"The Sky Protocol: Sky's Multi-Collateral Dai (MCD) System"

Introduction

Beginning in 2015, the Sky project (formerly known as MakerDAO) operated with developers around the globe working together on the first iterations of code, architecture, and documentation. In December 2017, the first formal white paper was published, introducing the original Dai (now Sai) Stablecoin System.

The white paper described how anyone could generate Dai using that system by leveraging Ethereum (ETH) as collateral through unique smart contracts known as Collateralized Debt Positions (CDPs). Given that ETH was the only collateral asset accepted by the system, the Dai generated was called Single-Collateral Dai (SCD), or Sai. That white paper also included a plan to upgrade the system to support multiple collateral asset types in addition to ETH. What was then an intention, became a reality in November 2019.

Since November 2019, further development of the Sky ecosystem has occurred in a decentralized manner. Sky governance has been developing its strategy for the project, while an ever-evolving contributor base spanning multiple autonomous teams across the globe have contributed work. Given the distributed nature of the project, the scope of this white paper is limited to the low-level core system components like the MCD system (also known as MCD), the Dai and USDS stablecoins, and vaults. Most of this white paper was written in 2019.

An Overview of the Sky Protocol and Its Features

The Sky Protocol

The Sky Protocol is one of the largest dapps on the Ethereum blockchain. Designed by a disparate group of contributors, including developers within the Maker Foundation, its outside partners, and other persons and entities, it is the first decentralized finance (DeFi) application to see significant adoption.

The Sky Protocol is managed by people around the world who hold its governance token, MKR. Through a system of scientific governance involving Executive Voting and Governance Polling, Sky Ecosystem Governance govern the Protocol and the financial risks of Dai to ensure its stability, transparency, and efficiency. One MKR token locked in a voting contractThe voting contract assures that MKR owners can vote with the full weight of the MKR they stake. equals one vote.

The Dai Stablecoin

The Dai stablecoin is a decentralized, unbiased, collateral-backed cryptocurrency soft-pegged to the US Dollar. Dai is held in cryptocurrency walletsA cryptocurrency wallet is a tool used to manage crypto assets and to interact with decentralized apps (dapps). In a crypto wallet, users can see a list of their coins and tokens, view their balances and transaction history, and make transfers. or within platforms, and is supported on Ethereum and other popular blockchains.

Dai is easy to generate, access, and use. Users generate Dai by depositing collateral assets into Sky Protocol VaultsSky Protocol Vaults facilitate the generation of Dai against locked-up collateral. Users open Vaults via the Oasis Borrow dashboard or one of many other user interfaces that allow management of Vault operations. within the Sky Protocol. This is how Dai is entered into circulation and how users gain access to liquidity. Others obtain Dai by buying it from brokers or exchanges, or simply by receiving it as a means of payment.

Once generated, bought, or received, Dai can be used in the same manner as any other cryptocurrency: it can be sent to others, used as payments for goods and services, and even held as savings through a feature of the Sky Protocol called the Dai Savings RateThe Dai Savings Rate (DSR) allows all Dai holders to earn savings automatically and natively by locking their Dai into the DSR contract. The DSR enables greater utility for Dai holders, which may include cryptocurrency traders, startups, and established businesses. (DSR).

Every Dai in circulation is directly backed by excess collateral, meaning that the value of the collateral is higher than the value of the Dai debt, and all Dai transactions are publicly viewable on the Ethereum blockchain.

What Properties of Dai Function Similarly to Money?

Generally, money has four functions:

1. A store of value
2. A medium of exchange
3. A unit of account
4. A standard of deferred payment

Dai has properties and use cases designed to serve these functions.

Dai as a Store of Value

A store of value is an asset that keeps its value without significant depreciation over time. Because Dai is a stablecoin, it is designed to function as a store of value even in a volatile market.

Dai as a Medium of Exchange

A medium of exchange is anything that represents a standard of value and is used to facilitate the sale, purchase, or exchange (trade) of goods or services. The Dai stablecoin is used around the world for all types of transactional purposes.

Dai as a Unit of Account

A unit of account is a standardized measurement of value used to price goods and services (e.g., USD, EUR, YEN). Currently, Dai has a target price of 1USD (1 Dai = 1 USD). While Dai is not used as a standard measurement of value in the off-chain world, it functions as a unit of account within the Sky Protocol and some blockchain dapps, whereby Sky Protocol accounting or pricing of dapp services is in Dai rather than a fiat currency like USD.

Archived copy · cryp2nova.com

Dai as a Standard of Deferred Payment

Dai is used to settle debts within the Sky Protocol (e.g., users use Dai to pay the stability fee and close their Vaults). This benefit separates Dai from other stablecoins.

Collateral Assets

Dai is generated, backed, and kept stable through collateral assets that are deposited into Sky Protocol Vaults on the Sky Protocol. A collateral asset is a digital asset that Sky Ecosystem Governance have voted to accept into the Protocol.

