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

Sutera Duniya
shadeprotocol.io

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.

The native cryptographically-secured fungible protocol token of Shade Protocol (ticker symbol SHD) is a transferable representation of attributed governance and utility functions specified in the protocol/code of Shade Protocol, and which is designed to be used solely as an interoperable utility token thereon. It functions as 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, as economic incentives for positive behaviour.

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

[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 for 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 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 the network and 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

Sutera Duniya
shadeprotocol.io

Abstract. Current stablecoins such as UST have been designed based on protocol level architecture and incentives - relying on validators to maintain positions despite short term price volatility in return for governance or DEX rewards. 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 and stability of both the stablecoin and the governance token is contingent upon risk and return placed squarely on the risk profiles of valiators.. Additionally, these systems have no uncorrelated underlying collateral or intrinsic value (on the protocol level) 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 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 basket of currencies and commodities via Band Protocol oracles integrated into Shade Protocol), is a unit of account (Silk peg starts at ~ $1.05) , and is a standard of deferred payment - all of which give Silk the four key fundamental properties of money.[2] To simplify explanations, graphics and explainers 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 of $1.05 based on the value of the basket.

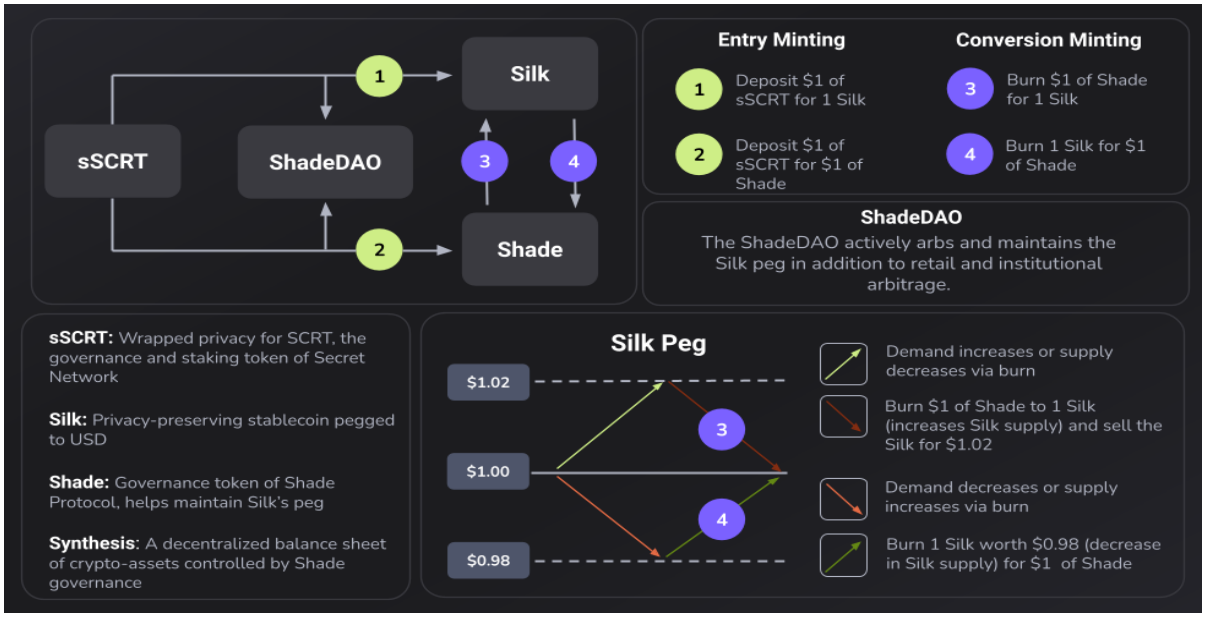
Silk is algorithmically stabilized by Shade - the governance token of both Silk and Shade Protocol. Silk replaces the payments value chain (credit card networks, banks, payment gateways) with a single application-layer protocol. Shade Protocol and Silk are credibly neutral, distributed, and have transactional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

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

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 two minting options with Silk and Shade - DAO entry and conversion minting. The DAO entry of sSCRT for Silk or Shade is one directional. Burning Shade for Silk and vice versa is considered conversion minting. 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. (DAO entry)
- Deposit $1 worth of sSCRT into DAO-> mint $1 worth of Shade. (DAO entry)
- Burn $1 worth of Shade -> mint 1 Silk (Conversion minting)
- Burn 1 Silk -> mint $1 worth of Shade (Conversion minting)



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.

