USDO

(USDoge Collateralized Stablecoin)

A Hyper-collateralized Algorithmic Stablecoin, designed for volatile & decentralized environments

Proposed by Studio Nova, for the consideration of Nova DAO

STUDIO NOVA

NOVA DAO

Note that this proposal does not in any way constitute any direct deliverable or guarantee of the works contained within, nor does it serve any purpose towards a full audit or technical review of the systems outlined. This proposal highlights only the intended design of said service, and is provided without warranty or guarantee by either Studio Nova, Nova DAO, or its constituents.

Algorithmic Stablecoins and other decentralized or token-based offerings inherently carry risk, which may be increased or decreased as the level of decentralization grows or shrinks. External factors such as chain viability or underlying asset/platform security cannot be mitigated for risk. The Algorithmic Stablecoin functionality proposed below in no way guarantees its functional ability to maintain a USD Dollar pegging, and in no way is regulated, approved, insured or otherwise by any States, agencies, or otherwise.

Stablecoins are not recognized as forms of currency, or as any replacement or competitor to their real world counterparts. In the event of any such proposal being accepted and published under Nova DAO, you accept that Nova DAO is a decentralized organization which makes said tooling available on an educational basis, providing no guarantees or warranties over its intended functionality, or over any losses incurred.

NovaDAO is a Decentralized Autonomous Organization controlled by NOVA token holders. Nova DAO LLC disclaims any responsibility for any outcomes, whether positive or negative, that may arise as a result of actions taken by the NOVA token holders. You acknowledge that the NOVA token smart contract operates autonomously and immutably on the Ethereum blockchain, the continued functionality and presence of the NOVA token are not contingent upon the endeavors of Nova DAO LLC, and ongoing development of NovaDAO is the responsibility of NOVA token holders.

Overview

USDO operates under the assumption that its underlying asset is an extremely volatile token; and as such, rather than increasing adoption/ease-of-access with an additional funding token (as seen in LUNA/UST), it instead relies on hyper-collateralization of a single asset.

This practice removes a heavy amount of abstraction and complexity from existing algorithmic stablecoin approaches, while also providing both a transparent window into the total network collateralization, while mitigating the risk of deliberate/malicious actors holding the ability to directly attack the health of the protocol.

This hyper-collateralization approach depends on this simplicity remaining intact, particularly in ensuring that it is deployed with the intent of serving only one chain per deployment - and in ensuring that said collateralization asset is natively available on said chain, readily available for both deposits and withdrawals without any third party bridging components or otherwise.

The core tenet in hyper-collateralization is in heavily increasing the amount of collateralization required as the underlying asset increases in value, thus requiring a constantly growing collateral pool in order to offset the risks posed by sudden retracement. This collateral is held under a “verify, don’t trust” approach, where direct collateral redemptions are blocked if the collateral falls below a given threshold as the value of the underlying asset experiences volatile price fluctuations.

Across this model, one centralization risk still remains in place; our heartbeat service, and pricing oracles for the underlying asset. While this can be heavily mitigated and fully decentralized on a per-chain basis (pending availability and affordability of pricing oracles), these options would likely not be as readily available on smaller/developing chains.

In incentivizing this approach, USDO proposes that 90% of all fees generated via mint/burn functionality is returned to active collateral stakers, ensuring real yield returns on their underlying asset. The remaining 10% of all fees would be allocated to the heartbeat service maintainer, described later in this document. This is an ideal mechanism for growing the amount of the underlying asset, while not guaranteeing the value of the underlying asset itself - and as such, a suitably liquid asset would be required in order to offset the risks posed by any staking periods.

For this approach, Dogecoin (current market capitalization: $11.3bn as per CoinMarketCap, November 19th 2023) has been chosen to demonstrate the viability of this hyper-collateralization model. We are proposing that we launch the USDO protocol on DogeChain, an developing chain which houses a large community, and utilizes wrapped dogecoin as its native gas token.

DogeChain has been without a stablecoin since multichain’s bridge exploit; which has resulted in a loss of protocol value, coupled with the inability of some services to operate as intended without a pegged stablecoin to derive pair valuations from. Our proposed hyper-collateralization stablecoin is intended to both provide a real yield staking service on DogeChain, while encouraging an overall growth in protocol TVL and activity.

Functional Components

USDO Smart Contract

Smart contract implementation of the USDO token, allowing for decentralized minting/burning of USDO tokens, along with holding the underlying hyper-collateralized asset, and allowing for collateral staking. Implements OpenZeppelin's ERC20, Ownable, and ReentrancyGuard.

Heartbeat Service

- **Centralized**

  Operates by pooling multiple price oracles via a centralized application, and providing the underlying asset's median price via direct call to the USDO smart contract. Can operate on a fixed, or random timer. Wallet costs are offset via the 10% fee allocation from mint/burn operations.

