

Overview

Shadows Network is a Polkadot parachain based on Substrate, focusing on the decentralized synthetic asset issuance. As long as you think valuable assets can be synthesized on the chain through the Shadows Network. These synthetic assets are guaranteed by the Shadows network pass **DOS**. As long as the DOS is locked, synthetic assets (**SyAs**) can be issued. This pooled collateral model allows users to directly perform conversions between synthesizers, avoiding the need for counterparties. This mechanism solves the liquidity and slippage issues experienced by DEX's. Shadows will support synthetic fiat currencies, cryptocurrencies (long and short) and commodities. Based on the user's contribution, the system will proportionally pay the transaction fees generated in the **Shadows.Exchange** to the token holders who participate in staking DOS to issue SyAs, thereby encouraging users to hold locked DOS. The value of DOS comes from the right to use the Shadows platform and the synthetic asset transaction fees it generates. But trading on Shadows.Exchange does not require holding DOS.

The shadows network will strive to become one of the Polkadot parachains by participating in the parachain slot auction. However, even if the slot usage rights are not successfully obtained by then, the shadows network will also be counted as parathreads to obtain cross-chain capabilities.

DOS as collateral

How DOS backs synthetic asset

All synthetic assets are backed by DOS tokens. Synthetic assets are minted when DOS holders stake their DOS as collateral. Synthetic assets are currently backed by a 750% collateralisation ratio, although this may be raised or lowered in the future through community governance mechanisms. The DOS mortgagor will incur debts when minting SyAs. To exit the system and unlock its DOS, the debt must be repaid by destroying SyAs.

Shadows V2 will support DOT, BTC, and ETH as collateral through cross-chain. This means that traders can use DOT, BTC, ETH to borrow SyAs and start trading immediately. Mortgage DOT, BTC, ETH requires a minimum mortgage ratio of 160%, and generates debt denominated in DOT, BTC, ETH.

Why DOS holders stake

DOS holders are incentivised to stake their tokens and mint synthetic assets in several ways.

1. here are exchange rewards. These are generated whenever someone exchanges one synthetic asset to another. Each trade generates an exchange fee that is sent to a fee pool, available for DOS stakers to claim their proportion each week. This fee is between 10-100 bps (0.1% - 1%, though typically 0.3%).
2. Synthetic asset rewards. Users who participate in the casting of SyAs can receive DOS rewards, which will be distributed to DOS stakers whose DOS mortgage rate is not lower

than the target threshold in proportion to each week.

3. Staking rewards. Users who hold DOS and participate in staking can get DOS rewards, which are distributed proportionally once a week. The required DOS comes from the inflation policy, and the terminal inflation of DOS is 2.5% per year. The initial supply of DOS is 100,000,000.
4. Governance. DOS token holders have the right to vote on the agreement, such as new feature additions, protocol upgrades and repairs.

Minting, burning, and the C-Ratio

The mechanisms above ensure DOS stakers are incentivised to maintain their Collateralisation Ratio (C-Ratio) at the optimal rate (currently 800%). This ensures synthetic asset are backed by sufficient collateral to absorb large price shocks. If the value of DOS or synthetic asset fluctuate, each staker's C-Ratio will fluctuate. If it falls below 800% (although there is a small buffer allowing for minor fluctuations), they will be unable to claim fees until they restore their ratio. They adjust their ratio by either minting synthetic asset if their ratio is above 800%, or burning Synths if their ratio is below 800%.

Stakers, debt, and pooled counterparties

DOS stakers incur a 'debt' when they mint synthetic asset. This debt can increase or decrease independent of their original minted value, based on the exchange rates and supply of synthetic asset within the network. For example, if 100% of the synthetic asset in the system were synthetic gold (xGOLD), which halved in price, the debt in the system would halve, and each staker's debt would also halve. This means in another scenario, where only half the Synths across the system were xGOLD, and xGOLD doubled in price, the system's total debt—and each staker's debt—would increase by one quarter.

In this way, DOS stakers act as a pooled counterparty to all synthetic asset exchanges; stakers take on the risk of the overall debt in the system. They have the option of hedging this risk by taking positions external to the system. By incurring this risk and enabling trading on Shadows.Exchange stakers earn a right to fees generated by the system.

Example:

	Alice	Bruce	Total Debt
Step 1. Staking xUSD	50000	50000	100000
Step 2. (xGOLD,xUSD)	(50000,0)	(0,50000)	100000
Step 3. (xGOLD,xUSD)	(75000,0)	(0,50000)	125000
Step 3. (Final,Debt Owed)	(75000,62500)	(50000,62500)	125000
Net Profile	12500	-12500	

Step 1. Alice & Bruce start with 50k xUSD , and the total debt of the network is equal to 100k. Among them, Both and Yan respectively Alice 50%.

