

So this has been coded. The resolve token mentioned is what I'm asking people to attack. It's the asset that governs the oracle/DAO (potentially sidechain).

We first start with something that is a blatant pyramid. A user can buy into the smart contract and receive bonds. Those who buy early, get bonds cheaper than those who buy later on.

The money spent on bonds and the time they were purchased is recorded within the smart contract.

When a user sells back to the smart contract, the price of bonds decreases.

When bonds are sold, the user get an amount of ether back along with a secondary "resolve" token.

The amount of resolve tokens a user receives is based on a "loss" & "hodl" multiplier. The more the bonds depreciate, the greater the loss multiplier. The longer the bonds were held (relative to current holdings in the contract), the greater the hodl multiplier.

$$\text{resolve tokens} = \text{investment} * (\text{investment} / \text{return}) * (\text{hodl} / \text{average hodl})$$

This way of minting resolve tokens harnesses market forces to drive their fair distribution. Only those that have sacrificed the most money and time get the most resolve tokens.

These tokens can then be used to back watchers that run the oracle. The oracle must respond to request tickets within a set time window.

Resolve tokens also have a deflationary component to "tighten" the ring of their distribution. They can be staked back into the contract to earn from the dynamic "friction fee".

$$\text{friction fee} = \text{resolve tokens outside contract} / \text{total resolve tokens}$$

The slope of the pyramid's bonding curve should also be dynamic.

$$\text{slope} = \text{ether in dividends} / \text{ether in pyramid}$$

If someone attacks the resolve supply, the pyramid will steepen as people sell bonds to meet the demand for resolve tokens.