About

Velodrome Finance, at its core, is a solution for protocols on Optimism to properly incentivize liquidity for their own use cases. Building on top of the groundwork laid out by Solidly, our team has addressed that first iteration's core issues to realize its full potential.

⚠️ Before using Velodrome Finance, you are required to read and agree to our legal disclaimer.

Who is behind this project?

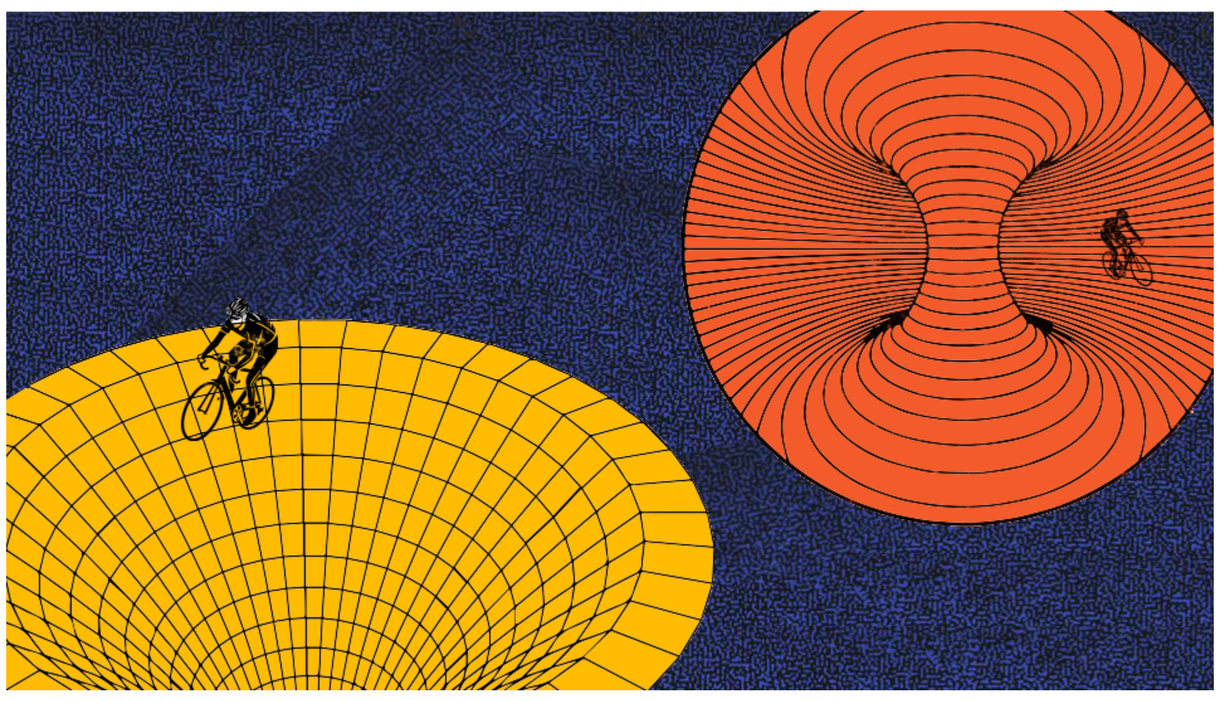
The team behind Velodrome Finance previously launched veDAO, an initiative incubated by Information Token. veDAO's founding mandate was to engage with the Solidly ecosystem, a protocol launched on the Fantom network by Andre Cronje, while driving long-term value to the veDAO community.

The veDAO team has since developed deep subject matter expertise on both Solidly, the veNFT primitive, and the ve(3,3) mechanism, becoming the go-to resource for protocols and chains seeking support around these topics.

By the numbers, veDAO, managed to attract $2.6B in TVL (total value locked) in the early days, securing ~10% of Solidly voting power and ~$1.1M USDC in treasury assets.

Resources

- Website: https://www.velodrome.finance
- Twitter: https://twitter.com/VelodromeFi
- Medium: https://medium.com/@VelodromeFi
- Discord: https://discord.gg/velodrome



Protocol Overview

Problems with Liquidity Incentivization

Almost every protocol in DeFi needs to have a certain amount of liquidity for one reason or another.

Liquidity	Example	Benefit
Native token	OP-USDC	Treasury access to capital markets
Stablecoins	DAI-USDC	Ensure stability by minimizing depeg risk
Pegged asset	ETH-stETH	Minimize opportunity cost of converting assets

However, current solutions for incentivizing liquidity come with their own tradeoffs and pitfalls:

- Pool 2 emissions (i.e. attaching a reward to staked LPs) can be costly to maintain, and often times result in a "farm and dump" resulting in "unsticky" liquidity.
- Protocol owned liquidity can be costly to bootstrap, and liquidity may only be needed occasionally, instead of on-going basis.
- Bribing voters in the CRV/CVX system can be costly as incumbents already have a sizeable lead. Additionally, the universe of pool types here are limited.

Introducing Velodrome

Velodrome addresses these issues and presents an attractive alternative by addressing the core issues in Solidly and adding its own improvements. To recall, the key innovation of Solidly was to align protocol emissions with fees generated, not simply liquidity. To do this, it would allow protocols and other large stakeholders to become veNFT "voters", using their locked voting power to direct future emissions and collecting fees (termed bribes in Solidly) from the pools they voted for.

