End - Detailed Documentation

Shutdown * Contract Name: * end.sol * Type/Category: * DSS *Associated MCD System Diagram * Contract Source * Etherscan *

1. Introduction (Summary)

TheEnd 's purpose is to coordinate Shutdown. In short, Shutdown closes down the system and reimburses Dai holders. This process can occur during upgrades (Dai iterations), as well as for security reasons in the event that implementation flaws arise in both in the code and in the design.

?

1. Contract Details

Glossary (Shutdown)

Key Functionalities (as defined in the smart contract)

cage - Locks the system and initiates shutdown. This is done by freezing the user-facing actions, cancelingflap andflop auctions, locking the rest of the system's contracts, disabling certain governance actions that could interfere with the settlement process, and starting the cool-down period.

cage(ilk) - Tags the Ilk prices / Sets the final price for an ilk (tag).

skim - Settles a Vault at the tagged price / Cancels owed Dai from the Vault

free - Remove (remaining) collateral from a settled Vault. This occurs only after there is no debt in the Vault.

thaw - Fixes the Dai supply after all Skims / Fixes the total outstanding supply of stablecoin.

flow - Calculates the fixed price for an ilk, possibly adjusting thecage price with surplus/deficit.

pack - Locks Dai ahead of Cash / Puts some stablecoin into abag in preparation forcash .

cash - Exchangepack ed Dai for collateral / Exchange some Dai frombag for a givengem , share proportional tobag size.

file - The Governance configuration—sets various parameter values.

skip - optionally cancel live auctions.

Other

wards(usr: address) - Auth Mechanism

vat - Vat contract

cat - Cat contract

vow - Vow contract

spot - Spotter contract

live - Cage flag

- "Live" contracts havelive
- = 1, indicating the system is running normally. Thus, whencage()
- is invoked, it sets the flag to 0. This includes theEnd
- contract, which means thatcage()
- can only be invoked once and the subsequent functions cannot be invoked until we are "dead" and in the End process
-

ilk - A collateral type

when - Time of cage / the time of settlement.

wait - Processing cooldown duration / the length of processing cooldown.

debt - Outstanding Dai after processing / outstanding stablecoin supply, after system surplus/deficit has been absorbed.

tag - Cage price / price per collateral type at time of settlement.

gap - Collateral shortfall / shortfall per collateral considering undercollateralised Vaults.

Art - Total debt per Ilk/outstanding stablecoin debt.

fix - Final cash price / the cash price for an ilk (amount per stablecoin).

bag(usr: address) - Dai packed forcash / nontransferable stablecoins ready to exchange for collateral.

out - Cash out / the amount of already exchanged stablecoin for a given address.

skip - Optionally cancel live auctions.

wad - Some quantity of tokens, usually as a fixed point integer with 10^18 decimal places.

urn - A specific Vault.

tend - To make a bid, increasing the bid size.

bid - The quantity being offered for thelot .

lot - The quantity up for auction.

dent - To make a bid, decreasing the lot size.

1. Key Mechanisms & Concepts

?

Cage (Summary)

Thecage is the most complex mechanism within the Maker Protocol. This is because thecage must alter the behavior of almost every component of the system as well as perform under a variety of possible undercollateralization regimes. Listed below are a number of key properties, such as Dai and Vault parity, or the lack of race conditions, which aredesirable (nice-to-have) properties of Shutdown, and are not, in fact, all satisfied by the real-world implementation of Shutdown.

- Dai Parity
-
    - Assuming there is enough collateral in the system, it is the sum of the values of each collateral redeemed from 1 Dai equal to the target price (i.e., 1.00), as judged by the collateral price used bycage
- .
- Vault Parity -
- Where each Vault is settled at the collateral price during the time of global settlement. For example, the value of the collateral left in every Vault aftercage
- will be the equity value of the Vault beforecage
- , as judged by the collateral price used bycage
- , or zero, whichever is greater.
- Dai no-race condition
-
    - Where every Dai holder will be able to redeem the same quantity of each type of collateral, regardless of when they interact with the contract. This is the most important property, as it ensures fairness for all Dai holders.
- Near-immediate Dai redemption
-
    - where all Dai can be redeemed for collateral immediately aftercage
- .
- Near-immediate Vault redemption
-
    - Where all free collateral can be retrieved immediately aftercage
- .
- No off-chain calculations
-
    - where the system does not require thecage
- authority to supply any off-chain calculated values. For example, it can rely entirely on the last OSM price feed values.
-