- **Decentralized**

  A Standalone smart contract which collects the aforementioned 10% fee allocation from mint/burn operations, which any decentralized user can then claim via submitting a pricing request from the target price oracle. Operates based off user incentive, with the intention of the fee/reward incentive allowing for frequent or automated user operation.

Hyper-collateralization

The USDO smart contract launches with a required minimum collateralization of 3.5x the underlying asset, which would allow for approximately a 71.4% drop in the underlying asset's value in order for the underlying asset to no longer be capable of supporting all dollar-pegged token claims (or, a de-peg event). In the case of Dogecoin, this would require the current price of Dogecoin (8c USD) to drop to 2.3c USD.

As the value of the underlying asset increases, the USDO smart contract will automatically recalculate the level of collateralization needed, linearly increasing to requiring a 20x collateralization in the event of Dogecoin returning to its prior all-time-high of approximately 70c - allowing for a 95% retrace in price while still remaining fully collateralized.

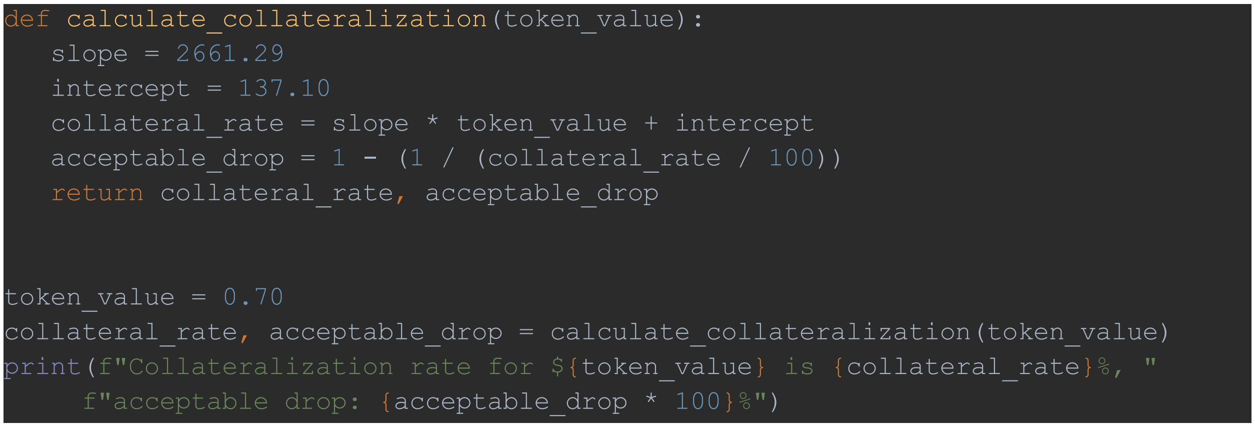
Scaling Collateralization Formula

From the above baselines, we can derive the following linearly scaling collateralization formula;

$$\text{Collateralization Rate} = m \times \text{Underlying Token Value} + b$$

Where m is the slope of the line, and b is the intercept

In our case of intended hyper-collateralization, m would be valued at 2661.29, while b would be valued at 137.10. With both m and b known, we can rely on the USDO smart contract to determine our required liquidity reserves, and the acceptable level asset depreciation from these levels. This logic can be tested with the below python snippet.



```python
def calculate_collateralization(token_value):
    slope = 2661.29
    intercept = 137.10
    collateral_rate = slope * token_value + intercept
    acceptable_drop = 1 - (1 / (collateral_rate / 100))
    return collateral_rate, acceptable_drop


token_value = 0.70
collateral_rate, acceptable_drop = calculate_collateralization(token_value)
print(f"Collateralization rate for ${token_value} is {collateral_rate}%, "
     f"acceptable drop: {acceptable_drop * 100}%")
```

Python implementation of the scaling hyper-collateralization algorithm

Scaled Collateralization Table

Token Price	Collateralization Required	Sustainable Depreciation
$0.08	350.00%	71.43%
$0.10	403.23%	75.20%
$0.12	456.45%	78.09%
$0.14	509.68%	80.38%
$0.16	562.91%	82.24%
$0.18	616.13%	83.77%
$0.20	669.36%	85.06%
$0.30	935.49%	89.31%
$0.40	1201.62%	91.68%
$0.50	1467.74%	93.19%
$0.60	1733.87%	94.23%
$0.70	2000.00%	95.00%
$1.00	2798.39%	96.43%

Due to the increasing amounts of collateralization required, we propose that collateralization is limited to 2000% (20x the underlying asset), allowing for a maximum sustainable depreciation of 95% of the underlying value. While extremely high, this protects against market peak draw-down.

Staking Incentive
Minting and burning of USDO tokens are handled in a decentralized fashion, where users can swap their underlying asset (in this case, wrapped Dogecoin) for USDO tokens, respective to the current value of Dogecoin as determined via pricing oracles.

