Stabull

Whitepaper

Defining the 4th Generation AMM for

Dynamic Stableswaps

Draft Rev. 2.1

Table of content

Summary

The single largest addressable market opportunity in the crypto industry today, as measured by notional TVL and trading volume, is a decentralized money market.

...The FX market is the biggest and most liquid in the world, though it is running on antiquated rails, relying on banks and third-party intermediaries to facilitate, and resulting in huge loss of funds with exorbitant fees (Alex McDougall, 2023).

Moreover, non USD stablecoins in particular are experiencing exponential growth in liquidity, users and use-cases. However, even within the largest existing AMMs, volumes for non-USD stables are minimal with a TVL less than 1% of overall TVL. ***Infrastructure has been built, but so far, no one has come (Kremsky, 2023).***

Stabull plans to radically change this landscape. The Stablecoin industry can capitalize on this opportunity by collectively supporting a common piece of infrastructure to economically and efficiently facilitate swaps through an issuer-operated and unified decentralized money market.

The vision of Stabull Finance is to deliver a common piece of infrastructure that defines the 4th Generation AMM and enables the purest form of stableswaps. In his report, Alex McDougall indicates that the lack of non-USD stables on-chain limits the effectiveness of the status-quo and proliferation of the blockchain industry as a whole.

...60% of global currency reserves are USD, yet 99% of on-chain FX is USD-denominated McDougall, 2023)

The exclusive purpose of Stabull Finance is to facilitate safe and permissionless instant swaps for tokenized FX and commodities.

In addition, Stabull Finance intends to be governed by the Stablecoin industry itself as a consortium (similar to ICANN for domain name registration) of vested partners.

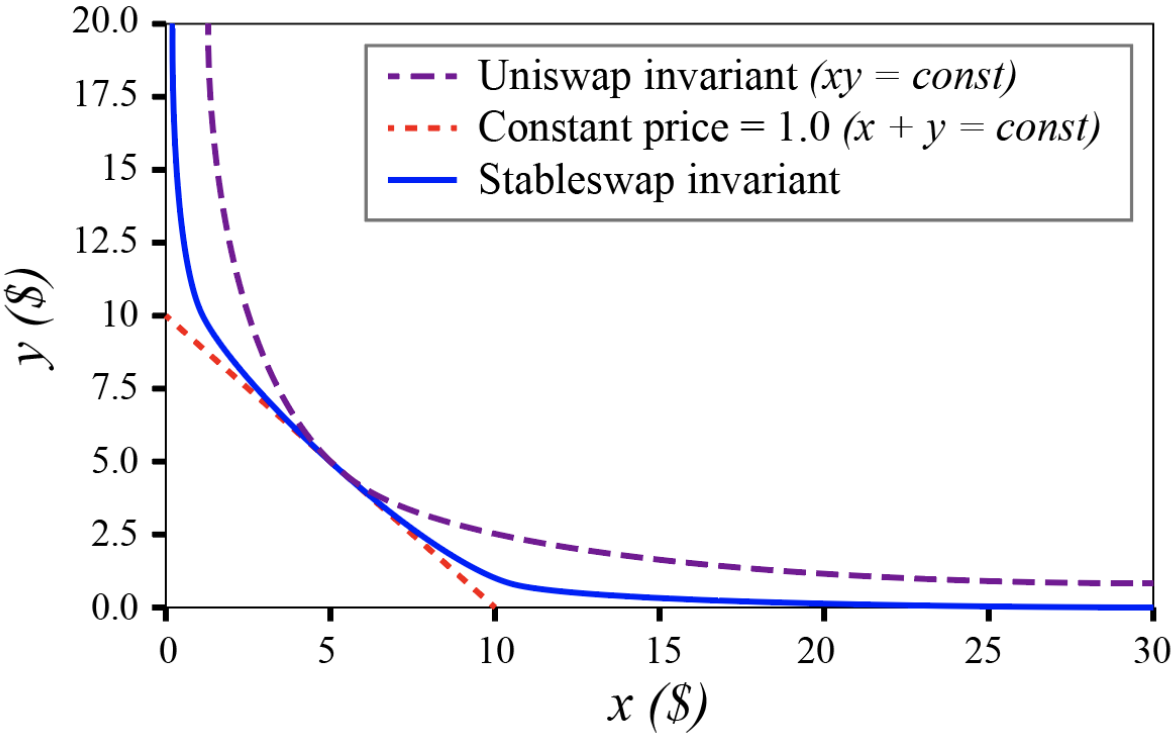
The keys to success are:

1) An improved bonding curve for swaps for greater Capital Efficiency.
2) Simplicity.
3) Liquidity.

