探索区块链的模块化：汇总介绍

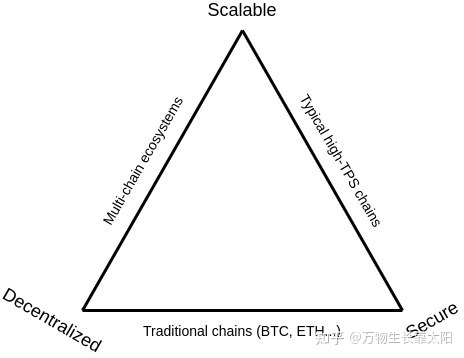


10 月 26 日，我收听了由 David Hoffman 和 Ryan Sean Adams 主持的关于整体区块链与模块化区块链的现场 Bankless 播客。如果这两个术语对你来说都没有任何意义，那绝对没问题，因为模块化区块链的概念让我很紧张，我决定在几篇文章中对其进行分解。我相信模块化区块链代表了区块链技术的未来，如果您希望在未来掌握区块链生态系统，那么它们对于理解至关重要。这个博客的目的是让你和我一起学习，所以我会把所有相关的概念都归结为基础，以便清楚地描绘出什么是模块化区块链，为什么它们很重要，以及如何投资在他们之中。

在完全掌握模块化区块链之前，需要了解两个关键概念：（1）汇总，以及（2）分片。本文将重点介绍汇总；它们是什么，它们如何工作，以及它们未来的发展方向。在不久的将来，一篇文章将关注分片。然后，我将用一篇将所有内容联系在一起的文章来完成这三部分的系列文章，以解释模块化区块链和区块链生态系统的未来。

**区块链三难困境和第 2 层的诞生**

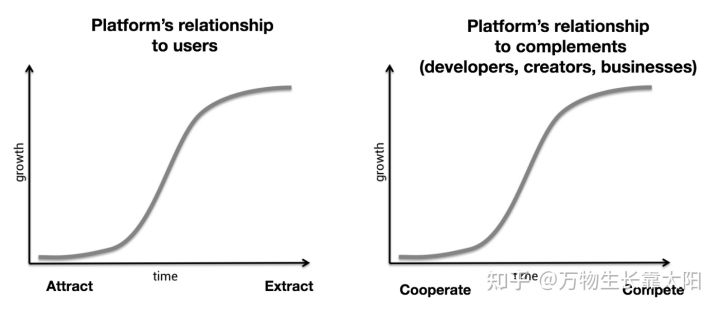
本质上，区块链面临着三难困境，称为区块链三难困境。这是指所有区块链都面临的一种权衡，在去中心化、可扩展性和安全性之间进行权衡，其中一个区块链只能优化两个，以牺牲第三个为代价。显然，安全性对区块链至关重要，因此这通常会导致对去中心化或可扩展性的妥协。



**为什么去中心化很重要？**

你可能想知道，为什么权力下放很重要？这通常是一个被误解的概念，经常有人提出 web3 提倡去中心化以抵制政府审查的建议。事实上，这并不是权力下放很重要的主要原因。答案主要在于激励创新。

中心化平台的问题主要在于其可预测的生命周期。一开始，平台非常有吸引力，因为它们必须吸引用户、开发者、企业和媒体组织，这将不可避免地使他们的平台变得有价值。他们降低了进入门槛，并榨取了很少的价值来创造一个积极的环境来鼓励参与者。正如 Chris Dixon[所说](https://link.zhihu.com/?target=https%3A//onezero.medium.com/why-decentralization-matters-5e3f79f7638e)，中心化平台这样做是为了“使他们的服务更有价值，因为平台（根据定义）是具有多边网络效应的系统。” 当平台向上移动其 S 曲线并获得对用户和开发人员的更多权力时，就会出现问题。



一旦中心化平台达到其 S 曲线生命周期的顶部，其与平台参与者的关系的性质就会从正和减少到零和。一般来说，这意味着中心化平台将转向从其用户那里提取和货币化数据，并与在其平台上开发的互补业务竞争注意力（例如，[推特对第三方客户的支持](https://link.zhihu.com/?target=https%3A//www.itpro.co.uk/development/31719/twitter-kills-support-for-third-party-clients" \t "_blank)）。这对创新和这些平台的持续发展来说是个坏消息。

在过去的十年中，我们已经看到这个生命周期在多个平台上发挥作用；Facebook、Twitter、微软、YouTube 和谷歌等等。这些是当今基本上拥有互联网的平台。最终，这促使企业家、开发商和投资者对这些类型的平台保持警惕，许多人完全拒绝建立与中心化平台相关的平台。当强大的中心化平台对他们的创作有如此多的控制权时，他们为什么要这样做？他们为什么要冒着自己的创作被带走的风险来建造？想想在 YouTube 上开发品牌的内容创作者，结果他们的观众人数被他们无法控制的推荐算法减半，或者开发者在全球社区开发游戏作为 Facebook 插件，只有 Facebook 删除了他们的第三方- 客户端 API。