To generate Dai, the Sky Protocol accepts as collateral any Ethereum-based asset that has been approved by Sky Ecosystem Governance. Sky Ecosystem Governance must also approve specific, corresponding Risk Parameters for each accepted collateral (e.g., more stable assets might get more lenient Risk Parameters, while more risky assets could get stricter Risk Parameters). Detailed information on Risk Parameters is below. These and other decisions of Sky Ecosystem Governance are made through the Sky Protocol decentralized governance process.

The USDS Stablecoin

Introduction

In 2024, MakerDAO rebranded to Sky Ecosystem and launched a range of new products including a new stablecoin called USDS. USDS is similar to the pre-existing Dai stablecoin, in the sense that it's a decentralized, unbiased, collateral-backed cryptocurrency soft-pegged to the US Dollar. Technically, USDS is an IOU token on the Ethereum blockchain representing a collateralized balance in the MCD protocol's 'vat' smart contract—just like the Dai stablecoin.

How is it different?

Although USDS aims to fulfil the same use-case as DAI, it does have a few differences. To ensure USDS can safely reach global scale, it may eventually be upgraded to include a freeze function similar to the industry standard of other major RWA-backed stablecoins if the decentralized governance of Sky decides so. The freeze function is **not yet implemented**, but the token deployment is proxy upgradeable (using the ERC1967Proxy standard) so that it can later be implemented through a decentralized governance vote by the Sky Ecosystem.

The potential freeze functionality upgrade would be subject to careful community deliberation and could be designed to align with legal frameworks from jurisdictions where Sky may seek to establish effective enforcement mechanisms for RWA collateral. This will result in a much greater level of security, stability and reliability of using large scale RWA collateral for USDS as it scales to global mass market adoption.

The consideration and potential implementation timeline for any freeze functionality would align with USDS's organic growth trajectory, potentially spanning months or years. Should such functionality be developed, it would be designed to harmonize and leverage the decentralized governance and transparent processes of the Sky Atlas (a comprehensive framework that outlines the governance, support, and stability mechanisms of the Sky ecosystem), to ensure it will be a risk-minimized process with checks and balances. This could include unique features such as a decentralized appeals process that would ensure all potentially controversial cases of a freeze being done are processed in public, in a fully transparent way.

How to get USDS?

The USDS token launched alongside a converter contract,which allows for free and infinitely liquid conversions between DAI and USDS. USDS can also be acquired through the Sky Savings Rate (SSR), Sky Token Rewards (STR) and can be acquired on third party exchanges and DeFi protocols.

Sky Vaults

All accepted collateral assets can be leveraged to generate Dai in the Sky Protocol through smart contracts called Maker Vaults. Users can access the Sky Protocol and create Vaults through a number of different user interfaces (i.e., network access portals), including Oasis Borrow and various interfaces built by the community. Creating a Vault is not complicated, but generating Dai does create an obligation to repay the Dai, along with a Stability FeeThe Stability Fee is a fee paid by every Vault owner when debt is paid down or completely paid off. It is an annual percentage yield that is calculated on top of the existing Vault debt. Stability Fees must be paid in Dai only., in order to withdraw the collateral leveraged and locked inside a Vault.

Vaults are inherently non-custodial: Users interact with Vaults and the Sky Protocol directly, and each user has complete and independent control over their deposited collateral as long the value of that collateral doesn't fall below the required minimum level (the Liquidation Ratio, discussed in detail below).

Interacting with a Sky Protocol Vault

- **Step 1: Create and Collateralize a Vault**

  A user creates a Vault via the Oasis Borrow portal or a community-created interface, such as Instadapp, Zerion, or MyEtherWallet, by funding it with a specific type and amount of collateral that will be used to generate Dai. Once funded, a Vault is considered collateralized.

- **Step 2: Generate Dai from the Collateralized Vault**

  The Vault owner initiates a transaction, and then confirms it in her unhosted cryptocurrency wallet in order to generate a specific amount of Dai in exchange for keeping her collateral locked in the Vault.

- **Step 3: Pay Down the Debt and the Stability Fee**

  To retrieve a portion or all of the collateral, a Vault owner must pay down or completely pay back the Dai she generated, plus the Stability Fee that continuously accrues on the Dai outstanding. The Stability Fee can only be paid in Dai.

- **Step 4: Withdraw Collateral**

  With the Dai returned and the Stability Fee paid, the Vault owner can withdraw all or some of her collateral back to her wallet. Once all Dai is completely returned and all collateral is retrieved, the Vault remains empty until the owner chooses to make another deposit.

Importantly, each collateral asset deposited requires its own Vault. So, some users will own multiple Vaults with different types of collateral and levels of collateralization.