Current Implementation Properties of Shutdown

- Dai no-race condition
-
    - every dai holder will be able to redeem the same quantity of collateral, regardless of when they interact with the contract.
- Vault Parity

-
    - Vault Owners are prioritized and are allowed to redeem their excess collateral before Dai holders.
-
    - At the time of Emergency Shutdown (ES), individual Vaults, entire collateral types, or the Maker protocol can be undercollateralized, which is when the value of debt exceeds the value of collateral ("negative equity").
-
    - Maker's current implementation favors Vaults owners in all cases by allowing them to free their entire amount of excess collateral. Thus, in the low likelihood event that Vaults become undercollateralized, the Dai holders receive a "haircut" to their claim on collateral. In other words, Dai holders' claim may be less than a dollar's worth of collateral.
- *
- Immediate Vault redemption
-
    - After ES is initiated, Vault owners are allowed to free their collateral immediately, provided that they execute all contract calls atomically.
- No off-chain calculations
-
    - The system does not require the cage authority to supply any off-chain calculated values (e.g. it can rely entirely on the last OSM feed prices).
- Vow Buffer Assistance
-
    - After ES is initiated, any surplus (and bad debt) in the buffer acts as a reward (and penalty) distributed pro-rata to all Dai Holders. e.g. if 10% of total system debt is in the form of net surplus in the Vow, then Dai holders receive 10% more collateral.
-

Dai Redemption vs. Vault Redemption Discussion

Since in some edge cases it will not be possible to satisfy all desirable properties at once, a choice must be made about which to prioritize. For example, in the presence of Vaults that have become less than 100% collateralized, a choice must be made between prioritizing Dai holders and Vault holders. If Vault holders are prioritized, those with over-collateralized Vaults keep their excess collateral, while Dai holders receive less than 1 of value per Dai. If Dai holders are prioritized, some collateral must be taken from over-collateralized Vaults to ensure Dai holders receive as close to 1 per Dai as possible. When choosing between Dai vs. Vault priority, Vault priority was chosen because we want to first prioritize Vault holders, meaning that even with a processing period for auction settlement, all Vault holders above their Liquidation Ratio (LR) should be allowed to retrieve their over-collateralization (This is accomplished by callingskim first on the Vault to remove the debt and the backing collateral and then callingfree to release the remaining collateral from the Vault).

Auction Settlement

- There is a time delay in Shutdown that is configurable by governance. The time delay must expire before any cashing can take place. The general guidance is that it should be long enough to ensure all auctions either finish or get skipped, but there is no guarantee of this in the code. Note that anyone can cancel aflip
- auction at any time by callingskip(ilk, auction-id)
- after theilk
- has beencage
- d (withcage(ilk)
-). Flap and flop auctions are frozen by the initialcage()
- . Both Flap and Flop auctions can beyank
- ed to return the bids to the last bidder.
- It's important to note that auction cancellation is not an immediate process as ecosystem participants must callskip
- for flip auctions or callyank
- directly for flap and flop auctions. If no one calls these functions, the auctions will not be canceled.
-

The Shutdown Mechanism (9 Crucial Steps)

As mentioned above, theEnd 's purpose is to coordinate the Shutdown of the system. This is an involved and stateful process that takes place over the nine following main steps.

1.cage() :

The process begins with freezing the system and locking the prices down for each collateral type (ilk). This is done by freezing the following user entry points:

- Halt the ability to deposit collateral and draw Dai from Vaults
- Flap/Flop Auctions
- Dai Savings Rate (DSR)
- Governance entry points like rely/deny and file

Next, the system will stop all of the current flop/flap auctions allowing individual auctions to be cancelled with calls toyank on the respective auction contract. One reason these auctions get frozen and canceled is because the shutdown process was designed to pass along the system surplus or system debt to Dai holders. Additionally, there are no guarantees regarding the value of MKR during a shutdown, so mechanisms that rely on MKR's market value cannot be relied upon, which means there is no reason to keep running the auctions that impact MKR supply. More specifically, the reason forflop andflap auctions getting canceled is as follows:

- flap
- auctions will no longer serve their purpose. This is because, after a shutdown, the surplus is designed to be allocated to Dai holders. Thus, cancelingflap
- auctions during shutdown allows the system to return the surplus Dai back to theVow
- ’s balance and ultimately back to Dai holders.
- flop
- auctions also stop serving their purpose. This is because the bad debt is passed as a haircut (lower-than-market-value placed on an asset being used as collateral in a Vault) back to Dai holders if there is no other system surplus available.

