MULTICOIN CAPITAL

THORChain (RUNE) Analysis

By Tushar Jain, Spencer Applebaum
& Shayon Sengupta

2021年2月23日

Multicoin Capital 是一家理论驱动的加密基金，投资于重塑全球经济所有领域的代币。 我们严格研究区块链协议、团队和市场机会，践行具有公共市场流动性的风险资本经济 学。

报告披露

声明：*Multicoin Capital 持有 RUNE 通证。出于道德原因，Multicoin Capital 对本报告所列资产在本文公开发布后的 72 小时 内（“无交易期”）遵守“无交易政策”。任何高级职员、董事或雇员不得在非交易期内买卖上述资产。*

本报告的发表日期，Multicoin 资本管理公司及其附属公司（统称“Multicoin”），为这份报告提供研究的其他人和收到这份 报告其他人（总的来说，“投资者”）可能有多头或空头头寸，也可能拥有期权，并且代币价格上涨或下跌过程中取得收益。 报告发布后，投资者可以使用本报告所述项目的代币进行交易。本报告所有内容均代表 Multicoin 的意见。Multicoin 从他 们认为准确可靠的来源获得了所有信息。然而，这些信息是“按原样”呈现的，不存在任何形式的保证——无论是明示的 还是暗示的。

本文件仅供参考，并不作为任何交易的正式确认。所有市场价格、数据和其他信息均不保证其完整性或准确性，均基于选 定的公开市场数据，并反映截至目前的普遍情况和 Multicoin 的观点，所有这些因素都可能因此而发生变化，恕不另行通 知。Multicoin 没有义务继续提供有关该项目的报告。报告是在所指明的日期写的，可能会由于后续市场或经济情况而变 得不可靠。

任何投资都存在巨大的风险，包括但不限于价格波动、流动性不足和潜在的本金完全损失。本报告的基本价值估值仅代表 对特定代币潜在基本价值的最佳表现估值，并不表示或暗示为对代币质量的评估、对过去业绩的总结或投资者的可操作投 资策略。

本文件并不以任何方式构成买卖本文所述任何投资或代币的要约或邀请。

本文件所包含的资料可能包括前瞻性陈述，或参考引用前瞻性陈述，它们包括任何非历史性的事实。这些前瞻性陈述可能 被证明是错误的，可能受到不准确的假设、已知或未知的风险、不确定性和其他因素的影响，其中大多数是 Multicoin 无 法控制的。投资者应在专业财务、法律和税务专家的协助下，对本文件中讨论的所有代币进行独立的尽职调查，并在作出 任何投资决策前对相关市场做出独立判断。

报告摘要

Multicoin Capital 持有大量 THORChain 原生代币 RUNE 的头寸，THORChain 是一个去中心化跨链自动做市商（AMM）。同时，RUNE 是我们最大的公开持仓之一。

我们相信 THORChain——一个通过最小化信任交易现货代币（不仅仅局限于衍生品)跨链 ——是加密交易基础设施的一个基本版块。随着加密生态的不断发展壮大和更加多样化， THORChain 将在其中扮演越来越重要的角色。

因此，一个信任最小化、支持跨链交易的产品存在着巨大的机会。在一个多链并存、代币 泛滥的世界，交易员自然存在着以最小化信任方式进行跨链交易的需求。

在跨链交易领域，第一个这样的产品是 Tier Nolan 原子交换。此后，市场中相继出现了像 简单支付验证、中继和合并共识等其他的方式。然而，尽管出发点很好，但是由于各种原 因（例如交易速度太慢、自由选择问题、成本太高等)，它们都没能成功获得市场的广泛关 注。

从几年前首个跨链兑换产品出现以来，加密生态变得越来越多样化：CoinGecko 市值排名 前 25 的代币中，有 80%属于一层区块链的代币。区块链之间的多样性很自然地产生了的 这个需求：通过最小化信任、去中心化的方式进行跨链交易现货代币。

