# vTokens: synthetic tokens using seigniorage

ValueDeFi team*†

January 18, 2021

**Abstract**

A major tenet of central banks and governments is the concept of seigniorage, or the right to expand or contract the monetary supply. It is an essential economic tool used to achieve price stability. In algorithmic stable asset protocols deployed on decentralized platforms, seigniorage is encapsulated as a token representative of a bearer instrument. In essence, instead of seigniorage being the sole right of central banks, anyone holding the bearer instrument has the right to seigniorage or the right to receive a proportional amount of the expanded supply. Previously, stable asset protocols have only been used for pegging assets to fiat currencies. We extend this concept to achieve a peg to the price of any arbitrary asset in a transparent, programmatic, and decentralized manner. We apply this concept of pegging the price of a token to an arbitrary asset and introduce vBTC and vDOT, pegged versions of BTC and DOT, respectively. In addition, we improve upon previous designs of stable asset protocols by introducing four key features. Finally, to the best of our knowledge, we deploy the first pegged asset whose price for the targeted peg is derived with a price oracle that does not rely on any assets that are controlled by centralized parties.

***Seigniorage, Stablecoin, Synthetic tokens, Algorithmic, Pegged Assets***

*contact@valuedefi.io

†The team would like to thank Matthew Niemerg, Ph.D. and Kyle T. Wang for helping with the editing of this manuscript.

# 1 Re-Introducing vUSD: Cross-chain Seigniorage stablecoin

## 1.1 Motivation

When we created vUSD as an elastic experiment on stablecoins, the AMPL concept was sufficient at the time for that purpose. As the protocol evolves, vUSD must meet even more complex demands that exceed the simple capabilities of a vanilla rebase token based on AMPL code. Not only does the AMPL design fall short of maintaining a stable currency, but its composability is also impaired since AMPL-based tokens are not ERC-20 compatible. This problem makes the implementation of lending extremely difficult. After intensive R&D to find an alternative, we determined that the new class of algorithmic stablecoins, modeled after the Basis protocol, has the right features for our purposes.

## 1.2 Our Innovative Features

We introduce four novel mechanisms to improve the price stability of pegged assets, or vTokens, of our protocol. First, we use an $80-20$ liquidity pool with the higher weight being that of the pegged asset. This in turn requires less capital of the asset weighted at 20% to maintain the price peg. Second, we introduce dynamic expansion based on the current liquidity of the pools used for the calculation of the current price of the pegged asset. Third, we allow for dynamic epoch length, depending if the protocol is in a contraction or expansion phase. Finally, during a contraction phase, when vToken is burned for a coupon, 5% of the burned vToken is redirected as a yield to those providing liquidity as an additional incentive to keep their liquidity in the pool during the contraction phase.

## 1.3 vUSD as an algorithmic stablecoin

Current seigniorage stablecoins have mostly selected standard, established stablecoins such as DAI, USDC or USDT to peg their prices to the dollar, but we see an issue with this approach. USDC and USDT are centralized stablecoins, meaning that their issuers under certain circumstances could blacklist the liquidity pools used to peg the asset price.

This may cause the asset to de-peg. For instance, it is quite contradictory for DAI, originally intended as a decentralized stablecoin, to be backed by USDC. As such, if the USDC issuer under any extraordinary circumstance chooses to blacklist the USDC contract that backs DAI, DAI's peg may

break. In addition, DAI collateral is expensive to maintain. For that reason, we chose another way to maintain the peg of vUSD. The ultimate goal is to have vUSD close to $1 as possible.

### 1.4 vUSD/WETH as a way to peg vUSD price

We have chosen Ethereum as the collateral to derive the price of vUSD. The price of 1 vUSD will be determined by the rate of vUSD/WETH at the vUSD/WETH pools. Then, we will use Chainlink as our oracle solution to determine the price of ETH/USD to calculate the rate of vUSD in USD.

Our approach of using Chainlink's oracle price feed for the price of ETH offers novel solution for mitigating flash loan attacks while at the same time removes the need of obtaining the price of a centralized asset.

All other algorithmic stable tokens are using Uniswap 50-50 pool as the only way to peg its price to the relative assets (for example USD). In both theory and practice, this approach of pegging the tokens is very expensive. This results in many tokens being under the targeted peg for a very long time, as speculators do not have proper incentives to increase the peg due to the high capital requirements to move the price back to the peg and to maintain it at those levels.

While we are still actively researching other sophisticated methods to protect the peg (for example using different bonding curves for the liquidity pool), we choose a simple, yet effective, approach, while utilising the advantages of ValueLiquid having flexible ratio pools.

