RAILGUN_

/// WHITEPAPER
MMXXI

RAILGUN PROJECT
NOVEMBER 6, 2021

目录

RAILGUN PROJECT

NOVEMBER 6, 2021

RAILGUN

RAILGUN是一个基于以太坊的健壮零知识框架，致力于链上应用和用户的隐私和匿名。

RAILGUN：用户首次在与以太坊上的DeFi智能合约交互时既可以保护隐私，又无需牺牲以太坊哈希力提供的安全性。

愿景

所有人类都本能地重视隐私。这是一项公认的人权，即便是不尊重他人隐私的人，也希望自己的隐私得到保护。隐私与匿名应当是默认设置，而非例外。任何人在获取你的个人或财务信息前，都必须征得你的同意。

RAILGUN应运而生，这是一个由多位热衷于保护用户隐私的技术人员开发的隐私、匿名系统，直接搭建在以太坊链上，允许用户直接与去中心化交易所、借贷平台和流行的智能合约应用交互，它不仅可以保证你的行为不为他人所知，保护你的隐私，还可以为你的身份保密，赋予你匿名性，且无须牺牲以太坊及其蓬勃生态系统的安全性和活性。此外，RAILGUN还将快速将其优势带到其它的区块链生态。

如果你需要透明化，RAILGUN可利用保护隐私的零知识手段，生成一份记录你的行为和账户余额的可验证报告（如提交给审计人员或合规专员）。这意味着你的资金信息仍将保密，但你可以向特定的同事或信息接收者提供资金来源证明。RAILGUN并不意在剥夺链上行为可由第三方验证的特性，而是让用户决定谁可以在何时出于何种原因查看哪些信息。

简介

区块链公链名副其实，是公开的。在今天最受欢迎的区块链上，全世界都能看到你在链上的一举一动，即便是十年后也是如此。商业化链上分析系统一直在不断改进，如今已经可以事无巨细地追踪你本人和你的所有交易。这对今天的区块链用户来说显然是个问题。除此之外，不少国家出现了专业的电子监控组织，它们同样具备信息追踪能力。这对个人、非政府组织、甚至企业大规模应用区块链构成了根本性挑战。想象一下这样一个世界：你在一家咖啡店买一杯咖啡，咖啡店、店里的咖啡师，还有这家店的顾客都能知道你的银行账户里有多少钱，你的收入有多少，你的钱花在了哪里。今天的大多数加密货币都面临这一问题。

以太坊无疑是开展交易和其他去中心化金融应用的主流区块链平台。但以隐私、匿名的方式与以太坊交互十分困难，实现这一功能的必要工具仍未出现。现有的解决方案需要专门的区块链，但它们无法直接访问以太坊上的去中心化交易所 、应用以及流动性，而且缺乏以太坊本身的公信力 。虽然不情愿，但许多用户不得不诉诸中心化解决方案，虽然后者也会追踪他们各种各样的个人数据，与时时刻刻与全世界分享他们的交易历史相比，这是两害相权取其轻的无奈选择。

RAILGUN是什么？

RAILGUN由可验证零知识证明的一系列智能合约组成，允许用户在不公开任何资产、金额或身份信息的情况下，发送或接收交易，或与智能合约交互，如用于去中心化交易所交易、收益耕作和其他去中心化应用（dApp）的智能合约。其上则是一套面向以太坊现有应用，且任何人均可以部署的适配器，名为“Adapt模块”（Adapt Module）。RAILGUN系统具有以下两大根本优势：

1. 该系统增加了匿名池的规模和噪音。所有转账、互换、借入、借出以及与去中心化应用开展的各类交易行为，都极大地提高了与RAILGUN交互的吞吐量和业务类型，使得识别向RAILGUN存款和从RAILGUN取款行为之间的相关性变得日益困难。这意味着与现有的其它链上系统相比，向 RAILGUN存款的用户可以更快地实现隐私和匿名。

