Metis：MEME叙事中的Layer2、Layer2竞争中的最强黑马？

作者：YBB Capital Researcher Ac-Core

### 前言：

Layer2在我们意识中应当是富有“以太坊正确性”的一种扩展路径，但受到市场传言 Metis 的创始团队是“ Vitalik Buterin 妈妈 / 闺蜜”的影响，Metis被冠以了MEME Layer2的头衔，这无疑直刺了市场投资者们对于以太坊正统性信仰的要害。但区块链目前本质属性仍是“代码+金融”，而站在投资角度考虑，技术与市场一直是一对既离又合的欢喜冤家，Metis是否可以借助其他Rollup中心化的排序器问题和强控经济模型的劣势，从众多Layer2中脱颖而出？

### Metis简介

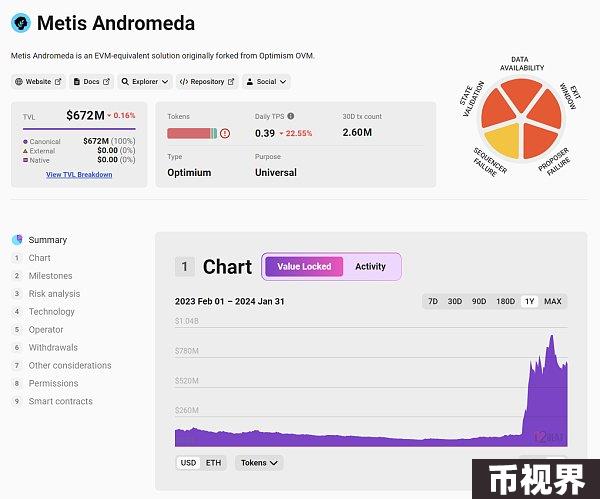


MEME属性的由来，据Metis官网信息，Metis的联创兼首席执行官Elena Sinelnikova一直在推动区块链行业的教育和普及工作，也是教育性非营利组织全球最大的女性区块链社区CryptoChicks的联创之一。CryptoChicks的另一位联创是Natalia Ameline，她是以太坊创始人Vitalik Buterin的母亲，此外Vitalik Buterin的父亲Dmitry Buterin也牵头创办了区块链教育公司Blockgeeks，致力于开发与区块链技术相关的课程。Metis Network于2018年成立，2021年5月发行。

Metis是一条基于以太坊链的Layer2，是Optimism最早的分叉项目，工作原理与其他Layer2相同，最大的亮点是其为首个成功实现排序器去中心化的Optimistic Rollup。该网络采用Proof-of-Stake Sequencer Pool机制以确保网络的持续可用性和审查抵抗力，同时启用费用共享和排序器质押。这些排序器负责确定交易的打包顺序，过程中必须获得排序器池中至少2/3以上的排序器签名，才能将数据打包上传至Layer1网络。为了防止恶意行为，Metis还引入了验证者角色，对区块进行抽样调查，确保排序器对交易的排序是正确的。

MPC（多方计算）在隐私保护和去中心化方面具有优势，然而在需要达成共识的区块链网络中，它也存在一些明显的劣势。由于缺乏中继节点分发信息，导致了通信次数的增加从而又导致了网络内通信成本的显著上升。Metis的解决方案是将单点排序器转变为排序器池，通过节点质押机制和轮换机制实现去中心化，从而使去中心化排序器能够达成共识完成签名。虽然这可能使网络成本最终并不比Layer1低太多，但却能够实现抗MEV和解决单点故障问题，同时将收益分发给节点质押者。

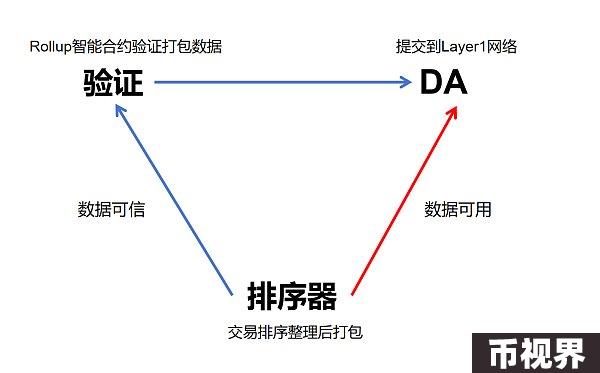
近期Metis TVL的急剧增长引起了人们对于去中心化排序器重要性的关注，据 L2BEAT 数据，当前在所有Layer2网络中OP方案的TVL排名第五。Metis的去中心化排序器设计初衷既能主动分配蛋糕，同时也能让市场看到Layer2原生代币的价值捕获。



