# RAILGUN_

/// WHITEPAPER
MMXXI

RAILGUN PROJECT
NOVEMBER 6, 2021

目次



RAILGUN PROJECT

NOVEMBER 6, 2021

# RAILGUN

***RAILGUNは、ユーザーやオンチェーンアプリケーションのプライバシーと匿名性を実現するイーサリアム上に構築された堅牢なゼロ知識システムです。***

RAILGUN: 業界初、ユーザーがイーサリアム上のDeFiスマートコントラクトを使用する際に、イーサリアムのハッシュパワーによる完全なセキュリティとトレードオフすることなく、プライバシーを保つことができます。

# ビジョン

プライバシーは、すべての人間が本能的に大切にしているものです。広く知られている人権であり、他人へのプライバシーを否定する人も、自身には要求します。プライバシーと匿名性は、例外ではなく、デフォルトであるべきです。個人情報や財務情報を公開する際には、同意が必要であるべきです。

イーサリアムのチェーン上に直接構築されたプライバシーと匿名性のシステムのRAILGUNは、情熱的で熟練したプライバシー愛好家の小さなコミュニティにより開発され、DEX、融資プラットフォーム、および人気のスマートコントラクトアプリケーションと直接やりとりすることができます。RAILGUNは、あなたの行動やアイデンティティを秘密にし、プライバシーを保護することにより、匿名性を実現します。しかもRAILGUNは、ユーザーが安全で活気のあるイーサリアムとそのエコシステムから離れることなく、これを実現します。それだけでなく、RAILGUNはその革命的な利点を他のブロックチェーンのエコシステムにも次々ともたらしていきます。

RAILGUNは、プライバシーを保護するゼロ知識方式で、監査役やコンプライアンスオフィサー用の検証可能な行動・残高レポートを作成することができます。資金が公的には隠されたままであることを意味しますが、ユーザーが選択した同僚や受取人にソースの証拠を提供することができます。RAILGUNの目的は、オンチェーンで行われるアクションの第三者による検証可能性を奪うことではなく、誰がいつ何を見るかを選択する力をユーザーに還元することです。

# はじめに

パブリックブロックチェーンとは、まさに「パブリック」なものです。現在最も普及しているブロックチェーンでは、ユーザーのオンチェーン活動のすべてが全世界に公開されており、10年後もそうであると考えられます。商業的なオンチェーン分析システムが改善され、ユーザーのすべての取引が簡単に追跡できるようになると、ブロックチェーンユーザーには様々な問題が生じます。これは、複数の国に既に存在するプロの電子監視組織の潜在的な努力や能力を考慮する前の話で、個人やNGO、さらには国が大規模に導入する際の根本的な課題となります。例えば、喫茶店でコーヒーを買うことを想像してみてください。代金を支払う時に、銀行口座にいくらあるのか、給与はいくらなのか、そしてどこでお金を使っているのかが、喫茶店とそのバリスタやお客さんに伝わる世界をイメージしてください。現在出回っている仮想通貨では、まさにこのような状況に陥ってしまう可能性が高いのです。

イーサリアムは、取引やその他の分散型金融アプリケーションのための主要なチェーンであることは間違いありませんが、イーサリアムと非公開かつ匿名でやりとりすることは困難であることがわかっています。必要なツールは、最近まで利用できませんでした。既存のソリューションは、イーサリアム上に存在するDEX・アプリケーション・流動性に直接アクセスできない特殊なブロックチェーンを必要とします。また、既存のソリューションにはイーサリアムのメインネットワークが提供する信頼性もありません。多くのユーザーは、自分の取引履歴を全世界で永続的に共有することに比べれば「より少ない悪」として、あらゆる種類の個人データを追跡する中央集権的なソリューションにしぶしぶ頼っています。

## RAILGUNとは

RAILGUNは、ゼロ知識証明を検証するスマートコントラクトの集合体であり、ユーザーは資産や金額、身元を明かすことなく、取引を行ったり、資金を送ったり、受け取ったりすることができるシステムです。同様に、DEX取引やイールドファーミングなどのdApps（分散型アプリ）に使用されているスマートコントラクトとのやりとりも可能です。このオンチェーンシステムの上に重ねられているのが、イーサリアム上の既存のアプリケーションのためのアダプトモジュールと呼ばれる、誰でも導入することができる一連のアダプターです。このようなシステムの利点は、主に2つあります。

