

Concepts

Vault: A singleton contract storing user-deposited tokens. It stores balances of pools and depositors. Users mainly interact with this contract.

Pool: A class of smart contracts holding their tokens in the vault and implementing certain callbacks. Liquidity pools, gauges, and bribes are all types of Pools.

Token: Velocore V2 supports not only ERC20 but also ERC721, ERC1155, and native tokens. Tokens are represented as a wrapped bytes32 (Token)

Design Objectives and Security Model

Our approach emphasizes abstraction and encapsulation. We aimed for the vault to make minimal assumptions about the pools' behavior. While gas optimization is a secondary goal, it remains crucial.

Pools deployed by anyone can interact with the Vault freely and permissionlessly. Vault always assumes the possibility of malicious behavior when interacting with pools. They're trusted for user-deposited amounts only, and users should avoid malicious pools at their discretion.

Last updated 4 months ago On this page