Step 2. Alice purchases xGOLD with his 50K while Bruce continues to hold xUSD.

Step 3. The price of GOLD rises +50%, which means that the value of Alice's position has become 75k, of which the profit of 25k brings the network's total debt to 125k.

Step 4. Alice and Bruce still each bear 50% of the total network debt, which is 62.5k each. When Alice's xGOLD value subtracts his debt, he can make a profit of 12.5k, even if Bruce's position is valued at 50k, his debt has increased by 12.5k, which is a loss of 12.5k.

SyAs Pegging Mechanism

The Synth peg is critical to a well functioning system, because traders require both liquidity and stability between a Synth/s and other cryptoassets in order to take profits from trading. Some Synths trade on the open market, so it is possible for them to fall below par with the assets they track. Incentives are required to ensure that deviations from the peg are minimal and that actors are motivated to correct them.

There are three methods to maintain the Synth peg:

- **Arbitrage:** DOS stakers have created debt by minting Synths, so if the peg drops they can now profit by buying xUSD back below par and burning it to reduce their debt, as the Shaddows system always values 1 xUSD at \$1 USD.
- **DOT liquidity pool on DEX:** each week, a portion of the DOS added to the total supply through the inflationary monetary policy is distributed as reward to people providing sETH/ETH liquidity on DEX. This has incentivised liquidity providers to collectively create the largest liquidity pool on DEX, allowing traders to purchase Synths to start trading or sell Synths to take profits.
- **DOS auction:** Shadows is currently trialling a new mechanism with the dFusion protocol (from Gnosis) in which discounted DOS is sold at auction for DOT, which is then used to purchase Synths below the peg.

Shadows.Exchange

Why trade synthetic assets?

Synthetic assets provide exposure to an asset without holding the underlying resource. This has a range of advantages, including reducing the friction when switching between different assets (e.g. from Tesla shares to synthetic gold), expanding the accessibility of certain assets, and censorship resistance.

Advantages of Shadows.Exchange

Trading on Shadows.Exchange provides many advantages over centralised exchanges and order book based DEX's. The lack of an order book means all trades are executed against the contract, known as P2C (peer-to-contract) trading. Assets are assigned an exchange rate through price feeds supplied by Off-chain workers, and can be converted using the Shadows.Exchange dApp. This provides infinite liquidity up to the total amount of collateral in the system, zero slippage, and permissionless on-chain trading.

Cross-chain

The Shadows Network will operate as a Polkadot parachain (parallel threads). Therefore, compared to the synthetic asset agreement between Ethereum and EOS, Shadows will have cross-chain compatibility. The ability to provide cross-chain asset mortgage, for example, users can mortgage BTC, ETH to cast synthetic assets, which is a huge advantage. Cross-chain compatibility has opened the way for us to reach new markets and acquire new users.

