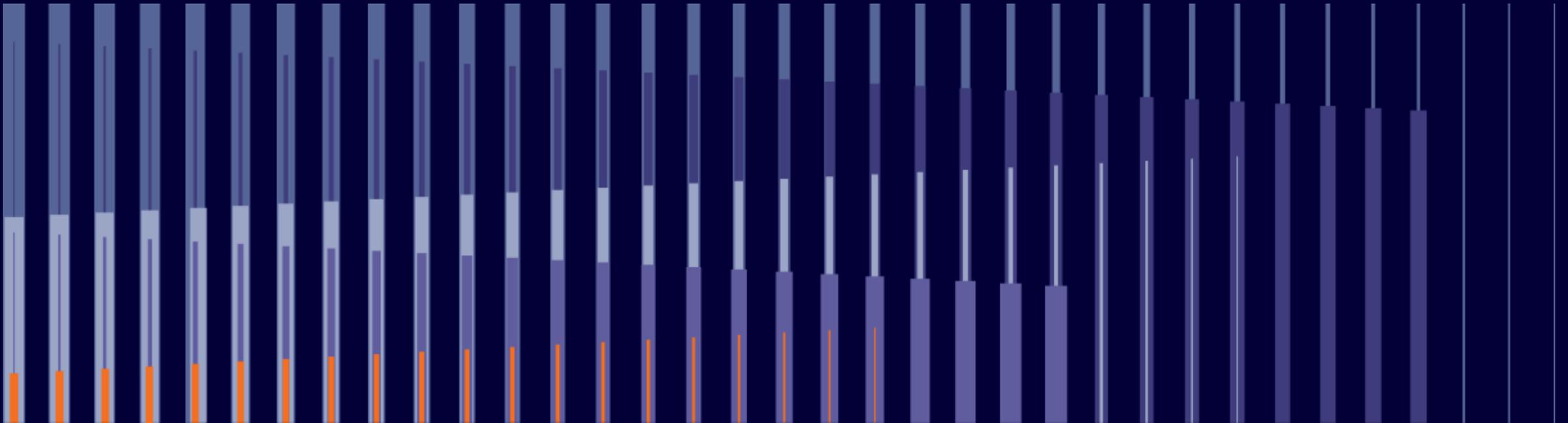


# Official Report Curve Finance



---

INDEX

1. Abstract
2. Problem Statement
3. Solution
4. Technology
5. Ecosystem
6. Community
7. Team Overview
8. Coinmetrics
9. Token Distribution
10. Roadmap
11. Exchanges
12. General Remarks

---

HODL TEAM



**Vladimir Mikirtumov**

Research Analyst

- Crypto Research Analyst & Trader since 2017
- BSc in Aerospace Engineering at TU Delft



**Tobias Datema**

Content Marketeer

- Worked in the crypto industry since 2019
- International Business Management and Global Marketing & Sales

This Hodl Research Report is written by our Research Analyst, Vladimir Mikirtumov and our Content Marketeer, Tobias Datema.

---

**ABSTRACT**

In the early days of cryptocurrency, centralized exchanges (CEXs) were able to lower the entry barrier for starting investors.

They provided user-friendly solutions that made buying, selling and storing cryptocurrencies accessible. These exchanges offer a wide variety of cryptocurrencies that can be easily bought and sold with low fees and provide strong security features to their users. However, this does create a dilemma because cryptocurrencies were meant to give the power back to their users through self-custody. These centralized solutions, however, function in the same way as a bank, removing self-custody and re-introducing a single point of failure.

In the quest for an alternative, users created the first “Decentralized Exchange” (DEX) with smart contracts. These exchanges operate in a decentralized environment, so users maintain self-custody over their funds while buying and selling cryptocurrency. The downside of these exchanges is the high slippage costs caused by the underlying smart contract mechanism.

Curve Finance aims to solve this problem by providing a decentralized exchange that is optimized for low slippage trades against pegged assets such as dollar-pegged stablecoins. Curve achieves this via its unique Automated Market Maker (AMM), a protocol that uses a mathematical formula to price assets. This AMM provides users with low slippage trades and liquidity providers a steady income coming from conversion fees.

"Automatic market-makers are one of the major innovations which decentralized finance brought."

---

Michael Egorov, Founder Curve Finance

---

**PROBLEM STATEMENT**

# When new technological advances are introduced, the usability of the technology is geared towards a small number of niche individuals – this was also the case with cryptocurrencies.

Centralized cryptocurrency exchanges were able to lower the barrier of entry for the general public by improving the user experience.

CEXs offer their customers a vast array of competitive financial products related to cryptocurrencies such as spot and derivatives markets. This advantage comes from centralized order books and professional market makers that bring a lot of liquidity. Additionally, these organizations provide their clients with high-level security in order to protect their customer's assets.

At the same time, when a user puts their funds on a CEX, he/she must give up self-custody rights. This creates a dilemma as one of the main mottos of the space is 'not your keys, not your coins', referring to the fact that users do not have direct access to their personal funds, as the exchange has them.

As the downsides of centralized exchanges became clearer, users started looking for, and building alternatives. This inclination gave birth to the decentralized exchange (DEX), an exchange built upon smart contracts.

These exchanges allow users to buy and sell cryptocurrencies while maintaining self-custody over their funds. However, users of DEXs often face high trading costs due to slippage caused by the underlying smart-contract mechanism. This results in a considerable difference between the expected and actual price of a trade.

Curve Finance aims to solve this problem by offering users a DEX that is optimized to execute low slippage trades between stablecoins and other pegged assets which are meant to have the same market value. Their uniquely developed Automated Market Maker (AMM) uses a special formula to price assets, making it possible for users to avoid unnecessarily high slippage fees.

---

SOLUTION

Curve Finance, previously named StableSwap which was launched in 2020, aims to provide traders with low slippage trades on stablecoins and other pegged assets.

Most of the current DEXs can't offer this service to their clients due to their underlying trading mechanisms. For a DEX to operate in a decentralized environment, it utilizes smart contracts, which combine the concepts of a liquidity pool and an Automated Market Maker (AMM). The liquidity pool typically holds two cryptocurrencies that users deposit, thus providing liquidity to the system which users and traders can use to execute a transaction.

An AMM refers to the smart contract algorithms that are used to determine the correct value of the assets bought/sold by the end-user. The team behind Curve Finance saw that most of the implemented AMM models couldn't offer low slippage trades on stable assets. Therefore, Curve decided to tackle this gap in the market.

