MegaETH真能实现实时区块链吗？

作者：knower，加密KOL；翻译：本站xiaozou

## 1、MegaETH简介

本文的主要内容将是我对MegaETH白皮书的一些个人想法，如果力所能及的话，我可能会从此处进一步扩展。不管这篇文章最后变成了什么样，我都希望你能从中了解到一些新的东西。



MegaETH的网站很酷，因为上面有一只机械兔，配色很显眼。在此之前，只有一个Github——有一个网站让一切变得简单得多。

我浏览了MegaETH Github，得知他们正在开发某种类型的执行层，但我要诚实地说，也许我这个想法是错的。事实是，我对MegaETH的了解还不够深入，现在他们成了EthCC的热门话题。

我需要知道一切，确保我看到的技术和那些酷酷的家伙看到的一样。

MegaETH白皮书说，他们是一个与EVM兼容的实时区块链，旨在为加密世界带来类似web2的性能。他们的目的是通过提供每秒超10万笔交易、不到一毫秒的区块时间和一美分的交易费等属性提升以太坊L2的使用体验。

他们的白皮书强调了L2数量在增长（在我之前的一篇文章中讨论过这一点，尽管这一数字已经攀升到50多个，还有更多L2处于“积极开发”中）以及他们在加密世界中缺乏PMF。以太坊和Solana是最受欢迎的区块链，用户会被其中一方所吸引，只有在有代币可挖的情况下才会选择其他的L2。

我不认为太多的L2是件坏事，就像我也不认为这一定是件好事，但我承认我们需要退后一步，来审视为什么我们这个行业创造了这么多的L2。

奥卡姆剃刀会说，风投们很享受这种感觉，知道他们真的有可能打造下一个L2（或L1）王者，并从对这些项目的投资中获得满足，但我也认为，也许许多加密开发者实际上想要更多的L2。双方可能都是对的，但关于哪一方更加正确的结论并不重要，最好是客观地看待当前的基础设施生态系统，利用好我们现有的一切。



我们目前可用的L2的性能很高，但还不够。MegaETH的白皮书说，即使opBNB（相对）较高的100 MGas/s，这也只能意味着每秒650次Uniswap交易——现代或web2基础设施每秒可以进行100万次交易。

我们知道，尽管加密优势来自于去中心化特性和实现无需许可的支付，但仍然相当缓慢。如果像Blizzard这样的游戏开发公司想要将Overwatch带到链上，他们是做不到的——我们需要更高的点击率来提供实时PvP和其他的web2游戏自然而然提供的功能。

MegaETH对L2困局的解决方案之一是将安全性和抗审查性分别委托给以太坊和EigenDA，将MegaETH转变为世上性能最高的L2，而无需任何利弊权衡。

L1通常需要同构节点，这些节点执行相同的任务，没有专业化的空间。在这种情况下，专业化指的是排序或证明之类的工作。L2绕过了这个问题，允许使用异构节点，将任务分离出来以提高可扩展性或减轻其中的一些负担。这一点可以从共享排序器（如Astria或Espresso）的日益流行和专业化的zk证明服务（如Succinct或Axiom）的兴起中看出。

“创建实时区块链涉及的不仅仅是使用现成的以太坊执行客户端和增加排序器硬件。例如，我们的性能实验表明，即使配备了512GB RAM的强大服务器，Reth在最近的以太坊区块上的实时同步设置中也只能达到大约1000 TPS，相当于大约100 MGas/s。”

MegaETH通过从完整节点抽象交易执行来扩展这种划分，仅使用一个“主动”排序器来消除典型交易执行中的共识开销。“大多数完整节点通过p2p网络从该排序器接收状态差异，并直接应用差异来更新本地状态。值得注意的是，它们不会重新执行交易；相反，他们使用证明者（prover）提供的证明间接验证区块。”

除了“它很快”或“它很便宜”的评论外，我没有读到太多关于MegaETH如何好的分析，所以我将尝试仔细分析它的架构并将其与其他L2进行比较。

MegaETH使用EigenDA来处理数据可用性，这在当今是相当标准的做法。像Conduit这样的Rollup-as-a-Service（RaaS：rollup即服务）平台允许你选择Celestia、EigenDA甚至Ethereum（如果你愿意的话）作为rollup的数据可用性供应商。两者之间的区别是相当技术性的，并不完全相关，似乎选择一个而非另一个的决定更多的是基于共鸣而不是其他任何东西。

