Shade Protocol: An Array of Connected Privacy-Preserving DeFi Applications

Carter Woetzel
shadeprotocol.io

Abstract. Shade Protocol is an array of distributed and interconnected privacy-preserving Decentralized Finance (DeFi) products that leverage the full capabilities of Secret Contracts on Secret Network. Using encrypted metadata for smart contracts unlock an entire layer of value previously inaccessible to DeFi protocols and users. Privacy integrated into DeFi products protects user anonymity, positions, and value transfer data. MEV (Miner Extractable Value) bots have decimated everyday users on various swap decentralized applications (dApps). Publicly visible collateralized positions have elicited larger market makers to leverage price movements to cause mass liquidation events for their own advantage. Front-running of NFT marketplaces have damaged the reputation of multiple platforms. Lack of transactional privacy has doxed various DeFi entities and has caused asset transfers to be monitored closely - restricting entities' ability to take a position privately without the market being made aware. Protocols such as Monero have long awaited DeFi products that have privacy by default.

Shade Protocol aims to fill this void and fully leverage Secret Contracts enabled by the architecture of Secret Network[1]. Shade Protocol is an interconnected ecosystem of privacy-preserving algorithmic stablecoins, synthetic assets and indices, lending products, leverage trading features, fixed income products, and option contracts. All of these products will be incorporated under the umbrella of Shade - the governance and utility token of Shade Protocol.

Shade Protocol

Shade Protocol is an ambitious array of application-layer products focused on a simple end user experience that involves the incorporation of privacy by default. These interconnected privacy-preserving DeFi products built on Secret Network will change DeFi as we know it - empowering the next generation of value creation and exchange. Silk is the first application of Shade Protocol. Silk is Secret Network's native privacy-preserving stablecoin that will underpin all of the other Shade Protocol applications that are created. Additionally, the governance token for Shade Protocol (Shade / $SHD) will be integrated into all of the products that are (or are not) listed on the product roadmap.

The native cryptographically-secured fungible protocol token of Shade Protocol is Shade (SHD) is a transferable representation of attributed governance and utility functions as specified in the protocol/code of Shade Protocol. The SHD token is designed to be used solely as an interoperable utility token thereon. SHD is the governance token for Shade Protocol and will be integrated into all of the products that are (or are not) listed on the product roadmap, as economic incentives for positive behavior.

DeFi is incomplete without privacy. Traditional financial markets offer a degree of privacy for users, and as a result offer up greater protections than existing transparent DeFi markets. Shade Protocol will provide the world's first truly decentralized and privacy-preserving financial applications - ushering in Web3 as originally envisioned by Secret Network. To echo the core

[1] Secret Network: Privacy-Preserving Secret Contract & Decentralized Application Platform [Whitepaper]

ethos of Secret Network, Shade Protocol will always push for privacy by default, privacy as an expectation, and privacy as the key to unlocking the full value of a decentralized future.

Shade Protocol Principles

- Privacy is a human right
- Privacy is the expectation
- All applications added to Shade Protocol must adhere to at least 1 of the following rules:
    - The application increases the utility for Shade
    - The application grows the Shade Treasury (Synthesis)
    - The application increases the utility of Silk
    - The application increases the demand for Silk
- No new unique token per application
    - Unique per application tokens create an end user experience designed around generating value for the specific application token as opposed to the end user
- Silk is agnostic with platform integrations
- Stability of Silk is a public good
- Triggers on actions that affect all token holders must be open-sourced
- Avoid non-collateralized inflation
    - Only exception: initial shade distribution pools
- Growth of the Shade treasury (Synthesis) > expenditures
- Treasury should passively build an account for liquidity providing rewards
    - LP is necessary for the functioning of Shade Protocol and is a long term public good
- Avoid fixed-rate values with Shade Protocol parameters when possible
    - Fixed rate values signal a lack of dynamic interaction with core attributes or a lack of measurement of value generation
- Do not overpay for security
- Do not sacrifice the end user experience in the name of tokenomics
- In order to realize the rewards of being a Shade staker, you must take on some level of risk to help stabilize the underlying protocol
- Periodic epoch transparency combined with privacy is the most effective way to create financially sensitive applications

Shade Protocol governance is responsible for enforcing and evolving these sets of principles over time as necessary. Principles are in the hands of the decentralized community - may these serve as powerful (initial) guidance towards a robust, effective, and useful protocol that will be adopted and used globally.

Definition Index

Abstract. Shade Protocol defines the following terms for the whitepaper linked below. Terms used in the whitepaper use the context as listed below and are not to be conflated with alternative definitions.

- **DeFi:** decentralized finance that is hosted on a blockchain platform.
- **Secret Network:** a blockchain that enables customizable privacy for smart contracts for developers and users to create and interact with.
- **Smart Contract:** programs stored on the Secret Network blockchain that run when predetermined conditions are met.
- **Shade Protocol:** an array of interconnected smart contracts that empower privacy-preserving DeFi applications.
- **Asset:** digital tokens that are traded in some capacity, thereby having a measurable amount of economic value and trading power.
- **Equity:** decentralized ownership of Shade Protocol via users holding SHD tokens. This ownership empowers users to vote on governance and management of the underlying protocol.
- **Liabilities:** the concept that the protocol holds a form of debt that needs to be accounted for within the protocol in order to maintain the stability of the system.
- **Redemption:** the process of depositing Silk into a Shade Protocol smart contract - upon doing this, the user receives a corresponding different token from the smart contract. The inverse is also true - Shade Protocol allows users to deposit assets into a smart contract and mint out a corresponding amount of Silk via a system of careful programmatic checks and balances.
- **SHD:** the governance and utility token of Shade Protocol.
- **Silk:** a decentralized stablecoin pegged to a basket of global currencies and commodities backed via a system of overcollateralization and careful checks and balances on minting.
- **ShadeDAO**: a decentralized treasury of assets and operations that is managed by SHD holders interacting with the Shade Protocol governance protocol.
- **Bounded Minting:** ability for Shade Protocol to mint Silk in relation to total protocol wide collateralization as well as collateral held on the ShadeDAO.
- **Collateralization**: the use of valuable assets to secure the stability of minted liabilities (in the form of Silk).
- **Overcollateralized Minting:** the ability for users to mint Silk by depositing an overcollateralized amount of value into a Shade Protocol minting vault.
- Balance Sheet: a tracking of all Silk that has been minted, and all assets controlled by Shade Protocol that are collateralizing the minted Silk.
- **Liability Appreciation Risk:** changes in the Shade Protocol balance sheet due to the appreciation in value of Silk in relation to the assets that are collateralizing the corresponding minted Silk.
- **Equity Depreciation Post Liability Issuance:** changes in the Shade Protocol balance sheet that emerge due to the depreciation in the value of assets controlled by Shade Protocol smart contracts.
- **Silk Issuance Policy:** a configurable governance parameter that represents the amount of Silk that can be issued (in relation to system wide collateralization) using the Bounded Minting mechanism.

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, and redemptions. Shade Protocol uses a diverse set of collateral (stablecoins such as USDC, ATOM, SCRT, etc.) as well as 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[2]. 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,

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

users have the option to share data with trusted necessary entities that need an audit trail of transactions.

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 Minting[3]
- Overcollateralized Minting[4]
- Collateral Redemptions[5]
- Reserve Redemptions[6]
- Bonds[7]

Bounded 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.

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

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

- Stability > Growth
- Silk > SHD
- Commerce creates stability
- Build reserves for unforseen bad debt
    - Silk liability appreciation risk
    - Bounded Minting
- 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

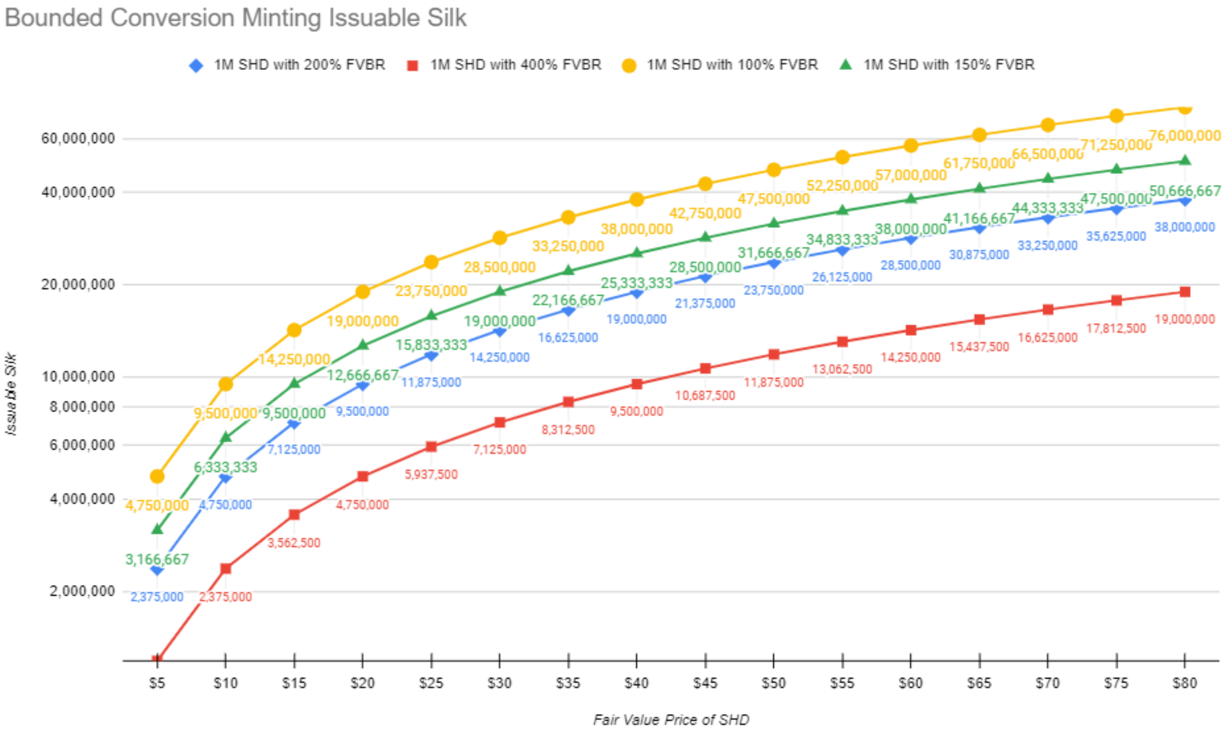
Here is a high level break down of the various mechanisms roles:

- 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 because the value of the assets collateralizing Silk is greater than the issued liabilities.
- 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 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).[8] Rather, Bounded Minting increases adoption of Silk on the peripheral by enriching user's interaction with Shade primitives and Silk.
- 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.
- 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.