1. 第一に、匿名性プールのサイズとノイズを増やすことができます。すべての転送、スワップ、貸し借り、そしてあらゆる種類の分散型アプリとの取引は、RAILGUNとの相互作用のスループットとバリエーションを大幅に増加させ、RAILGUNからの引き出しとRAILGUNへの入金を関連付けることが次第に困難になります。RAILGUNに入金したユーザーは、チェーン上で利用可能な他のどのシステムよりも早くプライバシーと匿名性を実現することができます。

2. さらに、ユーザーがRAILGUNシステム内で、別のトークンに変換することなく、元の形で資産を長期的に維持することができます。真のプライバシーと匿名性は、資産が非公開で取引されるだけでなく、非公開で保管されることで達成されます。RAILGUN内の資産であれば、ユーザーはRAILGUN外の資産でできることはすべてできるため、これらの資産を外に移すインセンティブを減らすことができます。これにより、匿名性プールのサイズとノイズが大きくなり、プライバシーと匿名性のレベルが格段に向上します。

プライバシー、匿名性、送金、取引、その他の活動がすべて一箇所で行われるエコシステムを構築することで、すべての参加者は、ますます大規模でノイジーな匿名性プールから利益を得ることができます。このシステムのすべてのユーザーは、他のユーザーの活動に便乗して、自身のプライバシーと匿名性を高めることができます。

## RAILGUN の仕組み

**RAILGUNは、下記の主要機能で構成されています。**
**ADD**は、RAILGUNに資産を転送し、すべての資産とその所有者を表す新しいゼロ知識ノートを作成します。このアクション自体は、プライベートなものではありません（システムの外から発信されているためですが、これはプライバシーを作るための最初のステップです）。このノートは、後にライブプールに追加されます。

**SPLIT**は、1つまたは複数のゼロ知識ノートを2つのゼロ知識ノートに変えます。入力ノートはライブプールからデッドプールに移動し、出力ノートはライブプールに追加されます。これらの作業はすべてゼロ知識で行われ、ユーザーは入力ノートを所有していること、入力ノートが以前に使用されていないことを、ノート自体を公開することなく証明します。分割は、新たに作成したノートの1つに別の所有者を設定することで、資金移動の手段としても利用できます。これにより、分割の正確な意図を隠すことができます。

**REMOVE**は、ノートを破壊することでRAILGUNから任意のアドレスに資産を移すものです。この場合も、破壊されたノートの所有権を証明するために、ノートや身分を明かすことなく、ゼロ知識で行われます。しかし、受信者はシステムの外にいるため、この行為により、資金の送金先や金額は明らかになりますが、実際のユーザーはわからず、RAILGUNシステムからの送金であることだけがわかります。

また、すべてのアクションには、さまざまなレベルのプライバシーと匿名性が設定されるため、ユーザーはアクションの種類を選択して、必要に応じてガスコストを削減することができます。また、ユーザーは複数のアクションをまとめて1つの証明にすることでガス代を削減することができます。

# テクニカル

RAILGUNは、ユーザーが以下のことを可能にするために設計されました。

- 仮想通貨資産を保管する完全にプライベートな場所の構築
- 完全なプライバシーとブロックチェーンのセキュリティを備えたDeFiプラットフォームへの参加と取引
- 他のユーザーとトークンを交換する際に、ブロックチェーン上の活動を追跡することなく、非公開でトークンを交換
- 資産の出所をコンプライアンス等のために証明

さらに、RAILGUNを可能にしている同じオンチェーン技術の中で構築された、外部からは見えないピアツーピアの取引を促進するRAILGUN DEXが（DAOが可決した場合）間もなくリリースされる予定です。

