Chaos Labs - Risk & Simulation Platform Proposal

[

AAVE <> Chaos Labs

1280×640 37.7 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/1/17da70bb04976c3fcb549739ec35612721882705.jpeg)

Summary

Chaos Labs is proposing to onboard the AAVE core team and the community into its risk and simulation platform to better test new protocol upgrades, parameters, and the GHO stablecoin in various market structures and scenarios. This platform will include ways to help the community onboard new collateral types and assets and bespoke protocol research with publicly available analysis and results.

Who is Chaos Labs?

Company background

Chaos Labs is a software company building a unified simulation platform that allows teams to test protocols efficiently while understanding how they will react to adversarial market environments. The backbone of our technology is a cloud-based, agent- and scenario-based simulation engine that allows users to create specific market environments to test new features & assets to understand risk parameters better. Our team comprises top engineers from companies such as Apple, Facebook, Instagram, Amazon, Microsoft, Google, and more with years of experience in infrastructure, security, and platform “chaos” testing.

The Chaos Labs simulation platform and environment is built to be as close to mainnet as possible. Each simulation run forks from a specified block height (default block height is the most recent) so that your inputs include up-to-date account balances and the latest smart contracts and code deployed across DeFi. While testing volatile environments, it is imperative to look at your protocol holistically. The Chaos Simulation platform helps understand how external factors (cascading liquidations, oracle failure, gas fees, liquidity crises, etc.) will impact a protocol in various situations.

Company values

Our mission is to secure and optimize

protocols through verifiable agent- and scenario-based simulations

.

- The best simulation testing is as close to production as possible.

The Chaos Labs’ cloud platform will spin up an EVM-compatible forked environment for every simulation. Since all simulations are executed on a fork, all code deployed to Chaos can immediately be transferred on-chain and/or used for production. An additional benefit is that the fork gives us a snapshot of mainnet out-of-the-box. This allows us to run simulations with minimal assumptions and deviations from mainnet conditions.

- Trust, but verify

. We can build a test environment and convince you that it is correct, but that trust only goes so far. Our tooling allows core team members (i.e., simulation creators) and anyone they permit (up to the entire community) to dig into the test environment and push back against assumptions, agent creation, scenario environments, optimization trade-offs, and more. Open source agents and scenarios allow the community to understand precisely how answers came to be determined. We have built a suite of tools and libraries for rich data visualizations, auto-generated analytics reports, and internal block explorer so that users can verify the simulation results down to each block and transaction.

- Community engagement

. We know that we can build the best tools to help test and optimize DeFi protocols, but we can only scale with lasting change if the relevant core team and community members are on board and actively engaged. Each protocol differs from the code to community risk tolerance, and we do not want to be the only voice translating that into proposed changes. We are a software company building tools to understand and mitigate DeFi protocols’ risks, ideally powered by the communities who care most about them. Thus, we want to engage the said community in each proposal, from simulation creation to testing review to proposed change enforcement.

Why economic security and testing are important & how Chaos protects against it

Security audits and penetration testing are crucial parts of the security stack, but they alone are not all-encompassing to limit the surface areas of vulnerability. Their primary function is to ensure that your code does what you want your code to do and that there are no major flaws, assumptions, or errors in what you wrote as you wrote it. We view Economic security as the next piece of cheese in the security stack (ref: Swiss Cheese Model), building upon the correctness of their reviews and manipulating the environment around the protocol to ensure the intended behavior plays out as intended in different scenarios ranging from business as usual to black swan events.

[

swiss_cheese_security_model

1790×896 241 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/c/c84108ed91045e44fff8aa8861c409a727c80062.jpeg)

Since the rise of "DeFi summer," we've seen nefarious actors managing to manipulate core protocols in increasingly creative manners. They are no longer looking for flaws in code, but they are manipulating the market around the target protocol to gain entrance and exploit it. This roundabout attack vector heightens the need for complex parameter setting procedures; knowing how different values for certain assets react in different environments will allow for more confident governance and usage of the protocol.

[

Exploit flows

2000×731 85.6 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/d/d4922739afd633c8f6f7761bc175398b6547d693.jpeg)

Proposal

We propose to build custom tooling for the Aave team and community to understand the protocol, including:

- testing of major upgrades
- parameter setting
- new asset listing
- comprehensive VaR calculation
- GHO launch
- and more.