These pools consist of cryptocurrencies that behave in a similar manner, with an emphasis on price volatility. High volatility creates high slippage costs as the value of the assets can deviate, disturbing the balance of the liquidity pool. So, the low volatility of the assets used on Curve typically results in minimal slippage.

The reduced-price fluctuations of stablecoins and other pegged assets provide a platform that offers minimal price slippage as well as an efficient 'savings account' for liquidity providers on the platform.

### How AMMs work



**Source** [consensys.net/blog/cryptoeconomic-research/maple-finance-creating-a-decentralized-credit-market/](https://consensys.net/blog/cryptoeconomic-research/maple-finance-creating-a-decentralized-credit-market/)

## Constant *Price*



$$X + Y = K$$

## Constant *Product*



$$X * Y = K$$

---

### CURVE'S FOUNDATIONS

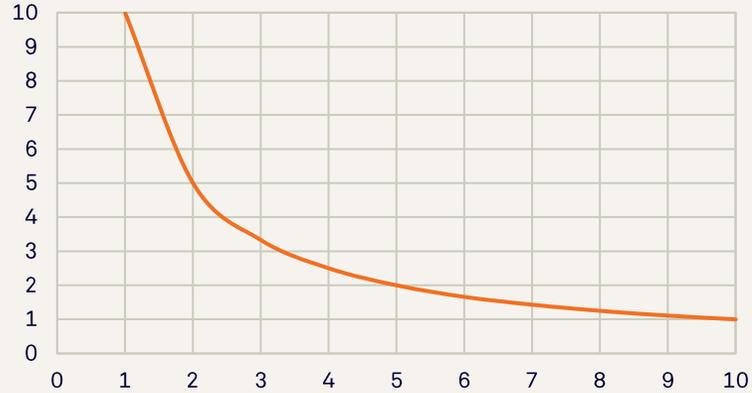
Curve Finance has combined two concepts which are known as the Constant Price and Constant Product formulas.

In order to provide low slippage and low fees when trading stablecoins such as USDC, DAI, USDT and pegged assets such as wrapped BTC.

These formulas represent ways on how to group two assets in a liquidity pool. In both formulas, X and Y represent the pooled assets present inside of the liquidity pool. The K represents the element that is meant to stay constant as people trade in-and-out of a liquidity pool.

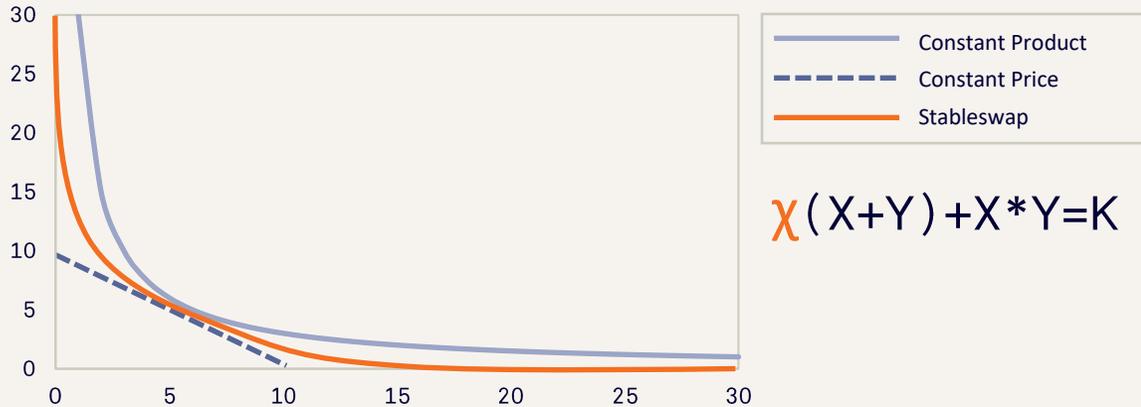
As users and traders get in-and-out of the liquidity pool, the balance of the assets within the pool changes. These usually start at the most balanced point of 50/50 and then the dynamics of the market changes the pool's balance over time.

## Constant *Product*



$$X * Y = K$$

## *Stableswap*



$$X(X+Y) + X*Y = K$$

### CURVE'S FOUNDATION

The downside of the Constant Price formula is that it by design allows the liquidity pool to be fully drained,

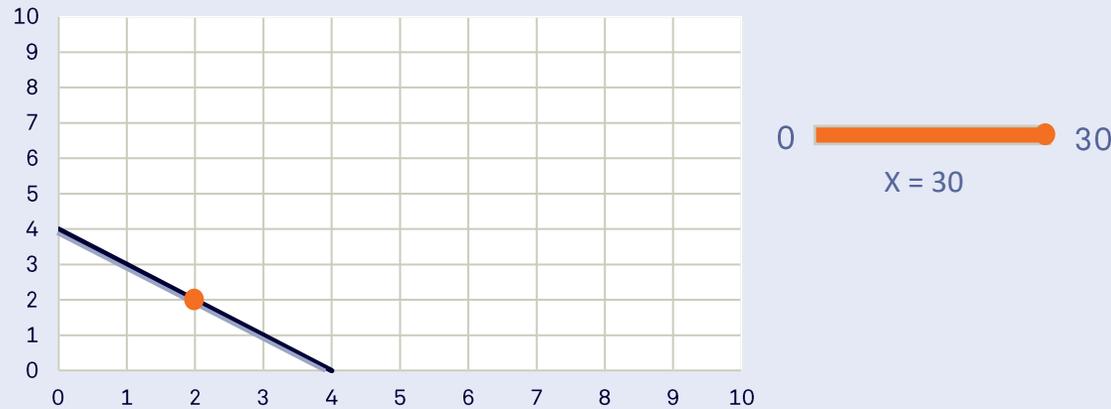
as the price of an asset will always remain the same regardless of the existing balance in the pools. On the other hand, the Constant Product has gained a lot of popularity as the algorithm auto-adjusts the price, ensuring that there is always liquidity at any price. The disadvantage of this model is that it requires enormous liquidity for slippage not to go unnoticed – the price goes up exponentially as we travel away from equilibrium.

By combining both concepts, Curve Finance merges both: the Constant Price formula allows users to have no slippage, but it is not ideal because the liquidity pool can run out of tokens. The Constant Product is self-regulating; however, the user gets a lot of slippage.