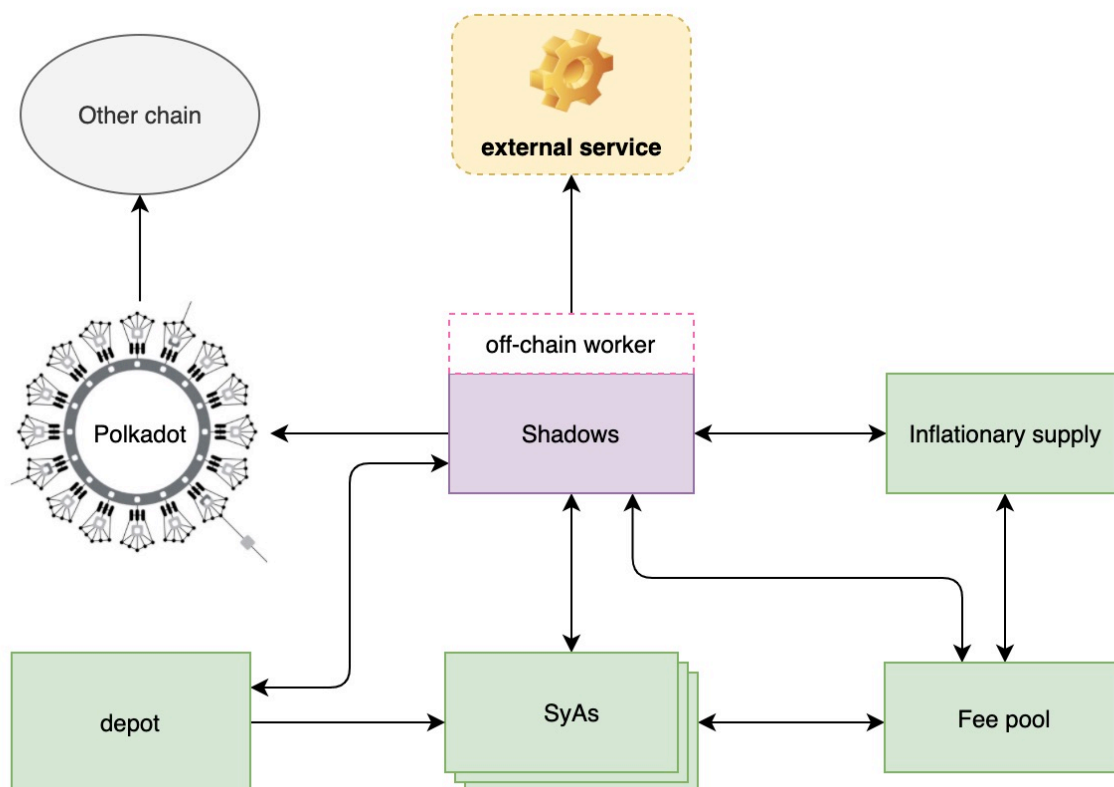
How SyAs work

SyAs are synthetic assets that track the price of the underlying asset. They allow holders to gain exposure on Polkadot to various asset classes without holding the underlying assets themselves or trusting a custodian. SyAs are backed by the Shadows Network Token (DOS), which is staked as collateral at a ratio of 800%.

SyAs Categories

The first batch will support five types of synthetic assets: fiat currencies, commodities, cryptocurrencies, inverse cryptocurrencies, and cryptocurrency indexes. Our fiat SyAs is xUSD. our commodity SyAs include synthetic gold and synthetic silver, both measured per ounce. our cryptocurrencies include sBTC, sETH, and sDOT, with more to come. and our Inverse SyAs inversely track the price of those available cryptocurrencies, meaning that when DOT's price decreases, iDOT's price increases. cryptocurrency indexes are sDEFI and sCEX (and their inverses), which respectively track a basket of DeFi assets and a basket of centralised exchange tokens.

System Architecture



Minting SyAs

An DOS holder can mint xUSD by locking their DOS as collateral. The steps involved when an DOS holder mints are:

- The Shadows contract checks that the DOS staker can mint SyAs against their DOS, which requires their Collateralisation Ratio to be below 800%.
- Their debt is added to the Debt Register. The debt is the amount of the new value minted, and is stored in xUSD
- With the debt assigned to the staker, the Shadows contract instructs the xUSD contract to issue the new amount. It adds it to its total supply and assigns the newly minted xUSD to the user's wallet.

If the price of DOS increases, an equivalent portion of a staker's DOS is automatically unlocked as collateral. For example, if a user locks \$100 of DOS as collateral, and the value of DOS doubles, then half of their DOS (total value: \$200) is locked and the other half is unlocked. If they wish, that extra unlocked DOS can then be staked to mint more xUSD.

Exchanges

The steps involved for the shadows to process a Synth exchange (from xUSD to xBTC in this example) are below:

- Burn the source SyAs (xUSD), which involves reducing that wallet address's xUSD balance and updating the total supply of xUSD.
- Establish the conversion amount (i.e. the exchange rate, based on the price of each currency).
- Charge an exchange fee, which is currently 0.3% of the converted amount, and send the fee as xUSD to the fee pool, where it can be claimed by DOS stakers.
- The remaining 99.7% is issued by the destination SyAs (xBTC) contract and the wallet address balance is updated
- The xBTC total supply is updated.

No counterparty is required to exchange, as the system converts the debt from one SyAs to another. Hence no order books or order matching is required, resulting in infinite liquidity between SyAs. No debt change is required to be recorded against the debt pool either, as the same value is burned from the source SyAs and minted from the destination SyAs.

Claiming Fees

When SyAs are exchanged through the Shadows contract, a 0.3% fee is extracted and sent to the fee pool to be claimed by DOS stakers. When claiming fees (also called SyAs exchange rewards) a staker also claims their DOS staking rewards, which reward them with extra DOS for staking the DOS they currently have. The shadows extrinsics' process once a staker requests to claim their fees is as follows:

- The fee pool checks whether there are fees currently available and whether the staker is eligible to receive fees.
- The amount of fees in xUSD is sent to the staker's wallet address and the balance of the fee pool is updated.
- Additionally, a pro-rata amount of escrowed DOS is assigned to the wallet address from the DOS staking rewards contract.

Fees are allocated based on the proportion of debt each staker has issued. For example, if a staker has issued 1,000 xUSD in debt, the debt pool is 10,000 xUSD, and 100 in fees are generated in a fee period, this staker is entitled to 10 xUSD because their debt represents 10% of the debt pool. The same proportional distribution mechanism is used for DOS staking rewards.