### Rollup三要素

Rollup是Layer2解决方案之一，也称为卷叠。其工作原理是将在以太坊主网（即Layer1）上进行的交易计算和存储迁移至Layer2进行处理和压缩，然后将压缩后的数据上传至以太坊主网，从而扩展以太坊的性能。

Rollup根据确保压缩数据有效性（即数据正确性）的方案不同可以分为ZK Rollup和Optimistic Rollup。它涉及链下计算，每隔几分钟将交易打包到链上，进行滚动验证和记账，并因此得名。然而尽管我们通常将其称为Rollup链，但Rollup的链下部分并非是完整的区块链，从字面上理解Rollup将一堆交易卷起来形成一个Rollup交易，所有节点在接收到此Rollup交易后不执行被卷起来的逻辑而只接受这些逻辑的执行结果。



排序器(Sequencer)

排序器是 L2 中负责将交易排序、整理、打包并提交到 L1 网络的角色，目前大多数 L2 项目，都依赖单一序列器（通常是项目方自己）来完成以上工作，这里存在着两个安全问题：1.单点故障，如果该序列器因为攻击或技术故障出现问题，整个网络会因此停摆；

2.扩展性问题，单一的序列器可能难以应付日益增长的交易量。

验证

交易过程中在排序器发送打包的数据需要经过验证，当前以太坊Rollup的验证大部分是由以太坊Rollup智能合约执行来以此保证数据的可信性。主要存在两种不同的验证方法：ZK Rollup（零知识证明Rollup）和Optimistic Rollup（乐观卷叠）。例如：

ZK Rollup:

验证方法： ZK Rollup使用零知识证明（Zero-Knowledge Proofs）来验证在Layer2发生的所有交易的正确性。零知识证明允许验证方在不了解具体交易细节的情况下确认其有效性；

隐私保护： ZK Rollup强调用户隐私，因为在Layer1上提交的是计算结果的“证明”而非交易的详细信息。具体的交易内容在Layer2上进行，而Layer1只验证零知识证明的有效性。

Optimistic Rollup:

验证方法： Optimistic Rollup采用“乐观”策略，即假设所有的交易都是合法的，然后在必要时才进行验证。验证是通过欺诈证明（Fraud Proofs）来完成的，即在Layer1上提交证明，证明Layer2上的交易违反了规则；

实时性： 由于假设所有交易合法，Optimistic Rollup在Layer2上的交易可以迅速进行，而验证发生在有争议或异议产生时。

DA(Data Availability)

DA即数据可用性，将链下处理的每笔交易的状态数据公开发布，使其他参与者也可以访问和使用这些交易状态数据。某些Layer2将交易的状态数据写入以太坊Layer1，从而实现DA。也有一些Rollup Layer2将交易关键数据写在第三方区块链上，数据可用性的前提是数据可信。

例如：

Optimistic Rollup中的DA: 确保Layer1上能够获得Layer2上所有交易的数据。如果数据不可用，任何人都可以在Layer1上提出异议，这有助于防止潜在的数据篡改或遗漏；

ZK Rollup中的Commitment: 在Layer2中，所有交易的计算和存储发生，但只有计算的结果（称为Commitment）被提交到Layer1。零知识证明用于证明这些Commitments的正确性。

注：在ZK Rollup中"Commitment" 更侧重于验证Layer2上交易计算结果的正确性，而"数据可用性" 更关注确保Layer1可以获得Layer2上所有交易的数据，这两者通常是相辅相成的，以确保整个系统的安全性和可靠性。

在Rollup的三个关键要素中，排序器被认为是最为关键的。排序器负责在链下执行对Layer2交易信息进行排序和压缩的过程。由于这一过程涉及数据的可信性验证，因此实现数据的可用性至关重要。然而当排序器是去中心化的时候，对于数据可信性验证和可用性的实现可能不再如此紧要。