Archived copy · cryp2nova.com

Liquidation of Risky Sky Vaults

To ensure there is always enough collateral in the Sky Protocol to cover the value of all outstanding debt (the amount of Dai outstanding valued at the Target PriceThe Target Price for Dai is 1 USD, translating to a 1:1 USD soft peg.), any Sky Protocol Vault deemed too risky (according to parameters established by Sky Governance) is liquidated through automated Sky Protocol auctions. The Protocol makes the determination after comparing the Liquidation RatioThe Liquidation Ratio is the collateral-to-debt ratio at which a Vault becomes vulnerable to Liquidation. to the current collateral-to-debt ratio of a Vault. Each Vault type has its own Liquidation Ratio, and each ratio is determined by MKR voters based on the risk profile of the particular collateral asset type.

Sky Protocol Auctions

The auction mechanisms of the Sky Protocol enable the system to liquidate Vaults even when price information for the collateral is unavailable. At the point of liquidation, the Sky Protocol takes the liquidated Vault collateral and subsequently sells it using an internal market-based auction mechanism. This is a Collateral AuctionIn a Collateral Auction, the winning bidder pays Dai for collateral from a liquidated Vault. The Dai received is used to cover the Vault's outstanding debt, as well as the liquidation penalty..

The Dai received from the Collateral Auction is used to cover the Vault's outstanding obligations, including payment of the Liquidation PenaltyThe Liquidation Penalty is fee that is paid by Vault owners when their Vaults are Liquidated. fee set by MKR voters for that specific Vault collateral type.

If enough Dai is bid in the Collateral Auction to fully cover the Vault obligations plus the Liquidation Penalty, that auction converts to a Reverse Collateral AuctionIn a Reverse Auction, Keepers bid in decreasing amounts of collateral they are willing to accept for a fixed amount of Dai. This process is part of the Collateral Auction and will only be initiated if there is enough initial interest in the collateral to cover the Vault's outstanding Dai. Once enough Dai is bid to cover those obligations, then the Reverse Collateral Auction kicks in. The purpose of the Reverse Collateral Auction is to provide a process that best enables the Vault owner to recover as much leftover collateral as possible, while ensuring all outstanding Dai obligations are first met. in an attempt to sell as little collateral as possible. Any leftover collateral is returned to the original Vault owner.

If the Collateral Auction does not raise enough Dai to cover the Vault's outstanding obligation, the deficit is converted into Protocol debt. Protocol debt is covered by the Dai in the Sky Protocol BufferThe Sky Protocol Buffer contains the Dai proceeds from the Collateral Auction (including liquidation penalties), as well as the Stability Fees accrued on Vaults. When the amount of Dai in the Sky Protocol Buffer reaches a specific number (determined by Sky Governance) the surplus amount is put into a Surplus Auction and is used to buy and remove MKR from the total supply. The surplus amount is net of system debts, such as outstanding Vault obligations in the Collateral Auction and DSR accruals.. If there is not enough Dai in the Buffer, the Protocol triggers a Debt AuctionDebt Auctions are used to recapitalize the system by auctioning off MKR for a fixed amount of Dai.. During a Debt Auction, MKR is minted by the system (increasing the amount of MKR in circulation), and then sold to bidders for Dai.

Dai proceeds from the Collateral Auction go into the Sky Protocol Buffer, which serves as a buffer against an increase of MKR overall supply that could result from future uncovered Collateral Auctions and the accrual of the Dai Savings Rate (discussed in detail below).

If Dai proceeds from auctions and Stability Fee payments exceed the Sky Protocol Buffer limit (a number set by Sky Governance), they are sold through a Surplus AuctionIn a Surplus Auction, the winning bidder pays MKR for surplus Dai from stability fees. The MKR received is destroyed, thereby reducing the amount of MKR in circulation.. During a Surplus Auction, bidders compete by bidding increasing amounts of MKR to receive a fixed amount of Dai. Once the Surplus Auction has ended, the Sky Protocol autonomously destroys the MKR collected, thereby reducing the total MKR supply.

[[note]] |Example (Collateral Auction Process): |*A large Vault becomes undercollateralized due to market conditions. An |Auction KeeperAn Auction Keeper is a human or automated bot incentivized by the Sky Protocol to monitor the system and trigger liquidation when a Vault's Liquidation Ratio is breached. |then detects the undercollateralized Vault opportunity and initiates liquidation of the Vault, which kicks off a Collateral Auction for, say, 50 ETH.* | |*Each Auction Keeper has a |bidding modelA bidding model is the strategy behind when to bid, how often to bid, and at what price to bid. |to assist in winning auctions. A bidding model includes a price at which to bid for the collateral (ETH, in this example). The Auction Keeper uses the token price from its bidding model as the basis for its bids in the first phase of a Collateral Auction, where increasing Dai bids are placed for the set amount of collateral. This amount represents the price of the total Dai wanted from the collateral auction.* | |*Now, let's say the Auction Keeper bids 5,000 Dai for the 50 ETH to meet this amount. The Dai bid is transferred from the |Vault EngineThe Vault Engine is the VAT smart contract. For more info, go to https://docs.makerdao.com/other-documentation/system-glossary#vat-vault-engine . |to the Collateral Auction contract. With enough Dai in the Collateral Auction contract to cover the system's debt plus the Liquidation Penalty, the first phase of the Collateral Auction is over.* | |*In order to reach the price defined in its bidding model, the Auction Keeper submits a bid in the second phase of the Collateral Auction. In this phase, the objective is to return as much of the collateral to the Vault owner as the market will allow. The bids that the Auction Keepers place are for fixed Dai amounts and decreasing amounts of ETH. For instance, the bidding model of the Keeper in this example seeks a bid price of 125 Dai per ETH, so it offers 5000 Dai for 40 ETH. Additional Dai for this bid is transferred from the Vault Engine to the Collateral Auction contract. After the bid duration limit is reached and the bid expires, the Auction Keeper claims the winning bid and settles the completed Collateral Auction by collecting the won collateral.*