## Pool is *Unbalanced*



## Pool is *Balanced*



$$\chi(X+Y) + X*Y=K$$

### CURVE'S ALGORITHM

When the pool is very balanced, Stableswap looks a lot like the Constant Price formula which offers low slippage.

As the pool becomes less balanced, the Stableswap algorithm begins to look more like the Constant Product formula. Thus, swapping then becomes expensive and the market is incentivized to bring the pool back to balance.

This change is measured by a particular factor called X (Chi) factor. This allows the algorithm to amplify the Constant Price portion of the equation which allows the end-user to experience less slippage.

As seen on the right where  $X = 0$ , when the pool is very out of balance, meaning that the two pooled tokens are very far away from being 50/50, the X factor will decrease. On the other hand, if the pool is close to a 50/50 balance, the X factor will increase giving the end-user one of the most competitive pricing mechanisms in all crypto, where very little is given away through slippage.

---

**AUDIT**

Curve Finance is a DEX specifically designed to offer traders low slippage trades on stablecoins and steady, low-risk earnings for liquidity providers.

Curve is one of the most popular DeFi platforms as the protocol favors stability and composability over volatility and speculation.

Currently, the protocol is entrusted with \$3.7B in value locked across 11 different networks, with most of the platform's activity still occurring on Ethereum. On average, the pool's trading volume varies from \$100 to \$200 million dollars per day. This puts it as the third most used exchange in DeFi by spot trading volume.

Curve was the first DEX to revolutionize the trading of stablecoins and pegged assets and has managed to hold its position as an important platform in the cryptocurrency market until this day.

As the Curve exchange is one of the biggest decentralized exchanges in the industry, the platform has undergone various security audits. The smart contracts of the Curve platform were audited by Trail of Bits and the Decentralized Autonomous Organization contracts were audited by Quantstamp and mixBytes. Important to note, although the contracts were audited, it doesn't eliminate the risk entirely.

---

**ECOSYSTEM**

Curve Finance launched in 2020 and has since then revolutionized the use and popularity of AMMs.

### **Yearn Finance & Compound**

This solution has attracted thousands of cryptocurrency traders as well as other established DeFi protocols within DeFi to integrate their products into Curve Finance. This includes platforms such as Yearn Finance and Compound, a yield aggregator and lending marketplace respectively, both of which are solid pillars within DeFi.

### **Convex Finance, Frax Finance and DAO's**

The proliferation of stablecoins and pegged derivatives throughout DeFi also gave rise to platforms such as Convex Finance, Frax Finance and many other Decentralized Autonomous Organizations to integrate the Curve platform within their ecosystem. This allows them to offer their own users low-risk, sustainable yields.

---

**COMMUNITY**

Since the founding of Curve Finance, the protocol has gained popularity among individuals and organizations native to the cryptocurrency market. Curve's unique use-case for low slippage trades and a steady income for liquidity providers have taken the market by storm.

The protocol has gained a massive following among various communication channels. Twitter is its largest communication channel with a total of 346K followers. Many enthusiasts want to stay up-to-date as the protocol keeps revolutionizing the scene.

The involvement of the community is also illustrated in the voting rounds of the protocol as it, in most instances, will have an impact on the yields that the liquidity providers receive. This has repercussions on a lot of platforms that are built around the Curve Finance ecosystem. Curve Finance manages to align the incentives of its stakeholders very well in the process.

---

MEET THE TEAM



**Michael Egorov**

CEO & FOUNDER

- Senior Software Engineer at LinkedIn
- Founder of NuCypher



**Julien Bouteloup**

CORE TEAM MEMBER

- Director at Doshup
- Founder of Flyingcarpet
- Founder Stake Capital Group

COINMETRICS

# Insights into *Curve Finance*

- Token type: ERC 20
- Current circulating supply: 868,073,642

General	
Total supply	1,978,662,906
Maximum supply	3,303,030,299
Market Cap	\$689,452,145
Full diluted market Cap	\$2,623,373,428

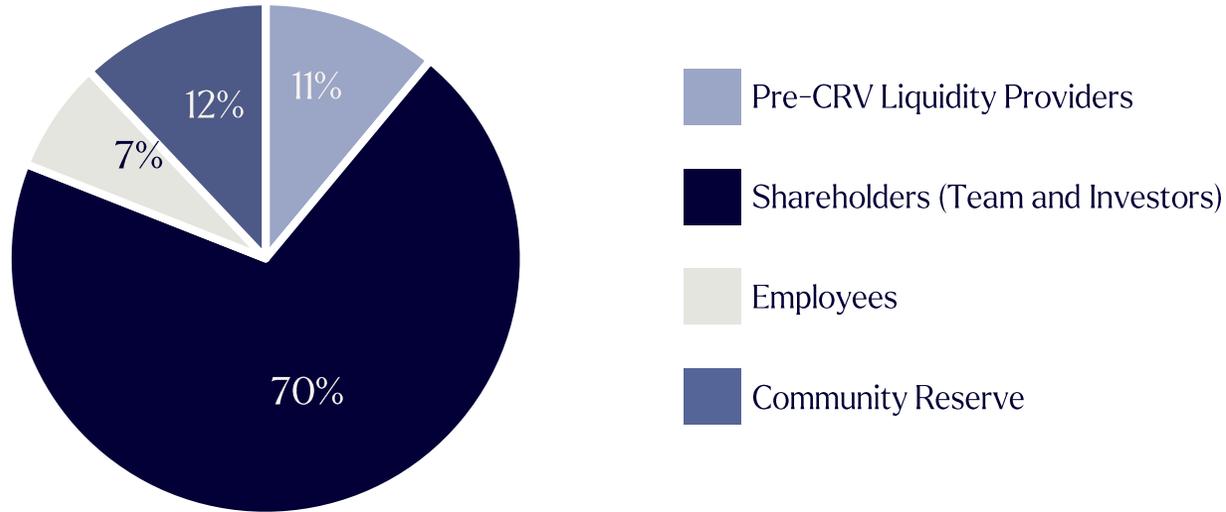
Pricing	
Price in USD	0,79
All time high in USD	\$15.37 (14-8-2020)
All time low	\$0.33157 on (5-11-2020)
30 Price Range	\$ 0,57 - \$ 0,82

