Four Pillars：zkRollup中构建的项目及主要zkRollup用例详览

来源：Four Pillars；编译：白水，本站

## 摘要

2023 年，zkRollups 从研究阶段过渡到生产阶段，Starknet、zkSync、Scroll、Polygon zkEVM 和 Linea 等项目推出了各自的解决方案。

随着协处理器、证明器市场、共享证明器和 zk 聚合层等新概念的发展，zkRollup 生态系统变得更加高效和去中心化。

zkRollup 的运行涉及三个主要阶段：执行、证明生成和证明验证，各种项目都专注于优化 zkRollup 供应链中的每个组件。

zkSync、Starknet、Merlin 和 SNARKnado 等 zkRollups 正在开发其基础设施，但它们仍处于优化供应链的早期阶段。

2022 年，zkRollups 主要处于研究阶段。2023 年标志着它们未来的开始。许多项目，包括 Starknet、zkSync、Scroll、Polygon zkEVM 和 Linea，都将其Rollup投入产品。其好处显而易见，因为与Optimistic rollups总相比，它具有更短的最终确定时间、更安全的互操作性和更低的运营成本。尽管取得了这些进步，但与Optimistic rollups相比，zkRollups 仍处于实验阶段，其技术路线图经常发生变化。

那么，zkRollups 的未来会怎样？许多项目中经常出现诸如协处理器、证明器市场、共享证明器和 zk 聚合层等新术语。zkRollup 正在以不同的方式开发，在 zkRollup 生态系统中，正在构建许多组件以使 zkRollups 更高效、更去中心化。如果我们考虑 zkRollups 的运作方式，该过程涉及三个阶段：执行、执行的证明生成和证明验证。每个阶段都有相应的项目。简要总结一下：

执行：zkVM、协处理器

证明生成：证明市场、证明聚合器

证明验证：结算层

这些类别中的每一个都处于早期阶段，但随着这个供应链变得更加发达，zkRollup 生态系统将变得更加高效。在本文中，我们将首先探索 zk 的基础知识，然后深入研究 zkRollup 供应链中正在构建的项目，以及以太坊和比特币中的一些主要 zkRollup。

## 1. ZKP 和 zkRollup 基础知识

本文标题提到的 zkRollup 是一种使用零知识证明（ZKP）的 rollup 方法。如果你在区块链生态系统中遇到过零知识证明这个术语，那么你可能对它有所了解（如果没有，也不用担心；稍后会解释）。但是，如果问为什么以及如何将这项技术应用于 rollup，你可能会很难立即回答。

为了找到这个问题的答案，在本章中，我们将探讨什么是零知识证明和 zkRollup，它们如何运作，以及为什么 ZKP 技术非常适合 rollup。

### 1.1 什么是ZKP？

1.1.1 ZKP概述

在深入研究 ZKP 的细节之前，让我们先了解一下这个过程所涉及的组件。主要有两个组件：

证明者：证明者持有他们想要在 ZKP 过程中向验证者证明的陈述。

验证者：验证者参与 ZKP 过程，根据提供的证据确定证明者的陈述是否真实。

现在，让我们详细探讨一下 ZKP。ZKP 是一种加密技术，其中证明者可以证明特定事实，而无需透露事实本身或任何相关信息。ZKP 具有三个主要特征：完整性、可靠性和零知识：

完整性：如果证明者的陈述是真实的，则验证者将确信该陈述是真实的。

可靠性：如果证明者的陈述是错误的，则证明者无法欺骗验证者相信它是真实的。

零知识：在证明过程中，验证者除了陈述的真实性或虚假性之外，不会获得任何其他信息。

1.1.2 ZKP示例

单看定义可能不太容易理解，我们用一个众所周知的例子“Ali Baba's Cave”（阿里巴巴的洞穴）来解释一下零知识证明。



考虑以下场景：在阿里巴巴的洞穴中，有两条路径 A 和 B，它们在洞穴深处汇合，但被一扇秘密的门挡住了。证明者 (P) 声称拥有通过这扇秘密门的钥匙，而验证者 (V) 想要验证 P 是否确实拥有钥匙。