Velodrome has made several improvements to the Solidly codebase, all of which were thoughtfully chosen to ensure that the protocol would carry out the original intended mechanism of allowing voters to *fairly compensate* LPs for impermanent loss.

Solidly had several key issues that prevented its success in the Fantom ecosystem:

Improvement: Tying Rewards with Emissions

In Solidly, voting rewards (i.e. bribes) were claimable *before* the emissions from that vote were committed. Velodrome addresses this with new mechanisms:

- First, we allow voters to make only one "active" voting decision (i.e. `Voter.vote()`, `Voter.reset()`) every epoch (note: this does not include the `Voter.poke()` function).
- Additionally, bribes from fees (*internal*) and external sources (*external*) are treated differently. Internal bribes function more or less the same way as they did in Solidly, streamed to voters who vote for them. External bribes, however, are rewarded *per epoch* rather than streamed, and are claimable only after the next epoch starts. This means that a bribe sent at the last minute of an epoch will accrue to all voters of that epoch, and be claimable once the epoch flips.

The goal of these changes is to ensure a healthy equilibrium between voters and external bribers. Bribers are incentivized to get their bribes early in that week, as to attract early voters. They also benefit from bribing later, as to have more information on competing bribes. Voters face a similar dilemma, as voting too early means forgoing potentially lucrative bribes that come later, and voting too late means voting with a lower (`$veVELO`) balance. Note that this latter affect is especially pronounced for voters who have locked for shorter time periods (e.g. voters who have locked for weeks rather than months/years will experience larger differences in the bribes they receive from voting later vs. earlier in the epoch).

Improvement: Ensuring Productive Gauges

In Solidly, exploitive voters were able to direct emissions towards unproductive gauges, including those for pools 100% owned by those voters. Velodrome addresses this in three ways:

- First, we've added an on-chain governor to whitelist pairs used in gauges. Voters will need at least 0.02% to submit a proposal, and 4% to reach quorum. To ensure that those who whitelist gauges are economically aligned economically with our system, we've also removed the ability to whitelist by paying a whitelisting fee. Note that the on-chain governor is currently not live, as we're still working with Tally to get the process set up.
- Second, we've also added an Emergency "Commissaire", which has the ability to kill any gauge it deems unproductive to the broader ecosystem. This Commissaire consists of folks from both the Velodrome core team, and the broader Optimism and DeFi ecosystems. The Commissaire multisig is available here, and signers include:

Signer	Affiliation	Address
Jack Anorak	Velodrome	0x9eBd10B46B43351097caB2D3c03Ccf440957A2a9
pooltypes	Velodrome	0xc0DE1436C4E247F8652476A0B9ff55699801e1d0
Nick	Velodrome	0x53e0b897eae600b2f6855fce4a42482e9229d2c2
vfat	Hundred Finance	0xeF0Ca09fbf9a5f61E657Fb208b46b8685c1d4766
0xHamZ	DeFi Independent	0x698c3619f9ecB540cEc21E056ae4A900Bca1649C
Optimism	Optimism	TBD

- Third, we've doubled the initial swap fee from 0.01% to 0.02% to ensure that voters have more twice the incentive to direct emissions towards productive liquidity. Note that this rate is still much lower than alternative exchanges (e.g. Curve at 0.04%). Stable and volatile pairs also have different fees, both modifiable up to 0.05%.

Improvement: Prolonged Emissions Decay

In Solidly, protocol emissions decayed too quickly, leading to minimal incentives for late entrants. Obviously early adopters should be rewarded for the risks they're taking, but we observed that the emissions decayed too quickly in the Solidly model. As a result, we made a few small tweaks to ensure that while early adopters would still be rewarded, the protocol would still be an attractive opportunity for future protocols.

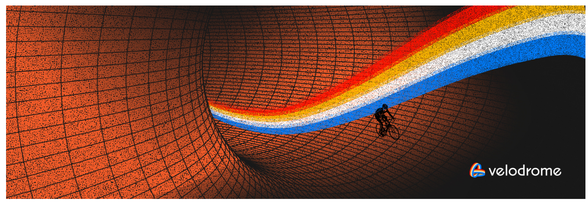
- First, we modified the emissions growth function to

> $(veVELO.totalSupply \div VELO.totalsupply)^3 \times 0.5 \times Emissions$

- Second, we removed negative voting, as we found it too zero-sum.
- Third, we removed the LP emissions "boost" for voters. Those emissions are instead reallocated towards all LPs, regardless of veNFT ownership status, to ensure voters are able to incentivize outside liquidity.
- Fourth, we adjusted the initial distribution to skew much heavier towards retail: the veDAO community and other sophisticated DeFi ecosystem participants. This was done to avoid an fleeting TVL race, and is implemented with both a standard MerkleClaim airdrop contract that dynamically mints VELO for eligible addresses, and a cross-chain WeVE burn contract powered by LayerZero.

Improvement: White-Glove Support

In Solidly, the lack of a "team" meant lack of support post-launch. In line with the veDAO ethos, we want to ensure that our protocol has white-glove support for our partners and other stakeholders. To ensure that our team has sufficient resources to pay contributors an expand on our product offering, 3% of perpetual emissions will be directed towards our team multisig.