Background

A **first generation (Gen 1)** "Stableswap" generally refers to the invariant created by Curve (v1) for a pool of assets with a **stable exchange rate (constant, 1:1)**; not necessarily a pool of stable coins (e.g. BTC/wBTC). The invariant (visualized as a curve), is a combination of the constant product function (popularized by Uniswap) and the constant sum function (constant price), forming a "flattened" curve. As a result it shares the benefits of unlimited liquidity (constant product), while still maintaining low slippage close to the equilibrium (constant sum).

$$An^n \sum x_i + D = ADn^n + \frac{D^{n+1}}{n^n \prod x_i}$$



Gen 2: Does not properly represent pure stableswaps

Second generation (Gen 2) AMMs, Curve v2, shell and DFX, for example, do not represent genuine stableswaps in their purest form either because they were created for non-pegged or volatile assets that lack a stable exchange rate, such as different currency pairs (NZDS/USDC, although less volatile than ETH/USDC, is not stable). They do use a similar invariant to "stableswap", however, but instead of maintaining the "stable" exchange rate (the gradient of the flat section) constant, "repegging" to a dynamic price (from an internal or external oracle) periodically occurs.

Gen 3: The embrace of modified bonding curves and extra features

The rise of **third generation (Gen 3)** AMMs marked a significant shift towards decentralization and interoperability in response to the evolving needs of the crypto industry by offering a more flexible and inclusive trading environment using features that mirrored that of their centralized counterparts.

The first Gen 3 DEX, Uniswap V3, offered a radical new concept known as "concentrated liquidity" where liquidity providers selected a range at which liquidity could be made available, thus enabling greater capital efficiency and profitability.

By contrast, Gen 1 and 2 DEXs spread liquidity across the entire possible price range, resulting in liquidity being wasted in lightly traded areas. Scalability however was enhanced due to multiple fee tiers and improved architecture, particularly given the mass adoption of layer 2 architecture already underway, such as Arbitrum, Optimism and Polygon roll ups on notable exchanges.

Gen 3 DEXs also introduced the concept of cross-chain interoperability to solve increasing issues of fragmented liquidity associated with the many L2 operated DEXs. Recognizing that interconnected ecosystems progress the future of blockchain away from isolated networks, cross-chain interoperability marked a significant step forward by removing barriers that previously restricted users to trading within their respective blockchain ecosystems.

Moreover, Gen 3 exchanges were characterized by the innovative use of smart contracts to automate trading operations, and by using the Uniswap V3 model as a base, further enhanced features like dynamic liquidity, dynamic fee tiers, single-sided liquidity pools, RFQ models, low-slippage and CEX-DEX hybrids trying to capitalize on the best of both worlds.

Gen 3 exchanges established the foundation for the next generation of exchanges and set the stage for the introduction of more advanced features and sophisticated trading mechanisms. Recent advances in ZK technology, for example, has led to liquidity migration toward ZK-based chains. Given the extra efficiency and privacy-enabling capabilities of these chains, wide-spread adoption is further anticipated by the general public. These advancements as well as the lack of an industry-led exchange have opened the door to the development of Gen 4 exchanges, such as Stabull.Finance, which is laser-focused on improving "capital efficiency" for a non-USD-based stable coin AMM that enables stableswaps in an accessible, cost-effective manner. There needs to be a key source of liquidity for non-USD stable coins that allows them to flourish and grow.

...Despite headwinds [with existing options] non-USD stables need some place decentralized to trade otherwise the value of interoperability decreases significantly. *Kremsky, 2023*

With collaboration and support of non-USD issuers Stabull could be that source.

Gen 1-3 AMM Solutions

AMM	Details	Invariant	Improvements
Curve Whitepaper Docs	"Stableswap" Constant Sum & Constant Product	Hybrid (flattened curve) Constant gradient 1:1 $An^n \sum x_i + D = ADn^n + \frac{D^{n+1}}{n^n \prod x_i}$ Unlike DFX there is not a completely flat / no slippage zone around equilibrium, it's just very close to flat.	Improving on Uniswap's large slippage, an AMM optimized for swapping of assets of the same value. Concentrates liquidity at center (1:1), while still having some liquidity at the tails to prevent pool being drained.
Curve v2 Whitepaper Curve v2 Parameters	Added support for non-pegged assets "CurveCrypto"	Hybrid (flattened curve) Re-pegging (internal oracle) $KD^{N-1} \sum x_i + \prod x_i = KD^N + \left(\frac{D}{N}\right)^N,$ $K_0 = \frac{\prod x_i N^N}{D^N}, \quad K = AK_0 \frac{\gamma 2}{(\gamma + 1 - K_0)^2},$	Dynamic peg allows for pools of non-pegged assets (volatile assets). Dynamic fee incentivizes pool back to balance.
Saddle About Saddle	Curve copy (but on Solidity).	"Stableswap" (no dynamic peg)	
Wombat Whitepaper - What is a stableswap Wombat vs The world	Simplified curve invariant.	Hybrid (flattened curve) Re-pegging (internal oracle). $\sum_{k \epsilon \tau} \left(x_k - \frac{A}{x_k} \right) = \mathrm{D}.$	Closed-form solution, so it is more gas efficient. Asset-liability management to enable single-side liquidity provision.
Shell Protocol Whitepaper	Similar to stableswap with different parameters.	Hybrid (flattened curve) Re-pegging.	Dynamic fee when volatility is high. Broken peg protections (min/max allocations).
DFX Docs	Fork of shell protocol v1 focused on FX stablecoins.	Hybrid (flattened curve) Re-pegging (FX oracle).	FX Stablecoin specific.

