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

Carter Woetzel
www.securesecrets.org

Abstract. Shade Protocol is an array of distributed and interconnected privacy-preserving DeFi products that leverage the full capabilities of Secret Contracts on Secret Network. Encrypted metadata for smart contracts unlocks an entire layer of value previously inaccessible to DeFi protocols and users. Privacy integrated into Defi products protects user anonymity, positions, and value transfer. MEV (Miner Extractable Value) bots have decimated every day users on various swap dApps. Publicly visible collateralized positions have elicited larger market makers to advantageously leverage price movements to cause mass liquidation events. Front-running of NFT marketplaces have damaged the reputation of multiple platforms. Lack of transactional privacy have doxed various DeFi entities and have 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 indexes, 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 Networks native privacy-preserving stablecoin that will undergird 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.

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

[1] Secret Network - A Privacy-Preserving Secret Contract & Decentralized Application Platform [Whitepaper, Carter Woetzel 2020]

- All applications added to Shade Protocol must adhere to at least 1 of 4 of the following rules:
    - The application increases the scarcity of Shade
    - The application grows the Shade Treasury (Synthesis)
    - The application increases the utility for Silk
    - The application increases the demand for Silk
- No new unique token per application
    - Unique per application tokens dilute the potential value for Shade, and create an end user experience designed around generating value for the specific application token as opposed to the end user
- Silk is agnostic with integrations
- Stability of Silk is a public good
- Triggers on actions that benefit all shareholders must be open-sourced
- Avoid non-collateralized inflation
    - Only exception: initial shade distribution pools
- Shade Protocol places value capture for Shade Protocol as the sole allegiance
    - Do not conflate assisting the underlying protocol as the optimal decision, as the underlying infrastructure already benefits from increased transaction usage
- Growth of the Shade Treasury > expenditures
- Treasury should passively build an account for liquidity providing rewards
    - LP is a long term public good
- Avoid fixed-rate values with Shade Protocol tokenomics 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.

Silk: A Privacy-Preserving Algorithmic Burn Stablecoin

Carter Woetzel
www.securesecrets.org

Abstract. Current stablecoins such as TerraUSD have been designed based on protocol level architecture and incentives - relying on validators to maintain positions despite short term price volatility in return for inflationary governance token rewards that exist to resolve peg disparities. While a protocol level design has certain advantages, having the supply of the stablecoin be tied to validators (as conduits for token expansion) limits the long term viability and effectiveness of the stablecoin for two reasons: decentralization of the stablecoin expansion is tied to the validator set, and the total supply of both the stablecoin and the governance token is contingent upon indefinite inflation so as to properly incentivize validators. Additionally, these systems have no underlying collateral or intrinsic value outside of the maintenance of the peg and continued demand for the underlying stablecoin. Finally, there is no stablecoin in DeFi with transactional privacy by default.

Silk is the solution to this problem - built on Secret Network as a native privacy-preserving algorithmic stablecoin using the SNIP-20 token standard. The Silk architecture is designed using a dual-burn minting process for both the governance token Shade and the stablecoin Silk. Total stablecoin supply is limited by initial Shade distribution as well as Total Value Burned (TVB) in the minting process of both Shade & Silk (which are convertible with each other). Native AMM support in combination with Shade and Silk convertibility resolves peg disparities.

Silk

Silk (i.e. sSCRT / USDT initially) is the first ever privacy-preserving and smart contract interoperable stablecoin in blockchain history - launching on Shade Protocol. 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 USDT via Band Protocol oracles integrated into Shade Protocol), is a unit of account (1 Silk ~ $1 for V0), and is a standard of deferred payment - all of which give Silk the four key fundamental properties of money.[2]

Silk is algorithmically stabilized by Shade - the governance token of both Silk and Shade Protocol.[3] Silk replaces the payments value chain (credit card networks, banks, payment gateways) with a single application-layer protocol. Shade Protocol and Silk are credibly neutral, distributed, and have transactional privacy by default. Important for compliance and transparency is that Silk and