## RAILGUNコアシステム＆プロトコル

Railgunプロトコルの核となるのはJoinSplitトランザクションであり、これは(U)TXO、つまり(未使用)トランザクションアウトプットモデルで動作します。ここで、括弧内のUは、外部のオブザーバーがどのTXO（トランザクションアウトプット）が使われていて、どれが使われていないかを判断できないためです。各UTXOは、誰が使用できるかを定める公開鍵、金額、トークンID（例えばUSDT、WETH、WBTCなど、それぞれのERC–20コントラクトアドレスで表される）、さらにノートのコミットメントをランダム化するためのランダムネスフィールド（＝ハッシュ）が暗号化されたノートです。これらの情報を維持するために、内部ではバッチ式インクリメンタルマークルツリー（暗号化ハッシュ関数を用いて大規模なデータ構造の内容を効率的かつ安全に検証できるツリー構造の一種）の効率的な実装を使用しています。

Nullifierは、ユーザーの秘密鍵を使って生成される特殊なハッシュで、外部からTXOにリンクすることはできませんが、二重支出の可能性を排除するためにトランザクションで決定論的に生成されます。Nullifierは、支出キー（当該UTXOの支出者の秘密キー）のハッシュとマークルルートのパスインデックスを用いて計算され、各ノートが常にユニークなNullifierを生成することが保証されています。このNullifierは発信者によってのみ生成されるため、RAILGUNはこれを二重支出の排除として利用することができます。どのNullifierがどのUTXOに属するかをリンクできるのは、使い手だけです。

RAILGUNでは、システム内でゼロ知識証明を多用しています。ゼロ知識取引は、いくつかの公開入力といくつかの非公開入力を持つ小さなプログラムと考えることができます。したがって、証明プログラムは、パブリックな入力とプライベートな入力の両方で証明を生成し、パブリックな入力をZKP（ゼロ知識証明）とともに検証プログラムに渡すことができます。検証プログラムはこの情報をもとに、証明プログラムが正常に実行した内容を検証することができます。公開入力は、プライベート入力が検証者の期待通りのものであり、偽造された値ではないことを証明するための情報の一部として存在します。UTXOセットのマークルツリーのルートは、検証者が「私は10000000000ETHのUTXOを持っている」と不正に主張できないことを非常に効率的に保証します。

私たちのゼロ知識プログラムでは、以下のような公開入力があります。

- アダプト ID（詳細は後述）
- 入金額
- 出金額
- マークルルート
- Nullifier
- アウトプットUTXOハッシュ
- 受取人のみが復号可能なアウトプット暗号化UTXO

また、次のような、任意の公開入力もあります。

- 入金または出金が必要な場合は公開されなければならないが、入金と出金の両方がゼロの場合は非公開となるトークンID
- 出金額がゼロでない場合は公開されなければならない出金先のアドレス

非公開入力は次の通りです。

- インプット値
- 支出されるUTXOの秘密鍵となる支出鍵
- メンバーシップのマークル証明
- 受取人の公開鍵
- アウトプット値

**これらの入力により、ゼロ知識プログラムは以下を検証します。**

- 入金額＋入力額＝出金額＋出力額なので、無からトークンを作ることができないこと
- 入力ノートは、マークルルートとマークルメンバーシップ証明を用いて、マークル木に存在すること
- ノートの秘密鍵のみが支出できるため、支出鍵は入力ノートに対して有効であること
- Nullifiersが正しく計算されていること

**コントラクトは、以下の項目をチェックします。**

- トランザクションのゼロ知識証明が有効であること
- 二重支出をなくすために、以前にNullifierを検出していないこと
- ユーザーがUTXOを作り上げるのを防ぐために、マークルルートが現在または以前のマークルルートであること
- 次に、スマートコントラクトは、入金額が指定されている場合は、ユーザーのウォレットからトークンを転送し、代わりに出金額が指定されている場合は、公開入力の指定されたユーザーのウォレットアドレスにトークンが転送され、出力されたUTXOのハッシュがマークル木に追加され、将来的に使用できるようになること。