验证过程遵循以下步骤：P 进入洞穴并选择路径 A 或 B。V 不知道 P 走了哪条路，但可以要求 P 通过特定的路径出来。如果 P 有钥匙，P 可以从任何路径出来。在重复此过程几次后，V 可以确信 P 拥有钥匙。但是，V 不会了解有关钥匙形状或性质的任何信息。

将其应用于零知识证明的特征：

完整性：如果 P 在多次重复中始终遵循 V 的指示，V 可以确信 P 拥有钥匙。

可靠性：如果 P 实际上没有钥匙，但对此撒谎，那么不可避免地会出现 P 无法遵循 V 的指示的情况，从而证明 P 的说法是错误的。

零知识：V 通过多次迭代确信 P 拥有钥匙，但对钥匙的外观或属性一无所知。

### 1.2 那么 Rollup 和 zkRollup 是什么？

到目前为止，我们已经探索了零知识证明的 A 到 Z。但是，必须记住的是，本文的重点是 zkRollups。现在，让我们深入了解什么是 rollups 和 zkRollups。

1.2.1 Rollup 快速概览

Rollup 是一种 Layer 2 扩展解决方案，它处理 Layer 2 区块链上的交易，然后将Rollup状态发布到 Layer 1 区块链进行记录和管理。

之前曾有过许多解决以太坊扩展性问题的提案。最早的是分片，即将以太坊网络划分为几个较小的“分片”，以显著提高交易吞吐量。与多台计算机同时处理任务的方式类似，分片使以太坊网络能够快速高效地处理更多交易。

尽管有诸多好处，但以太坊的开发人员由于担心潜在的中心化和技术挑战而放弃了直接分片，从而导致延迟。相反，他们采用了通过 Layer 2 解决方案进行间接分片的方法。在这种方法中，将交易数据批量传输到 Layer 1 的过程称为 rollup。目前，Optimistic Rollup 和 zkRollups 是引领该生态系统的两种主要类型。

1.2.2 为什么 ZK Proof 与 Rollup 是绝配

zkRollups 与 Optimistic rollups 的不同之处在于，它使用有效性证明而不是欺诈证明。zkRollups 使用 zk-SNARK 或 zk-STARK 将大量交易压缩为单个小证明，并在 Layer 1 区块链上记录和验证。与 Optimistic rollups 不同，这种方法显著提高了处理速度和效率，并且不需要为错误结果设置争议期。

零知识证明的非交互式特性对于 zkRollups 的效率和便利性至关重要。它允许 rollups 独立管理 rollup 过程，通过根据自己的时间表将交易数据捆绑并发送到 Layer 1 来最大限度地提高效率。这种非交互式方法可以防止 Layer 1 和 rollup 之间更具交互性的过程可能产生的潜在延迟和低效率。

简洁性是 zkRollups 有效性的另一个关键因素。 zk-SNARKs 和 zk-STARKs 能够将大量数据压缩为小的证明，这确保了在将交易数据发送到更昂贵但更安全的 Layer 1 时的经济效率。这种压缩能力使 zkRollups 能够将多笔交易作为单个批次处理，大大增强了 Layer 1 的可扩展性，同时为用户在 rollup 环境中提供了更具成本效益的区块链基础设施。

1.2.3 zkRollup 的运行

让我们进一步探索 zkRollup 的运作方式以及涉及哪些组件。zkRollup 主要由两个组件操作：

Sequencer：sequencer 收集和处理第 2 层发生的交易，并将处理结果提交给第 1 层。虽然一些 rollup 项目有独立的实体来排序和生成有效性证明，但为了简单起见，我们在这里将它们视为组合角色。