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

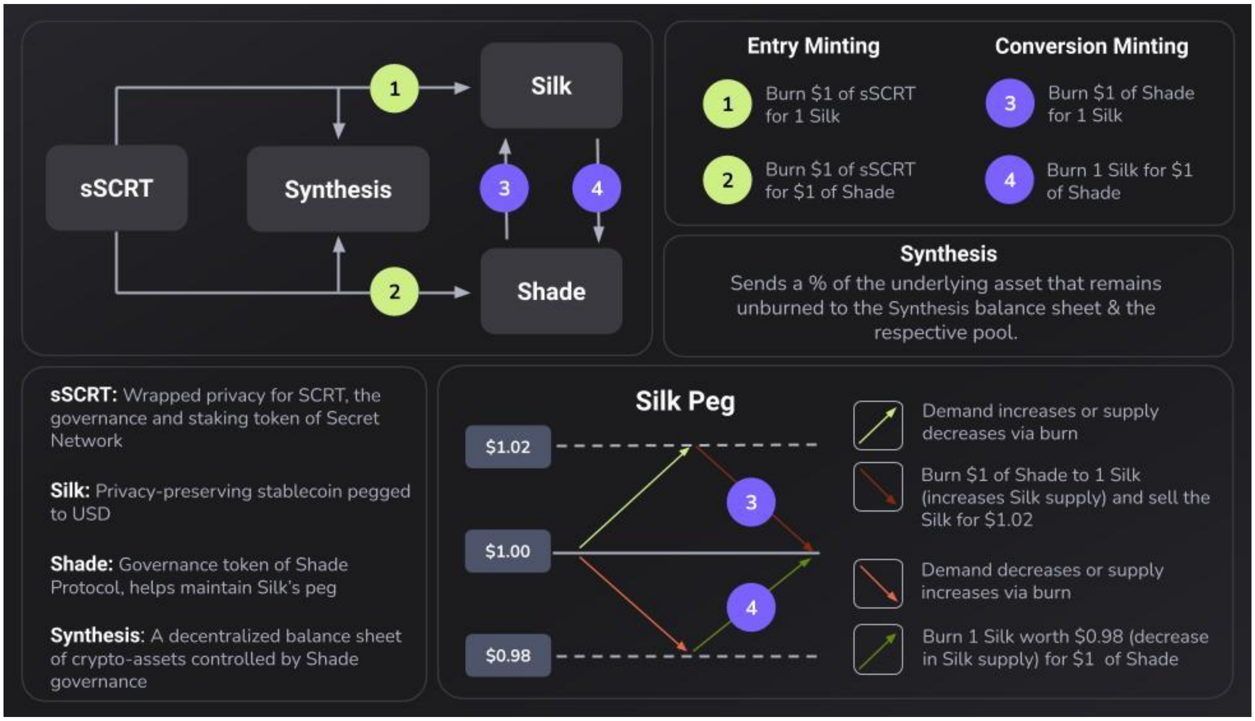
[3] Read the Shade Whitepaper: https://32184fa2-0116-41dd-971d-2057a7b58cc8.filesusr.com/ugd/b34138_3d2bbdb6575b47b29f7c5ec3fcb33289.pdf

Shade transactions can be decrypted with a viewing key unique to the address owner of the Silk; this empowers users to be transparent by choice. Additionally, users have the option to share data with trusted necessary entities that need an audit trail of transactions.

Minting

An important assumption of Silk architecture is that Silk is worth $1 over an indefinite period of time, despite experiencing peg fluctuations. There are four minting options with Silk and Shade - two of which are called "DAO entry" and two of which are called "conversion". The "DAO entry" of sSCRT for Silk or Shade is one directional. Burning Shade for Silk and vice versa is considered "conversion". Note that the process of conversion in tandem to exchange arbitrage is what helps maintain Silk's peg during periods of supply and demand expansion and contraction.

- Deposit $1 worth of sSCRT into DAO -> mint 1 Silk. (Silk entry minting)
- Despoti $1 worth of sSCRT into DAO-> mint $1 worth of Shade. (Shade entry minting)
- Burn $1 worth of Shade -> mint 1 Silk (Shade conversion minting)
- Burn 1 Silk -> mint $1 worth of Shade (Silk conversion minting)



1 Burn $1 of sSCRT for 1 Silk

2 Burn $1 of sSCRT for $1 of Shade

3 Burn $1 of Shade for 1 Silk

4 Burn 1 Silk for $1 of Shade

Synthesis

Sends a % of the underlying asset that remains unburned to the Synthesis balance sheet & the respective pool.

sSCRT: Wrapped privacy for SCRT, the governance and staking token of Secret Network

Silk: Privacy-preserving stablecoin pegged to USD

Shade: Governance token of Shade Protocol, helps maintain Silk's peg

Synthesis: A decentralized balance sheet of crypto-assets controlled by Shade governance

Demand increases or supply decreases via burn

Burn $1 of Shade to 1 Silk (increases Silk supply) and sell the Silk for $1.02

Demand decreases or supply increases via burn

Burn 1 Silk worth $0.98 (decrease in Silk supply) for $1 of Shade

Expansion / Contraction

In an expansion example, the price of Silk is trading at $1.02. To resolve the peg disparity, there needs to be an increase in the total supply of Silk in order to reduce the price of Silk to its intended target of $1.00. This increase in supply is facilitated by the following process: a holder of Shade will burn $1.00 worth of Shade and mint 1.00 Silk (Shade conversion minting). This holder of Silk will then have the opportunity to trade Silk that the market values at $1.02 (while the holder minted at a

$1.00 rate) to any asset available on an AMM. The sell pressure created by Shade conversion minting (expanding the total supply of silk) pushes the price of Silk to its intended target of $1.00.

$Initial\ Shade\ Position\ Value\ (\alpha)\ =\ Total\ Shade\ *\ Shade\ Price$

$Silk\ Arbitrage\ Position\ Value\ (O)\ =\ (\alpha\ /\ Silk\ Conversion\ Minting\ Rate)\ *\ Silk\ Open\ Market\ Price$

$Shade\ Arbitrage\ Profit\ (\tau)\ =\ O\ -\ \alpha$

$\tau\ =\ O\ -\ \alpha$

In a contraction example, the price of Silk is trading at $0.98. To resolve the peg disparity, there needs to be a decrease in the total supply of Silk in order to increase the price of Silk to its intended target of $1.00. This decrease in Silk supply is facilitated by the following process: a holder of Silk will burn 1 Silk and mint $1 worth of Shade (conversion). This holder of Shade will then have the opportunity to trade that amount of minted Shade that the market values at $0.98 (while the holder minted at a $1.00 rate) to any asset available on an AMM. The sell pressure of Shade arbitrage created by negative conversion minting as well as the decrease in the total supply of Silk are what pushes the price of Silk to its intended target of $1.00.