RWA Vaults

Introduction

Sky was one of the first projects in Decentralized Finance (DeFi) to introduce Real World Assets (RWA) as collateral to a stablecoin protocol.

About Real World Assets

Real World Assets (RWAs) are off-chain assets, such as real estate, loans, bonds, or commodities, that are tokenized for use in blockchain systems. They bridge the gap between traditional finance and decentralized finance (DeFi) by enabling these assets to be traded, used as collateral, or accessed more easily through digital means. RWAs bring stability, diversification, and liquidity to blockchain ecosystems but also require robust legal frameworks and mechanisms for accurate valuation and risk management.

How the vaults work

A **vault** in the Sky Protocol (specifically within its Multi-Collateral Dai system, or MCD) is a feature of the MCD system that allows users to lock up collateral assets and generate DAI. It is a core component of how the Sky Protocol functions, enabling users to leverage their assets while maintaining a decentralized and over-collateralized system for creating stablecoins. Traditional vaults exclusively deal with on-chain cryptocurrencies like ETH or WBTC, which are native to the blockchain, easily verifiable, and highly liquid. These assets enable the protocol to operate entirely on-chain, using automated smart contracts to manage collateralization, valuation, and liquidation processes with minimal external dependencies.

RWA vaults differ from traditional vaults primarily in the type of collateral they support and the mechanisms required to manage them. They are implemented as a set of predefined rules on how the vault is managed within the MCD system—this implementation is described in MIP21 as part of Sky's former MIP (Maker Improvement Proposal) framework. RWA vaults represent a protocol mechanism for interfacing with traditional financial instruments (ie. financial assets not natively issued on a blockchain and governed by off-chain legal agreements) and gaining exposure to them. The protocol's technical architecture enables governance-approved strategies for capital deployment into sovereign debt instruments and similar highly-rated securities, with returns accruing to the protocol's surplus buffer. These assets exist

Archived copy · cryp2nova.com

outside the blockchain and require tokenization to represent their value digitally. Managing RWA vaults involves more complex processes, which might include legal agreements to ensure enforceable claims on the underlying assets, reliance on third-party custodians and trustees to secure and manage these assets, and mechanisms to handle off-chain valuation and compliance. Unlike traditional vaults, which rely on decentralized oracles for near-instant price feeds for managing risk, RWA vaults incorporate complementary off-chain methods and settlement processes that bridge traditional and decentralized finance systems for valuing and liquidating the collateral to manage the risk.

High-Level Technical Overview

On a more technical level, each RWA vault is tailored for the specific requirements of the off-chain deal that drives it. However, there are some common components/patterns. Each RWA deal is composed of at least 3 smart-contract components:

1. **RWA Urn**: the actual RWA Vault, with the rules that define the operation of the lower-level vault. Unlike regular crypto vaults that can be created by anyone, only Sky Governance is able to create them. The operation of such vaults is delegated to Sky Governance-approved counterparties. For instance, they can draw or repay Dai back and forth while the vault is active. Borrower capital use is dictated by an off-chain legal agreement with the DAO.
2. **RWA Token**: tokenized representation of the off-chain asset, to ensure consistent accounting of the transaction. The token is locked into the vault as collateral, for which the price is determined by the RWA Oracle. RWA Tokens are not freely transferable, as they have no intrinsic value, since it is not possible to redeem them anywhere. It should be either in control of the vault operator, or ideally be locked into the vault when the RWA deal is set up.
3. **RWA Liquidation Oracle**: unlike regular crypto oracles, with live price feeds, the RWA Oracle is controlled by Sky Governance and only updated when required. Besides the RWA Token prices, the RWA Oracle also stores the link to the legal documents that govern the deal – usually in the form of an IPFS hash – and the "liquidation" status for the vault (see more on RWA Liquidation Process below).