Rollup Contract：rollup contract 是第 1 层上的智能合约，用于确定 rollup 的状态和交易。它接收、存储和验证由序列器提交的数据，确保在数据被验证后进行适当的存储和管理。

zkRollup 的运作流程如下：



[Sequencer <> L2] 交易批处理和状态变化计算：将 Layer 2 上执行的多笔交易汇总为一个批次，执行批次中的每一笔交易，并生成记录新状态变化的状态根。

[Sequencer <> L2] 有效性证明生成：使用新的状态根生成有效性证明来证明状态根的正确性。此证明保证批次内的所有交易均已正确执行，而不会泄露每笔交易的详细信息。

[Sequencer <> L2] 状态根和有效性证明的提交：生成的有效性证明、状态根和隐藏的交易数据提交给 Layer 1 Rollup 合约。Rollup 合约对提交的数据进行验证。

[Sequencer <> Rollup Contract (L1)] 验证和更新：Layer 1 Rollup 合约从序列器接收有效性证明、状态根和验证交易数据。它验证数据，更新状态根，如果没有问题，则存储验证交易数据。如果发现问题，则不会执行验证和存储过程。

## 2. zkRollup 供应链概况

从鸟瞰视角来看，我们来看看 zkRollups 的整个供应链是如何运作的。zkRollups 涉及三个主要过程：执行、证明生成和验证。

执行：这发生在链下，交易在单独的 rollup 网络上分批执行，从而更新 rollup 状态。

证明生成：编译交易批次和状态根等输入。证明路线处理交易，生成简洁的 zk 证明，以加密方式证明状态转换的有效性，而无需透露数据。

证明验证：zk 证明和相关数据提交给结算层（主要是以太坊）上的验证者合约进行验证。如果有效，rollup 合约将更新其状态以反映新的后状态，并在短暂的时间缓冲后完成更改。

有专门针对每个流程的项目，以使 zkRollups 更有效地运行。在下一节中，让我们深入了解每个流程的内容以及哪些项目正在处理它们。



### 2.1 执行 - 在 ZK 路线中执行

执行与结算层是分开进行的，计算在单独的机器上进行，执行的证明在zk路线中生成。这个执行环境可以分为两个部分：zkVM和Co-Processor。

2.1.1 zkVM



来源：Foresight Ventures：zk、zkVM、zkEVM 及其未来 | 作者：Foresight Ventures | Medium

zkVM（零知识虚拟机）是一种专门的虚拟机，旨在执行计算并生成零知识证明，以验证这些计算的正确性，而无需透露底层数据。zkVM 有几种类型，每种类型都针对特定的虚拟机和编程语言量身定制。以下是这些项目的一些分类：

zkEVM：它旨在复制 EVM 环境，同时结合零知识证明功能。这允许现有的以太坊智能合约和 dApp 无缝移植到基于 zkEVM 的Rollup。然而，由于为 EVM 开发 zk 路线的复杂性及其频繁升级，纯 EVM 存在兼容性问题。

基于 RISC-V 和 MIPS 的通用 zkVM：zkRISC 是 RISC Zero 开发的 zkVM 的特定实现。它被设计为一个通用的 zkVM，能够执行任意计算并生成零知识证明。它允许部署 C、Python 和 Rust 等编程语言并生成执行证明。

CairoVM：Cairo VM 旨在优化程序执行有效性证明的生成。与专注于使 EVM 与有效性Rollup兼容的 zkEVM 解决方案不同，Cairo VM 从一开始就设计为最大限度地提高 STARK 证明的效率。这种方法可以实现更好的性能和可扩展性，而不受 EVM 限制的限制。但是，由于开发人员需要学习一门新语言，因此构建 dapp 存在障碍。

2.1.2 协处理器



来源：Phala 的 2024 年路径：区块链的协处理器——AI、Hooks 和 DePin

协处理器是作为链下处理器开发的，用于协助特定计算。例如，图形处理单元 (GPU) 管理 3D 渲染所需的大量并行计算，使中央 CPU 能够专注于通用处理。从这个意义上讲，协处理器支持区块链进行复杂的执行，这在区块链上成本高昂。每种类型的协处理器都旨在最大限度地提高处理其专门工作负载的效率。