Bounded Minting

The innovative component that Shade Protocol is adding to Silk's hybrid stability model is known as *Bounded Minting (Bounded Minting)* - an iteration on Terra's seigniorage minting. Bounded Minting is focused on intensive risk parameters & protocol permissioning to drastically reduce long tail risk of a potential death spiral.

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



Before we can outline the mechanisms at length for Bounded Minting, 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 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. In high volatility 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* has been proven to be dangerous during *death spiral* events, the 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 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 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 Bounded Minting. A Bounded Minting-SIP of 5% implies if total value of assets backing the system is $100M, then 5M Silk can be issued via Bounded Minting (assuming a $1 peg for simplicity sake). It is recommended that Bounded Minting-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 Bounded Minting, 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 Bounded Minting-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 Bounded Minting? 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 Bounded Minting 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 Bounded Minting
- EDPLI is limited by the Bounded Minting SIP mechanism which assumes zero faith in the Bounded Minting backing of Silk.

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

- Risk adjusted value of SHD
    - Total Value Of ShadeDAO Assets/ circulating supply of SHD
- 200-day moving average of SHD price
    - Selected as an extremely conservative estimation of the market's estimation of SHD value. Compressed volatility is the primary risk of valuation, and thus a conservative estimate such as this helps reduce said risks.

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 Bounded Minting.[9] The ShadeDAO collateralization of Silk (issued via Bounded Minting using SHD from the treasury) is known as the *fair value backing ratio* (FVBR) which targets a collateralization ratio of 200%.[10]

Here is an example using the above risk parameters:

The Bounded Minting-SIP is comfortable issuing 20M Silk. 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 can mint the following amount of Silk through Bounded Minting (known as the EDPLI Risk Management Model):

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

[10] Configurable by governance, inspired by Djed.

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

$X = S * F (1 - V)$
$I = ((S * (F - (F * V))) / R)$ *OR* $I = (X / R)$

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

In the above example, despite the Bounded Minting-SIP being comfortable with 20M Silk in relation to system wide collateralization, the EDPLI Risk Management Model is only comfortable with 9M Silk being issued from Bounded Minting. 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. The protocol does so via buying Silk using the ShadeDAO's collective treasury assets (assuming there is sufficient liquidity markets). 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 Minting has properly accounted for EDPLI risk. Because SHD tokenholders govern SIP parameters, the introduction of additional risk via governance consensus for said tokenholders is both necessary and optimal.

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 Bounded Minting. 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 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 Bounded Minting 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 Bounded Minting 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

Bounded Minting accessibility for SHD staking (managed by the protocol) ultimately introduces additional stability for Silk by deepening locked liquidity. Bounded Minting 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 Bounded Minting 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 Bounded Minting 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[11] 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 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.

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

- 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.

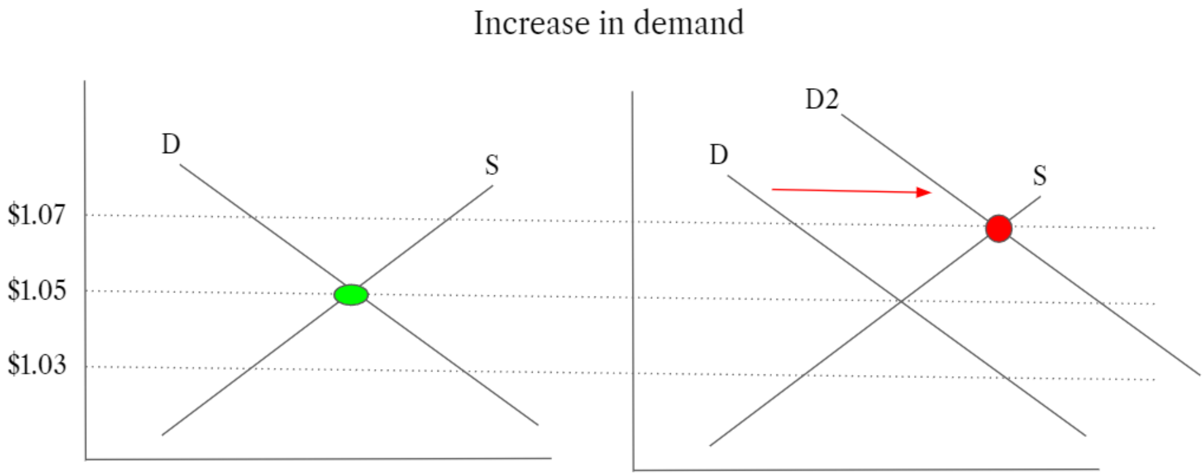
Collateral Redemptions

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:

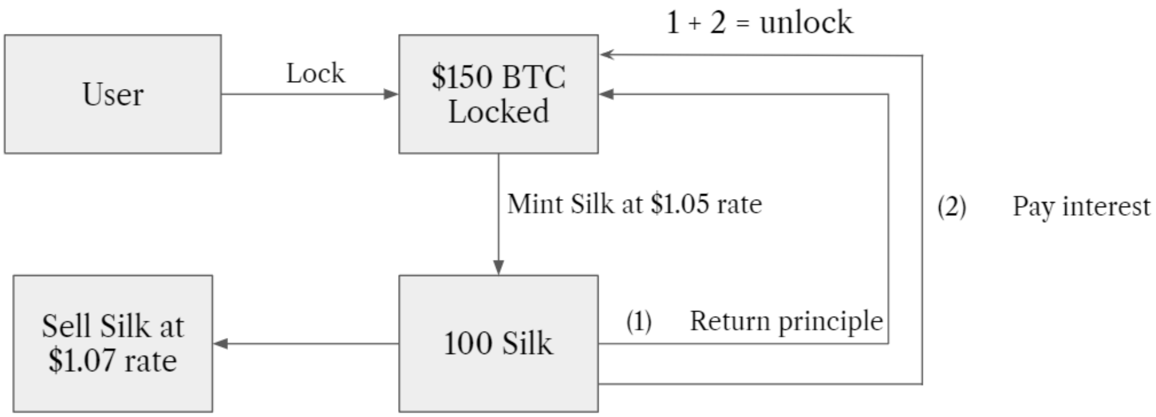
- User has $10,000 in BTC and $5,000 in debt. Maximum LTV for this loan is 60%.
- BTC drops 20% and the user's deposited collateral is now only worth $8,000, making their LTV 62.5%.
- The liquidation discount for this vault is 10%. To restore solvency, half of the user's debt is repaid by Silk in the 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.

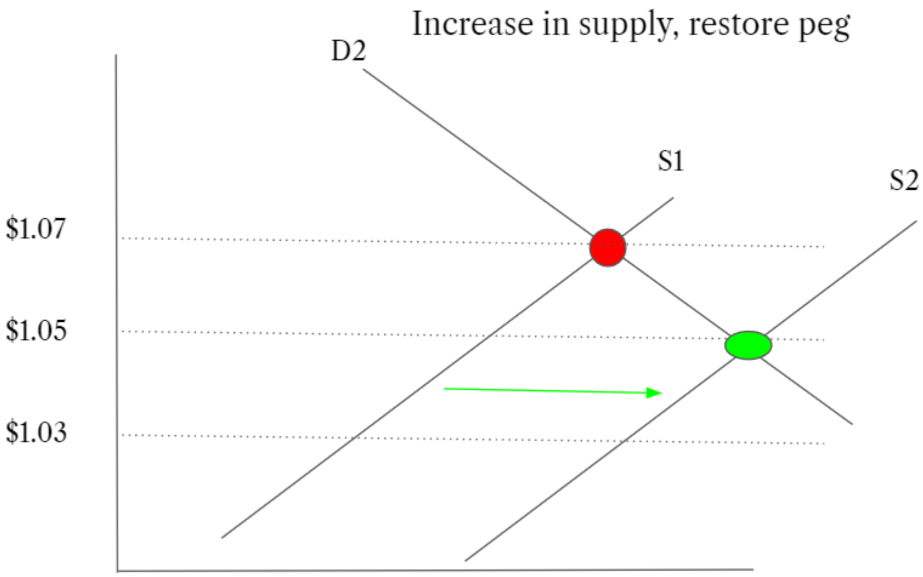
First, assume users have been purchasing Silk on a DEX such that the market price of Silk is greater than the target peg price as seen in the graphic below.



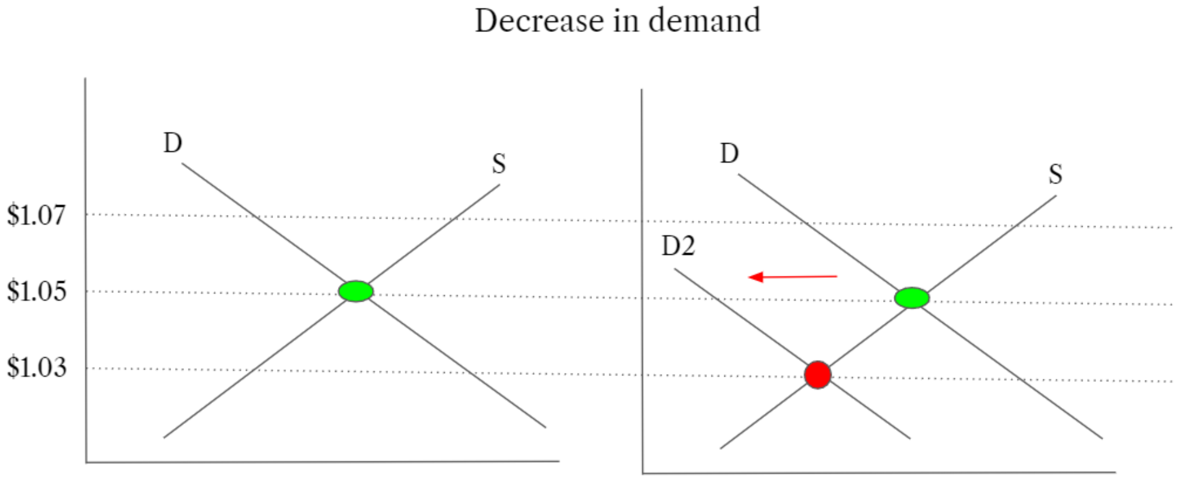
In order to bring Silk back to its target peg, there needs to be an expansion of the supply or a reduction in demand. The easiest way to achieve price parity is via expansion of supply which will be executed by a user due to the price disparity between the rate at which they can mint Silk compared to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



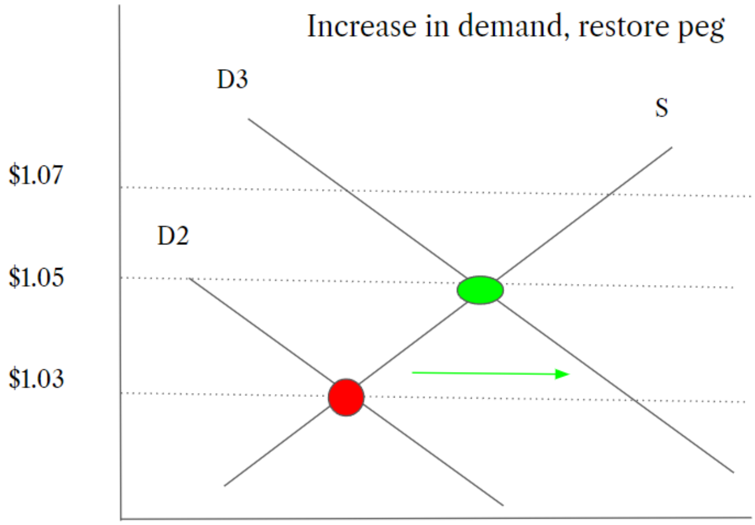
Once an arbitrage entity expands the supply and sells the Silk for arbitrage profit, the supply curve is restored back to equilibrium as seen in the graphic below.



