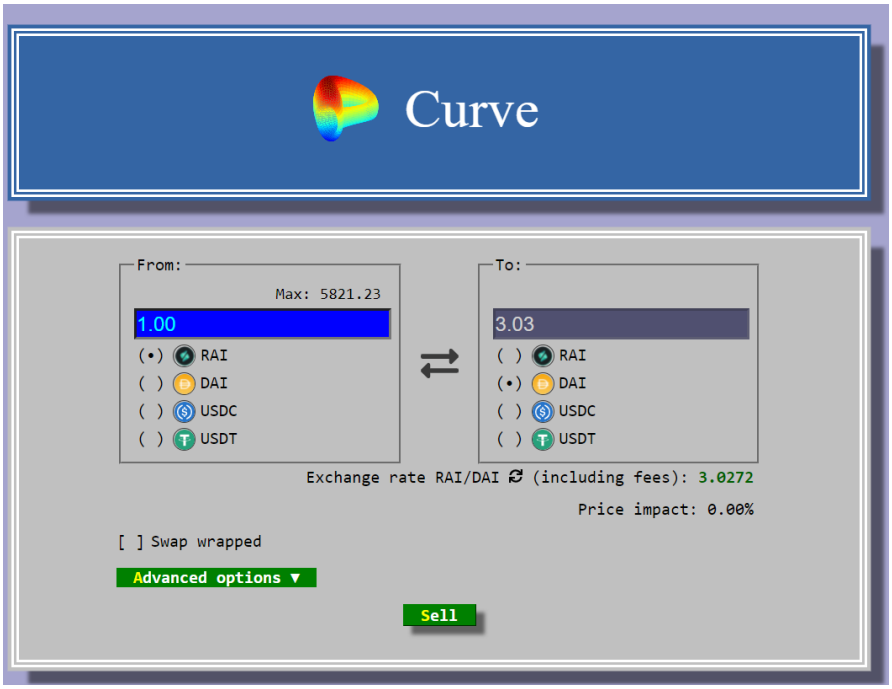
RAI3CRV Gauge onboarding | Risk analysis



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 what the risks there are 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

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 was designed as a reserve asset for other DeFi protocols as well as 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 by looking at the financial risks and technical/procedural risks.

Financial risk

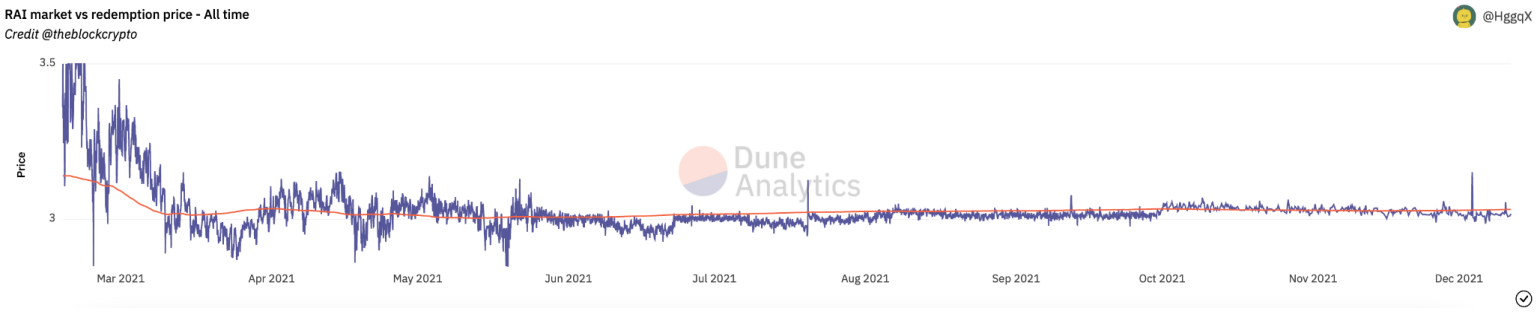
RAI is an algorithmic non-pegged stablecoin the underlying stability magnesium works by different monetary factors that keep the price “Stable”. Before you decide to deposit your assets in the RAI protocol, acquire RAI, use RAI3CRV or any other pool, you should do your research and understand the risks involved.