Additionally, some helper components might be required:

1. **RWA Output Conduit**[^1]: after the operator draws Dai, an intermediate step might be required before it reaches its final destination. For instance, a specified third party might be required to authorize the transfer, or Dai should be converted into another stablecoin (i.e.: USDC) and then transferred. In those cases, a specialized variation of RWA Output Conduit is added to the setup as the destination for the Dai drawn from the RWA Urn.
2. **RWA Input Conduit**: similar to output conduits, but used when the operator wants to repay Dai into the vault. Be it third party authorization, stablecoin swapping (i.e.: repayment is made in USDC instead of Dai), or something else, there might be a specialized variation of RWA Input Conduit added to the mix.
3. **RWA Jar**: stability fees in the Sky Protocol are inherently fixed—while they can be updated, they remain constant between updates—and accrue by the second.Some RWA deals don't align with this model because they invest in assets with variable interest rates. Rather than relying on approximate estimates and making frequent on-chain adjustments—which would be operationally expensive—certain RWA Vaults set their on-chain stability fee to zero, with the actual fee defined off-chain and enforced through binding legal documents. In these cases, for accounting consistency, the fees generated by the Dai drawn from the vault must be transferred into an RWA Jar. From there, the fees can be permissionlessly moved to the Sky Protocol's Surplus Buffer.

RWA Liquidation Process

Unlike crypto collateral, which can be sold on-chain immediately as soon as the liquidation conditions are met, RWA liquidations might take months or even years to complete. Liquidations for RWA vaults occur entirely off-chain, through manual processes requiring Sky Governance and Ecosystem Actor coordination.

The RWA Liquidation has 2 steps:

1. **Soft Liquidation**: some conditions of the deal terms (i.e. covenants) are currently not being met. Some deals have an on-chain enforced grace period through which stakeholders can fix such issues before hard liquidation kicks in. If the relevant counterparty can meet the terms defined in the legal agreement, the RWA vault can be moved out of the soft liquidation state.
2. **Hard Liquidation**: if the stakeholders and Sky Governance agree that the Dai drawn from a specific RWA Vault is unrecoverable after the soft liquidation and the grace period has expired, then the Sky protocol needs to write off the existing debt, so the accounting reflects the reality. That means that the total outstanding debt for that vault needs to be deducted from the protocol's Surplus Buffer. If there is not enough surplus to cover the losses, the protocol will perform Flop auctions (mint governance tokens and purchase Dai from the market) until the surplus buffer returns to zero.

The future of RWA Vaults

The inclusion of RWA vaults allowed Sky to diversify its collateral base and reduce dependence on volatile cryptocurrencies. However, this came with increased operational complexity, slower liquidation times, and legal complexity. Despite these factors, RWAs continue to be a key collateral type for the Sky Protocol. Since the rebranding from MakerDAO to Sky, the creation and management of RWAs will be spearheaded by Stars, which are independent projects within the Sky Ecosystem. Stars will be operating a new framework called the Allocation System to autonomously manage allocations into tokenized RWAs, which will be implemented with new and improved techniques from the historical RWA vaults described above. While the Stars will have some level of autonomy, their actions will still being subject to Sky's risk management systems. The allocation system is a framework designed to manage and deploy capital across the Sky ecosystem efficiently. It allows Stars to borrow funds from the Sky Protocol at favorable rates, enabling targeted liquidity injections into DeFi protocols and tokenized real-world assets. This system enhances the ecosystem's financial stability through significant allocations into liquid asset types, with an emphasis on risk management to ensure that capital allocations are optimized for risk-adjusted returns while fostering growth and diversification within the Sky ecosystem.

Key External Actors

In addition to its smart contract infrastructure, the Sky Protocol involves groups of external actors to maintain operations: Keepers, Oracles, and Global Settlers (Emergency Oracles), and Sky Ecosystem community members. Keepers take advantage of the economic incentives presented by the Protocol; Oracles and Global Settlers are external actors with special permissions in the system assigned to them by MKR voters; and Sky Ecosystem community members are individuals and organizations that provide services.

Keepers

A Keeper is an independent (usually automated) actor that is incentivized by arbitrage opportunities to provide liquidity in various aspects of a decentralized system. In the Sky Protocol, Keepers are market participants that help Dai maintain its Target Price ($1): they sell Dai when the market price is above the Target Price, and buy Dai when the market price is below the Target Price. Keepers participate in Surplus Auctions, Debt Auctions, and Collateral Auctions when Sky Protocol Vaults are liquidated.

Price Oracles

The Sky Protocol requires real-time information about the market price of the collateral assets in Sky Protocol Vaults in order to know when to trigger Liquidations.

The Protocol derives its internal collateral prices from a decentralized Oracle infrastructure that consists of a broad set of individual nodes called Oracle Feeds. MKR voters choose a set of trusted Feeds to deliver price information to the system through Ethereum transactions. They also control how many Feeds are in the set.