Launch Details

Velodrome launched on Thursday, June 2, 2022.

> ⚠️ As with any launch, we'd like to warn our users about the potential limitations of the first release. At launch, our dApp will render best in **desktop environments**.
>
> If at any point you require assistance, please join our Discord, where our community and we will be happy to help you!

Getting Ready

Velodrome Finance operates exclusively on the Optimism network (a layer 2 of the Ethereum main network that uses Optimistic Rollups).

If you are unfamiliar with Optimism, you can find a lot of resources about the network, its ecosystem, and its mission on the Optimism website https://www.optimism.io

To set up your wallet, please go to https://chainlist.org and search for *Optimism*. You can use the *Connect Wallet* button to automatically configure your default wallet to use Optimism. Use the *arrow down* to expand for more configuration options.

> 🪂 Be sure to learn about the Optimism Collective and see if you qualify for an OP token airdrop!

Bridging

New Optimism users who want to participate in Velodrome should make sure they have `$ETH` on Optimism in order to be able to pay for transaction/gas fees.

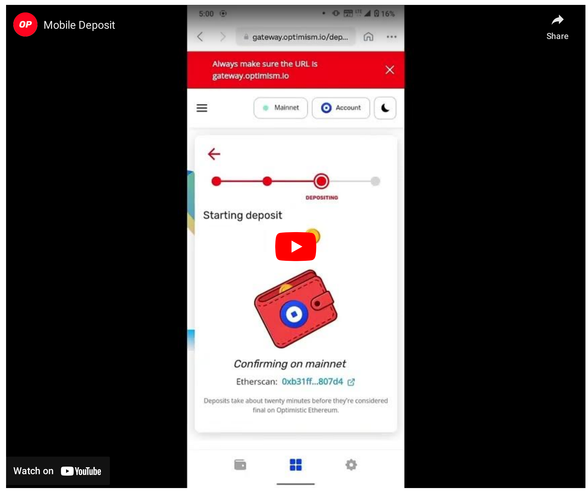
Bridging to Optimism is possible here: https://app.optimism.io/bridge

If you're bridging from a network other than the Ethereum network, we recommend the following services:

- https://stargate.finance/transfer — a multi-network bridge for stable coins
- https://www.bungee.exchange — an aggregator that shows the best available bridging options. Use their *Refuel* service to deposit smaller amounts in case you run out of `$ETH` to pay transaction fees.
- https://www.optimism.io/apps/bridges — for a full list of Optimism network bridging services.

> ⚠️ Some bridging services can take up to 20-30 minutes to complete a transfer of the assets.

Here's a walkthrough for how to use the Optimism Bridge on mobile:



A message to the veDAO community

The members of the veDAO core team learned a tremendous amount about `ve(3,3)` mechanics after receiving the 4th largest `$veNFT` in what's come to be called the *Solidly Wars*.

This experience resulted in a veDAO governance proposal, which passed, directing the team to seek opportunities outside of accruing Solidly vote share on the Fantom network.

The veDAO core team incubated Velodrome in accordance with DAO governance principles for the benefit of the DAO. veDAO's final governance act was to make good on this promise, distributing accumulated treasury in `$USDC` and `$VELO` tokens to `$WEVE` holders.

The veDAO community stuck with us through a seemingly impossible number of surprises, challenges, and disappointments. They're friends, allies, and, in some cases, central team members. Everything we do with Velodrome from here is rooted in our shared experience.

We believe that the veDAO members will be valuable, enthusiastic additions to the Optimism community in the coming weeks and will be instrumental in the long-term success of Velodrome.

Burning `$WEVE`

The redemption process uses LayerZero for a seamless experience. The process will burn user-provided `$WEVE` tokens on the Fantom network and will send `$USDC` and `$VELO` on the Optimism network.

The tokens will be sent to the same address, as with any bridging experience.

The `$WEVE` bridging service will be available at https://weve.velodrome.finance on May 31st and will be available until the 30th of June. Unclaimed `$USDC` and `$VELO` will be transferred back into the treasury.

Burning via Block Explorer

NOTE: There is currently a small UI issue with this process. TLDR the frontend is overestimating the amount of WeVE a user has to burn, which causes the contract call to fail.

Below are the steps you'll need to take in order to burn from the block explorer:

1. **Figure out how much WeVE you have to burn.** Go to https://ftmscan.com/address/0x911da02c1232a3c3e1418b834a311921143b04d7#readContract and navigate to Function #2, balanceOf. Enter in your address "0xabcd..." and click Query. Copy that value.
2. **Burn WeVE.** Navigate to the RedemptionSender (https://ftmscan.com/address/0x9809fB94eED086F9529df00d6f125Bf25Ee84A93#writeContract). NOTE Please double, triple check that this is the right address. Then enter the following arguments for Function #1, redeemWEVE

redeemWEVE: 30 (note that this value changes as gas on Optimism increases/decreases. Any leftover unused gas will be refunded by LayerZero)

amount: ANY value less than your balance found in Step 1

zroPaymentAddress: 0x0000000000000000000000000000000000000000

zroTransactionParams: 0x

Then click "Write" and your transaction should be good to go!