As forflip auctions, they are not immediately canceled (but can be canceled by any user) because they are still tied to the valuable collateral in the system. Collateral auctions continue to run and Keepers can continue to bid on them, and if not, the auctions can beskipped .

Despite the fact that auctions can continue to run, this does not guarantee that all of the remaining Vaults are overcollaterlized. There is also nothing that can prevent the undercollateralized and unbitten Vaults from existing at the momentcage() is called.

During this time,cat.bite cannot be called as the function requireslive == 1 , disabling liquidations after shutdown. Additionally, after the End begins, all vaults must beskim med and thenfree d.

Overall, this results in flip auctions being able to continue during Shutdown or by having them reversed by a user by usingskip() (similar logic toflap auctions). If an auction is skipped, the bids are returned to bidders and collateral is returned to the original Vault (with the liquidation penalty applied in the form of increased debt).

Other notes regarding flip :

- End callsyank
- on the Flipper.
- yank
- closes atend
- -phase (allows bids to be made, thereby increasing thebid
- size) of the auction by returning the guy's Dai bid and moving the Gems from the Flipper to the End.
- dent
- phase auctions (allows bids to be made, decreasing thelot
- size) continue to thedeal
- phase as they have already raised the necessary Dai and are already in the process of returning Gems to the original Vault holder.

Notes:

- MKR could still have value if the same token is tied to another deployment of the system. Note that the system makes no assumptions about the economic value of MKR post-Shutdown.
- It is important to note that on-auction debt and surplus are canceled and balances are transferred to theEnd
- contract. The last step in this process is to begin the cooldown period.

2.cage(ilk) :

Thecage(ilk) works by setting thecage price for eachilk . It does this by reading off of the price feed. This is required as we must first process the system state before it is possible to calculate the final Dai/collateral price. In particular, we need to determinetwo things:

(a) Thegap , which is the collateral shortfall per collateral type by considering under-collateralized Vaults. (b) Thedebt , which is the outstanding Dai supply after including the system surplus/deficit.

We first determine(a) by processing all Vaults with theskim function described below. Next, you can see how(b) unfolds below.

3.skim(ilk, urn)

Theskim(ilk) function works to cancel all of the owed DAI from the Vault. Any excess collateral remains within the Vault(s) for the owner(s) to claim. Then, the backing collateral is taken.

We then determine debt(b) by processing the ongoing Dai generation processes of the auctions. This is done to ensure that the auctions will not generate any further Dai income. This guarantees that ongoing auctions will not change the total debt of the system. This includes the two-way auction (Flip) model not allowing for any more Dai to be generated. This means that the Dai generation comes fromtend auctions. Thus, if everything is indent we know the generation is over. This occurs when all auctions are in the reverse (dent) phase. In addition to ensuring that the auctions will not generate any further Dai, the Dai Savings Rate (pot.drip) must also be shut off during the End so that the total debt does not change.

Example:

In terms of user scenarios, this means that the process begins with users starting to bid more and more Dai until reaching the debt. Next, they start offering less and less collateral.

The auctions that are in the second phase (dent - reverse auctions) no longer affect any more of the total debt, as the Dai was already recovered. Lastly, for the auctions in the first phase, they can be canceled and return the collateral and debt to the Vault.

