INRA Whitepaper

INRA is an Indian Rupee stablecoin backed by BUSD (Binance USD), independent collateral pools of INRA-BUSD, INRA-BAT and a rate stabilization algorithm using an internal exchange.

Summary

INRA is a stablecoin backed by BUSD stored in the contract.

The stabilization of the rate is ensured by using the internal exchange system at the current INR-BUSD rate using the average rate for 15 minutes of the Zebpay exchange. For more information about securing the exchange rate, see the relevant section.

Additional exchange rate stabilization is provided by independent pools of INR-INRA with a 1 to 1 exchange (excluding transaction fees), as well as independent pools to other stablecoins INR-USDT, INR-USDC and others.

The exchange algorithm seeks to reduce the collateral usage with each exchange:

- When exchanging BUSD for INRA, a commission is charged, subsequently the commission in INRA is completely burned. Burning will be secured as long as collateral utilization exceeds 50%.
- When exchanging INRA for BUSD, an additional fee is charged, which goes into the collateral pool, reducing collateral utilization and increasing stored collateral. Additional commission can be increased and decreased automatically, if collateral utilization exceeds 100%

INRA buying is available at any time in the internal exchange at the rate and commission indicated on the site.

BUSD buying is available at any time, subject to the availability of sufficient collateral at the rate and commissions indicated on the site.

Rate change

Changing the INRA rate is divided into two stages:

1. The rate is set by the centralized INRA oracle under the control of the development team, taking into account the exchange rate on external exchanges, as well as the economic situation.
2. In the second stage, control of the rate is transferred to the control of the

DAO, which owns the governance token, which will be distributed between the original owners of INRA tokens.

At the stage of centralized control, the exchange rate, burning, and minting of the token is controlled by an oracle managed by the INRA team. Aware of the fact that the centralized management is a bottleneck in trust in the stability of the token, there are plans to make the transition to DAO management after the completion of the following stages

- Marketing activity and popularization.
- Providing the integration of the token into trading systems, exchanges and DEX.
- Getting no more than 60% collateral usage.
- Issue of DAO tokens and contract.

The definition of completion of each stage is determined by the project team. To ensure process transparency, following procedures will be followed:

- Publication of daily and weekly reports on the use of collateral and issuance of tokens.
- Publication of information on the status of additional collateral pools.
- Publication of estimates on the completion of each of the stages of information on the burning of tokens and fees.
- Publication of information about the work and provision of gateway bridges.
- Technical user support, AMA sessions, participation in public events, etc.

Force majeure situations

- In case of a sharp change in the rate of the anchor currency, a situation of too high collateral utilization may occur. When the collateral utilization reaches more than 100%, the exchange system automatically increases the exchange commissions to increase the amount of collateral in the contract. If it is impossible to increase the collateral and the collateral usage exceeds 150%, trading in the internal exchange stops until the pool stabilizes to 102% OR 30 days whichever happens earlier.

  If stabilization has not been achieved after 30 days, each owner of the token has the right to demand a return from the provision of the pool share corresponding to the ownership of the token.

- Despite careful security checks and controls, in case of detection of critical or fatal errors in the operation of the smart contract, the exchange rate control system, as well as the detection of a hack, the team stops the operation of the smart contract and withdraws security to the escrow contract, which will freeze all BUSD for a period of 30 days to investigate the incident. After this period, the escrow contract will transfer all collateral to the contract address specified during the investigation.

- Even though control keys are unlikely to be leaked, the keys will be renewed every 6 months, contract ownership is also transferred to the renewed key (only in the team control phase)

Security

The most vulnerable elements of the system are:

- Exchange rate oracle
- Cross-chain bridge oracles

To ensure oracle security uses a three-point access control scheme:

- Signing oracle is located on an encrypted VDS.
- The VDS has a separate VPN network that is not connected to the network of the host machine.
- The exact location of the host is known only to the administrator serving the host, but the administrator does not have access to the VDS.
- The location of the host is not accessible to an administrator with update rights.
- The upgrade administrator does not have access to the source code and keys on the VDS.
- Developers do not have access to the host server, the VDS, or the keys stored on the server.
- Key rotation is performed fully automatically on VDS, without human intervention
- VDS backup is performed every hour, as well as every key rotation in encrypted form (snapshot) on the resources of the organization (at least 4 geographically separated storages) .

Independent pools

INRA tokens can be stabilized using independent exchange pools. Typically, such pools are participants performing a 1 to 1 currency exchange peg to a stablecoin, independent exchanges and exchangers.

INRA also implements its independent direct exchange pool, but the location of the pool remains anonymous to avoid attacks.