随着 Solana、Polkadot、Near 和 Avalanche 等新型智能合约平台的成熟，区块链的数量 也在不断增加。而这些生态成熟以后，整体的加密技术构成将变得越发多样化，而不是越 来越同质。

大多数投资者都持有他们看好的区块链的仓位；然而，他们当中很少有人能真正接触到整 个生态日益增长的多样化。这是一个巨大的机会，我们相信持有 THORChain 原生代币 RUNE 是践行该投资理念的最佳方式。

THORChain 概览

THORChain 是一个去中心化跨链自动做市商(AMM)交易所，它允许用户在不同区块链之间交易现货代币。通过 THORChain，交易员能够在不同的第一层区块链之间交易代币，而无 需承担对手或托管风险(例如，交易员不用通过中心化交易所就能够将 ETH 现货兑换成 DOT 现货)。

早在三年前，我们就曾撰文提出了中心化交易所存在的问题：

1. **交易对手风险**：在中心化交易所的模式，用户需要先将加密资产充值到交易所。资 产到账后，交易所在内部帐本登记该笔记录。中心化交易所维护着这个隐私、内部 的账簿。但是，业内出现过不少令人震惊的交易所，它们一直在储备不足的情况下 运行，然后慢慢走向破产；其他一些交易所则涉嫌操纵市场，在客户订单成交之前 进行抢先交易。

2. **速度**：为了最大程度降低交易对手风险，用户通常在交易完毕以后进行提现。这是 一个非常麻烦而且缓慢的过程。如果碰到交易所的提款限制，那更是雪上加霜。

3. **监管风险**：虽然中心化交易所的服务对象为全球用户，但它本身需要遵守当地法 规。当地政府可以强迫交易所下架某个代币（例如最近 Coinbase、Kraken 和 Gemini 下架了 XRP）。监管机构也可能叫停某个交易所并没收其资产（在韩国，该 问题尤为严重）。

4. **被盗风险**：交易所是全球最大的加密货币持有者，因此它们是黑客的首要目标。

5. **交易成本**：加密资产交易费用比传统的公共股票市场高一个数量级。例如 Coinbase Pro（交易量最大的交易所之一）对最低门槛的挂单方和吃单方都收取 0.50%交易 费。

而提到去中心化交易所（DEX），人们都会谈到例如 Uniswap、Sushiswap、Curve 和 Serum 等交易所的链间交易。相对于它们，THORChain 显得非常新颖，因为它支持许多 链上的原生代币，而且定位非常特别，可以实现任何资产之间去中心化交易的初心。

THORChain 带来的一个强大副效应是协议团队可以在任何集成 THORChain 的区块链进行 开发，并轻松启动其他加密生态的流动性。例如，目前大多数团队都选择在以太坊开发项 目，主要原因之一是他们可以轻松在 SushiSwap 或 Uniswap 发行一个代币，同时立即获 得流动性。如果某个协议开发团队认为 Polkadot 或 Solana 更适合他们的特定需求（例如 高吞吐量和低延迟），他们也可以选择这些区块链。而通过 THORChain，新协议可以充分 利用以太坊生态的流动性。加密市场还没有完全认识到这一点的价值所在，THORChain 为 不同智能合约平台创造了一个竞争环境。
市场机会

市场机会

加密市场主要的活动之一是交易。而在跨链交易中，用户通常需要信任中心化交易所，使 用两个钱包（如以太坊的 MetaMask 和 Solana 的 SolFlare 钱包）。这个过程非常麻烦， 例如把以太坊上的 PERP 代币兑换成 Solana 上的 SRM 代币，这是一个用户体验的噩梦。

解决该问题的一个方法是合成交易。我们最近也发布了一篇关于交易合成资产的所有主要 金融结构的文章。但是在许多用例中，合成交易无法取代现货交易。为什么现货交易非常重要呢？因为不同于股票和债券，实际上许多加密货币具备真实的用 途，并且具有原生实用价值。通常情况下，一层网络的用户会通过代币实现某些明确的目 标。举几个例子：