另一方面，去中心化平台不存在审查风险。企业家和开发人员可以问心无愧地自由构建。这与互联网的第一个时代（1980 年代至 2000 年代）非常相似，当时互联网服务主要建立在互联网社区本身拥有的开源协议上。根据定义，去中心化平台无法从用户和开发者那里提取价值，而是允许用户和开发者创造价值。为了明确这一点，谷歌将自己与“不作恶”的座右铭联系在一起，而在一个去中心化的平台中，这变成了字面上的“不能作恶”。



这一切听起来都很棒，虽然我认为我们有一个令人信服的去中心化平台案例，但它们真的赢了，甚至在现实中发生了吗？互联网的第一个时代是由去中心化的开源协议赢得的。第二个时代由集中式应用程序主导，例如 Google、Youtube 和 Twitter。我相信互联网的第三个时代很可能是去中心化的。原因很简单：这是建造者所在的地方。由于上述原因，企业家和开发人员被排斥在中心化平台上进行构建，因此纷纷涌向去中心化平台（如以太坊）上进行构建。如果没有企业家和开发者，互联网的第三个时代会怎样？当然，您可能会争辩说，中心化平台可能能够简单地向开发人员付款，但在我看来，他们无法超越那些建立在去中心化平台上的人，他们肯定无法与完全自由的企业家的创新速度相提并论。考虑到互联网第三个去中心化时代的代币化性质时尤其如此，在这个时代，企业家能够以惊人的速度筹集资金，减少中心化平台简单地支付给开发者社区的影响。

区块链技术是web3终极平台的温床。一种不需要第三方参与，并且在很大程度上消除了低效率的情况。如果我们要鼓励企业家、开发商和投资者在这些区块链平台上进行建设，我们必须让它们去中心化。有关此加载主题的更多细节，我会强烈建议阅读[该](https://link.zhihu.com/?target=https%3A//onezero.medium.com/why-decentralization-matters-5e3f79f7638e)文章。

太好了，从创新、用户隐私和数据所有权的角度来看，区块链去中心化是有意义的。不幸的是，这意味着在区块链三难困境中放弃可扩展性。

**区块链的组成部分**

这些区块链过去的工作方式是，当有人发布交易时，矿工对其进行验证，然后将其发布到区块链上，但随后网络中的所有其他矿工也必须对其进行验证。鉴于在去中心化网络中可能有大量矿工，这显然代表了许多低效和浪费的工作。

然而，去中心化、安全性和可扩展性只是区块链的属性，由组成所述区块链的组件决定。作为一个基本概念，概述这些组件很重要：(1) 共识，(2) 数据可用性，以及 (3) 执行。共识组件规定了网络中节点对交易的集体验证，为存储在区块链上的数据提供安全性和真实性。数据可用性是指结​​算层保证可用于在区块链上进行交易的数据（即转移、持有状态等）。执行是指用新信息更新区块链所需的计算。

简单地说，共识组件是对区块链上的交易记录进行商定和存储的地方。数据可用性组件是区块链在任何一个时间点有多少空间来添加额外的数据。执行组件是新交易在验证并写入永久记录之前在区块链上注册的地方。

作为区块链三难困境的解决方案，开发了第 2 层扩展解决方案。第 2 层协议可以被认为是以太坊结算层的扩展解决方案，它允许结算层优化去中心化和安全性。我将在本文后面介绍不同类型的扩展解决方案以及它们的工作原理。第 2 层扩展解决方案纯粹关注区块链的执行和（偶尔）数​​据可用性组件。共识组件本质上必须与结算层共存，以利用其去中心化和安全特性。

迄今为止，价值约 66.2 亿美元的价值已被锁定在第 2 层解决方案中，Arbitrum 和 dYdX（由 StarkEx 提供支持）等领先解决方案吸引了大部分份额。



有多种类型的扩展解决方案，包括状态通道、等离子、侧链和汇总。出于本文的目的，由于状态通道、等离子、侧链和验证扩展解决方案的固有限制，我将重点介绍汇总。在区块链的三个组件的上下文中，汇总主要关注执行层。

**汇总类型**

Rollup 是可扩展的解决方案，可将交易捆绑、压缩并将其发送到共识层进行验证。通过一次验证多笔交易，它们显着提高了效率，同时允许以太坊每秒处理 15 到 3000 多笔交易 (TPS)，而不会牺牲安全性。

本质上，用户不是将交易发送给第 1 层矿工，而是将他们的交易发送到汇总服务器，该服务器验证这些交易是否有效。所以他们在以太坊主链之外执行交易，但这些汇总然后将交易数据发布到以太坊主链。在将交易发布到主链时，它们继承了第 1 层的安全属性。