$Initial\ Silk\ Position\ Value\ (\sigma)\ =\ Total\ Silk\ *\ Silk\ Open\ Market\ Price$

$Shade\ Arbitrage\ Position\ Value\ (\boldsymbol{\lambda})\ =\ Total\ Silk\ *\ Shade\ Conversion\ Minting\ Rate$

$Silk\ Arbitrage\ Profit\ (\phi)\ =\ \boldsymbol{\lambda}\ -\ \sigma$

$\phi\ =\ \boldsymbol{\lambda}\ -\ \sigma$

An additional reason to convert Silk to Shade when it's less than $1 would be to own more Shade (at an arbitrage discount) so as to leverage any future expansionary arbitrage using an even greater position of Shade. Ultimately, the drop in value from the decrease in demand of Silk that resulted in a sub $1.00 price of Silk is absorbed by Shade holders, and as the Shade supply is diluted (and the Silk supply decreases), the value is essentially transferred from the Shade collateral to raise the price of Silk.

Entry Minting

The dual burn entry mechanism gives Silk and Shade unique value propositions over other stablecoins and their respective governance tokens. While other algorithmic stablecoins are by definition not backed by any collateral, Shade and Silk are backed by the burned collateral value of the sSCRT and other accepted tokens. While other protocols leave minting to validator inflation or collateralized leveraged positions, Silk architecture empowers users to directly transfer value into the Silk and Shade ecosystem via the dual burn entry mechanisms. This mechanism creates a supply sink for sSCRT - creating value for Secret Network and SCRT holders by decreasing the total supply of sSCRT from total value burned.

An additional benefit of burn entry is that decentralization of the governance token Shade is not largely controlled by a validator set as with other protocols. Instead, ownership will be attached to both investors and minters of Shade. This will increase the decentralization compared to other ecosystems where a subset of entrenched network participants (validators and stakers) benefit in the long run due to indefinite inflation required to secure the protocol and also to maintain peg-stability.

Finally, entry minting can be expanded to additional tokens beyond sSCRT. Due to Secret Network interoperability with IBC, other tokens such as sATOM could be burnable into Shade Protocol. Shade Protocol governance will have the opportunity to vote on token contract addresses that can be added as “entry burnable” assets.

Shade Treasury

The Shade Treasury (controlled by Shade decentralized governance) is created as a result of a controllable, dual-variable system (known as “synthesis”) incorporated into all Shade Products and many of their respective mechanics. The two variables are “burn” and “synthesize”. Burn is used to destroy a certain percentage of a token as a result of a given action executed. Synthesize sends the remaining unburned percentage to the Shade Treasury contract address which is controlled by staked decentralized Shade governance.

$$Burn = 1 - X$$
$$Synthesize = 1 - Burn$$

Entry minting as a mechanic incorporates Synthesis, giving Shade holders the opportunity to capture value on burn-based entries. With the synthesis mechanic, entry-minting and Shade Products build long term value for Shade holders on a treasury that is governed in a decentralized way as a public good.

Entry Minting Cap & Attack Vectors

Shade Protocol caps daily entry minting for Silk and Shade to a fixed amount of Shade on a daily basis. This parameter is controlled by Shade governance. To understand the reasons behind not having unfettered burn-based entry into Shade Protocol, this section will outline the possible attack vectors, as well as the thought process behind this design decision.

The primary attack vector against Shade Protocol and Silk is known as an “Entry Dilution Attack” (EDA) which would occur if Shade Protocol supported unfettered and unlimited burn entry into Silk or Shade at any given moment. Shade Protocol stops EDA by hard-capping Silk & Shade entry minting on a daily basis.

Here is an example of an EDA:

1. Attacker drives the price of Shade down on the open market with a mass sell-off of Shade
2. Attacker then entry-burns a massive amount of accepted tokens (sSCRT, sATOM, sBTC, etc.) to directly mint a large amount of Shade at a price rate significantly lower than currently circulating Shade.

EDA results in the following:

- Inflation of supply at the cost of all Shade holders
- Unpredictable price volatility that can impact peg stability
- Reduction of attacker’s total value
- Growth of Synthesis Treasury

EDA is a self-inflicted and sacrificial financial attack because the attacker upon entry minting is mass diluting their own Shade entry position with no promises of liquidity post EDA. Despite this, the following are reasons why EDA would still be executed:

- Hedge fund executes an EDA for $2,000,000,000 while having short position opened on the open market worth $10,000,000,000
- Competitor protocol executes an EDA, resulting in additional value or capital flowing to the attacking protocol

To put it into simple economic terms, EDA will be performed if :

$$Benefit\ of\ EDA\ >\ Cost\ of\ EDA$$

Imagination is the only limitation on picturing when this equation becomes true for a range of entities. As such, the protocol hard caps the amount of Shade and Silk that can be entry minted with no slippage on a daily basis using an epoch implementation, denominated in X amount of Shade that can be burned into.

By fixing the daily entry-burn cap to a fixed number of Shade on a daily basis, the protocol becomes immune to unpredictable mass dilution (EDA) in favor of a maximum amount of dilution on a daily basis. Shade Protocol replaces block-based inflation (which protocols like Terra need in order to secure the protocol and incentivise validators) by instead using a burn-based expansion of supply where the only limited dilution of the system goes directly to a public good (the treasury via the synthesis mechanics) that is by default not an active part of circulation.

Philosophically, the dilution from entry-minting is sent to a democratized and public address which all Shade holders have ownership of, which makes the specific dilution tradeoff deemed as acceptable. Additionally, the dilution was created by a burn and a sacrifice, as opposed to an indefinite block-based reward mechanic. The end result is that token supply expansion is tied to increases in Shade market capitalization (which increases the amount of Silk that can be supported) as well as the amount of value willing to be burned into Shade Protocol via entry minting.

