applications such as Maple and TrueFi in order to offer under-collateralized loans. Though, as is the case with Maple, Genesis may still need to rely on inhouse checks, it is safe to assume that these platforms have much more fleshed out diligent programs than any known token ecosystems do as of now. Of course, as the industry shifts over time many blockchains may very well develop KYC/AML checks that are more robust than any protocols, but for now many of these protocols have much larger access to capital as well as strategic partners, allowing them to run due diligence and credit checks more effectively. Despite this, these protocols are simply not capable of running institutional-level KYC/AML checks as of now, and Genesis must still run their own checks to ensure fines are avoided. For all these reasons, anything short of in house diligence checks on DeFi borrowers should be avoided for the time being until protocols or ecosystems achieve institutional grade diligence systems that can be fully trusted to run independently of Genesis. All these findings are summed up in the simple risk scorecard below.

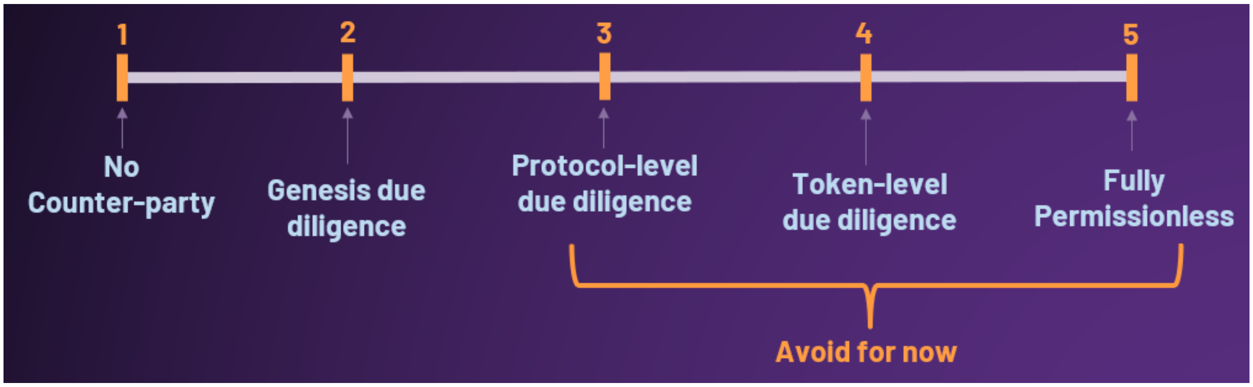

Figure 3. KYC/AML risk scorecard

Mitigation

The best way to mitigate KYC/AML risks is to run inhouse diligence checks, as is done with Maple and will likely continue to be done for participation in any such lending protocols for the near future. Unfortunately, for the time being, this along with careful selection of protocols/borrowers seems to be the only way to mitigate these risks. Due diligence has simply not been effectively integrated into DeFi yet.

Looking Forward

KYC/AML protocols and integrations with DeFi are slowly beginning to gain traction in the space. As touched on before, these may be grouped into either protocol level or token/ecosystem level checks. Protocol level checks are the most intuitive as they closely mimic the current banking system, where checks only need to be done when a transaction is to be processed or deal done. As such, they have been able to quickly acquire market share in the space. Despite this, ecosystem-level diligence shows much greater promise as a novel solution to create greater efficiencies for the financial system. The best examples of this are Avalanche subnets or permissioned Ethereum layer 2's. Though neither have been implemented yet for this specific use case, they both have the potential to create side-chains unique to companies or even entire industries, where wallets must be KYC checked before being whitelisted on the chain. Leveraging this, localized financial ecosystems could be created where all addresses are whitelisted and can participate freely in any DeFi protocol built on it. Ideally this could extend to create for example one chain exclusively used by institutional banks and their customers, removing the need for each institution to do their own due diligence separately, saving time and money and promoting interoperability of the financial system.

One more and even more theoretical possible solution to the KYC/AML problem in DeFi is the potential of so called ‘soul bound-tokens’ – or more simply put non-transferable NFTs – to serve as credentials. Once earned an held by an address for something such as a KYC check, an institution could simply check the address to ensure the credential is valid before interacting with them to ensure that the wallet holder is not a bad actor. As the space continues to develop inevitably these and more creative solutions will continue to be fleshed out. There is much to look forward to in regard to KYC/AML improvements in DeFi.

Operational Risk

Definition

Operational risks are an issue entirely unique to DeFi, and therefore will be investigated in greater detail in this report. These will encompass a fairly large swath of issues that can arise when interacting with DeFi protocols, including but not limited to user operational error, smart contract exploits, front-end attacks, and transaction flow exploits. Essentially, these are semi-loosely defined as the innate risks involved with interacting with and trusting smart contracts on the blockchain.