Over this engagement, we will deliver a suite of new products for team use and community analysis to open the tooling up to a broader community group to run it in the future. As we embark on product development with Aave, we anticipate managing simulation creation, feedback integration, and reporting until the platform is ready for community control. In the future, we can create a new AIP proposal creating an Aave-dedicated simulation creation and analytics team (similar to the Risk DAO proposal), which can provide another voice in risk-mitigation conversations powered by data.

To continue to enhance risk coverage of the Aave protocol and transparency to the community, we'd propose tooling to cover a few major areas:

1. Risk Parameter setting
2. Asset listing
3. GHO stablecoin launch
4. E-Mode and Borrowing Power for similar assets
5. Isolation Mode and Debt Ceiling for new assets
6. v3 Portals

Simulation engine platform & unified infrastructure

From a risk and infrastructure standpoint, we see a number of tools that need to be developed and maintained for Aave to increase its security coverage on top of that provided by teams like BGD, Certora, Gauntlet, & Sigma Prime. The current risk coverage covers Aave v2 (well) and asset onboarding (less so) but can be enhanced to analyze and optimize a number of areas with specific simulation and dashboard tooling to be delivered to either the community or the relevant Aave team.

Chaos Labs has developed a novel, cloud-based, agent- and scenario-based simulation platform. Our product is built on the ethos that a valuable testing environment is as close to a production environment as possible. Therefore, we utilize a hybrid approach of on-chain and off-chain simulations.

On-Chain Simulations

On-Chain Simulations fork the blockchain from a specified block height and deploy a catalog of agents, scenarios, and observations within the Chaos Cloud environment.

Agents emulate user behavior and allow us to emulate different risk behavior for protocol users. The Chaos Scenario Catalog lets us control macro variables and conditions such as gas fees, DEX and protocol liquidity, oracle return values, Black Thursday Level market events, and more. Observers allow for deep protocol analysis and better simulation insights.

Through this robust software, users can control and test a host of different factors that can impact protocol security and user funds, including

- Oracle prices
- Gas fees
- Account balances & liquidation prices
- Transaction latency
- Flash loans

Economic security testing and simulations via the Chaos Labs platform allow you to test your protocol in different scenarios and custom environments to understand where your risks lie before a malicious actor can exploit them.

In this manner, we will integrate directly with the Aave protocol and provide transparent simulation insights.

Off-Chain Simulations

Chaos Labs also deploys off-chain simulations, utilizing machine learning and statistical models that ingest data sets from various off-chain data sources to test economic structures prior to any solidity or on-chain code being written. As part of the off-chain simulations, Chaos Labs will run a massive number of Monte Carlo simulations to assess the protocol's VaR per Market (Chain) and across markets.

A combination of On-Chain and Off-Chain simulations allows us to control and test a host of different factors that can impact protocol security and user funds including:

- Oracle behavior
- Gas fees
- Account balances & liquidation prices
- Transaction latency
- Flash loans
- volatile markets impact on protocol reserves
- asset correlations and liquidations
- drastic price drops impact on liquidations and liquidity
- high gas fees impact the efficiency of the liquidation process
- new asset borrow demand, revenue, and liquidation processes

Product screenshots

[

car

2000×1113 143 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/c/c4fef22c76d3c9e1df44807b1c9b5a5c87a16e6b.jpeg)

[

car_pt_2

2000×1115 170 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/9/9a6d9486d6fe5aa18b8b095f7d186003827a13de.jpeg)

[

stETHDepegConfig

2000×1178 132 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/b/bc2ef858e55c65faeff84bdee129b19d98269034.jpeg)

[

aave_metrics_observables

1920×1475 114 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/5/57cfc1dd1f9c6787d38a659f64e7adcab5d61a07.jpeg)

[

chaos_block_explorer

1920×1445 131 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/d/d11d94a8c36671d2ebce1090567553f174c81191.jpeg)

[

deltoid

1388×936 73.3 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/a/a5303349528a9f52219d89e323445cbaf378a70d.jpeg)

The underlying tooling will have two main user access types:

Group 1 - Create/write

: This access will be available for the relevant core teams of Aave (protocol engineering, Aave Risk, BGD, etc.) so that they can create agents, scenarios, simulations, and interact with the simulation engine via all available methods (hosted interface, CI, API, etc.). As the Aave simulation integration is developed, they will have access to creating these test environments to suit their needs and analysis. There will be no limit on the number of users that have access, but they must be whitelisted by one of these groups.