Parameters: the nitty gritty

Although each dynamic stableswap parameter holds a slightly different naming convention, all fall roughly into one of two categories:

- **Curve Parameters**: control of the shape of curve (i.e. where liquidity is focused / how much slippage). Curve v2 uses Alpha and Lambda, DFX uses Beta & Delta.
- **Fee Parameters**: fixed and dynamic fees that increase with slippage (paid to LP's and protocol treasury).

DFX Parameters

parameter	description	value	explained
Weights (w)	Weighting of the pair (only 50/50)	50%	Ideal / target weight
Alpha (a)	The maximum and minimum allocation for each reserve	50%	To guard against a broken stablecoin peg, the pool has a minimum and maximum allocation (expressed as a percentage of ideal weight), for each reserve. The higher the value of alpha, the greater the range of allowed allocations around the ideal weight. for w = 50% and a = 50%, the pool will not accept any transactions that increases the actual weight beyond 75%.
Beta (b)	Liquidity depth of the exchange; The higher the value, the flatter the curve at the reported oracle price	35%	Once the actual weight is more than Beta percent away from the ideal weight, transactions will begin to incur slippage. i.e if the actual weight is less than 32.5% [w * (1-b)] or greater than 67.5% [w * (1+b)], then transactions will incur increasingly large slippage. Therefore, the higher the value of Beta, the "deeper" the pool ("deeper" in that the exchange rate is stable for larger transactions, not that there is more liquidity).
Delta/Max (d)	Slippage when exchange is not at the reported oracle price	15%	The rate at which price slippage increases (elasticity) once past Beta. The higher the value of delta, the more rapidly slippage will increase (more curve). If delta = 0, then there will be no price slippage at any point.
Epsilon (e)	Fixed fee	per pool	All trades incur this fee. Paid to LPs
Lambda (l)	Dynamic fee captured when slippage occurs	100%	Outside the slippage zone, an extra fee is charged on trades that worsen the imbalance. In effect, this fee widens the bid/ask spread or claims some of the arbitrage profits for liquidity providers.

Stabull is different

Stabull is a 4th generation AMM designed for Stablecoin and Commodity Swaps.

Stabull.Finance is laser-focused on improving "capital efficiency" for an FX stablecoin focused AMM to enable stableswaps in their purest form by building on top of the lessons learned of earlier iterations. To adequately describe its functionality, a distinction will be made between the demand-side (trader) and supply side participant (liquidity-provider) requirements.

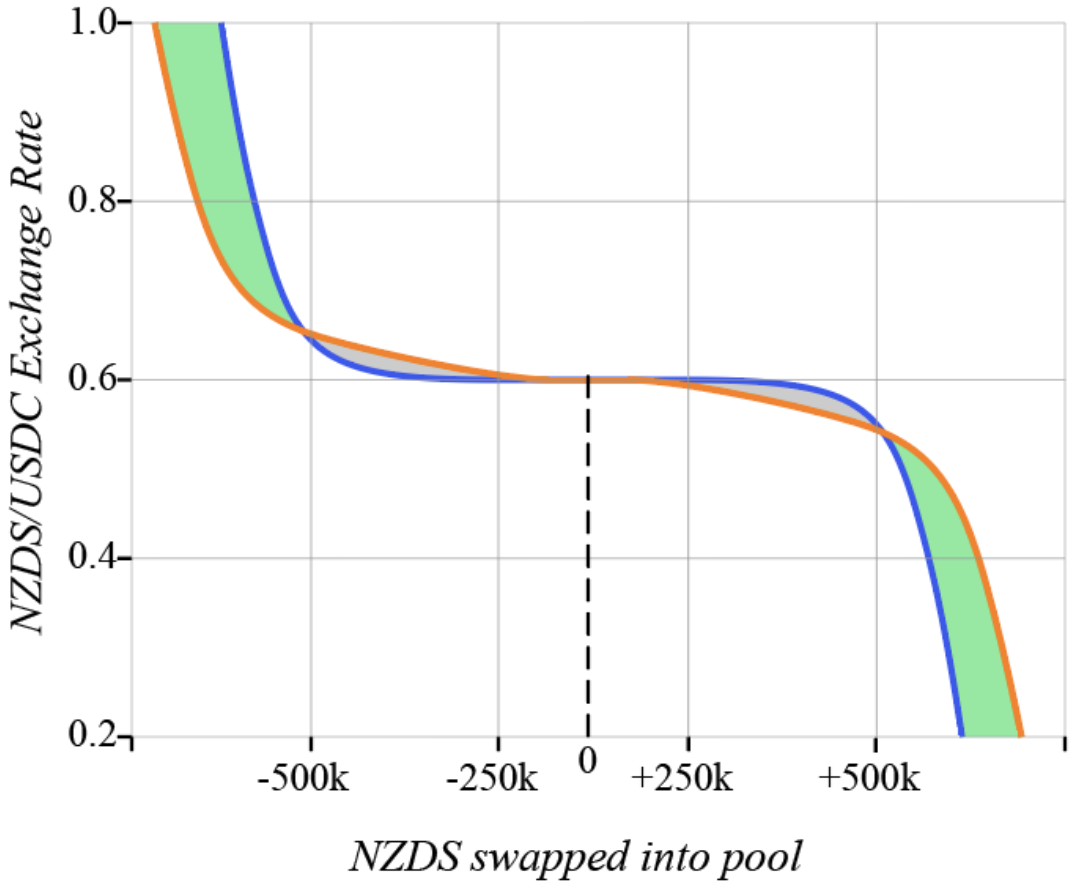
Demand-side

Traders benefit from lower slippage and fees.

