# Asset Risk Assessment: Silo Finance

### A look into Silo Finance and the XAI stablecoin

# Useful links:

* [Developer Docs](https://devdocs.silo.finance/protocol-architecture/protocol-overview)
* [Protocol Wiki](https://silopedia.silo.finance/welcome/read-me) (Silopedia)
* [Silo Lightpaper](https://drive.google.com/file/d/16-_I94y5d7Ts2R6J3vzm4qXwX8xjZ0X_/view)
* [Silo Interest Rate Model paper](https://drive.google.com/file/d/11jzbdIQ9KGm_ZVFIUwUu44O1ktWx5R30/view)
* [Formal Verification of Silo V1](https://www.silo.finance/_files/ugd/fd5034_98066b4c70ea46b5862a00670179f067.pdf) (Certora)
* [ABDK audit report](https://drive.google.com/file/d/1WXaB3ICLv4rSEX86POK3-NaOIxXwyq9l/view) (Silo core contracts - 6 Major, 1 Moderate and 65 Minor issues)
* [Quantstamp audit report](https://drive.google.com/file/d/10GyfA-nBJ5jqLWW9LEYJQeFem8qSgNH6/view) (Silo core contracts - 14 issues- 0 high,5 medium, 3 low and 6 info risks)
* [Silo Governance Forum](https://gov.silo.finance/)
* [Oracle - price providers](https://github.com/silo-finance/silo-core-v1/tree/master/contracts/priceProviders) (Chainlink as default price provider, UniswapV3 TWAP and BalancerV2 TWAP)
* [Timelock Controller](https://etherscan.io/address/0xe1F03b7B0eBf84e9B9f62a1dB40f1Efb8FaA7d22#code)
* [Development Fund Multisig](https://etherscan.io/address/0xdff2aea378e41632e45306a6de26a7e0fd93ab07#tokentxns) (2-out-of-3)
* Multisig owners - [Signer1](https://etherscan.io/address/0x9b8b04B6f82cD5e1dae58cA3614d445F93DeFc5c), [Signer2](https://etherscan.io/address/0x66B416a3114A737f0353DC74d1E12a7e23f686F9), [Signer3](https://etherscan.io/address/0xe153437bC974cfE3E06C21c08AeBbf30abaefa2E)
* [Vesting Contracts](https://docs.google.com/spreadsheets/d/1IcvYQlWQ34kIFIfIKWzJwGlw-Jv33_TMBDKCI0ziEa8/edit?usp=sharing) (Contributors, Advisors and Investors)
* [Github](https://github.com/silo-finance)
* [File list of 57 New Silos for deploying](https://docs.google.com/spreadsheets/d/1KkFXRRc_KiEwWIUYaSfjWa8Hk75WyRWrepWq2s_4bus/edit#gid=1510778453) - for community review

# Abstract

Silo is a permissionless and non-custodial lending protocol that allows the borrowing of any asset using any other asset as collateral. This is enabled through the creation of isolated (siloed) lending markets whereby the pool consists of only two assets, the unique token plus ETH. Silos are then connected through the bridge asset (currently only ETH).

**A quick TL;DR of our findings:**

* Silo Finance introduces a new money market design with isolated markets (silos) for every unique token. These isolated markets are paired with the same counterparty asset called bridge asset (ETH or XAI). Bridge assets represent a concentrated part of liquidity bridged across all isolated markets which facilitates the onboarding (listing) of any token, especially long-tail assets. The isolation of high-risk assets almost completely removes protocol systemic risk, while bridge assets prevent fractured liquidity and keep the protocol liquid and fluid.
* Silo protocol allows permissionless listing and parameter customization for each Silo through governance. Every newly created silo needs to have a reliable price feed source and starts with default collateral factors for Loan-to-Value (LTV), Liquidation Threshold and Liquidation Penalty.
* The Silo team takes security very seriously. The core smart contracts were fully audited by Quantstamp and ABDK, and tested by the core team through a formal verification process using Certora Prover.
* Silo introduced a new stablecoin named XAI, that will serve as the second bridge asset besides ETH. XAI can be minted and burnt by the SiloDAO via a governance vote (using Tally).
* Silo is very progressive in their endeavour to become a decentralised and trustless protocol. They have already fully transitioned to on-chain governance, so that SILO token holders are in full control over most of the protocol's functions.

# Silo Finance - An Introduction

## Siloed Lending Markets

Silo is a permissionless and non-custodial lending protocol that allows the creation of isolated (siloed) lending markets. The protocol is designed to support two types of asset categories, Unique Tokens and Bridge Assets. Unique tokens have their liquidity isolated in dedicated silos (1 silo for each token), while the bridge asset (currently ETH) is paired with every unique token across all isolated silos.