通过利用 ZKP，协处理器可以实现无需信任且可验证的链下计算，确保结果的正确性和完整性，而不会泄露敏感数据。一些已知的项目包括：

Axiom：Axiom 正在开发一个“ZK 协处理器”系统，该系统允许智能合约查询历史区块链数据并在链下执行复杂的计算，同时通过 ZKP 保持数据隐私和完整性。

Phat Contracts（Phala 网络）：Phat Contracts 是一种协同处理器，可增强可扩展性、实现无 gas 体验、支持多链功能并为 dApp 提供对链下数据的安全访问。

### 2.2 证明生成——产生零知识证明

为了证明状态转换的有效性，rollup 运算符（证明者）生成 ZKP。此证明确认新状态根是从先前状态正确计算出来的。由于生成 ZKP 需要大量计算资源，因此证明生成过程存在限制，尤其是对于大型交易批次或复杂的智能合约。这可能会限制 zkRollups 的吞吐量以及它们可以有效支持的应用程序类型。

此外，由于生成 zk 证明的实体需要该领域的专业知识，并且需要保持硬件最新，因此管理成本可能很高，更不用说集中化风险了。因此，该领域已经取得了一些进展，以使其更加高效。该方法分为两部分：建立证明生成市场以外包生成过程，并创建聚合层以使其更具成本效益。

2.2.1 证明生成市场



来源：Gevulot 介绍 | Gevulot

证明市场提供的关键功能包括去中心化证明生成、拍卖机制以及硬件利用率和成本效率。应用程序向网络提交证明请求，证明者使用证明生成硬件进行响应，确保有效处理证明请求。拍卖机制将这些请求与证明者进行匹配，从而实现有竞争力的证明定价。此外，证明者使用专用硬件，降低了证明成本，去中心化市场允许聚合不同应用程序的证明请求，从而提高硬件利用率和成本效益。

证明市场还确保了审查阻力和快速终结性，并实施了质押机制。市场保证了短期审查阻力，因此证明者的出价不会被不公平地阻止或忽略。证明者需要与网络进行质押，以防止恶意活动并确保网络的可靠性和完整性。

最后，市场利用规模经济。大规模协调 ZKP 生成可降低最终用户的成本。聚合证明订单流使证明者能够投资和运营更高效的基础设施。由于可以聚合证明以进行优化，因此应用程序还可以从降低的链上验证成本中受益。一些项目包括：

Succinct Network：Succinct Labs 正在开发一个去中心化的证明者市场，作为其 Succinct Network 的一部分，旨在为 ZKP 创建统一协议。这个市场将允许应用程序将其证明生成外包给专门的证明者网络，为基于 ZKP 的系统提供更高效、更具成本效益的解决方案。证明者市场将通过拍卖机制运作，该机制将应用程序的证明请求与一组不同的证明者进行匹配。

=nil; Foundation：=nil; Foundation 已经开发了一个证明市场，这是一个去中心化的分布式系统，旨在作为 ZKP 的现货市场。这个市场允许证明请求者（例如应用程序）将 zkProof 的生成外包给专门的证明生产者。证明市场在 =nil; Foundation 的数据库管理系统之上运行，功能更像是“Proof DEX”，而不是中心化服务。

Gevulot：Gevulot 不是传统的证明者市场，而是模块化堆栈的去中心化证明层。它是一个无需许可且可编程的第 1 层区块链，专门设计用于将证明系统部署为链上程序。与典型的证明者市场不同，Gevulot 允许用户直接在区块链上部署证明者和验证者程序，类似于在以太坊上部署智能合约。这种方法使应用程序能够从去中心化证明中受益，而无需引导其证明者网络或依赖中心化解决方案。