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

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

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

shade

$$\tau = 0 - \alpha$$

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.

$$\textit{Initial Silk Position Value } (\sigma) = \textit{Total Silk} * \textit{Silk Open Market Price}$$
$$\textit{Shade Arbitrage Position Value } (\boldsymbol{\lambda}) = \textit{Total Silk} * \textit{Shade Conversion Minting Rate}$$
$$\textit{Silk Arbitrage Profit } (\phi) = \boldsymbol{\lambda} - \sigma$$
$$\phi = \boldsymbol{\lambda} - \sigma$$

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 into collective Silk market capitalization in order to raise the price of Silk back to the target peg.

Entry Minting

The 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 a set of uncorrelated assets on the ShadeDAO (as a result of entry minting) which helps actively arb the Silk peg. 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 entry minting mechanisms as well as bonds. The entry minting mechanism creates a supply sink for sSCRT - creating value for Secret Network and SCRT holders by decreasing the total supply of active SCRT circulating supply,

An additional benefit of entry minting 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 holders 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 leverage entry-minting into Shade

Protocol. Shade Protocol governance will have the opportunity to vote on token contract addresses that can be added as possible entry assets.

Synthesis

A dual-variable system known as “synthesis” is incorporated into a range of Shade Protocol primitives 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 ShadeDAO contract address which is controlled by staked decentralized Shade governance. These functions are in place to allow users to reflect the accurate value of synthetic assets as well as to redirect revenue to the ShadeDAO.

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

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 ShadeDAO to promote ecosystem adoption and security
- Solves liquidity issues for users who use the daily limited no slippage entry
- Reduces active circulating supply of tokens that are entry minted
- 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 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, as well as SHD minted by the treasury for the sale of bonds.

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 decentralized 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 utility 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 hold collateral (Shade minters / holders) are supporting 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.

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

Silk: Global Volatility Shock Absorption via Standardized Currency 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.[3] While volatility can be hedged against within forex markets, this does not provide protection for every day end users of the respective fiat currencies. Additionally, forex markets lack liquidity for hedges against exotic currencies, the cost of which is expensive.[4] Importantly, volatility makes prediction of future values uncertain - creating a deterrent for investment and trade that negatively impacts wealth generation and economic activity.[5] 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

[3] *Exchange rate volatility and trade flows*. International Monetary Fund. (n.d.). From https://www.imf.org/external/np/res/exrate/2004/eng/051904.htm.
[4] 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.
[5] *Global currency stabilization - WOCU*. (n.d.).http://www.wocu.com/upload/20726.pdf.

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 $100 for Silk so the weighting mechanics are clearly understood. The dollar is nominally as a reference currency used for an initial target, but actual weights and price after initial establishment is 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):[6]

Country	Currency	GDP (bn)	Amount	Weight
United States	USD	22,939.58	30.08324438	30.083%
China	Yuan	16,862.98	141.6585561	22.114%
Japan	Yen	5,103.11	763.2184019	6.692%
Germany	Euro	4,230.17	4.798457242	5.547%
United Kingdom	Pound	3,108.42	2.978750323	4.076%
India	Rupee	2946.06	289.5199473	3.863%
France	Euro	2940.43	3.335451679	3.856%
Italy	Euro	2120.23	2.405064808	2.780%
Canada	Canadian Dollar	2015.98	3.276048906	2.644%
Korea	Won	1823.85	2,813.904807	2.392%
Russia	Ruble	1647.57	153.3139914	2.161%
Brazil	Real	1645.84	12.17579453	2.158%
Australia	Australian Dollar	1710.56	2.983401206	2.243%
Spain	Euro	1439.96	1.633406338	1.888%
Indonesia	Rupiah	1150.25	21,549.31212	1.508%
Netherlands	Euro	1007.56	1.142917088	1.321%

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

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 stabilising effect created for any and all cost and revenue projections due to the reduction in volatility due to the nature of 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. $100 is the initial starting price peg for Silk. New weightages are re-applied in relation to this new amount, and individual currency amount contributions to the larger peg are shifted.