Token Generation Event	
TGE Price	\$6.90
TGE Date	14-8-2020
Total USD Raised	\$0

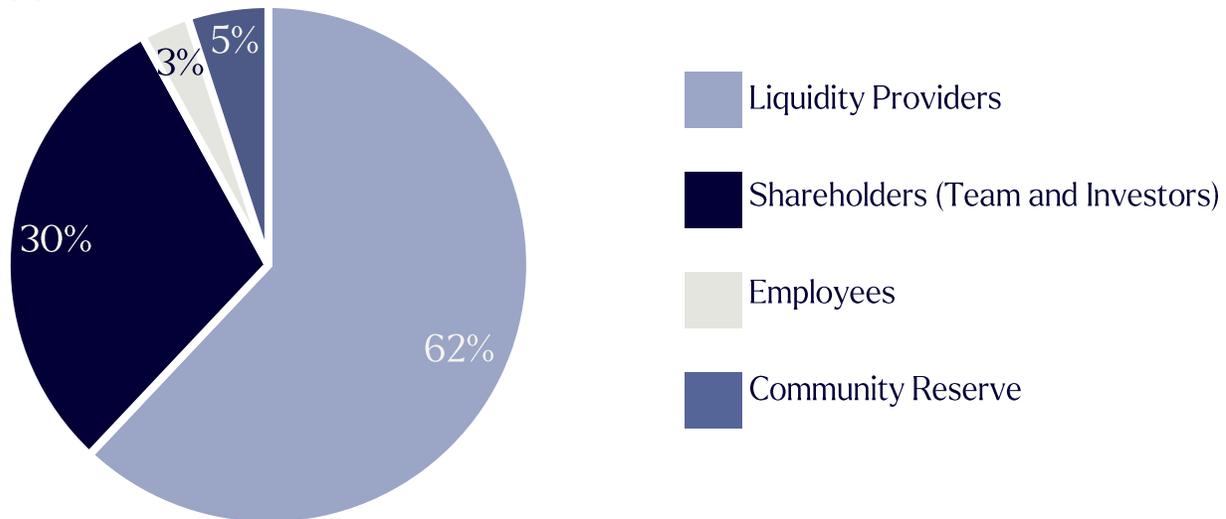
On-chain data	
Holders	79,598
Top 100 holders	94.04% of the supply
Total Value Locked (TVL)	\$3,628,622,792

Source [coingecko.com/en/coins/curve](https://coingecko.com/en/coins/curve) (11-7-2023)

### Initial Supply Distribution



### Total Supply Distribution



### DISTRIBUTION

Like many other DeFi native protocols, the launch of the \$CRV token happened without many outside investments,

with the initial creation of the token’s value coming from the team and early ecosystem participants.

The \$CRV token officially launched on August 13th, 2020, with no tokens in circulation and an initial release rate of 2M \$CRV tokens per day. This flow of tokens is distributed mainly to liquidity providers who are thus incentivized to provide liquidity on the Curve Finance platform.

It is important to note that any tokens allocated to the Team, Employees and Shareholders have vesting schedules which last up to four years. In the meantime, the clock of liquidity continues ticking as the \$CRV token keeps being distributed across the main users of its platform: approximately 57% of the total supply.

---

## TOKEN UTILITIES

The main purpose of the \$CRV token is to make its participants engage with the protocol and share benefits as the Curve Finance platform grows.

Currently, \$CRV has three main use cases: boosting rewards, staking and governance.

In order to get these benefits, Curve has integrated a vote escrowed token or \$veCRV. A vote escrowed \$veCRV is a token that can be locked in for a period of up to four years. If you lock 100 \$CRV for one year, you will get 25 \$veCRV. If you lock for four years, you will get 100 \$veCRV which is the maximum. This increases your voting power and the boost you can have on your capital while providing liquidity.

### Boosting

Vote locking your \$CRV tokens and converting them into \$veCRV can earn you a boost up to 2.5x on your existing liquidity. Thus, you can increase a 3% yearly yield on stablecoins up to 7.5% under certain conditions.

### Staking

Locking \$CRV into \$veCRV will also give you the right to earn a portion of the trading fees generated by the Curve platform. From the 19th of September 2020, 50% of all trading fees are distributed to \$veCRV holders.

### Governance

\$veCRV token holders decide which pools get the \$CRV tokens which are distributed daily. These additional \$CRV tokens allow your pool to get the yield boost. \$veCRV token holders can also participate in deciding the development of the protocol by voting on the submitted proposals.

# Curve recently launched its self-developed dollar-pegged stablecoin, crvUSD, with the aim of optimizing swaps between assets that are pegged to the same value.

This development positions Curve as a potential leading stablecoin exchange in the DeFi space, catering to Ethereum Virtual Machine (EVM) compatible chains.

To obtain CRVUSD, users need to provide collateral approved by Curve, which includes assets such as wseth, wbtc, sfrxETH, and ETH.