2.2.2 证明聚合



资料来源：证明它：共享证明器、证明聚合和证明器市场 - Delphi Digital

ZKP 聚合是一种将多个 ZKP 合并为一个证明的技术，可降低在链上验证这些证明的总体成本。这对于严重依赖 ZKP 的Rollup尤其有益。一些值得注意的项目包括：

Polygon AggLayer：它旨在通过利用聚合 ZKP 和统一桥接合约 (LxLy Bridge) 实现 Polygon 生态系统中 L2 解决方案之间的顺畅互操作性。聚合证明可确保依赖链状态和捆绑包一致，防止无效Rollup状态在以太坊上结算（如果它依赖于另一条链的无效状态）。

Nebra：其产品通用证明聚合 (UPA) 是用于聚合 ZKP 的协议。Nebra 的 UPA 可以聚合来自不同路线、证明系统和各方的证明，从而将链上验证的 gas 成本降低 10 倍以上。 Nebra 与 AltLayer 等项目合作，将 UPA 集成到他们的Rollup解决方案中，使 AltLayer 的用户和 dApp 能够从大幅降低成本中受益。

Electron Labs：Electron Labs 开发了 Quantum，这是一个聚合层，它利用 zk-recursion 将来自不同协议和各种证明方案的证明聚合成一个“超级证明”。然后在以太坊上验证这个超级证明，分摊多个协议的验证成本，并为单个协议提供更便宜的验证。

### 2.3 证明验证

zkRollups 中的证明生成过程计算量很大。但是，在以太坊主网上验证这些证明相对轻量，在保持底层区块链的安全保障的同时实现了可扩展性。

以太坊中的 zk 验证智能合约使用高效的加密算法来验证有效性证明。如果证明有效，则提议的状态转换是正确的，并且新的状态根被接受，从而更新主网上的 rollup 状态。一些项目（如 Aligned Layer）通过利用以太坊中的验证器提供更快、更便宜的验证。

2.3.1 对齐层



资料来源：whitepaper.alignedlayer.com

Aligned Layer 是专为以太坊设计的去中心化 ZKP 验证和聚合层。作为 EigenLayer 主动验证服务 (AVS)，它通过名为“再质押”的过程利用以太坊的经济安全性，确保 ZKP 在以太坊区块链上得到准确验证和结算。

Aligned Layer 提供两种不同的操作模式来满足不同的需求。快速模式针对最低验证成本和低延迟进行了优化，使其成为需要快速且经济高效的证明验证的应用程序的理想选择。另一方面，慢速模式利用证明聚合来充分利用以太坊的安全保障，从而提供全面的安全性。这种双模式方法使 Aligned Layer 能够提供灵活的解决方案，可根据不同用例的特定要求在速度和安全性之间取得平衡。

## 3. zkRollups 分析

如第 2 节所述，各种项目都在优化 zkRollup 供应链。让我们仔细看看生产中最值得注意的 zkRollup 项目，特别是与 EVM 兼容的项目 zkSync 和 Starknet，以及与比特币兼容的项目 Merlin Chain 和 SNARKnado。

### 3.1 zkSync

zkSync 是 Matter Labs 开发的 zkRollup 解决方案，旨在解决以太坊网络面临的可扩展性挑战。虽然 zkSync 最初的重点是扩展以太坊，但它的野心远不止于成为 L2 解决方案。Matter Labs 将 zkSync 设想为全面跨链生态系统的基础，旨在无缝连接各种基于 zkSync 的汇总。为了实现这一目标，zkSync 正在开发一个复杂但用户友好的跨链环境，其中包含 zkRollup 技术、ZK Chain 和 Hyperbridge。让我们来看看每个概念。

### 3.1.1 zkRollup——经济效率优化

zkSync 采用基于 zk-SNARK 的 zkRollup 技术，zk-SNARK 的证明生成和验证方法，证明体积小，验证速度快。但随着 zk-STARK 的量子抗性、大规模处理等优势凸显，zkSync 也在尝试部分采用 zk-STARK，比如名为“Boojum”的证明生成系统，就采用 zk-STARK 方法进行证明生成。

