Silk: A Privacy-Preserving Collateralized Reflexive Currency

Sutera Duniya, Christian Aghyarian, Carter Woetzel
shadeprotocol.io

Abstract. Pure supply-absorption algorithmic stablecoins without sufficient asset backing or economic value accrual carry a disproportionate amount of systemic leverage that has historically resulted in catastrophic depeg events (i.e. Terra/Luna, TITAN). In contrast to this, overcollateralized stablecoin models struggle with capital efficient supply growth despite consistently maintaining their respective pegs. Stablecoins that are pegged one-to-one with a sovereign currency inherit inflation and centralized monetary policy risks. Finally, a lack of privacy for stablecoins brings regulatory and consumer risks for Web2 integration.

Silk is a solution to the myriad of existing problems outlined above. Silk is a reflexive privacy-preserving collateralized stablecoin pegged to a basket of global currencies and commodities launching on Shade Protocol. Silk maintains its peg using a combination of overcollateralization, protocol level arbitrage, reserves, redemption, and supply-absorption mechanisms. Primary collateral backing the system is SHD ("Shade") the governance and treasury token of Shade Protocol. SHD holds intrinsic value due to receiving revenue streams from multiple Shade Protocol DeFi primitives (DEX, lending, payments, insurance, bonds, synthetics, etc.). Auditable privacy is an additional key component for bridging Silk from Web3 consumers to Web2 merchants. Silk achieves this transactional privacy using the SNIP-20 token standard on Secret Network.

Silk

Silk is a privacy-preserving and smart contract interoperable stablecoin. Built on Secret Network, and made possible via the SNIP-20 private and fungible token standard, Silk maintains transactional privacy for all token holders of Silk. Key to Silk is that it functions as a medium of exchange, is a store of value (pegged to a basket of currencies and commodities via Band Protocol oracles integrated into Shade Protocol), is a unit of account (with an initial peg of ~$1.05) , while also being a standard of deferred payment - all of which give Silk the four key fundamental properties of money[1]. To simplify explanations, graphics and explainers below will use $1 as the peg to explain mechanics, but in reality the Silk peg is always slowly migrating above and below the initial starting point based on the value of the basket of currencies and commodities that Silk is pegged to.

Silk is collateralized and stabilized by a variety of crypto-assets that exist within Shade Protocol primitives and Secret Network. Silk replaces the payments value chain (credit card networks, banks, payment gateways) with a single application-layer protocol. Shade and Silk are credibly neutral, distributed, and have transactional privacy by default. Important for compliance and transparency is that Silk and Shade transactions can be decrypted with a viewing key unique to the address owner of the Silk tokens; this empowers users to be transparent by choice. Additionally, users have the option to share data with trusted necessary entities that need an audit trail of transactions.

[1] Model inspired by
https://makerdao.com/en/whitepaper/#what-properties-of-dai-function-similarly-to-money

Minting & Stability

The minting of a stablecoin is the act of issuing a token that ultimately takes the form of a liability that the protocol must answer for at a later time via redemption or sale of the stablecoin for a corresponding amount of underlying promised value. The incentive for a protocol to issue a liability in the form of stablecoin to a user is on the basis of revenue received for the service provided. With Silk, users repay Shade Protocol for the service provided primarily via interest payments as well as liquidation profit-sharing. Silk uses a hybrid model utilizing the following stability mechanisms:

- Bounded Conversion Minting[2]
- Overcollateralized Minting[3]
- Collateral Redemptions[4]
- Reserve Redemptions[5]
- Bonds[6]

Bounded Conversion Minting is a heavily parameterized version and risk averse seigniorage style minting that can only be leveraged by the protocol as the only trusted actor. Overcollateralized minting follows the tried and true collateralized lending model inspired by MakerDAO. Collateral redemptions are a redemption mechanism for tranches of at risk lending positions. Reserve redemptions are a minting and redemption mechanism whereby users can deposit stables to mint Silk, as well as redeem Silk against a pool of stablecoins. This mechanism aspires to become dynamic and partially collateralized, similar to FRAX. Finally, bonds are a mechanism whereby the protocol can repurchase or issue Silk at a discount or premium to help grow the treasury as well as maintain stability of the Silk peg.

Between these five primary stability mechanisms, Shade Protocol has a wide range of tooling to safely grow Silk overtime with a level of fine tuning that is currently inaccessible to stablecoins that only have one or two stability mechanisms.

Stability Mechanism Interplay

With five different stability mechanism available for Shade Protocol, there becomes a need to address the collateralization philosophy of the protocol with respect to what stability and minting mechanism are most heavily relied on over the lifespan of the protocol.

The following are a set of stability principles for Shade Protocol:

- Stability > Growth
- SILK > SHD

---

[2] Inspired by Terra, with significantly safer risk parameters
[3] Inspired by MakerDAO
[4] Inspired by Yeti Finance
[5] Inspired by FRAX
[6] Inspired by OlympusDAO

- Commerce creates stability
- Build reserves for unforseen bad debt
    - Silk LAR
    - BCM
- Governance defines risk profile
- Diversify where Silk is used in DeFi
- Openly plan for the failure of Silk
- Openly plan prevention steps in event of failure
- Natural pessimism towards bridging solutions
- Natural pessimism about quality of assets

Here is a high level break down of the various mechanisms roles:

- Overcollateralization mechanism is a weak growth mechanism because volatility of the underlying collateral (backing the minting of Silk) can rapidly decrease or increase supply of Silk. However, this is the safest type of Silk minting. True long term adoption won't be built off of a mechanism that introduces Silk into circulation via leverage.
- The redemption pool mechanism is the most scalable solution to building Silk adoption as stable assets backing the minting of stable assets is sustainable and preferred to volatile assets backing the minting of stable assets.
- Collateral redemptions should be thought of as working side by side with the overcollateralized model and is not a growth mechanism in any capacity.
- Bounded conversion minting is a Shade Protocol growth mechanism for its primitives (swap & lend) focused on deepening liquidity and maintaining accurate prices - this should not be used as a direct mechanism to expand Silk supply (i.e. naked minting).[7] Rather, BCM increases adoption of Silk on the peripheral by enriching user's interaction with Shade primitive and Silk.
- Bonds are a treasury bootstrapping mechanism that allows the DAO to directly interact with the Silk and SHD market. Bonds are considered a bootstrapping tool, and a potential stability mechanism in the late game of Silk adoption and expansion.
- Recommended that collateralization ratio of Silk targets 90 - 150%

Bounded Conversion Minting

The innovative component that Shade Protocol is adding to Silk's hybrid stability model is known as *Bounded Conversion Minting (BCM)* - an iteration on Terra's seigniorage minting. BCM is focused on intensive risk parameters & protocol permissioning to drastically reduce long tail risk of a potential death spiral. Before we can outline the mechanisms at length for BCM, it is prudent to start with a summary of existing algorithmic stablecoin principles. Typically with algorithmic stablecoins, payment for the underlying service of maintaining stability of the issued stablecoin is paid to the protocol from users in the form of increasing the scarcity of the underlying equity token backing the liabilities as well as a conversion minting fees that gets returned to stakers that are

[7] Naked minting is the process of minting Silk without depositing it into a liquidity or stability mechanism.

absorbing the market volatility tied to the respective equity backing. Protocols that have used components of this method (FRAX, UST, TITAN) have justified this component by having the equity scarcity component be part of the algorithmic stability mechanism for the underlying issued stablecoin liabilities. This algorithmic stability method referred to in this work is defined as the *supply absorption mechanism* which is the process of redeeming liabilities (in the form of a stablecoin) by burning the stablecoin and minting out underlying equity tokens - a dilutive process that absorbs the volatility of the decrease in demand for the stablecoin by pulling stablecoins out of active circulation in return for the dilution of equity that was previously made more scarce by increases in demand for the respective stablecoin. During volatile environments, the supply absorption mechanism has created *death spiral* economic events (i.e. UST, TITAN) where dilution of equity and decrease in demand for the stablecoin occur at such a rapid rate in parallel that the equity backing the issuance of the stablecoins is no longer able to absorb the decrease in demand for the underlying stablecoin. While the *supply absorption mechanism* method has been proven to be dangerous during *death spiral* events, the claimed hypothesis within this work is that it is actually the supply creation mechanism that generated systemic risk that ultimately was the key destructive force behind the depeg events of UST & TITAN. The *supply creation mechanism* is defined as the process of burning underlying equity to mint liabilities in the form of a stablecoin that the protocol must answer for at a later time. That is to say, this work assumes the supply absorption mechanism works within a bounded set of market conditions tied to risk parameters that directly impact issuance and redemption of the stablecoin. Therefore, if the supply creation mechanism of the stablecoin can be properly bounded, it would stand to reason that the supply absorption mechanism will consistently perform its intended role.