Inside an isolated market, both assets can be used interchangeably as collateral and loan. In other words, when lending token A, one can only borrow the bridge asset ETH against it. The bridge asset ETH can then be used as collateral in another silo, to borrow token B. Thus, one can borrow any token with any collateral, while isolating the risks related to the collateral token within one pool.

In comparison, 1st generation lending markets like Compound or Aave have all collateral in one pool (shared-pool), hence the impact of exploits - e.g. through price manipulation - can be much higher. This results in a few drawbacks (e.g., limitation in listing new assets, high parameter maintenance cost, cumbersome collateral [listing process](https://medium.com/primedao/enabling-collateral-in-defi-lending-why-your-favorite-token-might-not-be-listed-yet-a1ef27fd19bb) or low capital efficiency). Silo aims to unlock long tail assets to be lent and borrowed using their new design.



(source: [Twitter](https://twitter.com/DefiIgnas/status/1586978700171452418?s=20&t=ObKc98elioQcJCEQ8rIetg))

Another distinguishing factor is the permissionless listing of new collateral. According to the Silo docs ([here](https://silopedia.silo.finance/governance/creating-silos) and [here](https://silopedia.silo.finance/risk-framework/collateral-factors)), anyone can propose the addition of a new asset silos to the protocol, as long as a price-feed (oracle) exists. Currently the core team offers to configure and create the on-chain votes to deploy new silos. However, there is a [guide](https://github.com/silo-finance/silo-core-v1/blob/master/docs/HOW_TO_CREATE_SILO.md) describing the process, so anyone with the right technical skills can deploy a new silo for vote.

## Shares Tokens (sTokens)

[sTokens](https://silopedia.silo.finance/deposit/shares-tokens-stokens) are ERC-20 tokens that represent a claim on the deposited asset. For instance, in return for depositing LINK into Silo the lender receives sLINK. *sTokens* also accrue interest, depending on the interest rate per token.

When depositing tokens, Silo provides an innovative feature that allows lenders to choose whether their deposits can be borrowed by others, or whether they want to “protect” their deposits, which disables others from borrowing said assets. However, in return for protecting the token the lender forgoes earning an interest rate. *sTokens* represent borrowable assets, and *spTokens* represent protected deposits. It’s also possible to do both for the same asset (e.g. 40% of the token is borrowable and 60% is protected). *spTokens* can still be used as collateral to borrow other tokens.

For bridge assets (ETH or XAI), the naming convention is slightly different, i.e. *sBridge-ABC*, whereby ABC represents the name of the silo that ETH or XAI is deposited into. For instance, when depositing the bridge asset ETH into the LINK silo, the lender in return receives *sETH-LINK* or *spETH-LINK*.

## Debt Tokens (dTokens)

Conversely [dTokens](https://silopedia.silo.finance/borrow/debt-tokens-dtokens) are ERC-20 tokens representing a borrowed asset. They are minted when an asset is borrowed and burned when the loan is paid back. Unlike *sTokens*, *dTokens* cannot be transferred out of a wallet. For bridge assets, the borrowed token is represented again as *dBridge-ABC* (e.g. dETH-UNI).

## Conclusion

In summary, Silo introduces a few innovations targeted to make lending markets less risky while simultaneously improving market access for long tail assets. The ability to protect tokens from borrowers can be a very interesting feature for other DAO’s to deploy their token and borrow tokens against it.

The reduction in risk, however, has one trade-off with the current design: Borrowing at Silo can result in up to six transactions. First, <allow deposit> and <deposit> of the collateral, then <borrow> the bridge asset, then again <allow deposit> and <deposit> the bridge asset, before finally the targeted asset can be <borrowed>. This can be quite costly on Ethereum mainnet, and might be a blocker for smaller accounts to use Silo as intended. The team is working on new features to improve this, but it will take some time.

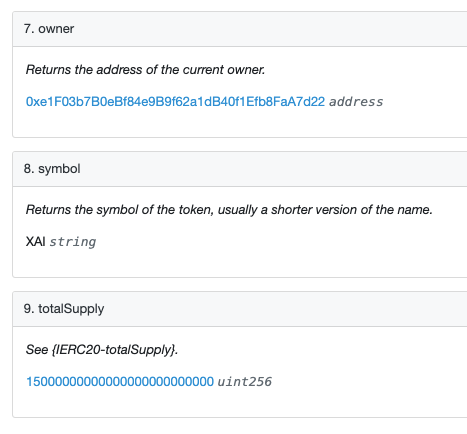
# The XAI Stablecoin

The Silo team aims to issue a new over-collateralized stablecoin with a soft peg to the US Dollar called XAI. The main use case for XAI is to serve as a second bridge token alongside ETH. Thus, enabling users to borrow XAI to bridge from token A to token B.

