RAILGUN 101

Copy

Overview

What is RAILGUN?

RAILGUN is code that exists on every Ethereum node. It's a privacy system built directly on-chain for Ethereum, BSC, Polygon, and Arbitrum. It uses Zero-Knowledge (ZK) cryptography to enable private use of smart contracts and DeFi, all without leaving the security of the user's preferred chain. The RAILGUN code has no owner. Interactions on your chain of choice are made private.

The RAIL token is purely a governance token and is not a privacy coin. Holding RAIL is not necessary to use the protocol and it does not confer any rights to holders. You can read more about governance here.

RAILGUN users have access to a special 0zk address that are confidential on Etherscan, Arbiscan, or any similar resource. Independent wallet providers can use the RAILGUN protocol, head here↗ to select from a list of wallet providers. RAILGUN is 100% non-custodial.

The user experience is similar to using a public wallet to interact with Ethereum/EVM chains, just with the added ability to interact privately.

Archived copy · cryp2nova.com

As RAILGUN is simply on-chain smart contract code, privacy is achieved without the need to move to a separate chain. This provides 2 main advantages:

1. **Security & Decentralization** - No centralized control, no extra validators, and no trusted bridges.
2. **Full Ecosystem** - Rather than an isolated ecosystem on a standalone privacy chain, RAILGUN users have full access to all the economic activity and functions that the chain provides, and benefit from the rich history of existing dApps and builders.

RAILGUN has 2 main components:

1. **RAILGUN-Integrated Wallets** - EVM wallets built by separate independent community developers through which users can use the RAILGUN protocol. A list can be found here↗.
2. **Developer Tools** – includes TypeScript SDKs for building RAILGUN privacy into existing/new wallets or a privacy enabled dApp. Head to the developer guide↗ to start building with RAILGUN.

RAILGUN's code is verified and publicly viewable, and its repository can be found here.↗

CRYP2NOVA

Archived copy · cryp2nova.com

Benefits and use cases of RAILGUN

As the diagram shows, looking from the outside in, when tokens are moved into RAILGUN’s smart contract, tokens and wallets become indistinguishable from one another without mixing one user's funds with another. Because of this, all transferring, swapping, lending, borrowing, and dApp calls create more noise and improve privacy for every other user. These DeFi interactions allow RAILGUN to function more privately than other protocols with a similar amount of tokens and users.

Read this article ↗ for more on how privacy works in the RAILGUN protocol.

Due to the availability of DeFi transactions, more rigorous privacy is achieved with RAILGUN with less liquidity and in a shorter timeframe than with other privacy systems. Arbitrary dApp interactions within RAILGUN’s privacy system also incentivizes users to hold their tokens for longer in RAILGUN as there is less reason to move tokens out of RAILGUN.

Potential use cases:

Archived copy · cryp2nova.com

1. **Alpha Protection:** Traders who want to keep their alpha confidential can trade freely and maintain their informational advantages. RAILGUN's privacy system enables users to trade with reduced risk of hard-fought trading strategies and patterns being discovered and ripped off by freeloading actors, who can obtain such data on-chain by tracing interactions, then running them through analysis software to reverse engineer said strategies, without doing any of the actual work.
2. **Compliance with Law:** Businesses and professionals must use privacy tools, such as RAILGUN, to make sure that financial data is not leaked when interacting with clients. Lawyers, doctors, and psychologists, for example, are not allowed to reveal that their clients have paid for advice. They must protect the identity of the person engaging their services, as set out in common law, professional rules of conduct, European and British GDPR, the USA's HIPAA, and other data protection legislation. Other businesses and professionals also have strict laws that apply to them to protect the financial information of their customers & staff. RAILGUN is used to comply with these laws.
3. **Private Payroll:** The privacy features of RAILGUN are needed for payroll services, when companies pay in cryptocurrency.
4. **Donation Privacy:** RAILGUN users can donate to charitable causes using cryptocurrency without needing to publicly reveal their link to these causes.
5. **Personal Protection:** RAILGUN users are not exposed on services like Nansen or Etherscan, where notable wallets are labelled or known. Any cryptocurrency user who wishes to protect their personal privacy can do so using RAILGUN.

CRYP2NOVA

RAILGUN is a revolutionary toolkit and is objectively the most uncompromising privacy solution for DeFi. Private DeFi will enable new business possibilities for the cryptocurrency industry that are not possible on public blockchains. All other privacy solutions have some trade-offs, such as requiring users to trust custodial bridges or trade with fragmented/non-existent liquidity.

Developer Guide

If you're a developer looking for the SDK documentation. You can find it here ↗.

Next

Archived copy · cryp2nova.com

Getting Started

Last updated 6 months ago

Was this helpful?

Archived copy · cryp2nova.com