

ONS Coin Whitepaper

Version: 1 (March 2021)

Abstract

Ons Coin is a decentralised synthetic asset issuance protocol built on Ethereum. These synthetic assets are collateralized by the Ons Coin (ONS) which when locked in the contract enables the issuance of synthetic assets (Synths). This pooled collateral model enables users to perform conversions between Synths directly with the smart contract, avoiding the need for counterparties. This mechanism solves the liquidity and slippage issues experienced by DEX's. Ons Coin currently supports synthetic fiat currencies, cryptocurrencies (long and short) and commodities. ONS holders are incentivised to stake their tokens as they are paid a pro-rata portion of the fees generated through activity on Ons Coin Exchange, based on their contribution to the network. It is the right to participate in the network and capture fees generated from Synth exchanges, from which the value of the ONS token is derived. Trading on Ons Coin Exchange does not require the trader to hold ONS.

ONS as collateral

How ONS backs Synths

All Synths are backed by ONS tokens. Synths are minted when ONS holders stake their ONS as collateral using Mintr, a decentralised application for interacting with the Ons Coin contracts. Synths are currently backed by a 750% collateralisation ratio, although this may be raised or lowered in the future through community governance mechanisms. ONS stakers incur debt when they mint Synths, and to exit the system (i.e. unlock their ONS) they must pay back this debt by burning Synths.

Ons Coin is also currently trialling Ether as an alternative form of collateral. This means traders can borrow Synths against their ETH and begin trading immediately, rather than needing to sell their ETH. Staking ETH requires a collateralisation ratio of 150% and creates a debt denominated in ETH, so ETH stakers mint sETH rather than sUSD and do not participate in the 'pooled debt' aspect of the system. In this model, ETH stakers do not receive fees or rewards as they take no risk for the debt pool.

Why ONS holders stake

ONS holders are incentivised to stake their tokens and mint Synths in several ways. Firstly, there are exchange rewards. These are generated whenever someone exchanges one Synth to another (i.e. on Ons Coin Exchange). Each trade generates an exchange fee that is sent to a fee pool, available for ONS stakers to claim their proportion each week. This fee is between 10-100 bps (0.1% - 1%, though typically 0.3%), and will be displayed during any trade on Ons Coin Exchange. The other incentive for ONS holders to stake/mint is ONS staking rewards, which comes from the protocol's inflationary monetary policy. From March 2019 to August 2023, the total ONS supply will increase from 100,000,000 to 260,263,816, with a weekly decay rate of 1.25% (from December 2019). From September 2023, there will be an annual 2.5% terminal inflation for perpetuity. These ONS tokens are distributed to ONS stakers weekly on a pro-rata basis provided their collateralisation ratio does not fall below the target threshold.

Minting, burning, and the C-Ratio

The mechanisms above ensure ONS stakers are incentivised to maintain their Collateralisation Ratio (C-Ratio) at the optimal rate (currently 750%). This ensures Synths are backed by sufficient collateral to absorb large price shocks. If the value of ONS or Synths fluctuate, each staker's C Ratio will fluctuate. If it falls below 750% (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 Synths if their ratio is above 750%, or burning Synths if their ratio is below 750%.

Stakers, debt, and pooled counterparties

ONS stakers incur a 'debt' when they mint Synths. This debt can increase or decrease independent of their original minted value, based on the exchange rates and supply of Synths within the network. For example, if 100% of the Synths in the system were synthetic Bitcoin (sBTC), 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 sBTC, and BTC doubled in price, the system's total debt—and each staker's debt—would increase by one quarter. In this way, ONS stakers act as a pooled counterparty to all Synth 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 Ons Coin Exchange stakers earn a right to fees generated by the system.

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

Ons Coin 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 Apple shares to synthetic gold), expanding the accessibility of certain assets, and censorship resistance.

Advantages of Ons Coin Exchange

Trading on Ons Coin 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 an oracle, and can be converted using the Ons Coin Exchange dApp. This provides infinite liquidity up to the total amount of collateral in the system, zero slippage, and permissionless on-chain trading.

How Synths work

Synths are synthetic assets that track the price of the underlying asset. They allow holders to gain exposure on Ethereum to various asset classes without holding the underlying assets themselves or trusting a custodian. Synths are backed by the Ons Coin (ONS), which is staked as collateral at a ratio of 750%.

The current Synths

There are currently five categories of Synths available: fiat currencies, commodities, cryptocurrencies, inverse cryptocurrencies, and cryptocurrency indexes. Our fiat Synths include sUSD, sEUR, sKRW, and many more; our commodity Synths include synthetic gold and synthetic silver, both measured per ounce; our cryptocurrencies include sBTC, sETH, and sBNB, with more to come; and our Inverse Synths inversely track the price of those available cryptocurrencies, meaning that when BTC's price decreases, iBTC's price increases. Our current 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 Synths

An ONS holder can mint sUSD by locking their ONS as collateral via the Ons Coin smart contract. The steps involved when an ONS holder mints are:

- The Ons Coin contract checks that the ONS staker can mint Synths against their ONS, which requires their Collateralisation Ratio to be below 750%.
- Their debt is added to the Debt Register. The debt is the amount of the new value minted, and is stored in sUSD
- With the debt assigned to the staker, the Ons Coin contract instructs the sUSD contract to issue the new amount. It adds it to its total supply and assigns the newly minted sUSD to the user's wallet.

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

Exchanges

The steps involved for the smart contracts to process a Synth exchange (from sUSD to sBTC in this example) are below:

- Burn the source Synth (sUSD), which involves reducing that wallet address's sUSD balance and updating the total supply of sUSD.
- 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 sUSD to the fee pool, where it can be claimed by ONS stakers.
- The remaining 99.7% is issued by the destination Synth (sBTC) contract and the wallet address balance is updated

- The sBTC total supply is updated.