Let's compare two liquidity pools, one is the standard 50-50 vUSD/USD pool with 1 million vUSD+ 1 million $ liquidity and another is the 80-20 vUSD/USD pool with also 1 million vUSD+125k $ liquidity. Suppose Sally wants to sell 200k vUSD to the 50-50 pool, she will receive $166,249.79, which equates to about a 16.8755% slippage. If she sells 200k vUSD to the 80-20 pool, she will receive $129,195.30, which is about a 35.4% slippage. This design encourages holders and discourages speculators at the beginning phase of the protocol.

Assume the price of vUSD is not calculated immediately, but instead uses the time-weighted average price (TWAP). vUSD uses multiple TWAP concepts, e.g. epoch TWAP (measuring the average over the epoch length by the amount of time it remained at each price) and a 1h TWAP (measured over 1 hour).

Using Chainlink's price oracle for ETH/USD, we calculate the vUSD price from the 80/20 vUSD/WETH pool and call it X. The WETH liquidity of the vUSD/WETH 80/20 pool in $ is also calculated using Chainlink's price

oracle and is denoted as Liq(X).

Similarly, the price of vUSD from vUSD/WETH 80/20 pool is Y and the liquidity of the WETH from that pool is Liq(Y). Then the TWAP of vUSD is calculated using the formula:

$$TWAP(vUSD) = \frac{X * Liq(X) + Y * Liq(Y)}{Liq(X) + Liq(Y)} \tag{1}$$

Another requirement for the liquidity is that Liq(X) and Liq(Y) have to be larger than $10.000 to avoid low liquidity manipulation.

### 1.5 vUSD mechanism

We build upon the previous work from [2] and [1] and introduce many innovative improvements. One adaptation we introduce is a dynamic epoch length. One could argue that epoch length should depend on the state of the protocol, instead of a fixed period. An expansion epoch should last longer to delay the minting of new tokens, while any contraction epoch should be shorter for participants to act swiftly to move the protocol out of debt. We propose a dynamic epoch length which depends on the TWAP of vUSD as follows:

In expansion:

$$next\_epoch\_length = round(10h * max(TWAP(vUSD), 2))$$

In contraction:

$$next\_epoch\_length = round(10h * min(TWAP(vUSD), 0.5))$$

#### 1.5.1 When vUSD > $1, the protocol is in expansion and vUSD will be minted to the Reserve Fund contract, vUSD liquidity providers (LPs) in the vUSD/WETH pools and LPs on ValueLiquid Farm-as-a-Service (FaaS).

Instead of fixing the expansion rate which determines the percent of the supply that will be minted for the next epoch, we use the concept of dynamic expansion with the goal of keeping vUSD as close to the peg as possible.

Suppose the current supply of vUSD is $S$. If the protocol is in expansion, then it wants to mint X% of current supply to increase sell pressure of the token so it can reach the $1 peg. All algorithmic stablecoins use a rather simple formula: if TWAP > $1 then $mint(TWAP - (1 + \epsilon))\% \cdot S$. The expansion could be capped at a threshold like 3% per epoch as in [2].

This approach has a major problem which has caused many algorithmic stablecoins to de-peg for longer periods of time due to the high minting rate. We propose another approach which is more elegant to implement and reduces the pressure of participants selling their tokens to the liquidity pools which are used to protect the peg.

Let the expansion of vUSD be $E = S \cdot X$, where $0 < X < 1$ is the expansion rate. Suppose the total current liquidity of peg-protected vUSD pools is $L$. Selling $\alpha \cdot E$ vUSD, with $0 < \alpha < 1$, to the pools with total liquidity $L$ might cause the vUSD price to decrease. We need to determine which $E$ will cause an increase so this new price is not larger than $X$.

Let $B_{vUSD}$ and $B_{WETH}$ be the balance of vUSD and WETH at pool $P$ before expansion. TWAP(vUSD) is the current epoch TWAP of vUSD. $P_{WETH}$ is the current USD price of WETH. We need to find $E$ which satisfies:

$$\frac{B_{vUSD} \cdot B_{WETH} - \alpha \cdot E \cdot \frac{TWAP(vUSD)}{P_{WETH}} \cdot B_{vUSD}}{B_{vUSD} \cdot B_{WETH} + B_{WETH} \cdot \alpha \cdot E} \geq \frac{S}{S+E} \tag{2}$$

We want to calculate the maximal value that that satisfies this inequality, which we will call $max_E$ (which can be computed simply via algebra). In case the protocol has no debt (where totalCoupons = totalRedeemable), the expansion will be $max_E$ vUSD and split to:

- 5% of minted vUSD in expansion goes to a Reserve Fund, which automatically sells vUSD at a threshold to keep the vUSD price on-peg.
- vUSD price is determined by vUSD/WETH LPs at the ValueLiquid FaaS pools. To reward LPs, 35% of the minted vUSD in expansion will go to vUSD LPs of 80/20 vUSD/WETH pool and 50% will go to vUSD LPs of 98/2 vUSD/WETH pool.
- 10% of minted vUSD in an expansion epoch will be used for incentiving VALUE users to provide liquidity like Value Vaults or FaaS liquidity pools on ValueLiquid.