Burn based entry with a cap achieves the following:

- Stops EDA
- Builds adoption of Silk
- Consistently grows the Synthesis Treasury for all Shade holders
- Solves liquidity issues for users who use the daily limited no slippage entry

- Creates supply sinks for entry tokens that are burned
- Predictable token expansion based on value burned

All of these are benefits. To realize these benefits, Shade holders have a % of their value diluted and pushed to the Synthesis treasury (a public good) whenever a user uses the limited burn-based entry minting of Shade Protocol.

The only unavoidable attack vector that remains is known as an “Entry Minting Discount Attack” (EMDA) which is performed as followed:

1. Attacker mass sells of a large amount of Shade, decreasing the price
2. Because the oracle entry minting rate is pointed at Shade pairs, attackers are able to entry mint into the limited amount of hard-capped Shade at a discounted rate while the price of Shade is temporarily reduced due to the mass sell-off

EMDA still grows the treasury, and still pushes value into the system. Additionally, the attacker must have a large amount of capital available, and must be willing to incur the risks of trying to move the price on the open market. The more liquidity provided on pairs that involve Shade, the more difficult it will be to execute an EMDA.

The end goal of Shade Protocol and the range of products that are set to be released on Shade Protocol is the following:

$$Daily\ Shade\ Entry\ Minted\ <\ Daily\ Shade\ Burned$$

Supply

The total supply of Silk (tsS) and the total supply of Shade (ts-S) is bounded by the following equations:

$$tsS\ =\ \Sigma\,(Silk\ Entry\ Minting\ +\ Shade\ Conversion\ Minting)$$

$$ts - S\ =\ \Sigma\,(Shade\ Entry\ Minting\ +\ Silk\ Conversion\ Minting\ +\ Initial\ Shade\ Distribution)$$

It is important to note that outside of the fixed initial shade distribution (ISD) all other upper-bounds are limitless - only tied to the amount of value burned and transferred into the Silk and Shade ecosystem over time.

Global Yield Derivation for Silk

The current set of stablecoins in the DeFi domain are pegged and collateralized based on perceived value retaining stable currencies such as USD. As a result of this, stablecoins in their current iteration are exposed to the respective depreciation or appreciation of the stable asset being collateralized against. Shade protocol will implement a Global Yield Derivation (GYD) mechanic as part of the product roadmap. GYD creates an index that Silk can be collateralized against. This GYD index is derived from a basket of the following stable assets:

- United States Dollar
- Swiss Franc
- Japanese Yen
- Norwegian Krone
- European Euro
- Canadian Dollar
- Singapore Dollar
- Commodities

GYD is integrated via Band Protocol. As a result of GYD integration, Silk retains a stable value in relation to the global economy significantly better than USD peg in isolation could ever hope to achieve. GYD peg migration is attached to decentralized governance voting on the following:

1. Which currency and asset contract addresses are included in the peg
2. The weights attached to the composition of the peg

Sustainability

Value enters the Silk and Shade ecosystem through Fiat -> SCRT -> sSCRT -> Shade or alternatively Fiat -> SCRT -> sSCRT -> Silk. In the future, other assets other than sSCRT (perhaps IBC enable Secret Tokens) could be burned as well. Shade collateralizes Silk because 1 Silk can always be exchanged for $1 worth of Shade or whatever the target peg is as determined by dectranzlied governance. Shade also stabilizes Silk since arbitrageurs will resolve the price difference and extract profit - profits that take the form of either Shade and Silk. The balancing of the peg revolves around exchanging value between currency and collateral. Silk's value will continue to grow by encouraging more Secret Apps and protocols to accept Silk due to its increased convenience, privacy-preserving benefits, and stability.

Those who invest in collateral (Shade minters / holders) are investing long-term in the network and are agreeing (in an abstract way) to absorb short-term volatility in exchange for the benefits of predictable arbitrage as well as the ability to influence governance of Silk and Shade Protocol. This system continues to work if there is enough value in Shade or Silk to continue the momentum of the rebalancing act. The value of Shade is attached to fees collected via use of Shade Protocol (a privacy-preserving synthetic assets marketplace), the value of predictable arbitrage profits to maintain the price peg of silk, value of dividends from the Shade Treasury, as well as the ability to impact governance and parameters of both Silk, Shade Protocol, and future products. Finally, the value burned from entry minting into both Silk and Shade adds to the value of Shade.

Terminology

- **TVB**: total value burned
- **tsS**: total supply of Silk
- **ts-S**: total supply of Shade
- **Silk**: privacy-preserving algorithmic stablecoin native to Secret Network

- **Shade**: Shade Protocol governance token, used to resolve Silk peg-disparity
- **ISD**: Initial Shade distribution

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

Carter Woetzel, Stephen Ash
www.securesecrets.org

Abstract. Shade Protocol, an array of connected privacy-preserving DeFi applications, are unified under a single governance and utility token called "Shade".[4] One of the primary value capture mechanics for Shade within this suite of DeFi applications is a result of consistent burn mechanisms that help increase the scarcity of Shade and by extension its value. While many protocols leverage burn mechanics and inflation to ensure the stability of the underlying value of the governance token, these protocols lack the ability to build flexible and controllable long term value for their respective governance token.

Synthesis, a privacy-preserving decentralized asset management protocol, is the solution to this problem for Shade Protocol by creating a balance sheet of crypto-assets controlled by Shade governance which can be used for buy-backs, hedged positions, leveraged positions, collateralization, liquidity provision, batched Shade burns, user incentivization, and dividend generation. These crypto-assets are added to the Synthesis balance sheet via a "synthesize" mechanic introduced into all of the Shade Protocol.