2. 该系统允许用户将资产以原始形式长期存放在RAILGUN系统内，无需兑换成另一种代币。归根结底，隐私和匿名不仅来自于交易过程，也来自于资产单纯地存放。将资产存入RAILGUN之后，用户仍可以不受限制地动用，与RAILGUN外的资产无异，从而减少从RAILGUN中取出资产的动力。这也有助于扩大匿名池的规模和噪音，进而提供更好的隐私和匿名保证。

通过创造一个兼具隐私和匿名性，集转账、交易和其他各类活动于一体的生态系统，所有的参与者都可以从一个规模和噪音量日益扩大的匿名池中受益。RAILGUN系统的所有用户都可以借他人的活动来获得更高的隐私和匿名性保证。

RAILGUN的工作原理

RAILGUN由以下三大关键功能组成：

ADD（“添加”）：将资产转入RAILGUN并生成一个代表所有资产及其所有者的零知识票据（note）。该操作本身并不保证隐私性（因为它起始于RAILGUN系统之外，但这是实现隐私的第一步）。这个票据随后被添加进动态池。

SPLIT（“拆分”）：将一个或多个零知识票据拆分成两个票据。输入票据(input note)从动态池移入静态池，输出票据(output note)放入动态池。这一切行为均基于零知识，即用户在不透露票据内容和自己身份的前提下，证明自己是输入票据的所有者，且该输入票据之前从未被使用过。也可用拆分转移资金，通过为新生成的票据设置一个不同的所有者来实现。这有助于隐藏拆分的真实目的。

REMOVE（“移除”）：通过销毁票据，将资产从RAILGUN转到任意地址。该操作同样基于零知识，即用户在不公开票据内容或自己身份的前提下，证明自己是被销毁票据的所有者。然而，由于资金接收者位于RAILGUN系统外部，该操作会公开资金的转入地址以及金额，但不会公开转出资金的用户身份，区块链上只知道资金是从RAILGUN系统转出的。

上述操作的隐私性和匿名性程度各不相同，必要时，用户可以根据需要选择某一类操作，以减少gas费用。用户还可以将多个操作打包进同一个证明来减少gas费用。

技术特点

RAILGUN旨在让用户可以：

- 建立一个完全保密的加密货币资产存储地；
- 在获得完整的隐私和区块链安全性的前提下，在DeFi平台上交易并参与DeFi平台；
- 与其他用户私下交换代币，而不会在链上留下任何痕迹；
- 生成证明，例如出于合规目的证明资产来源。

除此之外，RAILGUN 的去中心化交易所将很快面世（前提是DAO投票支持），以促进对外部各方不可见、但是基于RAILGUN所依托的链上技术的P2P交易。

RAILGUN核心系统及协议

RAILGUN协议的核心是JoinSplit交易（合并–拆分交易），这种交易基于 (U)TXO模型，即（未花费的）交易输出模型。U放在括号内是因为外部观察者无法判断TXO（交易输出）是否已经被花费。每个UTXO都是一个公钥的加密票据，规定了票据可以为谁花费、金额、代币ID（如USDT、WETH、WBTC等，以 ERC–20 合约地址的形式显示），以及一个让票据的承诺值（即哈希值）随机化的随机字段。我们内部利用高效的批量增量式Merkle树（一种树形数据结构，运用密码学哈希函数，可以安全高效地验证大型数据结构中的内容），在链上维护上述信息。

RAILGUN还使用Nullifier，一类利用用户私钥生成的特殊哈希值，外部观察者无法将其与交易输出（TXO）关联，但是它是在交易过程中确定性地生成的，以此来避免双花问题。Nullifier的值由Spending Key的值（即该UTXO中花费者私钥的值）与Merkle树根的路径索引值做哈希得出，该方法可确保每一个票据总能生成一个独一无二的Nullifier。由于Nullifier只能由花费者生成，因此可解决双花问题。只有花费者知道Nullifier与UTXO之间的对应关系。