SiloDAO is the only entity that controls XAI. The DAO can choose to mint unlimited XAI and deposit it into any number of silos via executive proposals. The DAO can also burn XAI that is extended to any silos via governance proposals. Hence, when minting XAI into a silo, the SiloDAO effectively determines XAI’s backing, which can also be reversed by burning XAI from a silo.

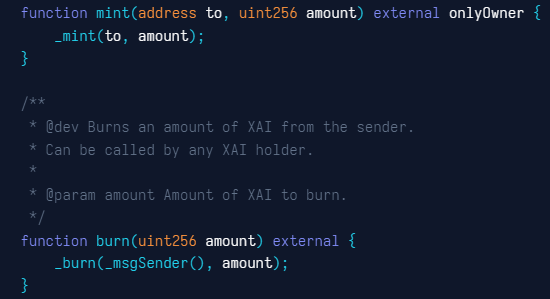
## Minting XAI

XAI is an ERC-20 [token contract](https://etherscan.io/address/0xd7C9F0e536dC865Ae858b0C0453Fe76D13c3bEAc#code) owned by the Silo Timelock Controller contract:



(source: [Etherscan](https://etherscan.io/address/0xd7C9F0e536dC865Ae858b0C0453Fe76D13c3bEAc#readContract))

The Timelock Controller is controlled by SiloDAO (i.e. SILO token holders voting via [Tally](https://www.tally.xyz/governance/eip155:1:0xA89163F7B2D68A8fbA6Ca36BEEd32Bd4f3EeAf61)), who control the XAI in circulation through the mint and burn function:



(source: [ContractRveader XAI](https://www.contractreader.io/contract/0xd7C9F0e536dC865Ae858b0C0453Fe76D13c3bEAc) )

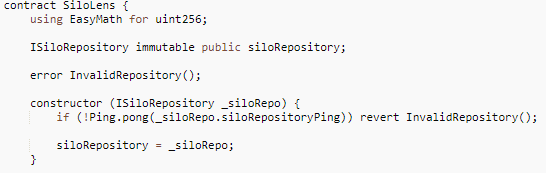
To create XAI, Silo used a set of [standard smart contracts](https://github.com/fractional-company/contracts/tree/master/src/OpenZeppelin) provided by OpenZeppelin (they used OZ standards for all their contracts).

Essentially, XAI works quite similar to other decentralised stablecoins such as DAI or FRAX, that are CDPs (Collaterlized Debt Positions), whereby a user mints new stablecoins when depositing a collateral. As mentioned above, XAI can only be minted by the DAO. Once in a silo, XAI becomes a CDP as users can now deposit collateral and borrow XAI in return (starting at an interest rate of 0.1%). This is a new method of creating stablecoins but is actually quite similar to MakerDAO’s [debt ceiling](https://makerdao.world/en/learn/governance/param-debt-ceiling/), whereby MKR holders decide how much DAI can be minted per collateral vault. This design helps to control risk exposure to certain collateral types.

## Silo Components

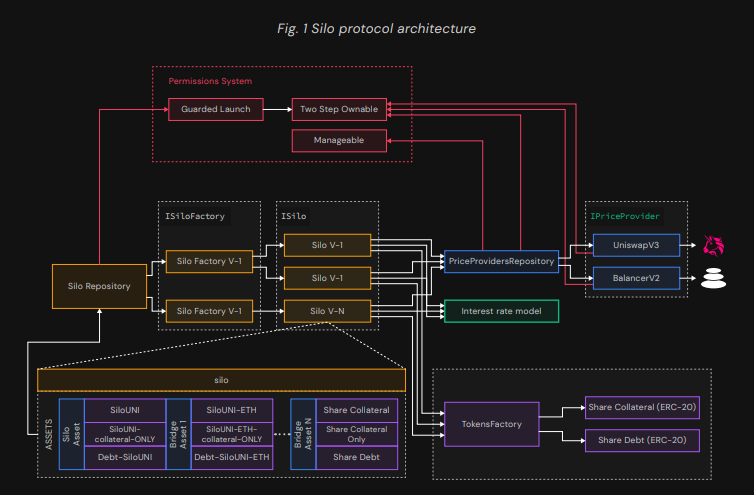
Silo Protocol smart contracts have a modular design and the protocol consists of [multiple components](https://devdocs.silo.finance/protocol-architecture/upgradability) that are not upgradeable, but replaceable. Only the SiloRepository component is not upgradeable nor replaceable. Components (registries) and description of each:

* [**SiloRepository**](https://etherscan.io/address/0xd998C35B7900b344bbBe6555cc11576942Cf309d#code) handles the creation and configuration of silos and stores the configuration of every asset in each silos. All assets have the same default configuration that later can be customised by the contract owner. As mentioned above, the SiloRepository contract is immutable:



(source: [SiloLens.sol](https://etherscan.io/address/0xf12C3758c1eC393704f0Db8537ef7F57368D92Ea#code))

* [**Silo**](https://etherscan.io/address/0xd998C35B7900b344bbBe6555cc11576942Cf309d#code) is the main component of the protocol that acts as a vault for assets, implementing the lending logic, managing and isolating the risk and performing liquidations.
* [**PriceProviderRepository**](https://etherscan.io/address/0x7C2ca9D502f2409BeceAfa68E97a176Ff805029F#code) manages the oracle modules and the price request routing for each silo. It can support many protocols and sources. Currently it supports three oracle sources: [Chainlink](https://etherscan.io/address/0xe37B8c83138caF12E57632D19c06Eb561D47e423#code) (default price provider), UniswapV3 TWAP, and BalancerV2 TWAP.
* [**Interest Rate Model**](https://etherscan.io/address/0x7e9e7ea94e1ff36e216a703d6d66ece356a5fd44#code). Silo Finance uses a dynamic interest rates model which is described in more detail in this [Interest Rate Model paper](https://drive.google.com/file/d/11jzbdIQ9KGm_ZVFIUwUu44O1ktWx5R30/view?pli=1).
* [**Silo Router**](https://etherscan.io/address/0xb2374f84b3cEeFF6492943Df613C9BcF45322a0c#code)is a utility contract that can batch any number or combination of actions (Deposit, Withdraw, Borrow, Repay) and execute in a single transaction.
* The permission system registry consist of three smart contracts: GuardedLaunch.sol, TwoStepOwnable.sol and Manageable.sol

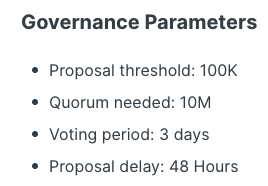


(source: [Certora Formal Verification Document](https://www.silo.finance/_files/ugd/fd5034_98066b4c70ea46b5862a00670179f067.pdf))

# SILO Governance

The governance process follows a standard procedure of forum discussion, Snapshot vote and finally on-chain vote. For more details visit the [docs](https://silopedia.silo.finance/governance/silodao). In practice, however, Snapshot is mostly applied for decisions concerning expenditures of the DAO’s funds, whereas changes that affect the protocol itself are directly voted on via an on-chain proposal on [Tally](https://www.tally.xyz/governance/eip155:1:0xA89163F7B2D68A8fbA6Ca36BEEd32Bd4f3EeAf61).

The screenshot below displays all governance parameters.



Notably the voting period for proposals is three days. Plus a voting delay of two days for on-chain proposals. This is in line with best practices and seems to be a reasonable time frame.

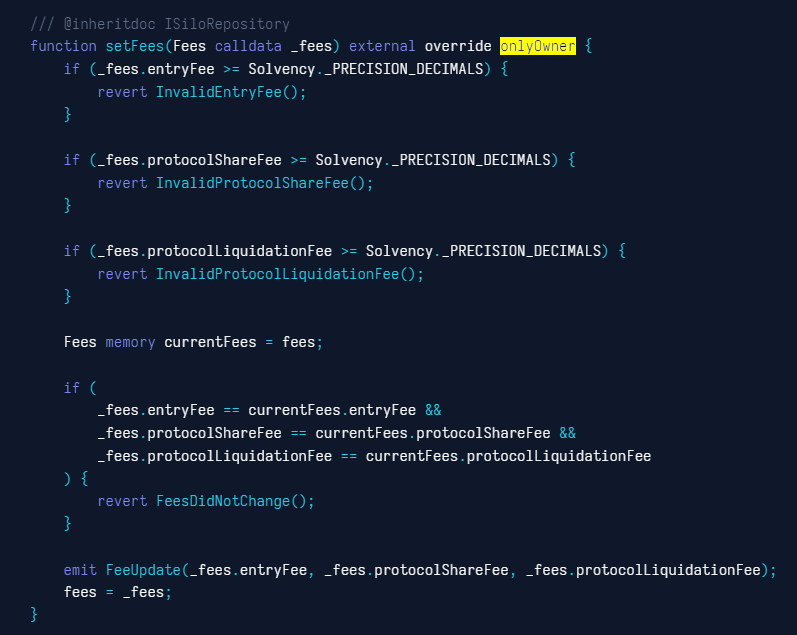
# Risk Vectors

Some of the risks are highlighted below.