- Lower slippage is generally achieved by a flatter curve (increasing Curve's alpha parameter) or a larger no-slippage zone (increasing DFX's beta parameter); as demonstrated by Curve's main improvement over Uniswap with lower slippage around some equilibrium price.
- Where Uniswap spreads liquidity across a range of exchange rates, stableswaps center liquidity around an equilibrium price, thereby lessening liquidity at the tails.
- The internal exchange rate is the oracle provided price, whereas external exchange rates are those offered by other exchanges, such as Uniswap, Curve or centralized exchanges. *Internal* exchange rate stability (low slippage) must be balanced by liquidity provision from a variety of *external* exchange rates (to protect draining of the pool).
    - E.g. A constant-sum AMM has complete internal exchange rate stability, but can only provide liquidity to a single external exchange rate. If they do not match, arbitrageurs can drain the pool of the undervalued currencies.

- The shape of the AMM curve (distribution of liquidity) can also determine the price stability between smaller sized swaps and larger ones.

For example:



The blue curve shows a larger flat section (zero-slippage), controlled by DFX beta parameter, but a steeper curve at the tail (delta parameter). Conversely, the orange curve shows a small flat section (small beta), and shallow tails (small delta). As a result the orange curve incurs more slippage on small trades (gray area), and less slippage for larger trades, compared to the blue curve.

- Lower slippage also reduces incentives for arbitrageurs to balance the pool. (arbitrage = slippage - fees). In the flat section, there is no incentive to rebalance the pool.

Supply-side

Capital efficiency is achieved when yield > (impermanent loss + withdrawal & deposit costs).

- Lower swap fees are preferred by traders, yet unattractive for liquidity providers. Excess fees however discourage trading, and are therefore bad for both.

Defending against exploits with Liquidity protection assurance is also necessary.

Prior generation AMMs have demonstrated that constant sum invariants should not be used in practice because any depegging triggers arbitrageurs to drain the undervalued currency from the AMM.

The exploit log in the Appendix reveals oracle attacks and flash loans as potential attack vectors in existing AMMs, and required either “unlimited liquidity” or some liquidity provision at a variety of levels, and reliance on constant sum invariants contributed to depegging and draining of pools.

Other Features

Broken Peg Protection:

- No improvement necessary, same as shell / DFX i.e. minimum / maximum allocations where swaps are not allowed if the asset's reserves move outside permitted boundaries (e.g. DFX was set to 25% → 75%). (see shell v1 whitepaper)

Oracle Protection:

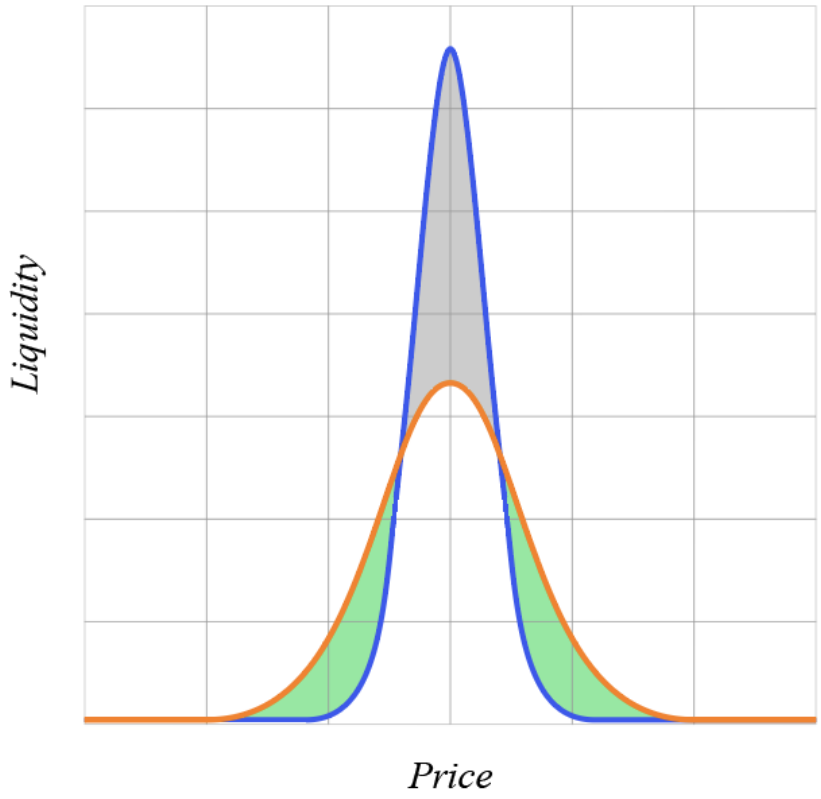
- Some anomaly detection on the oracle prior to pricing, particularly during slower FX weekend trading periods (when liquidity is known to be low and could be manipulated).
- The curve could unflatten (tend towards CPMM) during "untrusted oracle" periods. i.e., less reliance on oracle offers a chance for arbitrageurs to seize advantage.