The following are the fundamental risks and questions that exist within the supply creation mechanism:

- What entities can mint liabilities against equity?
- What entities can redeem liabilities for equity?
- How many liabilities can be issued against equity in relation to system wide collateralization?
- How many liabilities can be issued against equity in relation to equity depreciation post-liability issuance risks?
- What is the optimal speed of issuance & redemption policy execution?
- Where are the issued liabilities used and under what conditions?

With both TITAN and UST, any entity was capable of interacting with the seigniorage contracts to mint or burn the respective stablecoins. The smart contracts were designed to discourage certain conversion minting behavior based on market conditions via the amount of slippage incurred during the conversion process. Example: there were higher conversion fees for burning UST when the UST market price was greater than $1. In essence, the protocol was designed to discourage people from reducing circulating supply when it needed to expand the supply in order to bring dollar parity back to the UST peg. Ultimately, despite these slippage costs any malicious user could perform the following sequence of actions (even with slippage costs incurred):

1. Purchase 10,000,000 LUNA at $30 (assets = $30M, liabilities = $0)
2. Coordinate to push LUNA to $100 (assets = $100M, liabilities = $0)

3. Conversion mint 10M Luna into 100M UST (assets = $100M, liabilities = $100M)
4. Coordinate to push LUNA to $30 (assets = $30M, liabilities = $100M)
5. Sell 100M UST ($70M asset-to-liability disparity)

Observers of the UST depeg event have noted that the moment UST market capitalization was greater than the market capitalization of LUNA (equity backing the system) was the moment there was economic proof of systemic instability. Fundamentally, users could mint out liabilities in relation to a LUNA price that was not sustainable. This risk is what is referred to in this work as the *open liability issuance assumption*: the Terra and TITAN models made the assumption that any actor could be trusted to interact with the conversion minting smart contracts at any point in time, with the only counteractive force being slippage fees tied to the seigniorage model. However, an actor could easily space out conversion minting in the above sequence to still achieve the same target effect. Because seigniorage was the only mechanic to expand or contract the supply of the stablecoin, the protocols were entirely reliant on users interacting with these contracts in a non-malicious way. Because Shade Protocol has other stability and issuance mechanics, the reliance on permissionless participation in the supply creation mechanism is sidestepped.

In summary, the risks of having any entity be able to mint out liability against equity is simply too great and exploitable by patient counterparties that are capable of shifting market conditions (or waiting for said conditions) to generate an asset-to-liability disparity that can be economically exploited in an attack. With bounded conversion minting, Shade Protocol resolves the risks of the open liability issuance assumption by making it such that *only the protocol itself* is capable of issuing liabilities against equity and redeeming liabilities against equity.

This shift in model addresses the following two of six risks that exist from the supply creation mechanism in algorithmic stablecoin models:

- Only the protocol can issue liabilities against equity
- Only the protocol can redeem liabilities for equity

This leaves four remaining risks to be accounted for in the bounded conversion minting model:

- How many liabilities can be issued against equity in relation to system wide collateralization?
- How many liabilities can be issued against equity in relation to equity depreciation post-liability issuance risks?
- What is the optimal speed of issuance & redemption policy execution?
- Where are the issued liabilities used and under what conditions?

System wide collateralization is defined as the amount of value in the form of crypto assets that Silk can be redeemed against via direct redemption or sale. Management of the Silk Issuance Policy (SIP) is a configurable governance parameter that represents the amount of Silk that can be issued (in relation to system wide collateralization) using BCM. A BCM-SIP of 5% implies if total value of assets backing the system is $100M, then 5M Silk can be issued via BCM (assuming a $1

peg for simplicity sake). It is recommended that BCM-SIP targets a collateralization ratio across all stability mechanisms of greater than 110% percent until there is enough data to push towards a partially collateralized system ranging somewhere between 80-100% (FRAX used as inspiration for this range).

Example:

- $100M in assets backing Silk from Shade Lend (with 150% collateralization ratio)
- $100M in stablecoins backing Silk from Silk Redemption Pools (~100% collateralization ratio)

In the above example, prior to any minting of Silk via BCM, the total asset-to-liabilities ratio is ((100M * 1.5) + (100M * 1))/2 = 125% collateralization ratio. As such, assuming zero faith in the protocol's use of the supply absorption mechanism, having a BCM-SIP targeting 10% means 20M Silk could be strategically issued by the protocol while still maintaining a system wide collateralization ratio of 115%. This introduces a degree of flexibility that allows the protocol to deepen liquidity and increase the usage of Shade Protocol primitives in a safe and bounded fashion.

However, a fundamental problem exists whenever liabilities are issued against equity that is volatile. What if the market value of SHD drops while liabilities issued at a certain equity valuation are still in active circulation that must eventually be accounted for via BCM? This risk is defined as *equity depreciation post liability issuance (EDPLI)*. Pure algorithmic models inherit a significant amount of EDPLI risk because the entirety of the stability and expansion of the system is exposed to the unpredictability of the collective equity capitalization backing liabilities that have been issued at a range of time frames each with different levels of equity backing. In order for Shade Protocol to safely leverage BCM within a safer context, the model must address its management of EDPLI.

With Shade Protocol, EDPLI is bounded by risk management of the following three variables:

- Definition of the fair value of SHD
- Volatility buffer (VB) assumed with the divergence of market price of SHD from the fair value of SHD
- Amount of SHD backing the issuance of Silk via BCM

The fair value of SHD is defined as the average of the following two components:

- Treasury value of SHD
    - Value of all assets on the ShadeDAO / total SHD in the ShadeDAO
- 200-day moving average of SHD price

The volatility buffer is a configurable variable that should be treated as a variable that represents how much worse the protocol believes the market will diverge from the fair value of SHD (which already takes an extremely conservative stance on the SHD price valuation). The ShadeDAO holds a significant amount of supply (~1M SHD) that can be used to back Silk issued via BCM.[8] This

[8] Official Tokenomics:
https://medium.com/@shadeprotocoldevs/shade-protocol-tokenomics-833567473635

treasury backing of Silk issued via BCM using SHD on the treasury is known as the *fair value backing ratio* (FVBR) which targets an equity backing ratio of 200%.[9]

Here is an example using the above risk parameters:

The BCM-SIP is comfortable issuing 20M Silk. The price of SHD is trading at $50, with a fair value of $20 per SHD. The treasury holds 1M SHD and is comfortable with a 200% FVBR and is using a 10% volatility buffer. The ShadeDAO is capable of supporting the following (known as the EDPLI Risk Management Model):

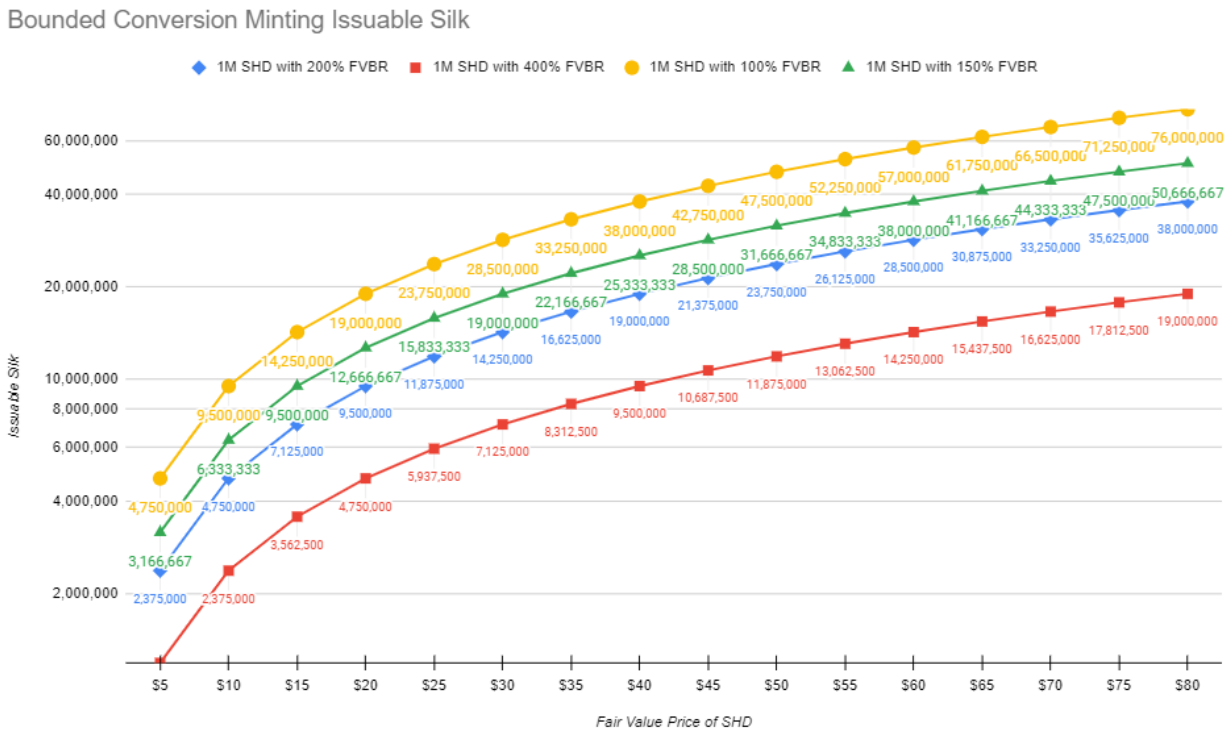
ShadeDAO SHD Supply = S
Fair value of SHD = F
Fair value backing ratio = R
Value of treasury = X
Volatility Buffer = V
Issuable Silk = I

