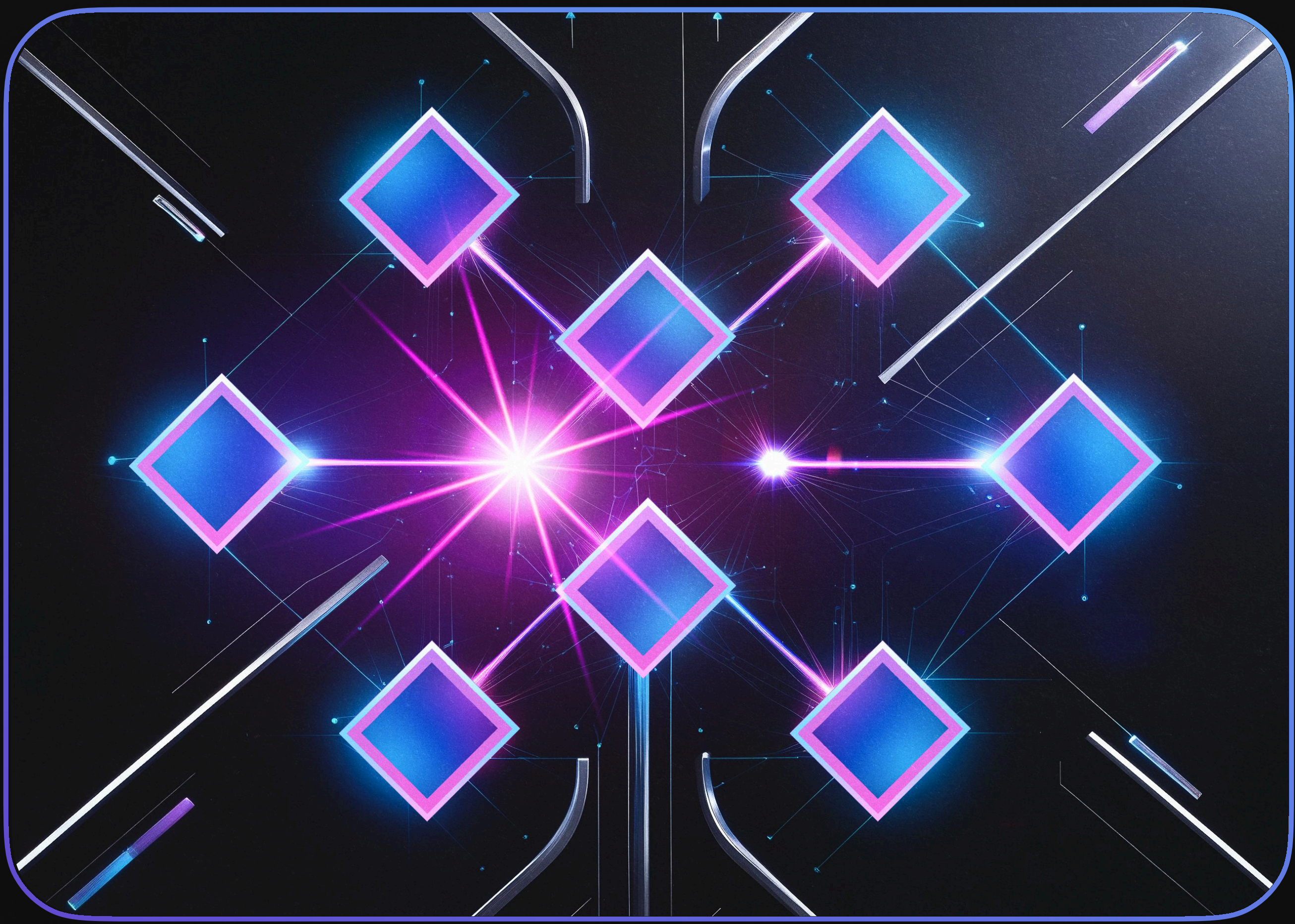
Collectif LABS × LIDO



LIDO DUAL GOVERNANCE

SIMULATION REPORT

2025

DISCLAIMER

This document is prepared for informational purposes only and does not constitute financial, legal, or investment advice. While every effort has been made to ensure the accuracy and reliability of the information, the authors and affiliated parties cannot be held responsible for any actions taken based on this report.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report presents findings from the Dual Governance (DG) simulation for Lido, assessing the system's resilience, efficiency, and optimization.

1

1 Executive summary

This report summarizes the evaluation of the Dual Governance (DG) mechanism for Lido protocol, using an Agent-Based Model (ABM) approach. The DG mechanism aims to enhance governance by involving stakers into decision-making, balancing the interests of LDO and stETH holders. Key innovations include the signalling escrow, dynamic user-extensible proposal timelock and the Rage Quit mechanism, which allow stakers to block unfavorable actions or safely exit the protocol.

The simulation framework by CollectifDAO models the behavior of stETH token holders, DG system states, dynamic timelocks, and thresholds, and assesses the resilience and parameter adequacy of the system. It simulates the life of DG, including the impact of governance proposals, staker reactions, and external factors on system performance. The findings confirm that DG provides a robust framework for governance, balancing inclusivity, security, and operational efficiency.

We conclude that the Lido DG design is both viable and robust in the scenarios tested, and highlight the following key results:

1. The 1% Veto Signalling threshold is validated to allow effective coordination of dissent, while posing significant challenges to long-term abuse
2. The 10% Rage Quit threshold is validated to enable reliable exit for stakers without asset impact, ensuring protection of capital and trust in the ecosystem
3. DG is tested to withstand most economically feasible attacks, although Rage Quit bottlenecks could impact governance under certain conditions and significant capital requirements
4. Long-term concentration of tokens among a small and inactive group of holders may challenge existing DG design by increasing the vulnerability to attacks

The study demonstrates that the DG design achieves its goals, with simulations highlighting key decision areas for potential parameter adjustments to maintain resilience under all conditions.

INTRODUCTION

2

2.1 Dual Governance Outline

The Dual Governance (DG) mechanism enhances Lido's protocol governance by involving stakers in decision making, balancing the interests of both LDO and stETH holders. It introduces two key innovations: **a dynamic user-extensible timelock** on DAO decisions and the **Rage Quit mechanism** for stakers, ensuring that they can block unfavorable governance actions or queue to exit the protocol without being affected by the proposal.

Purpose and Context

Lido's governance is currently driven by LDO holders through DAO voting, with an additional optimistic voting layer called Easy Tracks for routine adjustments. However, this structure lacks a direct voice for stETH holders, who represent a critical user base. DG addresses this by allowing stETH holders to veto proposals, signal dissent, and negotiate with the DAO, ensuring alignment between stakeholders and protecting the integrity of the protocol.

Key Simulated Components extracted from the detailed specification

1. **Governance States**
   DG operates as a state machine with distinct states:
   - **Normal:** DAO submits and executes proposals as usual.
   - **Veto Signalling:** Stakers lock assets in a signalling escrow to extend timelocks and block execution. Proposals cannot be executed. Has deactivation substrate, where DAO cannot submit and execute proposals but can vote on already submitted undecided proposals so they become decided.
   - **Veto Cooldown:** Provides resolution time after signalling. Proposals cannot be submitted.
   - **Rage Quit:** Allows stakers to exit governance while withdrawing their assets safely. Proposals cannot be executed.
2. **Dynamic Timelocks and Thresholds**
   Proposal execution depends on predetermined reaction windows and proposal delays/cancellations come from the amount of tokens staked in the signalling escrow.
3. **Signalling Escrow**
   stETH holders lock assets to signal dissent, influencing timelocks and governance transitions. Locked assets continue to earn rewards, maintaining user alignment with the protocol.
4. **Rage Quit Mechanism**
   For unresolved disputes, stETH holders can exit Lido Protocol by withdrawing assets through a dedicated process. This ensures dissenters are unaffected by new or pending decisions, protecting their stake in the protocol.

The simplified workflow of Dual Governance is as follows: Optional diagram

2.2 Goals of Dual-Governance System Optimization

The DG mechanism is designed to optimize the governance of Lido by achieving a balance between inclusivity, security, and operational efficiency. The goals of the DG system are outlined below, along with their relevance to simulations:

1. **Foot Voting Efficiency**
   DG improves "foot voting" by providing the Rage Quit mechanism that allows stakers to exit the protocol without being affected by new or pending decisions. This ensures that dissatisfied participants can leave without compromising their assets, thereby strengthening user trust
2. **Principal-Agent Problem (PAP) Diminishment**
   DG empowers stETH holders to challenge DAO decisions, reducing the risk of misaligned governance. Using the Veto Signalling mechanism and structured negotiation paths provided by DG, stakers can safeguard their interests and maintain trust in the protocol
3. **Security**
   The system is designed to minimize vulnerabilities and avoid new attack vectors or exploits. This includes safeguards against malicious agents attempting to manipulate the Veto Signalling or Rage Quit processes
4. **Stability**
   DG must integrate seamlessly with well-intentioned DAO operations, maintaining the efficiency of the decision-making without introducing excessive delays or complexity. This balance is essential to ensure that the protocol continues to operate effectively under normal conditions
5. **Future-Proofing**
   The system should remain resilient to changes in the distribution of token holders and balances or participation levels. It must accommodate passive participants and changing governance dynamics while ensuring that extreme scenarios do not destabilize the protocol

Balancing these goals is inherently challenging due to potential conflicts. For example, the Veto threshold must be low enough to allow for effective staker opposition in critical scenarios, but high enough to prevent abuse by a small number of malicious token holders.

Simulating such conflict cases is essential to understand how these goals interact and to identify appropriate parameter settings. By addressing these conflicts and testing parameters across scenarios, DG aims to create a governance system that is inclusive, secure, and resilient under a wide range of conditions. Details of the modelling and simulation objectives are provided in the next section.

2.3 Lido - CollectifDAO Modelling Objectives

CollectifDAO developed an agent-based model to test the core mechanisms of DG, assess its resilience and optimize its numerical parameters. The key goal is to identify potential bottlenecks and validate suitable configurations that ensure the system's functionality, security, and fairness in both normal and adversarial scenarios.

To achieve the goals of DG system optimization, the simulation explores the following questions:

1. **How can we test the resilience of DG?**
   The simulation evaluates the system's ability to handle adverse scenarios, including coordinated attacks and prolonged Veto Signalling loops
2. **Are the proposed parameters appropriate?**
   By testing thresholds, timelocks, and safety mechanisms, the model assesses whether the proposed values provide sufficient protection and functionality
3. **How sensitive is DG to parameter changes?**
   The simulation examines how variations in thresholds, reaction times, and agent distributions affect system performance and identifies the limits of its robustness

To address the above questions, the CollectifDAO simulation model focuses on the following DG components, including:

1. **General Architecture:** Thorough evaluation of all DG components and their assumptions for DG scope and agent behavior in the model
2. **Existing DG Parameters**
   a. **Timelock Adaptability:** Ensuring that stakers have adequate time to respond to proposals without introducing excessive delays that hinder DAO operations
   b. **Thresholds for Opposition:** Testing Veto Signalling and Rage Quit activation thresholds under diverse conditions to balance accessibility with protection against abuse
3. **Agent's Dynamics:** Modelling the behavior of stakers with varying reaction times and motivations to identify risks, optimize parameter settings, and enhance system resilience
4. **Edge Case Simulations:** Designing and simulating special scenarios, including attacks, bribing and other unlikely but potentially dangerous instances of governance interactions

This report summarizes the findings of these questions and the methodology used.

2.4 Modelling Approach

Agent-based modelling (ABM) simulation was developed to simulate the protocol's mechanisms, user behavior, and dynamic governance processes. The model leverages the strengths of ABM to emulate interactions between agents (stETH and LDO holders) and the system (governance mechanisms), incorporating both normal operations and adversarial conditions.

The simulation framework is structured around three core components:

1. **The System:** Represents the DG mechanisms, including proposal lifecycles, Veto Signalling and Rage Quit functionalities
2. **The Agents:** Models Lido governance participants (stETH holders, wstETH holders, and committee members), each acting independently based on their motivations and token balances
3. **The Environment:** Simulates external factors such as token distributions and predefined scenarios that reflect realistic governance challenges

The System is implemented in Python, allowing for rapid iteration and scenario testing. It includes:

Dynamic Timesteps	Parameter Flexibility	Monte Carlo Simulations
Captures the impact of governance proposals and staker reactions over time	Allows tuning of thresholds, timelocks, and agent behavior to evaluate the robustness of DG	Generates confidence intervals across multiple runs, providing statistical reliability of the results

Each Agent is modeled with unique parameters that affect their decision-making:

- **Wallet Type:** Includes private wallets, CEXs, smart contracts, and rogue agents
- **Token Holdings:** Tracks LDO, stETH, and wstETH balances, including locked and unlocked assets
- **Reaction Times:** Categorized as Quick, Normal, or Slow, influencing when actions (such as Veto Signalling) are triggered
- **Health Points (HP):** A dynamic metric that reflects each agent's willingness to stay/leave in the protocol. Reaching zero HP results in escrow lock and withdrawal

The Environment is organized into a set of configurable inputs that detail the simulation focus, test the sensitivity of each DG mechanism value, and identify the most suitable number.