有两种类型的汇总，具有不同的安全模型：(1) 乐观汇总和 (2) 零知识汇总。

**乐观汇总**

Optimistic Rollup 捆绑了数百次传输，并且仅发布链上所需的最低限度的信息，无需证明。这基本上假设没有发生欺诈或恶意行为，因此得名“乐观”。乐观汇总只会在转移或状态受到质疑时提供证据。

乐观汇总的好处，除了明显的扩展增强之外，还包括 EVM 和可靠性兼容性，这意味着你可以在以太坊第 1 层上做的任何事情，你都可以在乐观汇总上做。

然而，由于潜在的欺诈挑战，链上交易的等待时间可能很长。您必须等待大约 1 周才能从乐观汇总中提取资产，因为这为检测和解决欺诈留出了时间。这是假设没有发生欺诈或恶意行为的固有问题。

乐观汇总的另一个缺点是需要在链上发布所有见证数据，例如签名、预言机提要等。这限制了可扩展性，尤其是与零知识汇总相比时，我将在稍后讨论。

大型乐观汇总协议包括 Arbitrum 和 Optimism。我将在本文后面探索这些协议。

**零知识汇总**

零知识 (ZK) 汇总不同于乐观汇总，因为它们通过利用零知识技术集成了隐私。零知识是指向另一方证明某事（交易或状态）而无需披露证明它所需的信息的能力。

用户不是将交易发送到第 1 层矿工，而是将交易发送到汇总服务器，在那里执行交易。ZK rollup 中最常用的两种验证证明是 ZK-SNARKS 和 ZK-STARKS，我将在后面的部分中介绍 ZK-STARKS。然后生成 ZK-SNARKS（零知识简洁非交互式知识论证）作为交易有效性的证明，并发布到第 1 层主链。如果您对 ZK-SNARK 究竟是什么以及它们的形成方式感兴趣，我强烈建议您阅读[这篇](https://link.zhihu.com/?target=https%3A//z.cash/technology/zksnarks/" \t "_blank)短文。这些证据生成速度快，令人信服，而且验证速度快得令人难以置信。对于上下文，可以将数百个交易汇总到一个证明中，验证该证明需要大约 5 毫秒。

通过利用这项技术的零知识特性，第 1 层的矿工将永远不会知道交易中的数据是什么。只有汇总矿工会知道交易数据。这是一项非常令人兴奋的技术，因为它意味着数据可以是私有的，即使在公共区块链上也是如此。这对于像苹果这样的公司来说至关重要，他们可能希望保密他们向某些实体支付的费用等。

使用ZK rollup，提取资产没有延迟，因为ZK rollup合约接受的ZK-SNARK证明已经验证了资产。这是乐观和 ZK 汇总之间的主要功能差异之一。

如上所述，ZK 汇总的优点包括更快的确定时间，以及比乐观汇总更不易受到经济攻击的影响。然而，ZK-SNARK 证明的计算量很大，对于链上活动很少的应用程序来说，它可能被认为不值得。

到目前为止，我将在本文稍后介绍主网上的四个主要 ZK 汇总协议，但有关 ZK 汇总协议的完整目录，请查看[此](https://link.zhihu.com/?target=https%3A//www.zkrollups.xyz/" \t "_blank)链接。

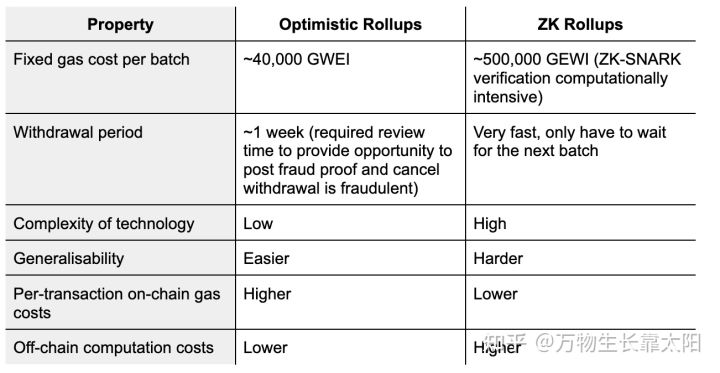
这里值得注意的是，目前大多数 ZK rollup 还没有真正利用 ZK 技术的隐私方面。相反，他们专注于可扩展性方面，即与本地计算相比，证明可以呈指数级小且易于验证。

**Optimistic 和 ZK Rollup 的技术比较**

以太坊的联合创始人 Vitalik Buterin 撰写了大量关于汇总技术以及乐观和 ZK 汇总的比较的文章。以下是基于技术比较的 Vitalik 对这两种技术的展望。