*X = S * (F - (F * V))*
*I = ((S * (F - (F * V))) / R) OR I = (X / R)*

I = (1M * ($20 - ($20 * 10%)) / 2)
I = 9M Issuable Silk

In the above example, despite the BCM-SIP being comfortable with 20M Silk in relation to system wide collateralization, the localized risk parameters handling EDPLI is only comfortable with 9M Silk being issued from BCM. The claim of the risk parameters is that the protocol can maintain the target peg of Silk assuming all 9M Silk was sold on the market with no other stability components of Shade Protocol stepping in to handle the sale or redemptions other than BCM. Due to the conservative FVBR as well as an extremely conservative FV calculation for SHD (combined with a volatility buffer) means that Shade Protocol's bounded conversion minting has properly accounted for EDPLI risk. Shade Protocol governance can dynamically adjust the risk profile as necessary. The less aggressive the EDPLI & SIP-BCM risk management variables are set to, the more risk SHD tokenholders carry. Because SHD tokenholders govern these parameters, the introduction of additional risk via governance consensus for said tokenholders is both necessary and optimal.

[9] Configurable by governance, inspired by Djed.



The above chart plots the amount of issuable Silk based on a variable fair value backing ratio (FVBR) from SHD on the treasury as well as varying amounts of fair value computations for the price of SHD. The more conservative the FV of SHD, as well as the more conservative the FVBR is per SHD, the less Silk that can be issued from BCM. In conclusion, the EDPLI risk management model Shade Protocol used attempts to reduce systemic risk by deploying extremely conservative estimates of the value of the treasury while also deciding on how much Silk said treasury can safely back.

This shift in model to solve for EDPLI risk as well as
system wide collateralization risk resolves an addition two risks summating which collectively means this work has addressed four out of the six risks that exist from the supply creation mechanism in algorithmic stablecoin models:

- What entities can mint liabilities against equity?
- What entities can redeem liabilities for equity?
- How many liabilities can be issued against equity in relation to system wide collateralization?
- How many liabilities can be issued against equity in relation to equity depreciation post-liability issuance risks?

This leaves two remaining risk to be accounted for in the bounded conversion minting model:

- What is the optimal speed of issuance & redemption policy execution?
- Where are the issued liabilities used and under what conditions?

The speed of issuance and redemption can be achieved via a Speed of Policy Execution (SPE) variable which is defined as the following:

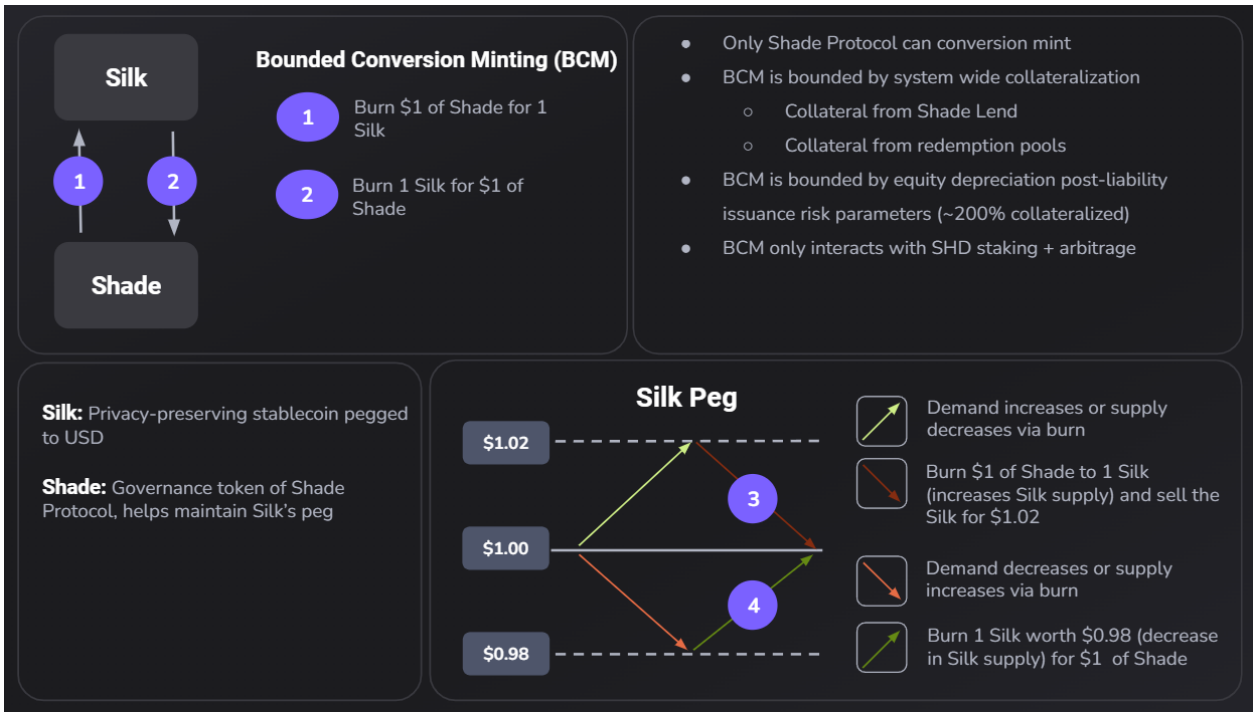
- (amount of Silk to mint or burn) / # of blocks

The more blocks desired for policy execution, the smaller the SPE variable. SPE determines how often the protocol arbitrage bot (Sky) performs desired executions to either pull Silk out of the market, or introduce new Silk into the market.

The final risk to address is where are these issued Silk liabilities used and under what conditions? Issuance of Silk and stability of said Silk via BCM is ultimately a service that must create a desired value accrual that is worth the additional risk introduced to underlying tokenholders. Where this Silk is used by the protocol also introduces an additional risk element. The following are the initial proposed actions / primitives that are assumed to be relatively safe to us BCM Silk:

- SHD staking
    - Burn staked SHD into Silk
    - LP the staked SHD with the conversion minted Silk
    - Burn Silk back to SHD when user bonds
- Protocol arbitrage
    - Burn staked SHD into Silk & arb price disparity, cycle back to SHD
    - Burn treasury Silk for SHD to arb price disparity

BCM accessibility for SHD staking (managed by the protocol) ultimately introduces additional stability for Silk by deepening locked liquidity. BCM accessibility for protocol arbitrage via staked SHD introduces additional stability for Silk from profitable price correction via arbitrage. Within both of these actions, Silk is introduced into the system wide collateralization equation from the depositing of Silk into an LP during arbitrage, as well as market buyers purchasing Silk from deepened LP pools from the BCM mechanic applied to SHD staking.



This work would contend that the supply absorption mechanism is sound if and only if the supply creation mechanism is bounded with proper permissioning and risk parameters while also ensuring that the mechanism is not the primary asset backing for the liabilities at large. Shade Protocol has properly bound the six primary risks of conversion minting that traditionally have only been tamed via slippage fees within other pure-algo stable models (UST, TITAN). Fundamentally, slippage fees only reduced the likelihood of certain negative short term behavior while ignoring the core compounding systemic risks tied to the open liability issuance assumption, system wide collateralization risks, asset duality reflexivity, lack of uncorrelated revenue streams, and a complete reliance on only a single stabilizing mechanism in the form of the supply absorption mechanism.

Overcollateralized Minting

With the proper exploration of BCM complete, this work now shifts to describing Shade Lend - the overcollateralized component of Silk issuance and stability that allows users to lend and borrow Silk against their underlying crypto collateral. This stability component maintains target parity via forced liquidation and sell off of collateral in order to pull Silk out of circulation in lockstep with changes in the value of the underlying collateral backing.

