

# V1 zkSyncEra (deprecated)

Velocore and Velodrome Finance use the same codebase, and the security documentation for Velodrome Finance is provided below.

## CONTRACT ADDRESSES (NEW, OFFICIAL VELOCORE)

Contract Name Contract Address VC [0x85D84c774CF8e9fF85342684b0E795Df72A24908](#) WETH [0x5AEa5775959fBC2557Cc8789bC1bf90A239D9a91](#) Gauge [0xd06aD497EB89716B34a5EF6B9A2aA1Fb14A4c75e](#) GaugeFactory [0xB7D98F552B4484b52181600fA5360BBAdd09fA98](#) ExternalBribe [0xD822315C30001bB85BAE8a9dE5dB98a87d0656d1](#) BribeFactory [0xc365acD05609D9125Eb77dDF44322F3F561C9713](#) PairFactory [0xE140EaC2bB748c8F456719a457F26636617Bb0E9](#) Router New [:0xF29Eb540eEba673f8Fb6131a7C7403C8e4C3f143](#)

Old [:0xB2CEF7f2eCF1f4f0154D129C6e111d81f68e6d03](#) RouterWrapper(deprecated. to fix gauge issues of solidly) [0xd999E16e68476bC749A28FC14a0c3b6d7073F50c](#) VotingEscrow [0xbdE345771Eb0c6adEBc54F41A169ff6311fE096F](#) RewardsDistributor [0xD7107a47B4fBBc585b25BbEe3777B2EDC11D156C](#) WrappedExternalBribe [0x0021C13C7bd19858E18EDdf54B82A6C7cd46cc96](#) WrappedExternalBribeFactory [0x5c5d9C7fe718cF3840d181C35c078aD6F4e315E1](#) Voter [0xe09A60FAe6d77658b9767A70e2f361b46Dd3f16A](#) Minter [0x8f0b4B3e211c84061ab5959Bd3D49C6B3EeC1d7D](#)

## CONTRACT ADDRESSES (OLD, FOR THE POAP EVENT)

Contract Name Contract Address VC [0x129c6e2D8619B3F20504dBB7188602300f4C7e16](#) WETH [0x99cd063A128A35b44b9Fb4ce4b79f8247baF746](#) Gauge [0xc3e495312300Ee0A940889a5af0394F01BBA30E5](#) GaugeFactory [0xA5DC997cE8D4443Ad9cB39d2aB46D8F929be46B1](#) ExternalBribe [0x3E7b8C06626089ABeB52C6B5A9D97F893451A32c](#) BribeFactory [0xcE2d259dD1DCCf84e0c064ECcc49Ef060Ff4d73E](#) PairFactory [0xF5719b1Ea3C9bF6491E22C49379E31060d0FbFc1](#) Router [0x389C30DafaEc0a0C637C33F39E1bDea75c4bA0e6](#) VotingEscrow [0x83CDDc0282D51d77d21e71190B02124D59f40918](#) RewardsDistributor [0xEb669307ff656a90E79a8AA5D635ad5f703a69f](#) WrappedExternalBribe [0x06daed51a1Bfe51Ce90fCb0c11daB43999e42e30](#) WrappedExternalBribeFactory [0x0Cc9A8fA422C7F8E17d9c3D98776b06F895Cb820](#) Voter [0x2C63AC5D42Bd20aB6A2a5bdB2b2B29597fC5Df77](#) Minter [0x594b5927AAcEf79a1bfe72959D2DF7d122AFBd63](#)

## SECURITY

As a commitment towards the safety of our users and partners, we want to be transparent about the changes and the status of the security audits of our smart contracts.

Velodrome Finance was adapted from Solidly, which [codebase was open sourced in full](#) by Andre Cronje and his team in March 2022. Since its release in February on Fantom network, no security incidents related to Solidly smart contracts were reported.

Velodrome Finance smart contracts can be found on Optimistic Etherscan at the links below.

Before moving forward, we'd like to remind to our users that security audits do not eliminate risks completely and that every user should read and agree to our [legal disclaimer](#) before using Velodrome Finance!

For security reports, please reach out to us or [Discord](#) , or to the contacts provided on our Github page.