There are two methods of ensuring this:

1. By usingwait
2. ; or
3. By usingskip
4. .
5.

4.wait orskip

1. wait
2. sets the cooldown period. The time duration ofwait
3. only needs to be long enough to be able toskim
4. all of the undercollateralized Vaults andskip
5. alltend
6. -phase auctions. This means that it can, in fact, be quite short (for example 5 minutes). However, due to the possibility of scenarios such as network congestion occurring, it may be set longer.
7. When usingskip
8. , it will cancel all ongoing auctions and seize the collateral. This allows for faster processing of the auctions at the expense of more processing calls. This option allows Dai holders to retrieve their collateral much faster. Theskip(ilk, id)
9. will then proceed to cancel each of the individual flip auctions in the forward phase (tend
10.) and retrieve all of the collateral and return Dai to the bidder. After this occurs, the reverse phase (dent
11.) auctions can continue as they normally would, by performing eitherwait
12. orskip
13. .
14.

Note that both of these options are available in this implementation, withskip being enabled on a per-auction basis. When a Vault has been processed and has no debt remaining, the remaining collateral can be removed.

5.free(ilk) :

Thefree(ilk) method will then remove the collateral from the caller's Vault. Afterskim has been called,free(ilk) allows the owner to call as they need. It will remove all of the collateral remaining after step3, basically, all of the collateral that was not backing the debt. If you did not have debt in your Vault at the time of theEnd you do not need to do step3 and can proceed directly to this step to free your collateral.

6.thaw()

After the processing period has elapsed, the calculation of the final price for each collateral type is possible using thethaw function. The assumption is that all under-collateralized Vaults are processed and all auctions have unwound. The purpose ofthaw is to fix the total outstanding supply of Dai. Note that it may also require extra Vault processing to cover thevow surplus. Thevat.dai(vow) == 0 requirement is what guarantees that the vow surplus has been taken into account, which means that before you canthaw , you mustskim as many Vaults as needed in order to cancel any Dai surplus in the vow. Canceling Dai surplus is done by callingvow.heal beforethaw .

7.flow(ilk)

Theflow(ilk) function will calculate the cash price for a given ilk (fix) and adjusts thefix in the case of deficit/surplus. At this point in the mechanism, we have computed the final price for each collateral type and Dai holders can now turn their Dai into collateral. Each unit of Dai can claim a fixed basket of collateral. Dai holders must firstpack some Dai into abag . Once

packed, Dai cannot be unpacked and is not transferable. More Dai can be added to a bag later.

8.pack(wad)

Thepack(wad) will place Dai into a bag in preparation forcash , which dispenses collateral tobag holders. The bigger thebag , the more collateral can be released.

9.cash(ilk, wad)

Lastly, we usecash(ilk, wad) to exchange some of the Dai from yourbag for gems from a specific ilk. Note that the number of gems will be limited by how much packed Dai you have (how big yourbag is).

1. Gotchas (Potential source of user error)

Keepers

We expect Keepers to buy up Dai from smallholders in order to claim collateral.

- This is because a majority of Dai holders are uncertain on how to do perform specific actions during theEnd
- process. Due to this fact, we depend on third parties to buy up post-cage Dai to use for reclaiming large portions of Dai. Overall, there will be large amounts of Dai leftover in the system.
-

Note regardingcash

At the end of the Global Settlement process, users will get a share of each collateral type. This will require them to callcash through each ilk in the system to completely cash out their Dai.

- Example:
- Users will need to callcash(ilk, wad)
- to redeem the proportional amount of the specified collateral that corresponds to the amount of Dai that waspack
- ’ ed, where thepack
- function is used to aid with the redeeming of the different collaterals in different transactions. For example, let’s say you have 1000 Dai. You firstpack
- for the respective collateral types (ilks
-), then for eachcash
- call, you will redeem what the 1000 Dai represents from the total Dai supply. In return, you will get the same proportion of that same collateral that was locked for all Dai holders. Therefore, the best approach a Dai holder can take is tocash
- every collateral type (ilk
-).
- An additional thing to note is that if anyilks
- are undercollateralized, Dai holders will end up taking a bit of a cut as a result. This is because otherilks
- will not be used to "cover for" an underwater collateral type.
-

DOS Attack

In order to prevent a DOS attack, whatever entity calls thethaw function should ensure thatVow.heal() is called within the same transaction.

- Example:
- An attacker can send small amounts of Dai in thevat
- to thevow
- . This would preventthaw
- from being called and thus, End from progressing. To prevent this, we would callheal
- to clear out that excess Dai and proceed withthaw
- .
-

Governance

It is important to set the correctwait period. If you set an incorrectwait /cooldown period (if this is set early on) then auctions are later extended and this is not reset.

