发一条公链要多久？原来只要十分钟

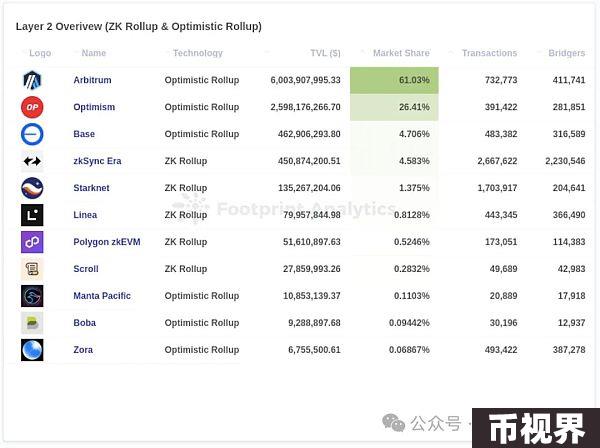
## 公链赛道人满为患

说起区块链，这个链那个链，很多人还认为是高端前沿科技。

要在几年前有人说自己发了一条链，那妥妥的大牛存在，

但是现在呢，各种链的赛道可以说人满为患，光是以太坊的Layer2项目，

粗略看了一下，现在整个加密行业可能有六千多个！



众所周知，区块链存在不可能三角的概念，区块链无法同时兼顾可拓展性、安全性和去中心化这三个维度。



例如我们的TBC和以太坊主链都是安全性和去中心化这两个维度拉满，但是可拓展性拉跨，每秒交易数 （ transactions per second，TPS)是人尽皆知的差。

以太坊主网的TPS是20左右，比特币的主网TPS只有7。

一些开发者就通过Layer2的解决方案来打补丁，牺牲一部分安全性和去中心化，— — 将主链处理的交易数据尝试迁移到主链之外，以提高交易速度及负载。目前大部分layer2的TPS都有几千，考虑到现在大规模应用场景有限，大部分链上交互都是炒币交易，这个TPS应该是完全够用的。

## 原来发链也可以“一键生成”

那做一条layer2的链是不是很难呢？

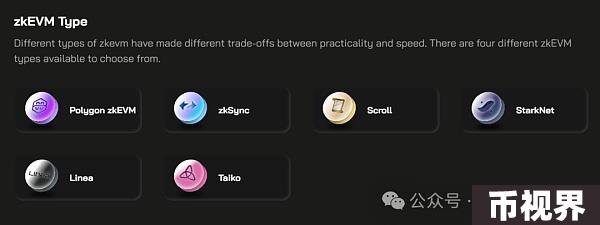
其实完全不难，有一个赛道叫RAAS（Rollups-as-a-Service)，这种服务商支持“一键发链”，据说10分钟就可以创建好一条链。（展示官网录视频）



而且各种生态随便选：什么比特/以太坊/solana都不在话下



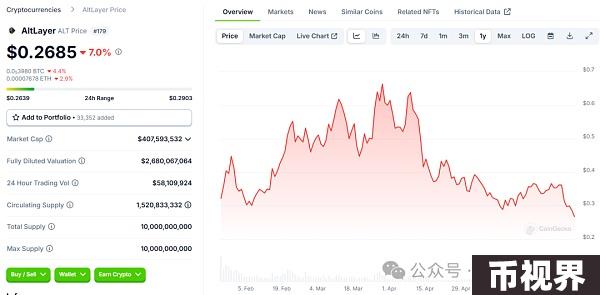
用的还是最先进的zk-rollup



你就说，牛逼不牛逼吧！

刚刚我举的这个例子就是Lumoz。

这个赛道也还有很多其他的知名选手，例如AltLaye这个项目就是RAAS赛道的佼佼者，今年一月底的时候上线币安，目前FDV有二十几亿。



Altlayer这个项目的特点是发明了一个再质押Rollup框架。

听到这里大家是不是要迷糊了？一会Rollup，一会ZK的，这些和Layer2有什么关系呀？

## Layer2技术路线回顾

现在和大家科普一下Layer2的技术路径，目前大部分的二层链使用的技术包括以下三种：

### 状态通道（State Channels）

这种方法允许两方或多方在链下进行多次交易，只在交易结束时将最终状态提交到区块链。一个典型的例子是闪电网络（Lightning Network），主要用于比特币。



这个方案有点像打白条，假设你是开饭店的，有个卖猪肉的每天来你这边吃一顿饭，同时你每天要向他买猪肉，正常情况下你们每天要发生两笔交易。但是如果你每天记账，月底再结账，那你们一个月下来就只要一笔交易。