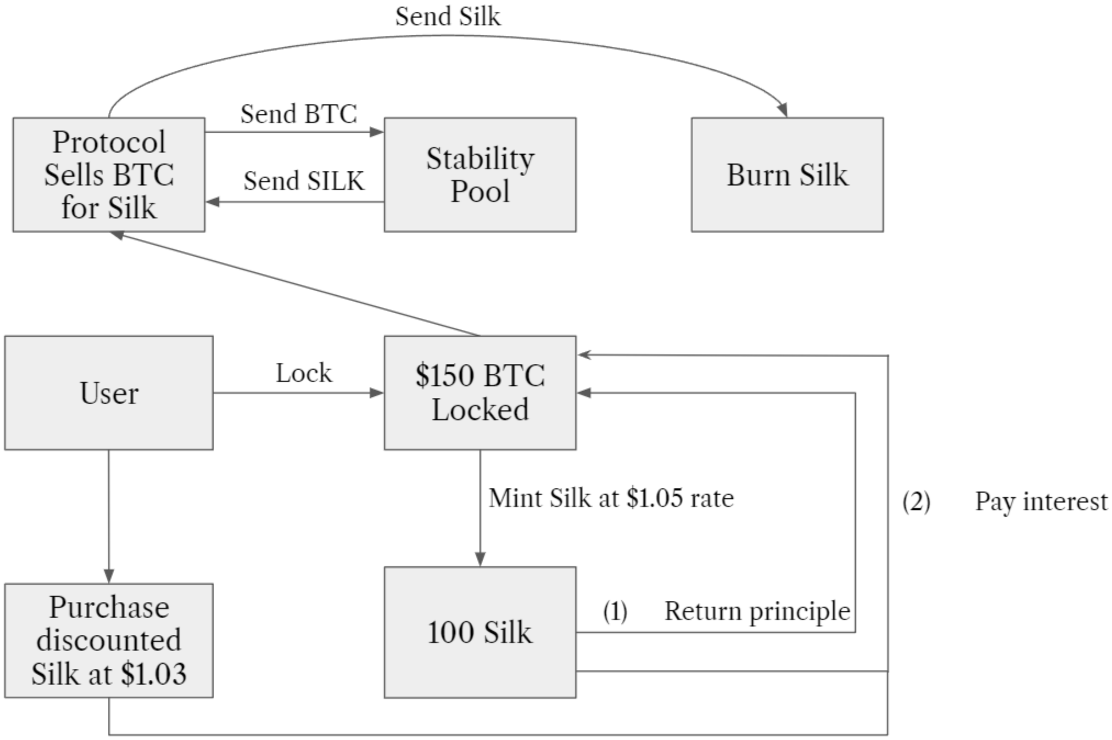
The next example is if Silk's market price decreases below its target peg due to a decrease in demand:



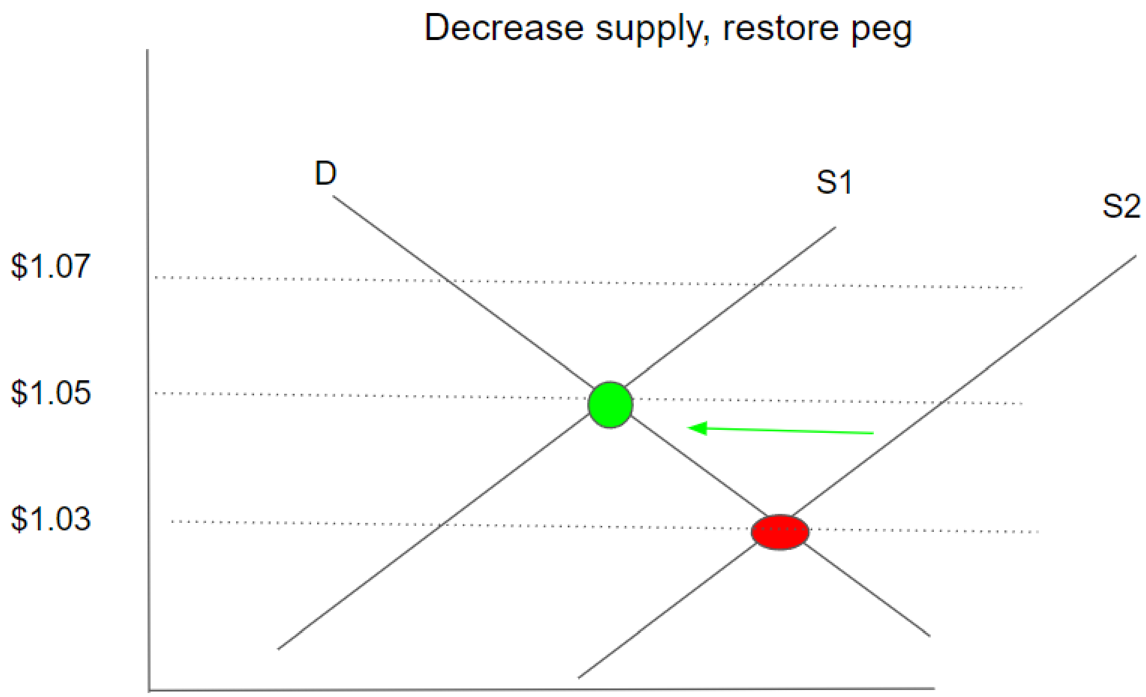
When Silk is below peg there are two solutions: increase the demand for Silk or reduce the circulating supply of Silk. Increasing demand for Silk is generated by the fact that users are able to purchase Silk at a discounted rate to pay back their loan interest payments to the protocol at a discount.



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 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).*[12] 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 Bounded Minting 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

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

redemption pool. **The more LAR that exists from the redemption pool, the greater the fees to either mint or redeem from the redemption pools**. Additionally, 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 Bounded Minting & overcollateralized stability mechanisms, the 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[13]. 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.[14] Importantly, volatility makes prediction of future values uncertain - creating a deterrent for investment and trade that negatively impacts wealth generation and

[13] *Exchange rate volatility and trade flows*. International Monetary Fund. (n.d.). From https://www.imf.org/external/np/res/exrate/2004/eng/051904.htm.

[14] 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.

economic activity[15]. 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 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)[16]:

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%

[15] *Global currency stabilization - WOCU*. (n.d.).http://www.wocu.com/upload/20726.pdf.

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

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%
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

Risk 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. 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.

Compliance Intent

Shade Protocol aims to instantiate and be compliant as it pertains to the following variables:

- KYC/AML/Cybercrime
- Tax Compliance
- Safety, efficiency, and integrity of the payment system
- Data privacy, protection and portability
- Sound governance
- Market integrity

- Auditability and compliance via permit key structure on Secret Network
    - Entities can decrypt their transactions and data

Shade Protocol development aims to create all of the necessary tooling to be future proofed in its compliance stance to the best of its ability. The following variables and code is capable of being modified by Shade Protocol governance over the long haul:

- Silk Issuance Policy
- Degree of privacy tied to Silk transactions
- Viewing key parameters
- Escrow parameters
- Composition of the Silk basket
    - Add assets
    - Remove assets
- Size of the weights within the Silk basket
- Oracle frequency
- Silk minting parameters
- Total mintable Silk

Stability Intent

Stability of Silk targets a collateralization ratio of Silk between 100 - 150% via Silk minting vault parameters.

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

[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.

    - 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 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 potential path to compliance within the existing international cryptocurrency and financial regulatory frameworks.

ShadeDAO: A Privacy-Preserving Decentralized Asset Management DAO For Shade

Sutera Duniya
shadeprotocol.io

Abstract. Shade Protocol, an array of connected privacy-preserving DeFi applications, are unified under a single governance and utility token called "Shade". The Shade token helps govern the ShadeDAO - a decentralized autonomous organization and treasury that has a range of asset accrual and distribution mechanisms.

ShadeDAO

The ShadeDAO is a decentralized balance sheet of assets controlled by Shade Protocol governance to help stabilize Silk while generating sustainable yield for SHD stakers. The ShadeDAO grows as a result of the following value accrual mechanisms:

- Silk transactions
- SHD transactions
- Silk/SHD entry minting collateral
- SHD bond collateral accrual
- SCRT staking derivative transactions
- SHD staking derivative transactions
- SCRT staking derivative revenue
- SHD staking derivative revenue
- Stabilizer token airdrops
- Silk synthetic entry minting deposits
- ShadeDAO L1 staking (SCRT, ATOM, LUNA) revenue
- ShadeDAO LP revenue
- Future SHD primitives revenue

This balance sheet of assets and revenue accrued are controlled by Shade governance. The ShadeDAO balance sheet could look something like the following:

Token	Amount	Value
sSCRT	2,300,000	$6,900,000
sETH	800	$1,600,000
Shade	150,000	$6,000,000
Silk	4,500,000	$4,500,000
USDT	500,000	$500,000
Total Value	N/A	~$55,000,000

Crypto-assets that are under control of the ShadeDAO balance sheet are considered “Locked” or “Unlocked”. Assets are locked by default until overridden by a Shade governance vote. This is to ensure that accumulation stages for the various pools of assets are encouraged.

Mechanics

The ShadeDAO secret contract has a variety of whitelisted contract addresses that can be interacted with via a Shade governance vote. The ability to interact with new addresses involves two governance steps:

1. Whitelist an address
2. Send X amount of crypto-asset to whitelisted address

The following is an example of what the whitelisted contract addresses could entail:

Action	**Contract Address**[18]
Liquidity Provide sSCRT X Silk	secret1grn3ob5cc6zhvyozmkldstzkyfhgycfhpdjom
Sell S-Tesla for Silk	secret1bll3ot7cx6zxvyozsdmrstzkyfhxxcfhheyuitv
Add Shade to LP Rewards Pool	secret1jer9zb3tn5uhuuknmzzlstzkygyycfhpfrdlzkr
Convert sSCRT to SCRT	secret15l9cqgz5uezgydrglaak5ahfac69kmx2qpd6xt
Distribute Silk Rewards for Participants	secret1del8ot2cx2zvlyozsdtodtzkyfhxxcfhheyuom
Stake SCRT	secret15l9cqgz5uezgydrglaak5ahfac69kmx2qpd6xt

As a general principle, the ShadeDAO is intended to take a capital conservation approach. Hardcoded into the ShadeDAO is that no more than 20% of a given asset pool can be sent during a single transaction. While multiple transactions could be voted upon that would ultimately empty a pool of assets from the ShadeDAO, this hardcoded restriction ensures due diligence from Shade governance token holders by introducing intentional friction into the spending process.

