Risk Report: oneFOX

What is oneFOX?

ICHI's oneTokens are a line of collateralized tokens which are intended to maintain a stable value. Only a portion of their collateral is fiat-backed; the rest is a combination of a particular community's native token and various DeFi investments. oneTokens achieve their stability by starting out over-collateralized, investing collateral to grow the treasury and stay over-collateralized, and offering rewards to oneToken holders in order to incentivize minting and holding of the oneToken.

oneFOX is a second-generation oneToken, which is mintable with USDC and FOX and whose treasury is ultimately controlled by the ShapeShift DAO. It is similar to a debt instrument, in that it is redeemable on demand for an equal amount of USDC from the oneFOX treasury.

Economic Risk

Like any debt instrument, oneFOX is subject to certain liquidity risk. It is possible that the oneFOX treasury may run out of USDC, which would prevent holders of oneFOX from redeeming their tokens for USDC. However, redemptions are not intended to be the primary way to exit oneFOX; an average user would likely use a DEX to trade through a oneFOX liquidity pool, rather than use the relatively gas-heavy oneFOX redemption process.

A portion of the oneFOX treasury's assets will be invested in DeFi positions approved by ICHI and selected by oneFOX governance. These positions are not denominated in USDC, and will carry market risk. They may decline in value, and may not be liquid; for example, certain positions and DeFi protocols may involve a staking or lockup period. This may limit the ability of oneFOX governance to immediately rebalance the oneFOX treasury in the event of high demand for oneFOX redemption.

Even if the oneFOX treasury is out of USDC, oneFOX tokens remain a claim against the oneFOX treasury's future USDC holdings. Holders of oneFOX must trust ICHI and the oneFOX governance process to manage the treasury's portfolio of assets responsibly, and to maintain the treasury reserve ratio such that a portion of the treasury's funds remain in USDC and available to service redemptions.

Technical Risk

oneFOX is a system of several contracts deployed on the Ethereum blockchain. These contracts have been audited by a reputable auditor.

While it is extremely rare (and costly) to prove that a smart contract is bug-free, audits are an extremely useful tool. The findings of the auditors indicate that oneFOX contract code adheres to best practices and carries a low level of technical risk.

Governance Risk

The system of oneFOX contracts is controlled by a Gnosis Safe. Control of this Gnosis Safe would grant an attacker the ability to change or replace any of the components of the system, or to misappropriate assets from the oneFOX treasury. Because every holder of oneFOX must trust this system to behave honestly, it is critical that it is as secure and transparent as possible.

The ShapeShift DAO will be granted ultimate authority over this Gnosis Safe; a passed proposal can execute any governance function. Day-to-day operations, however, will be handled via a multisignature scheme. This will require the consent of four out of six governance signers, and be protected by a combination of the Zodiac ScopeGuard and Delay modules. These modules are developed by the Gnosis Safe team, and have been audited by reputable auditors.

To mitigate the risk of malicious behavior by governance signers, the set of six signers will be composed of two signers from the ICHI community and four from the ShapeShift community. In addition, the ScopeGuard and Delay modules will restrict the governance actions it is possible for them to perform. A 48-hour delay period will be required for the most sensitive kinds of governance actions, which will also automatically send an alert to the ShapeShift DAO's Security Workstream for review.

Governance signers will have the ability to invest or disburse the oneFOX treasury's funds, or set the minting ratio within certain minimum and maximum limits. With 48-hour on-chain notice they may also change a governance signer's key or upgrade the code of one of the oneFOX contract's modules to a new, ICHI-approved version. Note that governance signers are *not* able to replace the core oneFOX contract's code, or to circumvent the requirement that ICHI approve all new modules added to the system.

If the governance signers act maliciously, they have the ability to misappropriate the oneFOX treasury's funds; however, none of the actions they are able to take are able to change the fundamental character of the oneFOX token as a ERC-20 token which represents a claim against the (current or future) USDC holdings of the oneFOX treasury.