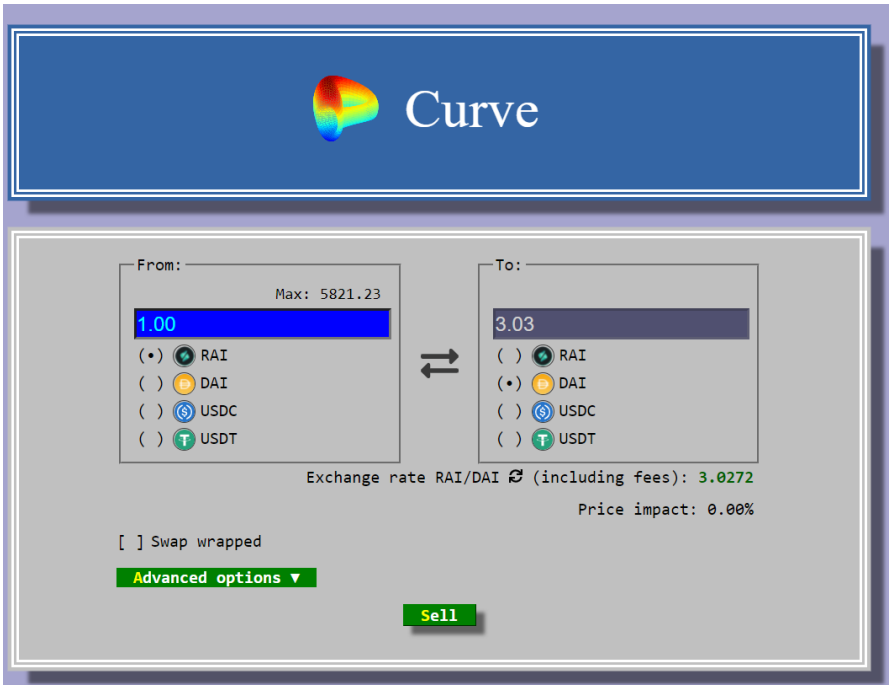
RAI3CRV Gauge onboarding | Risk analysis



https://curve.fi/rai

Key Information/Links:

- RAI Analytics (Provided by RAI)
- RAI Dune Analytics Overview, (Graph citations)
- ETHUSD Chainlink Oracle
- RAIETH Chainlink Oracle
- Curve RAI-3CRV Pool

Abstract

RAI has added a proposal to onboard the RAI3CRV Gauge Controller and enable veCRV holders to assign a gauge weight: https://gov.curve.fi/t/proposal-to-add-the-rai3crv-gauge/2422 This risk analysis report will inform veCRV holders about the RAI protocol and the potential risk of this protocol while using the RAI3CRV pool.

RAI Asset Profile

Nomics: https://nomics.com/assets/rai3-rai-reflex-index
Collateral Name (and symbol): Rai Reflex Index - RAI
Token contract: https://etherscan.io/token/0x03ab458634910aad20ef5f1c8ee96f1d6ac54919
History: RAI was deployed at block 11848304: Feb-13-2021 12:33:18 PM +UTC
Asset Short Description: RAI is a non-pegged, ETH-backed stable asset. It is useful as more "stable" collateral for other DeFi protocols (compared to ETH or BTC) or as a stable asset with an embedded interest rate.

Official Links

Website: https://reflexer.finance/
Whitepaper: https://github.com/reflexer-labs/whitepapers/blob/master/English/rai-english.pdf
Github: https://github.com/reflexer-labs
Twitter: https://twitter.com/reflexerfinance
Discord: https://discord.gg/83t3xKT
Medium: https://medium.com/reflexer-labs

Project summary

RAI is an ETH pure, non-pegged stablecoin that resembles the original vision for Single Collateral Dai. RAI solves an issue present in all decentralized pegged assets, namely the fact that they cannot charge negative rates to their holders and compel them to sell when the market price of the asset is above the peg. RAI is designed as a reserve asset for other DeFi protocols and is a first step to detach from the fiat monopoly.

