协处理器：关键用例和值得关注的协处理器项目

作者：Darshan Gandhi，FutureX Labs创始人；翻译：本站xiaozou

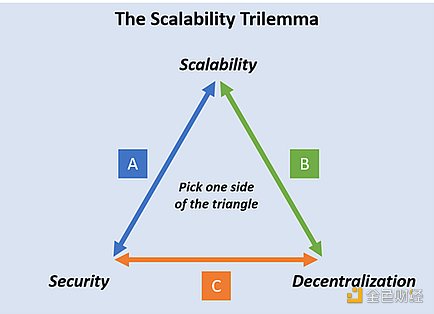
区块链经历重大的发展变化，已成为金融服务和供应链管理等各领域的核心技术。通过提高交易的安全性、透明度和效率，以及dApp和智能合约的创建，区块链解决了信任、防欺诈和数据不可篡改等方面的重大问题。

尽管取得了这些进步，但许多Layer 1区块链还面临着扩容挑战。高需求往往导致：

网络拥塞

交易时间较慢

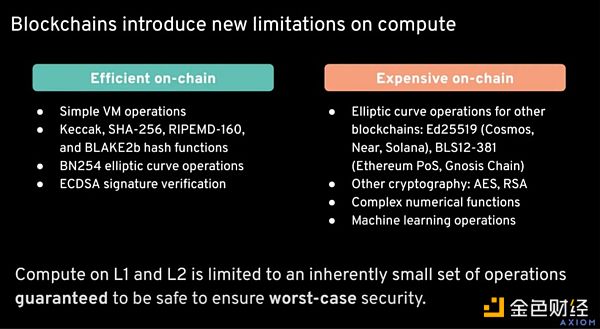
成本提高



Layer 2解决方案和分片（sharding）正在致力于解决这些问题。然而，随着消耗的增长，对更快速、更高效的交易处理的需求变得至关重要。

这就是“协处理器”（coprocessor）的用武之地。

协处理器是一种专用硬件，能够比通用CPU更高效地处理特定任务。协处理器通过与主处理器（本文中的L1或L2）一起工作来执行高要求任务，如加密操作和复杂计算，从而提供一种前景光明的解决方案。这有助于“卸载”主链上的负载，提高整体性能和吞吐量。



本文，我们将深入探讨协处理器生态，了解：

什么是协处理器

它们是如何工作的

为什么需要它们

用例及帮助解决的特定问题

值得关注的协处理器项目

本文主要焦点将放在零知识（ZK）协处理器上，因为它们是目前可用的最先进的协处理器。让我们开始吧！

## 1、什么是协处理器？

协处理器是专门用于与主CPU共同处理特定任务的硬件，可提高效率和性能。

协处理器的概念起源于计算机体系结构，目的是提高传统计算机的性能。最初，计算机是完全依赖于CPU的，但随着任务变得越来越复杂，CPU力所不及。于是，为了解决这个问题，推出了GPU等协处理器来处理特定的任务，例如：

图形渲染

加密

信号处理

科学计算

协处理器示例包括用于图形渲染的GPU、加密加速器和数学协处理器。通过在CPU和这些专用单元之间划分任务，计算机实现了显著的性能改进，使它们能够高效地处理更复杂的工作负载。



在区块链的背景下，协处理器帮助管理链下复杂任务，通过可验证计算确保透明度和信任。它们利用zk-SNARKs、MPC（多方计算）和TEE（可信执行环境）等技术来增强安全性和可扩展性。