Archived copy · cryp2nova.com

To protect the system from an attacker attempting to gain control of a majority of the Oracles, the Sky Protocol receives price inputs through the Oracle Security Module (OSM), not from the Oracles directly. The OSM, which is a layer of defense between the Oracles and the Protocol, delays a price for one hour, allowing Emergency Oracles or a Sky Governance vote to freeze an Oracle if it is compromised. Decisions regarding Emergency Oracles and the price delay duration are made by Sky Ecosystem Governance.

Emergency Oracles

Emergency Oracles are selected by MKR voters and act as a last line of defense against an attack on the governance process or on other Oracles. Emergency Oracles are able to freeze individual Oracles (e.g., ETH and BAT Oracles) to mitigate the risk of a large number of users trying to withdraw their assets from the Sky Protocol in a short period of time, as they have the authority to unilaterally trigger an Emergency ShutdownEmergency Shutdown serves two main purposes. It is used during emergencies as a last-resort mechanism to protect the Sky Protocol against attacks on its infrastructure, and used to facilitate a Sky Protocol system upgrade. The process is fully decentralized and controlled by Sky Governance..

The Dai Savings Rate

The Dai Savings Rate (DSR) allows any Dai holder to earn savings automatically and natively by locking their Dai into the DSR contract in the Sky Protocol. It can be accessed via the SummerFi portal or through various gateways into the Sky Protocol. Users aren't required to deposit a minimum amount to earn the DSR, and they can withdraw any or all of their Dai from the DSR contract at any time.

The DSR is a global system parameter that determines the amount Dai holders earn on their savings over time. When the market price of Dai deviates from the Target Price due to changing market dynamics, Sky Ecosystem Governance can mitigate the price instability by voting to modify the DSR accordingly:

- If the market price of Dai is above 1 USD, Sky Ecosystem Governance can choose to gradually decrease the DSR, which will reduce demand and should reduce the market price of Dai toward the 1 USD Target Price.
- If the market price of Dai is below 1 USD, Sky Ecosystem Governance can choose to gradually increase the DSR, which will stimulate demand and should increase the market price of Dai toward the 1 USD Target Price.

Initially, adjustment of the DSR will depend on a weekly process, whereby Sky Ecosystem Governance first evaluate and discuss public market data and proprietary data provided by market participants, and then vote on whether an adjustment is necessary or not. The long-term plan includes implementation of the DSR Adjustment Module, an Instant Access ModuleAn Instant Access Module contains components to create direct, bounded changes to the Sky Protocol without consensus in the DS-Chief. that directly controls both the DSR and the Base RateThe Base Rate is part of the Stability Fee that applies to all asset types (i.e., the total Stability Fee for each asset type includes the base rate plus the collateral rate).. This module allows for easy adjustment of the DSR (within strict size and frequency boundaries set by Sky Ecosystem Governance) by an MKR holder on behalf of the larger group of Sky Ecosystem Governance. The motivation behind this plan is to enable nimble responses to rapidly changing market conditions, and to avoid overuse of the standard governance process of Executive Voting and Governance Polling.

In 2024, MakerDAO rebranded to Sky and introduced the Sky Savings Rate for the USDS stablecoin. They coexist, although their rates may differ and the Sky Savings Rate utilizes the ERC4626 tokenized vault standard as opposed to the Dai Savings Rate.

Governance of the Sky Protocol

Use of the MKR Token in Sky Governance

The MKR token—the governance token of the Sky Protocol—allows those who hold it to *vote* on changes to the Sky Protocol. Note that anyone, not only Sky Ecosystem Governance, can *submit* proposals for an MKR vote.

Any voter-approved modifications to the governance variables of the Protocol will likely not take effect immediately in the future; rather, they could be delayed by as much as 24 hours if voters choose to activate the Governance Security Module (GSM). The delay would give Sky Ecosystem Governance the opportunity to protect the system, if necessary, against a malicious governance proposal (e.g., a proposal that alters collateral parameters contrary to established monetary policies or that allows for security mechanisms to be disabled) by triggering a Shutdown.

Polling and Executive Voting

In practice, the Sky Governance process includes proposal polling and Executive Voting. Proposal polling is conducted to establish a rough consensus of community sentiment before any Executive Votes are cast. This helps to ensure that governance decisions are considered throughtfully and reached by consensus prior to the voting process itself. Executive Voting is held to approve (or not) changes to the state of the system. An example of an Executive Vote could be a vote to ratify Risk Parameters for a newly accepted collateral type.

At a technical level, smart contracts manage each type of vote. A Proposal Contract is a smart contract with one or more valid governance actions programmed into it. It can only be executed once. When executed, it immediately applies its changes to the internal governance variables of the Sky Protocol. After execution, the Proposal Contract cannot be reused.

Any Ethereum AddressAn Ethereum Contract Account is controlled by its contract code. It cannot initiate new transactions on its own; rather, when it receives a message from an externally owned account or another contract account, it executes its code, allowing it to read, write, and send messages or create smart contracts. can deploy valid Proposal Contracts. MKR token holders can then cast approval votes for the proposal that they want to elect as the Active Proposal. The Ethereum address that has the highest number of approval votes is elected as the Active Proposal. The Active Proposal is empowered to gain administrative access to the internal governance variables of the Sky Protocol, and then modify them.