Initial Distribution

Velodrome will launch with initial distribution of 400M VELO airdropped to DeFi community members, protocols, and DAOs likeliest to play an active role in the Optimism ecosystem.

Details of the initial distribution and token emissinos are available in the Initial Distribution section of the Tokenomics.

Tokenomics

Velodrome Finance uses two tokens to manage its utility and governance:

- `$VELO` — ERC-20 utility token of the protocol
- `$veVELO` — ERC-721 governance token in the form of an NFT (non-fungible token)

`$VELO` is used for rewarding liquidity providers through emissions.

`$veVELO` is used for governance. Any `$VELO` holder can vote-escrow their tokens and receive a `$veVELO` (also known as veNFT) in exchange. Additional tokens can be added to the `$veVELO` NFT at any time.

The lock period (also known as vote-escrowed period, hence the *ve* prefix) can be up to 4 years, following the linear relationship shown below:

- 100 `$VELO` locked for 4 years will become 100 `$veVELO`
- 100 `$VELO` locked for 1 year will become 25 `$veVELO`

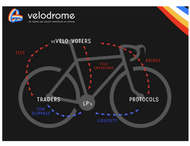
The longer the vesting time, the higher the voting power (voting weight) and rewards the `$veVELO` holder receives.

ve(3,3) Mechanics

Velodrome Finance mechanics reflect a combination of two DeFi concepts:

- Vote-Escrow — first introduced by Curve to strengthen incentives for long-term token holders
- Staking/Rebasing/Bonding or (3,3) game theory — designed by Olympus DAO

Combined, the ve(3,3) mechanism rewards behaviors correlated with Velodrome's success, such as liquidity provision and long-term token holding. Liquidity providers receive `$VELO` emissions, and `$veVELO` holders receive protocol fees, bribes, rebases, and governance power.



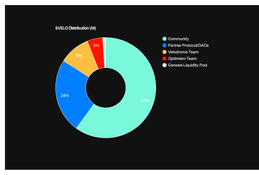
Below, we will walk through the components of the mechanism in order to explain how it helps the incentives flow to the most valuable of the ecosystem liquidity pools.

Initial Distribution

The airdrop claim period is now complete. Thank you to everyone who participated!

At launch we distributed `$VELO` and `$veVELO` to users and protocols we believe are likeliest to contribute to our mission to become the liquidity base layer of the Optimism ecosystem.

Distribution



Community

240M (60%) `$VELO` tokens will be distributed to the people who have played the biggest role in incubating Velodrome and those likeliest to contribute to its long-term success, including:

- `$AERO` holders (71%, 108M `$VELO`)
- `$OP` network users (19%, 72M `$VELO`)
  - 3755 `$VELO` wallet — Addresses qualified as Repeat Optimism Users
- Cross-chain DeFi users (10%, 60M `$VELO`)
  - 3500 `$VELO` wallet — Curve Protocol wallets with a 1450+ days (maximum) `$veCRV` lock time
  - 3000 `$VELO` wallet — Convex Protocol lockers of `$cvxCRV` since new lock contract deployment
  - 3000 `$VELO` wallet — Treasure DAO Genesis Miner `$MAGIC` stakers for 1- and 3-month periods
  - 2000 `$VELO` wallet — Platypus Protocol stakers with `$sPTP` and `$PTP` balance
  - 500 `$VELO` wallet — Redacted Cartel participants in genesis Dutch auction who didn't sell their `$BTRFLY`
  - 500 `$VELO` wallet — Eminence Finance wallets affected with EMN, eAAVE, eLINK, eYFI, eSNX or eCRV balance

Protocols

We will consider a variety of metrics in assessing the available protocols, including TVL, transaction volume, unique wallets, and Optimism team input.

The airdrop of 72M (18%) `$veVELO` is aimed at attracting and engaging 10-15 protocols most likely to contribute to Velodrome and Optimism's long-term success.

The amount of `$veVELO` airdropped will provide just enough voting power to familiarize the protocols with the ecosystem and give them a head start, but it will leave space for the protocols to accrue value by acquiring `$VELO` for long-term liquidity provision.

Grants

We have reserved 24M (6%) `$veVELO` to distribute to partner protocols after the launch. This will be used to engage partners in the ecosystem through grants.

Team

The team will receive an initial allocation that it will use to vote to drive emissions to key protocol pairs such as `$VELO-$USDC` and to support ongoing protocol development. The total team allocation is 40M (10%) in `$VELO` and `$veVELO`.

The team will vest 25% of its initial allocation in the form of a `$veVELO` and use it to vote for `$VELO` pairs in perpetuity.

While a fully autonomous and immutable protocol is an admirable objective, it comes at a cost. Velodrome Finance will ensure its long-term sustainability by employing a dedicated team focused on supporting the product, documentation, community, and ecosystem. As the protocol evolves, the Velodrome team will consider introducing more immutability or DAO components where appropriate.

To cover ongoing expenses and all the upcoming development efforts, 3% of the emissions will be going to the team address.