## Custody Risk

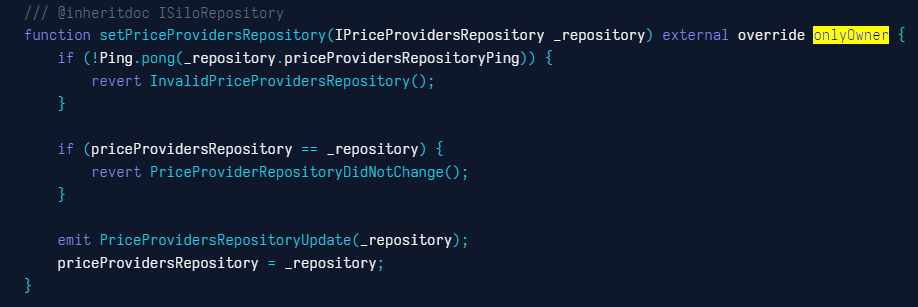
There is no direct custody risk, because SiloDAO as owner of the core contracts doesn't have the privileges to access any funds. However, there are two privileges that can impact user funds in some ways:

* setFees - The SiloDAO (as onlyOwner) can decide to set and adjust certain fees, such as borrow-entry-fees, protocol-share-fees and liquidation-fees. These fees can affect borrowers and users when getting liquidated.



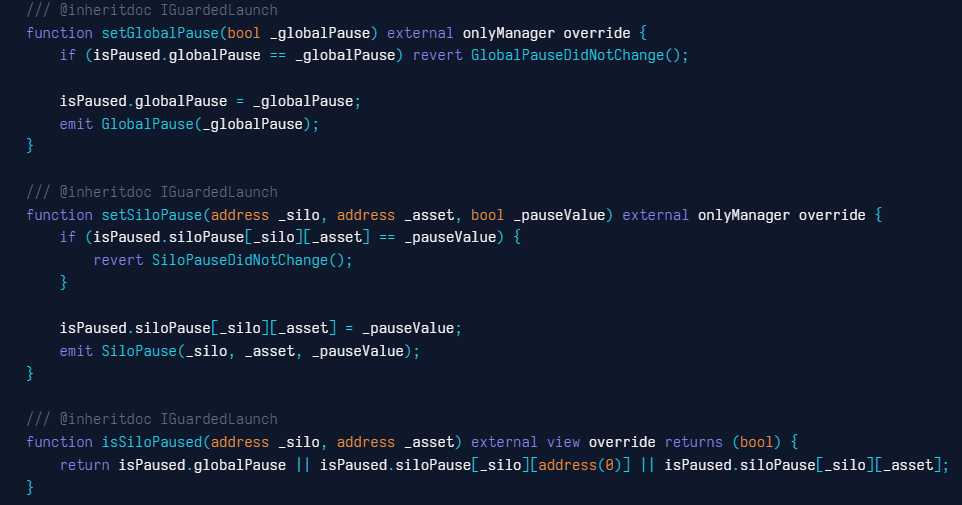
(source: [siloRepository.sol](https://www.contractreader.io/contract/0xd998C35B7900b344bbBe6555cc11576942Cf309d))

* setPriceProvidersRepository - The chosen oracle solution can also affect users' deposits. The DAO must ensure that to select the best oracle options for each silo.



(source: [siloRepository.sol](https://www.contractreader.io/contract/0xd998C35B7900b344bbBe6555cc11576942Cf309d))

* GuardedLaunch.sol - a contract which is part of Silo’s permission system - enables the SiloDAO (as Timelock Controller) to implement security and risk averse functions. For instance, it allows the contract manager (onlyManager) to pause specific silos in case of an exploit. If that happens, users deposited in the paused silos are at risk of liquidation, if their collateral value decreases below the liquidation threshold, after a new start (remove pause).



## (source: [SiloRepository.sol (GuardedLaunch.sol)](https://www.contractreader.io/contract/0xd998C35B7900b344bbBe6555cc11576942Cf309d))