Synthesis

The Synthesis balance sheet is created as a result of a controllable, dual-variable system incorporated into all Shade Products and many of their respective mechanics. The two variables are "burn" and "synthesize". Burn is used to destroy a certain percentage of Shade as a result of a given action executed. Synthesize sends the remaining unburned percentage of the underlying to the Synthesis balance sheet contract address.

$$Burn = 1 - X$$
$$Synthesize = 1 - Burn$$

A simple example of burn and synthesize used with a Shade Product is with Silk contracts. Users are able to mint Silk & Shade by burning tokens.[5] Based on the burn variable percentage set by Shade governance for minting, the remaining percentage of the assets that are not burned are "synthesized" i.e. sent to the Synthesis balance sheet contract address. This balance sheet of assets accrued are controlled by Shade governance.

The Synthesis balance sheet could look something like the following:

Token	Amount	Value
sSCRT	2,300,000	$6,900,000
sETH	800	$1,600,000

[4] Shade Protocol Whitepaper (Carter Woetzel, 2021)
[5] Silk: A Privacy-Preserving Algorithmic Burn Stablecoin

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 Synthesis 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 Synthesis 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**[6]
Burn Shade	0x000000
Buy Shade with Silk	secret1ban4qh5jy9zhvyknmjzlstzkygyycfhpfrdlzk
Liquidity Provide sSCRT X Silk	secret1grn3ob5cc6zhvyozmkldstzkyfhgycfhpdjom
Sell S-Tesla for Silk	secret1bll3ot7cx6zxvyozsdmrstzkyfhxxcfhheyuitv
Distribute Silk Dividend	secret1del8ot2cx2zvlyozsdtodtzkyfhxxcfhheyuom
Add Shade to LP Rewards Pool	secret1jer9zb3tn5uhuuknmzzlstzkygyycfhpfrdlzkr
Convert sSCRT to SCRT	secret15l9cqgz5uezgydrglaak5ahfac69kmx2qpd6xt
Stake SCRT	secret15l9cqgz5uezgydrglaak5ahfac69kmx2qpd6xt

[6] Fictional addresses.

As a general principle, the Synthesis balance sheet is intended to take a capital conservation approach. Hardcoded into the Synthesis Protocol 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 Synthesis balance sheet, this hardcoded restriction ensures due diligence from Shade governance token holders by introducing intentional friction into the spending process.

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

Stake Dividend

To benefit from the Synthesis balance sheet and the wealth generating "cash flows" generated from the various activities (LP, staking, dividend distribution) users must be staked to the Shade dividend contract. This contract has a 90 day "unbonding" period (quarterly). The more users wanting to participate in the Stake Dividend, the more Shade that will be staked - this will reduce the amount of Shade in active circulation, increasing the value of Shade. As a result of this dividend, Shade not only represents total value burned into the Shade Product ecosystem, total value collateralized in Shade Protocol, total value of governance, total value of assets on the Synthesis balance sheet, total value of utility across all Shade Products, but also the value of the dividend distributed on a quarterly basis.

The value of the Shade dividend is always sent in the form of Silk - the flagship privacy-preserving stablecoin that is native to Secret Network. The amount of dividend received is kept encrypted/private, as is the individual's amount of Shade locked into the Stake Dividend contract. Users will have the opportunity to decrypt their staking and dividend transactions with their viewing key - giving users the opportunity to report and stay compliant with their respective sovereign nation.

Flexible Value Spread

With the ability to create secret contracts that interact with Synthesis, Shade governance has an incredible amount of room for creativity and flexibility with how balance sheet assets get used. While most dApps are capped by the value of their individual governance token, Shade is the sum of its parts - empowering Shade governance to shift value around to elicit positive change for any of the products in the Shade product suite. Building up a healthy balance sheet over time with Synthesis, Shade Products will have the opportunity to be incredibly resilient during market contractions or hyper growth focused during expansionary phases with how the Synthesis balance sheet assets are utilized.

Simplified Valuation

Valuation models are incredibly complicated with most governance tokens; they are largely contingent upon hypothetical volume and potential fee rates. With Synthesis, Shade as a governance and utility model is now directly tied to a balance sheet of crypto-assets holding real value. In other words, the “fundamental” floor value of Shade will be tied to the value of the assets in Synthesis as well as the value of the dividend regularly distributed to holders. Naturally, complexity will continue with valuation models and Shade. How does the total value burned correlate to the underlying value of Shade? How does the collateral locked up in Shade Protocol (synthetic assets market) impact the valuation of Shade? How does one measure the impact of Silk adoption on the fundamental value of Shade? These will continue to be questions at large. However, at a minimum investors will have Synthesis as a baseline for valuation models.