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

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

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

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

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

Country	GDP	% of Total GDP	Currency	Dollar Quote	Currency amt.	Weight contr.
United States	40,000.00	33.058%	USD	$1.0000000	36.36363636	$36.363636
China	20,000.00	16.529%	Yuan	$0.1061100	171.3487719	$18.181818
Japan	50,000.00	41.322%	Yen	$0.0093685	4851.848797	$45.454545

Germany	3,000.00	2.479%	Euro	$1.2261000	2.22434771	$2.727273
United Kingdom	8,000.00	6.612%	Pound	$1.5685000	4.636740372	$7.272727

Legal Landscape Theory

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

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

However, while Silk is uniquely positioned with the above features, there will inevitably be scrutiny surrounding the following variables:[7]

- KYC/AML/Cybercrime
- Tax Compliance

Silk is well positioned for scrutiny under the following:

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

Special Drawing Rights

Special Drawing Rights (SDR) as defined by the International Monetary Fund (IMF) is an international reserve asset, created by the IMF in 1969 to supplement its member countries' official reserves. To date, a total of SDR 660.7 billion (equivalent to about US$943 billion) have been

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

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.[8]

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

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

SCB due to the frequency of the updates, decentralization of the peg, and the neutrality of the standard, all make Silk and the respective basket composition superior to SDR as an alternative.

Global Value Shift

In a scenario where commodities and cryptocurrencies such as Bitcoin gain a dominant 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 distinct path to

[8] *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.

compliance and regulatory freedom within the existing international cryptocurrency and financial regulatory framework.

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**[9]
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.

[9] 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 did not actively participate will not receive any SHD incentives.

In order to provide the pool of assets supporting the privacy layer for Shade Synthetics, users would be required to stake their assets into the pool, and take on some level of risk to help stabilize the underlying protocol. 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.

Further, usage of protocol to generate Shade Synthetics, or helping to maintain the peg would also entitle users to participate in Shade rewards for active users. The Shade rewards contract would calculate each user's contribution to the protocol based on a pre-determined formula.

It is the community members which would maintain and drive development of Shade Protocol, so 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 SHD token governance rewards.

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 utilised 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 interaction 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.

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. 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.

Conclusion

ShadeDAO 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 the various decentralized revenue streams directed to the ShadeDAO (introduced into all Shade primitives). The ShadeDAO directly empowers users to impact the synthetic assets, and be rewarded for maintaining the peg. The ShadeDAO 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

Sutera Duniya

shadeprotocol.io

Abstract. Current traditional financial markets are intentionally restrictive - denying access to many potential participants 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”).[10] 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

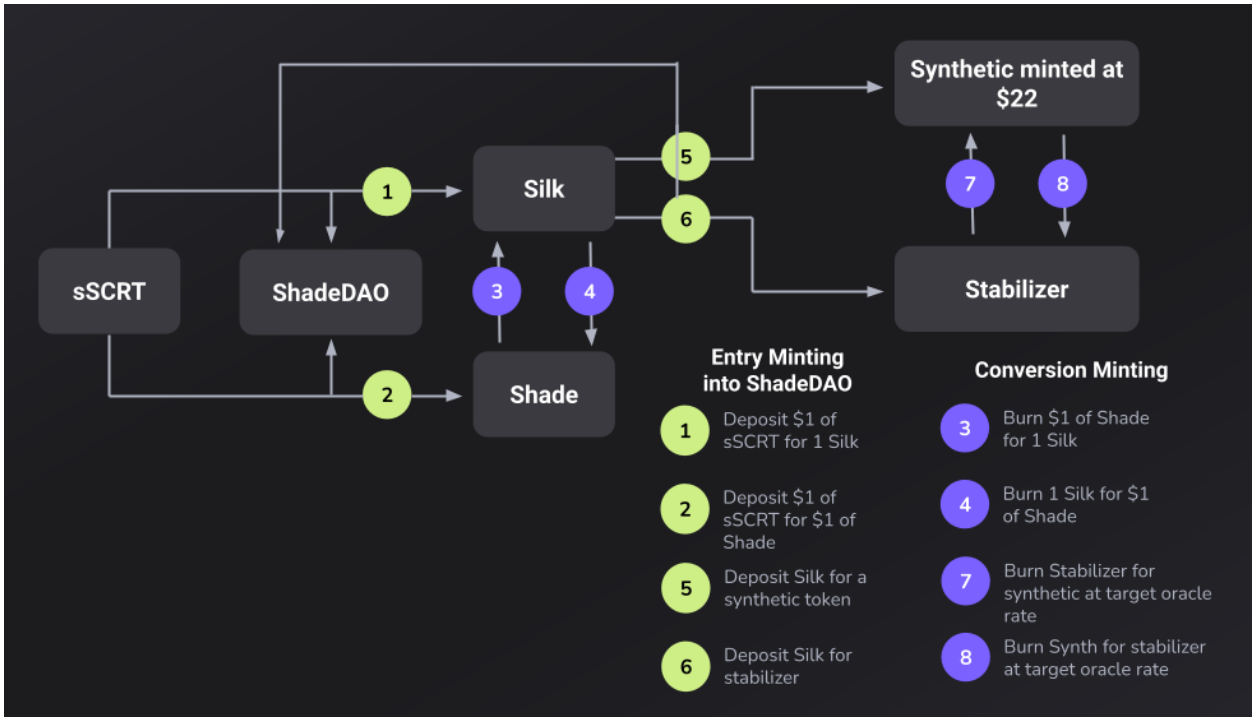
Shade Synthetics are specifically targeting S&P500, NASDAQ, gold, silver, bitcoin, Ethereum, and any individual currency that is demanded as a synthetic asset by the Shade community. Shade Synthetics will also target the creation of a cryptocurrency index which mirrors the top 100