Lending is one of the primary methods of generating yield with deposited assets in most financial systems. Protocols like Aave and MakerDAO have shown that lending is one of the most in-demand protocols in DeFi. Specifically, MakerDAO's DAI[10] is an overcollateralized debt-backed stablecoin that is entirely backed by reserves of debt. Similar coins such as MIM from Abracadabra and H2O from Defrost Finance have followed in the wake of DAI's monumental success, and

[10] MakerDAO Whitepaper: https://makerdao.com/en/whitepaper/

because of this, there is now a fairly large body of economic data to draw on to understand the macroeconomic behavior of an overcollateralized debt-backed stablecoin. Shade Protocol's Silk is uniquely positioned to integrate this debt-backed system in addition to its algorithmic stability mechanism to minimize volatility of the SHD token, strengthen the peg of Silk, and generate significant revenue for the protocol.

Lending is the foundation of the modern financial system. In DeFi, there are two proven lending primitives. Money markets like Aave allow depositors to deposit collateral into a pool which gives them borrowing power to borrow different assets from other pools. Overcollateralized stablecoin protocols allow users to deposit collateral to serve as reserve backing for an algorithmic stablecoin. This stablecoin is pegged at a value (usually $1), and the protocol will value the stablecoin at this pegged value regardless of the current market price. Stability is achieved by borrowing activity when the market price is greater than the peg price, and repaying of loans when market price is below the peg price. If the market price is higher than the peg price, then it becomes profitable to take out a loan and immediately sell the borrowed currency, driving the price back down to the peg. If the market price is lower than the peg price, then it becomes profitable to buy the discounted currency to repay your outstanding loans at a discount. The money market model has proven to be extremely resilient to attack, sustainable, and profitable.The overcollateralized stablecoin model, however, has consistently encountered a number of challenges such as the following:

- Most overcollateralized stablecoin protocols exist solely to deposit collateral and mint the debt-backed stablecoin, making it almost impossible to provide utility for the minted stablecoin.
- Relying solely on repayment of loans to drive a below-peg price up has proven to not be sufficient incentive in the case of many small and medium market cap tokens (e.g. $H2O, $MONEY, $AVAI)
- When a loan is taken out during a period of below-peg market price, these borrowers will actually lose money when the price is driven back up to peg, further disincentivizing repayment of loans.
- In the absence of stablecoin utility, most overcollateralized stablecoins experience significant downward pressure on the market price, even with stableswaps enabling 1-to-1 trades in extremely unbalanced liquidity pools.

Shade Protocol is capable of addressing all four of these challenges.

- Shade Protocol will be a whole array of privacy preserving DeFi primitives, meaning there will be no shortage of ways to provide utility for Silk.
- Because Silk will be overcollateralized, it is possible for some algorithmically backed Silk to exist in circulation and for the system to remain solvent, even if 100% of the algorithmically backed Silk in circulation becomes unbacked due to a catastrophic bank run, allowing for some additional protection from downward pressure on Silk's price.

- With a multitude of ways to generate upward pressure on market price, it is very unlikely that a user will ever take out a loan during below-peg market conditions since the length of time that Silk would be below peg is expected to be very short.
- Since absence of utility won't be a problem for Silk, and the growth of supply can be controlled through minting limits on Lend, conversion minting limits, and entry minting limits, we can likely ensure that Silk in circulation approximately matches its demand.

Shade Lend will combine these two models to provide additional overcollateralized backing for Silk, as well as providing a money market pool for borrowing Silk. At inception, Shade Lend will focus primarily on an *Isolated Risk Market*, an overcollateralized lending application in the style of Abracadabra or MakerDAO which will serve as the primary method of Silk expansion and contraction.

Isolated risk markets mimic traditional overcollateralized stablecoin protocols like Abracadabra. A vault contract will allow users to deposit a single asset as collateral. Silk is minted when a loan is taken out, and burned when the loan is repaid. Isolated risk markets will feature the following parameters:

- *Adjustable interest rates*. Interest rates will be determined based on the historical volatility trends of an asset. Interest rates can be raised or lowered by the protocol to capitalize on demand. For example, if we set a $10M limit on BTC backing for Silk, and we achieve that cap, we can increase the interest rate on BTC loans as there is surplus demand that we are not capitalizing on. These rates are fixed for simplicity, as the primary purpose of the first iteration of Lend is to provide strong backing for Silk. In a later version, variable interest rates to automatically adjust interest rates based on borrowing demand will be implemented, but more economic modeling has to be done before these yield curves can be confidently applied to the foundation of Silk. Interest rates can only be raised or lowered by small increments at a time to give borrowers ample time to adjust their positions.
- *Adjustable borrowing fees*. Borrowing fees are assessed when Silk is borrowed and is taken out of the borrowed Silk (e.g. if the user borrows 100 Silk with a 1% borrowing fee, they will receive 99 Silk in their wallet and have an outstanding debt of 100 Silk). The borrowing fee will be based on borrower demand (higher demand collateral = higher borrowing fees) and tail risk of the collateral (higher tail risk = higher borrowing fees). The borrowing fee can be adjusted by the protocol on demand, unlike the interest rate which will have an enforced time delay and step function to prevent sudden changes. Since the borrowing fee is charged when a loan is taken out, there is no impact to existing borrowers when the borrowing fee changes. Like interest rates, the protocol is working on experimental yield curves that can provide completely automatic dynamic borrowing fees, but these models must mature before they are used in Lend.

In order to maintain stability of Silk's peg, collateral must be liquidated when the loan-to-value ratio (LTV) of the vault is above the configured maximum. With Lend, liquidations will be a fair system using a stability pool. Most lending protocols in DeFi use a first-come-first-serve liquidation model which is an extremely competitive space that is completely dominated by bots. The barrier to entry is almost unachievably high, as the best liquidation bots will capture almost all liquidation value.

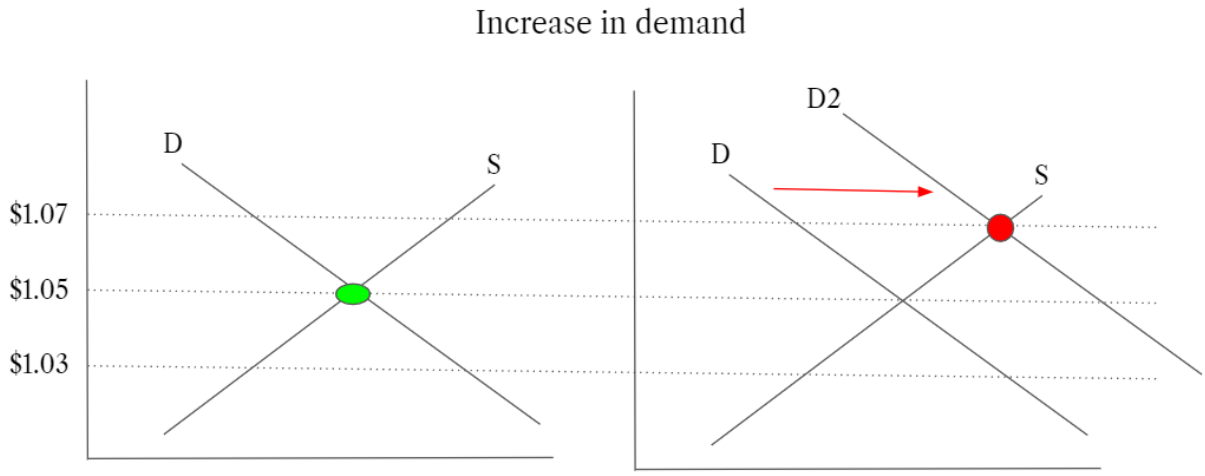
Collateral Redemptions

Introducing an additional stability mechanism to Shade Protocol is the creation of collateral redemptions via a stability pool. The *stability pool* is a pool of Silk deposits used for liquidations of vulnerable positions that violate the system wide collateralization rules. When a vault's LTV is too high, it will be marked for liquidation. When liquidated, Silk in the stability pool will be used to repay half of the outstanding debt, and the collateral backing the loan will be distributed to the stability pool depositors at a premium that is configurable per vault. The protocol will take a small percent of the liquidated collateral as revenue. Below is an example of stability pool driven liquidations for isolated risk markets:

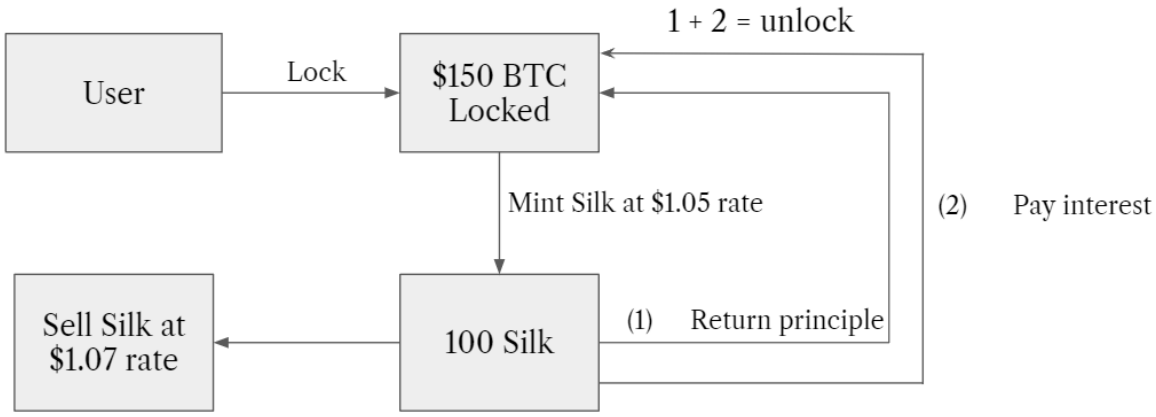
- User has $10,000 in BTC and $5,000 in debt. Maximum LTV for this loan is 60%.
- BTC drops 20% and the user's deposited collateral is now only worth $8,000, making their LTV 62.5%.
- The liquidation discount for this vault is 10%. To restore solvency, half of the user's debt is repaid by Silk in the stability pool, so $2,500 of Silk is taken from the stability pool and burned. $2,750 ($2,500 + 10%) of BTC is taken from the borrower's collateral.
- Liquidation profit is calculated at $250. If the protocol's share of liquidation profit is 20%, then $50 of BTC is sent to the protocol treasury, and the rest of the BTC ($2,700) is sent to the stability pool depositors as a claimable reward.
- In the event that the protocol's share would make a liquidation unprofitable for depositors, the protocol's share is instead also given to the stability pool depositors.

To understand the overcollateralized stability mechanisms and collateral redemptions role in building stability for Shade Protocol, this work will walk through a series of simple Silk economic examples.

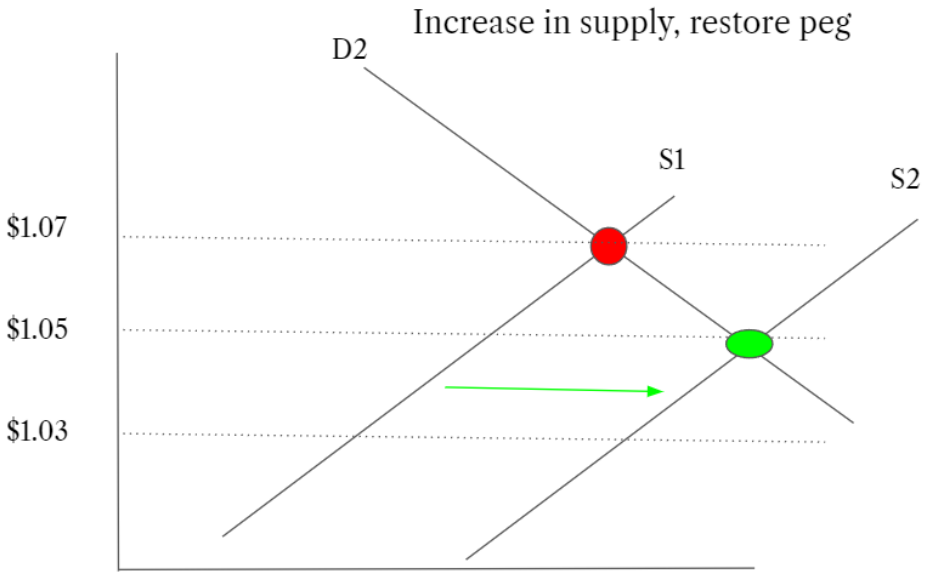
First, assume users have been purchasing Silk on a DEX such that the market price of Silk is greater than the target peg price as seen in the graphic below.



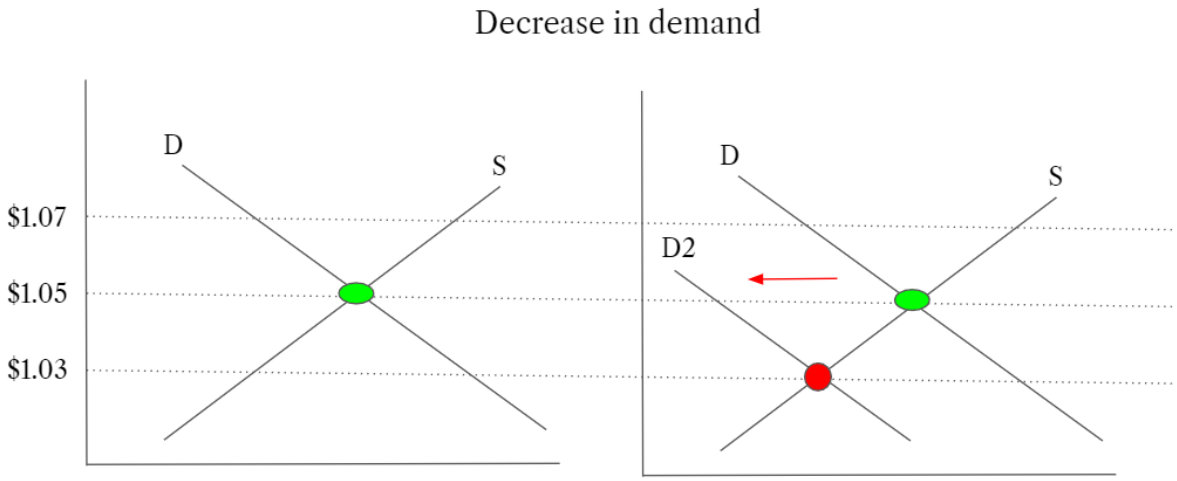
In order to bring Silk back to its target peg, there needs to be an expansion of the supply or a reduction in demand. The easiest way to achieve price parity is via expansion of supply which will be executed by a user due to the price disparity between the rate at which they can mint Silk compared to the market price of Silk - thus creating a profitable arbitrage opportunity.



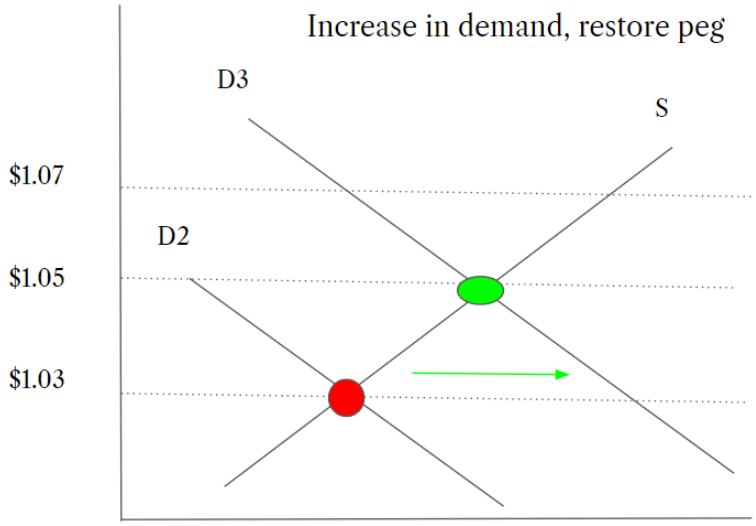
Once an arbitrage entity expands the supply and sells the Silk for arbitrage profit, the supply curve is restored back to equilibrium as seen in the graphic below.