The MKR Token's Role in Recapitalization

In addition to its role in Sky Governance, the MKR token has a complementary role as the recapitalization resource of the Sky Protocol. If the system debt exceeds the surplus, the MKR token supply may increase through a Debt Auction (see above) to recapitalize the system. This risk inclines Sky Ecosystem Governance to align and responsibly govern the Sky ecosystem to avoid excessive risk-taking.

Risk Parameters Controlled by Sky Governance

Each Sky Protocol Vault type (e.g., ETH Vault and BAT Vault) has its own unique set of Risk Parameters that enforce usage. The parameters are determined based on the risk profile of the collateral, and are directly controlled by Sky Ecosystem Governance through voting.

The Key Risk Parameters for Sky Protocol Vaults are:

- **Debt Ceiling**: A Debt Ceiling is the maximum amount of debt that can be created by a single collateral type. Sky Governance assigns every collateral type a Debt Ceiling, which is used to ensure sufficient diversification of the Sky Protocol collateral portfolio. Once a collateral type has reached its Debt Ceiling, it becomes impossible to create more debt unless some existing users pay back all or a portion of their Vault debt.

Archived copy · cryp2nova.com

- **Stability Fee**: The Stability Fee is an annual percentage yield calculated on top of how much Dai has been generated against a Vault's collateral. The fee is paid in Dai only, and then sent into the Sky Protocol Buffer.
- **Liquidation Ratio**: A low Liquidation Ratio means Sky Governance expects low price volatility of the collateral; a high Liquidation Ratio means high volatility is expected.
- **Liquidation Penalty**: The Liquidation Penalty is a fee added to a Vault's total outstanding generated Dai when a Liquidation occurs. The Liquidation Penalty is used to encourage Vault owners to keep appropriate collateral levels.
- **Collateral Auction Duration**: The maximum duration of Collateral auctions is specific to Sky Protocol Vaults. Debt and Surplus auction durations are global system parameters.
- **Auction Bid Duration:** Amount of time before an individual bid expires and closes the auction.
- **Auction Step Size**The minimum amount a bidder can offer above the current bid during an auction. : This Risk Parameter exists to incentivize early bidders in auctions, and prevent abuse by bidding a tiny amount above an existing bid.

Risk and Mitigation Responsibilities of Governance

The successful operation of the Sky Protocol depends on Sky Governance taking necessary steps to mitigate risks. Some of those risks are identified below, each followed by a mitigation plan.

A malicious attack on the smart contract infrastructure by a bad actor.

One of the greatest risks to the Sky Protocol is a malicious actor—a programmer, for example, who discovers a vulnerability in the deployed smart contracts, and then uses it to break the Protocol or steal from it.

In the worst-case scenario, all decentralized digital assets held as collateral in the Protocol are stolen, and recovery is impossible.

Mitigation: The Maker Foundation's highest priority is the security of the Sky Protocol, and the strongest defense of the Protocol is Formal VerificationFormal Verification means creating mathematical specifications of the intended behavior of the system, alongside mathematical proofs that the codebase implements behavior that is identical to the intended behavior, with no unintended side effects as there is no mathematical evidence that the intended behavior produces effects inconsistent with the intended behavior.. The Dai codebase was the first codebase of a decentralized application to be formally verified.

In addition to formal system verification, contracted security audits by the best security organizations in the blockchain industry, third-party (independent) audits, and bug bounties are part of the Foundation's security roadmap. To review the formal verification report and various Sky Protocol audits, visit Maker's Multi-Collateral Dai Security Github repository.

These security measures provide a strong defense system; however, they are not infallible. Even with formal verification, the mathematical modeling of intended behaviors may be incorrect, or the assumptions behind the intended behavior itself may be incorrect.

A black swan event

A black swan event is a rare and critical surprise attack on a system. For the Sky Protocol, examples of a black swan event include:

- An attack on the collateral types that back Dai.
- A large, unexpected price decrease of one or more collateral types.
- A highly coordinated Oracle attack.
- A malicious Sky Governance proposal.

Please note that this list of potential "black swans" is not exhaustive and not intended to capture the extent of such possibilities.

Mitigation: While no one solution is failsafe, the careful design of the Sky Protocol (the Liquidation Ratio, Debt Ceilings, the Governance Security Module, the Oracle Security Module, Emergency Shutdown, etc.) in conjunction with good governance (e.g., swift reaction in a crisis, thoughtful risk parameters, etc.) help to prevent or mitigate potentially severe consequences of an attack.

Unforeseen pricing errors and market irrationality

Oracle price feed problems or irrational market dynamics that cause variations in the price of Dai for an extended period of time can occur. If confidence in the system is lost, rate adjustments or even MKR dilution could reach extreme levels and still not bring enough liquidity and stability to the market.