Added functionality for the ShadeDAO can be extended by simply creating new contracts that handle or execute the intended functionality for assets on the ShadeDAO. Upon creation and testing of the contracts, Shade governance can simply add the new contract address to the ShadeDAO whitelist of approved addresses for future interactions.

[18] Fictional addresses.

Shade Rewards mechanism

SHD provides the economic incentives which will be distributed to encourage users to exert efforts towards contribution and participation in the ecosystem on Shade Protocol, thereby creating a mutually beneficial system where every participant is fairly compensated for its efforts. SHD is an integral and indispensable part of Shade Protocol, because without SHD, there would be no incentive for users to expend resources to participate in activities or provide services for the benefit of the entire ecosystem on Shade Protocol. Given that additional SHD will be awarded to a user based only on its actual usage, activity and efforts made on Shade Protocol and/or proportionate to the frequency and volume of transactions, users of Shade Protocol and/or holders of SHD which do not actively participate will not receive any SHD incentives.

In order to provide the pool of assets supporting the privacy layer for Shade applications, users would be required to stake their assets into a pool that helps provide liquidity for the underlying apps. This contract has a 21 day “unbonding” period - following the greater Cosmos blockchain ecosystem standard. Users would be rewarded with SHD incentives and other rewards. The Shade rewards contract would calculate each user's contribution to the protocol based on a pre-determined formula.

It is the community members who ultimately maintain and drive development of Shade Protocol. Therefore, SHD incentives would need to be distributed to promote enthusiasm for community governance, increase community activity, and compensate them for their time, expertise, and effort. Only users who have participated in submission of proposals, commenting, reviewing, and/or voting will be entitled to receive governance rewards in SHD.

SHD does not in any way represent any shareholding, participation, right, title, or interest in the Company, the Distributor, their respective affiliates, or any other company, enterprise or undertaking. Nor will SHD entitle token holders to any promise of fees, dividends, revenue, profits or investment returns, and are not intended to constitute securities in Singapore or any relevant jurisdiction. SHD may only be utilized on Shade Protocol, and ownership of SHD carries no rights, express or implied, other than the right to use SHD as a means to enable usage of and interactions within Shade Protocol. The secondary market pricing of SHD is not dependent on the effort of the Shade team, and there is no token functionality or scheme designed to control or manipulate such secondary pricing.

Conclusion

ShadeDAO is a privacy-preserving decentralized asset management protocol built on Secret Network and governed by Shade - which empowers Shade holders to directly use a balance sheet of crypto-assets created from the various decentralized revenue streams directed to the ShadeDAO (introduced into all Shade primitives). The ShadeDAO directly empowers users to impact the protocol by increasing the stability and liquidity of underlying apps. The ShadeDAO is the world’s first privacy-preserving decentralized balance sheet - an experiment that is breathtaking in scope, and trailblazing for privacy and DeFi.

References

[1] Silk: A Privacy-Preserving Algorithmic Burn Stablecoin [Whitepaper]

[2] Shade Synthetics: A Privacy-Preserving Synthetic Assets Protocol [Whitepaper]

[3] Shade Protocol: An Array of Connected Privacy-Preserving DeFi Applications

shade

Shade Protocol: Comprehensive Governance & Ethics

Sutera Duniyal, Mizan Cloud, C. Brandt
shadeprotocol.io

Abstract. Governance models in DeFi have struggled to optimize for flexibility of economic reactivity and growth in relation to total democratic approaches. Fluid governance that optimizes for the speed of management and implementation of change within a DAO while simultaneously having end accountability from baseline token ownership creates an optimal end state. Shade Protocol governance model is based on a variety of branches and representatives to empower the fluidity of Shade Protocol governance as it pertains to parameters, primitives, capital allocation, peg composition, protocol vision, accountability and transparency, and funding. Additionally, Shade Protocol governance is founded on an ethos of digital self-sovereignty - a set of guiding principles behind Shade Protocol governance.

The Ethos of Digital Self-Sovereignty

In the digital world, human beings occupy space with digital representations of their physical-world information. When viewed separately, these digital representations can be readily dismissed as merely random collections of digital assets. However, when examined as a whole, these same representations reveal themselves to be extensions of a person's digital self-sovereign identity. Moreover, as these two worlds, the digital and the physical, continue to merge into one space, this digital identity has become more commonly used as a primary means of validation and verification of a person's digital and physical existence. Therefore, the primary rights of ownership for this digital form of identity must be safeguarded and protected in the same manner, and with the same level of importance, as is typically observed with individual identity in the physical world. It is for this reason that the ethos of digital self-sovereignty is at the center of Shade Protocol governance for the community's consideration and adoption into the standard governance framework.

Primary Rights of Digital Self-Sovereignty

The Right to Digital Privacy

Digital privacy means that people are the sole owners of their own digital property and they inherently possess immutable authority over the use of that property. As owners, they have full right of control over the "why", "when", "where", and "how" their digital assets are accessed. Digital privacy also involves an individual's ability to maintain control of their digital property when interacting with any entity, system, or organization within a digital environment. Therefore, with every and any form of digital interaction, every person should have the expectation of privacy.

The Right to Digital Independence

Digital independence is the ability for individuals to interact freely with any entity, system, or organizations within the digital space. Centralized control of digital interactions is in direct conflict with the idea of digital independence. Within decentralized environments, there is no intermediary entity to serve as a central authority over the authenticity of digital relationships. Therefore, systematic decentralization must be promoted, propagated, and implemented throughout the digital world to ensure that the right to digital independence is fully available to every individual.

The Right to Digital Transparency

Digital transparency is the application of open, honest, and fair relationships between individuals, entities, systems, and/or organizations within a digital space. One can argue that transparency is required to secure trust between different parties in a digital-based relationship. However, a truly transparent digital relationship can actually eliminate the need for trust between parties; since each individual has the ability to confirm the validity of all interactions because all information about the shared relationship is openly available to all parties involved in the relationship.

The Right to Global Financial Access

Shade Protocol was created to empower individuals all over the world by giving them direct access to financial instruments, tools and currencies that respect their right to privacy. Shade Protocol empowers financial sovereignty and freedom by giving users around the world permissionless access to decentralized finance regardless of their financial or socioeconomic status. If you have an internet connection and a crypto-wallet attached to Secret Network, then Shade Protocol and its financial primitives are openly available for you to use.

Comprehensive Governance Structure

Shade Protocol governance consists of three components: voting representatives, foundational governance, and branches. Voting representatives are defined as wallet addresses that are able to vote for those who have “delegated" SHD votes to the respective wallet address. Foundational governance is defined as a SHD tokenholder voting structure. Branches are defined as a set of X multisigs consisting of Y entities that are focused on controlling and optimizing Z components of Shade Protocol. Foundational governance directly empowers the branch multisigs with a set of annual periodic elections that vote on which entities and individuals will be represented within the respective branch multisigs.

SHD would allow holders to propose and vote on governance proposals to determine future features and/or parameters of Shade Protocol, with voting weight calculated in proportion to the tokens staked (the right to vote is restricted solely to voting on features of Shade Protocol; it does not entitle SHD holders to vote on the operation and management of the core contributors, its affiliates, or their assets, or the disposition of such assets to token holders, or select the board of directors of these entities, or determine the development direction of these entities, nor does SHD constitute any equity interest in any of these entities or any collective investment scheme; the arrangement is not intended to be any form of joint venture or partnership). If Shade governance wishes to create a non-profit entity to help manage key components of the DAO, this would be encouraged.

Voting Representatives

Voting representatives are wallet addresses that SHD token stakers can optionally delegate their votes to - this addresses the problem of average users not typically participating in governance. Voting representatives initially have no economic incentive - it will be up to Shade governance to decide if individuals operating as representatives should be economically incentivized. Upstanding and valuable community members will naturally want to partake in governance as a public good, and as a voting representative they will be able to serve the protocol to earn rewards by participating in governance for both delegators and themselves simultaneously. Any wallet can be a voting representative, although it is generally advised that branch participants should not simultaneously be voting representatives. The exception to this rule are members of the community branch participants, outlined further below.

Branches

Shade Protocol governance consists of the following branches: primitives, treasury management, grants, Silk, human DAO, community, and protocol sustainability - with the ability for governance holders to create or remove branches as necessary. Each of these branches are entitled to the management of a set of parameters, actions, or capital in order to optimize for an end outcome. The following are descriptions of the branches:

- **Primitives Branch (PB)** - manages core SHD primitives and application parameters. As Shade Protocol continues to launch applications that directly plug into the ShadeDAO, it will be the job of the PB to optimize primitive parameters with respect to application growth, ShadeDAO revenue generation, and end-user experience.
- **Treasury Management Branch (TMB)** - manages the issuance of bonds from the DAO, trades, liquidity provision, reserves ratio, etc. TMB optimizes for ShadeDAO growth as well as stability of the Silk peg.
- **Grants Branch (GB)** - manages the community pool of the ShadeDAO with the goal of the creation of as many key SHD primitives as possible that adhere to the core principles of Shade Protocol as outlined in the original Shade Protocol whitepaper.
- **Silk Branch (SB)** - focused on optimization of Silk's peg composition. Additionally, SB helps facilitate Silk peg migration, in addition to Silk adoption recommendations.
- **HumanDAO Branch (HDAOB)** - aims to bootstrap legal entities and individuals that are funded by the ShadeDAO to maximize the growth of Shade Protocol as it pertains to education, marketing, listings, community engagement, community growth, events, documentation, development, hackathons, and any other conceivable component of a protocol that pertains to human capital.

- **Community Branch (CB)** - aims to raise community level concerns to all of the respective branches, and help facilitate dialogue and transparency between the community and the respective branches.
- **Protocol Sustainability Branch (PSB)** - aims to promote sustainable decision making for the long term adoption and success of both Silk and Shade Protocol applications. SB is also responsible for Shade Protocol governance process management and the creation of best practices for governance. It is tightly partnered with the CB and responsible for coordinating cross-branch decision making.

Branch wallets are elected via general elections from SHD stakers. All of the respective branches are multisig wallets that start as a standard set of 7 wallets. Shade governance has the ability to expand the number of entities that partake in each of the multisigs as well as create new branches. Shade governance should be careful to balance the decentralization of the branches with the ability of the multisigs to maneuver with flexibility in favor of the protocol.

