Title

: Rivus Guard – Automated Supply and Borrow Caps

Author

: Tyler Loewen (TRILEZ SOFTWARE INC. dba. Adrastia)

Date

: May 02, 2024

Summary

Rivus Guard is an automated supply and borrow cap controller designed specifically for Aave. The system reduces governance overhead while also allowing for tighter controls and more responsive updates. Not only are risk stewards able to set overarching caps like they're able to today, but they're also able to restrict the daily flow of assets with Rivus Guard.

Thanks to @eboado of BGD Labs for his oversight and guidance in the development and proposal processes.

Background

I am a 29-year-old automation veteran with over a decade of experience building automation programs and infrastructure and a B.Sc. in Computer Science. I started my automation journey in 2009 at SRL – an open-source machine-vision automation platform. After quickly climbing the ranks and serving as an official developer, I founded my own automation platform in 2010, TRiBot, that leveraged reverse engineering and AI.

I incorporated my company, TRILEZ SOFTWARE INC., in 2013 to grow the TRiBot business when its adoption exploded three years into the project. I continued to operate TRiBot for an additional eight years, serving nearly 500,000 total users, nearly 100,000 paying customers, and a high of 14,000 MAU through a team of about 30.

I decided to sell the TRiBot business in 2021 to chase bigger goals. Naturally, I transitioned to crypto – coincidentally, I learned about Bitcoin in 2010 through SRL. While mining with my Pentium D processor didn't produce any Bitcoin, I was fortunate enough to begin buying it in 2011 and later using it to collect payments and pay my international team.

I founded Adrastia after doing work for Compound in 2021, where I noticed deficiencies in the oracle and automation space. Notable work at Compound included listing markets such as Chainlink, providing guidance with their Chainlink-powered hybrid oracle system, and developing a market listing framework that OpenZeppelin later adopted and expanded. I've since branched from Compound, and after nearly three years of full-time commitment to Adrastia, we have a full suite of products.

To date, Adrastia has:

- Oracles
- Price oracles
- Liquidity oracles
- Interest rate oracles
- Volatility oracles
- Total supply and borrow oracles
- Utilization (and error) oracles
- Aggregation oracles (supports Chainlink, Pyth, Redstone, DIA, and many others)
- Time-weighted average oracles (arithmetic, geometric, and harmonic)
- Median-filtering oracles
- Min/max oracles
- Credit extension (loan issuance) oracles
- Correlated asset price oracles
- Price oracles

- Liquidity oracles
- Interest rate oracles
- Volatility oracles
- Total supply and borrow oracles
- Utilization (and error) oracles
- Aggregation oracles (supports Chainlink, Pyth, Redstone, DIA, and many others)
- Time-weighted average oracles (arithmetic, geometric, and harmonic)
- Median-filtering oracles
- Min/max oracles
- Credit extension (loan issuance) oracles
- Correlated asset price oracles
- Risk controllers
- Supply and borrow cap controllers
- Interest rate controllers
- PID controllers
- Linear kink controllers
- PID controllers
- Linear kink controllers
- And more
- Supply and borrow cap controllers
- Interest rate controllers
- PID controllers
- Linear kink controllers
- PID controllers
- Linear kink controllers
- And more

Motivation

Since introducing Risk Stewards in late April 2023, there have been35 proposals to update Aave's supply and borrow caps. With onchain activity picking up and Aave continuing to expand, one can expect the volume of proposals to grow. Rivus Guard aims to reduce governance overhead, improving the Aave protocol's ability to scale safely and efficiently.

Furthermore, the automation of supply and borrow caps allows for greater responsiveness and daily updates that would otherwise be impractical. This allows for tighter controls of the flow of capital – the second goal of Rivus Guard.

It should be noted that Rivus Guard is designed to work with two different caps, rather than just one:

- Hard cap

: These can be thought of as debt ceilings. I.e. the maximum total supply or borrow for a market.

- Soft cap

: These effectively work as rate limiters. I.e. the maximum amount that the totals can change in a period of time. They restrict net asset inflows and outflows. They're also referred to as daily caps when measuring and implementing day-to-day changes.

This proposal focuses on automating soft caps, leaving the calculations of hard caps to Aave's risk managers. Soft caps, or rate limiters, provide the same protection as traditional banking's daily limits; they protect against sudden changes

.

Scenario

Imagine a scenario where a risk manager increases a token's [hard] supply cap by 20%. Suppose a black swan event occurs – let's say a market manipulation-based attack where the value of the token skyrockets momentarily. An attacker can now take full advantage of the increased cap by supplying all their newly acquired tokens up to the capped amount and borrowing the maximum amount of stablecoins against it. The position could lead to bad debt as the value of the token rapidly returns to baseline.

Soft caps can greatly limit the impact of such black swan events. Let's say the hard supply cap was increased by 20%, and a soft cap of 1% daily increases was used. The soft cap would reduce the negative impact up to twenty-fold.

This is just one example, but the principle is that rate-limiting inflows and outflows through soft caps can protect the protocol against sudden, unforeseen changes

.

Specification

Rivus Guard introduces daily adjusting supply and borrow cap automation through both soft and hard caps. While hard caps are still manually set by risk managers, the introduction of soft caps gives risk managers more flexibility while also increasing the economic security of the protocol.

Rivus Guard's caps will automatically adjust depending on criteria and parameters agreed upon by governance and risk stewards. Two main components handle these updates:

1. Controllers
2. Computers

Components

Controllers

Controllers are top-level contracts that are configured to write to the Aave Config Engine. They're designed on a per-market basis to source data (from computers) and then apply clamping before pushing the new cap. Clamping is based on:

- Absolute min/max
- Relative change (increases and decreases are defined separately)
- Absolute change (increases and decreases are defined separately)

In essence, controllers guard the protocol against excessive cap fluctuations and delegate the responsibility of cap computations to computers.