Otherwise, in case the protocol has debt (where totalCoupons = totalRedeemable), the expansion will be $\beta \cdot max_E$ vUSD and split to:

- 5% of minted vUSD in expansion goes to a Reserve Fund.
- 15% of the minted vUSD in expansion will go to vUSD LPs of 80/20 vUSD/WETH pool.

- 10% will go to vUSD LPs of 98/2 vUSD/WETH pool.
- 5% of minted vUSD will be used for incentiving VALUE users.
- 65% will be used to redeem for vUSD coupons.

Note $\beta > 1$ and is a parameter which could be chosen through governance.

#### 1.5.2 When vUSD < $1, the protocol is in contraction and to return to its $1 peg, the supply of vUSD can be reduced through vUSD Coupons.

Coupons are the backup plan when the ability to buy vUSD on the market for less than $1 is not enough to restore the peg by itself. If the price gets stuck below $1 for an extended number of epochs, a method is needed to further incentivize movement back to the peg. Coupons incentivize token holders to voluntarily burn their vUSD by offering them coupons redeemable for future vUSD. These coupons are priced at a discount so that the holders who acquire the coupons are rewarded for taking the risk. vUSD coupons can be acquired by burning vUSD when the protocol is in contraction. By the end of an epoch, if price is below $1, the system will create debt. The debt accumulates in the protocol over time, so if there are multiple epochs when the vUSD is below peg, the debt continues to increase. No new vUSD will be distributed until the debt is paid off in full. When the vUSD price goes above peg, any new supply created pays off the debt first before anything is distributed to token holders.

One of the innovations from our approach is to use the Reserve Fund to restore the peg to $1. When the reserve fund is not enough to restore the peg, vUSD coupons, which are redeemable for future vUSD, will be given to vUSD holders who voluntarily burn their vUSD. vUSD coupons are offered at a discounted rate, determined by a specially designed bonding curve (see [1] for more details), to reward coupon holders for taking the risk.

When vUSD price goes above the peg, any new supply created will be used to pay off the vUSD coupons first before being distributed as described in the previous section. vUSD coupons expire after 360 epochs.

Furthermore, to encourage LPs to bind their liquidity to keep the vUSD price on-peg, we will implement a new mechanism to incentivize LPs. When a Coupons buyer burns his vUSD for Coupons, 5% of the burned vUSD goes instead to LPs in liquidity pools to incentivize liquidity providers. This mechanism is an improvement from the original design of Coupons.

The original design of Coupons was very inflexible and lacked sufficient incentives for Coupons buyers. For example, for ESD coupons, buyers had to wait for the epoch TWAP below $1 to buy Coupons (which takes 8h), then again for another epoch whose TWAP was higher than $1 in order to redeem his Coupons back to ESD.

We improved the design by allowing Coupons purchasers to burn their vUSD to Coupons when 2h TWAP (this is again a parameter and could be changed through governance vote) is below $1. As a result, the buyer can redeem his Coupons back to vUSD if 2h TWAP is higher than $1 (If there is enough vUSD to be redeemable in the contract).

To summarize, we have more novel mechanisms to protect the peg.

- Reserve Fund will initiate the buy back when the system is in contraction phase
- After a certain period of contraction phases, further buy back from VALUE ecosystem profit could be requested (subjected to VALUE governance vote)
- Coupon premium will change with 2h TWAP instead of epoch TWAP
- Further incentive for LPs from burned vUSD to keep their liquidity in contraction phase

LPs at the vUSD/WETH 80/20 pool will have their liquidity lockup for 4 epochs, every time the rewards is claimed or user provides more liquidity, the counter will be reset. LPs at vUSD/WETH 98/2 pool will have the lockup of 8 epochs.

*We should note that all parameters such as lockup length and coupon expiration period could be changed through a governance vote.*

### 1.6 vUSD governance

vUSD serves as a major asset later in the ecosystem of ValueDeFi protocol. All vTokens will be able to be used within ValueDeFi's recently announced elastic decentralized lending protocol [3]. All vUSD governance functionality will be delegated to VALUE holders.