Gas Efficient:

- Every swap has to solve a complex polynomial using numerical computation (Newton's method, iterative) and requires excess gas. A closed form solution (single iteration to solve), as proposed by Wombat AMM, is more gas efficient.

Enhanced User Interface:

- UI explaining slippage, anti-slippage, fees etc before and after swap.
- More visibility / transparency.



The above chart (roughly) illustrates liquidity distribution at different prices for a DFX pool (blue line) vs. a Stabull pool (orange line) which spreads liquidity slightly and eliminates the "no slippage" zone (flat and steep). Compared to Uniswap, the curve is still flattened, but less so in the center to allow for lower slippage further out.

Most importantly the orange curve lessens price stability (higher slippage) for small trades (represented by the gray area), but increases price stability (less slippage) for larger trades (green area).

Incentives to maintain or move the pool back to 50% are continuously available.

Pools labeled "Balanced" (i.e. between 32.5 and 67.5%), are probabilistically much closer to 67.5% (than 50%). The downside of pushing pool liquidity to the center

results in less supply, outside the "no-slippage" zone, leading to accelerated degradation (slippage increase) versus a constant product AMM (where liquidity is spread evenly). It is thus presumed swaps incurring high slippage on DFX were started just inside the no-slippage zone (balanced) but moved the pool just outside the zone where liquidity is shallow, and should therefore be tested.

Test Case for Slippage

- Slippage: $100k swapped in a pool containing liquidity of $3-4m should not result in 2-3% slippage when pools are not balanced 50/50, as occasionally occurs on DFX and other exchanges

MEV Protection via LVR

Loss Versus Rebalancing (LVR) is a recently emerged field of study within the Ethereum community that seeks to redefine the way we understand and quantify the costs associated with liquidity provision in decentralized exchanges (DEXs). Originating from a 2022 paper, LVR offers a novel perspective by comparing passive liquidity provision to actively rebalancing a portfolio of assets, akin to continuous hedging of options, albeit in a decentralized setting.

Relevance of LVR

The introduction of LVR is timely as it addresses the adverse selection costs borne by liquidity providers (LPs) in constant function market maker decentralized exchanges (CFMM DEXs). These costs arise from the tendency of arbitrageurs to exploit price discrepancies, often leading to LPs selling assets at less favorable prices. By conceptualizing these dynamics through the lens of LVR, we gain a deeper understanding of the trade-offs between passive liquidity provision and active rebalancing.

Enhancing DEX Efficiency

LVR is not merely a theoretical construct but has practical implications in enhancing the efficiency of our DEX. By analyzing the costs associated with liquidity provision through the LVR framework, we can devise strategies to mitigate these costs, making liquidity provision more attractive and reducing the overall cost of trading on our platform.

Dynamic Fee Structures:

- LVR also helps provide a foundation for developing dynamic fee structures that align better with market conditions, ensuring that fees are set at levels that compensate LPs adequately for the risks they undertake.

Improved Price Oracles:

- Incorporating reliable price oracles informed by LVR analysis can help in maintaining asset prices within our pools closer to external market prices, reducing the need for rebalancing and the associated costs.

Hybrid Bonding Curve:

- LVR-driven algorithmic adjustments to the pricing curve can help in reducing the adverse selection costs and the need for rebalancing, making our DEX more efficient and optimally suited to non-USD stablecoins.

Through the adoption and integration of LVR principles, our DEX is poised to minimize the costs associated with liquidity provision, thereby enhancing efficiency, reducing trading costs, and fostering a more rewarding environment for liquidity providers and hopefully create a flywheel that attracts more traders and users because of the liquidity. The ongoing exploration of LVR and its applications continue to position our DEX at the forefront of decentralized finance innovation, ensuring a competitive edge in a rapidly evolving DeFi landscape.

Stabull is Forward Looking

Stabull has a host of features such as limit orders, RFQ and cross-chain capabilities, once initial momentum is reached off the core product. Additionally, recent developments in AI cannot be ignored and Stabull will seek to integrate and leverage AI for protocol management and security as well as dynamically shifting fee structures and a bonding curve that best reflects current market conditions.

Some further avenues include but are not limited to:

Innovative Pool Designs:

- LVR also inspires the creation of innovative pool designs that are resistant to adverse selection costs, making passive liquidity provision more viable without increasing costs to traders.
- **Liquidity Bootstrapping Pools (LBPs):**
  - Our LBPs with adjustable weights and fees over time aid in reducing the rebalancing loss associated with LVR. This was notably done by Balancer Protocol and was a successful methodology for gradual bootstrapping and stabilization of pools over time.
  - **Cross-Asset Swapping Mechanisms:**
    - Our protocol facilitates direct asset swaps, reducing the necessity for intermediate trades, and minimizing the need for rebalancing, thus mitigating LVR.
  - **Rebates and Incentives:**
    - We offer rebates and other incentives to LPs during times of high volatility or loss, compensating for the losses incurred due to LVR.
  - **Multi-token Pools:**

- Multi-token pools with a balanced selection of assets reduce the need for rebalancing, mitigating LVR.