RAILGUN系统大量使用零知识证明。零知识交易可被视为包含公开输入和隐私输入的小型程序。证明程序因此可利用公开输入和隐私输入生成证明，然后将公开输入连同零知识证明一起发送给验证程序。在得到相关信息后，验证程序可对证明程序已成功执行的内容进行验证。证明隐私输入符合验证者期望且非伪造值需要提供充分信息，其中包括公开输入。我们UTXO集合的Merkle树根可确保证明者不会谎称："我有一个10000000000 ETH的UTXO。"

RAILGUN的零知识程序包含以下公开输入：

- Adapt ID（详见下文）
- 存入金额
- 提取金额
- Merkle根
- Nullifier
- 输出UTXO的哈希值
- 加密的输出UTXO（只有接收者可解密）

以下是可选的公开输入：

- TokenID（如果存入或提取金额不为零，TokenID必须公开，但如果存入或提取金额均为零，则必须保持隐私性）
- 提取地址（如果提取金额不为零，则地址必须公开）

隐私输入包括：

- 输入金额
- Spending Key（UTXO私钥）
- Merkle隶属证明
- 接收者公钥
- 输出金额

零知识程序可利用上述输入实施下列验证操作：

验证“存入金额 + 输入金额 = 提取金额 + 输出金额”，以确保没人可以凭空捏造代币数量

利用Merkle根和Merkle隶属证明，验证输入票据存在Merkle树中

验证Spending Key对输入票据是有效的，因为只有凭票据的私钥才可以花费票据

验证Nullifier的值计算正确

智能合约对相关内容进行检查，以确保：

交易的零知识证明是有效的

相关Nullifier之前从未出现过，从而避免双花问题

Merkle根是现在或过去的Merkle根，以防止用户伪造UTXO

如果规定了具体的存入金额，代币会从用户的钱包转入智能合约；如果规定了具体的提取金额，代币会从智能合约转到公开输入中指定的用户钱包地址。然后，输出UTXO的哈希值会被添加进Merkle树，以便在将来花费UTXO。

Adapt模块

Adapt模块是面向RAILGUN协议的独立智能合约扩展，有助于实现非公开交易和非同质化代币（NFT）等功能。Adapt模块可实现额外功能，但不会造成RAILGUN的核心代码规模过于膨胀。Adapt ID接口简单明了，但功能强大。

Adapt ID接口包含两个字段：合约地址和相关参数。

如果指定了一个合约地址，则RAILGUN核心合约只会处理由Adapt ID接口指定合约地址提交的交易。由于相关证明只能通过指定的合约提交，因此只有同时符合RAILGUN核心协议和Adapt模块验证标准的证明才是有效的。

RAILGUN核心代码并不验证Adapt ID的参数，因此Adapt模块可以实施任何定制逻辑（例如一组与AAVE等外部DeFi合约的交互）。

让Adapt模块配属单独的合约还可确保编码拙劣或恶意的Adapt模块不对RAILGUN用户的资金构成威胁。

让我们来看看Alice和Bob如何利用Adapt模块交换代币：

- Alice希望以100 USDT的价格出售100 USDC，于是生成一个表示自己可花费100 USDT的票据（“票据A”）
- Bob希望以100 USDC的价格出售100 USDT，于是生成一个表示自己可花费100 USDC的票据（“票据B”）
- Alice将票据A发送给Bob，Bob将票据B发送给Alice
- Alice为票据B创建一个Adapt ID为承诺A哈希值的证明（“证明A”）
- Bob为票据A创建一个Adapt ID为承诺B哈希值的证明（“证明B”）
- Bob将证明B发送给Alice，Alice将证明A发送给Bob。Alice或Bob将两个证明发送给双方共同的中继者（Relayer）。在本例中，由Alice发出两个证明。
- Alice（通过中继者）将两个证明提交至Swap模块。Swap模块检查证明A的Adapt ID与证明B中其中一个票据的哈希值是否一致，以及证明B的Adapt ID与证明A中其中一个票据的哈希值是否一致。如果均一致，则将两个证明提交至RAILGUN系统用于执行原子交易。如有不一致，则撤回交易。

