Vei - An Algorithmic Stablecoin on Genechain

Abstract

We introduce Vei Protocol and the VEI stablecoin. The VEI protocol is inspired by Fei Protocol - a well-known stablecoin project on Ethereum. The goal of the Vei Protocol is to maintain a liquid market in which VBC/VEI trades closely to the VBC/USDT price on Genechain. VEI uses Novaswap as its DEX at launch. Governance can add and update DEX integrations as needed.

New supply of VEI enters circulation via a buy-only bonding curve denominated in VBC. We refer to the VBC accrued from purchases on the bonding curve as *Protocol Controlled Value (PCV)*. We define PCV as any value which is completely owned and controlled by the protocol, without an IOU. It is a subset of Total Value Locked with a stronger use case. The Vei Protocol deploys its PCV exclusively as Novaswap VBC/VEI liquidity at the genesis of the protocol. This is a "liquidity-collateralized" model which removes the need for an overcollateralized debt position. As the supply grows, the bonding curve price approaches a fixed peg to the oracle price. The fixed peg bonding curve creates a guaranteed arbitrage opportunity when the Novaswap price trades above the peg. The protocol will use its liquidity PCV to backstop the Novaswap price when it trades below the peg for a certain period.

The CLAN governance token is used to upgrade the protocol over time. Vei Protocol releases CLAN to bonded VEI/CLAN Novaswap LP tokens. The Vei Protocol design has key advantages that are not present in other widely used stablecoin designs. VEI is decentralized and scalable. New supply is fairly distributed to new demand. PCV provides flexibility to governance to add future integrations. VEI holders benefit from the mechanisms designed to create a high fidelity peg and liquid exchange.

Protocol Controlled Value

In most DeFi applications, users deposit funds with an IOU attached. For example, users could be issued tokens representing the pro rata percentage of the supplied assets. These assets are a part of the Total Value Locked (TVL). The protocol would define a utility around how these funds are deployed. The contract may offer incentives to keepers to close unhealthy positions. There may even be some fee which accrues to stakeholders or a reserve. This value does not belong to the protocol in any meaningful sense, but rather to the users and owners of the protocol.

This lack of ownership creates the "mercenary capital" problem, evident in all user owned TVL-based mechanisms. For example, Novaswap LP tokens are redeemable for the underlying assets. During periods of high APYs or incentives, the TVL would increase. As soon as those rewards dry up, the capital will move on to the next best opportunity, perhaps Other Swap Apps or Lendland.

The key behind the Vei Protocol's mechanism is the idea of *Protocol Controlled Value (PCV)*, a subset of TVL in which the protocol outright owns the assets with no IOU. PCV opens up a new design space for DeFi protocols beyond what user-owned TVL models can do. The protocol can influence market conditions in fundamental ways that are not necessarily profit-motivated. Since there are no users to redeem to, these benefits are guaranteed on the contract level. The clearest use case of PCV is to have the protocol be a liquidity provider (LP) on an Automated Market Maker (AMM) like Novaswap. At sufficient volume, the protocol would essentially control the exchange rate of the trading pair. It can use its PCV to rebalance the price by executing trades against the market and locking or burning excess tokens. For example, let's say there is a Novaswap market denominated in VEI/USDT. The current liquidity depth is 1100 VEI and 1000 USDT. In this example, Vei Protocol owns 90% of the liquidity. Vei Protocol can atomically execute the following trade:

1. Withdraw all liquidity (990 VEI and 900 USDT)
2. Swap ~5 USDT for ~5 VEI (remaining liquidity is ~105/105 VEI/USDT)
3. Resupply 895 VEI and 895 USDT at the 1:1 exchange rate

The net effect of the above trade is the protocol spent ~5 of its USDT PCV to restore the peg.

This design aligns perfectly with the VEI stablecoin use case. This is a marked improvement over models in which all the TVL is user-controlled and frozen as collateral. PCV could also be used to deposit and borrow on lending markets like Lendland.