*在一般情况下，我自己的看法是，在短期内，乐观汇总有可能胜出的通用EVM计算和ZK汇总有可能胜出简单的支付，交换和其他应用程序特定的使用情况，但在随着 ZK-SNARK 技术的改进，中长期 ZK 汇总将在所有用例中胜出。— Vitalik Buterin（*[*来源*](https://link.zhihu.com/?target=https%3A//vitalik.ca/general/2021/01/05/rollup.html)*）*

下面我总结了乐观和 ZK 汇总之间的技术比较。



虽然目前乐观汇总比 ZK 汇总更实用，但仅仅由于它们的复杂性较低，ZK 汇总显然有可能为用户提供更大的好处。我将在本文的下一部分探索每种汇总类型的未来路线图。

**Rollup 的未来**

虽然目前这两种汇总类型都提供了高于原生以太坊链执行层的好处，但仍有一些具有挑战性的方面需要改进或完全开发。

**面临的挑战**

EVM 代表以太坊虚拟机，可以被认为是一个大型的去中心化计算机，可以计算区块链上的所有类型的任务。它本质上是以太坊整个运营结构的基石，运行执行和智能合约部署。

EVM 兼容性意味着另一个链，例如汇总链，将能够在该链上部署以太坊智能合约。因此，如果没有 EVM 兼容性，另一条链就不可能运行以太坊智能合约。EVM兼容性显然是非常有利的，因为这意味着已经部署在以太坊上的项目，比如Uniswap等DeFi巨头，都可以部署在兼容链上。这意味着兼容链在执行模块上吸引用户相对容易，如果他们比以太坊执行模块具有显着的竞争优势。考虑到以太坊社区内开发人员的规模，这对于兼容链来说也是一个巨大的优势。通过与 EVM 兼容来利用该社区，

EVM 兼容性的缺点源于复杂性以及相关的安全漏洞风险。因此，为什么 EVM 兼容性开发一般来说对于 rollup 来说是缓慢的，但是已经取得了一些突破，特别是在乐观汇总的背景下，我稍后会提到。

Rollup 的另一个挑战，实际上是我看到未来发展最兴奋的一个挑战，是直接法币入口。法定货币是指传统货币，例如美元、英镑和日元。On-ramp 是指一种服务，您可以在其中直接转换法定货币以换取加密货币。法币入口服务目前通常在中心化交易所 (CEX) 上找到，例如 Coinbase 和 Binance。

迄今为止，在购买加密货币的过程中存在几个瓶颈，这纯粹是因为难以从传统银行账户中获取法定货币并进入加密货币世界。如果您希望与去中心化交易所 (DEX) 进行交互，通常的做法是将法定货币存入 CEX，然后必须将此法定货币兑换成加密货币，然后才能将其转移到您选择的钱包中，例如[MetaMask](https://link.zhihu.com/?target=https%3A//metamask.io/" \t "_blank)，然后与您选择的 DEX 进行交互。这显然有点麻烦，并且显着降低了用户体验。值得注意的是，有一个项目叫[Dharma](https://link.zhihu.com/?target=https%3A//www.dharma.io/" \t "_blank)，这是唯一一个可以在您的银行账户和去中心化交易所（如 Uniswap）之间无缝转移法定货币的以太坊钱包，无论是在以太坊还是 Polygon，这是一个收费较低的侧链。但是，此解决方案仅适用于美国银行，并且相对较新。

汇总的挑战更大。为了在汇总时与加密进行交互，您面临着将加密放入您选择的钱包的瓶颈，从那里您必须将您的加密资产桥接到汇总本身。这是一种非常糟糕的用户体验，需要很大的耐心。值得注意的是，法币入口解决方案 Ramp 最近宣布与 Zk Rollup 的 zkSync 建立合作伙伴关系。我将在本文后面谈到这一点。

我真的相信直接法币入口的大规模采用，即从您的传统银行账户直接进入汇总的路径，将大大增加使用率。这就是为什么我对他们的发展如此兴奋；增强的用户体验无疑会让用户有理由不再直接与第 1 层交互，并将标志着从第 1 层执行到第 2 层执行的大规模迁移，让第 1 层专注于共识和安全。这将是模块化区块链采用的真正开始。

还值得注意的是，要使汇总达到最低费率，它需要最大化在第 1 层链上结算的交易。这是为了在汇总的许多交易中平均分配费用。所以 rollup 费用可以看作是 Layer 1 费用的乘积，也是 rollup 需求的乘积。因此，要使汇总在与以太坊相比的费用降低方面真正发挥其潜力，它们需要更高水平的需求。这通常被称为规模经济，意味着下一次边际交易的边际交易成本会降低。

这几乎创造了一个先有鸡还是先有蛋的场景，在这种情况下，用户需要大幅降低费用，但只有在费用极低时才可能切换。但是，我不认为这是一个特殊问题。事实上，从某种意义上说，它是一个突破，它颠覆了区块链的传统成本结构，通常每笔边际交易都会变得更加昂贵。这也是 ZK 汇总优于乐观汇总的一个实例，因为乐观汇总将始终需要包含每个交易的签名，从而增加了另一个成本因素。另一方面，ZK 汇总不需要签名，并且具有更好的数据压缩，从而具有出色的可扩展性潜力。