## 2、为什么需要协处理器？

协处理器提供了几个好处，特别是对于像以太坊这样面临着扩容问题的链。好处包括：

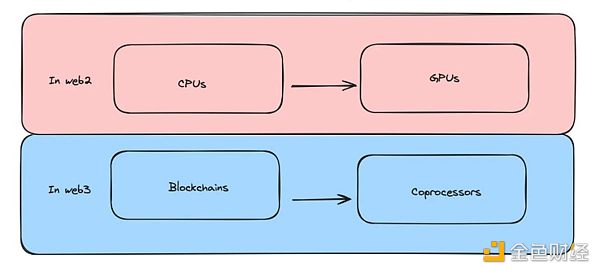
增强的可扩展性

无gas交易

多链支撑

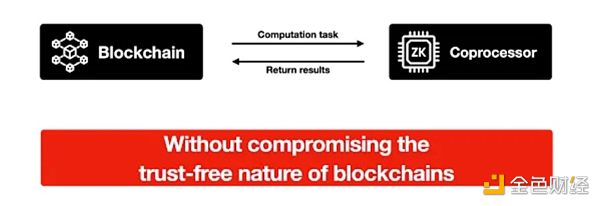
为了更好地理解这一点，我们来看一个比喻：

web3中的区块链可以比作web2中的CPU，而协处理器可以比作处理大量数据和复杂计算逻辑的GPU。



## 3、用例及帮助解决的问题

区块链的一个重要问题是链上计算的高成本。虽然archival nodes（归档节点）存储历史数据，但对于智能合约来说，访问这些数据既昂贵又复杂。例如，EVM可以很容易地访问最新的区块数据，但很难访问较老的数据。



区块链机器专注于安全地执行智能合约代码，而不是处理大数据或计算繁重的任务。因此，链下计算或扩容技术是必要的。

协处理器通过利用ZK技术来增强可扩展性，为这些挑战提供解决方案。具体如下：

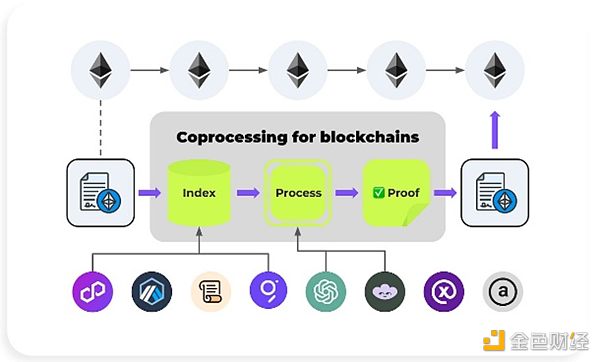
高效的大规模计算：ZK协处理器在维护区块链安全的同时处理大规模计算。

历史数据访问授权：它们允许智能合约使用零知识证明来授权历史数据访问和链下计算，然后将结果带到链上。

优化的可扩展性和效率：这种分离在不损害安全性的情况下提高了可扩展性和效率。

通过采用这种新设计，协处理器可以帮助应用程序访问更多数据并在更大范围内运行，而无需支付高昂的gas费。

那么，这些服务是如何工作的呢？下面是一个非常好的信息图可以让你更好地理解。



## 4、协处理器类型及其与rollup的比较

在将协处理器与其他技术进行比较时，必须要考虑到计算所需的安全模型和保证级别（assurance level）。

ZK协处理器

ZK协处理器是需要最大安全性和最小信任的敏感计算的理想选择。他们使用零知识证明来确保可验证的结果，而不依赖于操作员。然而，这是以牺牲效率和灵活性为代价的。

多方计算（MPC）和可信硬件

对于分析或风险建模等敏感度不高的任务，MPC和可信硬件是更有效的选择。这些方法虽然提供较少的安全保证，但却支持更广泛的计算。

FHE协处理器

基于FHE的协处理器，如Fhenix与EigenLayer合作开发的协处理器，在机密计算方面提供了重大改进。这些协处理器在卸载计算任务的同时保持了数据机密性。

这些技术该选哪一种取决于应用程序的风险承受能力和特定需求。

协处理器vs. rollup

另外还经常在协处理器和rollup之间进行比较：

Rollup专注于通过聚合交易和维护主链的状态来提高交易吞吐量并降低费用。这使得它们更适合高频交易。

另一方面，协处理器则独立处理复杂的逻辑和更大的数据量。它们是跨多个区块链和rollup的高级金融模型和大数据分析的理想选择。

## 5、用例和应用程序

协处理器本质上是高度模块化的，可以用于各种各样的应用。让我们来探索一些目前正在构建或可以构建的有趣用例：

DeFi项目中的复杂计算

协处理器可以处理DeFi项目中的复杂计算，支持实时适应的复杂财务模型和策略。它们卸载了主链的繁重计算，确保了效率和可扩展性，这对于优化交易策略和高频交易至关重要。