Funding PCV is a necessary design consideration. The protocol needs to be able to offer a token or service which earns the PCV. A natural mechanism for funding PCV would be protocol fees for functionality. A stronger funding mechanism might be a bonding curve. The bonding curve could mint a token controlled by the protocol for an influx of VBC or other ERC20 tokens. To accrue PCV, the bonding curve must include a spread earned by the protocol. Bonding curves have an elegant mathematical fairness to them. New demand for the token can buy directly from the bonding curve to expand the supply. This is in stark contrast to seigniorage models which centralizes rewards. Arbitrageurs profit off of any market dislocation between the bonding curve and spot exchanges. Users receive the newly minted supply in one of two ways:

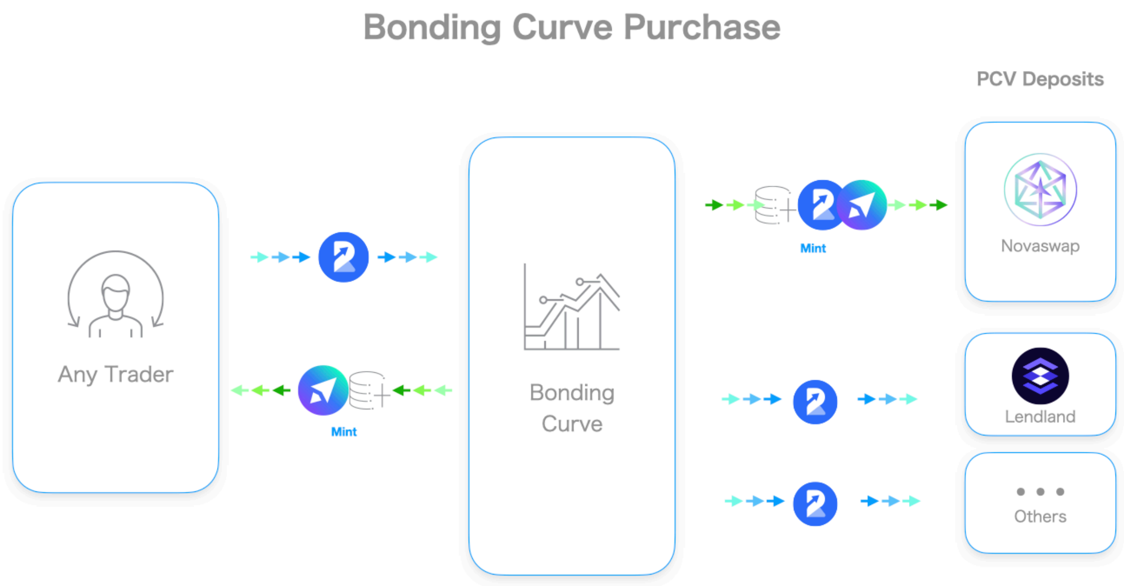
1. Directly from the bonding curve
2. Indirectly from arbitrageurs

Critically, arbitrage is not necessary as users can go straight to the curve. This results in a fair distribution of supply expansions. The protocol benefits in the form of PCV funding.

Vei Protocol uses PCV in the following way. It is funded by a one-way VBC bonding curve which does not allow selling. The PCV is deployed as Novaswap liquidity denominated in VEI and VBC. This can be considered indirect collateralization or "liquidity collateralization".

Liquidity collateralization inverts the traditional understanding of collateral for stablecoins. In an overcollateralized model, a user would supply a fixed amount of collateral like VBC. This collateral could be volatile. As long as the position stays solvent, the debt holder could close the position and redeem their collateral. This collateral now has a new market value. On the other hand, in the VEI model, the only way to redeem for the underlying asset is to sell VEI on a secondary market. For this reason, VEI cannot be used to lever or maintain exposure to collateral assets. Instead, VEI is collateralized by irrevocable protocol-owned liquidity.

This approach has fractional reserve properties. One can consider the collateralization ratio as the amount of PCV divided by the user-circulating VEI. If all outstanding VEI were to be sold or redeemed for PCV pro-rata, this ratio determines the amount received. In this model, there is no requirement for having equivalent levels of PCV liquidity and circulating VEI. The reasoning is the same as in traditional fractional reserve banking: it is inefficient to hold an excess of collateral for every single position if only a subset will ever want to liquidate.