互换交易和RAILGUN 去中心化交易所

互换交易通过Adapt ID接口实现。每一个RAILGUN交易都为其请求的输出指定了哈希值。Swap Adapt ID模块的验证规则可确保一个交易只有在另一个交易与该交易一起被提交，而且输出了该交易指定的哈希值的情况下才有效。因此，每个互换交易都是零信任的原子交易——只有输出与请求的内容相匹配的一对交易才是有效的，才会被执行。

中继者网络

在RAILGUN的生态系统中，任何人都可以成为中继者。用户指定其希望提交的交易和gas价格。中继者回复一个费用金额（用于支付中继者的以太坊gas费）。用户生成一个与中继者所要求费用相匹配的RAILGUN交易，并将该交易的其中一个输出发送到中继者的地址。中继者检查其地址是否收到了该交易的其中一个输出以及正确的费用，然后将该交易以指定的gas费率发送到RAILGUN网络和用户。这可以将用户的RAILGUN交易与用户的以太坊地址之间的联系隐藏起来。

技术路线图展望

在RAILGUN上线后，DAO用户可对下列事项进行投票：

- 利用参考前端部署RAILGUN Core
- 质押RAIL币以参与投票
- 在币安智能链（BSC）和Polygon上部署RAILGUN（预计2021年7–8月）
- 部署中继者网络
- 实现批量交易验证功能，以降低内部及互换交易成本
- RAILGUN 去中心化交易所（RAILYSWAP）
- 用另一种代币支付交易费
- 非公开的NFT支持
- 完全私人的NFT拍卖
- 通过质押的NFT进行非公开投票
- 部署SOL / Solana RAILGUN（SOLRAIL）（预计2021年11月）
- 部署Polkadot RAILGUN（DOTRAIL）（预计2022年1月）

治理模式

RAILGUN不受任何个人或团队控制，这一点永　不会改变。将由RAILGUN DAO——一个去中心化自治组织给予指导，而该DAO治理代币的持有者对涉及项目运营和发展方向的提案进行投票。只有在DAO治理投票通过后，才可以部署或更新RAILGUN智能合约代码。RAILGUN DAO上线时不会部署任何RAILGUN隐私合约——部署的代码版本为RAIL币质押人投票通过的版本。

RAIL币和投票

RAIL币是RAILGUN DAO的治理代币。持有一个质押在投票合约中的RAIL币可以投一票。未质押或处于解除质押期的用户无法参与投票。解除质押期（也即解除质押所需时间）为30天，故而用户在投票后会持币至少30天。这也意味着在对协议升级或费用事项进行投票之前，投票者不得不提前至少一个月做好安排。不会出现“突击投票”（Vote Raiding）现象，投票者不会把眼光局限在投票之后的几天。

RAIL代币分配结构

RAILGUN DAO的治理币——RAIL币的分配结构如下：

25%分配给空投

25%分配给隐私权基金会(Right to Privacy Foundation)

50%分配给RAILGUN DAO

RAILGUN上线时RAIL币的流通供应总量为5000万个。RAIL币的最大供应量为一亿个，不可能创造出超过一亿个RAIL币。

空投（25%）：如果一个以太坊地址通过以太坊网络给致力于保护隐私的慈善机构和非营利组织捐过款，如TOR项目（TOR Project）、隐私权基金会(Right to Privacy Foundation)和自由软件基金会（Free Software Foundation），该地址将收到空投的RAIL币。成立一个社区最重要的一步是吸纳成员，而已证明对RAILGUN的目标抱有长期兴趣的成员是最佳的RAILGUN DAO创始成员。由于无法直接通知RAIL币接收者，许多接收者可能一开始并不知道他们将收到RAIL币。

基金会（25%）：隐私权基金会提供了RAILGUN项目的初始启动资金。为维护项目的长　利益，该基金会主动提出由其管理25%的RAIL币。该基金会为登记在册的慈善机构，不以营利为目的。这部分RAIL币的唯一用途是调动开发人员的积极性以及推广RAILGUN平台，包括落实未来的部署计划。隐私权基金会在第一个DAO年不会出售RAIL币。