Sanity Checks

To defend against rapid decision making from multisigs that may not be representative of the larger token governance holders, Shade Protocol introduces “sanity check” proposals that resolve within 24 hours and require a greater than 50% approval with a 7.5% quorum so that the execution request from the respective branch can be performed. Sanity checks help defend against malicious multisig activity, while still empowering end token holders to have a direct voice in the daily activities of the various Shade Protocol governance branches. Sanity checks also help with the legal risk of centralization accusations attached to any given multisig, as ultimately, SHD tokenholders would govern features/parameters of the protocol (i.e. branch multisigs as well as approval of daily activities of the respective branches). Finally, sanity checks provide an on-chain archive of multisig activity and decision making - bringing a degree of transparency and methodology to Shade Protocol governance that is conducive to healthy and consistent decision making.

Primitives Branch

The Primitives Branch (PB) manages core SHD primitives and application parameters. As Shade Protocol continues to launch applications that directly plug into the SHD DAO, it will be the job of the PB to optimize primitive parameters in relation to growth of the respective applications, revenue generation to the Shade Protocol DAO, and end-user experience. The most important variable that core Shade primitives have is the “primitive fee rate” (PFR) which dictates the percentage of profit generated from a given primitive to the DAO. An example of this is a DEX fee rate. A 5% fee rate may be optimal for the DAO, but not for the user growth of the DEX. Or for synthetics, conversion minting fees can optimize DAO growth at the expense of stabilizer token holders. Enforced Silk transaction fees might generate revenue for the DAO, but damage usability. All of these types of primitive variables will be controlled directly by the PB which is responsible for updating, maintaining, and managing the long term growth of the Shade Protocol primitives.

Treasury Management Branch

TMB optimizes for consistent ShadeDAO growth as well as stability of the Silk peg. Bond issuance needs to be flexibly managed in order to maximize treasury growth. The primary objective of bond issuance and TMB is to maximize the number of uncorrelated assets that are held by the Shade DAO. Preferably, these are yield-bearing assets (such as layer-1 tokens or liquidity pool tokens) to stabilize Silk. The TMB should be considered an economic council that exists as a neutral entity to execute macro policy directives for token holders, specifically in confluence with the Protocol Sustainability Branch (PSB). The TMB operates with a significant amount of operational independence and should be elected on the basis of historical economic merit and experience.

Grants Branch

The Grants Branch (GB) manages the community pool of the ShadeDAO with the goal of the creation of as many key SHD primitives as possible that adhere to the core principles of Shade Protocol as outlined in the original whitepaper. The GB should push for primitives that will be controlled in part (or entirely) by the ShadeDAO (specifically via the Primitives Branch). The Grants branch should be heavily focused on aggressively funding the earliest primitives of Shade Protocol. Grants will be structured around milestone based completion and the approximate number of development hours.

Silk Branch

The Silk Branch is devoted towards the maintenance and optimization of Silk. This branch is heavily focused on research surrounding the creation of the optimal set of weights as well as update frequencies and peg composition (commodities, cryptocurrencies, currencies, etc.). The Silk Branch also exists to increase the adoption of Silk as much as possible - helping promote, create, and facilitate Silk integrations with other Web3 applications. Silk Branch can also initiate an update of the Silk peg at any given moment. Initially, quarterly intervals are recommended.

Principle: whatever set of weights and currencies/assets (must be available via oracles) maximally reduces the volatility of Silk in relation to other global currencies should be used.

HumanDAO Branch

The HumanDAO Branch aims to bootstrap legal entities and individuals that are funded by the ShadeDAO to maximize the growth of Shade Protocol as it pertains to education, marketing, listings, community engagement, community growth, events, documentation, development, hackathons, and any conceivable component of a protocol that pertains to long term human capital. The HumanDAO should be focused on creating sustainable and optimal set-ups that motivate individuals to build and help Shade Protocol succeed. The HumanDAO should be focused on long term engagements, with off-chain entities (such as a Shade Research Foundation) to help create, run, and maintain accountability for any entities that are to be hired by the HumanDAO. It is highly recommended that three legal entities are created off-chain (funded via the HumanDAO) - the Shade Research Foundation, the Shade Institute of Art, as well as the Shade DAO Institute. The Shade Research Foundation should be focused on the enhancement of existing or yet to be created Shade primitives. The Shade DAO Institute is focused on maintaining the accounting of any off-chain expenses for Shade Protocol separate from research and art. The HumanDAO Branch is funded directly by the Grants Branch. It is advised for these off-chain institutions and foundations to function as non-profits whenever possible, even in suboptimal conditions.

The Shade Art Institute will exist to promote human expression via art, dance, poetry, and all other forms of creative structure. Specifically, the Shade Art Institute is focused on expressions of privacy, sovereignty, decentralization, and freedom. In the world of the digital, and amidst a rapidly evolving community of cryptocurrency, it can be easy to forget the importance of the arts and humanities within the role of both prediction and reflection. While funding from the Grants Branch for this kind of institution may not be immediate, we hope that this institute will one day be created and supported, so as to remind the larger Shade Protocol community that their impact should be based on more than just the size of the ShadeDAO or the amount of Silk minted. It should also be based on the desire to reach the hearts and minds of everyday people around the world via the creative arts.

Community Branch

The Community Branch (CB) aims to raise community level concerns to all of the respective branches, and help facilitate dialogue and transparency between the community and the respective branches. Community Branch individuals should be able to facilitate the interoperability of all the branches. While transparency of all conversations cannot be strictly enforced, philosophically this should be maintained by all branches to the best of their ability. The Community Branch can be thought of as an auditing entity where the primary goal is to provide SHD token holders with as much data as possible and the reasoning behind any given branch's decisions. The Community Branch has the unique ability to propose the addition or removal of individuals from any given branch. This is the only set of DAO functionality given to the Community Branch, providing a distinct check and balance on other branches.

Entities that make up the Community Branch are voted on by SHD tokenholders on a bi-annual basis initially. It is recommended that the time between elections of the Community Branch multisig be modified as needed after initial trial and error.

SigSwitch

SigSwitch is the mechanism that is needed for the Community Branch to use its ability to add or remove individuals from branches (separate from branch elections). SigSwitch is necessary in order to resolve inter branch conflicts, help adherence to strong community feedback and signal proposals, and to resolve individual or branch misconduct.

Misconduct is defined as the following:

- Refusal to provide transparency of conversations to the Community Branch

- Refusal to provide periodic updates and the justifications behind the policy strategies of any given branch or individual
- Malicious branch or individual decision making
- Inept branch or individual decision making
- Malicious or inept interpersonal conduct or communication

Before initiating a SigSwitch, the Community Branch should consult with the Protocol Sustainability Branch and acquire an off-chain consensus on the need to perform a SigSwitch. The PSB functionality only extends to initiation of formalized signal proposals, making it unlikely that a SigSwitch will need to occur on PSB since a corrupted PSB has no direct impact on the financials of the ShadeDAO (separate from their vote for the execution of a SigSwitch on a separate branch).

SigSwitch steps are formalized as follows:

(1) A SigSwitch is initiated by the Community Branch specifying the modification of an existing branch
    - Note that both the Community Branch and the proposed modified branch are unable to vote on the SigSwitch

(2) Individuals that vote on the SigSwitch are those that make up the remaining branches not impacted by the SigSwitch vote
    - Initially this is 35 votes (49 votes across all branches - 14 votes that are barred from participating between PSB and SigSwitch branch)
    - At least 33% of the 35 votes (11>) from the individual branches must vote yes to execute the SigSwitch

(3) Sanity check

(4) SigSwitch is executed depending on result of the sanity check

The SigSwitch vote does not involve the Community Branch or the branch that would be modified to maintain neutrality of the vote. In order to be biased towards the Community Branches proposition, only 33% of the individual branch votes need to be a “yes” in order to bring the vote to the sanity check stage. Decentralized governance is powerful, and because the Community Branch is essentially a community whistleblower/watchdog, SigSwitch is a powerful tool to ensure that multisig activity and membership are not purely gated by election cycles in case of emergencies.

Protocol Sustainability Branch

The Protocol Sustainability Branch (PSB) aims to promote sustainable decision making for the long term adoption and success of both Silk and Shade Protocol applications. The Protocol Sustainability Branch is also responsible for governance process management and creation of governance best practices. Additionally, the PSB is tightly partnered with the Community Branch and is responsible for coordinating cross-branch decision making. The PSB multisig functionality is purely devoted to the creation of signal proposals on Shade Protocol - bringing attention to token holders the opinion of PSB on any given practice or decision of the other branches in relation to the sustainability and growth of Shade Protocol.

Foundational Governance

Current Shade Protocol governance proposal parameters, which are subject to change, are as follows:

- Deposit period - 1 week
- Voting period - 1 week
- Minimum deposit amount - 50 SHD
- Quorum - 25%
- Threshold - 50%
- Veto - 33.4%

There are five stages to on-chain governance proposals on Shade Protocol: submission, deposits, voting, tallying, and implementation. Submission can be done by any user, with the caveat that nothing is broadcasted on-chain until a proposal reaches the minimum deposit amount This is in place to protect Shade Protocol from proposal spam. Anyone can contribute to the minimum deposit amount. If the proposal does not reach the minimum deposit threshold, deposits are refunded. If the proposal is approved or if the proposal is rejected but not vetoed, the deposits will automatically be refunded to the respective proposal depositors. It is critical to note that if a proposal is vetoed with a supermajority, then the deposits are forfeited. After reaching the minimum deposit required, a one week voting period begins. During this timeframe, bonded SHD holders are able to cast their vote with one of four options - yes, no, no with veto, and abstain. Only bonded tokens can participate in Shade Protocol governance; this encourages users to bond their tokens to the network, which is an essential part of securing the network. Voting power is measured in terms of bonded SHD tokens.

Delegators inherit the vote of the representative they are delegated to unless the delegator casts their own vote (which automatically overwrites the representative's voting decision). Tallying the results of a proposal vote can result in an accepted proposal if the following requirements are met: quorum, threshold, and no veto. The quorum requirement programmatically checks that more than 25% of total bonded tokens participated in the vote by the end of the one week voting period. The threshold requirement programmatically checks that more than 50% of tokens that participated in the vote, after exclusion of abstain votes, voted in favor of the proposal. The no veto requirement confirms that less than 33.4% of bonded tokens that participated in the vote, after exclusion of abstain votes, vetoed the proposal. Finally, the code the proposal wishes to modify is altered by developers of the network and implemented during the next "patch" of Shade Protocol secret contracts.