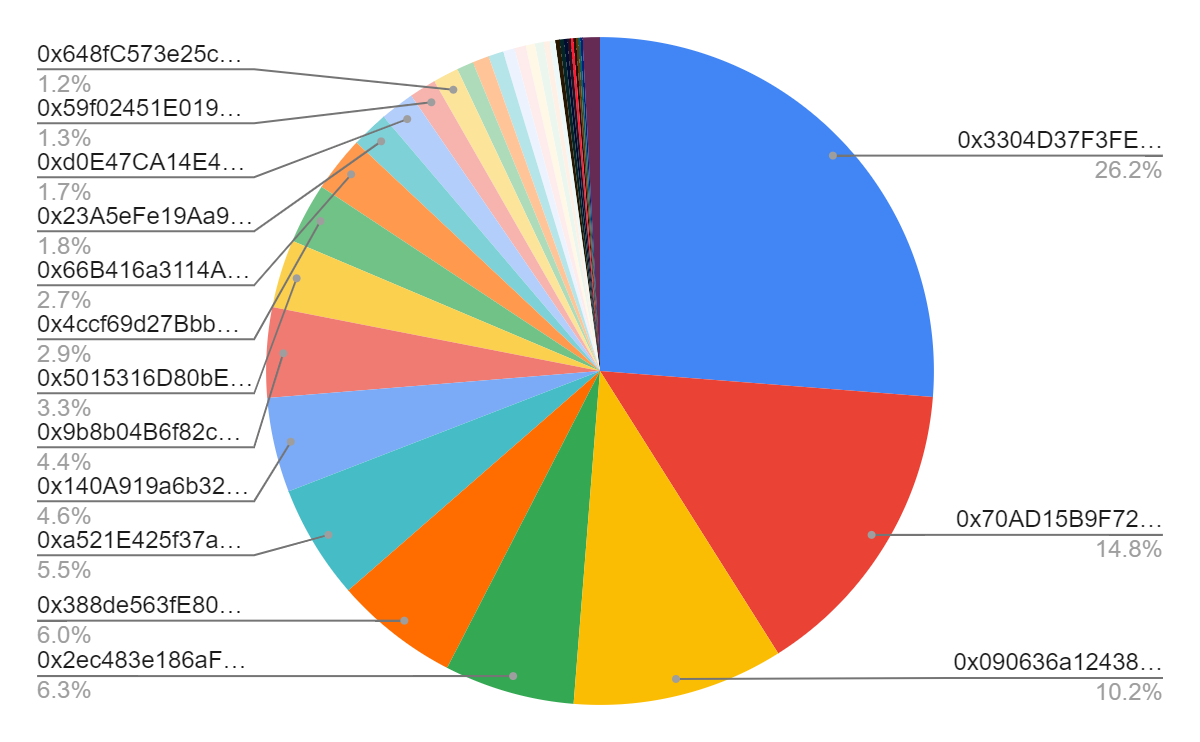
## Governance Risk

As mentioned above, all changes that affect the Silo protocol and its parameters are implemented via on-chain governance vote. These changes can include:

* Deployment of new markets (silos),
* Setting/adjusting silo parameters (LTV, LT, interest model, price feed),
* Minting/redeeming XAI
* Turning on/off fees
* Deploying new bridge assets,
* and even increasing the supply of SILO tokens

In summary, governance has extensive and very far reaching powers over Silo. Hence, the question arises “how likely is it that a malicious party can obtain a majority voting influence to instigate harmful changes to the protocol” (e.g. mint infinite XAI)?

In order for this to happen, the party would need to accrue a substantial amount of SILO tokens (or get voting power delegated). Presuming that the team and SILO investors only vote in the best interest of the DAO, the answer is: The possibility is very low. The chart below shows the voting power of all delegators. It’s important to note that in order to participate in on-chain voting, one has to delegate SILO to one's own wallet or to another delegate.



(source: [Boardroom - Delegates Voting Power Distribution](https://boardroom.io/silo/delegates))

As seen in the chart, the top three delegates control 51.2% of the overall voting power that is currently eligible to vote. This is quite a high concentration of power (basically a [Nakamoto coefficient](https://news.earn.com/quantifying-decentralization-e39db233c28e) of 3). With a bit of forensics on etherscan, using the [vested token overview](https://docs.google.com/spreadsheets/d/1IcvYQlWQ34kIFIfIKWzJwGlw-Jv33_TMBDKCI0ziEa8/edit#gid=1565912853), it becomes clear that the address with the most delegated voting power is controlled by the founding team. The same is true for rank 4, 7 and 10. The rest seem to be investors and community members.

This does not come as a surprise, given that the founding team will receive 27% of all tokens in circulation (vested over 3 years) according to the [vesting schedule](https://docs.google.com/spreadsheets/d/1IcvYQlWQ34kIFIfIKWzJwGlw-Jv33_TMBDKCI0ziEa8/edit#gid=1565912853) [side note: the team allocation stated in their [docs](https://silopedia.silo.finance/governance/token-allocation-and-vesting) is 5.25% lower (21.75%). Those tokens are currently sitting in a vesting contract untouched].