Configurable Inputs:

2.4 Modelling Approach

Agent Parameters	Governance Parameters	Scenario Characteristics
Token distributions, reaction time, and HP values	Veto thresholds, timelock durations, and Rage Quit triggers	Attack targets, proposal types (positive, negative, no effect), and timelines

The model supports two broad scenario categories:

1. **Regular System Behavior:** Tests DG functionality under normal conditions with randomized proposals
2. **Irregular System Behavior:** Simulates attacks, bottlenecks, or market disruptions to identify vulnerabilities

Simulations and their associated analyses are documented in Python notebooks, which are available in the following GitHub repo (experiments/notebooks). For each simulation, the notebooks provide the following key outputs:

General Analytics	Scenario-Specific Insights	Monte Carlo Results
System states, locked assets, and token distributions over time	Agent behavior, threshold activations, and governance state transitions	Confidence intervals for thresholds, reaction times, and attack resistance

2.5 Key Findings

This simulation-based evaluation confirms that the Dual Governance system provides a robust framework for protocol governance that effectively balances inclusivity, security, and operational efficiency. The simulations reveal both strengths in resilience and efficiency under various conditions, as well as a few areas for attention where possible future changes in power balance and stETH distribution could critically affect the resilience of DG.

2.5 Key Findings

Performance Highlights

- **Proposed design achieves the goals of Dual Governance:**
  - The 1% Veto Signalling threshold allows for timely coordination of dissenting voices while protecting against abuse
  - The 10% Rage Quit mechanism effectively allows stakers to exit the protocol without asset impact, ensuring trust and inclusivity
- **DG can efficiently withstand pressure and continue operation:**
  - The system resists most economically viable attacks, including dilution and bribery
  - Rage Quit bottlenecks could impact governance, but require significant centralization or coordination of capital in the system, reducing the possibility and feasibility of most attacks

Results in Terms of DG Goals

1. **Foot Voting Efficiency**
   The Rage Quit mechanism ensures that stakers can exit the protocol without compromising their assets. Simulation results demonstrate that the 10% Rage Quit threshold is sufficient for timely exits in most scenarios, even under slower reaction times (4.1, Cluster A)
2. **Principal-Agent Problem (PAP) Diminishment**
   The Veto Signalling mechanism allows stETH holders to effectively challenge DAO decisions. Simulations of attacks, such as fund stealing proposals, show that the 1% Veto Signalling threshold successfully protects against most economically feasible attacks, given sufficient actor engagement (4.1, Cluster B)
3. **Security**
   DG demonstrates strong resistance to all tested malicious vectors, including dilution and bribery attacks (4.1, Cluster C)
4. **Stability**
   The system effectively maintains operational stability under normal conditions, but is susceptible to prolonged bottlenecks due to Rage Quit exploitation. Growing stETH pool combined with fixed withdrawal throughput from the ETH ecosystem could potentially magnify these effects, requiring dynamic throughput adjustments or alternative safeguards to ensure governance continuity (4.1, Cluster D)
5. **Future-Proofing**
   Sensitivity analyses confirm that DG remains resilient under moderate changes in token distributions and community reaction time assumptions. The sensitivity analysis highlights the need for ongoing monitoring and the ability to adjust DG parameters in the major stETH concentration scenarios (4.2.2, Sensitivity Analysis)

2.5 Key Findings

Are the parameters proposed by the Lido team adequate?

The current parameters, including Veto Signalling and Rage Quit thresholds, are largely adequate. They strike a balance between inclusivity and operational efficiency, ensuring robust governance under most conditions. However, certain scenarios, such as extended Rage Quit loops and bribery under centralized distributions, reveal areas where long-term DG parameter upgradeability may be needed.

How sensitive is DG to parameter changes?

Dual Governance shows moderate sensitivity to variations in its parameters, with performance remaining robust under most conditions but showing vulnerabilities at extreme values. Key findings from the simulations include:

Thresholds: The Veto Signalling threshold is well calibrated, allowing for a timely reaction to stakeholder group attacks while protecting against abuse. For example, increasing the threshold beyond 1.5% significantly reduces coordination success rates, particularly for smaller stakeholders. Similarly, Rage Quit thresholds above 10% could make governance unresponsive in some scenarios

Reaction Times: Slow (>40 days reaction time) or abstaining DG participants could potentially hinder DG performance in scenarios requiring rapid transitions from Veto Signalling to Rage Quit states. Active participants (<5 days reaction time) play a key role in DG resilience, highlighting the importance of activating the core community with sufficient voting power and fair representation of stakeholders across the board

Token Distribution: Significant centralization of stETH distribution increases governance vulnerabilities, though this is driven by factors that are unpredictable and outside Lido’s control

In conclusion, the DG system is well designed to meet its core goals. Continued monitoring of token holder engagement, parameter sensitivity, and evolving governance dynamics will ensure the system’s long-term effectiveness and resilience.

METHODOLOGY

3

3.1 Model Overview

As previously discussed in Chapter 2.4, the simulation model leverages Agent-Based Modelling to assess the performance, resilience, and optimization of DG mechanisms. It provides a robust framework for analyzing governance scenarios under normal and adversarial conditions. The detailed model description and Python source code are available here.

The core model architecture can be represented by three equally important components, each with unique features that allow different questions to be posed to the overall system.

1. **System Representation** of DG as a whole
   - The DG system is modeled as a dynamic state machine encompassing governance processes (proposal lifecycles, Veto Signalling, Rage Quit) and their interactions with user actions
2. **Agent Representation** of Lido governance participants
   - stETH, wstETH, and LDO holders
   - Committee members and rogue agents. Agents have parameters such as token balances, reaction times, and decision-making dynamics, allowing for diverse and realistic behaviors
3. **Environment Configuration** of various parameter inputs for DG testing
   - Scenario input state, including proposal, attack vectors, timelines and impacts
   - Top 1,900+ wallet token distributions
   - Safety mechanisms of DG, including dynamic thresholds, timelocks and committees

The simulation is optimized for local or cloud-based execution, with detailed information available on Github (link). In summary, the following are required to generate new simulation results:

Language and Tools	Hardware	Output Format
Python, leveraging libraries for simulation, numerical analysis, and data visualization (e.g., radCAD, NumPy, Pandas, Matplotlib)	Scalable from consumer-grade systems to high-performance clusters, depending on the scenario complexity	Results are structured as Jupyter notebooks for clarity, allowing detailed visualization and reproducibility

3.2 Agents and HP

The model relies on a detailed simulation of wallet owners, referred to as agents, to capture realistic decision making dynamics and their impact on the system. Central to this approach is the novel Health Points (HP) framework, which was developed specifically for this Lido DG research grant. The HP framework allows the parametrization of each agent's inclination to stay or leave the protocol due to various conditions, such as misalignment of governance decisions, ongoing attacks, or accumulated dissatisfaction. Simplifications and assumptions ensure that the model remains computationally efficient while preserving critical insights.

We begin with a detailed description of agents. Agents represent different participants in the Lido ecosystem, each with unique attributes influencing their governance behavior. The main types of agents are:

- **stETH and wstETH Holders:** Core participants whose assets can be locked in escrow to signal dissent or execute a Rage Quit
- **Rogue or Malicious Agents:** Randomly assigned participants that represent malicious agents to test attack vectors such as Veto Signalling abuse or bribery attempts
- **Committee Members:** Pre-defined participants with active screening of negative proposals, and fast reaction time on locking funds to reach Veto Signalling

Each agent is parametrized by three main parameters:

- **Token Holdings:** stETH and wstETH balances, including escrow states
- **Reaction Times:** Defined as Quick, Normal, or Slow, influencing how promptly agents act on governance proposals
- **Health Points:** An initial amount of HP is assigned to an agent at the start of the scenario. This value is then affected by proposals during the scenario's lifetime

The HP framework is central to modelling agent behavior and decision-making. HP serves as a dynamic metric that represents an agent's satisfaction with the protocol and willingness to stay engaged, influenced by activities in DG. Key characteristics of HP:

- **Dynamic Behavior:** HP changes in response to governance proposals. For example, proposals that are perceived as beneficial increase HP, while harmful proposals decrease it
- **Threshold for Action:** When HP drops to zero, the agent locks their tokens in escrow and prepares to exit the protocol if the proposal passes
- **Proposal Impact:** Each proposal includes a "health change" parameter that affects all agents. This enables cumulative effects, such as gradual decay of the system, or extreme cases such as attacks, leading to mass Veto Signalling or Rage Quits
- **Proposal Target Group:** Every proposal could also be designed to affect a specific group of agents, e.g. institutional wallets in scenarios with increasing decentralization of protocol and reduction of KYC safeguards
- **Recovery Mechanism:** When a proposal that caused HP depletion is canceled, affected agents will recover their HP, thus maintaining system balance

Advantages of HP modelling

Facilitates numeric parameterization of decision-making, providing granular control over simulations	**Captures cumulative effects** of multiple proposals, including indirect attacks that exploit gradual dissatisfaction	**Provides a proxy for system health** that reflects the collective stability of all participants

To balance realism, the required number of Monte Carlo simulations and computational efficiency, several simplifications and assumptions are applied to the traditional ABM:

1. **Independent Agents:** Each wallet or agent acts autonomously based on its parameters. Coordinated actions (e.g., multi-wallet owners) are modeled using special initial scenario parameters
2. **Simplified Reaction Times:** Agents are categorized as Quick (reacting within hours), Normal (days), or Slow (weeks), and are randomized at the beginning of each scenario. This abstraction captures behavioral diversity without excessive complexity while running multiple simulations will produce different results based on the randomization of the reaction time for each wallet
3. **Response Timeline:** Reactions to governance proposals start five days (120 hours) before scheduling deadline, taking into consideration two days (48 hours) from the proposal objection stage on DAO single governance and three days (72 hours) on the DG after submission time until the proposal is scheduled on Aragon
4. **Static Role Assignments:** Agents such as committee members or attackers can be predefined for each scenario and do not change roles during simulations
5. **Limited External Dependencies:** The model assumes that external market dynamics (e.g., ETH price fluctuations) do not affect agent decisions and focuses solely on governance-related behaviors. Extended external dependencies could provide great scope for future governance research, but they do not answer any of the existing questions outlined in Chapter 2.2

3.3 Scenario Framework

The scenario framework for the DG simulation is designed to test the system's future resilience, operational efficiency, and ability to adapt to adversarial and evolving conditions. Each scenario targets specific DG components and aligns with the goals outlined in Chapter 2.2, including:

- **Foot voting efficiency**
- **Principal-agent problem (PAP) diminishment**
- **Security**
- **Stability**
- **Future-proofing**

The simulations leverage the parameters and agent behaviors described in 3.1 and 3.2. For a more structured approach, the developed scenarios are grouped into clusters to address key optimization questions from 2.3 while focusing on specific aspects of DG performance.

Cluster A: Foot Voting Efficiency

Objective: To evaluate whether stakers can coordinate to efficiently exit the protocol during contentious governance decisions, using the Rage Quit mechanism.

Scenarios:

Simulation of Scenarios with Different User Reaction Times [Notebook]: Examines how various reaction speeds affect staker coordination and the timeliness of exits

Simulation of Various Veto Signalling and Rage Quit Threshold Parameters [Notebook]: Tests whether stakers can effectively reach Veto Signalling and Rage Quit thresholds under different parameter configurations

Rationale: These scenarios measure the system's ability to support dissenting stakers through timely exits without unduly burdening governance.

3.3 Scenario Framework

Cluster B: Principal-Agent Problem (PAP) Diminishment

Objective: To assess whether DG can effectively address the misalignment between LDO governance and stETH holders by empowering the latter to veto harmful proposals or signal dissent.

Scenarios:

Fund Stealing Attack on the Entire Protocol [Notebook]: Simulates an attacker redirecting funds from the withdrawal queue through harmful proposals. This scenario tests the ability of stETH holders to veto and prevent misuse

Label Parametrization for Proposal Effects on User Groups [Notebook]: Explores how proposals targeted at specific user groups affect governance participation and the effectiveness of Veto Signalling

Rationale: These scenarios demonstrate whether the Veto Signalling mechanism allows stETH holders to safeguard their interests and reduce governance misalignment.

Cluster C: Security

Objective: To assess the resilience of the DG system to malicious actors and external attacks, ensuring the integrity of governance.

Scenarios:

Veto Signalling Loop Attack [Notebook]: Evaluates the risk of governance paralysis due to continuous Veto Signalling by a coordinated group of actors

Attack with Bribing Capital [Notebook]: Simulates coordinated attackers bribing agents to push harmful proposals, such as replacing the withdrawal queue

Rationale: These scenarios explore how the system defends against coordinated attacks and coercion, which are critical to maintaining security in adversarial environments.