**现有的乐观项目**

*仲裁*



我将涉及的第一个乐观汇总是[Arbitrum](https://link.zhihu.com/?target=https%3A//arbitrum.io/)，这是一个由[Offchain Labs](https://link.zhihu.com/?target=https%3A//offchainlabs.com/" \t "_blank)构建的乐观汇总协议。Arbitrum 于 2021 年 8 月全面上线以太坊主网，称为主网网络 Arbitrum One。全面启动恰逢[Lightspeed Venture Partners](https://link.zhihu.com/?target=https%3A//lsvp.com/" \t "_blank)领导的 Offchain Labs 筹集了 1.2 亿美元的资金。

Arbitrum 支持所有 EVM 语言，并且原生支持所有以太坊工具，无需任何特殊适配器，从而使其完全兼容 EVM。这包括部署智能合约和 dApp。然而，在幕后，由于 Arbitrum 虚拟机，这一切都是可能的，尽管这从未向开发人员或用户公开。

迄今为止，这种 EVM 兼容性使以太坊生态系统中的一些最大的 dApp 能够部署到 Arbitrum，包括 DeFi 巨头 Uniswap、SushiSwap、Aave、Curve 和 1Inch。可以在[此](https://link.zhihu.com/?target=https%3A//portal.arbitrum.one/" \t "_blank)链接中找到钱包、dApp 等生态系统的完整列表。这些部署的结果是锁定在网络上的总价值超过 26.5 亿美元。

从吞吐量的角度来看，Arbitrum One 的理论最大 TPS 为 40,000，但实际上目前记录的最大 TPS 约为 49。与以太坊主网相比，使用 Arbitrum One 的成本优势在很大程度上取决于传输类型，例如， Arbitrum One 的普通转账费用约为以太坊主网的 36%，而 Uniswap v3 交易的费用则为 6.9%。

*乐观*



[Optimism](https://link.zhihu.com/?target=https%3A//www.optimism.io/)是我今天要提到的第二个乐观汇总，它于 2021 年 7 月推出到主网上。自推出以来，Optimism 已累计锁定网络的总价值为 4.66 亿美元，处理了超过 220 万笔交易。

根据 Optimism 的说法，他们的乐观汇总解决方案在与以太坊主网进行交易时帮助节省了超过 1 亿美元的 gas 费用，表明您可以在几毫秒内进行交易，并节省 10-100 倍的费用。该网络本身拥有超过 100,000 个独特的钱包地址（用户）。

2021 年 11 月，Optimism 在 Optimistic Ethereum 上启用了 EVM 等效项，取代了之前使用的 Optimistic Virtual Machine 解决方案。EVM 等价性完全符合以太坊堆栈；每个调试器、工具链、节点实现，当然，还允许部署智能合约和 dApp。



这种 EVM 等效性使得以太坊生态系统中的许多关键参与者能够部署到 Optimism 网络。这些主要参与者包括但不限于 Uniswap、Synthetix 和 1Inch。

值得注意的是，目前 Optimism 正在运行，没有欺诈证明。换句话说，这意味着乐观汇总技术方面还没有开启。

**现有 ZK 项目**

*斯塔克网*



我将涉及的第一个 ZK 汇总项目是[StarkNet](https://link.zhihu.com/?target=https%3A//starkware.co/starknet/" \t "_blank)，它是[StarkWare](https://link.zhihu.com/?target=https%3A//starkware.co/starknet/" \t "_blank)的以太坊主网 ZK 汇总。StarkNet Alpha（StarkNet 的未经审计版本）于 2021 年 11 月 29 日在主网上发布，已部署到测试网，这是一个由较新版本的底层软件驱动的区块链的不言自​​明的实例，用于测试和调试， 2020 年 6 月。

StarkNets 的前身 StarkEx 于 2020 年 6 月在主网上线，并提供对通用智能合约的支持。StarkEx 上部署的应用程序有[dYdX](https://link.zhihu.com/?target=https%3A//dydx.exchange/" \t "_blank)、[ImmutableX](https://link.zhihu.com/?target=https%3A//www.immutable.com/" \t "_blank)、[DiversiFi](https://link.zhihu.com/?target=https%3A//deversifi.com/" \t "_blank)和[Sorare](https://link.zhihu.com/?target=https%3A//sorare.com/" \t "_blank)。迄今为止，他们已经处理了 6500 万笔交易，四个协议的累计交易额为 2150 亿美元。StarkEx 网络还展示了 9,000 TPS 的交易速率和 18,000 TPS 的传输速率，这相当于以太坊主网执行层的交易可扩展性提高了大约 600 倍。