- **Insurance Options:**

  We provide insurance options for LPs to safeguard against potential impermanent loss, enhancing confidence and security in liquidity provision.

Concentrated Liquidity:

- LPs have the flexibility to provide liquidity within specified price ranges, minimizing the exposure to price divergence and subsequently impermanent loss.

DEX Aggregators:

By integrating with DEX aggregators, we ensure efficient trade execution, which helps in maintaining balanced asset ratios in our pools, reducing the need for rebalancing, and mitigating LVR.

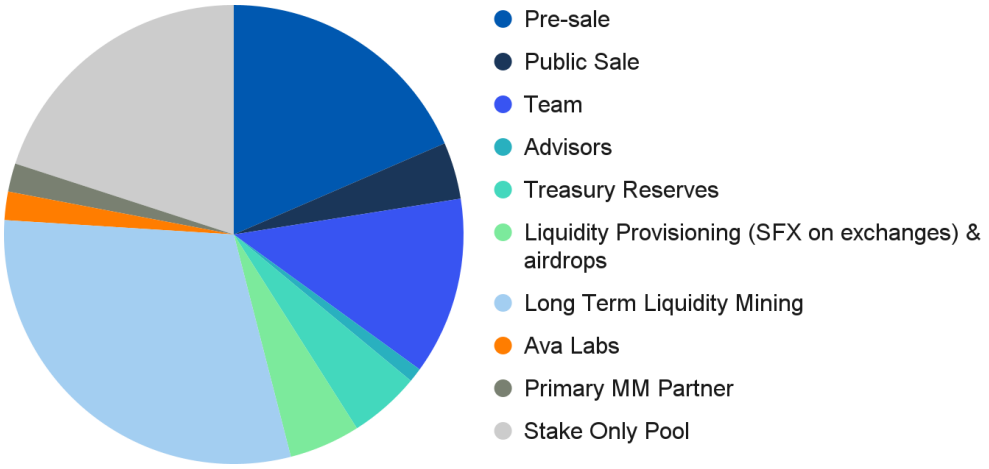
Tokenomics and Consortium Incentives

$SFX governance token is inspired by decentralized community driven projects such as Curve. $SFX will be required to vote on reward levels and distribution to preferred pools throughout the liquidity reward program, as well as to vote on key Stabull features. The economics are designed to create competition between liquidity providers, market makers and stablecoin issuers - but are open for any market participant to accumulate and vote/govern with.
Careful consideration was taken to align incentives for liquidity providers and avoid continuous sell pressure (See POL tokens below).

Tokenomics - Top Level Breakdown

$SFX governance token design must align incentives for all Market Participants including Liquidity Providers, DAO Maintainers, CEX Exchanges, FX Industry Participants & Strategic Partners.

Token basics, allocation & utility



TOKEN BASICS, ALLOCATION & UTILITY			
Token Name	Stabull		
Token Symbol	SFX		
Token Type	ERC-20		
Total Supply	10,000,000 tokens		
Initial circulating supply	2,250,000 tokens (22.5%) (pre/public sale + ecosystem development, protocol liquidity)		

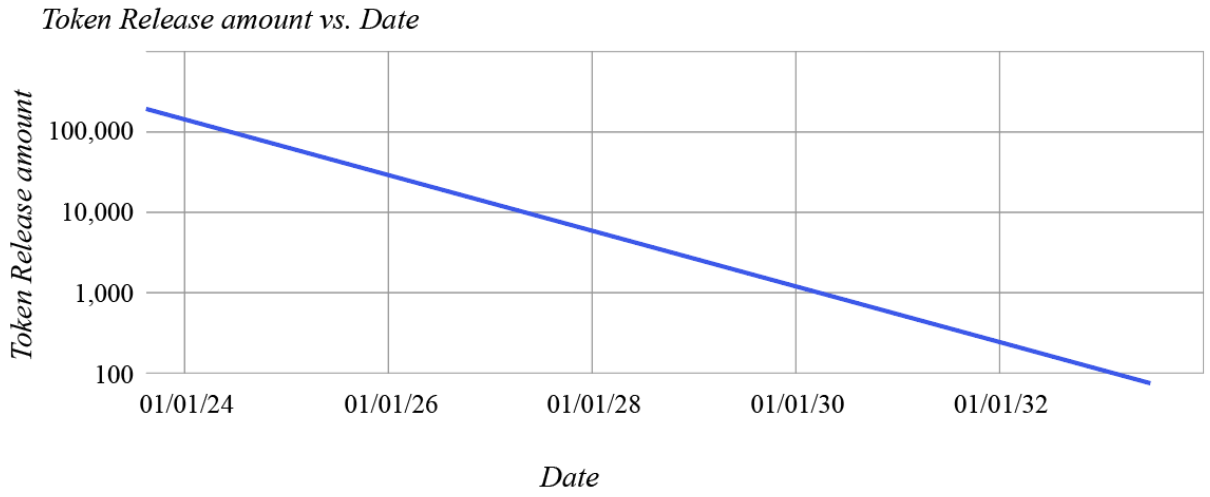
		Percentage	Vesting
- Pre-sale	1,850,000 tokens	18.50%	33% on TGE and 2 year linear vest
- Public Sale	400,000 tokens	4.00%	40% on TGE and 1 year linear vest
- Team	1,250,000 tokens	12.50%	1 month cliff, 2 year linear vest
- Advisors	100,000 tokens	1.00%	33% unlocked on TGE, 1 month cliff then 2 year linear vest
- Treasury Reserves	500,000 tokens	5.00%	33% unlocked on TGE, then 2 year linear vest
- Liquidity Provisioning (SFX on exchanges) & airdrops	500,000 tokens	5.00%	Unlocked for listings and liquidity
- Long Term Liquidity Mining	3,000,000 tokens	30.00%	No lock - liquidity mining with quarterly DAO vote
- Ava Labs	200,000 tokens	2.00%	15% on TGE and 2 year linear vest
- Primary MM Partner	200,000 tokens	2.00%	15% on TGE and 2 year linear vest
- Stake Only Pool	2,000,000 tokens	20.00%	Locked forever
Sum		100.00%	