### 基于PoS共识的Metis去中心化排序器



排序器的遴选

在 Metis 上锁仓$Metis有机会成为节点，会根据锁仓的 $Metis 数量计算权重，算法会为这些节点分别分配一个范围。Metis Rollup对"交易数据验证板块"进行了改进。在Layer2层的计算过程中，引入了一个名为"验证人"的角色，并通过竞争挖矿机制来激励验证节点快速验证交易，并且这一过程通过竞争机制实现。与其他采用Proof-of-Stake（PoS）机制的Layer1网络类似，Metis的交易也需要节点进行验证。因此，从Metis上打包并传送到L1上的数据不存在争议问题，也就避免了将资产从Metis提取到以太坊主网上出现间隔和延时的问题。

与Optimistic Rollup相比，Metis Rollup的一个显著区别在于，资产从Metis提取到以太坊L1层仅需要几个小时或几分钟。这突显了Metis Rollup在处理交易的效率和速度方面的优势。总体上，锁仓金额越高的节点加入排序器的概率越高。当然这其中也有一些随机成分。

排序器的MPC(多方计算)

Metis实现排序器的去中心化涉及三个关键角色：管理员（Admin）、排序器和基于PoS的共识层。

管理员：负责设置整体网络的关键参数，以及管理排序器加入排序器池的资格。协议方不再直接掌握此类事务的绝对控制权，而是通过提案审定后由管理员执行。实现去中心化的难点之一在于排序器的管理必须以去中心化的方式进行，同时要保持高效和便利；

排序器：Metis采用了基于 TSS（Threshold Signature Scheme）的MPC（Multi-Party Computation）签名来管理多个排序器的签名权限。每个排序器有权决定一个批次，并通过MPC签名的方式让所有排序器参与。如果签名数量超过2/3，则认为该批次有效，可以提交到L1上的Rollup合约中。排序器池进行的MPC签名由基于PoS网络中的另一个合约进行管理。当PoS网络检测不到MPC地址时，会触发MPC模块以生成密钥；

基于PoS的共识层：PoS网络负责管理排序器签名权限的合约，监控MPC地址，以及触发密钥的生成。生成的密钥会被分片后分发给池中的每个排序器，用于进行MPC签名。该模块的设置涵盖了密钥的生命周期管理，包括多重签名生成、密钥重新共享、应用签名、删除签名等；

采用TSS的原因在于其具有高容错性和高灵活性的属性。相较于多签，TSS无需在链上对每个签名进行验证，而是将所有签名者的签名聚合后统一进行校验，从而提高了交易确认速率。此外，PoS节点间的通信使用独立的Tendermint通道，而MPC运行时的通信则采用了libp2p协议。这一整套系统的设计旨在实现高效、安全的排序器去中心化管理。

Metis排序器的交易流程

1.启动用户开始交易；2.交易被转发到网络排序器节点；3.区块生成：排序器接受交易有效时创建区块；4.最终确定：多方计算（MPC）节点讲区块合并转发到以太坊主链。

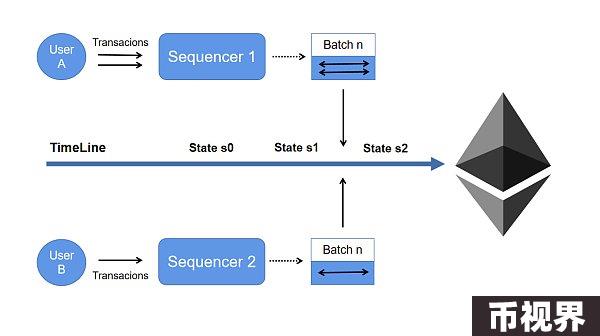
MetisEDF

Metis生态发展基金（MetisEDF）为此提供资金支持，涵盖了多个方面，如激励协议的开发和部署，提供流动性支持，进行安全审计和实施流动性挖矿计划等。分配包括：

Sequencer挖矿：65.4%（3百万$METIS / >2.6亿美元）;

生态系统资助：34.6%（1.6百万$METIS / >1.4亿美元）。

### 中心化的排序器问题



以太坊的原理是，每个节点都存储且执行用户提交给它的每笔交易，这种高级别的安全方式也导致整个网络十分昂贵，所以需要为整个网络扩容而采取Rollup解决方案。简单来说，Rollup = Layer1的一组合约 + Layer2的自身网络节点，即链上智能合约 + 链下聚合器，在结算、共识、数据可用性方面均依赖以太坊，自己仅负责执行 Rollup。