Strong points:

- Strong & respected team with a passionate & dedicated community;
- Strong technical workflow with security in mind;
- Positive data showing RAI's stability and growing TVL;
- A clear roadmap towards decentralization and governance minimization

Weak points

- Currently, RAI has a 3/5 multisig with a 24-hour delay for any governance actions

Additional Explainers:

- https://newsletter.banklesshq.com/p/defi-needs-trust-minimized-money
- https://medium.com/reflexer-labs/rai-system-simulations-part-1-safe-owners-876a6bd55385
- https://newsletter.banklesshq.com/p/defi-needs-trust-minimized-money
- https://medium.com/reflexer-labs/stability-without-pegs-8c6a1cbc7fbd
- https://medium.com/reflexer-labs/summoning-the-money-god-2a3f3564a5f2

Risks Analysis

We will explore the risks - involved in using the RAI3CRV pool – in relation to the financial and the technical/procedural side. Before you decide to deposit your assets in the RAI protocol, acquire RAI, use RAI3CRV or any other pool, you should do your research and understand the risks involved.

Financial risk

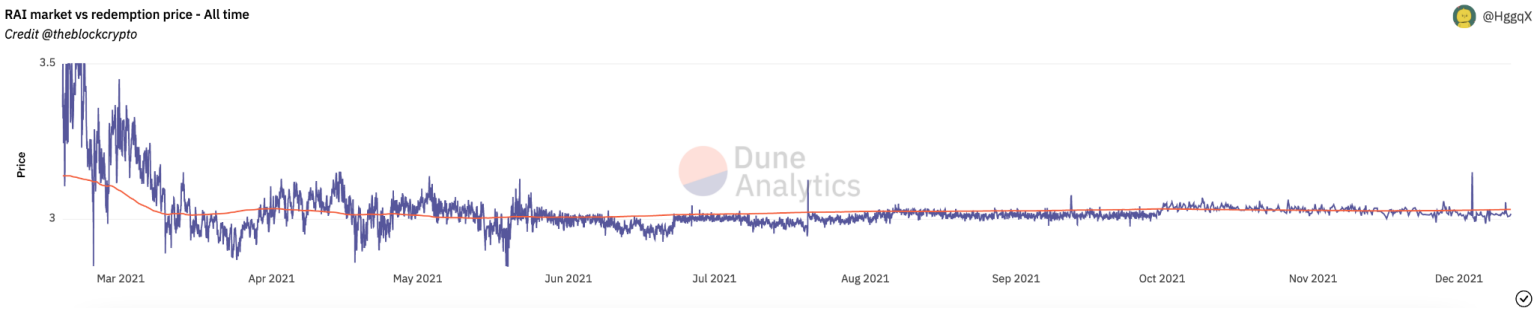
RAI is an algorithmic non-pegged stablecoin. The underlying stability mechanism works by different monetary factors that keep the price “Stable”. This section will look at the financial risks of RAI ever getting out of PEG.

RAI’s stability mechanism

To get an understanding of the financial risks it is important to understand the stability mechanism so that we can interpret the market data and can draw conclusions on the financial risks. GEB is a framework that is used to deploy RAI it is a modified fork of MCD that has several core differences (see their documentation: https://docs.reflexer.finance/).

Redemption price

The redemption price is the desired price of RAI and encourages people to deposit/borrow or repay/withdraw. The redemption price is set by the redemption rate that, if positive, increases the redemption price (re-values) or, if negative reduces the redemption price (de-values).



https://dune.xyz/queries/40087/79136

(Following graph is an example of RAI market vs Redemption price over time. As is visible from the plus two hundred days of existence of the protocol, RAI price is considerably stable, considering external factors as an ETH backed asset (e.g., ETH Losing nearly 50% of its value in 2021).

Market price

The market price of RAI refers to the price at which the asset is traded on the secondary market and is determined via a Chainlink oracle with the following sources.

- Uniswap v2
- Uniswap v3
- Coinbase RAIUSD

- Curve RAI-3CRV prices (Pending)

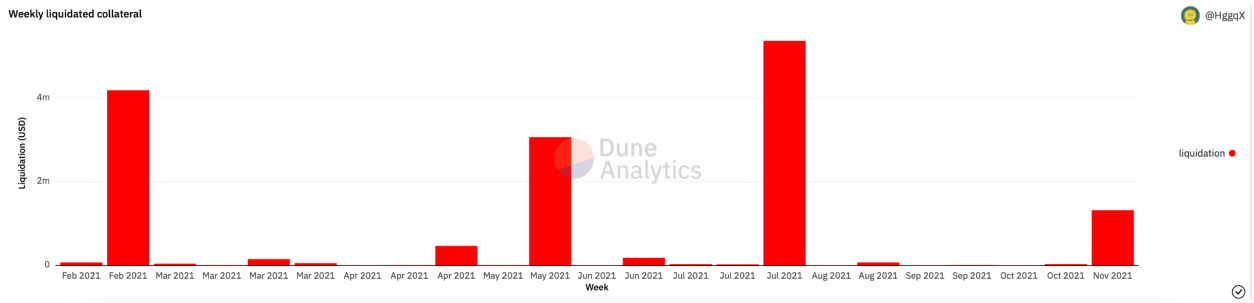
Redemption rate

The redemption rate refers to the price at which the asset is devalued or revalued. Devaluation or revaluation occurs when the redemption rate changes.
https://dune.xyz/queries/40091/79144