3.1.2 结构部件

Sequencer：zkSync 中的 Sequencer 按照特定的规则对交易进行排列和处理。Sequencer 包括 Prover，Prover 生成无法详细查看的证明和交易数据并发送到 Layer 1。

Prover：zkSync 中的 Prover 使用 zk-SNARK 生成证明，证明生成过程中使用的数据包括无法详细查看的交易数据和代表 L2 链状态变化的前后状态变化数据。生成的证明由 Layer 1 上的 Rollup 合约进行验证。

Settlement：zkSync 使用 Layer 2 上生成的数据进行验证，并在 Layer 1 智能合约中进行更新。如果出现验证问题，则受影响批次中的交易不会更新。这个过程是模块化的，下面将介绍每个 ZK Chain 连接一个或多个智能合约。

3.1.3 ZK Chain



ZK Chain 是一条超越 Layer 2 的区块链，包含了 zkSync 提供的基础设施。之所以被称为超越 Layer 2，是因为 zkSync 采用了不受限制的分层结构，包括 L3 之类的分形结构。

目前最知名的 ZK Chain 是由 zkSync 构建的 zkSync Era。它兼容 EVM，允许部署简单的 dapp。然而，对于 zkSync 最终的跨链生态系统目标而言，不同 ZK Chain 之间的关系至关重要。zkSync 专注于如何与其他未来的 ZK Chain 连接。

利用 ZK Chain 环境的一个例子是 Hyperbridge。通过 Hyperbridge，用户可以方便地将来自连接链的所有资产发送到他们链特定的钱包中。当用户需要使用他们链上的资产时，中继器会促进资产的桥接、销毁和发行。



例如，如果使用跨链 Uniswap，并且 era.zksync 链上的用户想要将 1 ETH 兑换为 10,000 DAI，则流程如下：

从 era.zksync 链钱包生成“1 ETH → 10,000 DAI”交易。

中继器将 1 ETH 转移到 uni.chain，将其兑换为 10,000 DAI。

然后，中继器将交换后的 10,000 DAI 转移回 era.zksync 链。

这样，用户可以轻松使用 zkSync 的环境执行跨链交易，而无需了解有关其他链的详细信息。

3.1.4 EVM兼容性

zkSync 目前声称与 Solidity 和 Vyper 的兼容性达到 99%。最初，zkSync 支持类似于 Rust 的语言 Zinc，以实现更合适、更高效的 zkEVM。然而，他们将重点转移到 Solidity 兼容性上，自 2021 年 9 月起停止了 Zinc 的开发，以确保全面优化。

### 3.2 Starknet

Starknet 与 zkSync 类似，都是基于 zkRollup 的第 2 层解决方案，但其技术堆栈和内部技术有所不同。值得注意的是，它使用 zk-STARK 而不是 zk-SNARK，并使用自己的智能合约语言 Cairo。

3.2.1 zk Rollup - 专注于高容量 Rollup 处理

Starknet 使用 zk-STARK 生成和验证与 Rollup 相关的证明。与 zkSync 类似，它仅使用前后状态变化来更有效地在第 1 层管理 Rollup 数据。

此外，由于 Starknet 采用 zk-STARK，它受益于无信任环境和同时处理大量交易的能力。这使得 Starknet 成为交易量大的 DeFi dApp 或游戏 dApp 的首选。

3.2.2 结构特点

从结构上看，Starknet 采用与其他 zkRollup 类似的架构。但它的不同之处在于积极利用 zk-STARK 零知识证明模型，并通过其专有编程语言 Cairo 保持 EVM 兼容性。