Foundational governance can propose changes to any modifiable parameter as well as perform any action that a branch has the ability to perform

Elections

Elections of multisig entities happen on a bi-annual basis. Multisig entities are voted on in sets, as opposed to individuals that are part of the multisig. The following is an example:

Choice 1: Bob, John, James
Choice 2: Bob, John, Jill
Choice 3: James, Johanne, and Greg

Set based voting simplifies the end-vote experience. With a starting set of 7 branches with 7 entities part of each branch, users would potentially need to vote 49 different times. Instead, users need to only vote 7 times, across a set of decisions. Front-ends hosted by the Shade DAO Institute and any respective Shade Protocol development teams should help assist with voting and education surrounding the entities on the respective ballots.

Conclusion

Shade Protocol governance uses branches to optimize for fluidity of DAO wealth and decision making management while still maintaining foundational governance accountability via periodic elections, sanity checks, representatives, and community branch participation. With this structure, Shade Protocol is designed to scale well beyond the initially imagined scope in reaction economic success and yet to be imagined branch responsibilities. Shade governance stands on principles of primary rights to digital sovereignty - empowering users from around the globe to have digital independence, digital privacy, transparency by choice, and financial access to Shade primitives.

Silk Pay: Secure Send/Receive Architecture

Sutera Duniya
shadeprotocol.io

Abstract. One of the key barriers of adoption for cryptocurrency transactions is the transfer of large amounts of capital between entities. Test transactions are a popular mechanism by which users check to make sure they are sending to the correct counterparty by sending a non-consequential amount of cryptocurrency to a target address. However, this does not create a true sender/receiver confirmation system as every “fresh” transaction can create a risk of destination error user input during the new send. Additionally, transactions on blockchains are traditionally completely transparent - exposing users’ privacy and transaction history.

Enter Silk Pay - a privacy-preserving payment application built on Secret Network that introduces a new sender and receiver confirmation architecture that empowers senders to escrow capital in a contract while awaiting intended counterparties to confirm the inbound transaction by interacting with the escrow contract. Using the send request and receive request architecture, Silk Pay ensures outbound capital both safely and consistently sent to the correct location, enabling peace of mind and usability for everyday users.

Silk Pay

Silk Pay is a simple payment application focused on the SNIP-20 token sending and receiving user experience on Secret Network. The primary goal of Silk Pay is to bring Silk, the privacy-preserving stablecoin of Shade Protocol, to everyday end users. The initial implementation of Silk Pay is focused on a web experience, with future iterations to be built directly on mobile. Silk Pay is uniquely differentiated because it solves the jarring and risky “wire-transfer” paradigm of the majority of Web3 user-to-user transactions. Silk Pay solves this by giving users a varying degrees of sending and receiving options:

- Send Request
- Receive Request
- Direct Transfer

Direct Transfer (DT) is the traditional method of sending funds using the traditional wire-transfer architecture. With *DT*, users specify X amount of funds to be sent to Y address. Upon execution of the transaction, if the destination address is incorrect or improperly input, there is no recourse. Note that there is no transaction confirmation from the counter-party prior to funds being sent with the *DT* architecture. All double-checking has to be done in advance of the transaction - introducing risks as each send transaction user interaction carries its own set of risks for potential mis-step. To date, *DT* is the standard means by which users send funds.

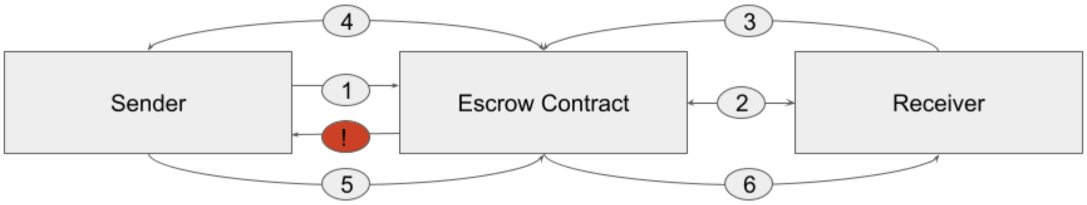
This is what the **send request** and **receive request** architecture is created to solve. Using escrow contract architecture, users can privately send X amount of funds to an encrypted destination address using a multistep process that involves confirmation interactions between both the sender, receiver, and escrow contract. As such, this architecture ensures that senders only ever send funds to correct addresses that are confirmed but the intended counterparty. Additionally, request infrastructure allows users the flexibility to privately request funds from other users. Eventually, Silk Pay will also include a system of monikers and registered addresses to make the initiation of a send or receive request even easier. While vetted addresses can remove the need for *send request* methodology (as send request is essentially a destination verification system), there will always be the need for *send request* architecture for first time transactions. With the incorporation of monikers and registered addresses, *receive requests* become an even more seamless UI/UX experience.

Send Request

Send Request (SR) architecture is a six part process (2 parts for sender, 1 part for receiver, 3 parts contract) that ensures the safe arrival of funds to intended destinations via a system of confirmations between the sender, receiver, and escrow contract. With the *SR* model, senders await confirmation from an escrow contract that interacts with the intended destination address.

Traditional Web2 payment request models involve users requesting a certain amount of funds from a counterparty, which the counterparty has the option to confirm. *SR* flips the traditional request model by instead having the sender initiate a “send ask” before funds are sent. A *send ask* is viewable by the potential counterparty, who can then create an inbound confirmation that is viewable by the sender. Upon seeing the inbound confirmation, the sender is guaranteed that the target destination address has been properly targeted, allowing the sender to safely perform an *execute send*.

Send Request



1 User sends funds and intended destination address to escrow contract - creating a **send ask**

2 Receiver queries escrow contract for **send ask**, confirming there is an inbound transaction

3 Receiver creates an **inbound confirmation** for the escrow contract in response to the **send ask**

4 Sender queries escrow contract checking for a corresponding **inbound confirmation**

5 Sender creates **execute send** command for the escrow contract after receiving **inbound confirmation**

6 Escrow contract sends X funds to the receiver

! Sender can retract funds at will

SR User Story

- Bob creates a *send ask*, which is first staged in the *escrow contract*
  - 100 SCRT
  - secret1zfk9yoptw7nlnwc4r66d84rgc3cqpd7hynczgq as the address he believes to be Alice
- Alice queries the escrow contract, expecting a *send ask* for 100 SCRT
- Alice does not see a *send ask*, and let's Bob know asynchronously
- Bob **retracts funds from the escrow contract** and destroys the original *send ask*
- Bob sends another *send ask* to the escrow contract, realizing the address was wrong
  - 100 SCRT
  - secret1zfkzyzptw7nlnwc4r66d84rgc3cqpd7hynczgq as the new address he believes to be Alice's
- Alice queries the escrow contract, and sees the incoming *send ask*
- Alice creates an "inbound confirmation" that gets sent to the escrow contract
  - Alice can send an asynchronous message to Bob that *send ask* was received
- Bob queries the escrow contract, and sees the *inbound confirmation* for his potential transaction
- Bob performs the *execute send*, funds are sent to Alice

SR Risks

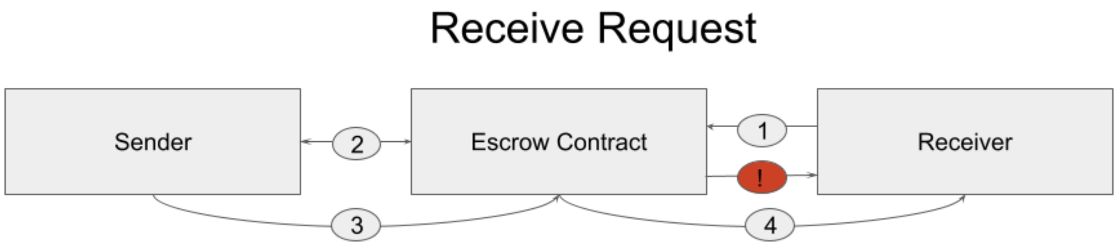
There is a potential risk that Bob potentially uses an address of another user who is not Alice, and that the malicious user would create an *inbound confirmation* for the escrow contract in hopes that Bob would perform an *execute send* after seeing the *inbound confirmation*. There are two safeguards against this:

- Possible addresses on Secret Network are 2^160 = 1461501637330902918203684832716283019655932542976 = 1.4615e+48. The odds that you accidentally put an address in that has an existing counterparty that is prepared to send an inbound confirmation message has less likelihood than a user accidentally sending to the wrong person on Venmo or PayPal by an order of magnitude.
- Due to Silk Pay being focused on A to B intermediary, it is highly unlikely that a Send Request is sent to a counterparty that does not have some form of asynchronous communication coordinating on the sending and receiving. That is to say, it will be highly obvious when a send-ask has not been received, with responsibility ultimately resting squarely on the sender for the final execution of the *execute send*.

In order to give senders maximum amount of flexibility, Senders will have the ability to perform an *execute send* prior to receiving an inbound confirmation from the receiver. Note that this will be highly discouraged within a UI/UX experience, but ultimately will be up to the user.

Receive Request

In addition to SR, there is also the **Receive Request** (RR) architecture which many users are already familiar with in Web2 that mirrors the traditional payment request operations.



1. Receiver creates a **receive ask** with the sender address and request fund amount to escrow contract
2. Sender queries escrow contract for **receive ask**, confirming there is an outbound transaction request
3. Sender creates **execute send** command for the escrow contract after receiving **receive ask**
4. Escrow contract sends X funds to the receiver

❗ Receiver can retract request at will

RR User Story

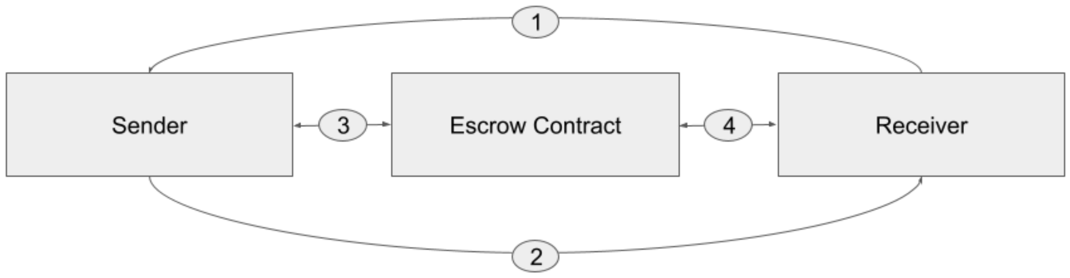
- Bob creates a *receive ask*, which is first staged in the escrow contract
    - Origin address
    - 100 SCRT
    - secret1zfk9yoptw7nlnwc4r66d84rgc3cqpd7hynczgq as the address he believes to be Alice
- Alice queries the escrow contract and sees the *receive ask* for 100 SCRT as well as which address created the *receive ask*
    - Alice can asynchronously check with Bob that he is the owner of the address and that he made the request
- Alice performs an *execute send* on the *receive request*
- Bob receives his requested funds from Alice

If Alice let's Bob know that she did not get the *receive ask*, Bob can retract the *receive ask* that was originally created by him. One of the risks of the Receive Request architecture is users could spam popular addresses requesting funds. Recourse for this behavior is spam filtering on the front-end where users will only see *receive asks* from addresses they have already registered on the escrow contract as "contacts".