The simulations they run and their related outputs will be private by default and opened up to the community once related to a public discussion, parameter change, or otherwise related governance vote.

Group 2- Read-only

: The community will have a dedicated read-only access interface to audit and analyze the work done by Group 1 as well as Aave-specific dashboards to facilitate community decision-making. This access will not be gated and will allow for full transparency to the community in how risk decisions are being made, especially regarding optimization trade-offs in different scenarios thus pushing towards more data-driven decision-making within the community on robust analytical toolsets.

There are two reasons why we cannot open “create/write

” access to the whole community:

1. Black Hats

: This tool is meant to understand how the protocol, both features in development and those already deployed to mainnet, react to volatile and adversarial market conditions. If someone unrelated to the Aave community could access this platform for their own usage or peer into private failed tests, they would be able to subsequently exploit them prior to the developers and community correcting them.

1. Compute usage

: These simulations will cover a multitude of transactions across various wallets and protocols over the duration of thousands of blocks. Running and maintaining this is not easy or inexpensive, thus we must make sure we have the appropriate guardrails in place to minimize its abuse over the duration of the engagement and, thus, minimize the cost to the community.

We will be public with product development, testing, and roadmaps to maximize transparency with the community and maintain alignment on the most pressing needs.

Protocol coverage

Risk and testing is a broad-ranging category. We will not cover security auditing or formal verification as those are covered elsewhere by protocol vendors, but we plan to maintain a flexible mandate to focus on what Aave deems most pressing in terms of feature deployment, risk analysis, and simulation development.

We will break the coverage into two distinct areas:

- Core Aave risk product and simulation development needs
- GHO launch and maintenance product and simulation development needs

With that, we’ve adapted BGD’s task framework to outline where we think the focus should be as we see it today.

On the following list, we present the ones that we believe Chaos Labs can help with. We divide them into these 2 classes:

- SURE

. Chaos Labs will tackle the task, and uncertainties apart (community not approving, model not really defined, etc), will compromise to complete it.

- PENDING PRIORITIZATION

. Chaos Labs will begin work on the task as it is prioritized by either one of the Core teams or the community at large, pending capacity.

- BEST EFFORT

. Chaos Labs will participate in the task, potentially completing it too, but usually, the scope is too broad or undefined at the moment to compromise to a level of completion at the moment.

Task

Type

Coverage Area

Notes

AAVE v3 Collateral factors

Sure

Parameters

Use simulations to provide community tooling and recommendations for parameter optimization. Users will have the ability to interact with each simulation on a block-by-block level to understand transaction differences and outcomes.

Aave v3 Risk Parameters

Sure

Parameters

Use simulations to provide community tooling and recommendations for parameter optimization. Users will have the ability to interact with each simulation on a block-by-block level to understand transaction differences and outcomes.

Asset Listing Portal

Sure

New Assets

More information is below.

Asset Listing Risk Assessment

Sure

New Assets

More information is below.

Borrow and Mint Cap Recommendations

Sure

Parameters

More information is below.

Community Agent Access

Sure

CL Products

Allow the Aave community to access agent modules for feedback and discussion around the most relevant user types to better test protocol.

Community simulation access

Sure

CL Products

Allow the Aave community to access simulation results and observable dashboards to further discussion around optimal protocol changes

Open-source agent code base

Sure

CL Products

Community engagement via public open-source agents

Aave Portal features

Pending Prioritization

AAVE Features

Determining the appropriate mint cap based on bridge throughput and native DEX liquidity + relevant risk factors.

Aave Seatbelt Enhancements

Pending Prioritization

AAVE Features

Enhance the existing governance tool with forward-looking simulations for impact and accuracy

CI Access

Pending Prioritization

AAVE Features

Integrate automated simulations as part of the code push process to detect regressions introduced.

Efficiency mode optimization

Pending Prioritization

Parameters

Simulate and optimize E-mode modules for the protocol.

Interest Rate Modeling

Pending Prioritization

Parameters

Iterate on interest rate curves in different market environments to measure impact and efficiency.