Cluster D: Stability

Objective: To determine whether DG can sustain long-term governance operations under strain without causing excessive delays, inefficiencies, or system bottlenecks.

Scenarios:

Long-Term Lock of Dual Governance with Constant Rage Quit [Notebook]: Simulates extreme exploitation scenarios the sustainability of the system under prolonged governance strain

Rationale: These scenarios analyze the ability of the system to handle normal operations and avoid governance bottlenecks caused by prolonged Rage Quit actions.

Sensitivity Analysis

Objective: To assess the sensitivity of DG system parameters and their adaptability to potential future changes in power dynamics, token distributions, and unforeseen challenges.

Scenarios:

Analysis of How Changes in Slow Actor Reaction Time Impact Governance Performance [Notebook]: Test how the assumption of Slow actor reaction time affects the DG performance

Analysis of Different Token Balance Distributions for the Existing Governance Assumptions and Scenarios [Notebook]: Test how potential future changes in the distribution of tokens across actors (more centralization - more large wallets and more decentralization - more small wallets) might affect the existing governance architecture

Rationale: This scenario explores the ability of the DG system to remain functional in extreme conditions, ensuring long-term adaptability.

3.4 Simulation Analysis

The Lido Dual Governance (DG) simulation model used the following parameters for an Agent-Based Modelling environment, unless specified differently in particular simulations:

Parameter	Value
First Seal Veto Signalling Threshold	1%
Second Seal Rage Quit Threshold	10%
Dynamic Timelock minimum duration	5 days
Dynamic Timelock maximum duration	45 days
Veto Signalling Minimum Active Duration	5 hours
Veto Signalling Deactivation Duration	3 days
Veto Cooldown Duration	5 hours
Veto Signalling Escrow Min Lock Time	5 hours
Rage Quit Withdrawals Minimum Timelock	60 days
Rage Quit Withdrawals Maximum Timelock	180 days
Rage Quit Withdrawals Delay Growth Factor	15 days
Rage Quit Extension Period Duration	7 days
Proposal Execution minimum timelock	3 days
DAO Single Governance objections stage	2 days

The simulation analysis workflow could be summarized as follows:

1. Identify clusters of scenarios and major problem groups
2. Detail scenarios that could validate different aspects of the identified problem clusters
3. Define the input parameters of each simulation scenario for the model
4. Run MCS for each scenario
5. Analyze the runs and extract insights from the simulations
6. Provide in-depth analysis of the parameters within each scenario
7. Provide in-depth analysis of the DG model as a whole

The simplified diagram in Fig. 1 below represents the process pipeline.

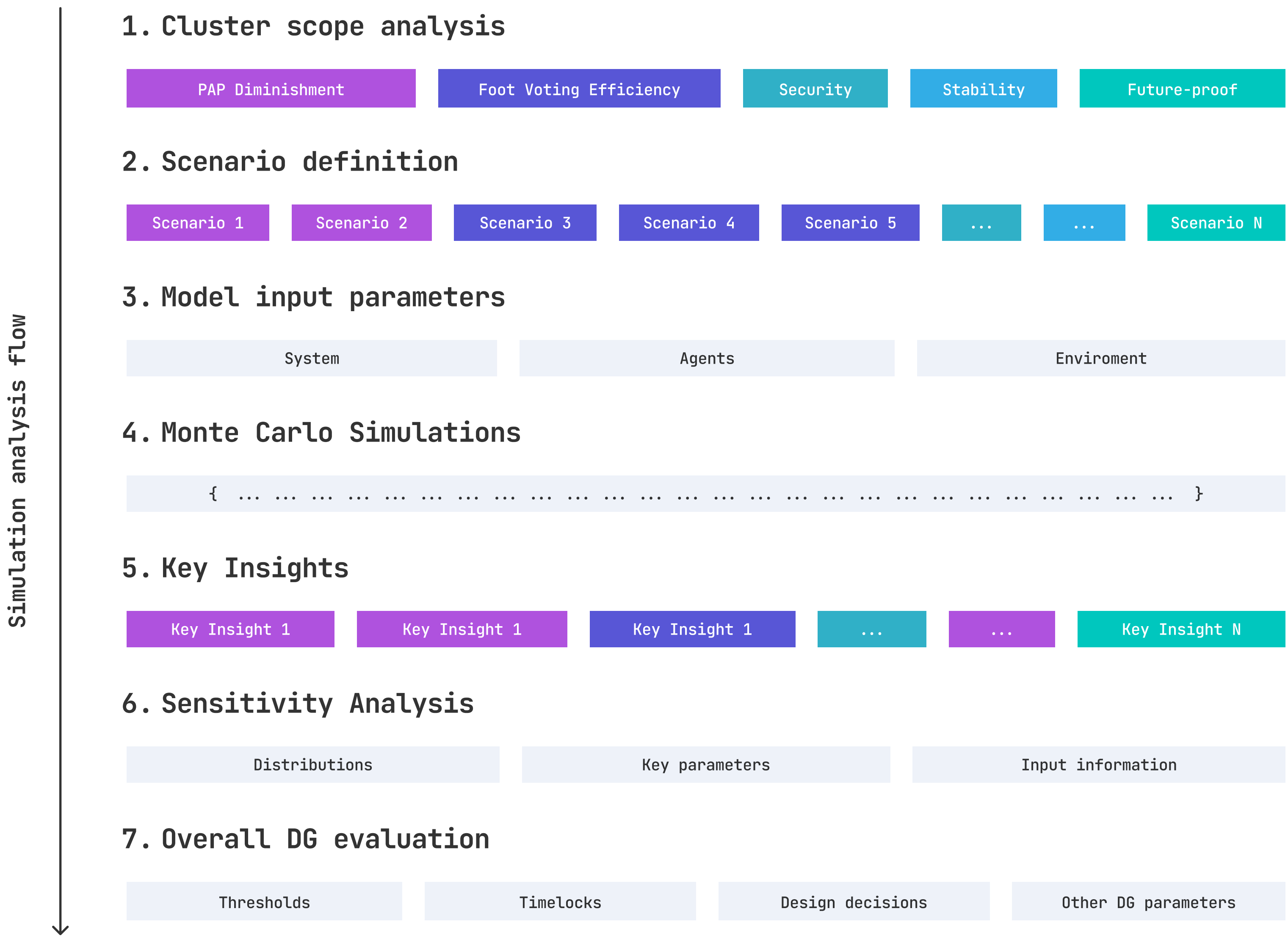


Figure 1. Simulation analysis workflow

3.6. Baseline Model Description

The baseline model serves as the foundation for all simulations, ensuring consistency across scenarios unless parameters are explicitly modified for testing. It incorporates predefined distributions of wallet balances, participant activity, and reaction times, reflecting realistic governance conditions for Lido's Dual Governance (DG) system. Part of these baseline parameters are extracted from existing Lido single governance and some are estimated to represent the current state of the protocol and provide a reference point for evaluating the impacts of parameter adjustments.

The model includes a range of wallet types and labels that impact governance participation. The pie charts in Fig. 2 below represent the wallet type distribution across actors.

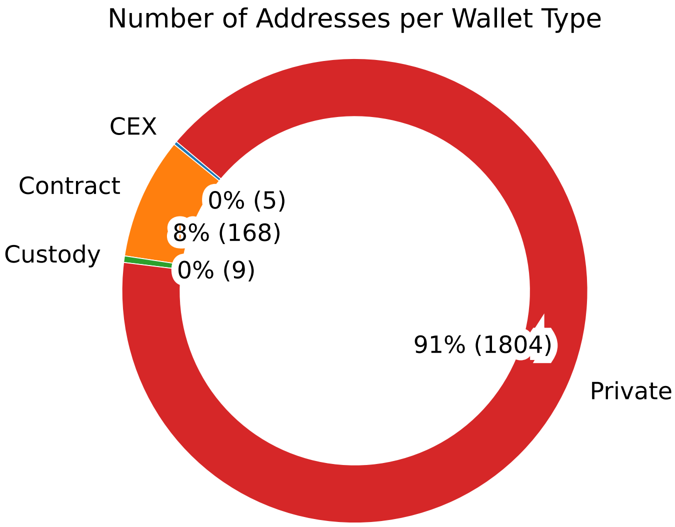


Figure 2. Base model actor address label distribution

Wallet Distribution: Top 1,900+ stETH wallet holders are included in the simulations, representing ~80% of the stETH supply and provided by the Lido team

Wallet Types: Approximately 0.45% custody, 90.84% private wallets, 8.46% contracts, 0.25% centralized exchanges (CEX).

Active Wallets: For simulation purposes, 90.84% of wallets are considered to be participating in governance, while 9.16% remain inactive, because CEX, Contract and Custody wallets are not expected to participate in any DG processes.

Excluded from DG participation: Contracts and CEX are excluded from DG participation, due to the nature of their design

Participation of funds in DG governance reflects distributions of balances across those wallets. The pie charts in Fig. 3 below represent the balance distribution across actors.

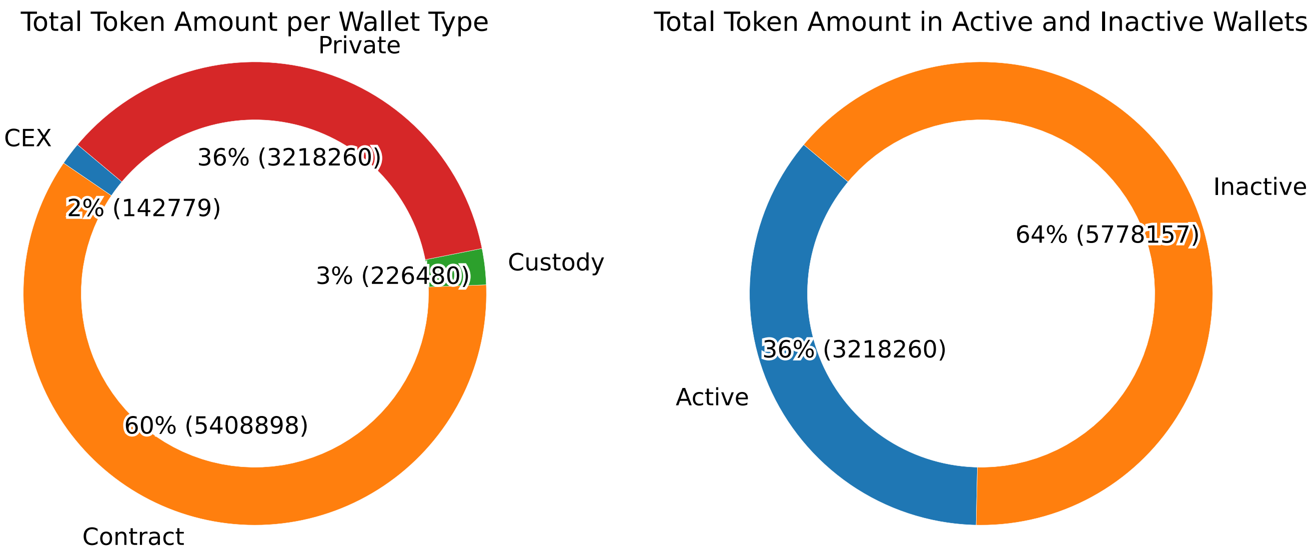


Figure 3. Base model balance distribution

- **Balance Distribution:** Reflects significant concentration in private wallets (36%) and contracts (60%), with smaller shares allocated to other labels (2% CEX, 3% custody).

- **Active Balances:** Active wallets control 36% of stETH, leaving 64% non-participating.

Participants are also categorized by their reaction times:

Quick (0-1 days proposal reaction time): ~1% of actors, typically highly engaged but small community	**Normal (1-5 days proposal reaction time):** ~10% of actors, moderate engagement	**Slow (5-15+ days proposal reaction time):** ~89% of actors, including all with balances exceeding 3,000 ETH

Reaction times are assigned randomly at the start of each Monte Carlo simulation to reflect variability in governance behavior. Detailed modelling of these actors can be found in **Section 3.2**, with validation of their distributions in **Section 4.1, Cluster A**.

This baseline ensures a consistent, representative starting point for testing how changes in thresholds, reaction times, and token distributions impact the DG system's performance and resilience.

3.7. Model Assumptions, Fidelity, and Limitations

The Lido Dual Governance (DG) simulation model evaluates the functionality and resilience of the system under various scenarios, using a number of assumptions and simplifications detailed in 3.1–3.3. While the model provides valuable insights, its outputs should be interpreted within the context of these limitations.