## アダプトモジュール

アダプトモジュールはRAILGUNプロトコルの個別のスマートコントラクト拡張で、プライベートトレードやNFTなどの機能を促進することができます。アダプトモジュールは RAILGUN のコアコードを肥大化させることなく追加機能を実装することができます。アダプトID のインターフェースはシンプルかつパワフルです。

Adapt IDインターフェースは、コントラクトアドレスとパラメータの2つのフィールドで構成されています。

コントラクトアドレスが指定された場合、RAILGUNのコアコントラクトは、トランザクションがアダプトIDモジュールインターフェースを介して指定されたコントラクトアドレスから提出された場合にのみ、トランザクションを処理します。関連する証明はすべて指定されたコントラクトからのみ送信可能であるため、RAILGUNコアプロトコルの検証ルールとアダプトモジュールのプロトコルの検証ルールとアダプトモジュールの検証ルールの両方に合格した場合のみ有効です。

アダプトIDパラメータは RAILGUN のコアコードでは検証されないため、アダプトモジュールは以下のようなカスタムロジックを実装することができます。アダプトモジュールが希望するカスタムロジックを実装することができます（例えば AAVE のような外部の DeFi コントラクトとのインタラクションのセットなど）。

また、アダプトモジュールのコントラクトを使い分けることにより、RAILGUN ユーザーの資金が不適切にコーディングされた、または悪意のあるアダプトモジュールによって危険にさらされることを防ぎます。

- アリスさんとBobさんがトークンを交換するために アダプトモジュールをどのように使用するかを見てみましょう。
- アリスさんは、100 USDCを100 USDTで売りたいので、自分で使える100 USDTのノートを作成します（これをノート A とします）。
- ボブさんは100 USDTを100 USDCで売りたいので、自分で使える100 USDCのノートを作成します（これをノート B とします）。
- アリスさんは、ノートAをボブさんに送り、ボブさんはノートBをアリスさんに送ります。
- アリスさんはノートBに使う証明を、コミットメントAのハッシュをアダプトIDとして作成します（これを証明Aとします）。
- ボブさんは、コミットメントBのハッシュをアダプトIDとしてノートAに費やす証明を作成します（これを証明Bとします）。
- ボブさんは、自分の証明をアリスさんに送り、アリスさんがボブさんに自分の証明を送ります。アリスさんとボブさんのどちらかが、両方の証明を共通のリレイヤーに送ります。この例では、アリスさんが両方の証明を送ります。
- アリスさんは、両方の証明を（リレイヤー経由で）スワップモジュールに提出します。スワップモジュールは、証明AのアダプトIDが証明Bのノートのハッシュの一つと等しく、証明BのアダプトIDが証明Aのノートのハッシュの一つと等しいことをチェックします。そうであれば、両方の証明がアトミックなトランザクションとしてRAILGUNシステムに提出されます。どちらかの証明が失敗した場合、トランザクション全体が元に戻ります。

## スワップトランザクションとRAILGUN DEX

スワップトランザクションは、アダプトID インターフェースを利用します。RAILGUN の各トランザクションは、入力したい出力のハッシュを指定します。スワップアダプトIDモジュールの検証ルールにより、指定された出力ハッシュを出力する別のトランザクションが並行して送信された場合のみ、そのトランザクションが有効であることが保証されます。つまり、スワップはアトミックで信頼性の高い方法で実行されます。お互いの要求に一致する出力を持つトランザクションのペアのみが有効に実行されます。

## リレイヤーネットワーク

RAILGUNでは、誰もがリレーヤーになることができます。ユーザーは、送信したい取引とガス代を指定します。リレーヤーはそれに対し、支払うべき手数料（リレーヤーのETHガス代をカバーするため）を提示します。利用者はRAILGUNトランザクションを生成し、要求された手数料に見合う出力の一つを中継者のアドレスに送ります。リレーヤーは、出力のひとつが正しい料金で自分宛に送られていることを確認し、そのトランザクションをネットワークとユーザーの両方に、指定されたガス代で送信します。これにより、ユーザーの内部のRAILGUNトランザクションが、ユーザーのETHアドレスに関連付けられることはありません。