RAI’s stability magnesium

To get an understanding of the financial risks it is important to understand the stability magnesium 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 to you can read in 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 it reduces the redemption price (de-values).



https://dune.xyz/queries/40087/79136
(Following graph is an example of RAI market vs Redemption price all time, as is visible from the plus 200 days of existence of the protocol, RAI price is considerably stable considering external factors as an ETH backed asset. (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)

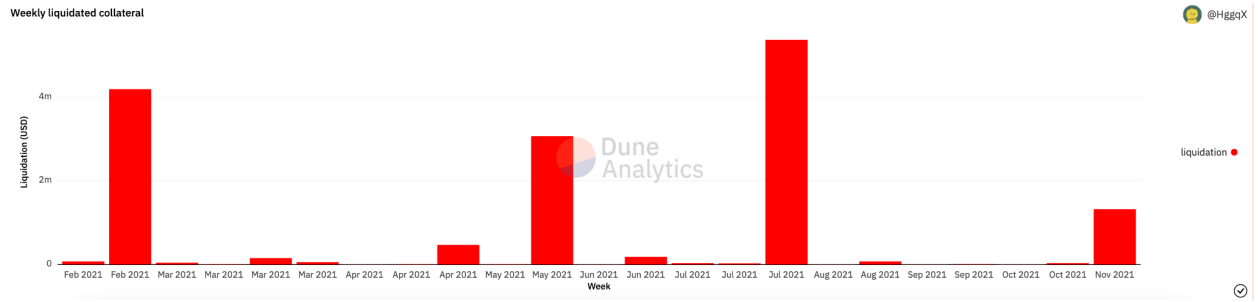
Redemption rate:

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 of time, the redemption rate will become negative
- When RAI's market price < redemption price for a sustained period of time, 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

Similar to Maker DAO in RAI has keeper bots that can 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.



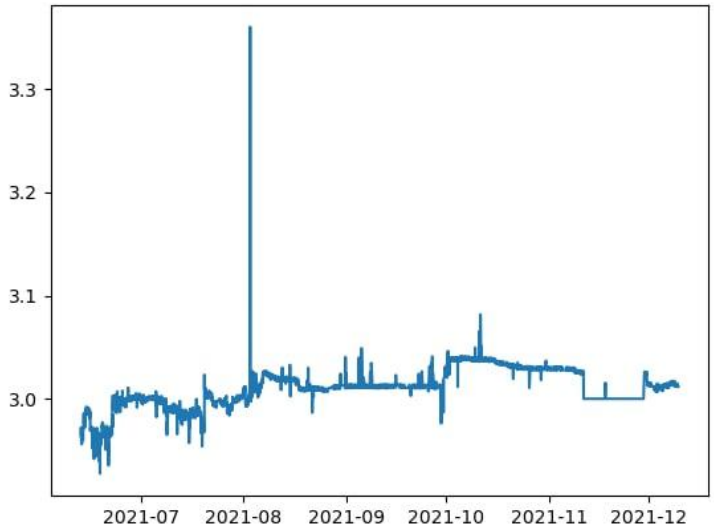
https://dune.xyz/queries/39772/78300

Shutdown Module:

The Shutdown Module is in charge of 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.
More info: https://docs.reflexer.finance/system-contracts/shutdown-module

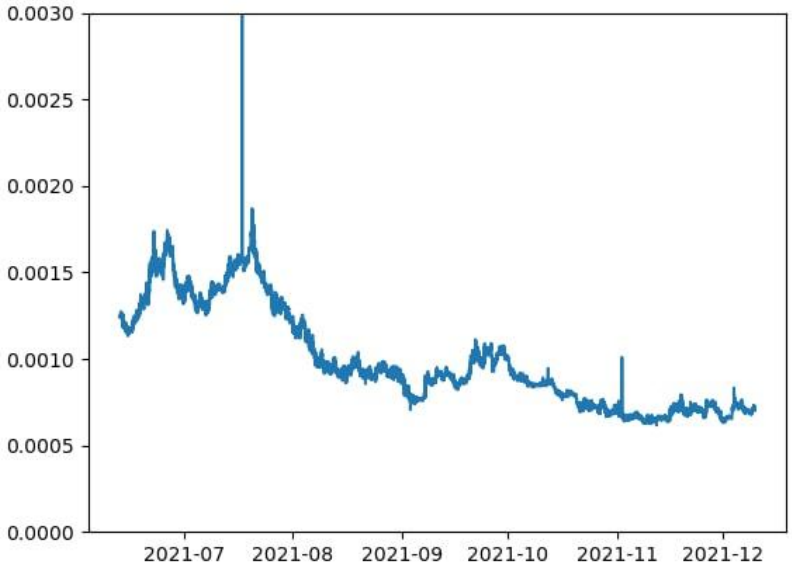
RAI $~PEG and Curve pool stats

Now we understand RAI's stability magnesium we can start to interpret the price data and look at potential risks and see how strong the $~PEG holds itself. As seen in the graphs



RAI-DAI (6 months @ 5min resolution)

ETH-DAI (6 months @ 5min resolution)



RAI-ETH (6 months @ 5min resolution)

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 as well as build a surplus buffer to fix bad debts. RAI is on a route off un-governance its protocol and move to community voting the community can vote via Reflexer Ungovernance Token (FLX) that is now distributed to users of the protocol.