1. 以太坊上的合成 XMR 代币无法保护隐私。
2. 合成的 Helium 网络代币（HNT）无法用于支付无线数据传输费用。
3. 合成的 Arweave（AR）无法在 Arweave 网络上购买存储空间。
4. 合成的 Siacoin（SC）或 Filecoin（FIL）不能用于支付数据存储费用。
5. WBTC 无法提供与原始 BTC 相同的抗审查性。

随着新型、用途更广的一层网络的推出，购买现货资产变得越发重要。除了单纯的投机， 如今各种代币已经嵌入了更多的功能。

而中心化交易所存在比较大的风险。THORChain 提供了一种优雅的选择：跨区块链之间的 非托管、无需许可、去中心化交易。对于一直追求保护隐私和/或保持资产保管的用户来 说，THORChain 提供了一个替代中心化交易所（CEX）的最重要功能之一。

THORChain 网络概述

THORChain 通过节点和流动性提供商（LP）组成的网络实现跨链交易。协议的原生代币 RUNE 担当着三个关键角色：1）保护网络安全；2）充当系统中每笔交易的通用定价货 币，最大程度提高交易所中所有资产的流动性；3）收取费用。

通过在不同区块链创建地址（节点控制着这些地址），THORChain 节点利用单向状态锚定 来连接各个区块链。THORChain 节点采用先进的多方计算（MPC）技术，例如分布式密钥生成（DKG）和阈值签名方案（TSS），来确保不存在某一个 THORChain 节点能控制 用户的资产。

我们来考虑一个简单的例子。THORChain 节点运行 DKG 生成私钥/公钥对，其中私钥是虚 拟化的，并且只有 67%的节点相互勾结（标准 BFT 网络安全阈值）才能恢复。用户可以将 BTC 发送到该地址，然后再发送到托管交易的 THORChain 网络。资产由 RUNE 的市值和

流动性以及多方计算系统提供保证。当用户请求从 THORChain 提取 BTC 时， THORChain 节点运行多方计算对消息签名，然后将资产放给用户。当 THORChain 节点托 管 BTC 时，用户可以先交易 BTC-RUNE，然后再通过 RUNE-[其他资产]，将 BTC 兑换成 THORChain 支持的任何其他资产。这些交易都是在 THORChain 去中心化交易所执行，完 全无需许可并且不受审查制度约束。通过简单的链上交易或通过任何 Web，移动设备或桌 面应用，交易者就能与网络进行交互。

连续流动性池

随着 Uniswap 这类自动做市商（AMM）的出现，许多团队一直在尝试多种改善买卖双方体 验的新想法。THORChain 发明了一种称为连续流动性池（CLP）的新系统——自 Uniswap 推出以来 AMM 的最有意义改进之一。在结构上，CLP 类似于 Uniswap 和 Balancer，但有 一个关键的区别：交易费用为交易滑点的一个函数，而不是固定百分比手续费（例如 Uniswap 的 30 个点）。

目前人们对 AMM 持有的一种普遍批评是，它们给套利者利用 AMM 的 LP 提供了空间。例如，如果由于某个消息，ETH 在所有大型交易所的价格从 0.03 BTC 飙升到 0.04 BTC，但 Uniswap 仍然按照 0.03 BTC 的价格出售 ETH，直到套利者将价格推升到 0.04 BTC。如果 ETH 价格再也没跌回到 0.03 BTC，那么 Uniswap 资产池中的 LP 会执行买入并持有策略— —通常这被称为无常损失（IL），虽然更准确的说法是未实现损失。

THORChain 的 CLP 设计可缓解该问题。如果套利者在单笔交易中将 ETH-BTC 从 0.03 推高到 0.04，他们就必须支付更高的交易费，这样就能让 LP 受益，并减少甚至消除 IL。交易引起的滑点越高，交易者为给该笔交易潜在的 LP 支付的费用就越多。