Conclusion

Synthesis is a privacy-preserving decentralized asset management protocol built on Secret Network and governed by Shade - empowering Shade holders to directly use a balance sheet of crypto-assets created from “burn” and “synthesize” mechanisms introduced into all Shade products. Synthesis directly empowers investors to impact the value of Shade and the respective products. Synthesis is the world’s first privacy-preserving decentralized balance sheet - an experiment that is breathtaking in scope, 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 Synthetics: Privacy-Preserving Synthetic Assets Protocol

Carter Woetzel
www.securesecrets.org

Abstract. Current traditional financial markets are intentionally restrictive - denying access to many users and investors globally as a result of prohibitive identity requirements, inability to handle fractional purchases of assets, minimum liquidity requirements, and transaction costs. All of which are barriers for entry and access to financial investments and infrastructure. A decentralized protocol that can mint synthetic assets generated from collateralized assets (with active value) would allow for a secondary reflexive market of synthetic tokens that can properly reflect the value of underlying traditional assets and products. These synthetic assets (holding their value because of an algorithmic peg) would empower an entire ecosystem of tokenized assets that hold the following properties: divisibility, simplicity, accessibility, holding-affordability, censorship resistance, minimized transaction fees, price accurately pegged to a 'real' world asset, and transferability. Synthetic asset markets such as UMA and Mirror have seen an increasing amount of adoption - enabling a new category of decentralized assets that have the potential to drastically change decentralized finance as we know it. Unfortunately, lacking within these trailblazing protocols is a key component to the future of DeFi - privacy. Transactions without privacy impair users' ability to discreetly interact with synthetic markets, and move assets around freely. Additionally, expansion of the token supply is based upon the creation or destruction of leveraged positions - an unstable architecture fundamentally when trying to mirror and create a lack of volatility between the real world market and the digitally pegged synthetic asset equivalent.

The lack of the fundamental property of privacy in current synthetic asset markets is solved by Shade Protocol: a privacy-preserving synthetic assets market where metadata attached to minting, governance, oracles, and staking contracts are kept entirely encrypted via secret contracts on Secret Network. Additionally, all synthetic tokens minted on Shade Protocol leverage Secret Network's SNIP-20 private and fungible token standard. Consequently, minted synthetic tokens have transactional privacy by default. Finally, utilizing a burn-based entry and algorithmic peg similar to Silk ← → Shade mechanics, the free market will be empowered to decide which set of assets will stay stable into perpetuity via open market arbitrage interaction with the underlying minting contracts.

Shade Synthetics

Shade Synthetics built on Shade Protocol is the first privacy-preserving synthetic assets protocol ever created - a historical moment for decentralized finance. Specifically, Shade Synthetics allows anyone to mint and trade privacy-preserving synthetic assets that reflexively track the price of real world assets using Band Protocol - a decentralized cross-chain oracle solution. On Shade Protocol, users globally have access to tokenized synthetic assets that are both affordable and easy to interact with - all while preserving the users underlying privacy. Notably, synthetic buyers on the secondary markets will be able to buy synthetic assets without needing to pay a premium incurred from risk disparities traditionally inherited from leverage based collateralized architecture of other protocols (such as Mirror). Band Protocol on Secret Network has initial implementation support for BTC, ETH, USDT, USDC, DAI, and SCRT with more assets to be supported in the future; additional support will unlock the possibility of an even larger number of synthetic asset pairs.

Shade Protocol is a secret application built on Secret Network - the first live blockchain with data privacy by default for smart contracts (i.e. “secret contracts”).[7] The unique feature of secret contracts is encrypted inputs, output, and state enabled by a decentralized network of Trusted Execution Environment (TEEs).

Synthetic assets issued on Shade Protocol are known as S-tokens (Shade Synthetic tokens) unless the token that is issued is a stablecoin (such as Silk) or a stabilizer token (s-token). The value of Shade Synthetic tokens mirror the asset price being targeted via Band Oracle and contract design. The value of each stabilizer token is contingent upon the total value of the arbitrage for the respective pair. Shade Synthetic tokens and their respective stabilizer tokens have minting contracts that target a real world peg (identical to Silk and Shade). That is to say, a Synthetic S&P500 token has a stabilizer-S&P500 token. Synthetic Gold has its own stabilizer-Synthetic Gold token. Original architecture contemplated having single stabilizers working for multiple synthetics. However, this increases the risk that market disparity in demand for peg maintenance of a single asset could crash the stability of multiple assets. Therefore, separation of each synthetic with its own stabilizer results in free-market mechanics determining what synthetic pairs succeed or not.

Shaded synthetic tokens functionality is similar to other protocols such as UMA and Mirror:

- Trading
- Minting
- Liquidity providing
- Burning

Synthetic Assets

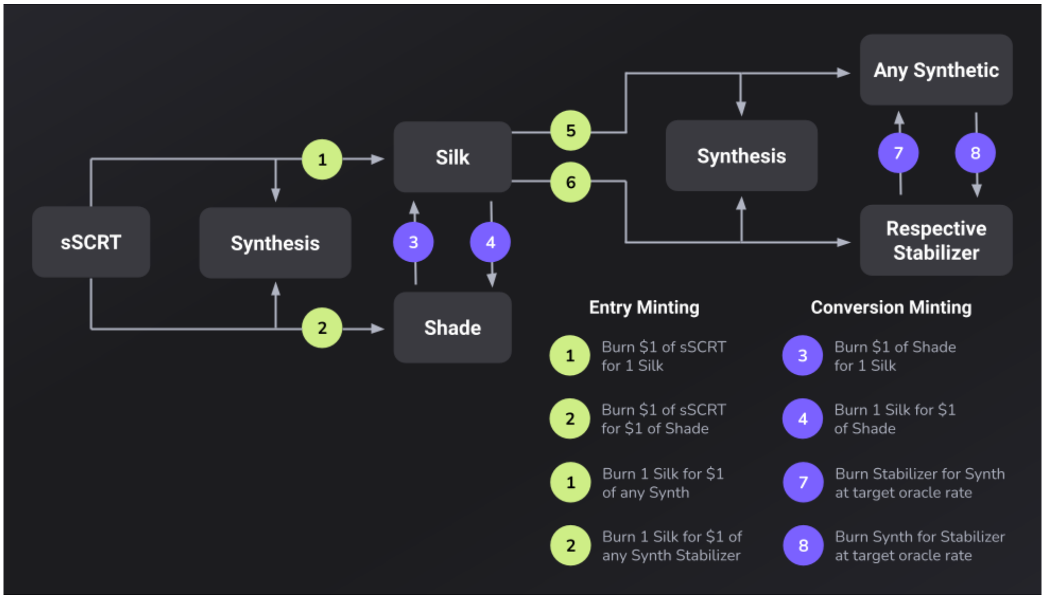
Shade Synthetics are specifically targeting S&P500, NASDAQ, gold, silver, bitcoin, ethereum, and any individual currency that is demanded as a synthetic asset by the Shade community. Shade Synthetics will also target the creation of a cryptocurrency index which mirrors the top 100 cryptocurrencies. This would give cryptocurrency users’ the ability to directly invest in a token that is a representation of cryptocurrency as an asset class. An index tokenization of the stabilizer tokens is also possible - empowering users to directly invest in the value of all stabilizer tokens of Shade Synthetics. Index tokens unlock the ability to programmatically track representations of value, and give the open market and opportunity to invest in these unique representations - all in a completely privacy-preserving way by default. The limitations of any synthetic pair is contingent upon liquidity provision, as well as demand by Shade governance to approve the addition of the synthetic/stabilizer pair to synthetic assets.