全链游戏

协处理器可以卸载EVM的复杂功能，实现更丰富的游戏机制和状态更新。它们可以支持高级游戏逻辑和AI驱动的功能，创造出比Web2游戏更具沉浸感和吸引力的游戏玩法。

永续合约和期权

协处理器为去中心化交易提供了透明和可验证的保证金逻辑，增强了衍生品平台的可靠性。他们在提供复杂的交易策略和风险管理实践的同时确保了隐私和信任。

智能合约的数据增强

协处理器可以提供数据捕获、计算和验证服务，使智能合约能够处理大量历史数据。这有助于实现更高级的业务逻辑和运营效率，增强智能合约的可靠性。

DAO和治理

协处理器可以卸载繁重的计算，以减少DAO操作的gas费用，简化治理过程和决策过程。这提高了DAO操作的效率和透明度，为社区驱动的项目提供支持。

ZKML

协处理器可以通过可验证链下计算支持链上机器学习应用程序，使用历史数据进行安全和风险管理。这种集成为区块链应用程序的高级分析和智能决策开辟了新的可能性。

KYC

协处理器可以获取链下数据并为智能合约创建可验证证明，在确保合规性的同时维护用户隐私。这使得Web3中的KYC流程更加安全、私密和高效。

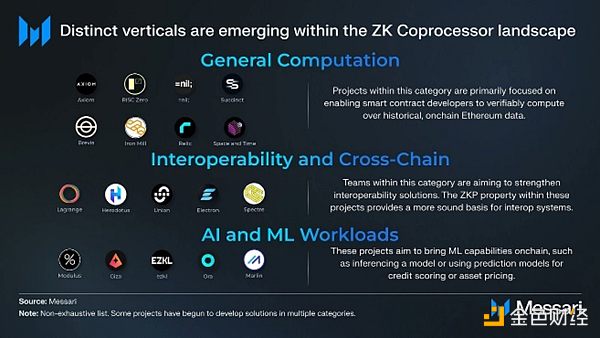
社交和身份验证应用程序

协处理器可以使用零知识证明来验证数字身份和历史行为，但不会泄露钱包地址。这增强了社交和身份验证应用程序的隐私性和可信度，实现了资质和活动的安全证明。

由于协处理器所提供的灵活性，应用程序几乎是无穷无尽的。上面是一些令人兴奋的例子，其中一些团队已开始着手构建创新项目。

## 6、谁在创建协处理器？

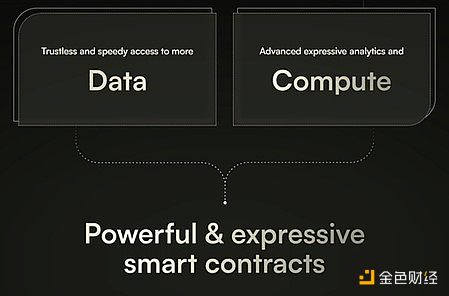
那么，下一个问题是：真正创建这些协处理器的团队都有哪些？



Axiom

Axiom是以太坊ZK协处理器，提供可以安全且可验证的方式访问所有链上数据的智能合约。它使用零知识证明从区块头、状态、交易和收据中读取数据，并执行分析和机器学习等计算。

通过为各任务结果生成ZK有效性证明，Axiom确保数据获取和计算的正确性，然后在链上进行验证。这种无需信任的验证过程为更可靠的dApp开发提供了空间。



RISC Zero

RISC Zero专注于区块链智能合约计算的可验证执行。开发人员可以使用Rust语言编写程序并将其部署在网络上，由零知识证明来确保每个程序执行的正确性。

像Bonsai和zkVM这样的组件也包括在内。Bonsai集成了RISC-V指令集架构的zkVM，为通用用例提供高性能证明。

Brevis

Brevis是一个ZK协处理器，它使去中心化应用程序能够以无需信任的方式跨多个区块链访问和计算数据。其架构如下：

zkFabric用于同步区块头

zkQueryNet用于处理数据查询

zkAggregatorRollup用于验证并向区块链提交证明。

Lagrange

Largrange是一个互操作性ZK协处理器协议，支持需要大规模数据计算和跨链互操作性的应用程序。其核心产品ZK Big Data处理并验证跨链数据，通过高度并行的协处理器生成ZK证明。