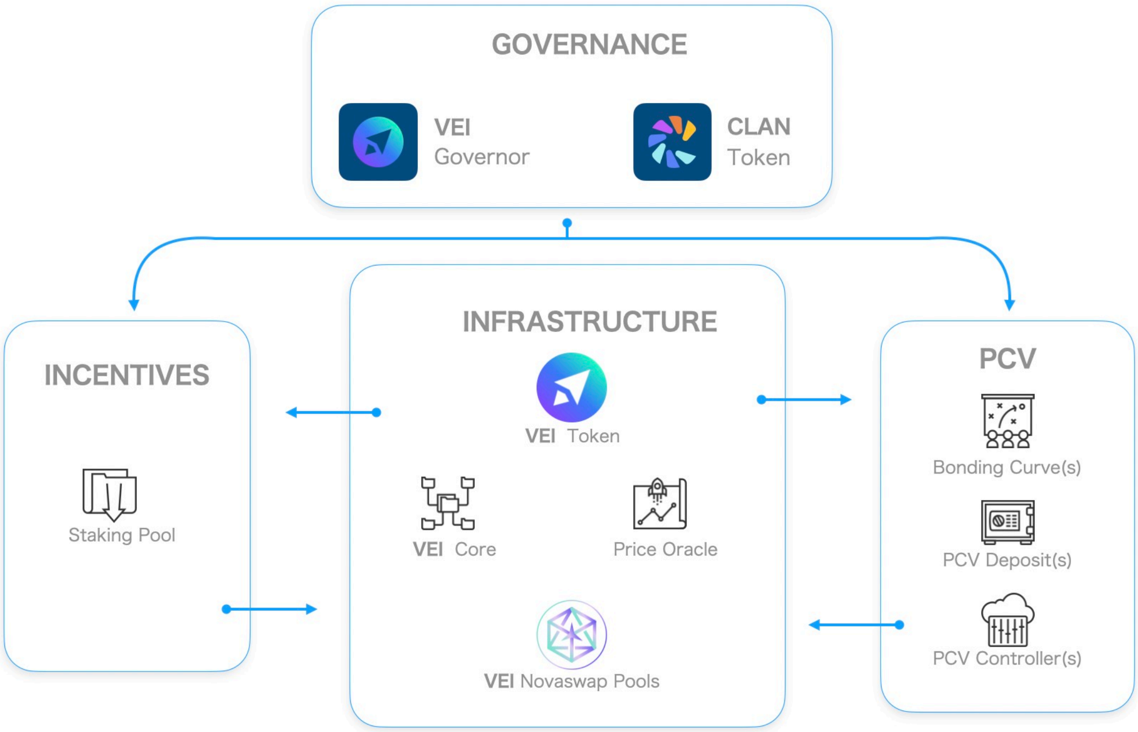


Behind the scenes, Vei Protocol allows for generalized PCV funding and deployment. The funding can come via additional bonding curves denominated in other tokens. Each bonding curve can deploy its PCV to a portfolio which is configurable by governance. A sufficient amount will be allocated to liquidity. The remainder can go to funding interest rate pools on lending markets like Lendland.

PCV represents a natural progression over Total Value Locked (TVL) in valuing a DeFi protocol. TVL is simply a metric of usage, whereas PCV represents irrevocable value controlled by the protocol.

Vei Protocol Design

As seen below, the system has several core components: Vei Core, the VEI stablecoin, bonding curve(s), PCV Deposits, PCV Controllers, VEI Incentives, and the CLAN governance token and DAO.



Vei Core

Vei Core is the access control hub for the Vei Protocol. It defines several roles and what each can do. It also maintains a mapping of which contracts have which roles. The roles are as follows:

- Minter - can mint VEI to any address
- Burner - can burn VEI from any address
- Controller - can move PCV in and out from their initial deposit
- Guardian - enables quick feature shutdowns during unforeseen events
- Governor - can grant/revoke any role, and upgrade the protocol components. This is

  discussed further in the CLAN and DAO section.

The role-based approach in Vei Core allows for complete modularization of the protocol. New features can be voted in by deploying a contract and granting it a role. This flexibility allows Vei Protocol to adapt to ecosystem changes and grow with DeFi.

VEI Token

VEI is the pegged stablecoin produced by Vei Protocol, following the ERC-20 standard. Its supply is uncapped. Minter and Burner contracts control its issuance, via bonding curves. The VEI token exhibits certain non-standard ERC-20 functionality, but only on a subset of transactions.

Within the protocol, there are three distinct types of VEI from an accounting perspective, with some overlap. These are all fungible and treated identically from a token perspective. The protocol calculates the supply of each to be used in calculations. The types are the following:

- VEI_p : Protocol-controlled VEI, deployed in LP pools or other allocations per PCV
- VEI_b : Bonding curve distributed VEI given to users. These will be accounted on a per bonding curve level
- VEI_u : User-controlled VEI, the totalSupply() of VEI less VEI_p

In general, there is overlap between VEI_p and VEI_u . When users sell to protocol LP via an AMM, VEI_u can become VEI_p . Vice versa — when users buy VEI, it goes from VEI_p to VEI_u .

Bonding Curves

Bonding curves are Minters appointed by the Vei Protocol. They issue VEI_b and generate PCV used to maintain the peg. The initial curve will be one-sided and denominated in VBC. Its pricing function approaches an oracle peg price. This bootstrapping mechanism offers early VEI at a discount to users for supplying PCV. The point at which the pricing function reaches the peg is known as *Scale.* Scale is the target VEI_b supply at which a Vei bonding curve pricing function switches to 1. The Scale number can be different for different bonding curves. This allows incentivized PCV funding for various underlying tokens. The initial Vei bonding curve will use VBC as the underlying asset. The peg will be the Time-Weighted Average Price (TWAP) of the VBC/USDT Novaswap pool over a 10 minute window.