- When RAI's market price > redemption price for a sustained period, the redemption rate will become negative
- When RAI's market price < redemption price for a sustained period, the redemption rate will become positive
- When RAI's market price = redemption price for a sustained period of time, the redemption rate will settle at a steady state (that may be non-zero)

Liquidations/Keepers

Like Maker DAO, RAI has keeper bots that read an auction's status directly from the blockchain or from a Graph node. Its unique feature is the ability to plug in external bidding models, which tell the keeper when and how much to bid. Bid prices are received from separate bidding models. Below we see the number of liquidations in the system and the liquidated RAI/ETH.



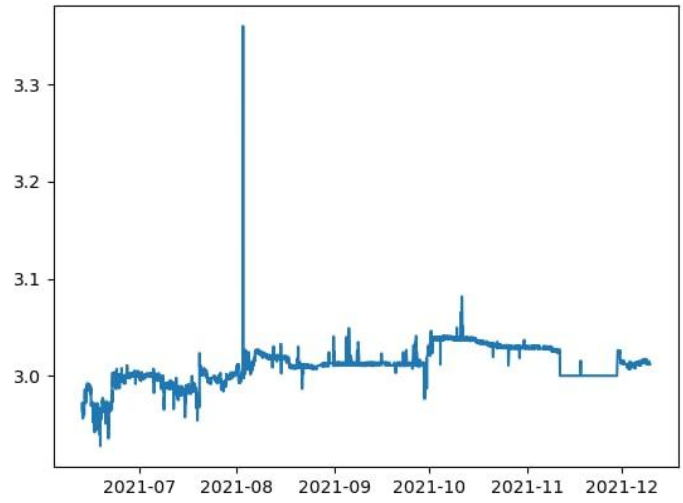
https://dune.xyz/queries/39772/78300
The auction-keeper can use an RAI/DAI Uniswap v3 flash-proxy to liquidate a large SAFE.

Shutdown Module

The Shutdown Module oversees winding down the system and returning all collateral back to users in case of a serious threat, such as long-term market irrationality, a hack, or a security breach. In case of any emergency, LP providers to the RAI3CRV pool can always withdraw the underlying value that backs RAI. Everyone can trigger the system shutdown, but in order to do so, has to burn 120K FLX tokens +- 12% of the supply. This might be lowered to 10% before ungovernance, more info: https://docs.reflexer.finance/system-contracts/shutdown-module

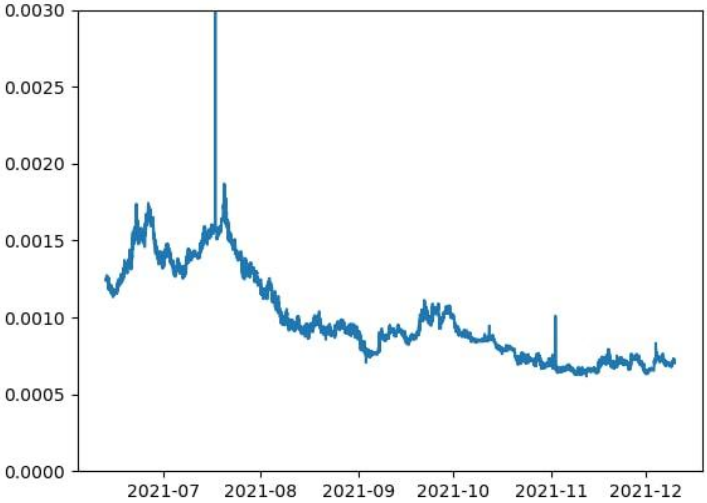
RAI $~PEG

Now we understand RAI's stability mechanism we can start to interpret the price data, look at potential risks, and see how strong the $~PEG holds itself. As seen in the data below the RAI price stays stable. It almost seems a bit over-damped its price in dollar value is barely affected by changes in ETH price. Looking at the Liquidations/Keepers statistics the network did not have a big liquidation shock in such a scenario the protocol still needs to prove itself.