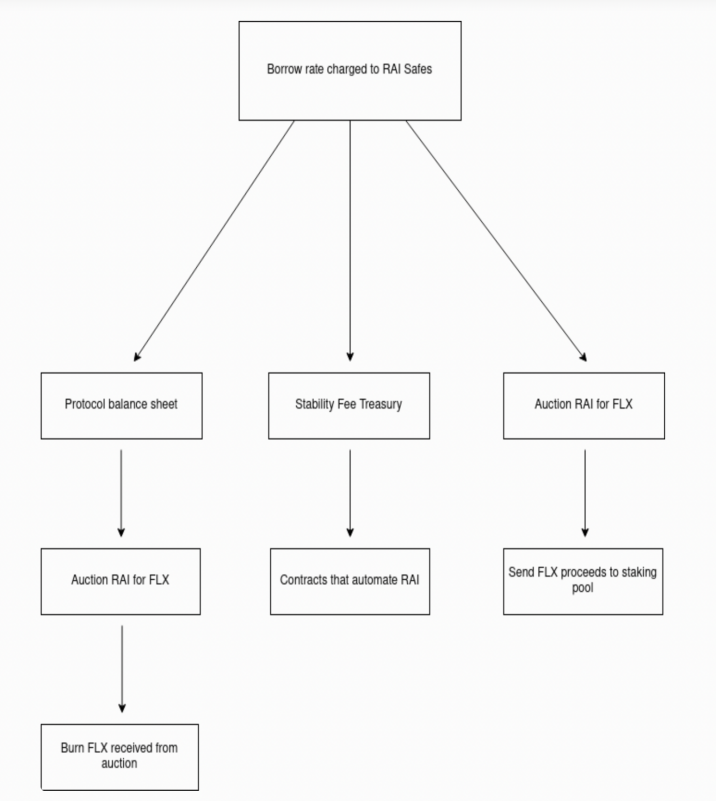
https://nomics.com/assets/flx3-reflexer-ungovernance-token

FLX Mechanism: (The Quest for Un-Governance).

FLX token will have two main functions in the RAI protocol:

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.

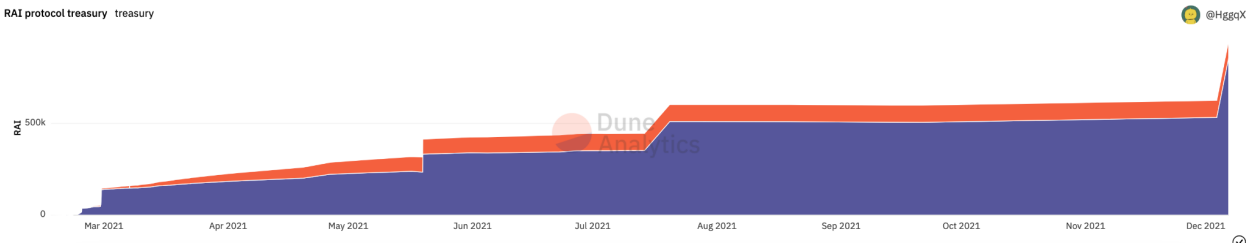
2. Ungovernance: once governance minimization is complete, FLX holders will be able to take management of any remaining RAI components or, if necessary, continue to manage components that may be difficult to ungovern (such as oracles or any other component interacting with other protocols)



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

Treasury Inflows:

Stability fee contract:
https://etherscan.io/address/0x83533fdd3285f48204215e9cf38c785371258e76



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

Technical/Procedural risks

There is multisig risk in the main RAI protocol that is managed by a 3-5 multisig with a 24-hour delay on any actions, the following leads to possible issues and exploits:

The multisig address is 0x427A277eA53e25143B3b509C684aA4D0EB8bA01b. The multisig will be in place until un-governance is complete, the following deadline is to be complete by August 2022 and we move to a community vote structure.

Required steps for **"Un-Governance"**:
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 tested in production.

3. The system must accrue enough surplus in its main treasury so that it affords to pay for oracle, PID, state management etc costs for at least 6 months.

So mid-August un-governance, soon after we switch to community

Audit reports:

Besides good audit coverage, there is an internal workflow that seems to be used that also hardens all the code produced and committed.

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

The RAI3CRV Pools:
https://github.com/reflexer-labs/curve-contract

seems solid and is a clean implementation and it is good that they have generated an audit that backs up our own research.

https://github.com/reflexer-labs/geb-audits/blob/master/quantstamp/curve/Reflexer%20RAI%20Curve%20Pool%20-%20Report.pdf

Conclusion

Looks good redemption rate: https://dune.xyz/queries/40087/79136