The bonding curve issues VEI at a discount with a sublinear growth rate based on the supply. Sublinear curves reward initial investors while still bootstrapping sufficient underlying value to the protocol. A linear or superlinear model would be explosive and lack retained PCV.

Let $O_A(B)$ be the oracle price of A paid in B e.g. $O_{VBC}(VEI)$ = 10 VEI/VBC. The oracle price represents the "target" at which that trading price would imply 1 VEI = $1. Let S be the Scale target of a given bonding curve, in terms of VEI_b . The instantaneous VBC price for a unit of VEI at current total supply X pre-Scale uses the following formula:

$$(1) \quad \sqrt{\frac{X}{S}} \cdot O_{\mathrm{VEI}}(\mathrm{VBC})$$

One can integrate the curve to determine the quantity Q of VBC required to get from a given

level of supply r to another level S:

$$(2) \quad \int_r^S P(X)\mathrm{d}x = Q$$

Using the above formula one can calculate the amount of VBC required to achieve Scale for S =

100 million VEI and $O_{VEI}(VBC)$ = 1/10 VBC/VEI:

$$\int_0^S P(X)\mathrm{d}x = 6,666,666.\dot{6} \quad \mathrm{VBC}$$

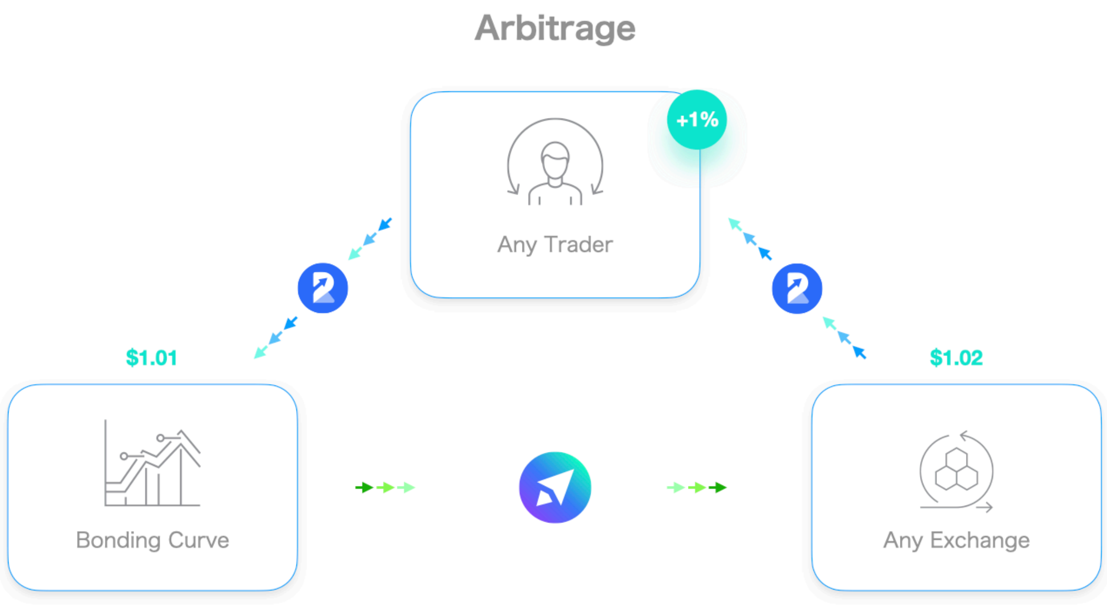
Regarding equation (2), we can define y as the end supply. One can rearrange the integral to solve for the amount $y - C$ of VEI received for a given VBC investment Q at a current user supply C:

$$\int_C^y P(X)\mathrm{d}x = Q$$

$$\left(\frac{2y^{\frac{3}{2}}}{3\sqrt{S}} - \frac{2C^{\frac{3}{2}}}{3\sqrt{S}}\right) \cdot O = Q$$

