OTOKEN Framework

ZYGOMEB - Optim Finance

Version 1.1

Within this document is described, at a high and cursory level, the otoken accounting framework.

Its planned application as currently announced are the systems referred to by as OADA and OUSD, which will be used as examples of asset-stability derived yield optimization systems.

To begin, the system issues a liability token OTOKEN (OADA, OUSD) as the primary point of accounting for the systems's balance sheet, and is otherwise an extensible base for algorithmic market operations (AMOs) that extend this functionality around this base liability asset.

Simplifying, OTOKENs is designed to leverage the utility and power of another token and create a derivative of this base, stable up to parameters acted upon by the system, that will be able, thanks to the modularity of it, to become much more flexible and adaptable to market conditions.

OTOKEN Core

The Core system consists of the base staking, deposit and collateral management modules.

In fact, the core system does not include the most important collateral management strategy, meaning one that would enable any kind of withdrawals or market peg protection. Such strategies, or as we call them, sub-AMOs of the Collateral Management AMO, are able to be customized and tailor made at a later date and not under purview here.

Henceforth, we assume that such systems exist and that there is economic justification for the system's existence. We assume that these systems are also able to provide yield, at some level of risk, tailor made to the protocol. Business strategy to best leverage the products are also not discussed but utmost required for its success.

The core system functionality, apart from this upgradeability, has control of the AMO activity given to the Controllers, which are themselves derived from the upgrade authority, a token assumed to be in control by a secure voting process.

Stakers, holders of the sOTOKEN asset are privy to both the upside of the system yield as well as exposed to any loss of it. It is not assumed in this document that these strategies will be low risk, but it is the intended approach to how the system should be used.

To answer a question begged, can the system suffer a loss greater than what the sOTOKENs security can absorb? Yes, but it would need to be quite catastrophic in its magnitude. In those dire circumstances it is expected that a security of last resort be provided from other sources to try and make the senior holders whole, or, through other means.

The OTOKEN/sOTOKEN dichotomy may be described as a 2-tranched structure where senior OTOKEN holders forsake all system yield to sOTOKEN for intrinsic benefit of the OTOKEN utility, protection from potential loss, and any extrinsic economic incentives put forward to utilize it; The unstaked side for an active use of the stability, and utility provided, the other, a staked passive yield aggragating strategy box that trades up yield for the risk of securing the system economically.

In the future it is possible to add a mezzanine, lower risk but still yielding tranche should demand for it surface. Currently, I don't believe that sufficient sophistication is shown to justify that added complexity, nor are the strategies for planned modules risky enough to expect such lossess to occur.

Ultimately, the system is endowed with sufficient upgadeability to be able to get modified to meet requirements from Liquidity Providers, and changing market conditions.

High Level Overview Of Core System Components

OTOKEN Policy

The extensibility of the system rests upon a whitelisting address which is responsible for partially adding ir removing scripts that authorize the minting and burning of the OTOKEN.

It is by the sole soul token authority that these permissions are added or removed, and, inclusion of a mint/burn rule is what defines a system as an AMO.

Staking AMO

A system that issues the sOTOKEN, and is the end destination of all of the system accounting. The system accounting which is a virtual number self-reporting profit by each of the AMOs.

This in turn, upon synchronization with the Staking AMO is coupled with marking of dao profits, a cut on the system yield that is kept as a virtual tally, added to the total of sOTOKEN, disregarding any limits placed upon the total sOTOKEN.

Such limits, and other system parameters, are in control of the soul authority while the fee claiming process is given to a fee claimer authority for security's sake as it may be leveraged quite more often.

Collateral Management AMO

Accounting of the system profits and movement of the assets of the system in and out of strategies as well as tallying of the profits is done via a hub and spoke shape around the CM AMO. Each strategy is present, much alike the OTOKEN rules in a whitelist of same management. And each instance of it while alive is tracked by an NFT ID kept in the datum of the CM AMO and through that whitelisting they can tally profits.

It is entirely intended for the system to be able to facilitate all strategies, including ones of custodial or semi-custodial nature but it is not required nor intended where possible.

Some Extensions Beyond Core

DEX AMO

For all practical intents and purposes, this is a necessary component of the system and without it there is no way for OTOKEN holders to redeem the underlying TOKEN, and it does it via manipulating available liquidity and injecting more as necessary to capture volume and support both purchases and sells with a set policy.

It is able to both buy and sell OTOKENs, using either the reserves to buy (and redeeming in the process) or by minting new ones in case of an upwards depeg.

More importantly, the system can also provide liquidity, a par of OTOKEN/TOKEN, pairing reserve TOKEN in a stableswap with newly minted OTOKENs that don't enter circulation until bought. This can be thought of as a dynamic redemption and minting pricing in demand and supply that allows the system to act only when the price goes outside of an accepted peg range.

