## Introduction

The best solution we have to the oracle problem is using economic incentives to coordinate humans. Different oracles have combined discounted future cash flows, skin in the game, and reputational/legal risk in hopes of only putting accurate data on-chain.

The most transparent and reliable is skin in the game

: that at any moment in time, it will cost more money to attack an oracle than could be earned by doing so. This idea was introduced by @vbuterin in his 2014 paper SchellingCoin: A Minimal-Trust Universal Data Feed.

In this post we will introduce a way to increase the amount of skin in the game defending the data, which we call Sovereign Security. Sovereign Security introduces an escalation pattern that would allow a Schellingcoin oracle (like UMA's) to escalate a dispute to a native protocol's token.

## Context

Vitalik's trust-minimized oracle design uses economic incentives to coordinate voters to behave in such a way as to arrive at a Schelling point. The 'coin' refers to the asset that voters in the oracle hold, and represents their economic exposure to the accuracy of the oracle.

In May '21, Vitalik appealed to UNI tokenholders arguing that UNI should become an oracle token, as "modeled after the Augur or UMA design." He explains that "a robust token-based decentralized oracle for a defi project must first and foremost be based on a token with a large market cap."

This was at a time when the temperatures of DeFi summer were melting faces. Below is the Uniswap price chart, flagged at the time of Vitalik's post:

[

only up

1496×1222 72.5 KB

](https://ethresear.ch/uploads/default/original/2X/6/6a327b8855d413d079640ca2231755dc0e67bbd8.jpeg)

At the time Vitalik posted, the price of UNI was what is now known to be its ATH to date, with a market cap of $22.5bn; today it is $3.7bn. Compare that to today's current market capitalization for stablecoins, today at $131bn. In order to secure the entire stablecoin market today, an oracle of this design would need to be valued at over $262bn.

Perhaps there are timelines where a single oracle token is able to grow in (2x) pace with the markets it secures; but those timelines have so far been out of reach. We'd like to propose a different way.

## Sovereign Security

Sovereign security introduces an escalation game pattern that ends with an appeal to the tokenholders of the protocol using the oracle. This contract is already live.

How does it work?

1. The first stage is how UMA operates now, as an optimistic oracle. An assertion is offered as truth, along with a bond. This starts a challenge window for a bonded dispute, which if lodged, would trigger a tokenholder vote to determine the winner of the bonds. The data would be need to be re-asserted.

2. Sovereign security is a path that a developer can choose to enable when integrating with UMA. This is done via the Full Policy Escalation Manager contract.

3. Enabling Sovereign Security introduces an override feature, where a protocol's own on-chain token voting system can be used to resolve a dispute.

4. If tokenholders of the DeFi protocol noticed a bribery attack against the $UMA token, it could vote via on-chain governance to disconnect from UMA's oracle and escalate the dispute to their own tokenholders who would vote in an on-chain, such as we'd see with the Compound Bravo contract.

This design is not conceptually extraordinary. It's not a novel concept to have people govern their own protocol with their own governance token, but what is novel is having on-chain governance with an optimistic oracle system layered on top of it.

What the system enables is for protocols to turn on this kind of protection in a feasible way. We would expect that because this lever can be pulled, it will never need to be pulled

, so long as the cost to attack both systems is still greater than the potential benefit. Protocols do not need to each build their own dispute and voting system, worry about voter participation, or tweak their own tokenomics. Each protocol does not need be an oracle.

## Conclusion and Request for Feedback

For simplicity we have presented this design as escalating to the protocol's native token, and assumed that the native tokenholders would not abuse their power (as if you're already

trusting them with that power.) We acknowledge that this is not always true–the escalation manager is customizable in some useful ways here that we'd be happy to discuss.

How satisfied with this design are you?

We believe that this problem is a sleeping giant, and one that will only rear its head the next time DeFi is going hyperbolic. We think it is necessary to level up our hero now, because otherwise projects will take centralized shortcuts to maintain growth in a hot market.