Liquidity Mining Emission Schedule

$SFX tokens will be distributed over 10 years via a non-linear emission schedule. The emission rate and timeline will initially be controlled by the Stabull team to ensure the best combination of liquidity pool APY and $SFX longevity. Progressive decentralization will occur in the future as control will be moved to the DAO.

200K $SFX tokens will be released in the first month, with emission rates reduced in each subsequent month. The emission rate could change as Progressive Decentralization occurs, and subject to an SFX Token Holders vote on APY following the 1st epoch.

Note: 70% of the network swap-fees will auto-buy and return $SFX to the Liquidity Mining pool for continuous top-up.



Protocol Owned Liquidity (POL) tokens

To avoid the constant sell pressure often experienced by many DeFi projects and to correctly align incentives for key protocol participants, 20% of the total supply is “non-sellable” Protocol Owned Liquidity (POL) tokens. These are $SFX tokens which cannot be sold. They can only be staked to receive a % of the protocol's success, and will never be withdrawn or sold on the market - unless a major change is voted on by the DAO.

It is important to note that POL tokens do NOT represent a separate token but are instead $SFX tokens locked into a staking protocol and will not be withdrawn and sold. Rewards however will simply be streamed to designated wallet addresses supplied by strategic POL token holders, and are designed to bootstrap initial liquidity and core services to maintain liquidity and balanced pools. Rewards - also create a mechanism to bolster the robustness of the protocol and avoid the type of unnecessary sell-pressure commonly associated with early token projects.

20% of all fees generated will be used to purchase $SFX from the market for distribution to POL token owners via a traditional pool claim feature, thus enabling POL token owners to claim 20% of all platform revenue indefinitely.

The primary function of the POL pool besides strengthening the protocol’s resilience and token is to provide a passive income stream for key stakeholders based on the platform’s performance to incentivise brand support and growth while simultaneously locking away 20% of the total $SFX supply permanently to reduce potential sell pressure.

Example: A market maker or Stablecoin Issuer may offer to provide X $mm in liquidity for a new pool for a minimum of N months/years. To cover their cost of capital they would receive an amount of POL tokens at a cost basis of $0. This

allows the participant to provide an invaluable service (liquidity) to Stabull without the ability to speculate on capital gains (unable to sell these tokens). Their cost of capital is covered by way of % of protocol gas/swap fees. Once their term expires (if not renewed) it is intended their POL tokens will be returned for allocation to future liquidity providers.

It is possible a mechanism could be introduced which would further increase the volume of POL tokens (non-sellable) and reduce the volume of regular $SFX tokens (sellable) over time.

Philosophy regarding listings

The success of a decentralized Money Market as illustrated in the summary on page 1 will stem from liquidity and simplicity. Liquidity will attract additional liquidity. For the initial MVP period it is logical to list any Stablecoin pool offering to bring sufficient minimum liquidity to the Stabull Finance platform.

Subsequent to the MVP launch the initial governance consortium will consist of initial liquidity providers, stablecoin issuers and project backers. Each will have an equal vote on accepting new pool proposals. Over time listings will occur subsequent to a democratic process voted on by all $SFX holders, and according to the weight of their holdings. Similar to the fantastic results of the Curve Ecosystem, the intention is to encourage holding and accumulation of governance tokens that generates competition and utility on the governance token over time.

Post V1 launch it may be possible for unofficial pools and aggregators to submit more creative proposals and integrations that further enhance functionality and liquidity for Stabull Finance - which will be vetted by the governance council and when vote-ready, voted on by $SFX holders in a democratic holdings-weighted process.

Progressive Decentralization

Governance: Fully decentralized and democratic governance structure will emerge over time.

Phase 1: Launch with essential partners 3-5 Stablecoin Pools on Avalanche and Polygon to swap and stake into. MVP will include Protocol Liquidity Staking and $SFX staking.

Phase 2: 3-5 additional pools with 1-2 additional chains integrated. Stabull Finance will follow liquidity and demand when considering new chains and pools to launch.