To control the peg, apart from the options from two paragraphs above, directly controlling liquidity provided by the system is an option by withdrawing and burning the excess OTOKEN.

When the system acts in any of the mentioned ways, it does so with a well-defined policy. As an example, it can be defined to act when the peg price is outside the range of [0.99, 1.001]. Given the context of the architecture of Cardano however, this action may and will be slightly delayed. Meaning that there will be times when, even if for but a short time, but for a time nonetheless, the open market price will be out of bounds.

It is, of course, expected that other market participants will be more than willing to accept a smaller discount and correct the price should it deviate in an even tighter bound sparing the system the cost and effort of rebalancing liquidity.

Stake Auction AMO
This is an AMO specific to the application of OADA. Given how ADA staking works, this module adds the ability to borrow stake from the system for a single epoch, without causing any lockup for OADA in the process.

Users provide bids on the APY they're willing to provide to the system as well as the total interest they're willing to pay, and from that it is derived how much notional size they can borrow for the epoch snapshot. The system, before the epoch ends, collects these bids and supplies the liquidity for the time of the snapshot and afterwards removes the liquidity to deploy it into productive strategies.

To maximally leverage the yield provided by this AMO the system can pull liquidity out of the DEX AMO provided redemption pool. It is in the best interest of the system to minimize the time for which this is the case as with a large, if not all of the reserves locked up for maximally, in my current estimation, an hour, for block inclusion guarantees – leaving the system without, or, with little POL liquidity provided for redemptions.

In this time should any large orders happen the system will not be able to react even if it posseses more than sufficient amounts of liquidity to do so. Any such seller would be either unaware of the slippage they'll incur, or, be a scheming attacker on it. As such any integration for collateral using OADA, or, any system using an equivalent staking auction, must have an accurately based oracle that would be resilient to such an attack and only falter based on a more prolonged depeg, or, based on the onchain data.

Ultimately, the stake auction module itself is considered safe, and the only care comes in systems that consider giving OADA a collateral status. It is important to acknowledge the limitation here, as outside liquidity may be watchful of such an attack like that as an opportunity to get OADA at a discount before the system itself is able to.

Future Work / V2 Implementation

Borrowing AMO
Defined as the ability to borrow OTOKENS from the system by supplying sufficient collateral.

For the sake of hiding the marvels of this design, no further technical details nor economic considerations are given.

Lending AMO
Defined as the ability of the system to lend both OTOKENs and TOKENS to another system. Notably most useful as it gives the system the ability to create a similar market for borrowing OTOKENs as via the Borrowing AMO, if lending to a money market AAVE-type protocol.

It gives less flexibility to control the direction and issuance of the assets but if attractive enough of a yield stream, especially for yield on the base TOKENs, it will be introduced.

Other AMOs
For the sake of keeping it brief other plans and ideas that expand beyond the mold are not discussed.

Alternative Stability Measures
While this document painted the DEX AMO as the only way to create OTOKEN stability, there are certainly other ways to do so.

We will not enumerate nor discuss them here as for the purposes of the OADA and OUSD systems, they are not planned, but nonetheless possible.

System Approach To Non-Base Assets

As part of execution of any AMO the system may and will acquire tokens that are completely exogenous to it.

The AMO should, by its definition be aware of such exogenous tokens and be programmed to be able to handle them appropriately. Approaches could be to accumulate and leverage those tokens, sell and add to system profit or any number of other mixed approaches.

When it comes to leveraging tokens that have utility, or yield unto themselves, in time when sufficient numbers are acquired, they may have an entirely specific AMO formed around them to best utilize the power they have.

An example of that would be a token that can be staked and yields governance and profit sharing powers. They are especially good if the voting they yield can be used for directing of incentives towards the OTOKEN protocol itself.

Flash Minting

For purposes of fully autonomous state-contention independent minting of the OTOKEN using a TOKEN deposit, the system provides the ability to always get 1 OTOKEN for 1 TOKEN sans transaction or other fees, only expecting the deposit TOKENs at the end of the transaction.

This feature is extraordinarily useful for arbitrage, but will be most useful when intracting with protocols that are designed to also work in a flashy way.

Multiple OTOKENs

As a final note, we must mention the mutual power sharing and uplifting induced by the existence of more than one OTOKEN systems deployed, which can create AMOs normally impossible to assist in bootstrapping, yield sharing and strategies that enchance the ecosystem.

It is, however, even in presence of multiple OTOKENs, best not thought as a platform for synthetic assets, as the stability of it is strictly derived from an already stable asset that is present as a TOKEN.

Furthermore the framework only makes sense if there can be yield and generally use found for the base TOKEN out in the ecosystem. Exogenous rewards may be injected to help bootstrap one anyway, when the endogenous utility of it is one that has benefits outside of yield. Such deployments are nonetheless possible, and, depending on the circumstances, planned.