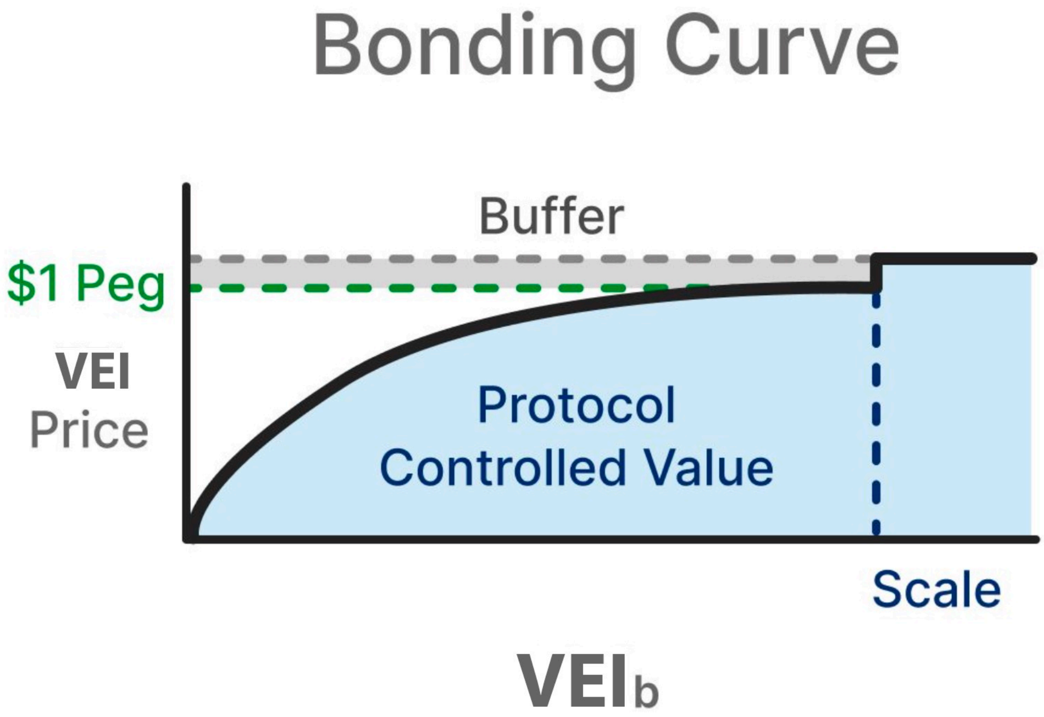
$$(3) \quad y - C = \left(\frac{3\sqrt{S} \cdot Q}{2 \cdot O} + C^{\frac{3}{2}}\right)^{\frac{2}{3}} - C$$

Once a bonding curve achieves Scale, it will fix the exchange rate at $1 + *b*. *b* is a buffer to keep the mean price around $1. When any secondary market price exceeds $1 + *b* there is a riskless profit opportunity. Arbitrageurs can purchase against the bonding curve and sell on the secondary market.



At b=0 the majority of the price variance is below $1. By adding in the buffer b, initially set to 1%, there is room for some variance above $1 as well. Including this price fix behavior, the pricing function extends to

$$P(X) = \min\left(\sqrt{\frac{X}{S}}, 1 + b\right) \cdot O$$



This pure arbitrage opportunity means the protocol requires no additional incentive to maintain the peg when prices exceed $1 + b. Governance can gradually vote to converge b to 0 as the liquidity increases and volatility decreases.

It is important to note that the curve is one-way and VEI cannot be sold on the curve. As previously mentioned, incoming tokens on the curve are retained as PCV. Deploying the PCV on Novaswap allows for "liquidity collateralization" as opposed to a traditional collateralized model.

Each bonding curve has an adjustable allocation rule which defines a set of PCV Deposits. PCV Deposits are contracts that receive incoming PCV and deploy them in predefined ways. The DAO can adjust ratios and add new contracts (appointed as Minters and/or Burners) as needed.

PCV Deposits

PCV Deposits are the recipients of PCV, funded by bonding curves. Because VEI cannot sell on these curves, it is crucial to create a liquid market that allows for the sale of VEI. The sale price should track the peg. The Vei Protocol will allocate all initial PCV to a Novaswap liquidity pool denominated in VEI and VBC. The concept extends to other token types assuming access to an oracle price to peg to. In this case, the PCV Deposit uses the VBC/USDT TWAP as the oracle. We will now explore the Novaswap PCV Deposit in depth.

The Novaswap PCV Deposit receives incoming VBC from the bonding curve and deposits it into an VBC/VEI Novaswap pool. The VEI for this deposit comes from minting, and therefore this PCV Deposit must be appointed as a Minter by Vei Core. The amount of VEI minted is equivalent to the amount of VBC times the spot price of VEI/VBC in the pool. This mint is distinct from the mint associated with the bonding curve and sent to the user. The former is VEI_p and the latter is both VEI_b and VEI_u . The bonding curve mint is associated with the bonding curve price and the PCV Deposit mint is associated with the Novaswap spot price. These numbers should be similar but do not have to be identical. It seems then that there is double the expected inflation associated with a bonding curve purchase, with half going to the user and half to the protocol-controlled LP. A c ritical caveat is this VEI_p does not circulate and will only be used as a burning mechanism for the protocol to reweight. It would not impact the price negatively as it would never be sold.