1. **Novelty of DG:**
   As a unique system without historical data for calibration, the model relies on insights from existing DAO governance practices and statistical approximations. Actor behavior, thresholds, and proposal impacts are informed by these observations
2. **Actor Representation:**
   - Over 1,900 wallets, representing 80% of the stETH supply, are included. Smaller holders (~20%) are excluded due to their minimal impact on governance without significant coordination requirements for a massive number of actors. Also, the distribution of holdings for these wallets changes rapidly, so it would be difficult to label them for modelling
3. **Statistical Simplifications:**
   - Health Points (HP): Reflects willingness to stay in the protocol or lock tokens in escrow. Normally distributed among actors with configurable mean and variance
   - Reaction Times: Simulated using distributions to mirror realistic variability in decision-making speeds
4. **Reaction Trigger Point:**
   - In all simulations reaction to proposal starts from the moment of objection stage in DAO single governance stage. This trigger point is used, because at that stage proposals are approved by single governance quorum and have increasing likelihood of impacting stETH token holders, therefore making reaction to it via DG impactful for Lido protocol decision making
   - Every timestamp in 4. Results is calculated from the reaction trigger point, making effective time to react to proposals 120 hours instead of the 72 hours mentioned in the DG spec itself.
5. **Scenario-Specific Proposals:**
   Proposals are classified by type and impact (e.g., random, negative, hack), directly influencing governance outcomes

To ensure robustness and address parameter ambiguity, the model ensures fidelity of the results from multiple perspectives:

3.7. Model Assumptions, Fidelity, and Limitations

1. **Addressing Parameter Ambiguity**
   - Multiple runs with randomized variables provide confidence intervals and reduce bias from specific parameter choices
   - Sensitivity analyses are conducted to explore the impact of parameter variations on system stability and performance
2. **High-Fidelity Actor Representation**
   - The model captures the behavior of large stETH holders and their influence on governance outcomes
   - Normal distributions for HP and reaction times ensure realistic variability among actors, mimicking real-world decision-making
3. **Scenario Diversity**
   The model covers a wide range of scenarios, from routine operations to adversarial attacks, ensuring comprehensive testing of the DG system under both normal and extreme conditions

The following limitations must still be considered:

1. **Simplified Environment:**
   External factors such as market volatility or cross-protocol interactions are excluded, isolating governance mechanism for focused analysis
2. **Exclusion of Smaller Actors:**
   The omission of 20% of stETH supply represented by significantly smaller wallets limits granularity, but reflects their negligible governance impact
3. **Behavioral Assumptions:**
   Static roles and reactions may not fully capture real-world complexities such as collusion or dynamic strategy shifts
4. **LDO Holders Voting Assumption:**
   In all simulated scenarios it is assumed that LDO holders passed the proposal vote in the first place. In reality, LDO voting also plays a significant filter for harmful proposals.
5. **No Historical Calibration:**
   Lack of DG-specific historical data limits calibration but is mitigated by using proxy data from similar systems

The simulation model offers reliable insights into the DG system by combining robust statistical methods, scenario diversity, and Monte Carlo techniques. While its focus on key actors and parameters ensures actionable findings, future refinements could address limitations by incorporating dynamic behavior, real-time data, and broader actor inclusion.

RESULTS

4

4.1 Assessment of Key System Parameters

This section evaluates the critical parameters of the Dual Governance (DG) system by aligning simulation scenarios with the goals outlined in 2.3. Using the scenario framework described in 3.3, this chapter provides insights into how the DG system performs under various conditions and identifies key areas for optimization.

The assessment methodology focuses on two key evaluations of the DG parameters:

1. Individual Parameter Testing

Analysis of individual governance variables, such as Veto Signalling thresholds, timelock durations, and Rage Quit activation levels, to assess their impact on DG performance

2. System Sensitivity Analysis

Conducting parameter sweeps over a range of values to test system resilience and identify configurations that provide a balance of stability and adaptability

Simulations are analyzed based on the outputs in Python notebooks for each case, which are available on GitHub with various output statistics, visualizations and additional information, including:

- Escrow behavior over time
- Activation times for Veto Signalling and Rage Quit mechanisms
- HP trends and agent responses to proposals
- System-level indicators such as locked token volumes and proposal success rates

Below are the condensed results from the detailed evaluations of how the system is meeting each objective.

Cluster A: Foot Voting Efficiency

Simulation of Scenarios with Different User Reaction Times via analysis of Fund Stealing Attack on the Entire Protocol scenario **[Notebook].**

1. **Scenarios: Tested over three major distributions of actor reactions in DG life:**
    - Normal system reaction (Mostly expected for future DG life):
    - Fast system reaction (E.g. extensive social media activity):
    - Slow system reaction (E.g. unimportant update or off-season):

DG reaction	Share of Quick actors	Share of Normal actors	Share of Slow actors
Normal system reaction	~1%	~10%	~89%
Fast system reaction	~2%	~20%	~78%
Slow system reaction	~0.5%	~5%	~94%

2. **Actor reaction delay**
    - Quick actors (0-1 days reaction time from proposal)
    - Normal actors (1-5 days reaction time from proposal)
    - Slow actors (5-15 days reaction time from proposal)

The basic reaction delay distribution for actors in the normal system reaction is shown in Figure 4.

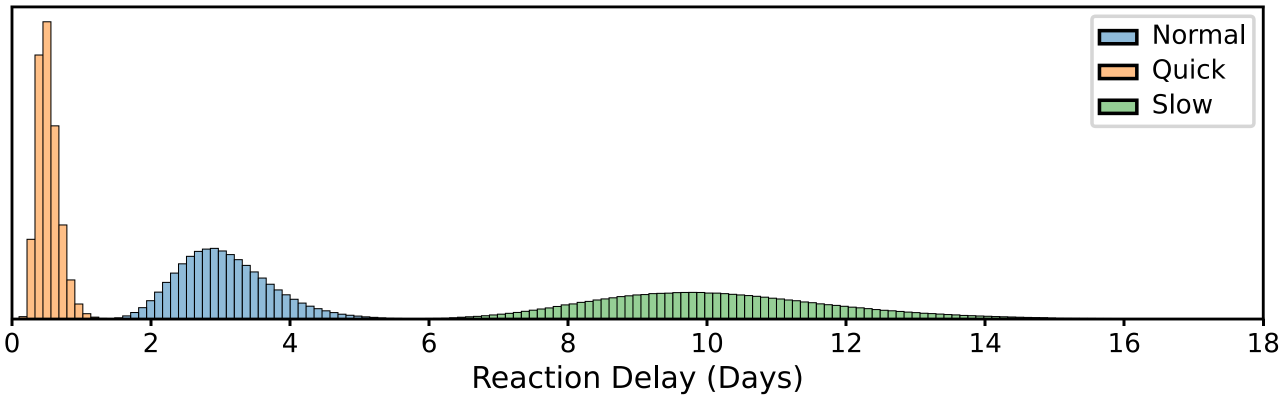


Figure 4. Reaction delay distributions of actors in the system

Cluster A: Foot Voting Efficiency

Quick and Normal actor total token share distributions in different system reaction simulations are shown in Figure 5.

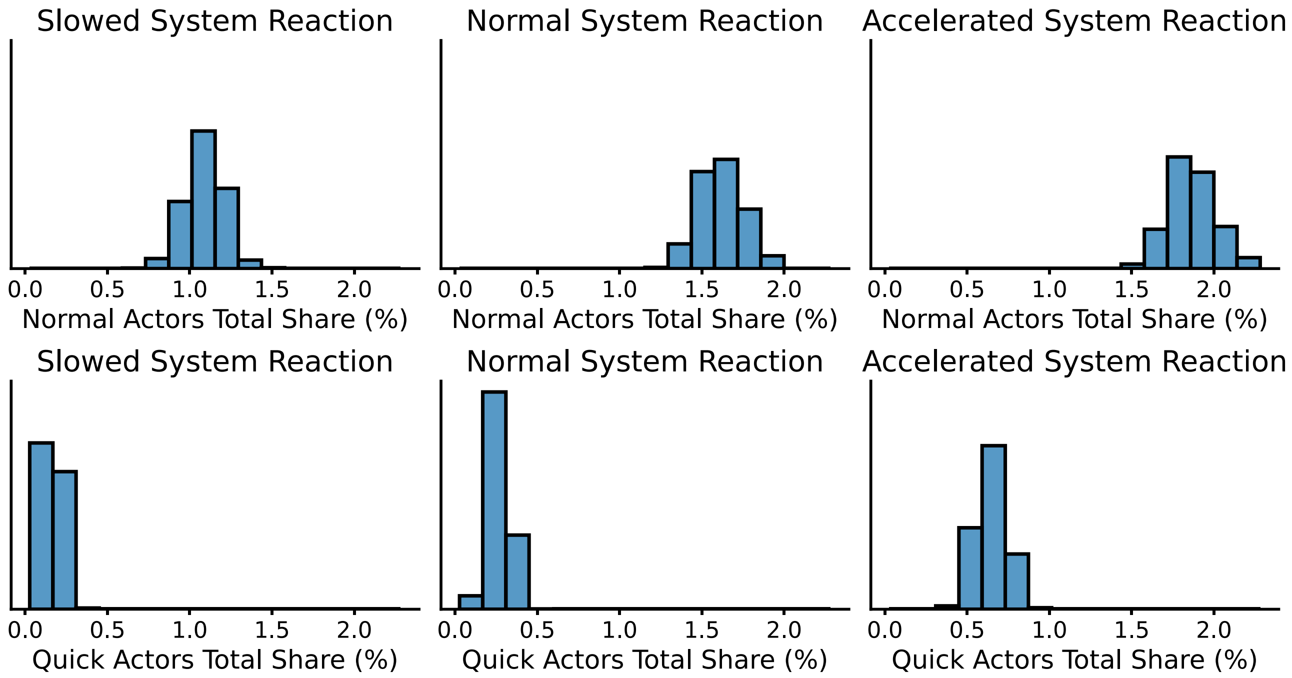


Figure 5. Histograms of total token shares of Normal (top row) and Quick (bottom row) actors under different reaction distributions

The effects of DG Reaction Times on Veto Signalling and Rage Quit are given in Tables 1 and 2.

3. 1% Veto Signalling analysis

DG reaction distribution	Reaching success rate	Median time to Veto
Normal	100%	72 hours (3 days)
Fast	100%	60 hours (2.5 days)
Slow	97%	87 hours (~3.6 days)

Table 1. Impact of DG Reaction Times on Veto Signalling

4. 10% Rage Quit analysis

4.1 Assessment of Key System Parameters

Cluster A: Foot Voting Efficiency

DG reaction distribution	Reaching success rate	Median time to Veto
Normal	100%	213 hours (~8.9 days)
Fast	100%	213 hours (~8.9 days)
Slow	97%	216 hours (9 days)

Table 2. Impact of DG Reaction Times on Rage Quit

What's being observed

1. In general, 1% and 10% thresholds work well for the majority of DG participants and different reaction scenarios, providing sufficient time to express opinions on changes or protect against attacks if necessary
2. Actors with quicker reaction times drastically reduce the time to Veto Signalling, but do not have much impact on Rage Quit, highlighting the importance of active participation in governance for DG protection
3. Unclear proposal evaluation or lack of interest in DG could reduce the timely responses to harmful proposals
4. Normal system reaction with ~1% Quick, ~10% Normal, ~89% Slow share of actors appears to be appropriate for all future simulations for default system reaction

Recommendations

- Introduce mechanisms to incentivize faster actor reactions, or find ways to alert large wallet holders to important proposals in the system
- At the launch of DG, monitor the activity of token holders to ensure adequate representation of Quick and Normal actors in the system

Simulation of Various Veto Signalling and Rage Quit Threshold Parameters via analysis of Fund Stealing Attack on the Entire Protocol scenario **[Notebook].**

4.1 Assessment of Key System Parameters

Cluster A: Foot Voting Efficiency

1. Varying Veto Thresholds

- The parameters tested and the resulting success rates are given in Table 3.