排序器排序并最终执行交易，但也负责发布区块、见证和状态差异。在L2上下文中，见证是证明者用来验证排序器区块的附加数据。

状态差异是对区块链状态的更改，基本上可以是链上发生的任何事情——区块链的功能是不断附加和验证添加到其状态的新信息，这些状态差异的功能是允许完整节点无需重新执行交易而确认交易。

Prover由特殊的硬件组成，用于计算加密证明以验证区块内容。他们还允许节点避免重复执行。有零知识证明和欺诈证明（或者是optimistic证明？），但它们之间的区别现在并不重要。

将所有这些放在一起是完整节点网络的任务，它充当prover、排序器和EigenDA之间的一种聚合器，（希望）使MegaETH魔法成为现实。



MegaETH的设计是基于对EVM的基本误解。尽管L2经常将其糟糕的性能（吞吐量）归咎于EVM，但已经发现revm可以达到14000 TPS。如果不是EVM，那是因为什么？

## 2、当前可扩展性问题

导致性能瓶颈的三个主要EVM低效因素是缺乏并行执行、解释器开销和高状态访问延迟。

由于RAM富足，MegaETH能够存储整个区块链的状态，以太坊的确切RAM为100GB。这种设置通过消除SSD读取延迟显著加速了状态访问。

我不太了解SSD读取延迟，但大概是某些操作码比其他操作码更密集，如果你在这个问题上投入更多RAM，则可以将其抽象出来。这在规模化情况下还有效吗？我不确定，但在本文，我会把这当作事实。我仍然怀疑链可以同时确定吞吐量、交易成本和延迟，但我正在努力成为一个积极的学习者。

我应该提到的另一件事是，我不想过于挑剔。我的想法是永远不要支持一个协议多过另一个协议，甚至在一开始就同等重视它们——我这样做只是为了更好地理解，并帮助任何阅读本文的人同时获得同样的理解。



你可能对平行EVM这一趋势很熟悉，但据说有一个问题。尽管在将Block-STM算法移植到EVM方面已经取得了进展，但据说“在生产中可实现的实际提速本质上受到工作负载中可用并行性的限制。”这意味着，即使并行EVM被释放并最终部署到主网上的EVM链上，该技术也受到大多数交易可能不需要并行执行这一基本现实的限制。

如果交易B依赖于交易A的结果，你就不能同时执行两个交易。如果50%的区块交易像这种情况一样是相互依赖的，那么并行执行并不像所声称的那样有重大改进。虽然这样说有点过于简单化（甚至可能有一点不正确），但我认为却正中要害。

Revm和原生执行之间的差距是非常明显的，特别是revm仍然慢1-2 OOMs，不值得作为独立的VM环境。另外还发现，目前没有足够的计算密集型合约来保证revm的使用。“例如，我们分析了历史同步期间每个操作码所花费的时间，发现revm中大约50%的时间花在了“主机”和“系统”操作码上。”



在状态同步方面，MegaETH发现了更多问题。状态同步被简单地描述为一个使全节点与排序器活动同步的过程，这个任务可以很快地消耗像MegaETH这样的项目的带宽。这里用一个例子来说明这一点：如果目标是每秒同步100,000个ERC20转移，那么这将消耗大约152.6 Mbps的带宽。这152.6 Mbps据说超过了MegaETH的预估（或性能），基本上是引入了一个不可能完成的任务。

这只考虑了简单的代币转移，如果交易更加复杂，还忽略了更高消耗的可能性。考虑到现实世界中链上活动的多样性，这是一种可能的情况。MegaETH写道，Uniswap交易修改了8个存储slot（而ERC20转移只修改3个存储slot），使我们的总带宽消耗达到476.1 Mbps，这是一个更不可行的目标。

实现100k TPS高性能区块链的另一个问题在于解决链状态根的更新，这是一项管理向轻客户端发送存储证明的任务。即使使用专业节点，完整节点仍然需要使用网络的排序器节点来维护状态根。以上文每秒同步100,000个ERC20转移的问题为例，这将带来每秒更新30万个密钥的成本。

以太坊使用MPT（Merkle Patricia Trie：默克尔前缀树）数据结构来计算每个区块后的状态。为了每秒更新30万个密钥，以太坊需要“转换600万次非缓存数据库读取”，这比当今任何消费级SSD的能力都要大得多。MegaETH写道，这个估算甚至没有包括写操作（或对Uniswap交易等链上交易的估算），这使得挑战更像是一场西西弗斯式的无休止努力，而不是我们大多数人可能更喜欢的爬坡战。