The team vesting compensation breakdown:

- 15,520,816 `$VELO` vesting for 12 months, 6-month lock in a `$veVELO` followed by a linear 6-month unlock period. 0.5% of total emissions, taken from emissions to treasury, will be added to this bucket for dilution control.
- 7,200,000 `$VELO` vesting for 24 months, 12-month lock in a `$veVELO` followed by a linear 12-month unlock period.
- All ongoing payments made to the team members in `$VELO` will vest for 6 months, 3-month lock in a `$veVELO` followed by a linear 3-month unlock period.

Optimism Team

The Optimism team has a vested interest in ensuring that Velodrome achieves its mission of serving as an ecosystem public good. The team will receive 20M (5%) `$veVELO` in the initial distribution, to support that interest.

Genesis Liquidity Pools

Genesis Pools will distribute 4M (1%) `$VELO` to liquidity providers of foundational token pairs to provide better liquidity and user experience from launch day. Genesis pool emissions will be first directed to the `$VELO-$USDC` pool and will start a few days before the first epoch votes are cast.

Emissions

The initial supply of `$VELO` is 400M.

Weekly emissions start at 15M `$VELO` (3.75% of the initial supply) and decay at 1% per week (epoch).

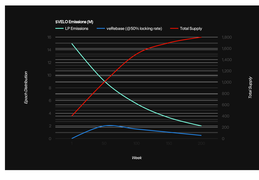
`$veVELO` holders receive a rebase proportional to epoch LP emissions and the ratio of `$veVELO` to `$VELO` supply, thus reducing vote power dilution for `$veVELO`!

The weekly rebase amount is calculated with the following formula:

```
(veVELOtotalSupply ÷ VELOtotalsupply)^2 * 0.5 * Emissions
```

`$veVELO` supply does not affect weekly LP emissions.

Emission Schedule



Gauge Voting

`$veVELO` holders decide which liquidity pools receive emissions in a given epoch by voting on their preferred liquidity pool gauges. `$VELO` emissions will be distributed proportionally to the total votes a liquidity pool receives.

In return, voters receive 100% of the trading fees and bribes collected through the liquidity pool they vote for.

Voting for gauges, or in fact any action related to the `$veVELO` NFT is allowed only once per epoch. This means that calling `Voter.reset()` (used for resetting an NFT vote state and usually required before merging it into another `$veVELO` NFT) or `Voter.poke()` (used to re-cast the votes for the current epoch in order to direct emissions and earn bribes) counts as an action for the current epoch.

While limiting the protocol participants to one action per epoch is not ideal, it does make the protocol safer against potential exploitative behaviour.

Unused `$veVELO` voting power is still taken into account as we calculate the weight of the vote upon epoch flip and based on the locked vesting slope.

Please make sure you always cast 100% of your voting power to avoid unexpected outcomes!

Rewards

There are 4 types of rewards on Velodrome Finance.

Emissions

Represent `$VELO` distributed to liquidity pool stakers. The amount of `$VELO` distributed towards every pool is proportional to the voting power received from the voters every epoch.

These rewards are streaming and are available for claim as these accrue.

Fees

Represent liquidity pool trading fees distributed to voters in pool tokens (e.g., if the pool is `sAMM-VELO/USDC` the distributed tokens are `$VELO` and `$USDC`).

The tokens are streaming proportionally to the voting power cast by a voter and the accrued amount of trading fees.

These rewards are available for claim as they accrue. They do not need to be claimed each epoch.

Bribes

In addition to the fees, liquidity pools allow external rewards from anyone (known as *bribes*). Bribes can be added to *whitelisted* pools and are distributed *only* to voters on that pool, proportionally to their share of pool votes.

These rewards are available for claim after the epoch flips (after Wednesday 23:59 UTC), and are proportional to the voting power cast by a voter (`$veVELO`).

Rebases

Represent `$veVELO` distributed to `$veVELO` holders in order to reduce the voting power dilution.

These rewards are available for claim as these accrue and are streaming proportionally to all `$veVELO` holders.

Rewards claim

Rebase rewards claim is available one full epoch after tokens are locked. External bribe rewards are claimable after a new epoch has started (epochs increment right after 23:59 UTC each Wednesday).

An example of bribes, voting, and rewards claim timeline:

- A new epoch starts Thursday (00:00 UTC)
- Bribes are deposited at any point in the epoch
- Voters vote for their preferred pools
- Once the next epoch arrives (the following Thursday), users are able to claim rewards from the UI or the corresponding `0x4ed4e862860beD51a9570b96d89aF5E1B0Efefed` contract

Whitelisting

While Velodrome supports permissionless liquidity pool and gauge creation, these can only include *whitelisted* tokens. The protocol will launch with an extensive list of pre-whitelisted tokens, including those from partner protocols.

Partners can request additional tokens to be whitelisted.