基于这一点，套利者可能会将交易分成多个小额订单，来避免高手续费。THORChain 又通 过优先成交最高手续费的交易来解决该问题。实际上该操作在共识协议本身中实施（不同 于以太坊的矿池运营商控制某个区块的交易顺序）。套利者必须权衡在支付更高滑点费用的同时，必须考虑他们的交易不被包括进去的风险。由于该机制本身是在共识中强制执行 的，因此可以确保在市场异常波动的情况下，THORChain LP 没法跟上节奏的问题。这降低了LP 的风险下限，保证他们为自然交易者提供更充分的流动性。

Gauntlet 是一家著名的加密货币量化研究公司，它模拟了 Uniswap 和 THORChain 的 LP 收益，最后验证了 THORChain 的 LP 有机会获得更高的收益。

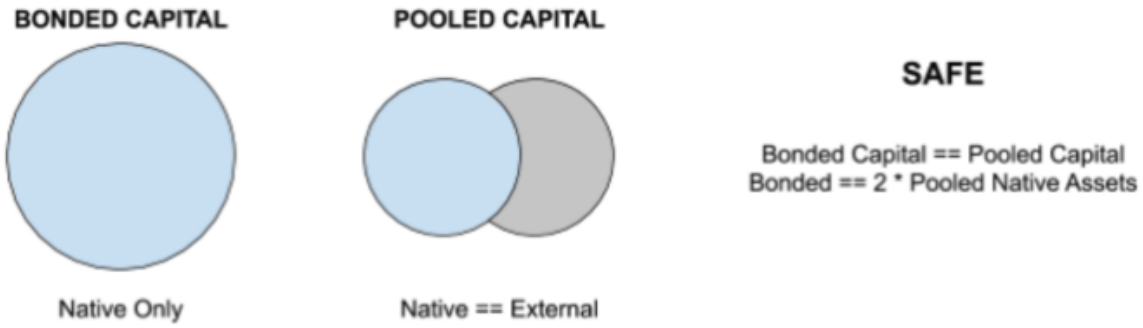
LP 必须将 RUNE 存入网络中的每个资金池，并且每笔交易都通过 RUNE 执行。例如，如 果用户将 ETH 换成 DOT，那么 THORChain 将出售 ETH/RUNE，然后买入 DOT/RUNE。 该过程会集中全球的流动性，而不会把流动性分散在例如 DOT/ETH 这样小额交易对中。

节点则必须质押最低数量的 RUNE，才能在网络上验证交易并赚取费用。在一定时间内， 节点会在“活动”和“备用”状态之间循环，确保节点的操作尽可能去中心化。网络的内部运作 脱离节点运营商，并且在将升级或修改部署到网络的时候，实现成本最小化。

请注意，所有的系统奖励（交易费、转账费、区块奖励）都由节点运营商和 LP 共享。节点 运营商和 LP 之间的奖励分配由激励调节机制控制，更多细节将在下一节进行说明。

RUNE 代币经济学

RUNE 是 THORChain 网络的原生代币。RUNE 与系统中的其他资产保持着相对平衡状态，维护网络安全。对于网络中的每 1 美元原生资产，LP 必须将价值一美元的 RUNE 质押到相应的连续流动性池，并且网络节点必须抵押价值 2 美元的 RUNE 来达成共识。该措施激励了节点运营商诚实地运营网络，因为它们可能被罚没的代币数量始终大于流动性池中资产的 价值。审查或盗窃资产是绝对无利可图的行为。因此，网络中的 RUNE 数量旨在在节点和 LP 之间达到 67%-33%的平衡。在整体上，该网络为每一美元其他资产质押三美元的 RUNE 代币。