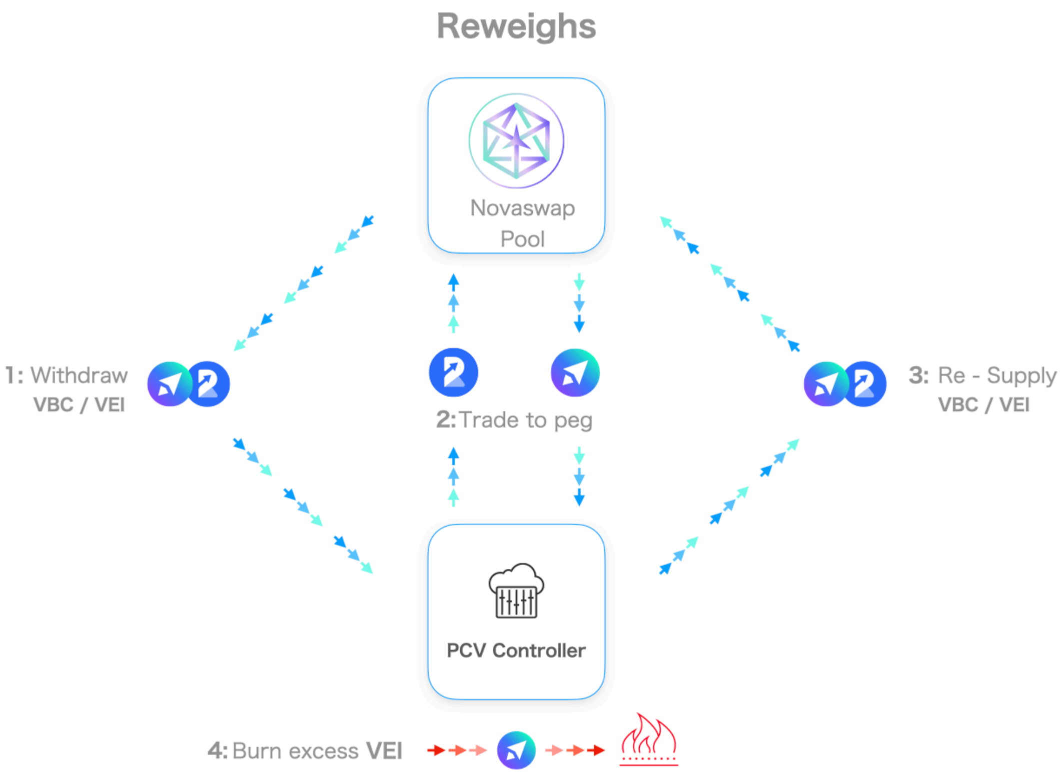
While this is the only PCV Deposit at launch, other implementations are possible to be added via governance. These include liquidity in AMMs other than Novaswap. They could also generate yield via a Lendland deposit. The flexible design will allow for new creative deployments of PCV and integrating with future DeFi protocols as they arise.

PCV Controller

A PCV Controller is a contract approved to withdraw and reweight PCV among PCV Deposits. PCV Controllers are essential to allow the full benefits of PCV to be explored over time. At launch, there will be one primary PCV Controller contract. Governance can add more as needed.

The initial PCV Controller will focus on reweighting the Novaswap VBC/VEI pool. A reweight would mean that the protocol leverages its PCV to bring the spot price of VBC/VEI back up to the peg. This is important in adverse conditions when traders are not willing to support the peg. When this condition is met, the protocol will open up the ability to backstop the price using this PCV Controller. Any external user, or keeper, can trigger a function which will cause the Controller to reweight the prices. The keeper will collect a mint reward denominated in VEI as an incentive. Reweights use the following algorithm:

1. Withdraw all LP from PCV Deposit
2. If remaining LP exists in Novaswap pool, buy VEI with VBC PCV to restore peg
3. Re-supply the remaining VBC/VEI at the oracle price ratio
4. Burn the excess VEI



Generally, additional Controllers would be able to reweight PCV into other DeFi protocols or Vei contracts. These could include:

- Moving PCV into an oracle LP pool to increase oracle attack difficulty

- Adding to Lendland to generate profits
- Using governance token denominated PCV such as LEND to vote on proposals
- Supplying collateral for VEI derivatives such as options and futures