Any mint or burn command will absorb a 0.25% fee, taken from the underlying asset (wrapped Dogecoin), of which 90% of this fee is redistributed to all staked parties, proportional to their staked amount of collateral. The remaining 10% is awarded to the heartbeat contract, or wallet in the case of a centralized pricing oracle setup.

Staking is a standalone process to swapping wrapped Dogecoin for USDO; with stakers solely providing wrapped Dogecoin, and then receiving any rewards due from any mint or burn command carried out while they remain in the pool.

Token swaps will contribute towards the collateralization of USDO, but only at their given 1:1 (sans fees) rate. Minting new USDO is only possible when the staking pool is **above** its target collateralization level.

Collateralized Functionality Limits
With the given scaling collateralization parameters known, USDO operates with a primary motive of protecting holders of the USDO token.

In the event of collateralization dropping below the required levels, the following functionality will be disabled;

- **Unstaking**
  Participants may not unstake from single-staking services under the USDO contract until the collateralization levels have recovered above any given minimums as determined by the heartbeat service.

- **Minting**
  USDO Tokens may not be minted in the event of collateralization falling below their minimum levels.

- **Burning**
  Burning/redeeming USDO tokens will increase to a cost of 1% in fees in the event of the USDO contract becoming undercollateralized. This fee increases to 5% if the collateralization falls below half of its intended target. This will ensure that in a dire case scenario, the USDO token will remain redeemable for 95% of its intended value.

Heartbeat-based Limits
The USDO smart contract should maintain a minimum heartbeat call requirement, ensuring that the underlying value of any tokens is correctly pegged. We recommend at least a 5 minute timer for any centralized services, or more frequently if affordable on any given chain.

In the event of a heartbeat target being missed, the USDO smart contract should assume a collateralization failure, and apply all relevant actions to its given services.

Finally, each heartbeat cycle should only allow for a 10% change in supply/collateral on mint, burn, and unstaking functionality. As an example, the amount of liquidity unstaked, or USDO redeemed/burned or minted within a single heartbeat cycle cannot exceed 10% of the total liquidity staked, or USDO in circulation.

In order to prevent against the attack vector of a malicious actor staking/unstaking a large amount of supply per heartbeat to lock users into staking positions, we propose a minimum 24 hour lock on all staked collateral.

Smart Contract Functionality

`Modifier _requiresOverCollateralization():`
Given operation will cease to function if the current staking pool is not overcollateralized.

`mint(uint256 n) _requiresOverCollateralization`
Accepts n amount of collateral/underlying tokens from the caller, and mints the equivalent token amount in USDO. Limited to minting 10% of the total USDO supply per heartbeat (or, a maximum of 3,000 USDO per heartbeat in the event of the current supply being under 30,000 USDO).

`burn(uint256 n)`
Burns n amount of USDO from the caller, returning the equivalent token amount in the underlying token asset.

`stake(uint256 n)`
Stakes n amount of collateral/underlying tokens from the caller, and issues internal shares to distribute any owed fees proportionally to the caller.

`unstake(uint256 n) _requiresOverCollateralization`
Unstakes n amount of collateral/underlying tokens from the caller’s shares, up to a maximum of 10% of the total collateral/underlying tokens per heartbeat.

`claim() _requiresOverCollateralization`
Allows for any staked caller to claim any rewards due - not automatically called on unstake.

`heartbeat(uint price_of_token) Ownable`
Heartbeat command, updating the current price of the underlying asset per token - and resetting any heartbeat-limited functionality per cycle.

`setHeartbeatTimer(uint seconds_between_beats) Ownable`
Sets the maximum acceptable time between each heartbeat, not exceeding 15 minutes.

`setHeartbeatRewardAddr(address addr) Ownable`
Sets the address to be rewarded with a fee share in the event of a heartbeat event being received. In the event of a decentralized smart contract being launched which allows for users to submit queries to any given decentralized pricing oracles, this reward fee should be received by said contract, and then distributed directly to said user.

Summary

The USDO hyper-collateralization model allows for deploying algorithmic stablecoins on chains which may only have access to more volatile assets; while keeping its functionality as simple as possible, and not relying on any proprietary ERC20 funding model or otherwise.

This model foregoes the typical staking incentives which have previously seen boom-and-bust stablecoins lose their peg; and instead focuses purely on incentive models which are fair to both stakers, and holders in their respective risk and reward models.

These allowances and concessions by both parties allows for a stablecoin which deliberately limits its own growth, in favor of increased security and stability at the protocol level; and in utilizing real yield reward incentives for stakers, rather than the token printing principles seen in other models attempted over the prior years.

Furthermore, the transparency of this system allows for increased risk management, along with incentivizing user-based arbitrage with direct on-chain minting/burning in order to maintain this pegged system.

We believe that stablecoins allow for a dramatic increase in on-chain volume, and overall total value on decentralized chains - and with the above hyper-collateralization model, it can be provided while mitigating the inherent risks that come from black-boxed solutions, or from bridge-pegged tokens.