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

Claiming Fees

When Synths are exchanged through the Ons Coin contract, a 0.3% fee is extracted and sent to the fee pool to be claimed by ONS stakers. When claiming fees (also called Synth exchange rewards) a staker also claims their ONS staking rewards, which reward them with extra ONS for staking the ONS they currently have. The smart contracts' 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 sUSD is sent to the staker's wallet address and the balance of the fee pool is updated.
- Additionally, a pro-rata amount of escrowed ONS is assigned to the wallet address from the ONS 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 sUSD in debt, the debt pool is 10,000 sUSD, and 100 in fees are generated in a fee period, this staker is entitled to 10 sUSD because their debt represents 10% of the debt pool. The same proportional distribution mechanism is used for ONS staking rewards.

Burning debt

When an ONS staker wants to exit the system or reduce their debt and unlock staked ONS, they must pay back their debt. At its simplest: a staker mints 10 sUSD by locking ONS as collateral, and must burn 10 sUSD 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 Ons Coin contract determines their debt balance and removes them from the Debt Register.
- The required amount of sUSD is burned, and total supply of sUSD is updated along with the sUSD balance in the user's wallet.
- Their ONS balance becomes transferrable.

The debt pool

The system tracks the debt pool (as well as each individual staker's debt) each time an ONS holder mints or burns Synths. It does this by updating the Cumulative Debt Delta Ratio. This measures the ONS 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:

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

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 Synth contract multiplied by the current exchange rates, each time new debt is issued/burned:

$$\text{totalDebtIssued} = \text{totalIssuedSynths}$$

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 Synths).

When a staker pays back their debt (i.e. by burning the Synths they minted) to unlock their ONS 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:

$$\text{user's new debt percentage} = \frac{(\text{existing debt} - \text{debt to be burned})}{(\text{debt pool} - \text{debt to be burned})}$$

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

$$\text{delta} = \text{debt to be burned} / (\text{debt pool} - \text{debt to be burned})$$

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.

The oracle

The value of all synthetic assets in the Ons Coin system are currently determined by oracles that push price feeds on-chain. It uses an algorithm with a variety of sources to form an aggregate value for each asset. The price feeds are currently supplied by both Chainlink's independent node operators and Ons Coin, and will soon all be supplied by Chainlink.

Current Risks and Risk Mitigation Strategies

Current risks

There are several risks in the current architecture, as Ons Coin is still an experimental system and complex systems require both empirical observations and theoretical analysis. Empirical observation and theoretical analysis ensure the mechanism design aligns incentives for all players.

One risk involves the debt ONS holders issue when they stake their ONS and mint Synths. As previously explained, this debt can fluctuate due to exchange rate shifts within the system. This means that to exit the system and unlock their staked ONS, they may need to burn more Synths than they originally minted.

Most people in the cryptocurrency space are aware of this risk, but the prices of most cryptoassets are highly correlated to Bitcoin and/or Ethereum. This means it's possible for major price fluctuations in the ONS token to occur for reasons that have little to do with ONS or the Ons Coin system.

Finally, there are a number of aspects of the system that are currently centralised. This decision has been made to ensure efficient implementation of the project. One example of centralisation is the use of proxy contracts across much of the architecture. This is to ensure the system can be upgraded easily but confers a level of control to the engineering team which requires trust from users. While these aspects will be phased out over time, it is important to understand the risks inherent in the current system architecture.

Risk mitigation strategies

As a decentralised protocol, the Ons Coin team is committed to decentralisation and censorship resistance — this will be a gradual process as the system matures. This includes crucial areas such as our price feeds. We have previously announced a partnership with Chainlink, a provider of decentralised oracle solutions.

Another important area is governance, we have recently initiated regular community governance calls to ensure the project's goals are aligned with the community. Another aspect of this process is a move to a formal change management process, we have introduced SIP's (Ons Coin Improvement Proposals) to allow the community to introduce change requests and to ensure that any changes to the system are well understood and considered by all stakeholders.

Future Functionality

Additional Synths

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

Synthetic futures

We expect to launch the ability for traders to take synthetic futures on Ons Coin Exchange in the near future. Many aspects of this functionality are yet to be finalised, but it's expected it will use a self balancing mechanism similar to the Uniswap auto market maker algorithm, where the total open interest of each position and therefore the risk to ONS stakers is capped and borrow rates are adjusted based on the current open interest. The system will also encourage traders to balance the risk in the system by paying a percentage of the fees to traders who rebalance positions, though this feature will not be in the initial release. There are already a number of derivatives trading platforms for cryptoassets, but they are all limited by counterparty liquidity. The unique design of the Ons Coin system means it may be able to capture market share in this area, similarly to how Binance captured market share by listing more cryptoassets than most other centralised exchanges.

Leveraged trading

Leveraged trading drives a significant amount of volume on crypto exchanges, and while synthetic futures will compete directly with centralised futures platforms, there is a lot of value in supporting tokenised leverage.

Advanced order types

The current version of Ons Coin Exchange supports only market orders which limits the usability of the exchange. An advanced order engine will be able to support limit, stop loss, stop limits, and other advanced order types. This will use a relay network for processing advanced orders. Advanced order types are critical to reaching feature parity with centralised exchanges.

Conclusion

Ons Coin has already delivered one of the most complex and useful protocols built on Ethereum to date. But the potential for censorship-resistant synthetic assets is still largely untapped. Further improvements to the mechanism as well as functional upgrades and new Synths will vastly increase the utility of the platform. Movement to a decentralised governance process will also reduce systemic risk and increase the long term viability of the project.