Veto Signalling Threshold	Reaching success rate	Median time to Veto
0.5%	100%	60 hours (2.5 days)
0.75%	100%	66 hours (~2.8 days)
1%	100%	72 hours (3 days)
1.25%	100%	78 hours (~3.3 days)
1.5%	97%	87 hours (~3.6 days)
2%	16.6%	156 hours (6.5 days)

Table 3. Veto Signalling success rates and time to reach the Veto Signalling threshold as a function of the threshold

- Success rates drop sharply past a 1.5% Veto threshold, dropping from 100% at 1% to only ~16.6% at 2%

2. Varying Rage Quit Thresholds

- The parameters tested and the resulting success rates are given in Table 4:

Rage Quit Threshold	Reaching success rate	Median time to Rage Quit
5%	100%	198 hours (~8.3 days)
7.5%	100%	210 hours (~8.8 days)
10%	100%	219 hours (~9.1 days)
12.5%	100%	228 hours (~9.5 days)
15%	100%	237 hours (~9.8 days)

Table 4. Rage Quit success rates and time to reach the Rage Quit threshold as a function of the threshold

4.1 Assessment of Key System Parameters

Cluster A: Foot Voting Efficiency

- Rage Quit thresholds were successfully reached in all scenarios

What's being observed

1. Based on the initial actor participation assumptions, 1% and 10% appear to be well-suited parameters for Veto Signalling and Rage Quit thresholds, respectively, where the majority of actors were able to react within the provided voting windows
2. Veto Signalling appears to be the most sensitive to actor reaction distributions, where ideally you want to have a pool of ~10% of actors as Quick and Normal in order to have no problems with reaching thresholds in time. The Rage Quit Threshold was less affected by the actor's reaction time distribution, as even Slow users were able to participate in the voting
3. While 1% and 10% thresholds are effective in most scenarios, close attention should be paid to the Veto Signalling thresholds, as they also play an important role in system stability against abuses such as Veto Loops. This is discussed further in clusters C and D

Recommendations

- Introduce mechanisms to incentivize actors to respond more quickly or find ways to alert big wallet holders when important proposals are happening in the system
- Understanding the best communication and outreach channels to major DG participants should play an important role in the DG system resilience to attacks

Cluster B: Principal-Agent Problem (PAP) Diminishment

The evaluation focused on the ability of stETH holders to veto and prevent misuse, and assessed whether DG can effectively address misalignments between LDO consensus and stETH holders. The misalignment between DAO and stETH holders could be represented by many different scenarios, but the easiest to model is a simulation of a proposal pushed by LDO that becomes a **Fund Stealing Attack on the Entire Protocol [Notebook].** The attacker's strategy is to acquire stETH through external capital to dilute the other token holders' share so that their share is not enough to reach Veto Signalling, with the assumption that LDO holders have voted for the proposal already. This attack design also allows us to evaluate various potential attack parameters together with attack feasibility and expected cost.

The main idea of the attack is that as the attacker adds tokens to the total stETH pool, the absolute amounts held by others remain the same, but the relative amounts become smaller. Thus, if the Quick and Normal token holders together have exactly 1% of the total stETH pool (Veto Signalling threshold), then after dilution they will not have enough to reach Veto Signalling. The greater the dilution, the less likely it is that active token holders will have enough stETH for Veto Signalling.

Key Results and Observations

1. **Attacker Influence on Veto Signalling**
    - Attacker Share vs. Attack Success across simulations:
      The results are given in Table 5 and in Figure 6.
        - Success rates remain negligible (1.5%) until the attacker holds 35% of the total supply in % of stETH TVL
        - Success rates rise steeply beyond 40% of the token supply

Attacker's share of total supply in % from stETH TVL	Attack success rate probability
25%	0%
30%	0%
35%	1.33%
40%	10.92%
45%	40.72%
50%	81.84%
55%	99.49%

Table 5. Attack success rates as a function of attacker share of the total supply

Cluster B: Principal-Agent Problem (PAP) Diminishment

2. Marginal cost for each additional 10% of success rate:

The results are given in Table 6.

- For a 10% success increase in success rate, the marginal cost is about 1.5-2.5% after reaching the initial success of 1% at about 35% of the total token supply

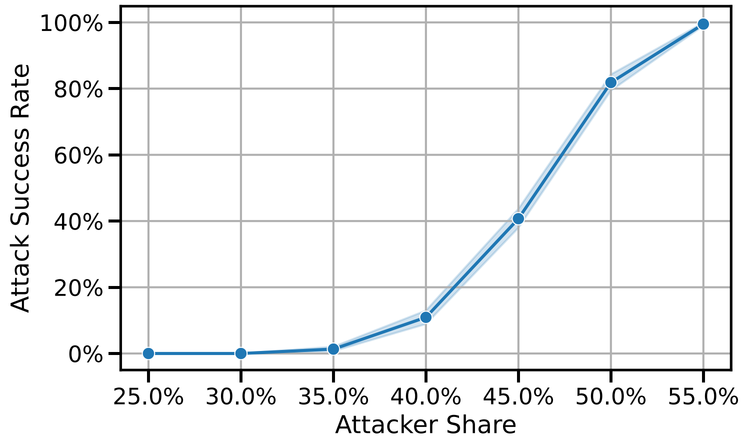


Figure 6. Attack success rate as a function of attacker's share of the total supply

Success rate	Attackers share of total supply	Marginal cost of 10% success increase
0%	0.00%	39.52%
10%	39.52%	2.00%
20%	41.52%	1.68%
30%	43.20%	1.68%
40%	44.88%	1.25%
50%	46.13%	1.22%
60%	47.34%	1.22%
70%	48.56%	1.22%
80%	49.78%	2.54%
90%	52.31%	2.69%

Table 6. The marginal cost of increasing attack success rate by 10%

Cluster B: Principal-Agent Problem (PAP) Diminishment

3. Cost of Attack:

- Coordinated attacks on the Lido protocol with significant success require substantial token acquisition. Achieving a 95% success rate necessitates ~53.7% of the newly diluted token supply, making such attacks economically infeasible for most actors to coordinate with external capital

What's being observed

- The Veto mechanism effectively discourages small-scale attacks, as attackers need to hold or acquire a significant share of the tokens to have meaningful success
- Potential danger might come from attacks on large existing token holders or the capture of external protocols with large stETH holdings
- Bribing active voters, rather than diluting the liquidity pool, may be a more effective protocol attack and it is analysed in detail in Cluster C

Recommendations

- Maintain Veto Signalling thresholds around 1-1.5% to ensure protection against economically viable attacks
- Regularly monitor token distribution to identify concentrations that could pose a risk to governance integrity

Label Parametrization for Proposal Effects on User Groups [Notebook] focused on how proposals targeting specific actor groups within the protocol could affect governance participation and the effectiveness of Veto Signalling. An example of such a proposal could be a protocol proposal for special KYC/KYB requirements that favor institutional actors and go against decentralization activists. In the simplest case, this could be represented by two groups within the existing stETH holder pool and the proposal only affects one of them, e.g. forcing them to lock funds, while the other group remains unaffected. This gives a better understanding of the group dynamics within the stETH governance layer and helps to understand the voting dynamics for two and more groups.

For example, defending group size is 45%. To get the defending group, a random sample without replacement of size floor(0.45 * n) is taken from all the Quick and Normal addresses.

Cluster B: Principal-Agent Problem (PAP) Diminishment

1. Governance Dynamics of Minority and Majority Groups

- Label-based simulations with two competing groups
- Veto success rates for different token shares of the defending group are presented in Figure 7. Similarly, Figure 8 shows Veto success rates against the defending group's token share relative to the Veto Signalling threshold.

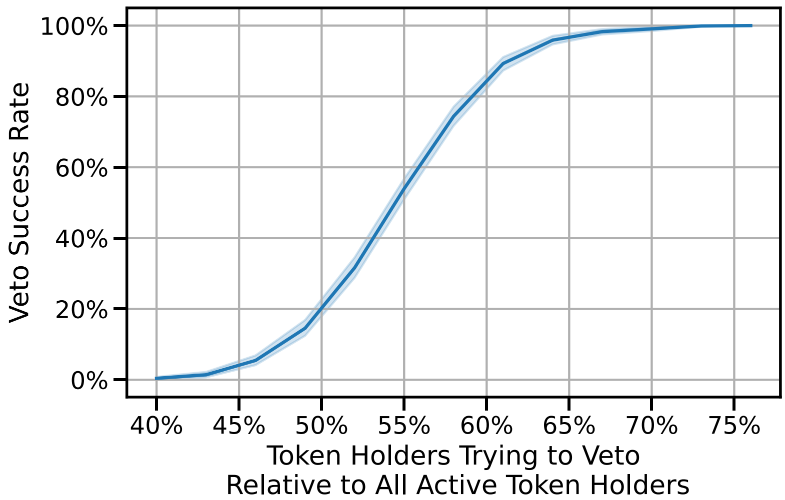


Figure 7. Veto success rate as a function of the defending group's token share

- Majority groups (~60% token share) require coordinated efforts to reliably push favorable proposals or protect against unfavorable ones
- Reaching at least 140% of the Veto Signalling Threshold for Quick and Normal actors of each label group ensures an effective response to potentially harmful proposals

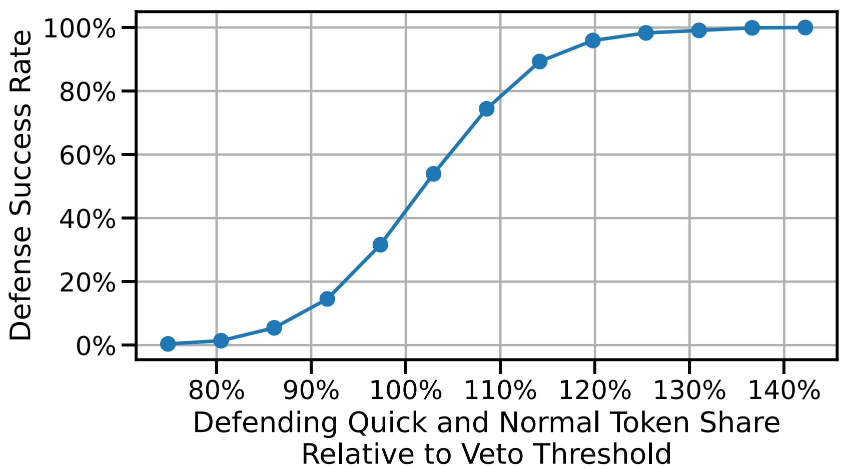


Figure 8. Veto success rate as a function of the defending group's token share relative to the Veto Signalling Threshold

Cluster B: Principal-Agent Problem (PAP) Diminishment

2. **Label Effects on Governance:**
   - Proposals targeting one label (e.g., institutional holders) at the expense of another (e.g., decentralized holders) create governance polarization, requiring enhanced minority representation to resist adverse impacts
   - Further testing could be done for analysis of multiple minority groups participating in stETH governance with different priorities

What's being observed

The Veto mechanism requires significant power concentration or coordination within the stETH community to ensure the protection of this group's interests, given the participation distribution as in the regular governance flow. Otherwise, minority groups wishing to defend themselves against harmful proposals will need to coordinate more effectively and increase the speed of their governance participation to have at least 140% of the Veto Signalling Threshold ready for voting within the governance timeframe.

Recommendations

- Increase proposal impact transparency to minimize governance conflicts between potential governance groups
- Provide the community with additional channels to activate their respective voting groups to more effectively protect minority groups from harming proposals
- Identify potential conflicting groups in the stETH governance space and try to estimate their respective power, ensuring that all these groups have sufficient community and social activation during the voting process

Cluster C: Security

The **Veto Signalling Loop Attack** evaluation **[Notebook]** focused on the risk of governance paralysis due to continuous Veto Signalling by a coordinated group of actors. To assess the ability of the DG system to defend against coordinated Veto Signalling loops, the scenario was designed with an actor or a group of actors attempting to lock DG for the longest period of time.

Key Results and Observations

1. **Veto Signalling Loop Attack**
   - **Potential Execution Delays from Continuous Veto Signalling**

The proposal execution delay due to Veto Signalling is illustrated in Figure 9. First, the scheduling of the proposal is delayed until the first VetoCooldown state. Then, the after schedule delay is passed and the proposal is executed.

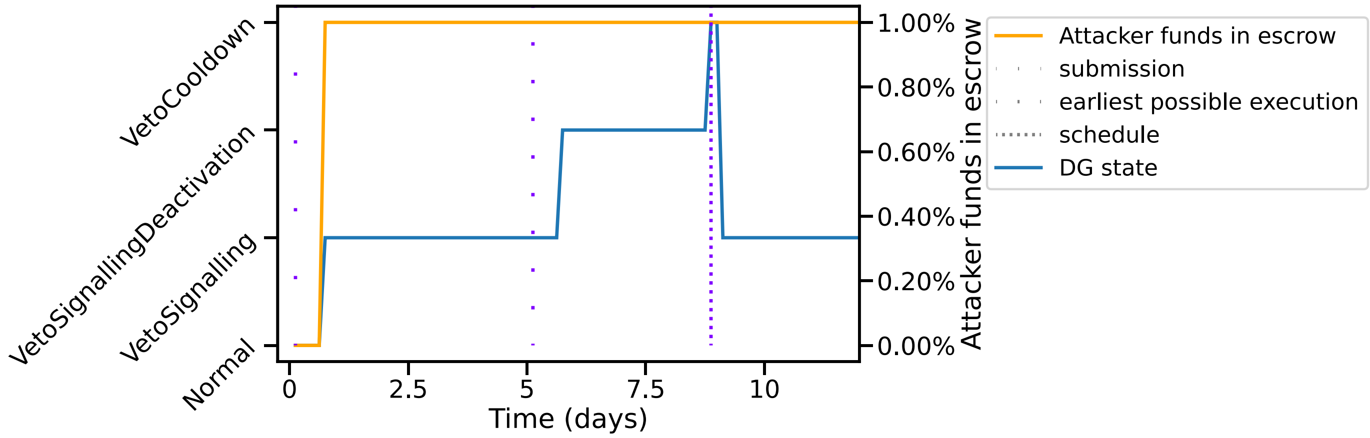


Figure 9. Representation of DG state transitions relative to time and escrow balance

The relationship between execution delay to attacker share is given in Table 7.