RAI-DAI
(6 months @ 5min resolution)

ETH-DAI
(6 months @ 5min resolution)



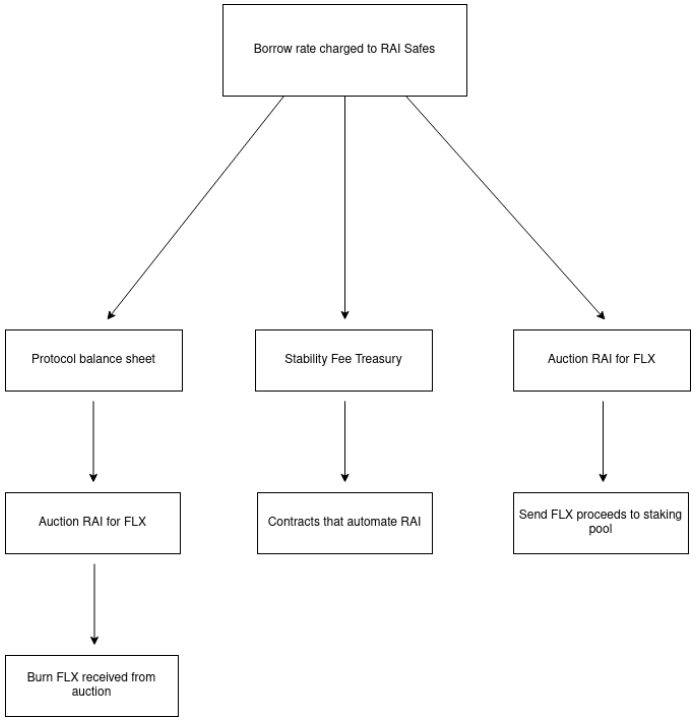
RAI-ETH
(6 months @ 5min resolution)

Technical/Procedural risks

Besides losing $~PEG there are also technical and procedural risks. In this chapter, we will look at these risks. Technical risks are Smart Contract risks, Governance risks, Black Swans, and Oracle Attacks. Procedural risks are mistakes that happen when people do not follow internal protocols and keys are leaked or code gets merged that should not be released.

DAO Backstop and ungovernance

In return for depositing collateral and minting RAI, users are charged a stability fee. The fee is used to encourage external parties to maintain the protocol and build a surplus buffer to fix bad debts. RAI is on a route off ungovernance its protocol and move to community voting; the community can vote with Reflexer Ungovernance Tokens (FLX) that is now being distributed to users of the protocol.



FLX token will have two main functions:

1. Backstop mechanism: If the RAI protocol goes down, FLX stakers are the first line of defense. Debt auctions, which mint new FLX and auction it in exchange for RAI, are the second line of defense.

2. Ungovernance: once governance minimization is complete, FLX holders will be able to take management of any remaining RAI components or, if necessary, continue to manage components that may be difficult to ungovern (such as oracles or any other component interacting with other protocols)

Link: https://docs.reflexer.finance/flx-mechanics

Governance Minimization

There is multisig risk in the main RAI protocol that is managed by a 3-5 multisig with a 24-hour delay. The multisig address is: 0x427A277eA53e25143B3b509C684aA4D0EB8bA01b. The multisig will be in place until ungovernance is complete, the following deadline is to be complete by August 2022, and move to a community vote structure.

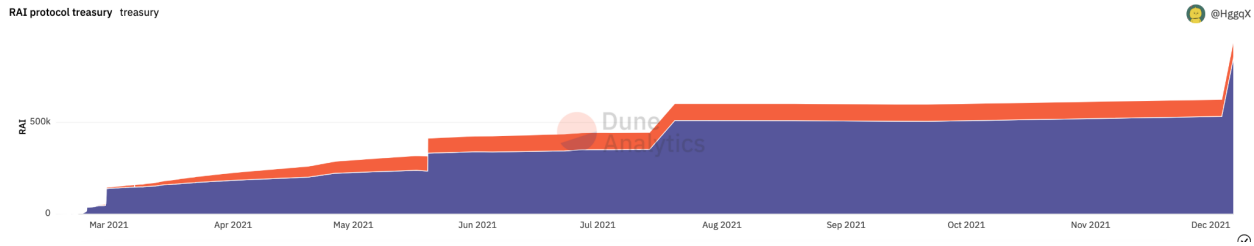
See here the full “ungovernance” documentation:
https://docs.reflexer.finance/ungovernance/governance-minimization-guide

1. The protocol’s governance must not add or plan to add any more collateral types.
2. All the infrastructure for governance minimization must have been audited and evaluated in production.
3. The system must accrue enough surplus in its main treasury so that it can afford to pay for oracle, PID, state management, etc. costs for at least six months.