还有另一个问题，我们到达了区块gas的极限。区块链的速度实际上受到区块gas限额的限制，这是一种自我设置的障碍，旨在提高区块链的安全性和可靠性。“设定区块gas限额的经验法则是，必须确保在此限制内的任何区块都可以在区块时间内被稳妥处理。”白皮书将区块gas限额描述为一种“节流机制”，在假设节点满足最低硬件要求的情况下，确保节点能够可靠地跟上步伐。

还有人说，区块gas限额是保守选择，用来防止发生最坏的情况，这是另一个现代区块链架构重视安全性胜过可扩展性的例子。当你考虑到每天有多少钱在区块链之间转移，以及如果为了略微提高可扩展性而损失这些钱，从而导致核冬天时，可扩展性比安全性更重要的想法就会崩塌。

区块链在吸引高质量的消费应用程序方面可能并不出色，但它们在无需许可的点对点支付方面却异常优秀。没人想把这搞砸。

然后要提到的是并行EVM速度依赖于工作负载，它们的性能受到最小化区块链功能过度“加速”的“长依赖链”的瓶颈制约。解决这个问题的唯一方法是引入多维gas定价（MegaETH指的是Solana的本地收费市场），这仍然难以实施。我不确定是否有一个专门的EIP，或者这样的EIP如何在EVM上工作，但我想从技术上来说这是一个解决方案。

最后，用户不会直接与排序器节点交互，并且大多数用户不会在家中运行完整节点。因此，区块链的实际用户体验在很大程度上取决于它的底层基础设施，如RPC节点和索引器。无论实时区块链运行得有多快，如果RPC节点不能在高峰时间有效地处理大量读取请求，快速将交易传播到排序器节点，或者索引器不能足够快地更新应用程序视图以跟上链的速度，那么实时区块链运行得多快也就无关紧要了。”

或许赘述过多，但却非常重要。我们都依赖于Infura、Alchemy、QuickNode等等，它们运行的基础设施很可能支持着我们的所有交易。对这种依赖最简单的解释来自经验。如果你曾经试图在某L2空投后的前2-3小时内申领空投，你就会理解RPC管理这种拥塞是多么困难。

## 3、结论

说了这么多，只是想表达像MegaETH这样的项目需要跨越许多障碍才能到达它想到达的高度。有篇帖子说，他们已经能够通过使用异构区块链架构和超优化的EVM执行环境实现高性能开发。“如今，MegaETH拥有一个高性能的实时开发网络，并且正在朝着成为最快区块链的方向稳步前进，仅受硬件限制。”

MegaETH的Github列出了一部分重大改进，包括但不限于：EVM字节码→原生代码编译器，大内存排序器节点专用执行引擎，以及面向并行EVM的高效并发控制协议。EVM字节码/原生代码编译器现已可用，名为evmone，虽然我对编码不够精通，无法知晓其核心工作机制，但我已经尽了最大努力来弄清楚它。

evmone是EVM的C++部署，它掌握EVMC API，将其转换为以太坊客户端的执行模块。它提到了一些其他我不理解的特性，比如它的双解释器方法（基线和高级），以及intx和ethash库。总之，evmone为更快的交易处理（通过更快的智能合约执行）、更大的开发灵活性和更高的可扩展性（假设不同的EVM部署可以每区块处理更多的交易）提供了机会。

还有一些其他的代码库，但其中大多数都是相当标准的，并没有与MegaETH（reth、geth）特别相关。我认为我已经基本完成了白皮书研究工作，所以现在我把问题留给任何阅读本文的人：MegaETH的下一步是什么？真的有可能实现有效扩展码？这一切要多久才能实现？

作为一名区块链用户，我很高兴能够见证这一切是否可行。我在主网交易费上花了太多钱，现在是时候改变了，但这种改变仍然感觉越来越难实现，而且不太可能很快发生。

尽管本文内容主要围绕着架构改进和可扩展性，但仍然需要内部rollup共享流动性和跨链工具，才能使rollup A的体验与rollup B一致。我们还没有做到这一点，但也许到2037年，每个人都会坐下来回忆我们是如何沉迷于“修复”可扩展性问题的。