来源：Starknet 架构：概述

Sequencer：Starknet 中的 Sequencer 在管理交易的验证和执行以及提议区块方面起着至关重要的作用。它的主要功能是批量处理交易。未通过验证的交易受到 Sequencer 的限制，只有经过验证的交易才会被纳入区块。Sequencer 还包括一个证明者，负责将完成的 rollup 数据发送到 Layer 1。

证明者：Starknet 中的证明者使用 zk-STARK 生成证明。在证明生成过程中，证明者保存每个交易执行步骤以创建 Execution Trace 并跟踪 L2 链中的状态变化，记录 State Diff。证明生成过程需要大量的计算资源，并设计为支持并行处理，允许多个证明者分工并同时执行任务。

结算：Layer 2 上生成的数据传输到 Layer 1（例如以太坊），其中组件接受交易并管理证明和状态差异。这些组件由两个智能合约处理：验证者合约和 Starknet 核心合约。验证者合约会分析从第 2 层收到的证明，如果发现任何问题，则对交易行使否决权。如果证明的有效性得到确认，则将其转移到 Starknet 核心合约，该合约使用提供的状态更改更新第 1 层链。此更新状态将添加到第 1 层链块中，一旦该块通过第 1 层的流程，它就会受到第 1 层的影响。

3.2.3 EVM 兼容性

Starknet 正在通过 Cairo 语言开发自己独特的 EVM 兼容性路径。要在 Starknet 上部署智能合约，必须使用 Cairo。虽然 Cairo 尚不支持许多 Solidity 功能，尽管 Cairo 开发人员的数量正在增加，但在社区规模和采用率方面仍落后于 Solidity。

Starknet 的智能合约语言 Cairo 继承了 Rust 的功能。它针对 zk-STARK 证明生成进行了优化，可以高效地执行和生成智能合约的证明。克服使用 Cairo 的障碍可以在更好的环境中部署和执行智能合约，并将数据安全地汇总到第 1 层。

下表概述了 Cairo 和 Solidity 之间的主要区别。



### 3.3 Merlin Chain

Merlin Chain 是 Bitmap Tech 开发的基于比特币的第 2 层 zkRollup 解决方案，该公司主要专注于以太坊。Merlin Chain 基于 Polygon 的零知识证明技术，具有与 EVM 兼容的优势，同时将Rollup数据安全地存储到比特币 L1。通过这种方式，Merlin Chain 旨在提高流动性并扩大比特币网络内的生态系统，包括 BTC，其口号是“让比特币再次变得有趣”。

3.3.1 zkRollup - 针对比特币特性的混合方法

Merlin Chain 使用结合了 zk-SNARK 和 zk-STARK 的 zkRollup 技术。最初，由于比特币网络的结构特性为图灵不完备，无法在比特币网络上直接验证 ZKP。然而，在 Taproot 升级后，部分验证变得可行。Merlin Chain 利用 Taproot 将链下生成的Rollup数据和证明数据记录到比特币网络上。



在 Merlin Chain 中，zkProver 负责验证交易数据的有效性，并根据验证的数据生成证明。这个过程的阶段如下：

Merlin Chain 的序列节点将当前状态信息存储在数据库中。

序列节点将交易发送给 zkProver。

zkProver 访问数据库以检索交易验证所需的数据。

一旦 zkProver 完成交易验证，它就会生成证明并将其发送给序列节点。

该过程涉及几个步骤。首先，使用 Polygon zkEVM 团队开发的基于 zk 汇编语言 (zkASM) 的 zkEVM 验证和处理交易。然后使用 zk-STARK 的高容量处理能力聚合生成的数据并进行压缩以优化Rollup经济效率。最后，使用 zk-SNARK 生成产生一致证明大小的证明。然后在去中心化的 Merlin Chain 预言机网络环境中验证生成的数据和证明，并通过 Taproot 上传到比特币网络。