## 技術ロードマップ候補

ローンチ後、DAOユーザーは以下に関する投票を行うことができます。

- RAILGUN Coreをリファレンスフロントエンドとともに展開
- RAILGUNをバイナンススマートチェーンとポリゴンに展開（2021年7月から8月頃の予定）
- リレイヤーネットワークの展開
- 内部取引やスワップ取引を安価に実現する一括取引検証機能
- RAILGUN DEX (RAILYSWAP)
- 取引手数料の取引内容と異なるトークンでの支払い
- プライベートNFT対応
- 完全にプライベートなNFTオークション
- NFT化されたステークによるプライベート投票
- SOL / ソラナ RAILGUN (SOLRAIL)の展開（2021年11月頃の予定）
- ポルカドットRAILGUN (DOTRAIL)の展開（2022年1月頃の予定）

# ガバナンス

RAILGUNは、特定の個人やチームの支配下にはなく、今後もそうなることはありません。ガイダンスは常にRAILGUN DAOから来ます。DAO（Decentralised Autonomous Organization）では、ガバナンストークンホルダーがプロジェクトの運　と方向性を定義する提案に投票します。RAILGUNスマートコントラクトのコードは、DAOのガバナンス投票の後にのみ展開または更新されます。立ち上げ時、RAILGUN DAOはRAILGUNプライバシーコントラクトが展開されていない状態で稼働します。展開されるコードのバージョンは、RAILトークン保有者による投票で決定されたものになります。

## RAILトークン&投票

RAILはRAILGUN DAOのガバナンストークンです。1トークン（投票コントラクトにステークしたもの）は1票に相当します。ステークしていないユーザーや、アンステークしているユーザーは、投票することができません。RAILトークンがステークされると、アンステーク期間は30日となりますので、投票後にトークンを保有するには実質的に30日の最低期間が必要となります。これは、投票者がプロトコルのアップグレードや料金の投票方法を選択する際に、少なくとも1ヶ月前には見ておかなければならないことを意味します。票の奪取は不可能で、投票者は数日先を見て行動します。

## RAIL分配

RAILGUN DAOのガバナンストークンであるRAILの配分は、以下のようにまとめられます。

- 25%をエアドロップに配分
- 25%を財団に配分
- 50%をRAILGUN DAOに配分

ローンチ時の流通トークンの総供給量は5,000万RAILトークンとなります。RAILトークンの最大生涯総供給量は1億トークンとなり、1億を超えるトークンを作ることは不可能です。

**エアドロップトークン（25%）：**ETHネットワーク上で、TORプロジェクト、Right to Privacy財団、Free Software 財団などのプライバシーに関する慈善団体や非　利団体に寄付を行ったイーサリアムアドレスには、RAILトークンがエアドロップされます。どのようなコミュニティを形成するにしても、最も重要なのはメンバーの参加であり、Railgunの目標に長期的な関心を持っていることをすでに証明しているメンバーは、DAOを開始するのに最適なメンバーです。分配を直接知らせる手段がないので、受取人の多くはエアドロップを受け取っていることを最初は認識していないかもしれません。

財団トークン（25%）：Right to Privacy 財団は、RAILGUNプロジェクトを開発するための助成金を提供し、プロジェクトの長期的な利益を支援するために、RAILトークンの25%をボランティアで預かっています。この財団は認定慈善団体であり、利益を目的としていません。これらのトークンは、開発者へのインセンティブと、将来の展開を含むRAILGUNプラットフォームのプロモーションにのみ使用されます。財団は、DAOの１年目にはトークンの売却はしません。

**DAOトークン（50%）：**DAOに与えられた5,000万トークンはロックされており、ミントされていません。RAILトークン保有者によるDAO投票によってのみミントされます。例えば、DAOがRAILトークンのリクイディティプールの運　者にボーナス利回りを与えたいと考えた場合、DAOはこの割り当てから必要な数のRAILトークンをミントし、ロックを解除するための投票を行います。DAOはRAILGUNの金庫からの取引手数料をRAILトークン保有者にどのように分配するかを投票することができます。