Isolation Mode

Pending Prioritization

Parameters

Simulate and optimize Isolation Mode

modules for the protocol.

Other protocol markets (Avalanche, Polygon, etc.)

Pending Prioritization

Parameters

Explore duplication of simulation engine and parameter setting simulations to other EVM chains for protocol optimization.

Aave v1 & v2 Risk factors

Best Efforts

Parameters

Duplicate v3 simulation tooling for older versions as is needed

Bridge risk analysis

Best Efforts

AAVE Features

Research and simulate bridge interactions to understand and report on potential risk factors for protocol consideration. Determine impact on user funds for ongoing monitoring.

Credit limit setting

Best Efforts

Parameters

Use simulations to provide community tooling for parameter optimization. Users will have the ability to interact with each simulation on a block-by-block level to understand transaction differences and outcomes.

Oracle Failure

Best Efforts

AAVE Features

Simulate and test the impact of oracle failure on the protocol and liquidations to ensure appropriate measures are in place to protect user funds.

Asset Listing Portal

[

alp

1920×1212 100 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/d/d0ce3cb368317961d073860c4fd203bbf5917989.jpeg)

One of the key focuses of this engagement would be building an Asset Listing Portal to help streamline new collateral onboarding to the Aave protocol similar to what we have built for dYdX, found here. This tool will help streamline community decision-making by automating the collection and analysis of key markets data around assets such as:

- Market beta & volatility
- Exchange liquidity and slippage
- Market cap
- On-chain activity
- Third-party lending integrations (i.e. compound, maker, etc.)
- Security & demand scoring
- Revenue estimation
- Initial parameter recommendations

This tool will help streamline the addition of new assets to the Aave platform, thus increasing platform fees to the treasury and token suppliers while balancing the overall protocol health.

GHO Simulations

Launching a stablecoin is hard; maintaining one is 10x so. The path to stability and scale for decentralized stablecoins is littered with best efforts, failed experiments (UST, IRON), and only a few true successes. Most decentralized stablecoins fail because of the depth and breadth of the unknown-unknowns: how do their stability mechanics react to uncertain and volatile environments? Does each new change and development expand the surface area of that potential vulnerability?

The thread announcing GHO is full of questions that could (and should) be answered with in-depth simulations to understand the mechanical reaction of the GHO implementation.

As a part of this engagement, our focus will not only be on the core Aave lending protocol, but also on the security and expansion of the GHO stablecoin. Potential simulations and tooling to be built can be found below.

Task

Type

Coverage Area

Notes

Depletion of liquidity

Sure

Simulations

What is the impact on stability if X% of liquidity is withdrawn from a given protocol (Aave, DEXs, etc.)? This is how UST initial began to break

GHO native interest rate modeling

Sure

Simulations

Iterate on interest rate curves in different market environments to measure impact and efficiency.

Collateral diversity

Sure

Simulations

New asset listing, parameter setting, and risk scoring

Facilitator diligence

Pending Prioritization

Simulations

Simulate the impact and volatility of different facilitators to help determine optimal bucket limits for initial GHO supply.

Liquidity incentive optimization

Pending Prioritization

Simulations

How to best spend funds to most efficiently create deep liquidity pools?

Staking module exploit

Best Efforts

Simulations

What would happen if Aave gets exploited in the staking module? If GHO is backed by stkAAVE would the token lose its backing and peg?

GHO oracle set up and manipulation

Best Efforts

Simulations

Testing oracle configuration and potential failures

Stablecoin arbitrage

Best Efforts

Simulations

How do lower borrowing costs on stablecoins impact protocol-level risks, especially around recursive borrowing? What are the key parameters to monitor to protect against this scenario?

GHO supply cap

Best Efforts

Simulations

Monitoring market exposure of GHO as it finds its footing and doesn’t become too large too quickly. What are the appropriate levels/thresholds based on liquidity and other factors?

stAAVE mint discount

Best Efforts

Simulations

Simulate user interactions and ROIs for stAAVE holders to determine the discount rate with the highest value-add to the protocol

For all of the proposed tooling, we will publish technical walk-throughs and repo links to any relevant open-sourced tooling (such as agent and scenario creation) for public review and feedback. We’ll open as many of the interfaces to the community as is applicable and appropriate shortly after deployment.