StarkNet 沿用了其令人印象深刻的前身，在完全可组合的网络上提供通用智能合约。可组合性是指应用程序协调、相互构建和互连的能力。其他 StarkNet 合约和通过 L1<>L2 消息传递的第 1 层合约都支持这种可组合性。StarkNet 也将是免许可的，这意味着它使 dApp 能够利用 StarkNet 的无限规模进行计算，而无需请求在网络上部署的许可。但是，目前 StarkNet Alpha 仅适用于列入白名单的 dApp。

StarkEx 和 StarkNet 与竞争性 ZK 汇总相比的最大优势之一是他们的 ZK-STARK（零知识可扩展透明知识论证）技术。ZK-SNARKs 和 ZK-STARKS 都是隐私增强技术，因为它们减少了用户之间需要交流的信息量。它们也是扩展解决方案，因为它们允许以比本地以太坊执行模块更快的速度验证证明，因为它们不包含非私有系统的全部信息。然而，虽然 ZK-SNARKS 需要可信的设置阶段，但 ZK-STARKs 使用可公开验证的随机性来创建无需信任的可验证计算系统。结果是，与 ZK-SNARKs 相比，ZK-STARKs 在计算速度和大小方面更具可扩展性。

最重要的是，由于强大的加密原语（如 has 函数），ZK-STARKS 对计算上无界的证明者具有稳健性。这意味着验证者相信虚假 ZK-STARK 的可能性为零。结果：ZK-STARK 是后量子的，因为它们的安全性不依赖于证明者的计算能力。有关更多详细信息，请查看下面的推文线程，在此背景下解释 ZK-SNARKS 和 ZK-STARKS 之间的比较。



然而，StarkNet 并不直接兼容 EVM。相反，他们开发了一种名为 Cairo 的 STARK 优化编程语言。Cairo 用于在区块链上编写可证明的程序，使开发人员能够使用证明技术。一个名为[Nethermind 的](https://link.zhihu.com/?target=https%3A//nethermind.io/" \t "_blank)软件解决方案团队随后开发了一种将[Solidity](https://link.zhihu.com/?target=https%3A//github.com/NethermindEth/warp)（EVM 语言）转换为 Cairo的解决方案，因此存在间接 EVM 兼容性。STARK 和 Cairo 均由 StarkWare 内部开发，并为其所有生产级应用程序提供支持。

从下面的 StarkNet 路线图可以看出，最后一步是将 StarkNet 引入去中心化治理模型。StarkNet 目前不以代币表示，这意味着日常投资者没有流动的方式来投资项目和技术。但是，去中心化治理模型很可能会引入相关的代币，可用于推测该技术。话虽如此，StarkNet核心开发者多次拒绝回答“文令牌”问题，纯属猜测。



*同步*



第二个 ZK 汇总项目我将看一下它[zkSync](https://link.zhihu.com/?target=https%3A//zksync.io/" \t "_blank)，这是 Matter Labs 的主网 ZK 汇总。几个月前，Matter Labs 从 a16z 那里获得了 5000 万美元的投资，以帮助他们将 ZK 汇总可扩展性引入以太坊。zkSync 于 2020 年 6 月在主网上线，主要用于可扩展支付。这意味着用户可以存入网络并在其他 zkSync 帐户之间转移，而成本只是以太坊的一小部分。

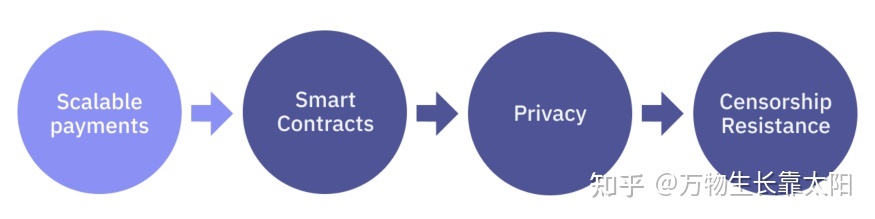
迄今为止，zkSync 已经处理了 400 万笔交易，锁定在网络中的总价值为 2400 万美元。2020 年 7 月，该网络通过[zkNFT](https://link.zhihu.com/?target=https%3A//zknft.xyz/%23/" \t "_blank)添加了 NFT 功能。

Matter Lab 的 zkSync 迭代 zkSync 2.0 计划在主网上启动，旨在在 ZK 汇总上提供完全可组合的智能合约。zkSync 2.0 将引入 zkEVM，一种模拟以太坊等环境的虚拟机，从而使其与 EVM 兼容并实现以太坊智能合约的部署。zkEVM 测试网已成功引入 UniSync（Uniswap V2 的一个分支）以演示其功能。自 10 月推出以来，UniSync 已在其测试网上处理了超过 3,000,000 笔交易。