- Since the attacker tries to postpone the execution of the proposal for the longest duration possible, they are incentivized to lock into escrow just before the execution timeline
- Proposed Veto Signalling dynamic timelock duration duration results in:
  - 1% coordinated attacker share results in ~11-day delay
  - 9% coordinated attacker share extends the delay to ~46 days

Cluster C: Security

Attackers' share	Execution delay from proposal submission
1%	~11 days
2%	~15 days
3%	~20 days
4%	~24 days
5%	~29 days
6%	~33 days
7%	~37 days
8%	~42 days
9%	~46 days

Table 7. Proposal execution delay due to Veto Signalling Loop attack with different attacker shares

Veto Signalling	Deactivation sub-state	Veto Cooldown
60%	37%	3%
74%	24%	2%
80%	17%	1%
84%	14%	1%
87%	10%	1%
89%	9%	1%
90.3%	9%	1%
91.4%	7%	1%
92.3%	7%	1%

Table 8. Duration of each DG system state in the Veto Signalling loop relative to the total loop duration. Calculated for different attacker shares

2. Distribution of DG States in the scenario of constant Veto Signalling loop:

This scenario can happen when the group of attackers keep their tokens locked in escrow to delay the updates as much as possible. We can also imagine the situation where some neutral token holder locks their tokens in escrow and then loses access to their wallet.

The simulation runs for 180 days and we calculate the duration of each system state. The results for different attacker shares are given in Table 8.

- **Veto Signalling dominates:** For higher attacker shares (e.g., 9.9%), ~92% of the time is spent in the Veto Signalling state, with minimal cooldowns (~1 day) and deactivation states (~13 days)

Cluster C: Security

What's being observed

- The DG system becomes increasingly locked as the attacker share grows, with proposal execution delays extending significantly, while still leaving enough room for proposal approval and execution during the deactivation state
- This could only be used to delay proposals rather than block them completely, and the high capital requirements make it almost useless, apart from rare cases where preventing proposals for a few days could provide a massive return to the attacker
- Consecutive Veto Loop attacks are not possible with existing DG design

Recommendations

- Clearly communicate to the community that even extended Veto Signalling states of Dual Governance do not directly harm the Lido ecosystem
- Use the Gate Seal mechanism as a backup to ensure that time-critical proposals can bypass prolonged delays caused by Veto Signalling

Attack with Bribing Capital [Notebook] focuses on the assumption that the attacker could bribe the actor who locked funds in Veto escrow with funds greater than the actor's balance in Lido. A rational actor should be willing to take an amount of funds in Lido + 1 to accept the bribe and unlock funds from escrow. The simulation can then show how many actors the attacker would need to bribe and what the minimum amount of capital the attacker would need to have to bribe.

Cluster C: Security

1. Simulation of Bribery Targeting Quick and Normal Actors with reaction time less than 5 days.

The results are given in Table 9.

Reactions	Early reaction actors count			Early reaction actors token share of Total Token supply			Amount for bringing to lower below 1% Veto Signalling		
	Median	Min	Max	Median	Min	Max	Median	Min	Max
Fast	331	288	393	2.46%	1.90%	3.20%	1.46%	0.90%	2.20%
Normal	248	205	305	1.85%	1.34%	2.40%	0.85%	0.34%	1.40%
Slow	165	131	211	1.23%	0.84%	1.61%	0.23%	0.00%	0.61%

Table 9. Summary statistics of token distribution for Bribing attacks. Early reaction actors are Quick and Normal actors who are able to delay proposal execution by initiating Veto Signalling

- **Median number of voters who will vote in the first 5 days and their token share:**
  - **Fast Reaction:** ~331 actors (2.46% of the total token supply)
  - **Normal Reaction:** ~248 actors (1.85% of the token supply)
  - **Slow Reaction:** ~165 actors (1.23% of the token supply)

2. Comparison to Dilution Attack Costs:

- Bribing costs are significantly lower than dilution-based attacks in Cluster B because bribers only need to influence a fraction of the most responsive actors
- For example, a bribing attack targeting fast reactors (~2.5% of the token supply) costs less than acquiring 35+% of the total supply for dilution
- The Bribing scenario introduces more uncertainty as it is based on bribing rational actors, while in the real world participants usually act much differently from the optimal strategy, especially when there are 100+ actors making decisions at the same time. Moreover, bribing 100+ actors in the real world is a complex challenge in itself

Cluster C: Security

What's being observed

- Bribing provides a more cost-effective attack vector but the attack execution is significantly more complicated
- Attackers need fewer resources to bribe key participants than to achieve the same outcomes through dilution
- Strategies involving last-minute bribery or the attacker's fake self-locking with a plan to unlock in the last few minutes before the proposal is approved could be particularly effective, as it may influence other actors that locking in no longer necessary because the threshold has already been passed

Recommendations

- Introduce escrow unstaking lock mechanisms on the last day of Veto Signalling to avoid last notice unstaking inconsistencies. Additional withdrawal lock on escrow during the last 12+ hours before potential proposal scheduling could significantly constrain bribing attacks without major problems to regular actors
- In cases of very low actual actor participation in DG, consider additionally promoting individual actor responsibility and risk for participating in the first Veto Signalling staking as the lower the number of participants, the easier it is to bribe
- Consider anti-bribery mechanisms, such as locking actor rewards, to safeguard against Quick actor exploitation
- Increase transparency of proposal impacts to reduce susceptibility to bribery among Quick and Normal actors

Cluster D: Stability

The **Long-Term Lock of Dual Governance with Constant Rage Quit** evaluation **[Notebook]** focused on scenarios where attackers aim to repeatedly exploit the Rage Quit mechanism, causing prolonged governance bottlenecks and reducing the ability to upgrade the protocol, which could be used as an attack vector in itself or be used as a part of a more sophisticated attack.

Key Results and Observations

1. **Guiding principle**
    - Provided by Lido: “If one or several actors (further will use only the word ‘actor’ for simplicity) have enough stETH to trigger Rage Quit, such actor should be able to trigger Rage Quit once per normal to normal state cycle (i.e. could not trigger several consecutive Rage Quits with the same stETH).”
    - The above principle was tested in the simulations with the current DG design parameters
2. **Simulation details**
    - Days in each state for each run, number of Rage Quit events, full table and example run are available in **[Notebook]**. The main results are given in Table 10 below
    - Simulations ran for 48 months or until Rage Quit was no longer constant
    - After the Rage Quit withdrawal, the total stETH pool becomes smaller by 10%, so the attacker needs only 10% * 0.9 = 9% of the total stETH to initialize another Rage Quit. Following this logic we use 10%, 19%, 27.1%, and 34.4% to simulate attackers having funds for 1, 2, 3, and 4 consecutive Rage Quits, respectively, plus the attacker makes sure that after Rage Quit, there is still 1% in escrow

Cluster D: Stability

Attacker's share	Lido Protocol Total ETH Balance	Days in: Veto Signalling	Days in: Rage Quit	Days in: Veto Signalling Deactivation	Total days of blocked DG	No. of Rage Quits
0.1075	4.5 mil	45	20	0	65	1
	9 mil	45	35	0	80	1
	18 mil	45	65	0	110	1
0.1955	4.5 mil	183	82	5.625	271	4
	9 mil	186	139	3.125	328	4
	18 mil	276	374	3.125	653	6
0.2710	4.5 mil	410	178	4.75	593	9
	9 mil	457	334	3.125	794	10
	18 mil	**632**	**808**	**0**	**1440**	**14**
0.3440	**4.5 mil**	**1027**	**413**	**0**	**1440**	**22**
	9 mil	**857**	**582**	**0**	**1440**	**19**
	18 mil	**632**	**808**	**0**	**1440**	**14**

Table 10. The number of consecutive Rage Quit events and days in each DG state was calculated for different Lido Protocol total ETH balances and different attacker's shares of these total balances. Bold indicates cases where Constant Rage Quit was maintained until the end of the simulation.

3. Impact of Attacker Share on Loop Cycles:

- **Low Attacker Share (10%):** Attacker funds are exhausted after a single Rage Quit cycle, resulting in minimal disruption and matching the guiding principle
- **Moderate Attacker Share (19%):** Allows up to four Rage Quit cycles in smaller pools (~4.5M stETH total supply) and five cycles in larger pools (~18M total supply)

- **High Attacker Share (27%+):** Sustains up to eight cycles in smaller pools and 14 cycles in larger pools, creating prolonged governance strain

4. **Pool Size Dependency:**
    - Larger pools significantly extend Rage Quit duration due to the fixed throughput of the withdrawal queue

What's being observed

- Attackers with sufficient liquidity can exploit the Rage Quit mechanism to disrupt governance for prolonged periods of time, particularly in large pools with fixed withdrawal throughput
- Larger pools magnify the impact of Rage Quit cycles, as extended withdrawal durations allow attackers to recycle funds for subsequent disruptions
- Competition for ETH validator exit share could become an issue in the future, creating even more problems with extended durations

Recommendations

- Consider scenarios where large existing or future protocols, smart contracts or external companies with sufficient funding go rogue or get hacked, while using the obtained funds to disrupt the flow of Lido Dual Governance
- Consider creating critical governance windows every X Rage Quits, that could be used to pass proposals that are different from those currently vetoed. Adding a mechanism like this could reduce the incentive for these attacks and maintain the ability to upgrade the protocol with critical patches without having to take over DG completely

4.2 Sensitivity analysis of DG parameters

This section evaluates the sensitivity of the model's outputs to its parameter assumptions, with a focus on two key parameters: actor reaction times and token wallet distributions. By testing how variations in these parameters affect the model's outputs, we aim to assess whether deviations from the assumptions significantly alter the results. This will help validate the robustness of the model and provide insights into how changes might impact real-world DG performance. The following two simulations were conducted to test these new conditions:

1. The impact of changes in Slow actor reaction time on governance performance
2. The impact of changes in wallet distribution on DG performance

4.2.1 Impact of Slow Actor Reaction Assumptions on DG modelling

Analysis of how changes in Slow actor reaction time impact governance performance [Notebook] evaluates how increasing Slow actor reaction times from 15 up to 60 days might impact governance performance, particularly in reaching the Rage Quit state.

The model is designed so that Slow actors play a minor role in the first Veto Signalling threshold, as they almost never react within the first five days. Their influence is primarily observed during the transition from the 1% to the 10% escrow threshold, where their reaction time and token balances can significantly affect the system's transition and success in reaching Rage Quit.

The distributions of Slow actors' reaction delay used for the sensitivity analysis are shown in Figure 10.

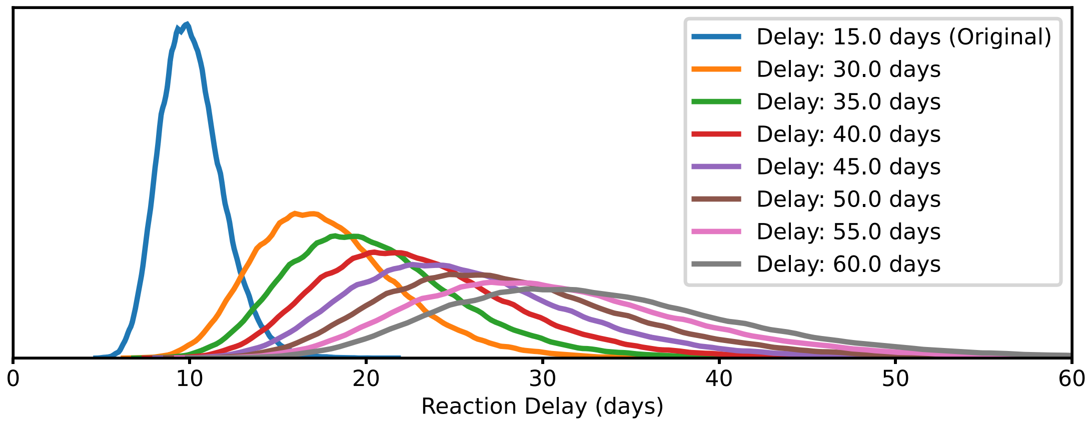


Figure 10. KDE estimates of different Slow actor reaction delay distributions

4.2 Sensitivity analysis of DG parameters

4.2.1 Impact of Slow Actor Reaction Assumptions on DG modelling

The simulation results are given in Table 11. We can see that for Slow actor delays of up to 35 days, there is little to no impact on the system's ability to reach Rage Quit thresholds. Beyond that, the rate of successful Rage Quit events drops sharply.