DAO（50%）：分配给DAO的5000万个RAIL币处于锁定状态，尚未被铸造。铸造RAIL币只能通过RAIL币持有者参与的DAO投票决定。举例来说，如果DAO打算为RAIL币的流动性池运作者提供额外奖励，DAO将投票决定是否从分配给DAO的RAIL币中解锁并铸造所需数量的RAIL币。DAO可发起关于如何将RAILGUN财政库（Treasury）收到的交易费分发给RAIL币持有者的投票。

总结

所有用户都应在RAILGUN项目中发挥重要作用，应对项目的发展和方向具有影响力，携手共建致力于数字化时代隐私保护的社区。DAO治理体系将利用RAIL币推动用户之间的合作。用户将能以隐私、安全的方式提交变更提案并对变更进行投票。今天，我们仍可以看到项目的早期支持者早已提出过的提案，内容包括桌面和移动端原生RAILGUN 应用程序的创意，以及将RAILGUN Treasury收到的交易费在RAIL币持有者之间分配。

经济系统

以下为将在RAILGUN上线后的第一个七天内提交给RAILGUN DAO成员投票表决的RAILGUN经济政策提案。拥有DAO投票权的RAIL币质押人可投票支持或反对该经济政策提案，或提出替代方案。如需关于治理模式和流程的详细信息，请参阅“治理模式”部分。

RAILGUN及RAIL币的经济政策

RAILGUN网络的经济政策将由与RAILGUN系统及其匿名池直接交互并为其直接作出贡献的人控制。RAIL币将用于管理RAILGUN系统及其更新和参数。RAIL币还将用于激发参与项目治理和发展的积极性。

RAIL币将被持续释放到各个流动性池。RAIL流动性池将成为第一个流动性池，其流动性提供者将获得与他们存入的RAIL币数量成比例的治理权。流动性池的隐私和匿名性让RAIL币持有者可在不公开身份的情况下参与治理，这是RAILGUN系统所独有的功能，既能保护投票，又能让RAILGUN DAO更具活力、更独立。RAIL币持有者有权管理具体的RAIL币释放安排，但最初设定为分十年释放。

费用和RAILGUN 财政库（Treasury）

每一次交互都会产生费用，已收取的费用会被发送到RAILGUN DAO 财政库的地址。任何人均不得动用财政库内的资金，只有在获得DAO投票者多数支持的情况下方可动用这笔资金。除ADD功能费（0.25%）和REMOVE功能费（0.25%）之外，所有RAILGUN费用的初始费率均为零，换言之，在将代币存入RAILGUN系统或从RAILGUN中取出代币时，RAILGUN隐私保护智能合约会收取存入或取出的代币的0.25%作为费用。RAILGUN上线后，预计马上会有大量交易通过RAILGUN智能合约完成，因此财政库收到的来自RAILGUN智能合约的费用预计将十分庞大。

RAIL币流动性准备

DAO管理的RAIL币将被释放给项目早期版本和原型的早期用户和流动性提供者，以激励他们参与开发和测试。今后十年，RAIL币将被分发给流动性提供者和活跃用户，分发量与他们在RAILGUN网络上的活跃度成正比。这不仅有助于提升RAILGUN网络的活跃度，还可确保RAILGUN的治理权掌握在真正在使用RAILGUN、为项目的成功做出重要贡献的用户手中。

多链部署

RAILGUN将首先被部署在币安智能链和Polygon上，之后是Solana和Polkadot，相应的新代币（如POLY–RAIL、SOLRAIL和DOTRAIL等）将以空投方式分发给正在质押RAIL币和持有 RAIL LP代币的人。多链代币，如基于币安的BSC RAILGUN（BRAIL）和基于Polygon的Polygon RAILGUN（POLYRAIL），将以空投方式分发给在去中心化交易所上提供RAIL币流动性（持有LP代币）的人，而不仅仅分发给RAIL币质押人。

以空投方式分发的新代币不会提供给除上文提及的分发对象以外的其他人，而且不会留下部分代币作为备用。这些新的非以太坊链代币将拥有独立于RAIL币的全新的市值和市价。

隐私&匿名

NOVEMBER 6, 2021