- It is important to note that the main problem to point out here is that if thewait
- allowsthaw
- to be called too early, all theFlip
- auctions may not have completed and the system may have an incorrect accounting of totaldebt
- .

-

Other

- The Cooldown period's purpose is so that auctions can beskip
- ped andskim
- applies to all Vaults (not just the undercollateralized ones).
- Once the time period between global settlement and the cool-down period has passed, Dai holders are exposed to the ability to redeem their Dai for collateral.
-
    - Therefore thewait
-
    - value should not be too large, so governance should advise for this at least.
- *
- Vault (Skim/End) Keeper - is a tool to skim underwater Vaults if not all undercollateralized Vaults are accounted for. This Keeper could be used by Maker Stakeholders such as large Dai holders/custodians, MKR governors, Redemption keepers and more.
-

1. Failure Modes (Bounds on Operating Conditions & External Risk Factors)

SinceEnd will read the Collateral price from thepip , this can result in the collateral price being only as accurate as the last recorded price. Ifpip returns a bad price due to oracles getting hacked, theEnd will be affected.

- For example:
- Calling Global Settlement because an oracle is getting attacked, we must make sure the oracles attack won't affect the Global Settlement price becauseEnd
- reads the price off of thepip
- (for reference, this occurs online 261
- ofend.sol
-).
-

If a bad price is queued up in the OSM, we need to make sure to fix thetag before the price is called on Global Settlement.

- Example Scenario:
- If a bad price goes through themedian
- , it takes approximately 30 min for the OSM, and then the Global Settlement process takes over an hour to work. Therefore, by the time it triggers, you will have a bad price in thepip
- and this will cause the system to fail.
-
    - Saving this from happening depends on how quickly you react when it comes to an oracles attack as well as overallgovernance
-
    - decisions.
-
    - We do not believe Global Settlement is a viable solution to bad Oracles. They impact the system too quickly for Global Settlement to help.
- *
-

An Oracle attack can be caused by two main events:

- Low prices, which makes liquidations easy.
-
    - During Global Settlement, setting fake low prices would allow Dai holders to get too much collateral for their Dai, making this attack profitable.
- *
- High prices, which helps with buying a lot of Dai.
-
    - When paired with a subsequent Global Settlement, this could be used to steal a lot / all of the collateral as that Dai would then be used to cash out.
-
        - Example:
-
        - If a user is able to push up the price of a collateral type, it would allow them to mint a larger amount of Dai, resulting in a larger share of the Dai pool. Thus, they could claim a larger proportional share of the collateral

whether it was of one type or a slice of all types. They could then readjust the manipulated prices before that collateral slice was fixed in theEnd

-
  -
    - .

- *
-

Critical Failure Modes

- End.wait
- when set to maximum can result in it not being possible to callthaw
- and therefore resulting in the Shutdown not being able to proceed.
- End.wait
- , when set to the minimum, can result inthaw
- being called before all auctions have finished, resulting in debt being calculated incorrectly and ultimately setting a wrong collateral price.
- WhenEnd.cage
- is called, all Dai holders are left holding an unstable asset in place of their desired stable asset. This could result in a market price crash across all collateral due to liquidations & sell-offs.
- Catastrophic Scenario:
- End.vat
- /End.vow
- /End.cat
- /End.spot
-
  - when set to attacker (address
- : set to attacker-controlled address), can cause shutdown to fail. This is unfixable. For this scenario to occur, the malicious entity (governance or otherwise) would need to beauth
- 'ed on theEnd
- .
-

Previous The Emergency Shutdown Process for Multi-Collateral Dai (MCD) Next ESM - Detailed Documentation Last updated4 years ago On this page * 1. Introduction (Summary) * 2. Contract Details * Glossary (Shutdown) * 3. Key Mechanisms & Concepts * Cage (Summary) * Current Implementation Properties of Shutdown * The Shutdown Mechanism (9 Crucial Steps) * 4. Gotchas (Potential source of user error) * 5. Failure Modes (Bounds on Operating Conditions & External Risk Factors)

Export as PDF