Slow Actor Max Delay (days)	Rage Quit Success (%) R2=10%
15	100%
30	100%
35	100%
40	97%
45	49.5%
50	13.7%
55	1.3%
60	0%

Table 11. Rage Quit Success rates for different Slow actor reaction delay distributions

4.2 Sensitivity analysis of DG parameters

4.2.1 Impact of Slow Actor Reaction Assumptions on DG modelling

Key Results and Observations

1. **Limited Sensitivity at 15-35 Days**
   a. The system demonstrates strong resilience to changes in Slow actor reaction times within this range
   b. Slow participants still provide sufficient Veto power and token availability to match the linear growth in Veto Signalling thresholds during this period
2. **Critical Threshold Beyond 40 Days**
   a. When Slow actor delays exceed 40 days, the reduced participation of these actors begins to hinder Rage Quit success rates
   b. This limitation occurs because fewer tokens are available in escrow to meet the Rage Quit threshold, prolonging governance inactivity
3. **Realistic Assumptions for 15-Day Baseline**
   a. While the DG system lacks real-world data to validate Slow actor behavior, using 15 days as a baseline is reasonable for the current DG model
   b. This assumption is consistent with the design of the system, which allows active minorities to block decisions in the Veto Signalling state while also accommodating negotiations and eventual transitions to the Rage Quit state if necessary

Slow actors contribute primarily by locking their tokens in the Veto Signalling escrow, thus influencing the duration and transitions between governance states:

4.2.2 Impact of Wallet Distribution Assumptions on DG modelling

1. Role in Veto Signalling

Quick and Normal actors dominate the 1% Veto Signalling threshold due to their timely responses, while the delayed participation of Slow actors has a negligible impact during the 1% Veto Signalling state duration (targeted at 5-45 days, according to the proposed parameters for the model)

2. Role in Rage Quit Transitions

Slow actors' tokens become critical during transitions from the Veto Signalling state to the Rage Quit Accumulation state, particularly as the Veto Signalling thresholds scale toward the 10% Veto Second Seal Threshold

With the goal of assessing the adaptability of the DG system to changing power dynamics, token distributions, and unforeseen challenges, the **Analysis of Different Token Balance Distributions for the Existing Governance Assumptions [Notebook]** was conducted. Simulations tested how the existing scenarios, particularly in Clusters A and C, will perform under potential future changes in token distributions among actors (e.g., more centralization - higher number of large wallets and more decentralization - higher number of small wallets).

Key Results and Observations

1. **Assumptions on potential token distribution changes**
    - Three general options for future wallet distributions are shown in Figure 11.

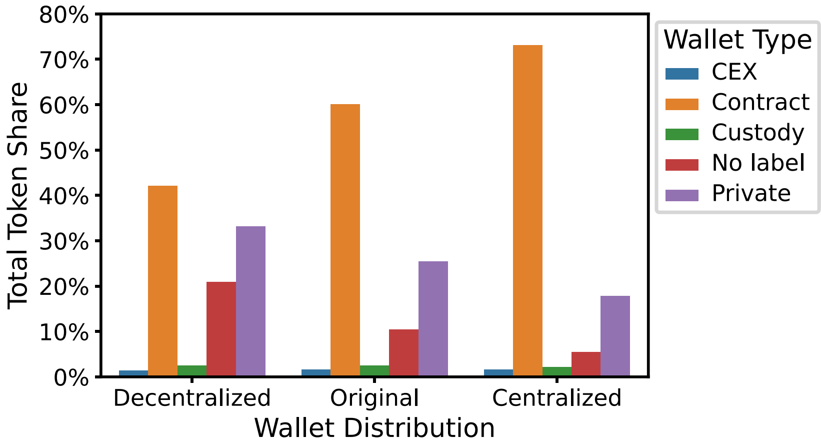


Figure 11. Bar charts of token shares of different token holders in decentralized, centralized and original Lido wallet distributions

4.2.2 Impact of Wallet Distribution Assumptions on DG modelling

- **Original:** Provided by Lido and based on the top 80% of token holders in the wallet distribution
- **Decentralized:** To simulate greater decentralization of the protocol, 30% of the funds from Contracts, 15% of the funds from CEX, 0% of the funds from Custody were redistributed equally among the existing Private Wallets. As a result, the system has more private wallets with similar balances
- **Centralized:** To simulate greater centralization of the protocol, each balance was raised to the power of 1.2 and then the balance distribution was normalized to match the original balance sum, amplifying the disparity between balances, causing larger balances to grow disproportionately more than smaller ones. As a result, the wallet distribution appears to be more centralized, with tokens concentrated in fewer entities

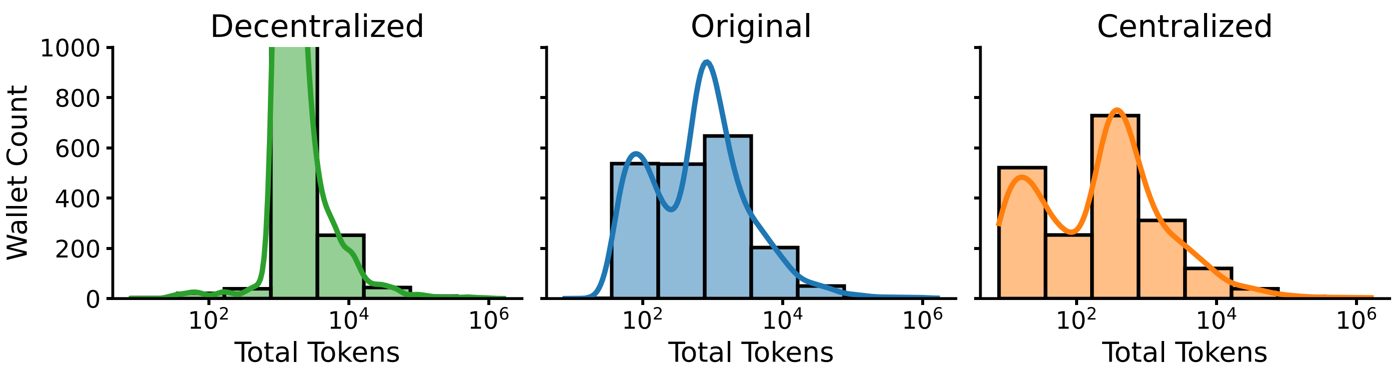
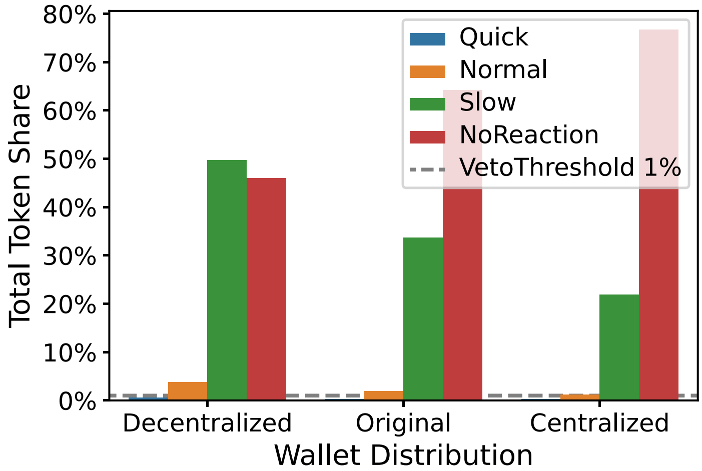


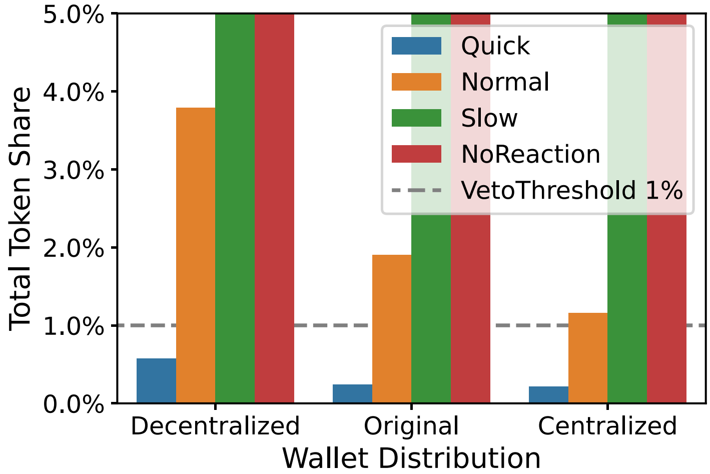
Figure 12. Histograms of simulated wallet balance distributions

Table 12. Bins of simulated wallet balance distributions

Token balance	0 - e1	e1 - e2	e2 - e3	e3 - e4	e4 - e5	e5 - e6	e6 - inf
Decentralized	0	17	351	1508	100	10	0
Original	0	350	889	641	93	12	1
Centralized	117	586	867	348	56	10	2

4.2.2 Impact of Wallet Distribution Assumptions on DG modelling





Changes to reaction times based on the wallet distribution updates are shown in Figure 13.

2. Token Distribution Impact on Veto Success Rates (Cluster A)

The results are given in Table 13

- **Decentralized Distribution:** Decentralization improves Veto success rates across all actor reaction speeds, with **fast reactions achieving a 100% Veto success rate** in as little as 15 hours. Normal and Slowed reactions also maintain high Veto rates due to the increased relative wealth of active wallets.
- **Centralized Distribution:** Centralization hinders Veto Signalling, especially for Slowed reactions. **Veto rates drop to 2% for Slowed reactions**, and even for Normal reactions we see significant delays in reaching Veto thresholds. Fast reactions maintain 100% success, but take 75 hours, significantly longer than in decentralized distributions.
- **Original Distribution:** Results are balanced between the centralized and decentralized scenarios, with Veto success rates and times largely in line with baseline assumptions.

4.2.2 Impact of Wallet Distribution Assumptions on DG modelling

Distribution	Reaction Speed	Veto Success Rate (%)	Mean Time to Veto (hours)
Decentralized	Fast	100	15
	Normal	100	57
	Slow	100	66
Centralized	Fast	100	75
	Normal	92	90
	Slow	2	165
Original	Fast	100	60
	Normal	100	72
	Slow	97	87

Table 13. Veto Success rates and time to Veto for different wallet distributions and reaction times

3. Dilution attack (Cluster A)

The results are shown in Figure 14.

- Compared to the simulation in Cluster B, coordinated attacks on the Lido protocol with significant success become a significant threat when the protocol becomes more centralized

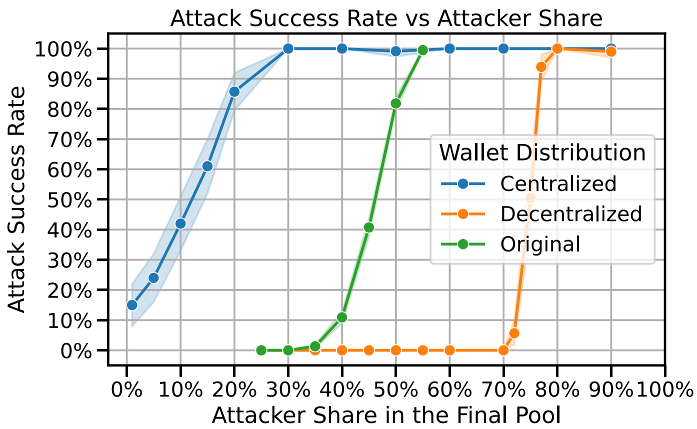


Figure 14. Attacks success rate vs attackers' share for different wallet distributions

4.2.2 Impact of Wallet Distribution Assumptions on DG modelling

- In the worst-case centralized distribution scenarios, even attacks with almost no capital have non-zero chances of success, requiring the protocol to be more robust in case of future centralization

4. Governance Dynamics of Minority and Majority Groups (Cluster B).

The results are shown in Figure 15.

- To protect the interests of minority groups, represented by a share of active voting group in the protocol, further balance decentralization is beneficial, as it is more likely that wallets in the minority group will have sufficient funds in time to veto the proposal that harms them
- In more decentralized wallet distributions, minority groups with as little as 20% share of the active voting wallets were able to defend their interests successfully and reach the first Veto threshold. In the case of centralized distributions, even an 80% share in the active voting wallets did not guarantee group interest protection, as in many cases, actors were too Slow to react before the proposal was automatically executed

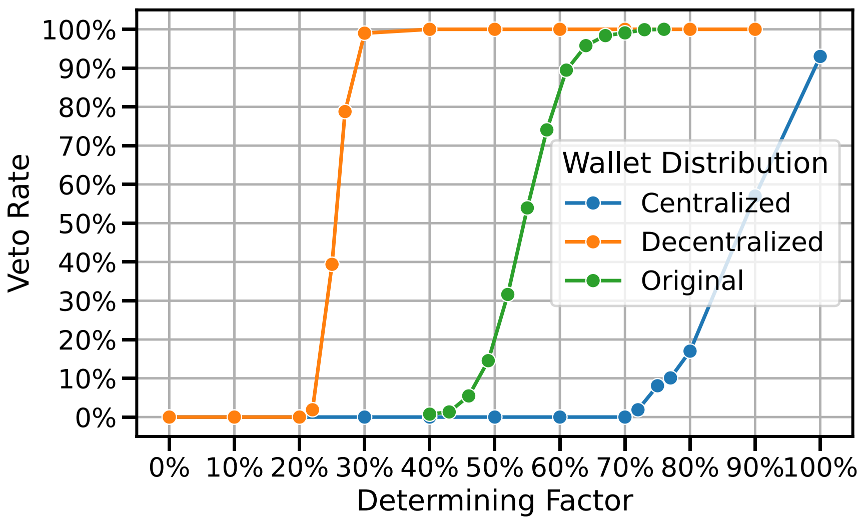


Figure 13. Veto rate success of minority group based on their share in the large community for different wallet distributions

5. Impact of Bribing in Different Token Distributions (Cluster C)

The results are presented in Table 14.