### 1.7 Bootstrapping Period

To ensure a healthy growth of the protocol at start, we set the oracle price of vUSD to $1.2 for first 14 epochs. That means one epoch at bootstrap phase will be full 12h long and the bootstrap phase is 7 days.

After this phase, the system will react according to the true vUSD market price.

### 1.8 vUSD airdrop & distribution

vUSD currently has a supply of 1.709 millions vUSD (Token address). We will airdrop 100 vUSD to all users of our ValueLiquid DEX from its inception until block 11565018 (Dec-31-2020 11:59:57 PM +UTC) who had total trading volume greater than 50 VALUE equivalent (in total 4943 users).

Current vUSD users will have the ability to migrate their old vUSD to new vUSD using our migration contract. The deadline for the migration is 30-June-2021. In total, about 2.203 millions vUSD will be distributed fairly to users (over 10k token holders).

## 2 vBTC: First seigniorage synthetic BTC on Ethereum and Polkadot

Building further on our work with vUSD and existing experimentation on the seigniorage concept, we can create synthetic assets that did not exist before on the Ethereum network in a decentralized manner. As such, we are proud to present vBTC, an alternative BTC synthetic on the Ethereum network without a centralized approach like WBTC or renBTC.

### 2.1 vBTC pools

We have chosen vBTC/WBTC and vBTC/WETH as two pools to stabilize the vBTC to BTC peg. The first vBTC/WBTC pool give you the vBTC price regarding BTC (assuming 1 WBTC = 1BTC), let's call it X (for example X = 0.995 BTC) and the liquidity of the vBTC/WBTC pool is Liq(X).

Then, the vBTC/WETH price from vBTC/WETH pool gives us the vBTC price regarding ETH. Using Chainlink's price oracles, we can determine the current ETH/USD and BTC/USD price, hence we could calculate the vBTC price from vBTC/WETH pool.

Let's call it Y (for example Y = 1.01 BTC) and the liquidity of the vBTC/WETH pool is Liq(Y). Then the TWAP of vBTC could be calculated using the formula:

$$TWAP(vBTC) = \frac{X * Liq(X) + Y * Liq(Y)}{Liq(X) + Liq(Y)} \tag{3}$$

This mechanism ensures the robustness of vBTC price using ChainLink's price oracle to prevent manipulators.

### 2.2 vBTC mechanism

Similar to vUSD, vBTC adopts our innovative features like dynamic expansion rate and dynamic epoch length. When 1 vBTC $>$ 1 BTC, if the system has no debt, expansion will mint $max_E$ vBTC to:

- 5% of minted vBTC in expansion goes to Reserve Fund, which automatically sells vBTC at a threshold to keep the vBTC price on-peg
- 60% of minted vBTC in expansion will go to LPs of vBTC/WETH 98/2 pool.
- 35% of minted vBTC in expansion will go to LPs of vBTC/WBTC 80/20 pool.

When 1 vBTC $>$ 1 BTC and the system has debt, expansion will mint $\beta \cdot max_E$ vBTC to:

- 5% of minted vBTC in expansion goes to Reserve Fund, which automatically sells vBTC at a threshold to keep the vBTC price on-peg
- 10% of minted vBTC in expansion will go to LPs of vBTC/WETH 98/2 pool.
- 15% of minted vBTC in expansion will go to LPs of vBTC/WBTC 80/20 pool.
- 70% will be used to redeem for vBTC coupons.

When 1 vBTC $<$ 1 BTC, the system goes into a contraction phase and users could burn vBTC for vBTC coupons at a premium. We also implement similar innovative mechanisms from vUSD to protect the peg.

- Reserve Fund will initiate the buy back when the system is in contraction phase
- After a certain period of contraction phases, further buy back from VALUE ecosystem profit could be requested (subjected to VALUE governance vote)
- Coupon premium will change with 2h TWAP instead of epoch TWAP

- Further incentive for LPs from burned vBTC to keep their liquidity in contraction phase

The lockup mechanism of vBTC is similar to vUSD (4 epochs lockup for vBTC/WBTC 80/20 pool and 8 epochs for vBTC/WETH 98/2 pool).

### 2.3 Bootstrapping Period

During the bootstrapping phase, the vBTC price oracle will be set to 1.2 BTC for the first 14 epochs (7 days). After this phase, the system will react according to the true vBTC market price.

### 2.4 How to get vBTC?

Current vETH has a supply of 1,609.32 vETH. All current vETH users will have the ability to migrate their vETH to new vBTC at a fixed rate of 0.024 vBTC/vETH (current BTC/ETH price at the time of writing). This results in 38.62368 vBTC as the initial distribution of the token.