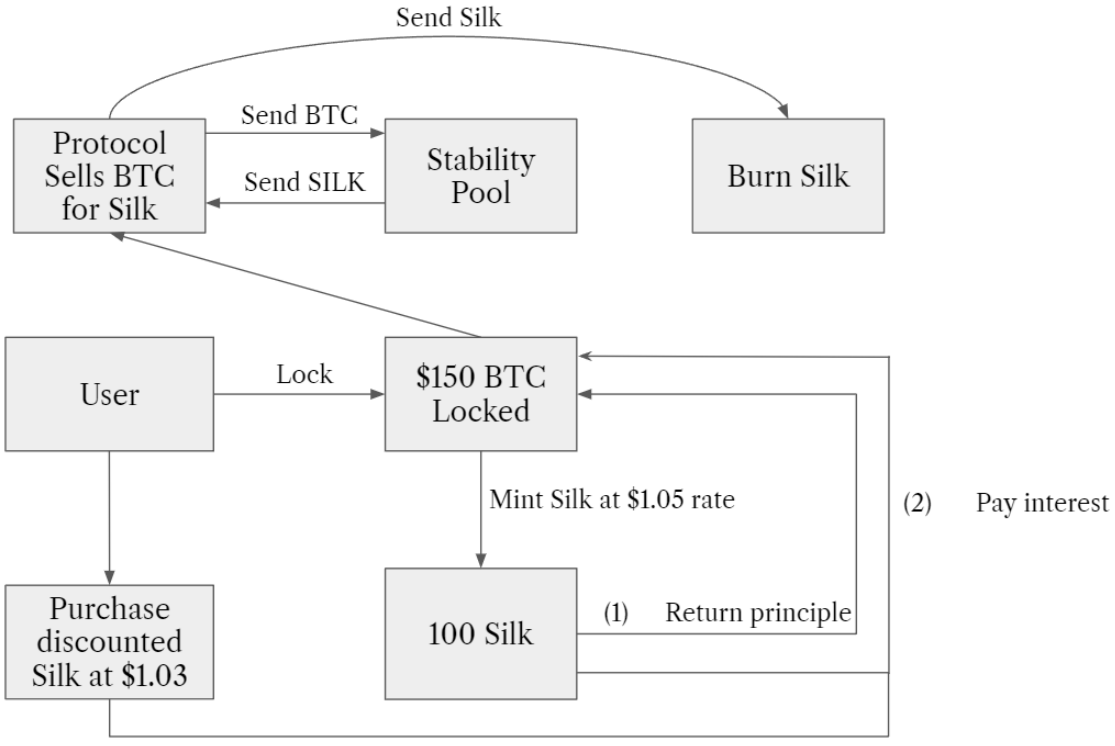
The next example is if Silk's market price decreases below its target peg due to a decrease in demand:



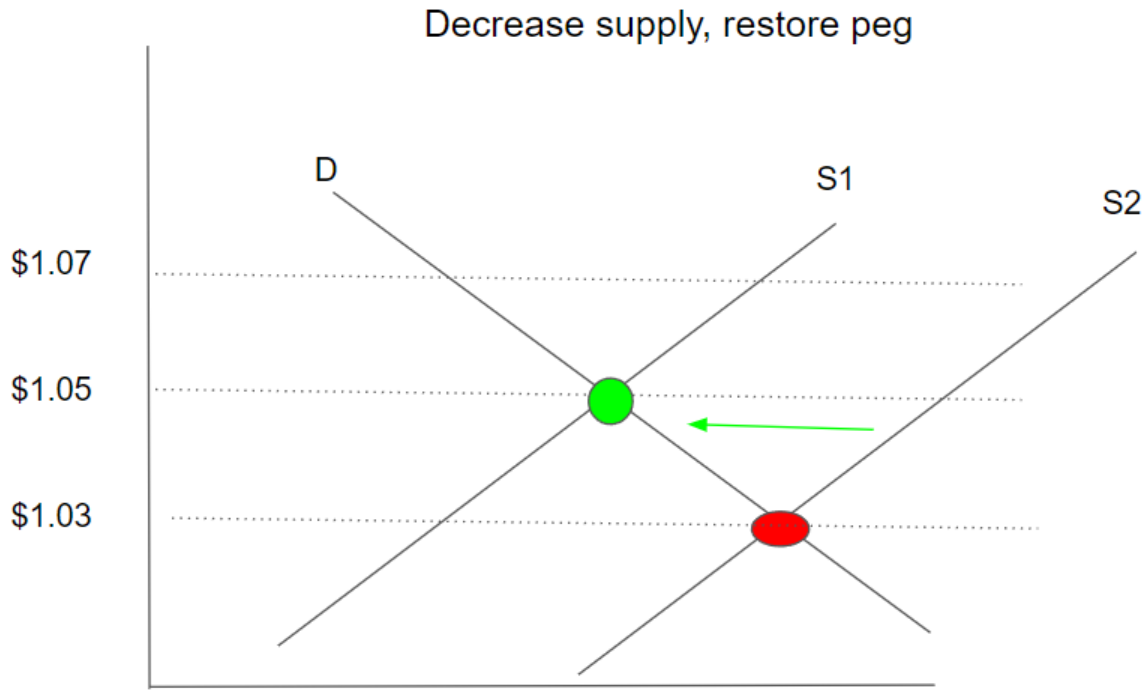
When Silk is below peg there are two solutions: increase the demand for Silk or reduce the circulating supply of Silk. Increasing demand for Silk is generated by the fact that users are able to purchase Silk at a discounted rate to pay back their loan interest payments to the protocol at a discount.



Discounted Silk and interest payments are a powerful effect (visualized effect above), but on its own is not enough to manage a sharp decline in demand for the overcollateralized stablecoin. In order to maintain proper system wide collateralization, the assets backing the issuance of Silk as a liability are liquidated by the protocol and sold directly for Silk using an auction system in order to pull Silk out of the secondary market.



The Silk is then burned (thus reducing the supply) in order to ensure no accidental bad debt is incurred (effect shown below). This overcollateralized auction is the primary mechanism used to keep Silk at its target peg during a contractionary event.



Redemption Pools

One of the core problems with overcollateralized issuance methodology is that users are required to enter into leveraged positions in order to arbitrage price disparities. Additionally, the supply of the stablecoin is tightly tied to the collective value of the underlying collateral that enabled the safe minting of the stablecoin. During contractionary events, massive amounts of stablecoin liquidity are withdrawn from the market due to forced liquidations. This is an inevitable side effect of the overcollateralized model working with volatile assets. However, if you introduce other stablecoins into the issuance model of Silk, then a new risk profile and stability mechanism emerges whereby users can deposit their stablecoin asset and mint out a corresponding amount of Silk. At a later time, a user can burn their minted Silk and redeem a corresponding amount of underlying stablecoin that was deposited into the redemption pools.

Redemption pools are defined as pools of accepted stables that Silk can be redeemed against. Users would choose to mint Silk via depositing a stablecoin into the redemption pool for the following reasons:

- No leverage required
- Less slippage than a DEX
- Silk can be redeemed against the redemption pool at a later time
- User can immediately mint Silk to then deposit into yield opportunities on the various Shade Protocol primitives

- Users can seamlessly convert their dollar stablecoin for a reflexive stablecoin that is pegged to a basket of global currencies and commodities

The redemption pool methodology was the original starting point for the FRAX algorithmic model before it incorporated more dynamic growth mechanisms that are similar to bounded conversion minting. FRAX started with a 100% collateralized stable pool that eventually migrated to being partially fractionalized once enough liquidity and adoption had been generated for FRAX. Using the redemption pool methodology, whenever the stablecoin is above the target peg, a user can simply deposit an accepted stablecoin into the redemption pool and mint out Silk which can then immediately be sold for arbitrage profits (deposit at $1 conversion rate, sell for $1.02). Whenever Silk is below peg a user can redeem their Silk for a corresponding amount of deposited stablecoins (using the target peg conversion rate) from the redemption pool. This redemption process burns the user's Silk while also creating an arbitrage opportunity where the user can purchase Silk at a discount and recursively follow the same redemption cycle until the peg reaches its target peg price parity.

A problem that emerges with the redemption pool methodology is a gap in assets to liability backing due to a potential appreciation in the value of Silk in relation to the collective USD capitalization of the redemption pool. This risk is known as *liability appreciation risk (LAR).*[11] An example of appreciation risk is as follows:

- User deposits 100 USDC into the redemption pool
- User mints out 95.23 Silk using the $1.05 target peg ratio
- Silk organically appreciates in value to $1.07 over the course of a year
- User returns to redeem their 95.23 Silk for the corresponding USD value ($101.89)

Due to the appreciation in price, the user is unable to fully redeem for their underlying promised value purely using the redemption pool. Fortunately, due to the overcollateralized and BCM stability mechanisms, the unaccounted LAR can be picked up by these two components on DEX pools to ensure that the user is ultimately able to redeem Silk (via sale) for the corresponding amount of promised value. Additionally, as the Silk appreciates in value over the course of the year, users will be depositing stablecoins to mint Silk at the ever changing target peg. This will in theory smooth out LAR from the range of entry points into the redemption pools. In the event that the dollar appreciates in relation to the Silk basket of currencies and commodities, there will actually be a surplus of available stablecoins in relation to the amount of USD value demanded by Silk redemptions.