Computers

Computers are where the magic happens – they form the algorithms that calculate new values for the caps. With a simple open-source (MIT-licensed) interface, anyone can build these to create a wide variety of algorithms. The following are the pre-built computers that exist today.

Manual computers

Utilizing these computers in Rivus Guard would make it function like the Risk Stwards contracts today – Aave's risk managers manually adjust the caps. Unlike the current system, the benefit of this approach is that the overarching controller can smoothen out changes across multiple updates over time.

Mutation computers

These computers introduce automation by sourcing data from the chain and applying mutations – mathematical transformations to adjust the data.

The existing mutation computers support scalars and offsets. Offsets are useful when spinning up new markets where

scalar adjustments would be slow.

There are two existing mutation computers that differ by their source of data, described below.

Mutation computers – straight from the source

With this approach, current supply and borrow amounts are fed into the computer before being mutated. The current totals can be scaled and offset by configurable amounts. Aave's risk managers would determine the mutation parameters and set hard caps.

Mutation computers – sourced from oracles

Reading the current total supply and borrow amounts directly from the Aave protocol not only opens up the possibility of just-in-time attacks, but such an algorithm may be too noisy. Various approaches can be applied to strengthen the data. Delays of a few blocks, time-weighted averaging, and median filtering can all be used to enhance the data.

One caveat of using such a computer is that Adrastia is the only oracle solution to provide such data feeds, requiring additional trust in Adrastia Oracles, unlike with the other computers.

Check out Adrastia's Aave v3 Total Supply & Borrow Oracle on Polygon to analyze the performance of our 24-hour geo-mean time-weighted averages.

Updation Process

Utilizing any automation platform such as Adrastia, Chainlink, or Gelato, here's a flow chart of the process of how new supply and borrow caps are computed and pushed.

Automation infrastructure will continually monitor Rivus Guard, checking for needed updates. When an update is needed, an automation worker will promptly send an update transaction with the controller working in unison with the computer to calculate the new cap. Once computed, clamping is applied before sending the update to the Aave Config Engine. Below is a flow chart describing the clamping process.

Demos

Rivus Guard demos have been running on Polygon since September 2023. Note the change of config on April 13 that allowed decreases. Check out our UI for more information:

- Supply cap controller
- Borrow cap controller

Summary

Rivus Guard introduces the notion of soft caps, i.e., daily caps. We reduce attack surface area by limiting the collateralization and borrowing that can occur in a day.

Aave's risk managers are still responsible for setting debt ceilings and can quickly do so with less governance overhead, thanks to the controller's guard rails.

Audits

Zellic has audited all contracts used in Rivus Guard, and the details are in theAdrastia v4.2 audit report.

FAQ

- What's the uptime of Adrastia?
- We've had 100% uptime since launching ouruptime monitoring system.
- We've had 100% uptime since launching ouruptime monitoring system.
- Where can I find performance metrics for Adrastia's Aave oracle workers?
- Metrics related to total fees, gas prices, mining delays, and more can be foundhere.
- Metrics related to total fees, gas prices, mining delays, and more can be foundhere.
- How do status checks work for Adrastia?

- Heartbeat signals are sent every 30 seconds if the worker has recently read or written to the blockchain. Downtime is recorded if there is no heartbeat for 2 minutes or more.
- Heartbeat signals are sent every 30 seconds if the worker has recently read or written to the blockchain. Downtime is recorded if there is no heartbeat for 2 minutes or more.
- What steps have been taken to ensure the reliability of Adrastia?
- We have four geographically distributed bare-metal dedicated servers across California, New York, Miami, and Switzerland to handle failures across multiple servers and regions.
- We use two different dedicated server providers to handle provider-wide outages.
- We use four distinct RPC providers for every chain to handle RPC provider downtime.
- Rolling updates prevent newly introduced bugs from taking down the entire network.
- Datadog, BetterStack, and Grafana powered monitoring and altering allow us to identify and quickly respond to problems.
- RHEL-based service orchestration automates the quick recovery of faulty services.
- We have four geographically distributed bare-metal dedicated servers across California, New York, Miami, and Switzerland to handle failures across multiple servers and regions.
- We use two different dedicated server providers to handle provider-wide outages.
- We use four distinct RPC providers for every chain to handle RPC provider downtime.
- Rolling updates prevent newly introduced bugs from taking down the entire network.
- Datadog, BetterStack, and Grafana powered monitoring and altering allow us to identify and quickly respond to problems.
- RHEL-based service orchestration automates the quick recovery of faulty services.
- What steps have been taken to ensure efficient gas spend?
- Our four worker nodes are set up to fire incrementally with continually increasing gas prices. This ensures minimal gas spend while still being responsive amidst network congestion.
- Mutable change thresholds modulate gas consumption and can be increased to reduce spending.
- Our four worker nodes are set up to fire incrementally with continually increasing gas prices. This ensures minimal gas spend while still being responsive amidst network congestion.
- Mutable change thresholds modulate gas consumption and can be increased to reduce spending.
- What's the precedence of the clamping mechanism?
- Delta change clamping takes precedence over the changed min/max to prioritize stability.
- The more restrictive limit is used between absolute and relative change limits.
- Delta change clamping takes precedence over the changed min/max to prioritize stability.
- The more restrictive limit is used between absolute and relative change limits.

Next Steps

Should the Aave community be interested in Rivus Guard, feedback is required to determine the exact configuration.

Copyright