Community engagement

Community Risk Calls

As part of our commitment and efforts towards community engagement to further drive protocol security, Chaos Labs would organize a monthly risk call for the AAVE community alongside all other protocol security contributors. This call would be focused on any new major protocol or market developments such as:

- New risk tooling and analyses
- Protocol launches and technical proposals (GHO, v3, etc.)
- Asset listing proposals
- The broader market environment
- and anything else the community deems important and relevant for discussion

We would schedule said calls for a recurring hour-long block on a monthly basis in addition to any ad-hoc community risk calls when deemed necessary. A recording and summary of these calls will be provided.

Ongoing updates

Aave's dedicated relationship manager will be an active participant in organizing the risk conversation and updating the community in the forums. We will commit to a monthly update post focusing on both works complete and ongoing as determined by the community. We will also host monthly office hours to be available for community Q&A.

Proposal services coverage

- Unlimited seats to the Chaos Labs simulation platform for white-listed users
- Simulation capacity up to 50k monthly limit
- Dedicated headcount from Chaos Labs supporting Aave, including:
- One relationship manager primarily dedicated to Aave.
- Support of one PM covering Aave's needs and proactively providing support for new simulations and dashboards
- Two engineers and two data scientists/analysts building simulations and risk-related dashboards and reports.
- The balance of the Chaos Labs team will be available on an as-needed basis to support Aave with ad-hoc requests at the time of high concern.

- One relationship manager primarily dedicated to Aave.
- Support of one PM covering Aave's needs and proactively providing support for new simulations and dashboards
- Two engineers and two data scientists/analysts building simulations and risk-related dashboards and reports.
- The balance of the Chaos Labs team will be available on an as-needed basis to support Aave with ad-hoc requests at the time of high concern.

- Chaos Labs will build or facilitate the development of all relevant agents, scenarios, and simulations for the Aave core team and community.

Long-term relationship

As has been stated above, we are a software company at our core. We're building a robust platform which empowers communities to develop, test, and risk-manage their protocols at a more sophisticated level without needing to rely on any single outside third party. While our focus is to use this engagement period on product development for the AAVE community, our hope is to eventually onboard a consortium of community members to create the relevant testing environments and risk evaluations for the Aave protocol on top of the Chaos Labs platform. We promise to be as transparent as possible during the process while it is centrally managed to build towards this more open and decentralized future.

As a first step toward this future, we anticipate onboarding a small subset of community members by the end of this engagement to be paid bounties for the creation of Aave-specific agents and scenarios within the Chaos Labs environment. We will provide more updates on this as it is closer to launch.

Measures of Success

Security and testing is a tough realm to measure appropriately. The successful completion of the AAVE protocol's objectives will be measured against KPIs that will be derived from the specific objectives agreed upon between AAVE and Chaos Labs. On top of those, We will also look to measure things such as:

- Product deliverables & task completion

- Usage & users onboarded into the simulation and testing environment
- Community and core team member NPS of our relationship
- Participation in the GHO stablecoin launch
- Communication and transparency to the community on work done and product access

Previous AAVE Work

- AAVE v3 Risk Application
- stETH Depeg Simulation and Analysis
- Diving Deep into AAVE v3 Subgraph Data Validity
- AAVE v3 Risk Bot

Pricing

- 12-month engagement term
- $3,000,000 flat engagement fee
- $750,000 paid upfront in stablecoins
- $750,000 paid in stablecoins streamed linearly over the course of the contract
- $1,500,000 in AAVE tokens vested linearly over the course of the contract
- $750,000 paid upfront in stablecoins
- $750,000 paid in stablecoins streamed linearly over the course of the contract
- $1,500,000 in AAVE tokens vested linearly over the course of the contract
- $300,000 additional stablecoins for community agent and scenario creation
- This will be distributed at the signing of the engagement and all unused funds returned either to the DAO or to the Grants multisig a the end of the initial term if not renewed
- This will be distributed at the signing of the engagement and all unused funds returned either to the DAO or to the Grants multisig a the end of the initial term if not renewed

Next steps

We are eager to have a lively discussion with the community in the forum about our proposal and potential engagement. If the initial snapshot vote is successful, we will propose an initial product roadmap in prep for the on-chain vote.