In summary, the team has by far the largest allocation. All other stakeholder groups don’t even come close, even all investors combined only achieve 6.3% voting power. While it’s not up to us to judge what token allocation is fair, it still leads to the conclusion that SiloDAO is fully controlled by the founding team, and will be for the foreseeable future.

## Smart Contract Risk

Useful links:

* [Formal Verification of Silo V1](https://www.silo.finance/_files/ugd/fd5034_98066b4c70ea46b5862a00670179f067.pdf) (Certora)
* [ABDK audit report](https://drive.google.com/file/d/1WXaB3ICLv4rSEX86POK3-NaOIxXwyq9l/view)
* [Quantstamp audit report](https://drive.google.com/file/d/10GyfA-nBJ5jqLWW9LEYJQeFem8qSgNH6/view)

Silo has undergone two audits by ABDK and Quantstamp, and has tested the smart contracts against formal verification rules with Certora. This process revealed a few critical vulnerabilities that the team was able to resolve. There is also a $100k bug bounty program live on [Immunefi](https://immunefi.com/bounty/silofinance/)

As mentioned above, Silo Finance used OpenZeppelin’s construction tools (i.e. secure smart contract [standards](https://github.com/fractional-company/contracts/tree/master/src/OpenZeppelin)) for creating XAI.

Overall Silo is taking security seriously and has taken the necessary measures to circumvent vulnerabilities. However, both audits were limited to Silo’s lending platform before XAI was introduced. It can be argued that XAI is a standard mint/burn contract controlled by the DAO that doesn’t need an audit, however, it must be highlighted nonetheless as potential risk.

## Depeg Risk

XAI is a new stablecoin. There is no historic data about its price stability or behaviour during highly volatile market conditions. We can, however, presume that Silo has and will implement all the right measures to ensure XAI’s stability.

As with other stablecoins, keeping the peg depends on a few key factors:

1. The underlying collateral needs to be fit for purpose (i.e. highly volatile collateral increases the risk of default and the risk of liquidations)
2. In order for the market to absorb liquidations, as well as arbitraging to keep the peg, both the stablecoin and the collateral asset need to have deep enough liquidity
3. The protocol can support price stability via parameter adjustments
4. Ideally the protocol has some fallback solution in case of a black swan event

We’ll discuss the collateral risk (1) in more detail in the next section. The other stabilisation mechanisms highlighted above are mostly covered:

* XAI is an over-collateralized stablecoin. At first only USDC and ETH will serve as collateral for XAI
* Arbitrage possibilities are given and liquidity in the open market will be seeded by the DAO and incentivized through CVX gauges (see [proposal](https://gov.silo.finance/t/building-on-chain-liquidity-for-xai/309))
* The DAO has influence over XAI via parameter adjustments, such as borrow rate, adding/removing collateral, increasing/decreasing XAI availability

The only measure that is missing is a concrete fallback solution, that the DAO can execute in case things go south (e.g. use SILO as backup to stabilise the stablecoin). However, this can also come at a later stage, once XAI has achieved some product market fit.

The last thing to highlight related to stability is that Silo’s TVL is currently around ~$1M. More than half of that TVL was [seeded by the DAO](https://snapshot.org/#/silofinance.eth/proposal/0x013bbb154af9317ab7a78b72a498d16e069fdba5e78b710e6785fc938d644e76) itself. There needs to be significant growth in TVL to enable sufficient backing of a stablecoin that aims to facilitate bridging between 60+ assets (10 assets are already live and [57 assets](https://gov.silo.finance/t/deploying-57-new-silos-to-the-protocol/306/2) will be added in the near future). While there are plans to incentivize liquidity for XAI, there is currently no plan presented that defines anything specific about how the DAO plans to attract more TVL for its long tail asset silos (a potential [veTokenomics](https://gov.silo.finance/t/tokenomics-proposal-vesilo-v2/226) discussion seems to be stuck).

## Collateral Risk

In the beginning, the only collateral enabled to borrow XAI will be USDC and ETH. Thus, eliminating other risks that come with long tail assets (e.g., low asset liquidity, high price volatility, depeg of the collateral, etc.).

Both ETH and USDC are highest tier assets with more than enough liquidity to offset potential liquidations. Even when XAI will be enabled as a bridge asset for more silos, the collateral risk is limited only to those isolated markets.

We currently don’t see any risks related to collateral, however, anyone can propose to add new credit lines. [Credit lines](https://silopedia.silo.finance/welcome/cross-silos-stablecoin) describe the process of allowing silos to use XAI as a bridge asset. While new credit lines need to be approved by governance first, this process can change the composition of XAI’s backing. Potential risks occur in cases where XAI supports illiquid and highly volatile assets. Hence, we recommend that each credit line and silo addition is carefully considered. Silo should also think about installing or incentivizing more detailed risk assessments for each collateral. A bad debt dashboard (as provided by RiskDAO for instance), is another option to better inform users about the health of individual silos.