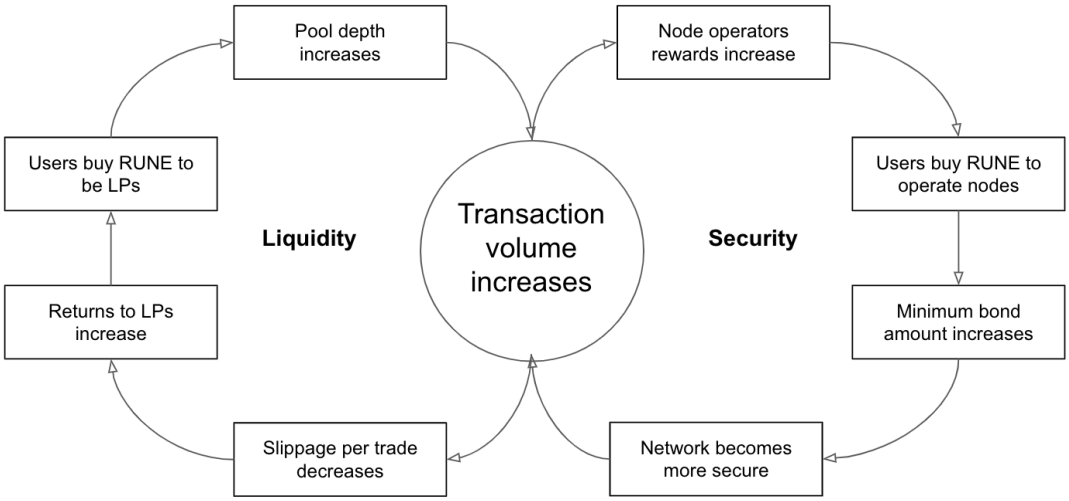


当系统失衡时，网络会调整区块奖励和网络费用，来激励节点运营商和 LP 恢复平衡状态— —这种机制称为“激励钟摆”。

例如，如果系统中超过 67%的 RUNE 质押给节点运营商，那么协议将分配更多的奖励给 LP。如果系统中超过 33%的 RUNE 位于流动性池中，那么协议会分配更多的奖励给节点 运营商。

在过去的一个月，市场份额排名前五的以太坊 DEX 的平均日交易量为 20 亿美元（相比之 下，Coinbase 为 40 亿美元），并且这些 DEX 仅交易 ERC-20 资产。随着 THORChain 在 未来几个月内增加对所有主流区块链的支持，它很有可能取代许多中心化交易所，成为交 易的首选场所。

而随着越来越多的交易通过 THORChain，RUNE 将变得越来越有价值。RUNE 持有者可 以通过质押 RUNE 或成为 LP 来获得系统的收入。这直接将 RUNE 的价值与 THORChain 去中心化交易所的交易量和流动性绑定在一起。



发展历史

许多人不知道 THORChain 的出现比现在许多流行的去中心化交易所要早，它诞生于 2018 年币安赞助的黑客马拉松比赛。在黑客马拉松之后，一个致力于开发去中心化交易的匿名 团队接手了该项目，并持续进行了几个月的迭代。但是，由于当时缺乏基础架构和开发者 工具，项目开发停滞了。

2019 年，随着 GG18 门限签名方案（TSS）的发布，该项目再次发力，将 TSS 应用到 THORChain 的无信任跨链桥接机制中。KZen（来自 ZenGo 的制造商）对 TSS 实施提供 了一种在多方之间分配签名权的有效方法，最终让 THORChain 实现了单向状态锚定。 TSS 的改进还能与 Tendermint Core 和 Cosmos SDK 的强大突破相互组合。这些发展使 THORChain 能够顺利开发核心协议。

随着基于绑定/流动性池的系统安全模型的初始概念融合在一起，在 2019 年 6 月的柏林 Cosmos 黑客松，团队以"Instaswap"这个绰号开发了概念证明。该产品以 BEPSwap（币安链上的 DEX）的名称推出，用于交易币安链资产。2019 年 7 月，团队采用了 THORChain 这个名字，并通过币安链发行 RUNE，筹集到 150 万美元的首次去中心化交 易所公开募资（IDO）。