Another variable that can assist with handling LAR is a slippage curve that converts fees into underlying stables that are returned to the stablecoin redemption pools - this makes it such that a bank run on the redemption pool is biased towards individuals that are the last to arrive at the redemption pool. The larger the redemption made within a compressed time frame of redemptions, the greater the fee incurred. It must be acknowledged that slippage curves alone do not solve LAR, however moving in parallel to BCM & overcollateralized stability mechanisms, the

[11] This risk is alluded to by Vitalik B. *"Two thought experiments to evaluate automated stablecoins* " - https://vitalik.ca/general/2022/05/25/stable.html

slippage curve can assist in smoothing out short-term malicious or dangerous usage of the redemption pools.

$$\sum(RedemptionFees) + \sum(RedemptionPoolStables) >= \sum(SilkRedemptionPoolLiabilities)$$

Silk was built with modularity in mind. Eventually, redemption pools will migrate towards the partially collateralized model used by FRAX whereby users (as a fictitious example) provide a summated 100% of value to mint out the stablecoin consisting of a deposit whereby 98% of the value is accounted for via assets in the form of stablecoins and the other 2% is accounted for in the form of SHD that gets burned. Redemption follows a similar pattern where a user is able to redeem their stablecoin for a mixture of uncorrelated stables and SHD. With proper design, the greater the volatility the more the redemption model shifts to being fully collateralized by stables versus being only partly collateralized by a mixture of stables and SHD. Shade Protocol aspires to implement this model as it fundamentally builds value for underlying equity (SHD) while also serving as a dynamic stability mechanism.

Bonds

The final stability component of Silk are bonds - Shade Protocol has the ability to sell an asset at a discount for a desired asset off the secondary market. If Silk is trading overpeg for an extended period of time, the ShadeDAO could issue a Silk bond at a discount in exchange for a desired yield bearing asset. This is not necessarily optimal as the discount rate is in essence an asset to liability mismatch that has to be accounted for at a later date, but if Silk is trading overpeg and other arbitrage mechanisms are not impacting the supply and demand disparity quick enough, the issuance of a Silk bond can help rapidly expand supply. The more useful stability mechanism with Shade Bonds is the ability to pull Silk out of the open market by selling treasury assets (specifically assets that are uncorrelated to SHD). With the discounted bond mechanism, Silk supply in active circulation can rapidly be reduced as users would take advantage of selling their Silk for another asset at a discounted rate. The less aggressive the vesting period and the greater the discount, the stronger this mechanism is for pulling Silk out of circulation.

A user story for this would be as follows:

- ShadeDAO offers to sell $1,000 worth of $ATOM for $990 worth of Silk with 14 days of vesting
- User deposits $990 worth of Silk
- ShadeDAO burns the Silk (reducing supply)
- User claims $990 worth of $ATOM 14 days later from the ShadeBond

Bonds are a more cost efficient way of acquiring a desired asset compared to buying and selling directly on a DEX. This is because the spot price is fixed and completely avoids slippage which is advantageous for both the user and the protocol assuming both counterparties are satisfied with the given spot price of the Silk bond.

Silk: Global Volatility Shock Absorption via Standardized Currency & Commodity Basket

Sutera Duniya
shadeprotocol.io

Abstract. Fiat currencies have become widely implemented for stablecoin pegs in Web3. Stablecoins built on top of single-fiat infrastructure inherit the individual underlying sovereign fiat currency risks and fundamentally lack monetary policy independence. Monetary policies attached to fiat systems introduce volatility into pricing relationships between goods and commodities in relation to that of the respective fiat currency. Fiat currencies have no intrinsic value and are not directly convertible into traditional stores of value (such as gold or other commodities). Value within a fiat system is derived from supply and demand for the fiat currency in addition to the demand and supply of all products and goods natively denominated by said fiat currency. Demand for fiat currency is fundamentally generated by the need to pay taxes denominated in the underlying fiat currency. Supply of fiat currency is entirely dictated by central banking systems (influenced by treasury bond markets and interest rate expectations/valuations).

Silk, a privacy-preserving global stablecoin, aims to solve the volatility and sovereign currency risk of single fiat currency stablecoins by pegging Silk to a basket of global currencies used by top 20 largest economies, with weights determined by relative GDP. The Silk peg is adjusted via Shade Protocol governance - benchmarking target weights by tracking relative GDPs and their respective size on an annual basis. The advantages of the Silk Currency Basket (SCB) are the following: lower volatility than fiat currencies and stablecoins, relative stability, bank independence, immunity to any single sovereign currency monetary risks, transparent standardization, and decentralization of governance. Additionally, Silk has the ability to add additional commodities and currencies to the peg via Shade Protocol governance - empowering Silk to not be tied to any single configuration into perpetuity.

Volatility

Fiat currencies are subject to a range of uncontrolled and semi-controlled variables: inflation, geopolitical conflicts, interest rates, FX markets and cascading lending risks attached to domestic market interactions with central banking lending policies[12]. While volatility can be hedged against within forex markets, this does not provide protection for everyday end users of the respective fiat currencies. Additionally, forex markets lack liquidity for hedges against exotic currencies, the cost of which is expensive.[13] Importantly, volatility makes prediction of future values uncertain - creating a deterrent for investment and trade that negatively impacts wealth generation and economic activity[14]. Any stablecoin pegged to a single sovereign currency (such as USD) by extension inherits the underlying risks and volatility. With the Silk Currency Basket (SCB), volatility is reduced via broad diversification and index mirroring of the global economy. As risk migrates through the global economy, it manifests itself within bilateral currency volatility and the respective currency exchange rates. This volatility is even more noticeable within smaller

[12] *Exchange rate volatility and trade flows*. International Monetary Fund. (n.d.). From https://www.imf.org/external/np/res/exrate/2004/eng/051904.htm.
[13] Zhang, R., Aarons, M., & Loeper, G. (2021, May 11). *Optimal foreign exchange hedge tenor with liquidity risk - Journal of Risk*. Risk.net. https://www.risk.net/journal-of-risk/7801426/optimal-foreign-exchange-hedge-tenor-with-liquidity-risk.
[14] *Global currency stabilization - WOCU*. (n.d.).http://www.wocu.com/upload/20726.pdf.

currencies. As such, a currency index basket that mirrors the global economy makes Silk extremely resistant to all of the uncontrolled variables and fluctuations of the global economy and by extension any single fiat currency. Thus, Shade Protocol and the architecture behind Silk posits that the creation of Silk is a net positive from a Global Modern Monetary Theory (GMMT) perspective.

Silk Currency Basket

The initial starting peg price of Silk will nominally target $1.05. To simplify examples, the SCB will use a target peg of $1.00 for Silk so the weighting mechanics are clearly understood. The dollar is used nominally as a reference currency for an initial target, but actual weights and price after initial establishment are decided purely by the value of the amounts of each of the respective currencies within the peg. After the initial establishment of Silk, the price of Silk will fluctuate in relation to whatever reference currency a user uses. The fluctuation in Silk price is based on the relationship of the reference currency to the rest of the basket of currencies within SCB. The SCB will be pegged to the following currencies using weights based on relative nominal GDP percentages of the top 20 largest economies (GDPs derived from IMF monthly reports) with available currency oracle datasets (Band Protocol used for V1)[15]:

Country	Currency	GDP (bn)	Amount	Weight
United States	USD	22,939.58	30.08324438	30.083%
China	Yuan	16,862.98	141.6585561	22.114%
Japan	Yen	5,103.11	763.2184019	6.692%
Germany	Euro	4,230.17	4.798457242	5.547%
United Kingdom	Pound	3,108.42	2.978750323	4.076%
India	Rupee	2946.06	289.5199473	3.863%
France	Euro	2940.43	3.335451679	3.856%
Italy	Euro	2120.23	2.405064808	2.780%
Canada	Canadian Dollar	2015.98	3.276048906	2.644%
Korea	Won	1823.85	2,813.904807	2.392%
Russia	Ruble	1647.57	153.3139914	2.161%
Brazil	Real	1645.84	12.17579453	2.158%
Australia	Australian Dollar	1710.56	2.983401206	2.243%
Spain	Euro	1439.96	1.633406338	1.888%
Indonesia	Rupiah	1150.25	21,549.31212	1.508%

[15] International Monetary Fund. (2021, October). *World Economic Outlook Database*. IMF WEOD.