Mechanics

Generalization of the Silk/Shade peg mechanisms means that any real world value can be tied to a synthetic token that tracks its value as long as there is a stabilizer token that can respectively balance it. The value of the stabilizer token is determined by the free market and is ultimately a

[7] Secret Network is a layer one solution built with the Cosmos SDK using Tendermint’s Byzantine fault-tolerant consensus algorithms.

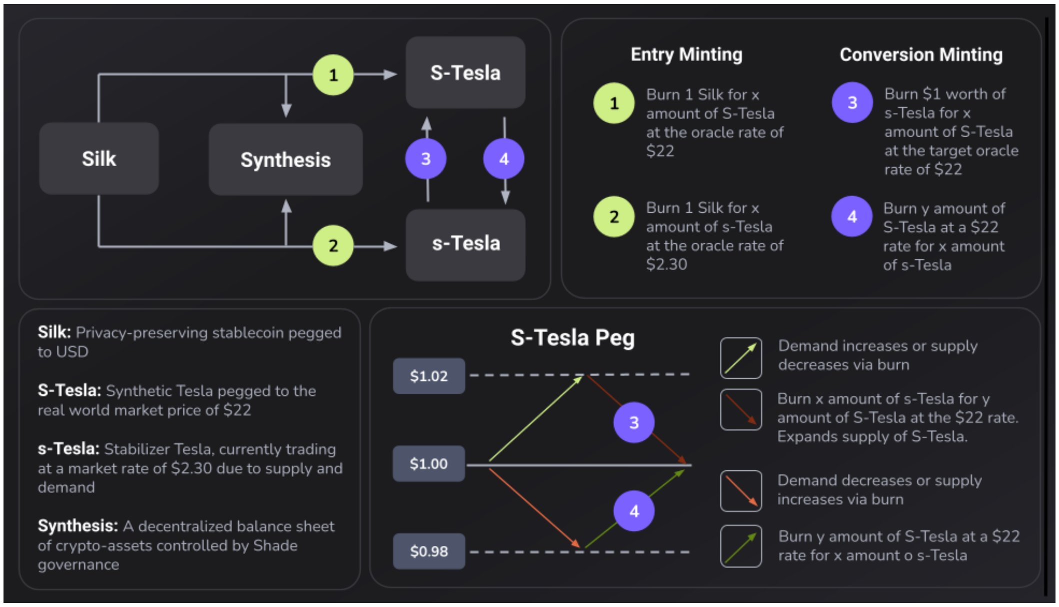
reflection of the value of the arbitrage profits that can be performed with the stabilizer token, as well as any dividend received by holding the stabilizer token. Conversion minting contracts target real world assets in comparison to secondary Secret DeFi price disparities, creating arbitrage opportunities that are able to push synthetic asset prices back to target prices.


Any Synthetic
Silk
Synthesis
sSCRT
Synthesis
Respective Stabilizer
Shade
1
2
3
4
5
6
7
8
Entry Minting
1 Burn $1 of sSCRT for 1 Silk
2 Burn $1 of sSCRT for $1 of Shade
1 Burn 1 Silk for $1 of any Synth
2 Burn 1 Silk for $1 of any Synth Stabilizer
Conversion Minting
3 Burn $1 of Shade for 1 Silk
4 Burn 1 Silk for $1 of Shade
7 Burn Stabilizer for Synth at target oracle rate
8 Burn Synth for Stabilizer at target oracle rate

As such, a synthetic economy will emerge consisting of stabilizer tokens and their respective synthetic tokens. Silk is the only allowable entry-minting token for any synthetic pair. This makes Silk the gateway to synthetics with a limited no slippage entry using the same entry-minting cap mechanic that Silk & Shade entry minting utilize so as to avoid dramatic amounts of dilution.[8]

[8] See “Entry Dilution Attack” in the Silk Whitepaper

Minting Examples



Entry Minting

1 Burn 1 Silk for x amount of S-Tesla at the oracle rate of $22

2 Burn 1 Silk for x amount of s-Tesla at the oracle rate of $2.30

Conversion Minting

3 Burn $1 worth of s-Tesla for x amount of S-Tesla at the target oracle rate of $22

4 Burn y amount of S-Tesla at a $22 rate for x amount of s-Tesla

Silk: Privacy-preserving stablecoin pegged to USD

S-Tesla: Synthetic Tesla pegged to the real world market price of $22

s-Tesla: Stabilizer Tesla, currently trading at a market rate of $2.30 due to supply and demand

Synthesis: A decentralized balance sheet of crypto-assets controlled by Shade governance

S-Tesla Peg

Demand increases or supply decreases via burn

Burn x amount of s-Tesla for y amount of S-Tesla at the $22 rate. Expands supply of S-Tesla.