CLAN and the Governance Process

CLAN governance is critical to the decentralization of the Vei Protocol. The governance mechanism will fork the Compound DAO, where holders can delegate votes. CLAN is the governance token controlling the DAO, analogous to COMP. Actions follow the proposed → queued → executed flow, if they do not fail or cancel. Governance has control over the following actions:

- Appoint Minter and Burner contracts (including new bonding curves)
- Adjust Scale target and allocation rule on bonding curves
- Percent reward for reweight peg restoration
- Reweighting any of the peg Novaswap pools

The Vei Protocol DAO will be able to function like a central bank of DeFi. It can use PCV to adjust rates and market incentives on other platforms. This creates a dynamic ecosystem around VEI.

VEI Economic Security

The goal of the Vei Protocol is to maintain a liquid market in which VBC/VEI trades at approximately the VBC/USDT price. This should be true even in adverse conditions. PCV allows the protocol to accomplish this goal. When trading activity does not support the peg for extended periods, Vei Protocol spends some of the PCV to reweight the price. We define the *liquidity ratio* as PCV / VEI_u . This is similar to a collateralization ratio. The difference is the PCV is deployed as liquidity rather than directly as collateral.

The liquidity ratio is a measure of how many reweights and corresponding selloff events the protocol can support. If it is less than 1, the protocol is effectively undercollateralized. However, under normal circumstances the protocol would still maintain the ability to repay all outstanding VEI with the collateral. Overcollateralization for every single position simultaneously is inefficient. Vei Protocol pools the would-be collateral into a single liquidity pool for any user to redeem. This pool can be either over- or undercollateralized. If it is undercollateralized, it relies on the assumption that not every user would want to sell at once. The protocol is designed to improve the liquidity ratio under normal circumstances. This offsets risks associated with the under-collateralization inherent in the mechanism.

In this section we analyze how the liquidity ratio is impacted by trading activity and reweights. We then provide security analysis on the bounds within which the liquidity ratio improves over time.

Liquidity Ratio Updates

A sequence of interactions with Vei Protocol would change the PCV or VEI_u , often in combination. For example, a purchase of VEI on Novaswap or the bonding curve would put VBC into the PCV liquidity pool, and increase the VEI_u . Conversely, a sale of VEI would decrease both values. Let the change in PCV associated with a user action be ΔPCV and likewise ΔVEI_u be the change in user-circulating VEI.

We can define the following update rule to the liquidity ratio for user actions:

$$L_{t+1} = \frac{\mathrm{PCV}_{t+1}}{\mathrm{VEI}_{u,t+1}} = \frac{\mathrm{PCV}_t + \Delta\mathrm{PCV}}{\mathrm{VEI}_{u,t} + \Delta\mathrm{VEI}_u}$$

Ideally $L_{t+1} \geqslant L_t$, i.e. the liquidity ratio improves over time. This property is true when the following inequality is true for positive ΔPCV :

$$\frac{\Delta\mathrm{PCV}}{\Delta\mathrm{VEI}_u} \geq L_t$$

For negative ΔPCV , we flip the sign. Let us call the ratio $\Delta PCV/\Delta VEI_u$ the *capital factor*.

To summarize, when *PCV* and VEI_u are increasing, we want the capital factor to be greater than the liquidity ratio. When they are decreasing, we want the capital factor to be less than the liquidity ratio.

Effect of Activity on Liquidity Ratio

In this section we explore isolated activities and their effect on the liquidity ratio. Novaswap fees are ignored in the analysis. They are generally beneficial for the liquidity ratio by either increasing *PCV* or reducing the VEI_u of a trade.

Bonding Curve

The bonding curve has the price of VEI increasing relative to VBC with each purchase. This means the capital factor is increasing. The reasoning is that the new VEI costs more than the previous VEI relative to the same amount of PCV. All else equal, the liquidity ratio must be lower than the capital factor. This is because all prior VEI had a lower liquidity ratio to enter circulation. Each new purchase improves the liquidity ratio and capital factor. Once Scale is reached, the capital factor would fix and the liquidity ratio would converge to it. This can work positively if the liquidity ratio is low and negatively if the liquidity ratio is high.

Trading Activity

When analyzing trading activity, we assume we start at the peg with a certain liquidity ratio. When VEI trades above the peg, pure arbitrage should always bring the price down to *$1+b*. Due to path independence on Novaswap, a return to the peg should return to the same liquidity ratio as when last at the peg. When VEI trades below the peg, reweight will do it's work.