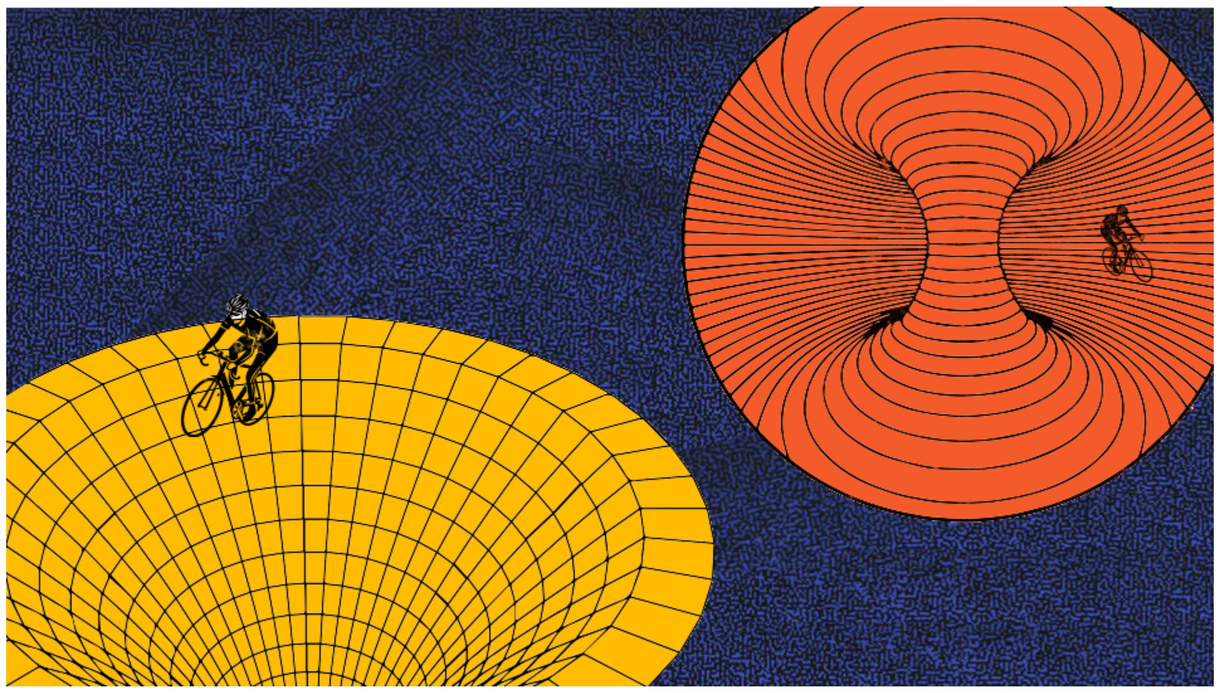
A permissionless whitelisting-on-chain governance process will be implemented in the future, pending required on-chain governance infrastructure on Optimism.

Commissaire

Requirements for whitelisting are critical to ensuring that the protocol cannot be exploited by actors attempting to game emissions.

To support the health of the protocol and ecosystem, the Commissaire (a Curve-esque *Emergency DAO*) will have the right to disable hostile gauges.

The Commissaire will initially consist of seven members from the Velodrome team and prominent figures from within the Optimism community.



Liquidity Pools

The core functionality of Velodrome Finance is to allow users to trade digital assets in a secure way, with very low fees and low slippage.

Slippage is the difference between the current market price of an asset and the price at which the actual trade/transaction is executed. This difference could result in a smaller amount (higher price paid) or a higher amount (smaller price paid) of desired tokens returned from a trade.

To provide access to the best rates on the market, we identified two types of assets:

- correlated - for example *stable coins* (`$USDC`, `$DAI`, etc.)
- uncorrelated - for example `$LINK` and `$CRV`

Velodrome Finance offers two different liquidity pool types based on token pair needs, *Stable Pools* and *Variable Pools*.

The protocol router evaluates both pool types to determine the most efficient price quotation and trade execution route available. To protect against flashloan attacks, the router will use 30-minute TWAPs (time-weighted average prices). The router doesn't require *upkeep* (external maintenance).

The *deeper* the liquidity of a given pool (higher value locked), the smaller the slippage it will offer.

Fees

On Velodrome Finance the trading fees are kept in the originally traded tokens (if you trade `$USDC` and `$VELO` the fees will be kept in the same tokens).

The trading fees for both liquidity pool types are 0.02%, and can be adjusted for up to 0.05%.

The Variable and Stable liquidity pools can be assigned different trading fees on Velodrome Finance.

Stable Pools

Stable pools are designed for assets which have little to no volatility. This means that the formula used for pricing the assets allows for low slippage even on large traded volumes.

> $x^3y + y^3x \geq k$

Variable Pools

Variable pools are designed for assets with high price volatility. These pools use a generic AMM formula.

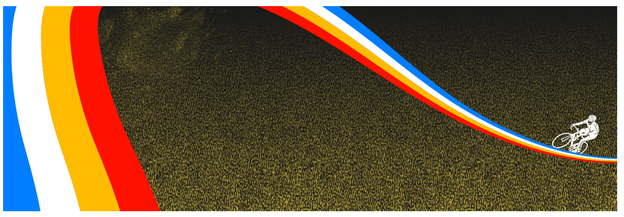
> $x \times y \geq k$

A visual representation of the formulas

The mathematical formulas are used to keep the total pool liquidity the same at all times.

Below, you can find a visual comparison between the stable (red) and volatile (green) AMM pricing equations, where:

- `x` is the amount of first asset in the pool
- `y` is the amount of second asset in the same pool
- `k` is a fixed constant



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 on 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).