Burning debt

When an DOS staker wants to exit the system or reduce their debt and unlock staked DOS, they must pay back their debt. At its simplest: a staker mints 10 xUSD by locking DOS as collateral, and must burn 10 xUSD to unlock it. But if the debt pool fluctuates (and therefore their individual debt fluctuates) while they are staked, they may need to burn more or less debt than they minted. The process for reducing debt to zero is as follows:

- The Shadows contract determines their debt balance and removes them from the Debt Register.
- The required amount of xUSD is burned, and total supply of xUSD is updated along with the xUSD balance in the user's wallet.
- Their DOS balance becomes transferrable.

The debt pool

The system tracks the debt pool (as well as each individual staker's debt) each time an DOS holder mints or burns Synths. It does this by updating the Cumulative Debt Delta Ratio. This measures the DOS staker's proportion of the debt pool at the time they last minted or burned, as well as the debt change caused by other stakers entering or leaving the system. The system uses this information to determine the individual debt of each staker at any time in the future, without having to actually record the changing debt of each individual staker.

Updating the Cumulative Debt Delta Ratio on the Debt Register allows the system to track every user's % of the debt. It calculates the % change the new debt introduces against the debt pool using the formula below and appends it to the Debt Register:

$$\text{New Debt Minted} / (\text{Total Existing Debt} + \text{New Debt})$$

The staker's last mint/burn action is then recorded in the Debt Register within their issuance data and the relative index number at which this action happened. The detail recorded is the percentage of the debt pool they represent, which is calculated by this formula:

$$\text{User debt percentage} = (\text{New Debt} + \text{Existing Debt}) / (\text{Previous Debt Pool} + \text{New Debt})$$

The Debt Register holds the Cumulative Debt Delta Ratio, which is the product of the calculation above, and the relative time (index) the debt was added, so that it can be used to calculate any user's % of the debt pool at any index in the future based on the % shift in the debt pool their last mint/burn caused.

We recalculate the debt pool by summing the number of tokens in each Shadows contract multiplied by the current exchange rates, each time new debt is issued/burned:

```
totalDebtIssued = totalIssuedSyAs
```

This enables the calculation of the current debt pool, and is included in the updated Cumulative Debt Delta Ratio so that we know at each Debt Register entry the size of the debt (in SyAs).

When a staker pays back their debt (i.e. by burning the SyAs they minted) to unlock their DOS collateral the system updates the Cumulative Debt Delta based on the % shift in the amount of debt to be burned against the total value of the system's debt after the reduction in debt.

This is the inverse calculation from when a user mints new debt:

```
user's new debt percentage = (existing debt - debt to be burned) / (debt pool - debt to be burned)
```

This is the formula for calculating the updated Cumulative Debt Delta:

```
delta = debt to be burned / (debt pool - debt to be burned)
```

If a staker burns all their debt, their issuance data in the Debt Register will be set to 0 and they will no longer be part of the debt pool.

Liquidation

If the staker's position drops below 800%, the staker will not be able to claim transaction rewards. At the same time, in order to avoid systemic risks, we have also introduced liquidation. When the staker's position is lower than 750%, the system will prompt the liquidation risk. If the position has not been increased for a period of time, the collateral will be liquidated. Here is the introduction of "deposit liveness period": staker can add positions during the active period (such as 1 hour) to avoid liquidation. But if after the active period ends, if the staker's position is still below 750%, any DOS holder can initiate liquidation of the collateral at this time. After the liquidation is successful, the liquidator can obtain a certain amount of income from it.

Ingestor

Ingestor is our implementation of Off-chain workers. The prices of all synthetic assets in the Shadows system need to query and/or process off-chain data before it can be included in the on-chain state. The conventional way of doing this is through oracles. Oracles are external services that typically listen to blockchain events and trigger tasks accordingly. When these tasks complete, their results are submitted back to the blockchain using transactions. While this approach works, it still has several flaws with respect to security, scalability, and infrastructure efficiency.

To make the off-chain data integration secure and more efficient, We use Substrate off-chain workers. The off-chain worker subsystem allows execution of long-running and possibly non-deterministic tasks (e.g. web requests, encryption/decryption and signing of data, random number generation, CPU-intensive computations, enumeration/aggregation of on-chain data, etc.) that could otherwise require longer than the block execution time.

For specific details about off-chain workers, can refer to:

Future Functionality & Conclusion

There are many different kinds of SyAs that can be added to the system to provide greater utility to Shadows.Exchange. These include leveraged assets that are not available on other platforms as well as indices like the S&P500 and equities like APPLE and TSLA.

Shadows may be one of the most complex and useful protocols in Polkadot ecology. We hope that through Substrate's excellent system architecture and the powerful cross-chain capabilities provided by Polkadot, the current pain points of asset on-chain can be solved. Make great contributions to the implementation of blockchain applications and the construction of web3.0.