Quantification

Endeavoring to quantify the operational risks in DeFi is far too complicated to rely on number lines as done with counterparty and KYC/AML risks. The risks are unique to each transaction taken, and arise the second a private key/password is used to access a wallet. For the purposes of this report, it will be assumed that any interaction with a smart contract adds risk, while interactions with certain protocols such as DEXs and bridges exponentiates this risk. The only way this risk is reduced is in the case of audits by credible companies – though this does not fully eliminate operational risk. From this starting point, tit is attempted to assign any and all DeFi interactions an operational risk score of 1-10 by adding/subtracting risk based on the operations undergone. Note that the scoring begins at 1 as it is simply impossible to have 0 risk when any movement of cryptocurrency is occurring. The designated risk score affect for each these interactions has been chosen deliberately to most accurately weigh overall risk, though bear in mind that they will have to be changed along with the ecosystem as it moves forward, and is only a best estimate to simplify risk assessment.

Risk Addition

Beginning with how risk is added, the baseline smart contract operation will add +1 to the risk score. This includes signing and transactions themselves, as any of these exposes a wallet to risk namely in the form of front-end attacks. Front-end attacks occur when a harmful interaction is disguised as a benign one and is largely done through phishing schemes. A wallet user may believe they are signing a transaction to allow their wallet to interact DEX, when in reality they are allowing a bad actor access to drain funds from their wallet. This risk may seem obvious though it must be taken seriously – BadgerDAO for example was recently hacked for $120 million through a simple front-end attack.[5]

This guide may be followed for general smart contracts and protocols, though there are two special cases addressed in this report – DEXs and cross-chain bridges. Note cross-chain bridges are specified, as bridges across Ethereum layer 2s for example are still secured by the Ethereum network and therefore do not pose a greater security risk. These protocols incur additional risk upon initial interaction as they expose users to unique and more dangerous risks than a general smart contract interaction. DEXs add +4 to the risk score upon interaction and cross-chain bridges add +6, while each additional interaction with one of these protocols will only add +1 as the risk inherit to the protocol has already been factored in. These scores are chosen relative to the effect of audits on risk score which will later be explained.

DEX Added Risk

The additional risk of interacting with DEXs is primarily due to sandwich bots and front-running bots. These are attacks leveraging the order of transactions on the blockchain to benefit the attacker generally at the cost to the user. Sandwich bots function by detecting a large transaction (in the Ethereum mem pool for example) being processed on a DEX and will order transaction flow such that they buy the token first, the large transaction executes driving up the price, and they sell immediately after words. This results in them making a small profit on the change in price caused by the large purchase, but more importantly causes the large purchase to be processed at a worse price due to the sandwich bot's initial transaction. This and many other exploits fall under MEV (miner/maximum extractable value) attacks, where transaction orders are manipulated and rearranged to benefit the block miner, often at the expense of users.

For these reasons, any first interaction with a DEX will add 4 to the risk score for a protocol operation. This is done such that even if an A rated audit has been done on the firm subtracting 3 from the score (explained further below), there is still 1 point of risk added purely for interacting with the DEX.

Bridge Added Risk

Cross-chain bridges are a very nascent solution to the problem of chain interoperability, and as such continue to face issues with exploits draining their funds. In order to bridge to another chain, these protocols act as sort of banks, holding onto coins in their smart contracts until redeemed when users bridge again, leaving the tokens within as sitting ducks for hackers.

At the time of this write up, the most recent exploit was just 5 days ago when Harmony's cross-chain bridge was drained of $100 million.[6] As such, any interaction with a cross-chain bridge immediately adds 6 to the operational risk score – even if an A rated auditor has approved the bridge's smart contracts, the usage of it alone shall ad 3 to the risk score.

Risk Subtraction

The only way to reduce the operational risk score of interacting with a protocol is to confirm the efficacy of its auditors if there are any. Obviously, if there have been no audits done, the risk score is not reduced. Auditors were researched and received grades that value the benefit of there audit and in turn how much the audit affects the operational risk score. An A rated audit reduces the risk score by a maximum of 3, B by 2, and C by 1. Note that the operational risk score can never dip below 1, which is why it is stated that these are the max reductions possible. The auditors were graded based on 2 factors: the number of audits they have done, and the number of appearances on the 'rekt' leaderboard.[7]

Mitigation

Test transactions on testnets

FlashBots

Institutional wallets

Looking Forward

Conclusion

Bibliography

1 https://www.occ.treas.gov/topics/supervision-and-examination/capital-markets/financial-markets/counterparty-risk/index-counterparty-risk.html#:~:text=Counterparty%20risk%20is%20the%20probability,default%20on%20the%20contractual%20obligations.

2 https://www.nasa.gov/sites/default/files/atoms/files/s3001_guidelines_for_risk_management_-_ver_g_-_10-25-2017.pdf

3 https://app.nexusmutual.io/cover

4 https://maplefinance.gitbook.io/maple/protocol/pool-cover

5 https://www.theblock.co/post/126072/defi-protocol-badgerdao-exploited-for-120-million-in-front-end-attack

6 https://thepaypers.com/digital-identity-security-online-fraud/harmonys-cross-chain-bridge-exploited-for-usd-100-mln--1257164

7 https://rekt.news/leaderboard/