[TEMP CHECK] Integrate Oval for the BAL & SNX Ethereum V3 Markets

Title: [TEMP CHECK] Integrate Oval for the BAL & SNX Ethereum V3 Markets

Author: UMA

Date: 2024-01-31

Summary

This proposal seeks to integrate Oval developed by UMA into the BAL and SNX Ethereum V3 markets. This pilot program

will enable Aave DAO to capture MEV associated with oracle updates from liquidations that occur in the BAL & SNX markets. This proposal is purposefully small in its initial scope, targeting only two isolated pools (BAL & SNX), to allow Aave to experiment with MEV capture with a bounded, low-risk pilot.

Motivation

Aave incentivizes third parties to liquidate Aave debt positions that have become distressed through a liquidation bonus. These liquidations generate enough profit that searchers compete to send their liquidating transactions immediately after the Chainlink price feed update. The MEV from Aave liquidations has benefitted searchers, block builders and validators, but not Aave protocol, which could have generated up to $62.2MM

(Jan 2021 to Jan 2024) via Oval.

Oval allows Aave to capture the majority of this MEV as revenue. Oval is a MEV capture tool for Oracle Extractable Value built on Chainlink Data Feeds and Flashbot's MEV-Share infrastructure. Oval requires no smart contract code changes to integrate.

Specification

1. What is Oval?
2. Oval Revenue
3. Chainlink & Oval
4. Implementation
5. How Oval Works?
6. Pilot Program Updates
7. Support
8. Security
9. Other
10. Glossary

What is Oval?

Oval enables OEV capture by wrapping Chainlink price updates as they are pushed onchain so that OEV cannot be extracted without the consent of the protocol.

With Oval, when searchers perform a liquidation on Aave an order flow auction is triggered using Flashbots' MEV Share—a trusted tool that allows MEV searchers to compete for MEV extraction offchain.

To extract the OEV created by an update, searchers must submit a winning bid, most of which is paid to the protocol as revenue. The winner of the auction gets the right to backrun the oracle update transaction—performing the liquidation by adding their transaction to the block immediately after the price update

.

If no bid is received by the end of the auction window, the Chainlink price is automatically released and Aave liquidations function as normal.

The diagram below showcases, at a high level, this flow.

[

](https://lh7-us.googleusercontent.com/skZcZPjPMLEQlr_gY0te7Fp1f-GwZ00BvDe1fAtmcG_b-rQxn12PQFl8ipAWjEo9fvpgxEvEWHCNnCZ5wk8YhSzLYQ86RYk-wHvXdT3yt8cPHJTx_oInXFAt-7fgxVts0XkQILVfrqRF9VELHJQACCU)

This approach utilizes the solid foundation of Chainlink price feeds and MEV-Share to extract OEV from liquidations. Oval is applicable to all markets within Aave that employ Chainlink price feeds.

As a comparison, the diagram below shows the current Aave liquidation process.

[

](https://lh7-us.googleusercontent.com/4791keGhzQvesB2Bsd_RWk358kG-uBvNtIyfYJ21jNp3powU5wbRbIomllo85EsLJjE1nM0tzv07SzHmLXelgTcNjzVQoxDed5J7Oj_IISBc4xhTog4EqrhqvtM8A6g7n2ruSeLD54159LzBQOnh3r4)

Oval is fully compatible with the liquidation fee the Aave protocol currently takes on all liquidation bonuses.

Oval Revenue

As mentioned earlier, Oval enables Aave DAO to capture up to 90% of the liquidation bonus. The liquidation bonus depends on the asset used as collateral. These bonuses range between 5-10% and can be found at the bottom of the dashboard.

The data below offers an in-depth analysis of the potential Oval recapture across the BAL & SNX markets, from January 2021 to January 2024.

Market

Liquidations

Total collateral Liquidated

Potential Oval Revenue

BAL

112

$961,403.07

$76,139.67

SNX

156

$681,286.40

$45,986.83

Source: Aave OEV (Jan 2024) with methodology

Given the fundamental differences between isolated and non-isolated markets, we recommend the integration of Oval initially within isolated markets for this pilot program. This ensures that Oval's operational scope is strictly confined to these BAL & SNX markets, thereby eliminating any impact on other markets within the Aave ecosystem.

Despite the relatively modest potential for Oval recapture in these isolated markets, this small scope was deliberately chosen to enable the Aave DAO to gain confidence in the integration's performance. The successful integration of Oval within the BAL & SNX markets will serve as a compelling indicator of its applicability and efficacy for additional markets.

Aave DAO could have profited over $62M if Oval had been integrated into the entire protocol over the past 3 years.

Chainlink & Oval

Oval is not an oracle, and it does not replace Chainlink.

- Using Oval means still using Chainlink price feeds. Oval wraps incoming prices from Chainlink, shielding them from MEV searchers.
- The Oval contract will use the Chainlink price feed and initiate an auction for the OEV searchers to bid for access to liquidations.
- No additional pricing logic is inserted.
- If no one participates in the auction, the price update will be released after 36 seconds (3 blocks).