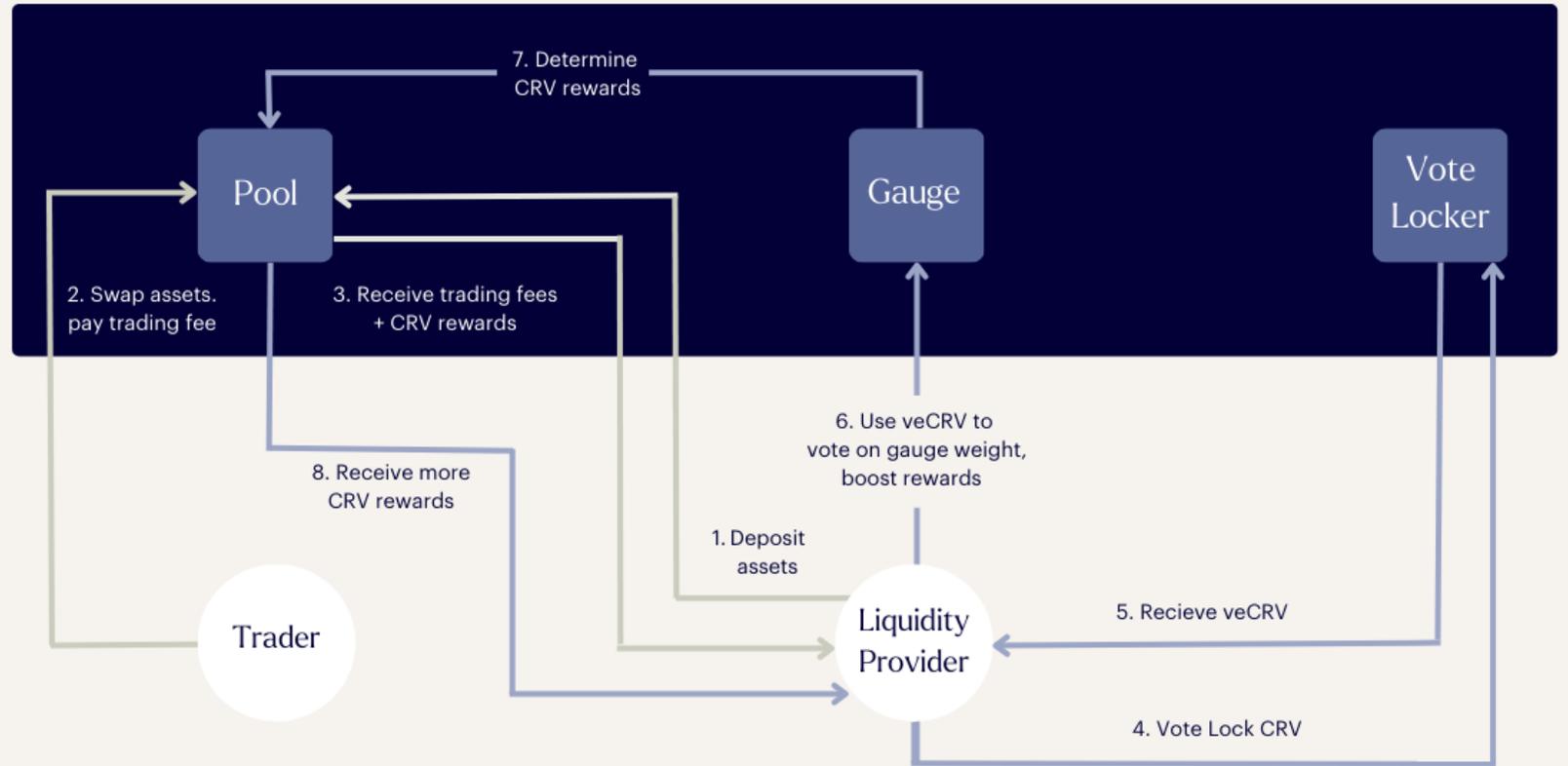
To maintain the dollar-peg, the system automatically sells a portion of the collateral if its value decreases. Conversely, if the collateral value increases, the system acquires CRVUSD.

What sets CRVUSD apart is its approach to managing these sales and purchases. It employs a system called LLAMMA, which gradually sells or buys small amounts based on the rate at which the collateral value changes.

This differs from other systems that might sell everything at once in the event of a rapid decrease in value.

The introduction of CRVUSD is expected to attract more liquidity providers to participate in Curve's liquidity pools, allowing them to maximize capital efficiency. Additionally, LLAMA's constant rebalancing of users' collateral will increase trading volume in Curve's pools, resulting in more fees for the protocol and benefits for veCRV token holders. Furthermore, CRVUSD loans are likely to incur borrowing fees, creating a new revenue stream for the protocol and its veCRV token holders.

# Flow of the *\$CRV Token*



Source [twitter.com/cryptopothu/status/1516227398093533186](https://twitter.com/cryptopothu/status/1516227398093533186)

---

**TOKENOMICS**

By introducing the \$veCRV token, Curve has popularized a mechanism that allows to align incentives of \$CRV token holders to Curve's incentives.

By vote locking \$CRV, \$CRV tokens are temporarily taken out of the circulating supply and thus cannot be sold – this is good for the Curve protocol. Moreover, \$veCRV is non-transferrable so vote-lockers are committed to their position for the duration of the lock.

At the same time, \$CRV vote-lockers benefit from this model as well: they receive 50% of Curve's trading fees which are paid in stablecoins. Also, certain Curve pools will also get rewarded with \$CRV via gauge weights. Gauge weights determine how many \$CRV tokens will be allocated to each pool from a fixed number of \$CRV tokens, programmed to be distributed daily. This distribution can only be voted upon if you hold \$veCRV tokens.

---

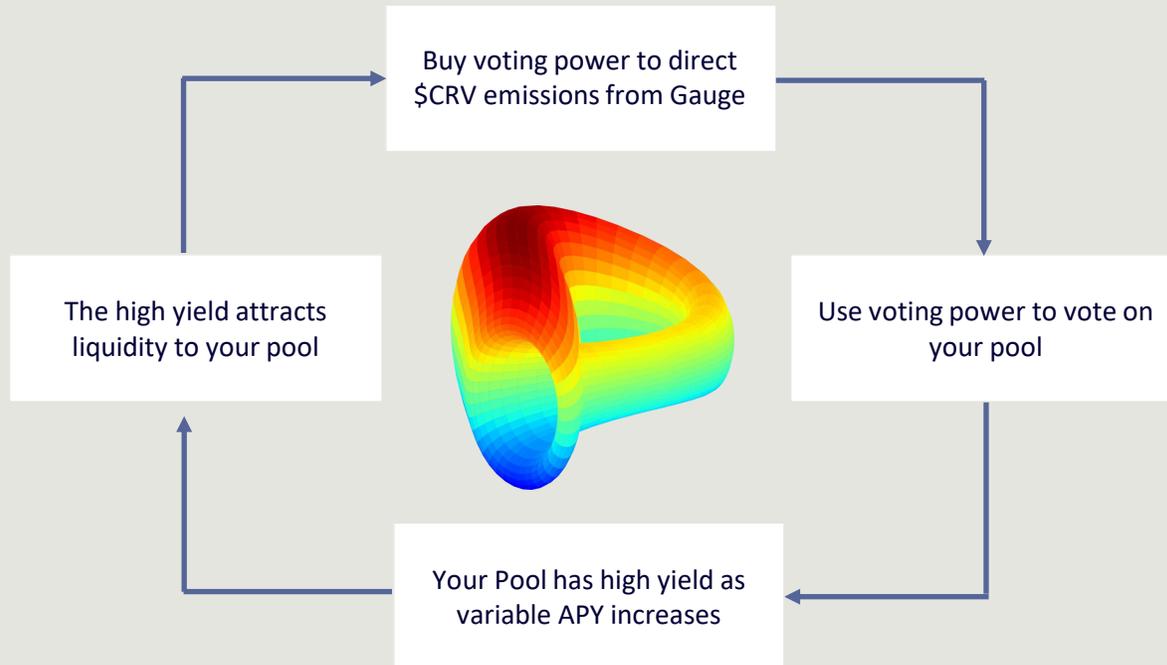
TOKENOMICS

This circular mechanism has created an interesting incentive structure that has a lot of game theory.

