Unichain和Flare为何都引入可信执行环境？

作者：Haotian

最近，围绕 ZK 和可信执行环境（TEE）的差异性，有很广泛的讨论。原因是，新晋入局 layer2 的 @unichain 声称其毫秒级子区块是基于 TEE 构建，而号称数据区块链的预言机老链 @FlareNetworks 则集成 Google Cloud 等传统互联网渠道，通过 TEE 引入可验证的离链计算。结合这两件事，谈谈我的看法：

1）TEE（Trusted Execution Environment）是一种硬件级别的安全技术，简单而言，TEE 是在处理器中创建了一个独立、安全、隔离的 Enclave 飞地环境，与主操作系统程序完全隔离，可以安全存储和保护敏感数据，同时有严格的访问控制机制。

这意味着，开发者可以在 TEE 中执行特定程序，在确保安全的前提下，充分放大硬件的执行效率和性能。目前包括 Intel SGX ARM TrustZone 等有多种不同的 TEE 实现方式，其在移动互联网、物联网等领域有更广泛的应用，区块链场景下的应用正在被发掘。

2）Unichain 基于 TEE 环境，可以允许交易被预先执行和验证，让其发生在交易正式被打包出块前，这打破了原先交易统一上传 Mempool 等待打包的限制，又能有相对安全封闭的防篡改作恶环境，因此得以实现。

Flare Network 做预言机的思路也是借助 TEE 环境得以放大。做预言机数据区块链纯粹为 DeFi 合约环境喂价（Price 指标）会很卷，若把数据范围扩大到体育比赛结果、社交媒体数据、选举实时排名等等需要庞大的链下计算和处理能力，最终再把可验证结果传递到链上环境。

Flare 将通过 Google Cloud 提供的 TEE 环境，进行密集的计算操作，仅把可信的结果喂到链上，避免了庞大数据源在链上堆积产生较大的成本。其思路很简单：复杂的计算任务在链下执行，然后通过简短的证明在链上验证，这样可以减少链上的数据负载和计算需求。

3）类比之后不难发现，TEE 可信执行环境某种程度上是依赖硬件制造商（如 AMD、英特尔）再结合谷歌云等传统上游服务商提供「可信度」，对原始数据进行了一次 Pre 预加工处理，最终再将数据结果作用到链上。这和 ZK 基于数学原理和密码学算法不依赖任何硬件提供的信任有一个关键区别：TEE 需要一个第三方信任方。

要如何解决此问题呢？逻辑也很简单：TEE+ 可验证性的 Prove 网络。引入一个可验证的证明网络就可以显著提高 TEE 系统的透明度和可信度。Unichain 要引入的去中心化验证网络，Flare 本身区块链架构提供分布式节点治理架构都充当了此验证网络的角色。

尽管，Unichain 还没透露此验证网络的实现和治理细节，但如何利用 TEE 飞地环境的远程可认证特性，如何在硬件提供安全保密的前提下生成证明和链上环境进行交互一定是关键点。