GFDao Oracle Module - Concept Draft

Summary

Introduction

GFDao Oracle Module - Objective

- Provide trusted reference prices to Ghost Finance products.

Core On-chain Components

- Ghost Signer - GS

- The `GhostSigner` provides Ghost Finance's trusted reference price. In short, it works by maintaining a whitelist of price feed contracts which are authorized to post price updates.

  Every time a new list of prices is received, the `median` of these is computed and used to update the stored value.

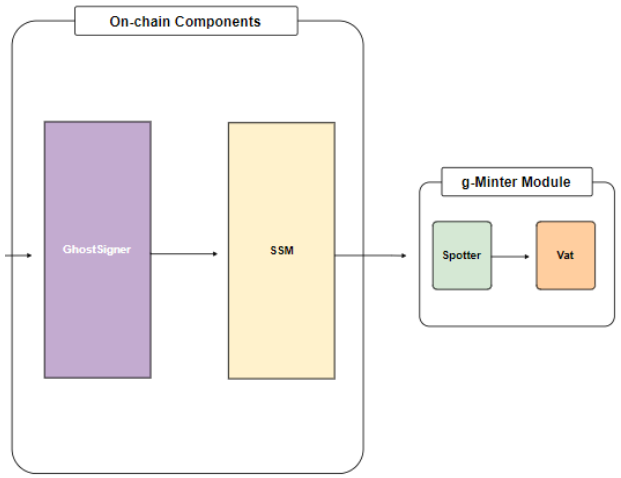
  The `GhostSigner` has permissioning logic which is what enables the addition and removal of whitelisted price feed addresses that are controlled via governance. The permissioning logic allows governance to set other parameters that control the Ghost Signer's behavior — for example, the `bar` parameter is the minimum number of prices necessary to accept a new median value.

- Signer Security Module - SSM
  - SSM - The `SSM` (named via acronym from "Signer Security Module"):

    Ensures that new price values propagated from the Oracles are not taken up by the system until a specified delay has passed.

    Values are read from a designated DSValue contract (or any contract that implements the `read()` and `peek()` interface) via the `poke()` method; the `read()` and `peek()` methods will give the current value of the price feed, and other contracts must be whitelisted in order to call these.

    An SSM contract can only read from a single price feed, so in practice one SSM contract must be deployed per collateral.



On-chain Core Components

Other On-chain Components

- Spotter
  - The `Spot` liaison between the oracles and the core contracts. It functions as an interface contract and only stores the current `ilk` (a given collateral type) list.

- Vat
    - The Vat is the core Vault engine of dss (Core System Accounting). It stores Vaults and tracks all the associated Dai and Collateral balances. It also defines the rules by which Vaults and balances can be manipulated. The rules defined in the Vat are immutable, so in some sense, the rules in the Vat can be viewed as the constitution of dss.

Core Off-chain Components

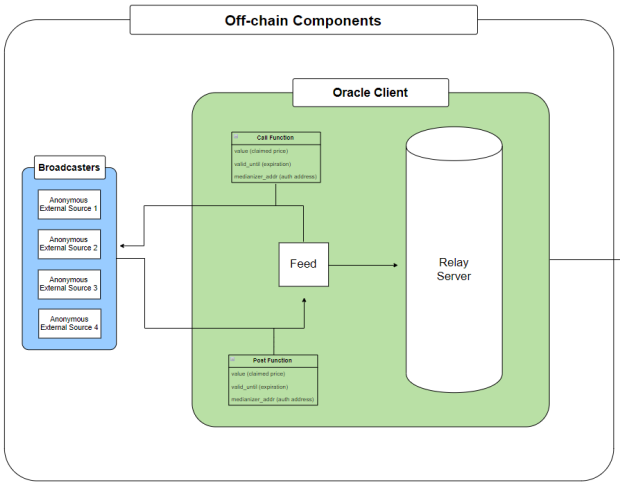
- Broadcasters
    - The broadcasters will be anonymous members of GFDao's community that will deposit XXX GHO tokens as *Minimum Stake Deposit* to assume this protocol role.