Mitigation: Sky Governance incentivizes a sufficiently large capital pool to act as Keepers of the market in order to maximize rationality and market efficiency, and allow the Dai supply to grow at a steady pace without major market shocks. As a last resort, Emergency Shutdown can be triggered to release collateral to Dai holders, with their Dai claims valued at the Target Price.

User Abandonment for Less Complicated Solutions

The Sky Protocol is a complex decentralized system. As a result of its complexity, there is a risk that inexperienced cryptocurrency users will abandon the Protocol in favor of systems that may be easier to use and understand.

Mitigation: While Dai is easy to generate and use for most crypto enthusiasts and the Keepers that use it for margin trading, newcomers might find the Protocol difficult to understand and navigate. Although Dai is designed in such a way that users need not comprehend the underlying mechanics of the Sky Protocol in order to benefit from it, the documentation and numerous resources consistently provided by the Sky Ecosystem community help to ensure onboarding is as uncomplicated as possible.

General Issues with Experimental Technology

Users of the Sky Protocol (including but not limited to Dai and Sky holders) understand and accept that the software, technology, and technical concepts and theories applicable to the Sky Protocol are still unproven and there is no warranty that the technology will be uninterrupted or error-free. There is an inherent risk that the technology could contain weaknesses, vulnerabilities, or bugs causing, among other things, the complete failure of the Sky Protocol and/or its component parts.

Mitigation: See "A malicious attack on the smart contract infrastructure by a bad actor" above. The Mitigation section there explains the technical auditing in place to ensure the Sky Protocol functions as intended.

Price Stability Mechanisms

The Dai Target Price

Archived copy · cryp2nova.com

The Dai Target Price is used to determine the value of collateral assets Dai holders receive in the case of an Emergency Shutdown. The Target Price for Dai is 1 USD, translating to a 1:1 USD soft peg.

Emergency Shutdown

Emergency Shutdown (or, simply, Shutdown) serves two main purposes. First, it is used during emergencies as a last-resort mechanism to protect the Sky Protocol against attacks on its infrastructure and directly enforce the Dai Target Price. Emergencies could include malicious governance actions, hacking, security breaches, and long-term market irrationality. Second, Shutdown is used to facilitate a Sky Protocol system upgrade. The Shutdown process can only be controlled by Sky Governance.

MKR voters are also able to instantly trigger an Emergency Shutdown by depositing MKR into the Emergency Shutdown Module (ESM), if enough MKR voters believe it is necessary. This prevents the Governance Security Module (if active) from delaying Shutdown proposals before they are executed. With Emergency Shutdown, the moment a quorum is reached, the Shutdown takes effect with no delay.

There are three phases of Emergency Shutdown:

1. **The Sky Protocol shuts down; Vault owners withdraw assets.**

   When initiated, Shutdown prevents further Vault creation and manipulation of existing Vaults, and freezes the Price Feeds. The frozen feeds ensure that all users are able to withdraw the net value of assets to which they are entitled. Effectively, it allows Sky Protocol Vault owners to immediately withdraw the collateral in their Vault that is not actively backing debt.

2. **Post-Emergency Shutdown auction processing**

   After Shutdown is triggered, Collateral Auctions begin and must be completed within a specific amount of time. That time period is determined by Sky Governance to be slightly longer than the duration of the longest Collateral Auction. This guarantees that no auctions are outstanding at the end of the auction processing period.

3. **Dai holders claim their remaining collateral**

   At the end of the auction processing period, Dai holders use their Dai to claim collateral directly at a fixed rate that corresponds to the calculated value of their assets based on the Dai Target Price. For example, if the ETH/USD Price Ratio is 200, and a user holds 1000 Dai at the Target Price of 1 USD when Emergency Shutdown is activated, The user will be able to claim exactly 5 ETH from the Sky Protocol after the auction processing period. There is no time limit for when a final claim can be made. Dai holders will get a proportional claim to each collateral type that exists in the collateral portfolio. Note that Dai holders could be at risk of a haircut, whereby they do not receive the full value of their Dai holdings at the Target Price of 1 USD per Dai. This is due to risks related to declines in collateral value and to Vault owners having the right to retrieve their excess collateral before Dai holders may claim the remaining collateral. For more detailed information on Emergency Shutdown, including the claim priorities that would occur as a result, see the published community documentation.

APPENDIX

System and Community Resources

- Sky Ecosystem main information website
- Sky Info Dashboard
- Sky Governance Portal
- Sky Forum
- Sky Discord
- Sky official Twitter/X account
- Sky Developer Documentation

[^1]: Vaults that integrate with other protocols might have bespoke smart contract components that fulfills the role of both input and output conduits. That is the case with Centrifuge integrations.

CRYP2NOVA

Archived copy · cryp2nova.com