- Phase 2 will aim to include Limit Orders and/or RFQ facility institutional and larger swap sizes.
- Governance voting via https://snapshot.org/ integration to begin in phase 2. $SFX holders to decide % ratios of network fees and amount of $SFX emissions for all pool APY.
- Governance Proposal will be conducted via https://www.discourse.org/ integration.

Phase 3: Even more pools/chain integrations.

- Further governance decentralization allowing $SFX token holders to vote on use of Network Liquidity and more advanced proposals including hiring/firing administrators.
- 1 Inch, Balancer and Curve integrations to bring “external pools” functionality.

Socials

Website:	https://stabull.finance/
Whitepaper:	https://stabull.finance/assets/stabull-whitepaper-v1.pdf
Twitter:	https://twitter.com/stabullfinance
Discord:	https://discord.stabull.finance/
Telegram Announcements:	https://t.me/stabullfinanceannouncements
Medium:	https://medium.com/@stabullfinance
Partner Outreach Form:	https://stabull.finance/partners/
Gitbook:	https://docs.stabull.finance/
Youtube	https://www.youtube.com/@StabullFinance

Appendix

Exploit / Vulnerability Log

AMM	Date	Attack Type	Details	Amount
DFX	2023-04-28	Vulnerability Report	DFX Finance Rounding Error Bugfix Review [Immunefi]	(100k bug bounty)
Platypus	2023-04-18	Withdrawing unpaid debt	Hack Analysis: Platypus Finance [Immunefi]	$8.5M
DFX	2022-11-10	Reentrancy	Decoding DFX Finance Exploit [QuillAudits]	$7M
DFX	2022-07-04	Oracle Attack	The oracle wasn't manipulated itself, but the attacker took advantage of oscillating fx oracle price over the weekend. NZDS/USDC Pool Post Mortem [DFX]	$250K
Saddle	2022-04-30	Asset value miscalculation	Hack Analysis: Saddle Finance [Immunefi]	$11M
Curve	2020-10-07	Vulnerability Report	Curve Vulnerability Report [Peter Zeitz]	

Why do DFX pools often situate at the boundary of the no-slippage zone?

Slippage incentivises arbs to rebalance pools (swap the overvalued / underweighted asset for the undervalued asset). That is the definition of "anti-slippage" rather than a fee for rebalancing swaps, because in actuality an underweighted asset either sells at a higher price than expected, or the overweighted asset can be purchased for less than expected ($0.99) (in a $1.00 pegged pool). Due to the shape of the curve, there is very little incentive to rebalance the pool in the no slippage zone (move pool from 67.5% to 50%), but there are higher incentives for rebalancing outside (e.g. from 70% to 67.5%).

Disclaimer & Risk Statement

This Whitepaper has been issued on behalf of the Stabull Platform ("Stabull"). This Whitepaper does not constitute a prospectus for the purposes of Directive 2003/71/EEC (the "Prospectus Directive"), and the amending directive 2010/73/EU Regulation (EU) 2017/1129 (the "Prospectus Regulation") or offer document of any sort and is not intended to constitute an offer of securities or financial products or a solicitation for investments in securities or financial products in any jurisdiction. The purpose of this Whitepaper is to provide information on Stabull's proposed project ("Project") to allow participants an opportunity to make their own decision as to whether or not they wish to support the Project.

This Whitepaper does not constitute an offer or invitation, or any other solicitation for the sale or purchase of shares, securities, financial products or any other assets. Any possession of $SFX or POL tokens (together "Tokens") shall not grant any rights in any form to the user, including but not limited to any rights of ownership, interest, profit, redemption, property or intellectual property, decision making, or any other such rights, such as any rights of financial or legal nature, in Stabull or the Project.

No representation, warranty, assurance or undertaking is made as to the accuracy of the information contained in this Whitepaper. The information contained in this Whitepaper may be subject to modification, supplementation and amendment at any time and from time to time. Statements that look forward in time are subject to risks and uncertainties, and actual results, actions or events could differ materially from those set forth in the Whitepaper.

This Whitepaper describes the proposed Platform and proposed Tokens. It has not been reviewed, verified, approved or authorized by any regulatory or supervisory authority. The content provided is for informational purposes related to Stabull's approach of providing a solution based on blockchain technology. The information may not be comprehensive and does not imply any elements of a contractual relationship.

This document does not constitute the provision of investment or professional advisory services. Stabull does not guarantee, and accepts no legal liability whatsoever arising from or connected to, the accuracy, reliability, or completeness of any material contained in this document. It is the responsibility of prospective purchasers of Tokens to undertake their own due diligence. Prospective purchasers of Tokens are wholly responsible for ensuring that all aspects of the Project are acceptable to them.

The purchase of Tokens may involve special risks that could lead to a loss of all or a substantial portion of the purchase amount. Stabull does not represent, warrant, undertake or assure that the Tokens are defect/ virus free or will meet any specific requirements of a prospective purchaser. You should only purchase Tokens if you can afford a complete loss. Unless you fully understand and accept the experimental nature of the Platform and the Tokens and the potential risks inherent in the purchase of cryptographic assets you should not purchase Tokens.