Reweights

A reweight by itself only burns VEI_p assuming no other Novaswap LPs. However, reweights must be coupled with a sell. Selling can have a positive or negative effect on the liquidity ratio depending on the current liquidity ratio, the size of the sell, and the associated burn.

Selling reduces VEI_u because the VEI leaves circulation to enter the protocol-owned Novaswap pool. Likewise it decreases the PCV because VBC is leaving the pool. We need to have the capital factor be less than the liquidity ratio. For a sell amount of x VEI we need to have:

$$\Delta \mathrm{PCV} \leq -L_t \cdot (x + B(x))$$

We know $\Delta PCV / -x = 1$ because we are selling equivalent amounts of VEI and PCV.

Rearranging the formula and pulling out the x we get:

$$\Delta \mathrm{PCV} \leq -x \cdot L_t \cdot \left(1 + m^2 \cdot 100\right)$$

$$1 \leq L \cdot \left(1 + m^2 \cdot 100\right)$$

For $L > 1$ this is always true. For lower liquidity ratios we would need a larger burn to hit the appropriate capital ratio. However, the burn formula starts at relatively low numbers. A series of sales coupled with reweights could worsen the liquidity ratio. This would happen when the corresponding burns are too low. The protocol would be relying on excess burning in the peg support case to offset the needed burns for reweights. We formalize this concept below.

External LPs

External LPs are any non protocol actor who supplies liquidity in the incentivized pool. The PCV LP should greatly exceed user LP. This is because all circulating VEI was purchased by VBC which became PCV. User LP does negatively impact the liquidity ratio in the event of a reweight. Reweights would also cost the protocol some PCV if external LPs are in the pool. This is because it needs to execute a trade against the remaining LP to bring the price back up. The relative impact of this grows with the amount of external LP.

PCV Volatility

Volatility in PCV directly affects the liquidity ratio. When the VBC PCV drops in value, traders would sell VBC to the VEI/VBC pool. This increases PCV in the sense that more VBC enters the protocol's control. However all of the other VBC already held as PCV dropped in value. Conversely, appreciation in VBC will have a positive ultimate impact on the liquidity ratio. New bonding curves added to the protocol would diversify the PCV. Diversification would improve the robustness of the protocol because it would be less susceptible to volatility. This follows the same reasoning as traditional diversification of asset portfolios.

Vei Economic Analysis

We have analyzed the effect of individual outcomes on the liquidity ratio. Now we can combine them to formalize the economic security bound of Vei Protocol. We have established the following relationships:

- Bonding curve purchases drive liquidity ratio towards 1
- Trading activity below peg improves liquidity ratio
- Reweight can hurt liquidity ratio when below 1
- External LP amplifies the effect of reweights
- Volatility affects the liquidity ratio

Governance is incentivized to steward the liquidity ratio and protect the peg. By guarding the key protocol metrics, governance would improve fidelity in the system and grow the protocol. The flexible architecture allows multiple avenues through which governance can add dynamic and autonomous incentives.

Conclusion

The Vei Protocol promotes the sustainable creation of a stablecoin known as VEI. VEI issuance is controlled by Minters including one-sided bonding curves used to bootstrap the system. The price approaches the pegged oracle at Scale, after which new VEI can enter circulation seamlessly in direct proportion to demand. The bootstrapped funds are retained as Protocol Controlled Value (PCV) which is used to support the peg. This idea creates a "liquidity as collateral" concept. Value is strategically deployed to create liquidity and incentivize the peg for token holders. This further range bounds the peg. As the platform extends beyond Scale, the collateralization ratio generally increases due to trading activity.

Vei Protocol presents several key advantages over existing decentralized stablecoin models. These include:

- high liquidity via PCV
- decentralized collateral
- capital efficiency
- strong peg
- fair distribution

Vei Protocol is a central bank-like infrastructure that could serve as a backbone to current and future DeFi applications.

References

1. https://fei.money/whitepaper
2. https://docs.fei.money/
3. https://genechain.io/whitepaper.pdf
4. https://github.com/NovaSwap/whitepaper/blob/master/nova.pdf
5. https://docs.lendland.finance/whitepaper
6. https://medium.com/hackernoon/stablecoins-designing-a-price-stable-cryptocurrency-6bf24e2689e5
7. https://makerdao.com/en/whitepaper/
8. https://github.com/emptysetsquad/dollar/blob/master/d%C3%B8llar.pdf
9. https://docs.frax.finance/overview
10. https://compound.finance/documents/Compound.Whitepaper.pdf
11. https://yos.io/2018/11/10/bonding-curves/https://docs.fei.money/
12. https://uniswap.org/whitepaper.pdf