Demand decreases or supply increases via burn

Burn y amount of S-Tesla at a $22 rate for x amount o s-Tesla

Expansion Example:

Price of Tesla is trading at $22 dollars. However, synthetic Tesla (S-Tesla) is trading at $26 dollars on a DEX being tracked by a Shade Protocol oracle. This is not optimal as the real world price of $22 dollars is what S-Tesla should be traded at, not $26.

The user owns 600 stabilizer Tesla (s-Tesla) trading at a $2.30 rate = 600 * 2.30 = $1,380. The user converts via mechanism (3) the 600 s-Tesla for $1,380 / $22 target oracle rate = 62.72 S-Tesla. The user then sells the 62.72 S-Tesla on the open market for $26 dollars for 62.72 * $26 = $1,630.72 for a total arbitrage profit of $1630.72 - $1,380 = $250.72. Note that conversion minting from the stabilizer to the synthetic expands the supply of the synthetic and reduces the supply of the stabilizer, ultimately driving the price back to the intended price target of $22.

$$Initial\ Stabilizer\ Position\ Value\ (\chi)\ =\ Total\ Stabilizer\ Token\ *\ Stabilizer\ Price$$
$$Synthetic\ Arbitrage\ Position\ Value\ (\Psi)\ =\ ((Total\ Stabilizer\ Tokens\ *\ Stabilizer\ Price)\ /\ Conversion\ Minting\ Rate)\ *\ Synthetic\ Open\ Market\ Price)$$
$$Stabilizer\ Arbitrage\ Profit\ (\text{Ш})\ =\ Arbitrage\ Position\ Value\ -\ Initial\ Stabilizer\ Position\ Value$$
$$\text{Ш}\ =\ \chi\ -\ \Psi$$

Contraction Example:

Price of Tesla is trading at $22 dollars. However, synthetic Tesla (S-Tesla) is trading at $18 dollars on a DEX being tracked by a Shade Protocol oracle. This is not good as the real world price of $22 dollars is what S-Tesla should be traded at, not $18.

A user owns 100 S-Tesla trading on the open market at a $18 rate = $1,800. The user converts via mechanism (4) the 100 S-Tesla to sTelsa where the 100 S-Tesla are respected at a $22 target peg price (contrary to the open market) for 100 * $22 = $2,200 worth of value. This $2,200 worth of value in the form of sTesla is ($2,200 value being respected/converted / $2.30 s-Tesla market price) = 956.52 s-Tesla. Total arbitrage = $2,200 - $1,800 = $400. Note that the minting from the synthetic to the stabilizer decreases the supply of the synthetic, ultimately driving the price back to the intended price target of $22.

$$Initial\ Synthetic\ \ Position\ Value\ (\nu)\ =\ Total\ Synthetic\ \ Tokens\ *\ Open\ Market\ Synthetic\ \ Price$$
$$Stabilizer\ Arbitrage\ Position\ Value\ (\xi)\ =\ Total\ Synthetic\ Tokens\ *\ Conversion\ Minting\ Rate$$
$$Synthetic\ Arbitrage\ Profit\ (\dot{o})\ =\ Arbitrage\ Position\ Value\ -\ Initial\ Stabilizer\ Position\ Value$$
$$\dot{o}\ =\xi\ -\nu$$

As such, assuming the market values the underlying arbitrage and value earned from being in a stabilizer position, Shade Protocol allows a user to burn X amount of Silk (pegged to a $1) for Y amount of a Synthetic Asset or stabilizer that will maintain its price peg over time. If a synthetic/stabilizer peg fails, it is a result of the open market demand for maintaining that asset, not because the mechanics don’t work.

Shade Protocol Reflexive Growth

Silk is the only allowable asset that has access to the daily epoch capped burn-based no-slippage entry feature of Shade Synthetics. Having this feature set be tied exclusively to Silk builds additional demand for Silk, and by extension Shade. Because Silk is burned in the process of entry minting, a supply sink for Silk is created. Fundamentally, arbitrage that involves Silk scarcity is significantly easier to resolve as it does not pull from the market capitalization of Shade as with a contractionary event. Additionally, the burn-based entry into Shade Synthetics with Silk is also captured by the Synthesis mechanism - sending a % of assets from the burn-based entry to the Shade Treasury, building additional value for Shade holders. In order to safely launch a new Synthetic asset, the stabilizer price needs to first be established in order to safely launch the respective synthetic asset. As such, Shade stakers will be part of receiving stabilizer token airdrops - an additional reason for owning Shade.

References

[1] Maker DAO. (2017). The Dai Stablecoin System [Whitepaper].
[2] Silk: A Privacy-Preserving Algorithmic Burn Stablecoin [Whitepaper].
[3] Mirror Protocol. (2020). Mirror: Reflecting Asset Value On-Chain [Whitepaper].
[4] UMA. (2018). A Decentralized Financial Contract Platform [Whitepaper].
[5] Synthesis: A Privacy-Preserving Decentralized Asset Management Protocol For Shade [Whitepaper].