On one hand, locking \$CRV and holding \$veCRV gives you a boost on your provided liquidity and a portion of the platform's fees. In return, you must lock \$CRV for a long period of time which has an opportunity cost.

This has led a lot of external platforms and DAOs to try to accumulate \$CRV tokens to convert them into \$veCRV. In this way, they can offer their own users additional benefits which would be very hard to achieve for a single individual – notably Convex Finance owns 51% of all \$veCRV tokens.

Despite its clear first-mover advantage, other platforms aim to offer similar and superior services than Convex Finance. This has led to the term of 'Curve Wars' where different protocols aim to accumulate and lock as many \$CRV tokens as possible.



Source [twitter.com/Riley\\_gmi/status/1531259708094304256](https://twitter.com/Riley_gmi/status/1531259708094304256)

The total supply of \$CRV tokens is set to 3,303,030,299. This figure is not set in stone, it is merely a limit that is reached due to Curve Finance's inflation system.

Initial inflation is set at **279.6M \$CRV** tokens per year and decreases **16%** year-over-year. This eventually reaches a limit in 357 years after the protocol's establishment where the last token will be emitted.

Currently, there are **868M \$CRV** tokens in circulation, with the maximum supply set at **3303M** tokens this means that **26,28%** of all tokens are now in circulation. This is because the inflation model of the \$CRV tokens is designed for the coins to be distributed over the course of hundreds of years, including the current lockup of tokens allocated to the core team and shareholders, which will release slowly as the vesting schedule progresses. The distribution of the token seems quite fair, as the top 100 wallet addresses contain **1857M \$CRV** tokens.

Compared to the total supply this is quite a lot, however, it is worth mentioning that the top 100 addresses include vested tokens, exchanges and grouped pools of \$CRV accumulators that convert the token into \$veCRV.

The inflationary model of Curve has been quite hard on the ecosystem, more specifically on the token price. At the same time, we can argue that the \$CRV token distribution has incentivized a lot of DeFi participants, having gathered many token holders with well-over **416** wallets. Lastly, **38.6%** of circulating \$CRV tokens have been converted into \$veCRV and will be locked in for an average of 56 years. This phenomenon will likely lead to less selling pressure on the token which, when combined with the decreased yearly inflation, might result in \$CRV scarcity on the open market.

---

**TOKEN ALLOCATION**

Like many of the projects that were early in DeFi, Curve Finance's token distribution is fairly even as it is designed to grow the protocol organically. To highlight this fact, it is relevant to compare the initial supply distribution with the total supply distribution.

Most notably liquidity providers go from 11% to 62% of the total distribution. The shareholders decrease their token allocation from 70% to 30%. There is no denying that this contributes to the token allocation becoming more decentralized. This is an indication of a healthy ecosystem where new players come in naturally.

---

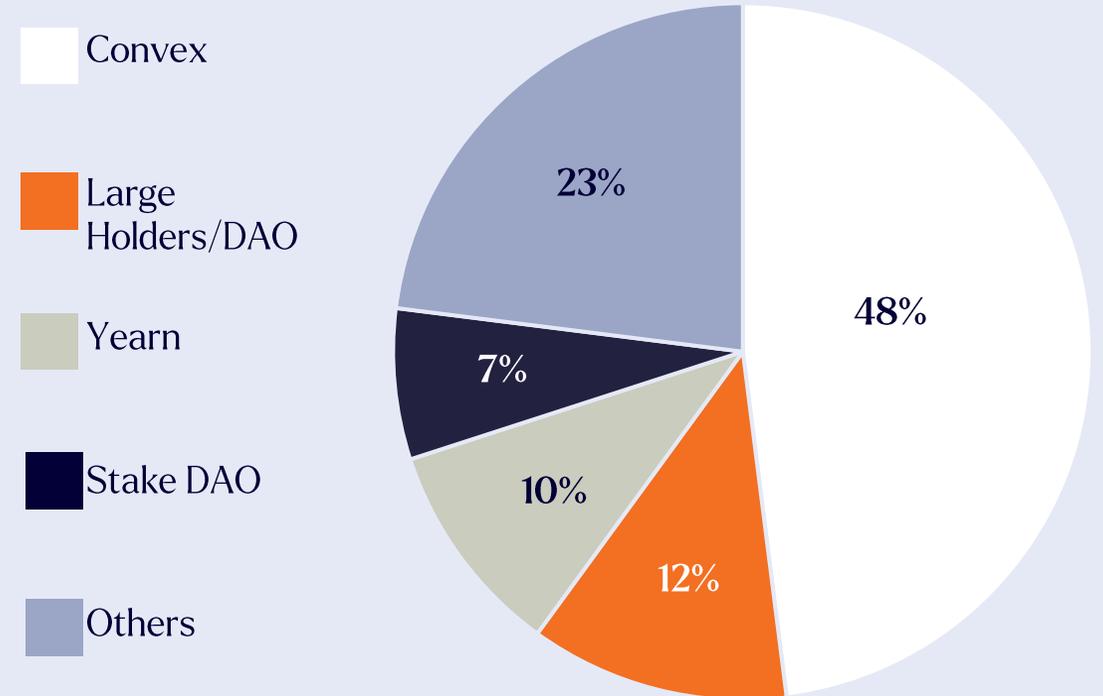
VALUE OF THE \$CRV TOKEN

When determining the value of the \$CRV token as well as its future value,

it is important to consider that there is still a significant amount of inflation on a yearly basis, at least for the next 2-5 years.

The value of the \$CRV token comes from the utilities that come with it, and these utilities can only be accessed if a \$CRV token is locked for a period of up to four years and converted into \$veCRV. If you have locked \$CRV into \$veCRV you can use the token for governance, boosting your own liquidity provision rewards and shared rewards from the platform's fees.

This is a novel approach that gives the \$CRV token utmost importance within the ecosystem. This is a growing trend with three projects already getting ahead, and locking \$CRV into \$veCRV: these are Convex Finance, Yearn Finance and StakedAO.



---

**ROADMAP**

As one of the most active DAOs in DeFi, Curve Finance does not have a delineated roadmap for the next few years.