Revenue/TVL

The stability fee that generates revenue comparable to Maker DAO and is expected to be switched on at a later date. The TVL is 51,386 ETH (12-12-2021). The treasury contract: [0x2D3cD7b81c93f188F3CB8aD87c8Acc73d6226e3A](0x2D3cD7b81c93f188F3CB8aD87c8Acc73d6226e3A)

Via the RAI's analytics dashboard we can see the treasury balances.



https://dune.xyz/queries/62716/125083

Audit reports:

Fork of Multi-Collateral DAI that is a great starting point, as MCD was developed by some of the brightest minds in the space. Not only that, but the system was formally verified, audited, and went through a generous bug bounty before hitting production. It was then battle-tested for more than a year before RAI hit main net. The changes RAI made include all features you do not see on MCD (the PID controller, liquidation protection, different auction houses, and others) and translated the cryptic Maker DAO terminology to readable English.

Besides a good codebase, there are multiple audits done:

1. Open Zepppelin
    - https://github.com/reflexer-labs/geb-audits/blob/master/open-zeppelin/core-contracts/oz-geb-protocol-audit.pdf
2. Quantstamp
    - https://certificate.quantstamp.com/full/reflexer-staking-and-auction-house
    - https://github.com/reflexer-labs/geb-audits/blob/master/quantstamp/helper-contracts/second-audit/Reflexer%20Second%20Engagement%20-%20Final%20Report.pdf
    - https://certificate.quantstamp.com/full/reflexer-rai-curve-pool
3. Solidified
    - https://github.com/solidified-platform/audits/blob/master/Audit%20Report%20-%20Uniswap%20V3%20Liquidity%20Manager%20%5B24.06.2021%5D.pdf
    - https://github.com/reflexer-labs/geb-audits/blob/master/solidified/helper-contracts/Solidified%20Audit%20Report%20-%20Reflexer%20%5B26.01.2021%5D.pdf

Besides the 3 audits, they have an ongoing bug bounty campaign:
https://immunefi.com/bounty/reflexer/

RAI3CRV Curve pool

The RAI3CRV Pools: https://github.com/reflexer-labs/curve-contract (Created at 17-11-2021) is a custom implementation by Reflexer Labs and Curve DAO. They have generated an audit in collaboration with QuantStamp.
https://github.com/reflexer-labs/geb-audits/blob/master/quantstamp/curve/Reflexer%20RAI%20Curve%20Pool%20-%20Report.pdf

Current pool statistics 12-12-2021

```
Currency reserves

RAI: 8,097.77 (26.67%)
3Crv: 22,267.73 (73.33%)
RAI+3Crv: 30,365.50

Fee: 0.040%
Admin fee: 50.000% of 0.040%

Virtual price: 1.0008 [?]
A: 100

Liquidity utilization: 0.00% [?]
Daily USD volume: $0
```

https://curve.fi/rai

Conclusion

We can conclude and reflect on the financial risks and the technical/procedural risks.

- RAI price stays stable, it is almost over-damped, its price in dollar value is barely affected by changes in ETH price and stays at $3;
- RAI is a fork of Multi-Collateral DAI that is formally verified, audited, and went through a generous bug bounty program before hitting production. The changes made are small but effective for the long-term growth of the protocol;
- There have not been big liquidation shocks in the system. The liquidations/keepers mechanism still needs to prove itself, but looks promising.
- There is multisig risk in the main RAI protocol that is managed by a 3-5 multisig. The multisig will be in place until ungovernance is complete by August 2022 and RAI moves to a community vote structure.

If there are ever any issues with RAI, an emergency shutdown would happen. This means that all RAI holders can claim the underlying collateral. This means reducing risk and always provides a way out in case of a black swan event.

RAI is a strong crypto native team that showed hands-on support in getting their pool audited and pushing implementation forward. This gives confidence in the long-term vision of RAI and why it would be good for veCRV holders to onboard this pool so it can benefit from the trading fees once the pool gets more volume.