此后，THORChain 一直将开发和资金运营的透明性放在首位。团队充分发挥了大众开发的 精神；他们每周都分享开发进度和优先级更新，并积极采纳社区在机制设计和架构方面的 宝贵贡献。该方式得以围绕着核心协议打造了一个丰富的生态，社区成员使用 THORChain 开发者 SDK 构建了浏览器、前端、钱包和流动性展示板。THORChain 的核心团队有八名开发者。财政储备目前价值 2500 万美元，可提供充足的支 持。有关协议储备金和社区资助计划的详细信息，您可以点击这里阅读。

2020 年 8 月，THORChain 推出了它的第一个概念验证网络 Chaosnet，其中有 14 个节点 运营商。BEPSwap，运行 Chaosnet 的客户端现在有 74 个节点。它致力于在币安链资产 之间进行兑换交易，每天处理大约 3000 万美元的交易量，其中大约 7000 万美元集中在流 动性池。2020 年 1 月，THORChain 团队发布了币安链-以太坊桥，并与 SushiSwap 达成 合作，为以太坊上的 ERC-20 RUNE 建立流动性。目前，SushiSwap 上的 RUNE 交易对 （如 ETH、ALPHA、USDT、PERP 和 AAVE）的流动资产价值为 2600 万美元。

所有这些工作最终迎来了即将到来的重大网络事件：多链发布。此次发布将扩大对 BTC、 ETH、LTC、BNB 和 BCH 的支持。正式启动后，交易者将能够将 ETH 和 BNB 或任何 ERC-20 或币安链资产交易成 BTC、LTC 或 BCH，反之亦然（假定网络具备足够的流动 性），而无需牺牲其资金托管。

THORCHAIN 社区

THORChain 非常了解模因（meme）在社区发展共同身份中的作用。第一次听到 THORChain 这个名字的时候，我们认为它傻乎乎的。但是随着时间推移，团队证明了这是 一个深思熟虑的决定。由于涉及北欧神话，它为大众提供了丰富的角色和 meme 内容。而 易于关联的 meme 可以协助项目品牌的扩散。

自发布以来，THORChain 吸引了一大批第三方团队开发产品，以帮助推动生态的发展。一 些示例包括：

1. **Pusher Labs 开发的 THORChain Explorer**—THORChain.net 是 THORChain 项目 的区块浏览器。该浏览器提供了一个文档齐全的 API、网络统计信息摘要和交易记 录。
2. **XDEFI**——一个类似于 MetaMask 的浏览器钱包，将会支持连接到 THORChain 的区 块链。
3. **BEPSwap Simulator**—一个简单的工具，可协助计算 THORChain 的资产池价格。
4. **THORChain 帮助中心**—THORChain 团队面临的最大挑战之一是用非常容易理解的 方式向非技术用户介绍该产品。幸运的是，有个第三方团队开发了一个面向非技术 用户的简单的 THORChain 解释程序。
5. **MIDGARD API**—查询 THORChain 的公共 API，社区在上面开发了一个展示板，例 如 THORChain.net（网络活动监视）和 Runestake.info（LP 返回跟踪）。
6. **XChainJs**—基于 THORChain 的一组 JS 库。

THORChain 社区是当今最大的资产之一。THORChain 团队在培养文化方面做得非常出 色。它们共同体现了去中心化网络的精神。他们还有一个主动更新的"计划过时"日期，这表 明核心开发人员将把代码库的所有权转让给社区进行维护的时候。当前设置为 2022 年 7 月。

竞品分析

ChainFlip 正在自定义状态机上、使用 TSS 达成共识，来构建类似的基于 AMM 的跨链交易 产品。该项目于 2020 年 7 月宣布，团队目前正在验证概念的可行性。