## AUDITS

Solidly went through a partial (only the AMM part was sent for audit) security audit in January 30, 2022. The audit was done by PeckShield and did reveal 5 low-severity and 1 informal findings.

The full audit is available for [download from Solidly git repository](#) .

Velodrome Finance went through a security audit and a peer review as part of the Code4rena bug bouncy contest. Finally, a full MythX deep scan on Velodrome contracts found just a handful of false-positive, low-severity issues reported.

The Code4rena contest results were released on August 8, 2022 and are available [here](#) . All high- or medium-risk issues were either resolved pre-deploy, except for one known issue (users can claim eligible rewards from ExternalBribe contracts more than once) that's currently being addressed (via a wrapped contract solution). No user funds are at risk from this vulnerability, and protocols who wish to deposit external bribes should get in contact with the core team to discuss alternative solutions. More information about our C4 contest can be found [here](#) .

Lastly, we also engaged with Coelacanth ([@ImpossibleNFT](#) ) for an informal full audit. Reports from that audit are available [here](#) .

## BUG BOUNTY PROGRAMS

Velodrome Finance ran a [bug bounty contest on 23rd to 30th of May 2022 with awards up to 75,000 on Code4rena](#). The main scope of the contest was to cover all the new changes to the new and the original contracts.

Solidly's bug bounty program was launched in February 2022 on Immunefi.com. There were no claims for any of the 200,000 rewards ([on their Github](#)).

## DIFFERENCES FROM SOLIDLY

These are the listed differences by Velodrome Finance between Solidly and their own platform.

### MAJOR CHANGES

- Treat external bribes differently than internal bribes (i.e. fees).
- We split Bribe into two separate contracts, InternalBribe
- and ExternalBribe
- .InternalBribe
- functions essentially the same way as Bribe
- did, but ExternalBribe
- ensures that rewards are eligible to be claimed by any voter who votes for the underlying gauge during the epoch, instead of only voters who vote after the rewards are sent. ExternalBribe
- also ensures that rewards can only be claimed after the epoch ends. ExternalBribe
- rewards must also be whitelisted
- via on-chain governance.
- One vote per epoch. In Velodrome, voters are only allowed to make "active" voting decisions (i.e. vote and reset) once per epoch.
- Voters must wait until the next epoch to change their votes. Voters can, however, cast
- their votes throughout the epoch.
- On-chain governance.
- To handle protocol-wide decisions (such as eligible tokens for external bribes), we introduce an on-chain Governor. This will likely be Tally's first on-chain governor on Optimism following their support for the network.
- Killable gauges.
- To dissuade emissions exploitation via dummy gauges, we're allowing the Velodrome Commissaire
- (akin to Curve's Emergency DAO) to kill any "bad" gauges. The Commissaire is composed of individuals from varying parties meant to serve as a credibly neutral decision-maker for the broader ecosystem.
- 

### MINOR CHANGES

- Removed the LP boost for voters.
- We removed the boost that voters receive when staking their LPs with gauges they voted for. This removes the need for a veNFT aggregator (more on this later...).
- Removed negative voting.
- We found negative voting to be zero-sum for Solidly, so we decided to remove it.
- Team emissions.
- 3% of new emissions will be sent to a team address, meant to cover on-going expenses and future development.
- 

### SMALL CHANGES

- Modifiable fees.
- Fees are now doubled to 0.02%, modifiable up to 0.05%, and tracked differently for volatile vs stable pairs.
- Upgradeable veNFT art.
- Self-explanatory
- Velodrome specific.
- Initial distribution.
- Initial distribution will be handled in two ways: a redemption process that uses LayerZero to burn WEVE
- for USDC
- and VELO
- on Optimism, and a Merkle airdrop contract. Unclaimed VELO
- is never minted to ensure emissions aren't affected.
- 

Last updated 4 months ago On this page \* [CONTRACT ADDRESSES \(NEW, OFFICIAL VELOCORE\)](#) \* \* [CONTRACT ADDRESSES \(OLD, FOR THE POAP EVENT\)](#) \* [SECURITY](#) \* [AUDITS](#) \* [BUG BOUNTY PROGRAMS](#) \* [DIFFERENCES FROM SOLIDLY](#) \* [MAJOR CHANGES](#) \* [MINOR CHANGES](#) \* [SMALL CHANGES](#)