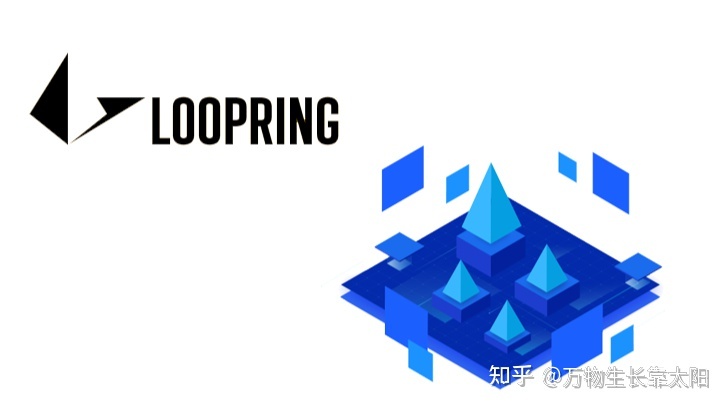
zkSync 的一个巨大发展是宣布与[Ramp](https://link.zhihu.com/?target=https%3A//ramp.network/" \t "_blank)建立合作伙伴关系，以直接在 zkSync 协议上提供法定入口。这是一般汇总的主要缺点之一的解决方案，毫无疑问将推动 zkSync 网络的大量采用。



下面的 zkSync 路线图与 StarkNet 的路线图类似。我们已经看到了将 zkSync 引入主网的第一阶段。zkSync 2.0 将在部署到主网时完成第二阶段。最后一个阶段，审查阻力，最终将要求平台去中心化并变得无需许可，这可能意味着引入治理令牌。zkPorter 是一个权益证明链，将为 zkSync 2.0 提供链下数据可用性，预计将拥有自己的代币。



*环印网*



Loopring 是一种 ZK 汇总协议，允许构建高度可扩展的交换和支付解决方案，从而允许在以太坊上进行高吞吐量、低成本的交易和支付。Loopring 3.0，他们的第一个 ZK rollup 迭代于 2019 年 12 月发布到主网上，并且是第一个部署到以太坊主网上的零知识汇总 DEX 协议。最新版本的路印 v3.6 已于 2020 年 12 月部署到主网上。

迄今为止，Loopring 在协议中的总锁定价值超过 6.5 亿美元。据 Loopring 自己称，他们的 ZK Rollup 吞吐量达到了以太坊的大约 1000 倍的交易，或者高达每秒 2,025 笔交易，这是对原生以太坊执行模块用户体验的显着增强。Loopring 利用 ZK-SNARKS 来实现这一点，就像 zkSync 一样。

Loopring 是唯一一个拥有自己的智能钱包的 ZK rollup 协议，可以在 iPhone 和 Android 上作为应用程序下载。它允许您将您的加密资产存储在他们的汇总中，并与他们的 ZK 汇总的功能进行交互，包括交易和支付。但是，目前设置路印本机钱包的费用约为 300 美元。这有望在不久的将来被完全免费的路印钱包的发布所取代。2021 年 8 月，Loopring 宣布它现在直接在其 ZK 汇总协议上支持 NFT 铸造、交易和转移。

Loopring 有一个原生代币 $LRC，可在许多交易所使用，包括 Coinbase 和 Binance。该令牌是在整个 2018 年的三个阶段空投期间向路印 v1 的早期采用者发布的。$LRC 作为路印协议的治理代币，使其完全去中心化。$LRC YTD 的表现如下。



就 Looping 的路线图而言，他们的团队概述了 2021 年第四季度需要注意的一些事项。鉴于距离这个时间框架只剩下不到一个月的时间，我们应该会很快看到其中的一些功能被添加。第一个将是在 Loopring 上开发 NFT 市场。与 StarkWare 合作的分布式自动做市商也受到了嘲笑。