Contract Addresses

Contract Name	Contract Address	Network
Velo	0x3c8B650257cFb5f272f799F5e2b4e65093a11a05	Optimism
GaugeFactory	0xC5be2c918EB04B091962fDF095A217A55CFA42C5	Optimism
BribeFactory	0xA84EA94Aa705F7d009CDDF2a60f65c0d446b748E	Optimism
WrappedBribeFactory	0xFC1AA395EBd27664B11fC093C07E10FF00f0122C	Optimism
PairFactory	0x25CbdDb98b35ab1FF77413456B31EC81A6B6B746	Optimism
Router	0x9c12939390052919aF3155f41Bf4160Fd3666A6f	Optimism
VelodromeLibrary	0xfb1Fc21D2937bF5a49D480189e7FEd42bF8282aD	Optimism
VeArtProxy	0x5F2f6721Ca0C5AC522BC875fA3F09bF693dcFa1D	Optimism
VotingEscrow	0x9c7305eb78a432ced5C4D14Cac27E8Ed569A2e26	Optimism
RewardsDistributor	0x5d5Bea9f0Fc13d967511668a60a3369fD53F784F	Optimism
Voter	0x09236cfF45047DBee6B921e00704bed6D6B8Cf7e	Optimism
Minter	0x3460Dc71A8863710D1C907B8d9D5DBC053a4102d	Optimism
RedemptionReceiver	0x846e822e9a00669dcC647079d7d625d2cd25A951	Optimism
VeloGovernor	0x64DD805aa894dc001f8505e000c7535179D96C9E	Optimism
MerkleClaim	0x00D59BC35174C3b250Dd92a363495d38C8777a49	Optimism
RedemptionSender	0x9809fB94eED086F9529df00d6f125Bf25Ee84A93	Fantom

All contracts are immutable. The latest public testnet deployment can be found here.

Tokenlist

In addition to the official Optimism tokens list, we maintain one as well with our partner tokens: https://docs.velodrome.finance/tokenlist.json

Differences from Solidly

As of August 2022, we've compiled a list of key differences between Velodrome's contracts and Solidly's.

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.

Addressing Issues in Our C4 Contest

Our Code4rena contest results were released on August 8, 2022 and are available here.

Below details how our team addressed these issues prior to our mainnet deploy.

High Risk (6)

[H-01] Users can get unlimited votes

- Fixed in our mainnet deploy, VoterEscrow.sol:L508.

[H-02] `VotingEscrow`'s merge and withdraw aren't available for approved users

- Still exists in our mainnet deploy, VoterEscrow.sol:L510.
- However does not result in major disruptions to user needs, also will not impact our future product plans.

[H-03] User rewards stop accruing after any `_writeCheckpoint` calling action

- Got rid of tracking user votes with a `prevVoteStatus` boolean, Gauge.sol.

[H-04] Bribe Rewards Struck In Contract If Deposited During First Epoch

- Got rid of the `deliverBribes()` method, also did not experience issue in prod. ExternalBribe.sol.

[H-05] Voting overwrites `checkpoint.voted` in last checkpoint, so users can just vote right before claiming rewards

- Got rid of tracking user votes with a `prevVoteStatus` boolean, Gauge.sol.

[H-06] Attacker can block LayerZero channel

- Added checks on RedemptionReciever.sol to ensure that no more WeVE tokens than eligible should be burned.

Medium Risk (17)

[M-01] Gauge set can be front run if bribe and gauge constructors aren't run atomically

- Got rid of `setGauge` method in both Bribe contracts, ExternalBribe.sol and InternalBribe.sol.

[M-02] `VeloGovernor`: `proposalNumerator` and team are updated by team, not governance

- "Issue" is expected behavior.

[M-03] Alter velo receptions computation

- See judge's comments, attack could only be pulled by deployer and wasn't.

[M-04] Malicious user can populate `rewards` array with tokens of their interest reaching limits of `MAX_REWARD_TOKENS`

- Judge's comment is accurate, does allow team to change real reward tokens (but so far non-issue).

[M-05] `Bribe.sol` is not meant to handle fee-on-transfer tokens

- Addressed in mainnet deploy by requiring reward tokens to be whitelisted, ExternalBribe.sol:L288.

[M-06] Voting tokens may be lost when given to non-EOA accounts

- Confirmed, see judge's comment.

[M-07] `RedemptionSender` should estimate fees to prevent failed transactions

- Done in mainnet deploy, RedemptionSender.sol:L32.

[M-08] Temporary DOS by calling `notifyRewardAmount()` in Bribe/Gauge with malicious tokens

- Addressed by adding whitelist for reward tokens, ExternalBribe.sol:L288.

[M-09] Owner's delegates should be decreased in `_burn()`

- Addressed in mainnet deploy, VotingEscrow.sol:L508.

[M-10] Rewards aren't updated before user's balance change in Gauge's `withdrawToken`

- Addressed in mainnet deploy, Gauge.sol:L502.

[M-11] Griefing Attack By Extending The Reward Duration

- Addressed in mainnet deploy by reverting to original implementation, Gauge.sol:L546.

[M-12] Rewards can be locked in Bribe contract because distributing them depends on base token reward amount and `Gauge.deliverBribes()` is not always called by `Voter.distribute()`

- Addressed in mainnet deploy by decoupling bribe delivery from gauge reward distribution, Voter.sol:L369.