Motivation of the INRA

The team receives a commission, proposed at 1% from each operation on internal exchange. The commission will also be saved when switching to DAO management. Until the collateral level reaches 50%, the team intends to burn all the commission received in INRA and also to exchange the received BUSD for INRA with subsequent burning, except for the costs incurred to ensure operation.

INRA we trust.

Usage Policy

Risks

INRA does its best to reduce the risks of using the token, but you should always be aware of external risks of market changes, technical failures, external factors, including currency instability, targeted attacks on the integrity of the security. The project team cannot be held responsible for losses caused by force majeure, technical failures, external attacks, and others. INRA is not an investment asset, pyramid scheme or casino. By using INRA, you acknowledge that you are fully aware of all the risks associated with cryptocurrency trading and possible losses when using it.

Technical Policy

Why don't we use upgradable contracts?

The refreshable contacts mechanism typically uses proxy contracts. Our policy implies the simplest and most direct implementation, so that any person, even with basic programming knowledge, can understand how the contract works. If updates are needed, we will create a separate contract, and set up migration options between the new and the old one.

Affiliation with the Indian Republic

INRA is not affiliated with the Indian Republic or with any state or country. The goal of the project is to create an asset with the main collateral in an alternative currency and the ability to create a direct exchange using independent pools that are provided by third-party project participants.

Sanctions

Project not affiliated with the Indian Republic, but the token may also fall under the sanctions of the United States and Europe. The token is implemented in such a way that we do not have the technical ability to block funds on user's wallets, however, various exchanges (PancakeSwap, Binance) have the ability to control the exchange of the token for specific addresses. Be careful when choosing how to store and exchange the token.

Technical implementation

Internal exchange

Internal exchange works on the basis of information about the course issued by the oracle. The order of the exchange:

- The user goes to the exchange page on the INRA website.
- The user enters the required amount and direction of the exchange.
- The site makes a request to the smart contract and a request to the oracle about the current exchange rate.
- Information about the results of the exchange is displayed to the user.
- The user initiates the exchange.
- If the contract does not have access to tokens for exchange, an approval request is sent to the BUSD / INRA contract and the user is prompted to sign the transaction
- If the transaction is successful or if confirmation is not required, the site sends a request to the oracle server with information about the exchange. The oracle sends to the site a signed message with information about the exchange and expiration time - 60 seconds.
- Within 60 seconds, the user signs and sends the exchange transaction to the INRA smart contract.
- The user receives tokens as a result of the exchange, excluding the commission.
- The platform fee is sent to the INRA team wallet.
- The fee for providing the service remains in the smart contract

Exchange rate updates

The exchange rate source is the Zebpay API in the INRA/BUSD pair. The rate is aggregated over a period of 15 minutes and an average is calculated. Checks for errors are performed before updating the rate:

- The average rate change over 15 minutes should not exceed 10%. If the change persists for 40 minutes, it performs a rate update
- Exchange rate fluctuations for a period of 5 minutes do not exceed 30%. This condition is satisfied until stabilization.
- If the rate fluctuation does not exceed 5% in 5 minutes, the current received rate value is used

Control protection

One-time large transactions are blocked by the oracle for 10 minutes if the volume of the transaction exceeds the collateral by more than 10%. The Oracle notifies the INRA team of a large exchange. If the command does not block the exchange operation within 10 minutes, it can be performed. The condition is temporarily disabled for the duration of the stablecoin launch**.**

Exchange operations are blocked if the internal rate and the exchange rate in the INRA/BUSD pair on PancakeSwap differ by more than 10%. The condition is temporarily disabled for the duration of the stablecoin launch**.**

Stabilization

The main mechanism for stabilizing the currency in foreign markets is an internal exchanger operating at the external INRA/BUSD rate. If the exchange rate diverges by more than the amount of the exchange commission, it becomes profitable for users to sell or buy INRA on the internal exchanger, thereby not only equalizing the exchange rate between the external markets of INRA and INR, but also, thanks to the collateral commission, increasing the amount of BUSD in the smart contract.

BUSD-INRA stabilization fee: 0%

INRA-BUSD stabilization fee: 1%

The Stabilization Commission increases when the utilization of the collateral is exceeded by more than 99%.

When exceeding from 99% to 110%, the commission is calculated by the formula

Fee = (110 - PoolUtilization) / AvgSwaps

Where PoolUtilization - the current pool utilization percentage AvgSwaps - the total number of exchanges for the last hour.

If the pool utilization exceeds 110%:

Fee = (PoolUtilization - 100) / AvgSwaps

The fee is changed automatically.