## XAI as Collateral Risk

Silo also aims to enable XAI as collateral within the protocol. As highlighted above, for XAI to become a low-risk collateral, there needs to be enough liquidity in the open market. This will help to facilitate potential liquidations and arbitrage, which is needed to support XAi’s stability.

The team is working on two [initiatives](https://gov.silo.finance/t/building-on-chain-liquidity-for-xai/309) that will ensure the initial provisions of adequate liquidity. First, seeding the initial Curve pool with $3M (50% USDC / 50% XAI) from their development fund. And secondly, Silo will use 130k of their own vlCVX to vote for incentivization of their pool. Hence, we believe there will be enough liquidity for XAI’s early stage.

# Discussion and Conclusion

1. Is it possible for a single entity to rug its users?

No, SiloDAO does not have access to user funds. It can, however, mint XAI to silos or redeem XAI. The DAO also controls the interest rates for XAI. Thus, having a strong influence on the price stability of XAI.

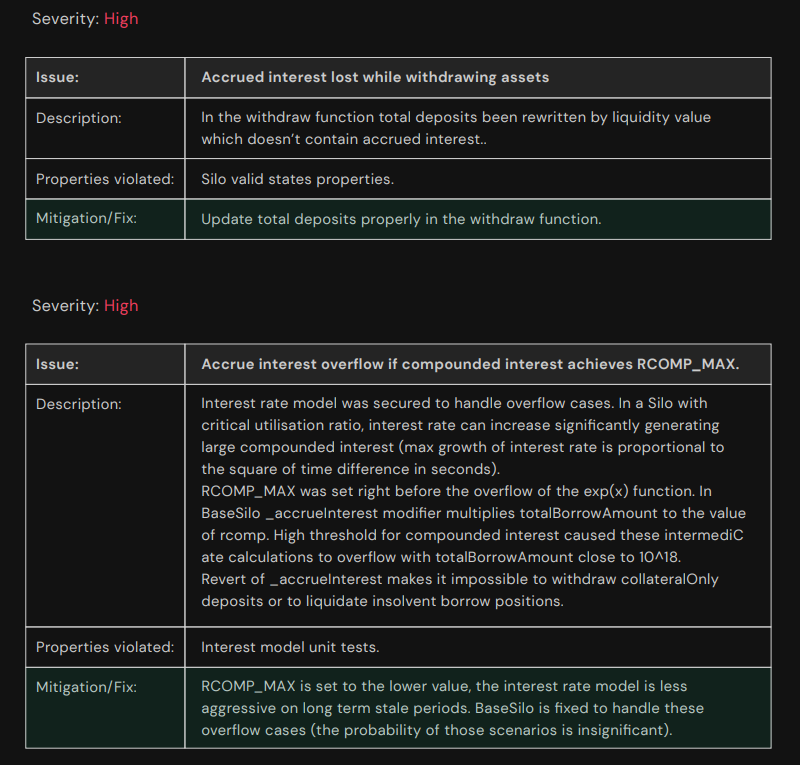
1. If the team vanishes, can the project continue?

Yes, Silo is managed via governance votes. Even if the team would disappear to the Bahamas, anyone with SILO tokens could still operate the protocol (i.e. adding / removing silos, minting / redeeming XAI, changing parameters, etc.).

The developer fund on the other hand - which contains most of the DAO’s funds - would probably not be accessible any longer, as it’s controlled by a 2-of-3 multisig belonging to the team.

1. Do audits reveal any concerning signs?

In a [formal verification process](https://www.silo.finance/_files/ugd/fd5034_98066b4c70ea46b5862a00670179f067.pdf) with **Certora Proven**, the team discovered 2 high and 3 medium severity issues:



(source: [Certora Formal Verification Audit](https://www.silo.finance/_files/ugd/fd5034_98066b4c70ea46b5862a00670179f067.pdf))

# 

(source: [Certora Formal Verification Audit](https://www.silo.finance/_files/ugd/fd5034_98066b4c70ea46b5862a00670179f067.pdf))

**ABDK Consulting** auditors in their [Audit Report](https://drive.google.com/file/d/1WXaB3ICLv4rSEX86POK3-NaOIxXwyq9l/view) found 6 major, 1 moderate and 65 minor issues.

**Quantstamp** [audit report](https://drive.google.com/file/d/10GyfA-nBJ5jqLWW9LEYJQeFem8qSgNH6/view) recorded 14 issues: 0 high, 5 medium, 3 low and 6 info risks

# Summary

Text

## Sources