S/R High Level

The end result of Send/Receive architecture is a simplified experience that empowers users to safely send funds to new counterparties in a controllable manner that is managed by an escrow privacy-preserving smart contract. Users will still have the flexibility to send funds "wire-transfer" style with Silk Pay, but this will generally be discouraged (unless an "address book" or "moniker" contact is used). Cryptocurrency transactions require both privacy, security, and usability. Silk Pay using this brand new Sender Request architecture will help bring Web3 comfortably to Web2 users.

Send/Receive High Level



1 Request Funds

2 Request Send

3 Check for **send requests** and **inbound confirmations**, perform **execute send**

4 Check for **send ask,** create **inbound confirmations** and **receive asks**

Silk Pay Fees

Silk Pay is a key primitive of Shade Protocol - empowering an entire suite of privacy-preserving DeFi applications. Direct transfer payments will not be charged any additional fees, as this is simply a "normal" transaction by blockchain definition. Whenever a SR or RR is generated or executed upon, a small additional flat rate gas fee will be generated and sent to the Shade Protocol treasury address - creating an additional revenue stream for Shade Protocol SHD stakers.

Conclusion

The next generation of payment applications must ensure users have a way to safely send to new addresses with large amounts of capital. Current architecture in blockchain is essentially a blind wire transfer with no recourse for mistakes. By leveraging Secret Network's privacy via secret contracts, Silk Pay provides a best in class experience that is currently unmatched by any other payment verification platform on Web3.

Shade Bonds

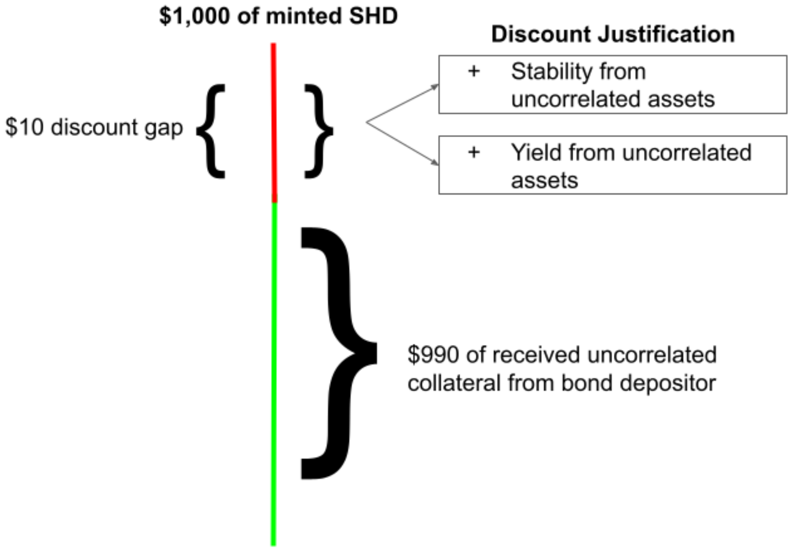
Sutera Duniya
shadeprotocol.io

Abstract. One of the most powerful bootstrap mechanisms available for DeFi protocols are Protocol Issued Bonds (PIB) which empower decentralized treasuries to ask for specific types of collateral at a specific price rate. In return for depositing collateral into the bond, the depositor receives freshly minted governance tokens from the protocol at a slightly discounted rate from the market price. Users receive their tokens after x number of days (blocks) that can then be freely used on the market. Arbitrage between the discounted rate and the market rate encourages users to interact with the bonds, and in return the treasury is able to bootstrap itself with uncorrelated assets in a sustainable manner.

Shade Bonds function similarly to other traditional DeFi bonds, with the distinct difference that users can purchase bonds in a privacy-preserving way as a result of the encryption attributes powered by secret contracts on Secret Network. Additionally, Shade bond issuance is managed via Shade Protocol governance and branches - empowering SHD tokenholders over time to determine the rate of issuance as well as the types of collateral gathered on the Shade Protocol treasury.

Shade Bonds

Shade Bonds are collaterally backed issuance of SHD minted via the treasury. The only non-collaterally backed component of Shade Bonds is the gap between the discount rate and the market price of SHD. While this could be perceived as an inflationary mechanic, the increase in the strength of the Silk peg from the uncorrelated assets as well as the yield bearing capabilities of the incoming collateral received by the Shade treasury increases the fundamental value of SHD at a rate that approximates (if not exceeds) the discount to market rate - making this sort of mechanic justifiable as long as liquidity shocks are accounted for.


$1,000 of minted SHD
Discount Justification
$10 discount gap
+ Stability from uncorrelated assets
+ Yield from uncorrelated assets
$990 of received uncorrelated collateral from bond depositor

.

With Shade Bonds, users deposit the desired amount of tokens into the bond contract and receive their SHD tokens (at a rate targeting a discount to market price) upon claiming after x number of days/blocks. Arbitrage between the discounted rate and the market rate encourages users to interact with the bonds, and in return the treasury is able to bootstrap itself with uncorrelated assets in a sustainable manner.

Example:

- User deposit $990 worth of sSCRT/SHD LP tokens into the bond contract
    - $1,000 worth of SHD at $10 is minted (100 SHD) and locked inside the bond contract
    - Timer begins
- User waits 5 days
- User unlocks their 100 SHD from the bond contract
- SHD is still trading at $10, user sells their 100 SHD
    - User earns a $10 profit ($1,000 sell value - $990 value of initial collateral deposited)

Users' optimal outcome is that the price of SHD remains the same or increases while they wait to claim their bond. In the future, bond issuance could use other uncorrelated assets from the treasury to rebalance and modify the existing portfolio composition of the ShadeDAO.

Unbounded Bonds

Shade Bonds are advantageous for issuance when the treasury value of SHD is less than the market value of SHD. Treasury value of SHD is the hypothetical floor value of SHD since SHD token holders have a claim to revenue streams and collateral that exists on the ShadeDAO.[19]

$$Treasury\ Value\ =\ (\#\ of\ SHD\ in\ circulation\ /\ \Sigma\ of\ all\ the\ value\ of\ the\ uncorrelated\ assets\ on\ treasury)$$

Whenever the market price of SHD is greater than the treasury value of SHD, there is an opportunity to sell SHD to the open market at a rate that is advantageous for the ShadeDAO (and by extension the protocol).

$$(Treasury\ Value\ <\ Market\ Value)\ -{>}\ Issue\ Bonds$$

$$(Treasury\ Value\ >\ Market\ Value)\ -{>}\ Buyback\ SHD$$

$$(Treasury\ Value\ =\ Market\ Value)\ -{>}\ No\ operations$$

Due to the nature of the relationship between the treasury value of SHD and the market value of SHD, there will be a range of opportunities that emerge that must be managed by the branch of Shade governance responsible for issuing bonds. Within this set of equations, bonds are “unbounded” as there is no reason for the protocol to limit itself into perpetuity with its ability to acquire uncorrelated assets from the open market within favorable conditions as outlined above. Therein, the most important consideration is the *rate of issuance* of SHD resulting from bonds. The greater the rate of issuance, the greater the potential liquidity shocks that could result from

[19] Note that the term “ShadeDAO” is interchangeable with the term “Shade Treasury”

bond arbitrage and speculators. Thus, issuance of bonds is always a careful interplay between opportunity derived from the gap between market price and treasury price versus the risks of rapid issuance of SHD onto the market (even within the confines of what is considered favorable conditions).

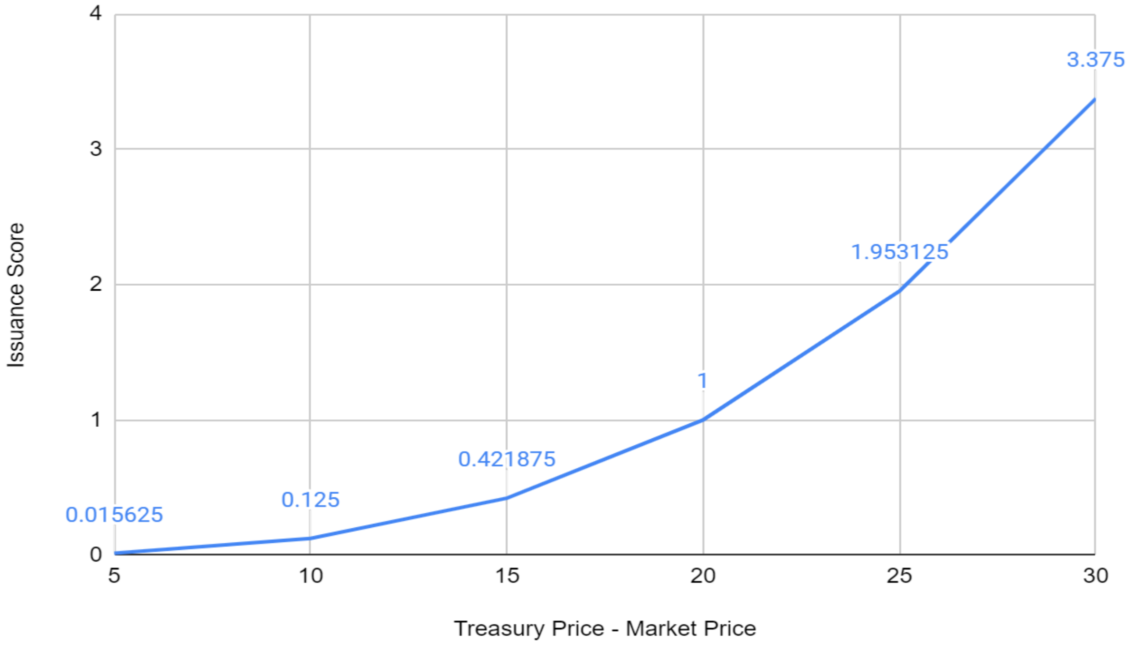
To create a value that is a signal for the significance of the opportunity to acquire assets at a favorable rate in relation to the treasury value of SHD, a price normalized cubic function is used to generated the *issuance opportunity score (IOS).* Due to the nature of being a cubic function, the greater the discount, the greater the exacerbation of the available opportunity for the bond issuance.