3.3.3 未来升级：链上欺诈证明

虽然 zkRollup 似乎可以很好地应用于以太坊生态系统的 L2 解决方案（如第 3.2.1 节所述），但它本身无法完美保证 rollup 内交易的有效性和准确性。为了弥合比特币网络结构差异造成的差距，Merlin Chain 独特地计划引入类似于 optimistic rollup 的链上防欺诈机制。

链上防欺诈机制在 rollup 数据提议者和挑战者的关系中运作。如果挑战者认为 rollup 数据不正确，他们可以挑战上传到比特币网络的交易数据、ZK 状态信息和 ZK 证明。大多数 L2 交易不需要在比特币网络（L1）上重新验证，但如果对先前提出的 rollup 数据提出挑战，则必须重新执行和验证数据和交易。如果发现某个角色有过错，他们将受到惩罚。

3.3.4 EVM 兼容性

Merlin Chain 通过在其 zkProver 中使用基于 zkASM 的 zkEVM 实现 EVM 兼容性。这使得使用现有以太坊开发工具和基础设施开发的智能合约可以在比特币网络上执行，从而提供了将以太坊的功能扩展到比特币的优势。

### 3.4 SNARKnado

SNARKnado 是 Alpen Labs 使用 zk-SNARK 实现的基于比特币的第 2 层解决方案。Alpen Labs 旨在利用 SNARKnado 使区块链更专注于验证而不是计算，从而在比特币生态系统中实现更高的可扩展性和效率。

3.4.1 zkRollup - BitVM 的继任者

SNARKnado 是一种经过修改的模型，它针对 zk-SNARK 进行了进一步优化，该模型借鉴了 BitVM Optimism方法中使用的证明者-挑战者结构。与 BitVM 相比，这使其性能提高了约八倍。但是，它仍然没有达到 BitVM2 允许任何人发起挑战的优势，因为 SNARKnado 目前将挑战能力限制在允许的角色中。

3.4.2 结构特点

证明验证方法 - 二分多项式

使用 zk-SNARK 允许 SNARKnado 以较小的证明大小管理比特币上的Rollup数据和证明数据，但比特币对复杂计算的限制需要对证明验证进行优化。SNARKnado 通过使用二分多项式转换证明数据来解决此问题。验证过程通过 Taproot 升级启用的链上计算进行。

当证明者收到挑战时，他们会披露挑战所需的一些数据，并与挑战者一起进行验证过程。二分多项式方法用于验证，确定哪个角色（证明者或挑战者）有错。

3.4.3 SNARKnado 与 BitVM 或 BitVM2

SNARKnado 与 BitVM 有许多相似之处，特别是作为 BitVM 和 BitVM2 之间的中点出现。那么，它们之间有什么区别呢？（由于 BitVM2 是比 BitVM 更先进的模型，因此比较将主要集中在 BitVM2 上。）

首先，考虑比特币内部资源的使用情况。BitVM2 固有地显示链上资源使用量的线性增加，而 SNARKnado 将这种增加降低到平方根级别，从而优化链上资源使用量。另一个区别在于能够发出挑战的角色的可访问性。虽然 SNARKnado 将挑战限制在允许的角色中，但 BitVM2 允许任何人在未经许可的情况下发出挑战。

3.4.4 EVM 兼容性

根据 Alpen Labs 的最新记录，EVM 兼容性尚未得到官方支持，目前也没有任何关于 EVM 兼容性的未来计划。

## 4. 展望未来

回顾最近推出的 zkRollups 主网，我们看到了 2023 年 8 月推出的 zkSync Era 和 2023 年 12 月推出的 Polygon zkEVM。这些项目推出的时间并不长，因此大多数项目仍在积极开发中。此外，开发范围已不仅限于 zkEVM。通用 zkVM、zkWasm 和链下协处理器也在执行部分开发中，其中使用自定义 zk 路线。

随着基本执行和证明生成变得更加可靠，人们正在努力提高供应链效率。策略包括建立证明者市场、聚合多个证明以及创建验证层以进行经济高效的验证。预计未来 zkRollups 的供应链将变得更加高效和实惠。