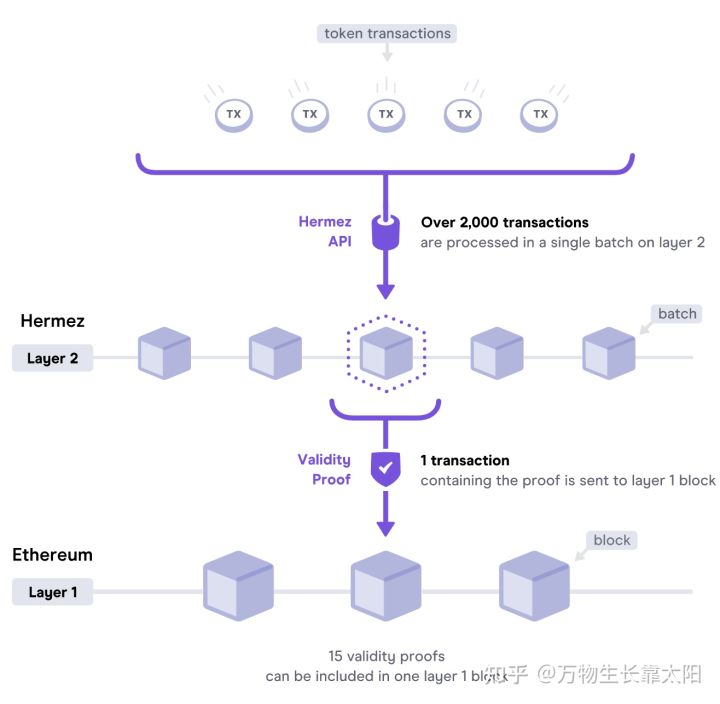
*多边形赫梅兹*



2021 年 8 月，以太坊扩展协议 Polygon 宣布收购并与 Hermez 合并。Polygon 是一种用于构建和连接与以太坊兼容的区块链网络的协议和框架，目标是在以太坊上聚合可扩展的解决方案，从而支持多链以太坊生态系统。他们通过开发执行和数据可用性模块的功能，从本质上支持以太坊生态系统的模块化。

Hermez 本身是 Polygon 生态系统的一部分，是一个开源 ZK 汇总，针对安全、低成本的代币传输进行了优化，由以太坊网络提供保护。Hermez 表示，通过利用零知识技术，与以太坊主网相比，他们能够将吞吐量提高 133 倍，同时将代币转移成本降低 90% 以上。

下面是 Hermez 制作的直观图表，它概述了我们在本文中讨论的一般汇总概念，同时解释了如何在单个 Hermez 网络批次中处理 2,000 笔交易。



Hermez 是一个完全去中心化的网络，很像 StarkNet 和 zkSync 计划在他们的路线图中。这意味着它有一个原生代币 $HEZ，用于治理以及网络内的其他事情。$HEZ 代币可在包括 Uniswap v2 在内的 DEX 上使用。$HEZ YTD 的表现如下。然而，鉴于 Hermez 已被 Polygon 收购，Polygon 拥有现有的原生代币 $MATIC，目前尚不清楚 $HEZ 未来会发生什么。



**即将推出的汇总催化剂**

*EIP-4488*

这篇文章中的一个重要提及（如果你已经做到了这一点，我假设你对理解 ZK 汇总非常感兴趣！）是 EIP-4488 。对于那些不熟悉 EIP 的人，它们代表以太坊改进提案，是为以太坊指定潜在新功能或流程的标准。以太坊社区内的任何人都可以创建 EIP，但必须充分同意才能实施。

总而言之，EIP-4488 将 calldata 成本从每字节 16 gas 降低到 3 gas，并对每个块的 calldata 设置了上限以降低安全风险。从本质上讲，这意味着汇总开销成本降低，对于汇总的最终用户而言，这意味着费用更低。要更详细地了解 EIP-4488，请查看 proto.eth 在 Twitter 上的以下主题。



*分片*

汇总的另一个重要催化剂是分片。共享是模块化区块链上下文中需要理解的关键概念，本质上是解决以太坊数据可用性约束的方法。我将发布一篇纯粹关注分片的文章，作为关于区块链模块化的三部分系列的第二篇文章。但是，如果您迫不及待地想了解共享，我建议您查看[这篇](https://link.zhihu.com/?target=https%3A//notes.ethereum.org/%40vbuterin/data_sharding_roadmap)文章。

**结束语**

Rollup 无疑对区块链的未来至关重要，并且可以说是 dApp 的日常用户与区块链技术交互的网络。这些用户甚至可能不知道他们正在使用哪个汇总，就像在互联网上我们经常不知道网站使用哪种云托管服务一样。

这就是我对汇总感到非常兴奋的原因。我们仍处于其生命周期的早期，因此技术的复杂性和某些情况下缺少的功能。这意味着我们将能够观察它们的发展，甚至可以推测未来几个月和几年的各种汇总技术。

如果您想了解更多信息，或了解汇总的技术进展及其采用情况，我建议您在 Twitter 上关注这些人：

* [@likebeckett](https://link.zhihu.com/?target=https%3A//twitter.com/likebeckett)
* [@epolynya](https://link.zhihu.com/?target=https%3A//twitter.com/epolynya)
* [@SwagtimusP](https://link.zhihu.com/?target=https%3A//twitter.com/SwagtimusP)
* [@EliBenSasson](https://link.zhihu.com/?target=https%3A//twitter.com/EliBenSasson)
* [@l2beatcom](https://link.zhihu.com/?target=https%3A//twitter.com/l2beatcom)

当然，我会定期在 Medium 和我的 Twitter 帐户[@0xbenharvey](https://link.zhihu.com/?target=https%3A//twitter.com/benharvey_10)上提供内容。给我一个关注或订阅此时事通讯以保持最新状态。谢谢，两周后见。瓦格米。