ChainFlip 实现非监管跨链交易的主要区别在于，它采用阈值签名的变体 EdDSA（与 THORChain 的 ECDSA 相比），在状态机中结合了特定区块链的逻辑。THORChain 完全 不同于 UTXO/帐户模型，而 ChainFlip 需要知道每个区块链的细微差别。结果导致 ChainFlip 在增加新区块链的支持更加困难和耗时。它的取舍是通过将交易发布到称为"引 号"的许可 API 来更快地生成和签名密钥，这意味着整个系统中的子金库更少，但受攻击面 却更大。

ChainFlip 团队此前曾为 Monero 开发基础架构，并推出了 LOKI，这是一种具有低延迟、 匿名网络的隐私代币。

如果 Polkadot 和 Cosmos 能实现它们白皮书中概述的愿景，它们就能完美连接各种区块 链。但是，现在它们主要使用 Substrate（Polkadot）和基于 Cosmos SDK 的区块链。例如，Polkaswap 无法处理现货原生 ETH/BTC 兑换。

Ren 是另一个正面竞争者。RenVM 专注于固定资产转移，并计划逐步通过多个阶段实现去 中心化。RenVM（零以下阶段）当前的实现方式主要集中在核心开发者维护所有功能节点 的同时，社区节点仅对 p2p 网络层进行操作。在未来的迭代中，社区节点将达成共识，并
可能增加对大型资本资产的支持。Ren 拥有丰富的开发人员资源和机构支持，但市场定位 缺不同：封装代币，而不是现货交易。封装代币具有重大风险；也就是说，由于它在根本 上不如持有现货 BTC 安全，因此可能失去锚定。

KEEP 的 tBTC 可能是打包/固定 BTC 最去中心化的实现。目前，以太坊上有超过 1,800 tBTC，覆盖 1,000 多个地址。tBTC 系统类似于 THORChain，它们也使用 ECDSA 阈值签 名进行多方计算，但是在绑定模型、签名者选择和存款验证的实现方面存在关键差异。

与 Ren 相似，Keep 追求的是固定资产市场，而不是现货交易。Multicoin Capital 对 Keep 同样进行了投资，并且对他们开发的产品（特别是 tBTC）非常满意。

即将到来的大事件

THORChain 团队最近发布了多链测试网，该网络支持原生 BTC 兑换成 ETH、LTC、BCH 和 BNB 资产。核心团队目前正在积极探索，增加对 Dogecoin、Monero、Zcash、 Polkadot、Haven Monero 和其他几个区块链的支持；随着主网的发布，这些支持也将在未 来几个月内逐渐公布。

从长远来看，该团队希望通过杠杆交易功能来改善网络的资本效率。一些示例包括：

1. **提高资本效率**——使用流动性份额作为抵押的池贷款，并按照债务资产相关的资产 池收集利息
2. **合成资产**——THORChain 合成器的独特之处在于它们支持流动性份额，并且现货资 产和 RUNE 的份额分别占 50%。它们还兼容 IBC，因此可以发送到 Cosmos 生态中 的任何地址。
3. **复合资产**——THOR.USD 或 THOR.ALT 等复合资产是多资产合成池的 LP 股票代 币，可在交易活动中产生费用。

结论

THORChain 团队一直在坚持不懈地执行路线图。他们是加密该领域中最透明的团队之一， 持续提供开发进度、库房/业务储备金管理以及常规开发节奏来执行长期策略。在沟通方面 他们也是最好的，这有助于建立并吸引一个强大的社区。

THORChain 团队致力于以开放、可访问的方式开发其核心基础架构，确保 THORChain 的 去中心化由社区控制。目前，财政部每月通过社区开发向第三方开发者分配 20 万美元的赠 款。

THORChain 代表了信任最小化的跨链交易的未来，他们一直在开发突破性技术，培养了一 个面向庞大市场的惊人社区。

我们对投资并支持 THORChain 团队感到无比兴奋，并相信跨区块链的最小化信任和无许 可交易将主导现货加密货币交易。