## 3 vDOT: First seigniorage synthetic DOT on Ethereum and Polkadot

vDOT is another experiment to move Polkadot tokens onto the Ethereum network in a decentralized manner. Initially, vDOT will be an experiment on Ethereum, but as time progresses, we aim for the community to support migration and change parameters (choice for liquidity pools to derive the price, etc.) as we move forward. This shows Value Defi's commitment to develop a cross-chain solution for the Polkadot network.

### 3.1 vDOT pools

Similar to vBTC, we choose two pools as vDOT/WETH 98/2 pool and vDOT/WBTC 80/20 pool to peg the vDOT price. The TWAP of vDOT will be subsequently calculated using BTC/USD and ETH/USD price feeds provided by Chainlink team to ensure maximal robustness and efficiency.

Let's call A the vDOT price calculated from vDOT/WETH pool and B the vDOT price from the vDOT/WBTC pool, then we have:

$$TWAP(vDOT) = \frac{A * Liq(A) + B * Liq(B)}{Liq(A) + Liq(B)} \tag{4}$$

### 3.2 vDOT mechanism

vDOT will also utilize the dynamic expansion rate and dynamic epoch length from vUSD. We again use the Chainlink price feed of DOT/USD to compare vDOT and DOT. When 1 vDOT $>$ 1 DOT, and if the system has no debt, $max_E$ VDOT will be minted to:

- 5% of minted vDOT in expansion goes to Reserve Fund, which automatically sells vDOT at a threshold to keep the vDOT price on-peg.
- 60% of minted vDOT in expansion will go to LPs of vDOT/WETH 98/2 pool.
- 35% of minted vDOT in expansion will go to LPs of vDOT/WBTC 80/20 pool.

When 1 vDOT $>$ 1 DOT and the system has debt, expansion will mint $\beta \cdot max_E$ vDOT to:

- 5% of minted vDOT in expansion goes to Reserve Fund, which automatically sells vDOT at a threshold to keep the vDOT price on-peg.
- 10% of minted vDOT in expansion will go to LPs of vDOT/WETH 98/2 pool.
- 15% of minted vDOT in expansion will go to LPs of vDOT/WBTC 80/20 pool.
- 70% will be used to redeem for vDOT coupons.

When 1 vDOT $<$ 1 DOT, the system goes into a contraction phase and users could burn vDOT for vDOT coupons at a premium. We also implement similar innovative mechanisms from vUSD to protect the peg.

- Reserve Fund will initiate the buy back when the system is in contraction phase
- After a certain period of contraction phases, further buy back from VALUE ecosystem profit could be requested (subjected to VALUE governance vote)
- Coupon premium will change with 2h TWAP instead of epoch TWAP
- Further incentive for LPs from burned vDOT to keep their liquidity in contraction phase

We also have 4 epochs lockup for vDOT/wBTC 80/20 pool and 8 epochs for vDOT/WETH 98/2 pool.

### 3.3 Bootstrapping Period

During the bootstrapping phase, the vDOT price oracle will be set to 1.2 DOT for the first 14 epochs which results in 7 days. After this phase, the system will react according to the true vDOT market price.

### 3.4 How to get vDOT?

To distribute vDOT fairly to users, we have chosen 4 seed pools: VALUE, WBTC, WETH, LINK to distribute vDOT. 10k initial vDOT will be distributed to 4 seed pools across 7 days (2.5k vDOT for each VALUE, WBTC, WETH and LINK pool).

**The ValueDeFi team is committed to working with the Polkadot and Moonbeam teams to port over the vTokens concept to the Polkadot/Kusama Parachain. As the first proof of concept, vTokens will be ported to the MoonBeam parachain to demonstrate its capabilities. Chainlink's upcoming integration on the MoonBeam Parachain irens one of the reasons why we chose MoonBeam for our project. Nevertheless, we are also evaluating other ecosystems to extend our cross-chain capabilities.**

**The decentralized lending platform from ValueDeFi [3] will accept vUSD, vBTC, vDOT, ESD and BAC as a new class of seigniorage tokens.**

## References


[1] Empty-Set-Squad. "Døllar". In: (2020). https://github.com/emptysetsquad/dollar/raw/master/d\OT1\ollar.pdf.

[2] J. Chen N. Al-Naja and L. Diao. "Basis: A Price-Stable Cryptocurrency with an Algorithmic Central Bank". In: (2018). https://www.basis.io/basis_whitepaper_en.pdf.

[3] ValueDeFi team. "Elastic Decentralized Loans powered by Chainlink". In: (2020). https://valuedefi.medium.com/elastic-decentralized-loans-powered-by-chainlink-479c137866c8.