链上智能合约，表示了它的信任模型就是以太坊上的一个智能合约，借用了以太坊的安全性；

链下聚合器，表示了它会链下执行并聚合交易，将大批量的交易进行压缩，并最终放上以太坊主网，达成更快且更便宜的目的。

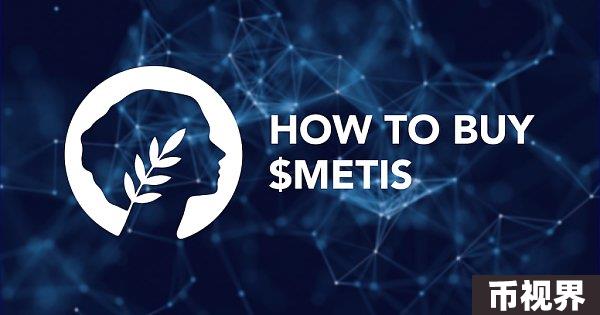
Layer2网络节点又由很多部分组成，其中排序器组件最为重要。它负责接收Layer2上的交易请求，以此决定它们的执行次序并将交易序列进行Batch，最终传送给Rollup项目在Layer1上的合约，目前以太坊所有Layer2 Rollups的排序器都是中心化的，Metis却正好占据了去中心化排序器的先机。

Layer2的全节点可以通过两种方式获得交易序列：一是直接从排序器获取，二是读取排序器发送到Layer1的Batch，但后者拥有更强的不可修改属性。由于交易执行会改变区块链账本的状态，为确保一致性，Layer2全节点除了需要获得交易次序，还必须与排序器同步账本状态。因此，排序器的任务不仅是将交易批次发送到Layer1的Rollup合约，还要将交易执行后的状态更新结果StateRoot/StateDiff传送至Layer1，通俗来讲排序器的工作是将交易处理和排序为添加到区块链中的块，负责批量处理交易并将其发布到 Layer1 智能合约。

对于Layer2的全节点来说，只要获取了Layer1上Rollup的交易序列和最初的StateRoot，就能够还原出Layer2的区块链账本，并计算得出最新的StateRoot。反之，Layer2全节点自己计算得到的StateRoot与排序器发布到Layer1的StateRoot不一致，就意味着排序器存在欺诈行为。综上相比Layer2自身的网络，Layer1会更加去中心化、去信任（Trustless）和更安全。

Optimistic Rollup举例它允许Layer2全节点提供欺诈证明，证明排序器在Layer1发布的数据是错误的。但对于没有欺诈证明的Optimism来说，如果它真想通过排序器来盗走Layer2的用户资产，只需让排序器运行者伪造交易指令，并将其他人在Layer2的资产转移至自己的地址，最后通过Rollup自带的Bridge合约来把盗来的币转移至Layer1。

### 对于Metis的看法



Layer2近期最大的炒作热点无疑是坎昆升级，但这对于Metis不会产生独有的利好而是普遍性的。抛开“ Vitalik Buterin 妈妈 / 闺蜜”的市场情绪影响，Metis与其他Layer2最大的竞争点在于其去中心化的排序器和权益下放的经济模型，TVL表现出的市值整体更加贴合市场用户对于Metis信心的反馈。

Metis与其他Layer2自己紧握财政大权的方式不同，而是把更多的收益分给了用户。OP Rollup的经济模型整体是强控制状态，通过中心化的方式，不断给生态发放OP Token奖励来刺激开发和交互以此通过赚取Gas价差获利，与此方式不同的是，Metis则是把收益权益下放给了质押者们参与竞争，大幅释放Layer2基础设施金融化的属性，以此吸引到市场的大量关注度。

MEME更多代表着一种文化和一些社会经济学因素，好比我们在买MEME的过程中除了对它十倍、百倍甚至千倍的投资预期外，更多一部分是来自我们对它叙事方式和各类因素的认可和喜爱， 但总归拉盘即正义，Metis不断增长的TVL也是市场对于其投资预期的一种反馈。MEME属性问题在抛开技术层面站在市场端的角度来考虑，我的观点是，如果铭文是公链性能的测试器，那MEME一定程度上是市场认可度的试金石。