      They will report assets prices and companies' valuations every time the `Feed` requests this information.

      Inconsistent work or malicious actions can lead to partial or total slash of MSD. The Broadcasters will receive rewards from Ghost Finance reserve for executing this role.

      In the future, the Ghost Oracle Module can possibly sell data products to other protocols and companies and the costs to run the system will be covered by these products.

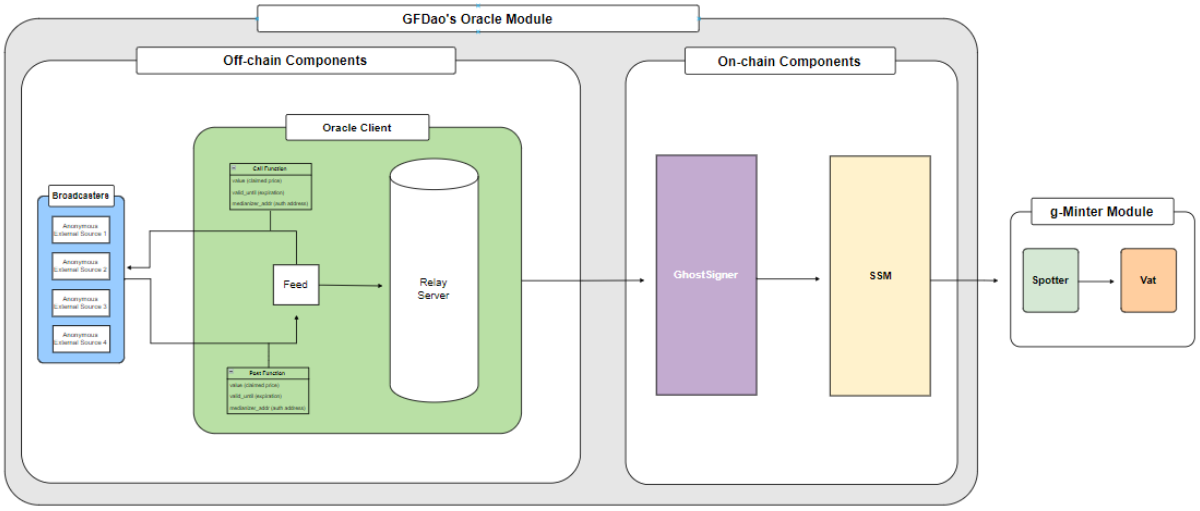
- Oracle Client
    - Feed
        - The `Feed` runs a Feed client which pulls prices through Setzer, signs them with an ethereum private key, and broadcasts them as a message to the secure scuttlebutt network.
    - Relayer
        - Relayers monitor the gossiped messages, check for liveness, and homogenize the pricing data and signatures into a single ethereum transaction.



Off-chain Core Components

Other Off-chain Components

- Data Models
    - The data model for a collateral type is the formula used by the oracles to determine its price. It is comprised of:
        - List of price sources: A list of trading pairs that include the collateral or private companies' intelligence data providers, typically coming from 3 to 5 exchanges or data providers.
        - Quorum: Minimum number of feeds necessary to provide price information for the Oracle price to be considered valid.
        - Feed models: How the individual feeds aggregate the price sources. Typically, "median" is used.
        - Oracle models: How the Oracle will aggregate the price information from the individual feeds. Typically, "median" is used.



Oracle Module Overview

References

- Reference Docs - On-line Components
    - GhostSigner - Median Documentation
    - GhostSigner - Medianizer2 Contract
    - SSM - OSM Documentation
    - Spotter - Spot Documentation
    - Vat - Vat Documentation

- Reference Docs - Off-line Components
    - Readme Oracles v2
    - Collateral Onboarding Guide
    - Maker Protocol 101 Deck