- When the attacker tries to bribe voting actors instead of diluting the Veto threshold, there is a significantly smaller amount of token supply needed to perform an “ideal” attack (where any actor could be bribed with their own balance + 1 token), but in the distribution, the number of actors to be bribed is usually quite significant to attempt in real life

4.2.2 Impact of Wallet Distribution Assumptions on DG modelling

Distribution	Early Responders (Count)			Early tokens share relative to total supply (%)	Amount of total supply to bribe by attacker (%)
	Median	Min	Max		
Centralized	262	218	316	1.1	0.1
Original	248	205	305	1.8	0.8
Decentralized	237	192	288	3.9	2.9

Table 14. Summary statistics of token distributions for Bribing attacks. Early reaction actors are Quick and Normal actors that are able to postpone proposal execution by initiating Veto Signalling

- **Decentralized distributions** require significantly higher bribery costs to influence early responders due to the increased number of actors holding veto-critical tokens
- **Centralized distributions** allow attackers to achieve influence with minimal bribery costs because Veto power is concentrated in fewer wallets
- **Original distributions** balance bribery costs and actor response dynamics, aligning with expected governance behaviors

6. Threshold Combinations and Wallet Group Dynamics

The distribution of tokens per wallet is given in Table 15.

Wallet Distribution	Total Token Share (%)	
	Mean	Median
Decentralized	0.0503	0.0171
Original	0.0503	0.0030
Centralized	0.0503	0.0074

Table 15. Mean and median token shares per wallet for different wallet distribution

- **Decentralized Distribution**
  - Small wallet groups efficiently achieve Veto Signalling due to the even distribution of tokens

4.2.2 Impact of Wallet Distribution Assumptions on DG modelling

- Governance actions remain accessible to a wider range of participants, reducing the likelihood of governance bottlenecks
- **Centralized Distribution**
  - Governance relies heavily on single-wallet Veto Signalling, increasing the risk of governance delays or vulnerabilities
  - Larger groups cannot effectively achieve Veto Signalling, limiting collaborative decision-making
- **Original Distribution**
  - Provides a balanced approach where Veto Signalling remains accessible to smaller groups, maintaining efficiency while avoiding over-reliance on single wallets
  - Serves as a middle ground, balancing inclusivity and concentration

What's being observed

- The future decentralization of token distribution is favorable across the board. It improves Veto success rates, reduces bribery risks, and facilitates faster governance reactions
- Long-term centralization of funds has the potential to pose significant governance challenges, including, but not limited to, delays and vulnerability to attacks due to lack of timely response

Recommendations

- Develop tools to analyze governance engagement and closely monitor governance participation throughout the DG lifespan
- Aim to provide a variety of solutions and alternatives within the Lido ecosystem to support and encourage funding decentralization and greater system stability
- Safeguards are needed to maintain the ability to adjust model parameters in the future if the distribution of wallets in the protocol moves toward greater centralization

4.3 Overall DG design evaluation

4.3.1 Thresholds

The threshold parameters in the Dual Governance design are critical to balancing inclusivity, security, and operational efficiency. The simulation results confirm that the chosen Veto Signalling threshold of 1% and Rage Quit threshold of 10% are well suited for most simulated scenarios, ensuring sufficient time for stakeholder participation without introducing undue governance delays.

Key Observations

- **Veto Signalling:** The 1% threshold effectively deters small-scale attacks and facilitates timely response by active participants (4.1. Cluster A). Simulations showed that success rates dropped sharply past the 1.5% threshold, confirming the appropriateness of the current threshold to balance accessibility and protection against abuse. Reaction times were a critical factor, with quicker actors significantly reducing the time to reach thresholds

- **Rage Quit:** The 10% threshold ensures that stakers can exit efficiently without impacting the protocol stability (4.1. Cluster A). This threshold demonstrates consistent success across scenarios, even with slower actor reaction times, highlighting its robustness

Key Suggestions

- The current 1% and 10% thresholds work appropriately in most simulated scenarios but it is worth continuously monitoring governance participation to ensure sufficient participation and funds reaction time for core groups in stETH holders (4.2.2)
- Consider mechanisms to incentivize faster reactions among large token holders to improve timely responses and the degree of participation in critical governance decisions (4.2.1)

Finding optimal parameter ranges is complicated and, in many cases, unnecessary, because 1) we cannot clearly define the utility function and 2) the significant part of DG design decisions is based on model assumptions (3.6).

4.3 Overall DG design evaluation

4.3.1 Thresholds

However, from the results described in Chapter 4, especially from the analysis of parameter values in simulations where “something started to break”, we can make a set of preliminary conclusions and suggest “reliable” threshold intervals.

“Reliable” parameter range estimations:

- **Veto Signalling “reliable” threshold range is 0.75% - 1.5%**
  - From auxiliary calculation in 4.2.2. **Impact of Wallet Distribution Assumptions [Notebook]**, starting from an R1=0.75% Veto threshold, the number of wallets that could support coordinated attacks drops significantly
  - From Cluster A - Varying Veto Thresholds: success rate of reaching Veto Signalling drops sharply past an R1=1.5%
- **Rage Quit “reliable” threshold range is 7.5% - 12.5%**
  - From auxiliary calculation in Cluster D **Long-Term Lock of Dual Governance with Constant Rage Quit [Notebook]**, R2=5% significantly decreased the capital required for Rage Quit Loop attack without providing significant upside for achieving Rage Quit in time, and R2=7.5% is the next relatively stable step from it
  - From auxiliary calculation in 4.2.1., **Impact of Slow Actor Reaction Assumptions [Notebook]**, starting from an R2=12.5% Rage Quit threshold, the ability of Slow actors starts to reach Rage Quit decays significantly already at 30 day Slow actor max delay, which poses significant model risks from DG participation assumptions

4.3.2. Timelocks

Dynamic timelocks are a foundational element of DG, enabling stakers to signal dissent while providing adequate reaction windows for governance decisions. Simulations confirm that timelock durations are well calibrated to support governance participation and reaction on proposals without excessive delays.

Key Observations

- **Timelock Efficiency:** Timelocks were shown to provide sufficient reaction time for all actor groups to engage in Veto Signalling or Rage Quit, even under adverse conditions (4.1. Cluster A)
- **Veto Signalling Loops:** Prolonged Veto Signalling by malicious actors can delay proposal execution, with delays reaching up to 45 days for coordinated attackers with a 9.9% share (4.1. Cluster C). However, these loops do not completely paralyze the system, as proposals can still proceed during cooldown and deactivation states
- **Rage Quit Loops:** Repeated exploitation of the Rage Quit mechanism can lead to governance bottlenecks, especially in larger pools, due to the fixed withdrawal throughput and ETH ecosystem underlying validator design. A large stakeholder going rogue in Lido could extend the duration of governance disruptions significantly but probability of this is extremely low due to required capital restrictions (4.1. Cluster D)

Recommendations

- Consider additional mechanisms that could be used to update timelock durations based on wallet distribution and reaction time parameters for long-term scenarios to ensure alignment with governance dynamics, as seen in the sensitivity analysis (4.2.2)

4.3.3 Design Decisions

The design decisions of the DG system, including Veto Signalling, Rage Quit mechanisms, and dynamic thresholds, demonstrate strong alignment with the protocol's goals of inclusivity, security, and resilience. However, a few long-term scenarios in the sensitivity analysis highlight potential issues with fixed thresholds and potential areas for refinement.

Key Observations

- **Veto Signalling Effectiveness:** The mechanism effectively prevents harmful proposals but is sensitive to reaction times and token distribution (4.1. Cluster B). Protocol upgrades that are urgent, but non-critical enough to utilize circuit breaker committees, could be locked for the maximum Veto Signalling delay and pose risks to governance integrity
- **Rage Quit Resilience:** While robust, the Rage Quit mechanism is susceptible to exploitation during prolonged bottlenecks, particularly in large pools where withdrawal throughput is constrained by Ethereum design decisions (4.1. Cluster D).
- **Bribing Risks:** Bribery provides a relatively cost-efficient attack vector compared to dilution, particularly when targeting Quick actors (4.1. Cluster C). Simulations showed significantly lower resource requirements for successful bribery, especially with centralized token distribution
- **Sensitivity to Token Distribution:** Centralized token distributions increase susceptibility to attacks and reduce inclusivity, while decentralized distributions improve Veto success rates and mitigate bribery risks (4.2.2)

Recommendations

- Develop anti-bribery mechanisms, such as temporary locking of rewards for escrowed funds, to safeguard against the exploitation of Quick actors, especially in the last hours of the 5-day Veto window
- Monitor and add levers to adjust future DG parameters to mitigate risks associated with extreme centralization scenarios (4.2.2).
- Enhance simulation tools to provide real-time insights into DG performance and inform proactive governance adjustments

5. CONCLUSIONS, RECOMMENDATIONS AND FUTURE RESEARCH

5

5. Conclusions, Recommendations and Future Research

5.1. Conclusions

Throughout the engagement between Lido and CollectifDAO, the team has developed and conducted agent-based simulations to assess the upcoming Dual Governance system for Lido. The research confirmed the robustness, inclusivity, and adaptability of the proposed governance model, while also highlighting potential areas for refinement.

Key achievements of this research include

1. Performance Validation

- Simulations verified the functionality of the proposed DG thresholds, timelocks, and other design decisions under both normal and adversarial conditions.
- The 1% Veto Signalling threshold and the 10% Rage Quit threshold were confirmed to be well suited for stakeholder participation, safeguarding against governance abuse while ensuring operational efficiency

2. Scenario Analysis

- Simulated scenarios provided in the GitHub repo encompassed regular governance flows, coordinated attacks, malicious exploitation, and extreme stress scenarios
- Results demonstrated the ability of DG to deter most attack vectors, including bribery and Veto Signalling loops, given sufficient participation and decentralization

3. Sensitivity Analysis

- The DG model remains robust to moderate changes in parameters such as reaction times and token distributions, and shows sufficient stability in the most future scenarios

5.2. Recommendations

To enhance the resilience and adaptability of Dual Governance, the following recommendations are derived from the analysis and findings detailed in this report:

1. Parameter Monitoring and Adjustment

- Maintain the current Veto Signalling (1%) and Rage Quit (10%) thresholds, but establish processes for regular monitoring of governance participation and explore solutions for reaction time dynamic updates (2.5, 4.3.1)
- Establish pipelines to effectively engage with large token holders to improve the speed of reactions during critical governance decisions and ensure timely participation (4.2.1, 4.3.1)

2. Mitigation of Exploitation Risks

- Consider extending signalling escrow minimal lock times towards days, as it could significantly help reduce vulnerabilities in Quick-actor bribery scenarios with "last minute" bribing swings before proposal scheduling. Additional withdrawal lock on escrow during the last 12+ hours before potential proposal scheduling could significantly constraint bribing attacks without major problems to regular actors (Cluster C, 4.3.3)
- Increase transparency of proposal impacts to deter malicious influence and enhance stakeholder trust in the system (4.3.3)

3. Ensuring Long-Term Governance Stability

- Consider developing flexible thresholds to adapt to future changes in token distribution and potential centralization risks (4.2.2, 4.3.3)
- Evaluate timelock durations periodically to ensure they align with evolving token holder dynamics and governance requirements (4.2.2, 4.3.2)

These recommendations are based on the insights gained from the simulations and focus on ensuring that DG remains resilient, inclusive, and adaptable under varying governance conditions.

5.3. Areas for Improvement and Future Research

1. Enhanced Simulation Tools

- Expand modelling to include external factors such as market volatility and cross-protocol interactions for a holistic evaluation of DG performance in real-world conditions
- Incorporate more granular representations of smaller stETH holders to capture their potential impact in edge cases

2. Dynamic Participation Analysis

- Develop tools to analyze governance engagement and closely monitor governance participation throughout DG lifespan

3. Future Governance Risks

- Investigate the impact of token holder concentration due to institutional actors or evolving market dynamics
- Explore new governance models or hybrid approaches to address emerging challenges, such as unexpected centralization or technological constraints

5.4. Summary

This research provides a comprehensive evaluation of Dual Governance through advanced simulations and scenario testing.

It validates the core mechanisms of DG, identifies potential vulnerabilities, and provides actionable recommendations for optimization.

By bridging stETH holders and DAO participants, DG strengthens protocol governance, safeguards stakeholder interests, and ensures long-term adaptability in a dynamic decentralized ecosystem.

The findings and recommendations lay the foundation for the successful deployment and continued evolution of the system.