## おわりに

すべてのユーザーがRAILGUNの一員となり、デジタル時代のプライバシーを大切にするコミュニティとして、プロジェクトの成長と方向性に影響を与えるべきです。RAILトークンは、このようなチームワークのために、DAOのガバナンスシステムで使用されます。ユーザーは、変更のための提案を提出し、変更に対する投票を非公開かつ安全に行うことができます。最初の数週間で、RAILGUNのネイティブデスクトップアプリやモバイルアプリのアイデアから、RAILGUNの金庫に集められた取引手数料をステークしたRAILトークン保有者に分配することまで、初期の支援者による提案が見られました。

# 経済性

*以下は、RAILGUN DAOメンバーによる投票のために、ローンチ後の最初の1週間に届けられる経済的提案です。DAOの議決権を持つRAILの保有者は、代替案を提案したり、この特定の提案に賛成か反対かを投票することができます。ガバナンスモデルとプロセスの詳細については、「ガバナンス」の項をご参照ください。*

## RAILGUNとRAILトークンの経済性について

RAILGUNネットワークの経済政策は、RAILGUNシステムとその匿名性プールに直接対話し、貢献する人々によってコントロールされます。RAILトークンは、システムの管理、アップグレード、パラメータの管理に使用され、管理と成長への参加を促すためにも使用されます。

RAILは、すべてのリクイディティプールに継続的に放出されます。RAILのリクイディティプールは最初から存在し、流動性の提供者は預けられたRAILの量に比例してガバナンス力を獲得します。リクイディティプールの私的かつ匿名の性質により、RAIL保有者は匿名のままで秘密裏に運　することができます。これは、有権者を保護し、より強固で独立したRAILGUN DAOに貢献するRAILGUNシステムに特有の性質です。正確な排出スケジュールは、RAILホルダーによって管理されますが、10年の排出スケジュールで開始されます。

## 手数料とRAILGUNの金庫

手数料はすべての操作にコード化されます。徴収される手数料はRAILGUN DAOの金庫のアドレスに送られます。DAOの多数決のみがDAO金庫の資金の支出をコントロールでき、他の人は動かすことができません。RAILGUNの全ての手数料は、最初に25ベーシスポイントに設定されるADD機能手数料とREMOVE機能手数料を除いて、ゼロに設定されます。つまり、RAILGUNのプライバシー・スマートコントラクトは、トークンの0.25%の手数料で入出金を行うことになります。RAILGUNプライバシーコントラクトを通じて大量のプライバシー保護のための取引が行われることが予想されるため、開始当初から、RAILGUNプライバシーコントラクトの活動により、金庫に徴収される手数料が非常に大きくなることが予想されます。

## RAILへの流動性の提供

RAILは、開発やテストへの参加を動機付けるために、初期バージョンやプロトタイプの初期ユーザーや流動性提供者にDAOから放出されます。RAILトークンは今後10年間にわたり、ネットワーク上での活動に比例して、流動性提供者やアクティブユーザーに放出されます。これは、ネットワークを積極的に利用する動機付けとなり、RAILGUNのガバナンスが実際にRAILGUNを使用し、その成功に強く結びついているユーザーに行き渡るようにします。

## マルチチェーン

RAILGUNプロジェクトでは、RAILGUNをまずバイナンススマートチェーンとポリゴンに展開し、その後ソラナとポルカドットに展開するため、対応する新しいトークン（POLYRAIL、SOLRAIL、DOTRAILなど）は、RAILをステークしている人やRAILのLPトークンを保有している人にのみエアドロップされます。バイナンススマートチェーンRAILGUN (BRAIL)やポリゴンRAILGUN (POLYRAIL)のようなオルタナティブチェーンの展開は、RAILのステークホルダーだけではなく、DEXでRAILの流動性を提供している人（LPトークンを保有している人）にエアドロップされるべきです。

それ以外の人はこれらの新しいトークンのエアドロップを受け取ることはなく、予備の供給は一切ありません。これらの新しい非ETHチェーントークンは、RAILとは独立した全く新しい時価総額と価格を持つことになります。

# プライバシー& 匿名性

NOVEMBER 6, 2021