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

cryptocurrencies. This would give cryptocurrency users' the ability to directly get exposure to 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 participate 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 an opportunity to participate 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

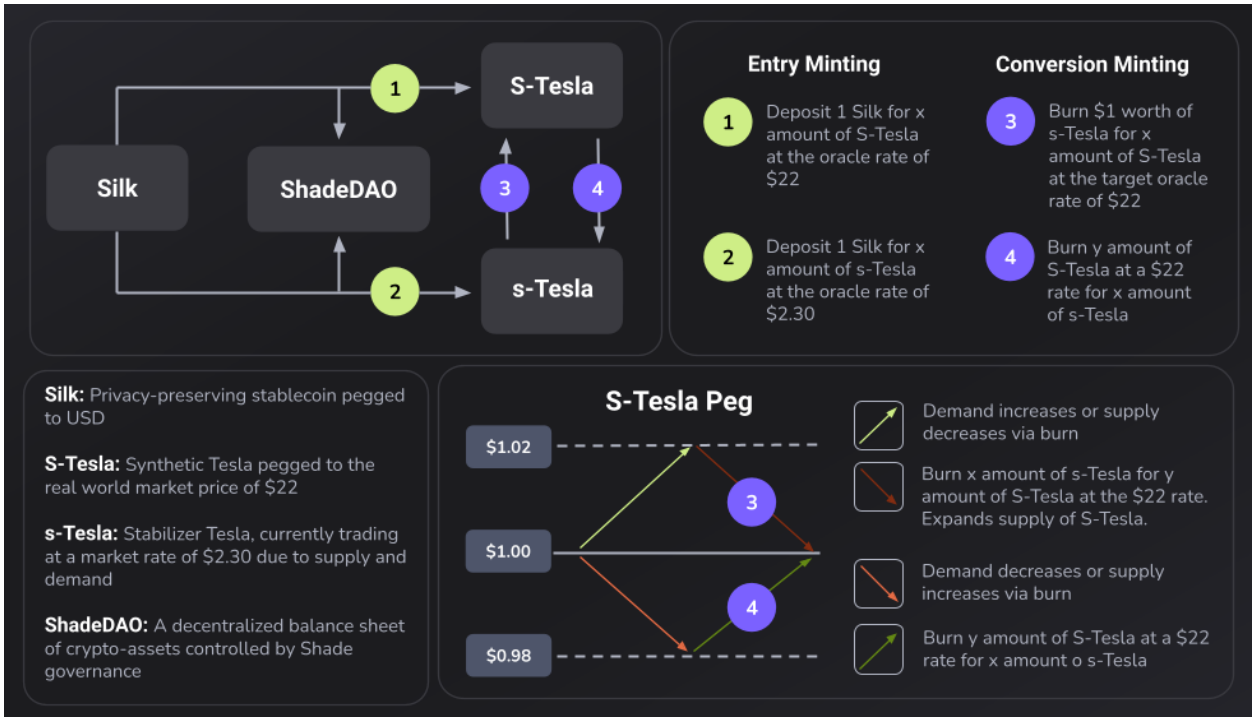
Generalization of the Silk/Shade peg mechanisms means that any real world value can be tied to a synthetic token that tracks its value as long as there is a stabilizer token that can respectively balance it. The value of the stabilizer token is determined by the free market and is ultimately a reflection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



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.[11]

[11] See "Entry Dilution Attack" in the Silk Whitepaper

Minting Examples



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.

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

shade

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.

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

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, a % of assets from the burn-based entry will be sent to the Shade Treasury. 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.

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].

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 communities' 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 the respective 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 Company, 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).

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. 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 stabilise 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 - 100 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.