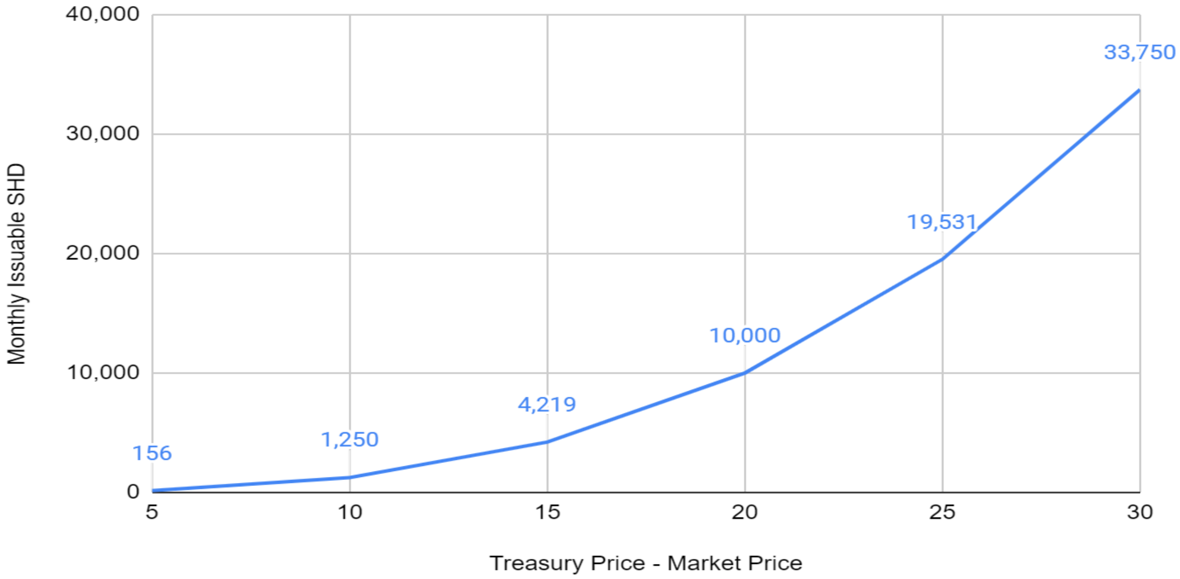
$$\beta = Treasury\,Value - Market\,Value$$
$$Opportunity\,Floor\,(\delta) = Normalization\,Value$$
$$Issuance\,Opportunity\,Score\,(IOS) = (\beta/\delta)^3$$
$$Monthly\,Available\,Issuance = IOS * ((Issuance\,Rate * Total\,SHD)/12)$$

A negative IOS would imply a SHD buyback opportunity from the treasury at a discounted rate in relation to the treasury value of SHD. The more buyback that occurs, the less SHD that will exist in active circulation, thus pushing market price back to a price point that is greater than or equal to the treasury value of SHD. Whenever the opportunity floor is greater than β, the rate of potential issuance is drastically throttled. This is to prevent aggressive issuance tied to opportunities that are not significant. Ultimately, governance will have control over this opportunity floor.

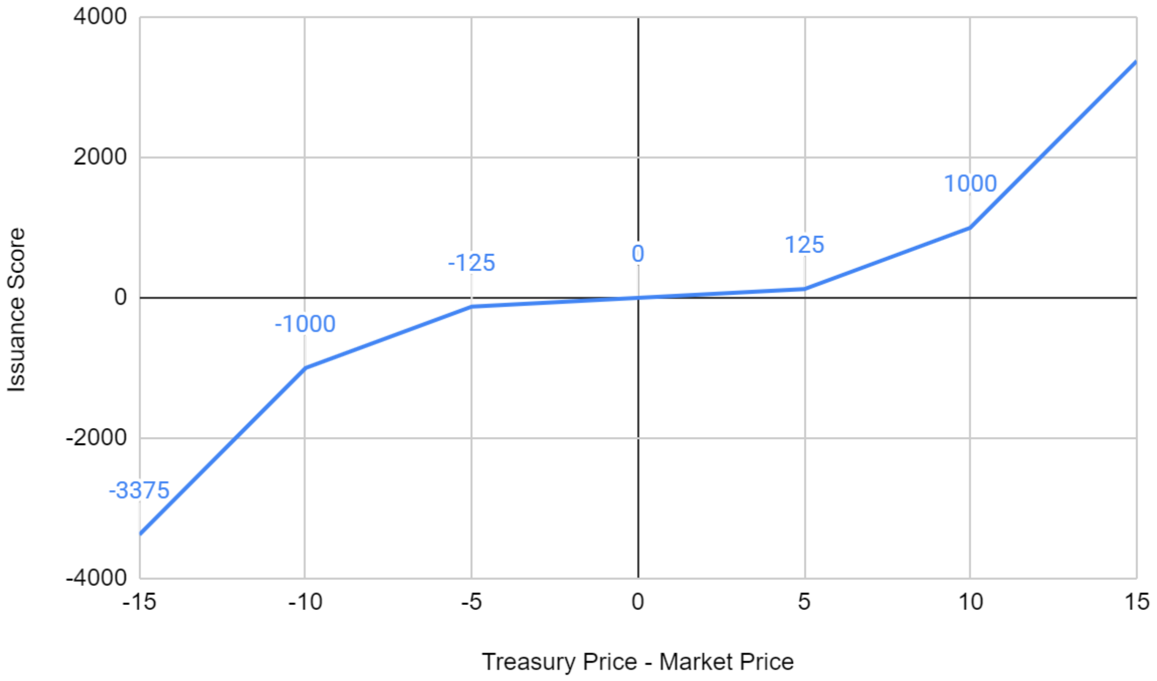
The smaller the opportunity floor, the smaller the required β is needed before the cubic function begins to influence the issuance opportunity. Due to the nature of the cubic function's impact on β, the greater the β, the more aggressive issuance is. Finally, the issuance rate is a percentage value that loosely determines what percentage of supply can be released in the form of bonds over the course of a year. Between the modification of the issuance rate and the opportunity floor governance from both tokenholders, the respective bond issuance branch should be able to finalize a bond issuance policy that is stable and sustainable while also remaining opportunistic to pricing disparities.

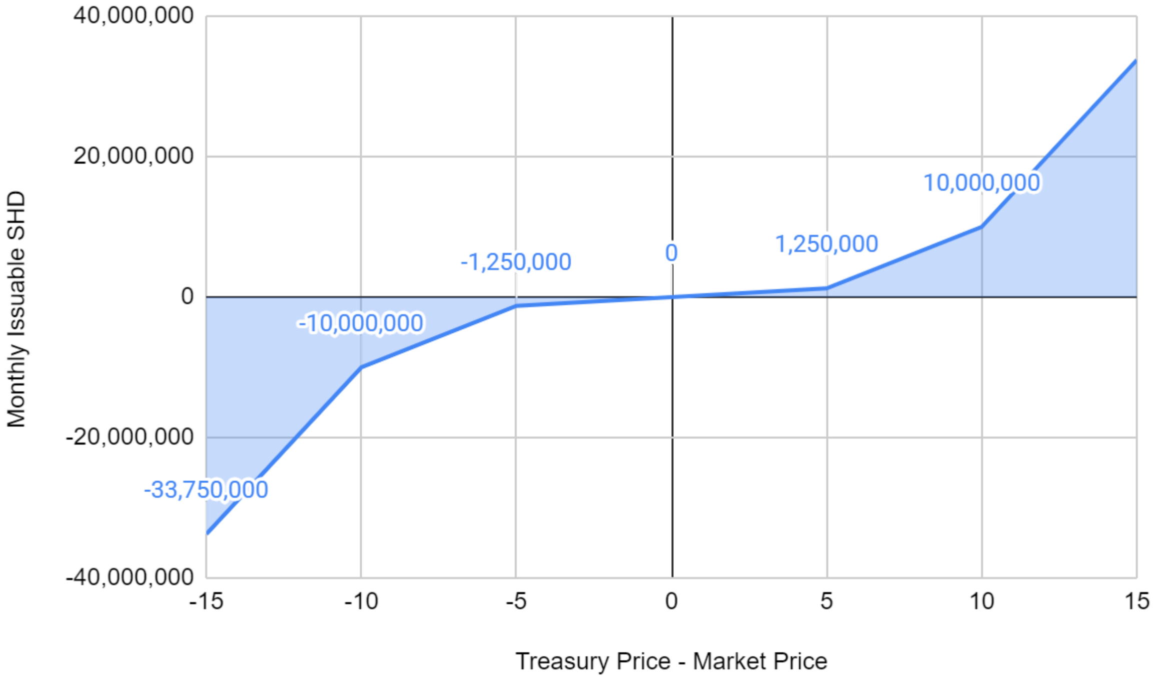
The following charts are examples of when the opportunity floor is set to $20 (bond issuance isn't drastically modified until β grows beyond $20) and where the monthly available issuance amounts to IOS * 10,000. Additionally, scenarios where β < 0 signals SHD buyback opportunities that should be performed by the ShadeDAO.


Issuance Score
4
3
2
1
0
5
10
15
20
25
30
Treasury Price - Market Price
0.015625
0.125
0.421875
1
1.953125
3.375


Monthly Issuable SHD
40,000
30,000
20,000
10,000
0
5
10
15
20
25
30
Treasury Price - Market Price
156
1,250
4,219
10,000
19,531
33,750

shade





Targeted Collateral

The role of uncorrelated assets pulled into the ShadeDAO via bonds fall into four categories of optimization: yield generating, stablecoins, scarce store of value, and liquidity tokens. *Yield*

Generating is any sort of collateral that is capable of generating yield *without experiencing the risks of impermanence loss*. Examples of *yield generating* assets are Layer-1 governance tokens such as $ATOM, $LUNA, and $SCRT which are all capable of being staked. The next category is *stablecoins*. The level of attractiveness for the ShadeDAO to acquire a stablecoin is based on three variables: liquidity, degree of decentralization, and volatility. Examples of stablecoins that fall into this category are UST, USDT, and USDC. Next is *Scarce Stores of Value* - these are "hard-assets" such as bitcoin, ethereum, and monero that have deep liquidity, halvening cycles, and/or historical relevance within the cryptocurrency domain. Finally, the last category are *liquidity tokens* which are mathematical claims on a portion of tokens tied to liquidity pools on decentralized exchanges. The more *liquidity tokens* owned by the ShadeDAO, the more locked-liquidity is available for the Shade Protocol community.

Initially, the ShadeDAO will be heavily focused on acquiring yield generating and LP tokens during the beginning of the protocol's lifecycle. Overtime, there should be a steady shift towards holding more and more stablecoins and scarce stores of value as adoption for Silk solidifies.

Conclusion

Bonds are an incredibly powerful primitive that will help bootstrap, scale, and grow the ShadeDAO throughout the duration of its lifespan. Importantly, governance and branches managing the issuance of Shade bonds must carefully balance the rate of issuance so as to not introduce damaging liquidity shocks into the larger market. Simultaneously, bonds must be well positioned to capitalize on large discrepancies between the market price and the treasury price of SHD. If balanced properly, bonds can be the fundamental source for gathering the necessary collateral to add both additional liquidity and stability for Silk and other key Shade Protocol primitives.