Netherlands	Euro	1007.56	1.142917088	1.321%
Switzerland	Franc	810.83	0.973631646	1.063%
Turkey	Lira	795.95	10.02900189	1.044%
Taiwan	Taiwan Dollar	785.59	28.67331718	1.030%
Sweden	Krona	622.537	7.021610027	0.816%

Silk Currency Basket Advantages

Conceptually, Silk can be considered a hub or intermediary of swaps between different assets or currencies. Each currency or asset on the opposite end of Silk is valued according to the conversion rate between the local currency and Silk. As such, Silk functions as a stability hub. SCB is a direct alternative to direct conversion rates between currencies (inheriting the volatility of the currency relationships and risks) or between a currency and a respective commodity priced relative to the currency. Commodities and goods priced in relation to a sovereign currency inherit the volatility risks of the respective reference currency. By using Silk for everyday payments and settlement, there is a stabilizing effect created for any and all cost and revenue projections due to the reduction in volatility from Silk being an index currency. Additionally, Silk is a transparent derivative - making it easy to calculate its present and future value due to the collective stability of the underlying basket of currencies. As a result of Silk being a hub for swaps, settlement, and daily transactions, and due to the nature of the composition of the peg, Silk is essentially a perpetual hedge instrument that reduces sovereign currency risk. The end result is that ownership of Silk and the respective risk of holding Silk is independent of predictions for any of the following: future foreign exchange trends, currency relationship dynamics between pairs of currencies, individual currency volatility factors.

SCB is as reliable a store of value as the currencies within the composition of the Silk basket of currencies. However, due to the fact that Silk's peg composition is diversified, a Silk holder would retain value even in the case of a currency crisis within a constituent currency within the Silk peg. Silk holders would only risk losing the weighting of that particular currency within the basket. For those who generate income across multiple international demarcations, Silk vastly simplifies the question of where value can be safely stored due to the reduced costs of hedging (by simply holding Silk instead). Another benefit of SCB is that it can be deployed and used today without regulatory scrutiny. International political agreement is not required for index currencies, and therefore it is unnecessary to wait for political processes to culminate since Silk never claims to be pegged one-to-one with a sovereign currency (thus massively reducing regulatory risk). In summary, Silk has all of the advantages of national fiat currencies without the drawbacks of volatility that are native to single-fiat protocols. The more Silk is adopted, the more Silk will be used directly to settle payments between users, merchants, firms, and institutions on a global scale. This will empower Silk to become the de facto international meta-currency - increasing wealth across international communities by giving direct access to reduced volatility and hedging costs.

Peg Migration

The peg migration of Silk is based on governance votes for changes in weightages of the underlying peg composition. The new basis for currency amounts is rebased on a snapshot of the price of Silk before a shift to the new set of weights and currency amounts per governance update of weights. New weightages are re-applied in relation to this new amount, and individual currency amount contributions to the larger peg are shifted. In the below example, we will use $100 as the initial starting price peg for Silk - using a higher starting peg price makes changes in the weights more visible/understandable.

$$New\ Currency\ Amount\ =\ (\$100\ *\ New\ Weight)\ /\ Current\ Currency\ Quote\ (in\ USD)$$

$$\Sigma\ \{New\ Currency\ Amount\ *\ Currency\ Quote\ (in\ USD)\}\ =\ target\ peg$$

The following is a nominal and contrived example with a $100 starting peg:

Country	GDP	% of Total GDP	Currency	Dollar Quote	Currency amt.	Weight contr.
United States	22,939.58	43.908%	USD	$1.000000	43.90832601	$43.908326
China	16,862.98	32.277%	Yuan	$0.1561100	206.7592838	$32.277192
Japan	5,103.11	9.768%	Yen	$0.0087685	1113.963706	$9.767791
Germany	4,230.17	8.097%	Euro	$1.1561000	7.003640374	$8.096909

Now imagine that the collective value of the SCB is now worth $110 at the end of the year. Shade Protocol governance will then vote on new weights such that the underlying amounts of currency contribution to the peg shifts such that the currency amounts * currency quote adds up to the current price of Silk ($110). This is done instantaneously such that there is no jump in the price of Silk during weight changes, only direct modification to the currency contribution amounts. You will note that in the below example, the quotes for all of the currencies have changed with respect to the dollar (as well as the weights post governance ratification). These weight changes were determined by changes in GDP of the respective countries. Note that the weight contributions post update still add up to $110, as this was the price snapshotted (and is the existing quote for the value of SCB).

Country	GDP	% of Total GDP	Currency	Dollar Quote	Currency amt.	Weight contr.
United States	40,000.00	33.058%	USD	$1.0000000	36.36363636	$36.363636
China	20,000.00	16.529%	Yuan	$0.1061100	171.3487719	$18.181818
Japan	50,000.00	41.322%	Yen	$0.0093685	4851.848797	$45.454545
Germany	3,000.00	2.479%	Euro	$1.2261000	2.22434771	$2.727273
United Kingdom	8,000.00	6.612%	Pound	$1.5685000	4.636740372	$7.272727

Legal Landscape Theory

Stablecoins tied to individual sovereign currencies run the risk of a greater amount of legal scrutiny because of the derivative nature of the stablecoin. The nature of the scrutiny is tied to how large capital concentration on a derivative layer of a sovereign currency (in the form of a stablecoin) can negatively affect said sovereign currency stability and monetary policy. That is to say, stablecoins add additional risk to fiat systems because central banks no longer have 100% direct control over a portion of supply generation and contraction. Additionally, reserve backed stablecoins run the risk of directly impacting macroeconomics if enough liquidity is concentrated within these reserves as opposed to other key components of fiat distribution.

Silk is uniquely positioned because it is neither a reserve currency, nor is it directly tied to a single sovereign currency. Because Silk is not directly pegged to any given sovereign currency, it lives firmly outside the majority of regulatory scrutiny as Silk is not an underlying fiat derivative. Silk aims to be a hub and facilitator for global transactions, and does so with a level of neutrality and decentralization that is novel within Web3.

However, while Silk is uniquely positioned with the above features, there will inevitably be scrutiny surrounding the following variables[16]:

- KYC/AML/Cybercrime
- Tax Compliance

Silk is well positioned for scrutiny under the following:

- Safety, efficiency, and integrity of the payment system
- Data privacy, protection and portability (unique to Silk)
- Sound governance, including the investment rules of the stability mechanism
- Market integrity
- Auditability and compliance via permit key structure on Secret Network

[16] *Investigating the impact of Global Stablecoins*. (n.d.). Retrieved October 30, 2021, from https://www.bis.org/cpmi/publ/d187.pdf.

- Entities can decrypt their transactions and data

Special Drawing Rights

Special Drawing Rights (SDR) as defined by the International Monetary Fund (IMF) is an international reserve asset, created by the IMF in 1969 to supplement its member countries' official reserves. To date, a total of SDR 660.7 billion (equivalent to about US$943 billion) have been allocated. This includes the largest-ever allocation of about SDR 456 billion approved on August 2, 2021 (effective on August 23, 2021). This most recent allocation was to address the long-term global need for reserves, and help countries cope with the impact of the COVID-19 pandemic. The value of the SDR is based on a basket of five currencies—the U.S. dollar, the euro, the Chinese renminbi, the Japanese yen, and the British pound sterling[17].

Despite the global significance of SDR within the G8 and China, the SCB does not use SDR for weight standardizations for the following reasons:

- SDR is updated every 5 years
    - This frequency is not granular enough for Silk to be reflective of changes in the global economy and the respective weights associated with individual sovereign currencies
- SDR is defined by IMF, a political institution deeply impacted by sovereign nations
    - Representatives of IMF are mandated to pursue the self-interest of the countries represented within SDR
    - Currencies such as USD have an unfair weighting in relation to their respective GDP contribution - this is a result of political influence on the IMF
    - Excludes smaller economies and currencies on the global stage

Due to the frequency of the updates, decentralization of the peg, and the neutrality of the standard, SCB as outlined above is superior to SDR as an alternative basket composition.

Global Value Shift

In a scenario where commodities and cryptocurrencies such as Bitcoin gain a dominant, stable position in the global volume of transactions and trades, Shade Protocol will have the opportunity to include these commodities (digital or not) into SCB in order to make Silk more resilient and reflective of the existing macro environment. Conceivably, Silk could include any type of asset or currency into the peg - creating a degree of flexibility and reactivity (subject to Shade Protocol governance) that empowers Silk to exist beyond any significant global black swan events that impact any set of currencies and economies.

Conclusion

The age of globalization is being accelerated as a direct result of Web3. Now more than ever, the need for a stablecoin that does not inherit the risks of any single sovereign fiat is key. Also, because

[17] *Special drawing rights (SDR)*. IMF. (2021, August 5). Retrieved October 29, 2021, from https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/14/51/Special-Drawing-Right-SDR.

stablecoins to date are derivatives of individual fiat systems, they add additional risk to those existing economies. Silk is the solution - a globally distributed stablecoin pegged to a basket of currencies based on relative GDPs of the world's major economies. Silk serves as a lucrative settlement layer for transactions of every kind - Silk as a currency is more resistant to volatility and monetary policy than any stablecoin to date due to the design of SCB. Finally, Silk is uniquely positioned as neither a derivative stablecoin nor reserve currency, giving a distinct path to compliance and regulatory freedom within the existing international cryptocurrency and financial regulatory framework.