The current tokenholders, specifically those that hold \$veCRV, are incentivized to improve the current product. This can include starting discussions and voting on new liquidity pools being created, changing parameters within existing liquidity pools or other plans that develop the future of Curve.

Curve Finance does have one main objective, which is the reduction or vanishing of impermanent loss which is a very well-known problem within AMM pools that hold two different assets.

With the recent release of the Curve v2 whitepaper, the team shares how they aim to reduce impermanent loss. This will hopefully lead to more liquidity providers and volume coming to the Curve platform: the graph on the right displays the volume share of the top 5 decentralized exchanges, with Uniswap still leading.

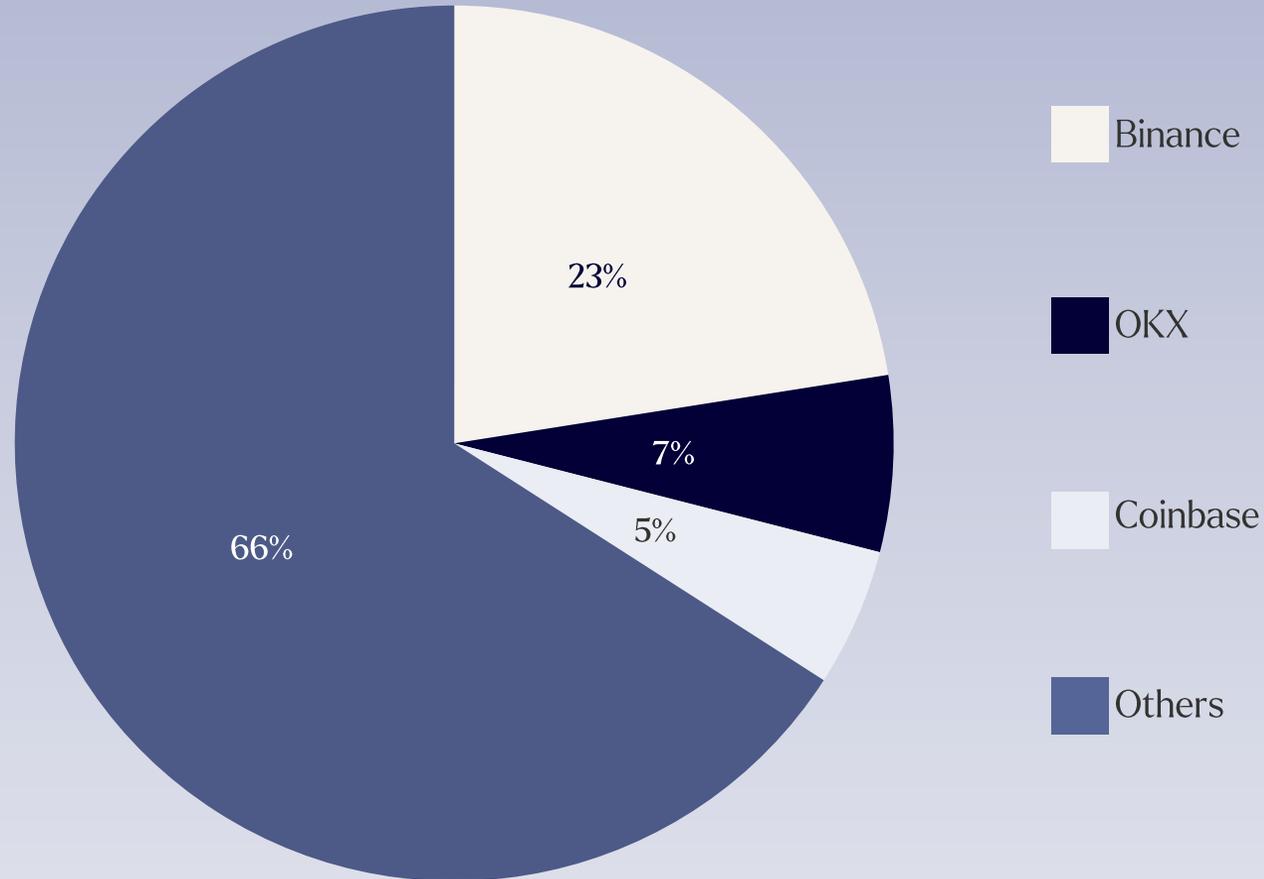
---

EXCHANGES

The Curve Finance token was launched at the beginning of Q3 in 2020 with a small percentage of the supply being distributed among the early liquidity providers on the platform.

The token was listed on Binance within 5 minutes after the launch, which caused extreme price fluctuations.

## Volume share on exchanges



Source [coingecko.com/en/coins/curve](https://coingecko.com/en/coins/curve)

---

## FINAL CONCLUSION

### General remarks

Back in 2019, a whitepaper was released which aimed to solve big inefficiencies in the DEX market. This resulted in the development of Curve Finance and months later the \$CRV and \$veCRV tokens.

Curve has allowed a considerable increase in capital efficiency for liquidity pools that hold two assets that are meant to represent a similar value, for instance stablecoins such as USDT,USDC,DAI or renBTC and WBTC - both representations of Bitcoin on Ethereum. This has led to liquidity providers having low to no impermanent loss on their deposits, a very frequent problem seen in most liquidity pools. Also, a very vibrant ecosystem has sparked around the voting power of the \$veCRV token.

### Long-term investment

As with most DeFi platforms, the protocols are forced to balance rewards distributed to community members versus creating mechanisms to lock some of the tokens from the circulating supply. The first approach will attract volume which will be looking for yields, but on its own, it would lead to the demise of the protocol's reward system given enough time. This is because most members would sell \$CRV tokens on the open market, making future rewards less valuable.

That is why the introduction of the \$veCRV token is so impactful as it allows Curve to distribute rewards, but most of these rewards will be given to individuals who have proven their long-term commitment to the Curve Finance platform by locking \$CRV and holding \$veCRV. For a platform that has been around for less than two years, the market seems to value the long-term prospects of the \$CRV token, as more of it keeps locked away as \$veCRV. On top of this, stablecoin market share continues to grow (one of Curve's primary markets) and in the medium-term, holding the token allows you to boost the yield in your pools substantially (up to 2.5x).