Lagrange包含一个可验证数据库、动态更新和智能合约的SQL查询功能。该协议支持复杂的跨链应用，并集成了EigenLayer、Mantle和LayerZero等平台。

## 7、AI协处理器

协处理器通过卸载复杂的计算，确保各种任务（如DeFi管理、个性化助理和安全数据处理）的效率、安全性和可扩展性来增强加密AI领域的应用程序。以下是针对不同用例和技术使用协处理器的一些值得关注的项目：

Phala Network

Phala Network将区块链与可信执行环境（TEE）整合在一起，以实现安全的AI交互。他们的Phat Contracts通过协处理器将复杂计算转移到Phala的网络上，这对于AI驱动的DeFi管理任务（如投资组合管理和收益管理）至关重要。

Phala的跨链互操作性使AI智能体能够实现跨链交易，保护隐私的计算同时可保护敏感数据的安全。

Ritual Network

Ritual正在使用Infernet开发首个社区所有的主权AI网络，这是一个去中心化oracle网络（DON），允许智能合约访问AI模型。

Ritual Network的战略伙伴关系凸显了其模块化本质：

EigenLayer：利用再质押机制增强经济安全性，防范潜在威胁。

Celestia：提供对Celestia可扩展数据可用层的访问，提高数据管理效率和整体可扩展性。

Modulus Labs

Modulus Labs专注于使用ZK协处理器将复杂的机器学习算法直接带到链上。他们的项目展示了各种可能的应用：

Rockybot：一款链上AI交易机器人，利用协处理器进行高频交易操作。

Leela vs The World：一款使用协处理器处理游戏内操作追踪的交互式AI游戏。

zkMon：使用零知识证明来验证AI生成艺术。

Giza

Giza是一个旨在简化使用零知识（ZK）证明的可验证机器学习模型的创建、管理和托管的平台。它允许开发人员将任何ML（机器学习）模型转换为可验证模型，确保ML执行的防篡改证明。

Giza为AI工程师提供了一个控制面板，可以轻松监控、调度和部署AI操作，并与不同的云提供商和ML库无缝集成。该平台还通过EVM verifier（验证者）支持协议集成，提高效率，促进收益增长和去中心化应用程序的采用。

EZKL

EZKL将zk-SNARKs与深度学习模型和计算图相集成，使用熟悉的库，如PyTorch或TensorFlow。它允许开发人员将这些模型导出为ONNX文件并生成zk-SNARK电路，通过在不泄露底层数据的情况下证明有关计算的声明来确保隐私和安全性。

这些证明可以在链上、浏览器中或设备上进行验证。EZKL支持各种应用程序，包括金融模型、游戏和数据证明，并提供Python、JavaScript及命令行接口工具，以简化链下计算，同时保持安全性。

## 8、协处理器的未来

总的来说，协处理器对区块链生态至关重要。我认为它们是区块链更快、更安全的“类固醇”。

协处理器对很多应用来说都将至关重要，包括：

开发无需信任和抗审查的AI应用程序

对大型数据集进行可验证的分析

提高加密领域AI驱动应用的可靠性和透明度

允许智能合约以更低的成本访问更多的数据和链下计算资源，而不会影响去中心化特性。

协处理器的潜在应用可能会彻底改变去中心化金融（DeFi）等领域，它们可以帮助维持Sushiswap和Uniswap等平台的竞争力。

然而，与任何技术一样，协处理器也一系列自身挑战，例如开发复杂性和高昂的硬件成本。

尽管存在这些挑战，但一些团队仍在不断努力解决这些问题。例如，Fhenix和EigenLayer之间的合作体现了增强计算任务和加速隐私链上交易发展的努力。这种合作对于克服现有障碍和释放协处理器在该领域的全部潜力至关重要。

## 9、结论

协处理器生态正在迅速发展，各种各样的项目都在为开发通用解决方案和专业应用做出贡献，例如Phala和Ritual为AI领域量身定制了一些解决方案。

随着这项技术的不断发展，我们预计将会出现新的用例和创新应用程序。协处理器的未来看起来充满光明，我们很高兴能够见证该领域的发展变化。