Implementation

Deploying Oval requires two simple steps:

1. Deploy Aave's own instance of the Oval smart contracts for the BAL and SNX markets (UMA is happy to assist with this).
2. Update the BAL and SNX market's oracle address from the Chainlink price feed to the Oval smart contract that points to the same Chainlink price feed.

These steps are further detailed in ourdocs. UMA is committed to providing ongoing support to ensure a successful implementation of Oval.

How Oval Works

Integrating Oval requires no code revisions to Aave smart contracts. Currently, Aave smart contracts receive price data directly from Chainlink price feeds. To integrate Oval, Aave would instead receive Chainlink price data through Oval smart contracts. It's crucial to note that Oval cannot modify Chainlink price data

in any way. The only function of Oval smart contracts is to temporarily lock the latest Chainlink price from Aave so it can be auctioned off to MEV searchers. The steps below outline the basic Oval flow and how it integrates with Chainlink and MEV-share. Please see the docs page here for more info on this flow:

1. Chainlink price update is released to the public Ethereum mempool.
2. Searchers see this update and submit liquidation bundles to the Oval Node to backrun the update and perform a liquidation.
3. The Oval Node creates a transaction that unlocks the newest price (unlockLatestValue). This unlock transaction is added to the searcher bundle along with refund instructions and forwarded to MEV-share. This is done for each searcher bundle sent to the Oval node.
4. MEV-share forwards all bundles to all connected builders; this includes all themain block builders. The builders run a standard Flashbots auction, selecting the winning bundle based on the builder payment. Because of the refund instructions, the builder is required to refund most of this payment to the protocol (Aave).
5. The refund will be directed to a multi-sig controlled by Aave DAO stakeholders & UMA.

6. Oval's revenue distribution: For the pilot program, we propose utilizing the revenue to fund Aave OEV research (i.e. to evaluate the efficiency of Oval on the BAL & SNX Markets).
7. The refund will be directed to a multi-sig controlled by Aave DAO stakeholders & UMA.
8. Oval's revenue distribution: For the pilot program, we propose utilizing the revenue to fund Aave OEV research (i.e. to evaluate the efficiency of Oval on the BAL & SNX Markets).
9. The winning bundle is selected by the builder and is sent within the proposed block to the proposer.
10. The proposer appends the block to the Ethereum chain. The relevant parts of this block execute the following actions, in this order:
11. Oval unlock transaction
12. Winning searcher bundle (may include Chainlink price update)
13. Oval unlock transaction
14. Winning searcher bundle (may include Chainlink price update)

Due to possible inclusion delays within the Ethereum MEV/PBS supply chain, in some situations there can be a small delay between steps 4 and 6. For example, if the proposer for a given slot does not use mev-boost (90% of proposers use mev-boost). In this case, the searcher bundle would not land in the same block as the Chainlink update and might execute in a subsequent block. Oval bounds the delay that integration must wait before receiving the latest price to 36 seconds (3 blocks). This means that—in the worst case scenario—a Chainlink update will be delayed 36 seconds (3 blocks). For more information on how this could happen and the mechanism that controls when to release the price see here and here.

Pilot Program Updates

We will create a dune dashboard that will track Oval revenue recapture and provide quarterly updates on Oval's performance within the BAL and SNX markets. These updates will be shared in the "UMA [Oval Updates Thread]" on the Aave forum.

Support

Oval documentation contains all the information to perform an integration. In addition to these docs, Aave DAO will benefit from the dedicated support of the UMA team to facilitate this integration process.

To ensure seamless collaboration and efficient problem-solving, we propose establishing a direct communication channel between the UMA and Aave teams.

Security

- To ensure the security of this system, Oval has completed an audit by Open Zeppelin (public report available soon) and has an additional security bounty of up to $1M for any vulnerabilities that are identified.
- UMA has worked closely with Flashbots to develop Oval. Flashbots has updated the MEV-Share design to add support for Oval, and is committed to helping support this pilot.

Other

- The integration requires no modifications to Aave's UI and does not impact any normal user actions of creating new positions, increasing debt or repaying loans.

Glossary

Maximal Extractable Value (MEV):

the maximum value that can be extracted from block production in excess of the standard block reward and gas fees by including, excluding, and changing the order of transactions in a block.

Oracle Extractable Value (OEV):

a subset of MEV created by oracles posting new price data onchain.

Oracle Value Aggregation Layer (Oval):

an OEV capture product developed by UMA

MEV-Share:

an orderflow auction infrastructure built by Flashbots that enables MEV capture for private transactions.

Liquidation Bonus:

a financial incentive for participants to execute liquidations.

Useful Links

- Aave Liquidations
- Oval documentation
- Flashbots MEV-Share
- Aave OEV Dashboard
- Oval Launch Post

Disclaimer

This proposal is powered by Skywards. The Aave Chan Initiative is not directly affiliated with UMA Team and did not receive compensation for creation this proposal.

Next Steps

1. If consensus is reached on this [TEMP CHECK], escalate this proposal to the Snapshot stage.
2. If the Snapshot outcome is YAE, this proposal will be escalated to ARFC stage
3. Publication of a standard ARFC, collect community & service providers feedback before escalating proposal to ARFC snapshot stage
4. If the ARFC snapshot outcome is YAE, publish an AIP vote for final confirmation and enforcement of the proposal

Copyright