[M-13] Bribe Rewards Not Collected In Current Period Will Be Lost Forever

- Addressed in mainnet by reverting to an implementation more similar to Solidly's, which does not couple gauge and bribe rewards. ExternalBribe.sol.

[M-14] Wrong reward distribution in Bribe because `deliverReward()` won't set `tokenRewardsPerEpoch[token][epochStart]` to 0

- Will be addressed with an upcoming fix (will be linked here once contracts are live). In the interim, relevant parties (i.e. protocols who wish to bribe) should get in touch with our team.

[M-15] Wrong calculation for the new `rewardRate[token]` can cause some of the late users can not get their rewards

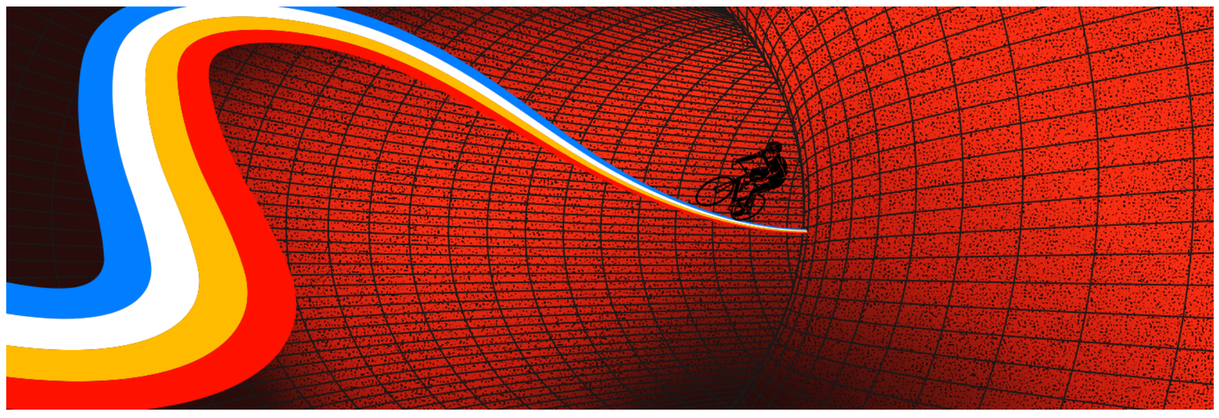
- Addressed in mainnet deploy as we reverted to a duration of 7 days instead of 5, Gauge.sol#L535.

[M-16] Wrong `DOMAIN_TYPEHASH` definition

- Not addressed in mainnet deploy, but see judge's comment.

[M-17] WeVE (FTM) may be lost forever if redemption process is failed

- Error won't happen as long as contracts were initialized correctly (which they were in prod).



Legal Disclaimer

Please read this disclaimer carefully before using https://velodrome.finance and/or any of its sub-domains (hereinafter referred to as the "Website").

By using the Website, you confirm that you accept this legal disclaimer and agree to comply with it. If you do not agree, you must not use the Website.

Information published is not advice

The information provided on the Website does not constitute investment advice, financial advice, trading advice, or any other sort of advice, and you should not treat any of the Website's content as such. Our team provides the Website as a service to the public, and is not responsible for, and expressly disclaims all liability for, damages of any kind arising out of use, reference to, or reliance on any information contained within the Website. While the information contained within the Website is periodically updated, no guarantee is given that the information provided in the Website is correct, complete, and up-to-date.

Usage risks

The Website will not be responsible for any losses, damages, or claims arising from events falling within the scope of events like, but not limited to: mistakes made by the user (e.g., payments sent to wrong addresses), software problems of the Website or any related software or service (e.g., malware or unsafe cryptographic libraries), technical failures (e.g., hardware wallets malfunction), security problems experienced by the user (e.g., unauthorized access to wallets), actions or inactions of third parties (e.g., bankruptcy of service providers, information security attacks on service providers, and fraud conducted by third parties).

Investment risks

The investment in cryptocurrencies can lead to loss of money and prices having large range fluctuations. The information published on the Website cannot guarantee no money loss.

The Website user is responsible for understanding these risks, doing own due diligence, and making own decision on how to interface with the Website.

Compliance with tax obligations

The users of the Website are solely responsible to determinate what, if any, taxes apply to their cryptocurrency holdings. The owners of, or contributors to, the Website are NOT responsible for determining the taxes that apply to user transactions.

No warranties

The Website is provided on an "as is" basis without any warranties of any kind regarding the Website and/or any content, data, materials and/or services provided on the Website.

The Website functionality is not guaranteed and could be disabled fully or in part without prior notice.

Security

Security audits don't eliminate risks completely. The Website is not guaranteed to be secure or free from bugs or viruses.

Limitation of liability

Unless otherwise required by law, in no event shall the owners of, or contributors to, the Website be liable for any damages of any kind, including, but not limited to, loss of use, loss of profits, or loss of data arising out of or in any way connected with the use of the Website.

Arbitration

The user of the Website agrees to arbitrate any dispute arising from or in connection with the Website or this disclaimer, except for disputes related to copyrights, logos, trademarks, trade names, trade secrets or patents.