### Risks and threats

Curve has cemented itself as the main platform for stablecoin trades and peg preservation i.e. assets keep trading one-for-one. This has severe consequences when liquidity pools become unbalanced: holding a different ratio than a 50/50 share of two coins, or 25/ share of four coins as for example in the UST pool on Curve. As we can observe on the right, this is a screenshot of the pool, hours after the initial UST de-peg occurred. The pool was flooded with UST, making the other assets in the pool scarcer and thus, swapping from UST into another stablecoin incurred significant slippage – over 10% as seen on the right.

In the case of UST, there wasn't significant demand to restore the peg, however, short-term depegs happen on a frequent basis and, as long as the market has confidence in all assets, the balance will typically be restored. At the same time, bigger de-pegs will typically cause several liquidations as many platforms use Curve's pricing to track the value of certain assets. Once the price goes below a certain threshold, some leveraged positions will usually get liquidated. \$CRV inflation outpacing \$CRV locking

As we have covered extensively in this report, there is a fine balance playing out, with \$CRV rewards being distributed across liquidity pools and \$CRV being locked to receive all the boosting, stacking and governance benefits of \$veCRV. The question is whether the goal of accumulating \$CRV and locking it for \$veCRV becomes unprofitable below a certain price level of the \$CRV token as boosting is achieved by distributing \$CRV tokens across many liquidity pools.

# HODL

/RESEARCH

---

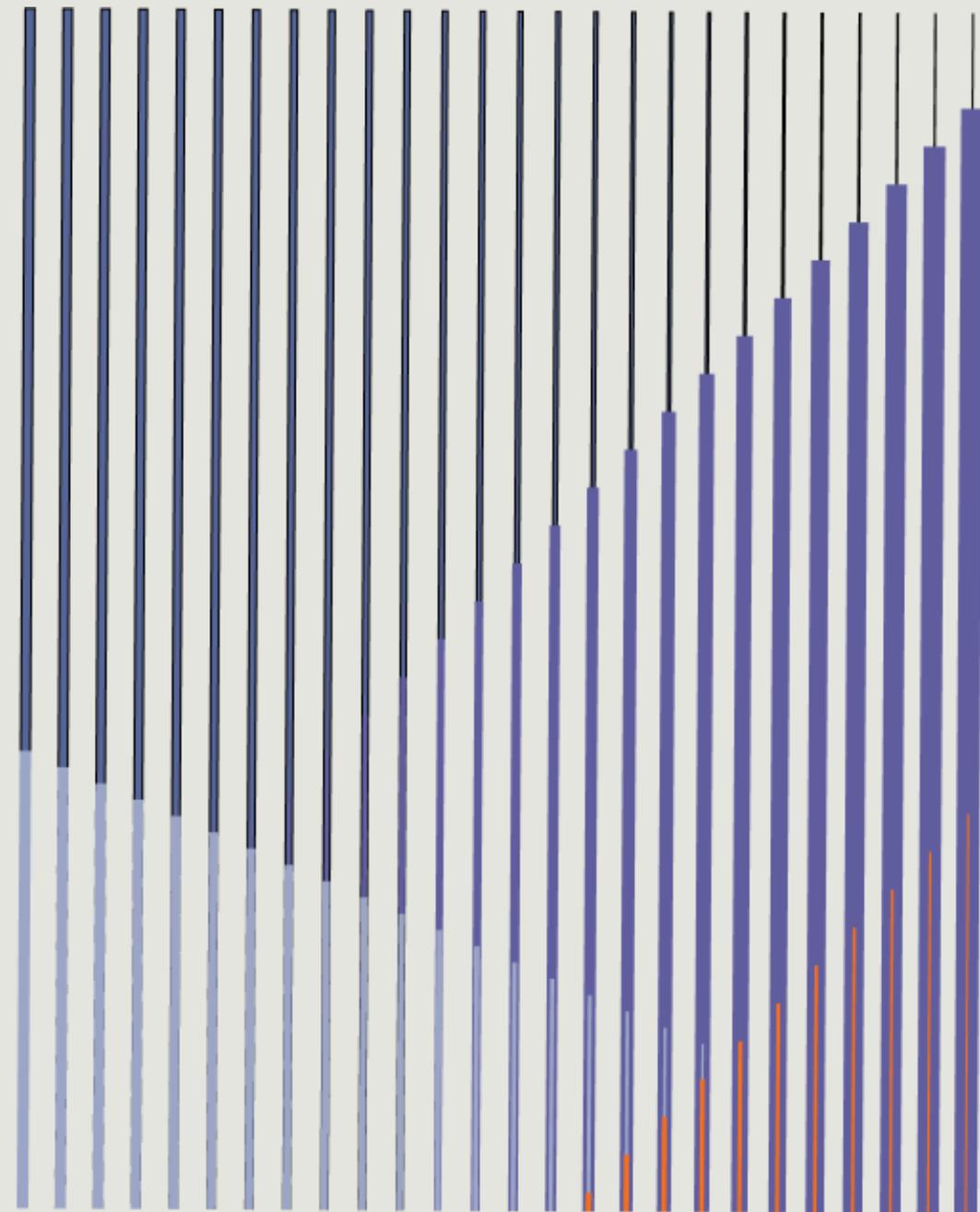
visit [www.hodl.nl](http://www.hodl.nl)



[@hodl\\_research](https://twitter.com/hodl_research)



[Hodl Research](https://www.linkedin.com/company/hodl-research)



This report is created and authored by Hodl.nl Management B.V., (Hodl) and is published and provided for informational purposes only.

The information in the report constitutes Hodl's own opinions and it should not be regarded as a description of services provided by Hodl.

The opinions expressed in the report are for general informational purposes only and are not intended to provide specific financial advice or recommendations for any individual or on any cryptocurrency. It is only intended to provide education about cryptocurrencies. It is very important to do your own analyses before making any investments based on your own personal circumstances.

You should take independent financial advice from a professional in connection with, or independently research and verify, any information that you find in our report and wish to rely upon, whether for the purpose of making an investment decision or otherwise. The views reflected in the commentary are subject to change at any time without notice.

Hodl.nl Management B.V. is registered with the Dutch regulator, Autoriteit Financiële Markten (AFM). Hodl.nl Management B.V. is acting as administrator for the following funds: Hodl.nl Consensus Fund with registration number 50025133 and Hodl.nl Genesis Fund with registration number 50025134.

At publication date of this report, Hodl.nl Consensus Fund and Hodl.nl Genesis Fund hold long positions in Merit Circle token (MC). This may change any time without notice.