这个方案尤其适用于长期、重复、小额支付的情形，但是不适合临时增加或者减少参与方。因此目前闪电网络也在交易所账户转账用得比较多，其他场景限制较大。

### 侧链（Sidechains）

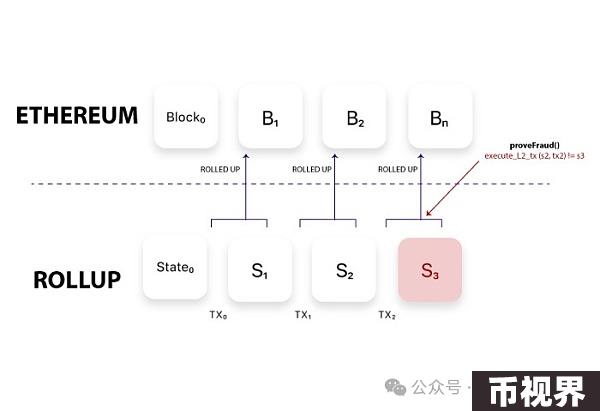
侧链是一条独立的区块链，使用其自身的共识机制，但通过双向锚定与主链（母链）连接。侧链可以自由地实现不同的功能和优化，同时主链依旧保持其主要的安全和稳定性。



大名鼎鼎的Polygon就是使用的这个方案，用户将以太坊从主网发送到 Polygon 的时候，其实转移从未真正发生过。真实发生的事件是将转移的金额锁定在主网上，并在Polygon上铸造出资产的镜像版本。这就是为什么发送到 Polygon 的以太坊可以作为 wETH （ Wrapped Ethereum）来使用。

### 卷叠（rollups）

这第三种技术方案就是卷叠（rollups）了，这种方案的原理是把多笔交易卷到一条数据里面上主链。



就好像你去饭店点菜，一下子点了50道菜，而你并不需要支付五十次，只需要支付一次就可以了。

而这种技术方案也有两种路径：

分别是OP和ZK，也就是Optimism 乐观和Zero Knowledge零知识证明。

OP rollup很乐观，假设所有卷叠进去的数据都是有效的，就像你去饭店买单，相信饭店的账单都是正确的。为了防止欺诈交易，OP rollup 协议允许人们对虚假交易提交挑战。欺诈交易直接在以太坊网络上提交，以检查其是否合法，并解决争议。

我们熟悉的 Arbitrum/Base链都是用的OP rollups。



而 zk-rollups则依靠一种称为零知识证明的密码学来工作，它允许某人在数学上证明一个陈述是正确的，而无需披露有关该陈述的其他信息。有点把你点的每道菜都加密，最后生成一个独一无二的密码，最后这个密码只要能对上，那店家是不可能纂改你的菜单的。

最近争议很大的zkSync就是用的zk rollups。



另外我们熟悉的merlin chain用的也是zk rollups

那OP和ZK到底哪个更先进呢？

V神曾多次表示“短期 OP，长期 ZK”，OP 门槛低，现在也形成了规模效应，但在安全性上却不如ZK。因此也有一种说法是ZK技术是Layer2的终局。

ZK的缺点呢，就是消耗算力太多。

## 技术升级太快，ZK也变标配

本轮大火的模块化能填补上消耗算力过多的短板。

从技术原理上来看，一个 Rollup 至少分为 3 个模块：

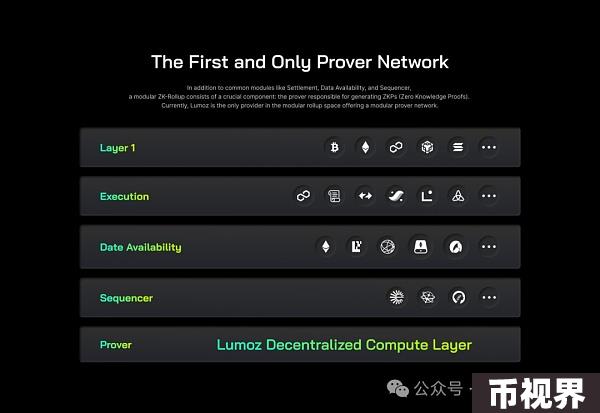
数据可用性（DA）、序列化器（Sequencer）、证明者（Prover）。

总体来说数据可用性（DA）是指区块生产者将区块的所有交易数据都发布到网络中，以便使验证者可以进行下载。

序列化器（Sequencer）负责将 Layer 2 网络中的交易排序、组织、打包并提交到 Layer 1 网络。

证明者（Prover）则需要通过密码学的方式证明Layer 2的数据和上传到 Layer 1 网络的数据一致。

在这些模块中，DA 和 Sequencer 领域已经有项目取得了显著成就，比如几百亿市值的 Celestia、EigenDA 等都为区块链模块化发展树立了榜样。然而，在 ZK-Rollup 领域中，Prover 模块的成本甚至高于 DA，且目前尚未出现强有力的竞争对手。Lumoz 目前是该领域唯一的算力提供者。

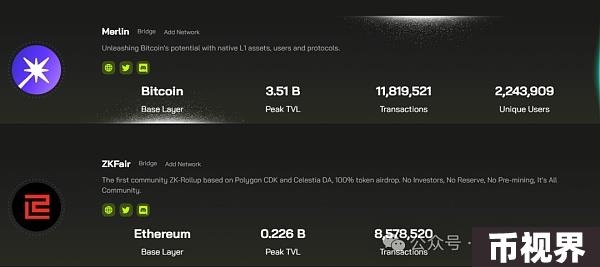


这个Lumoz 团队技术实力不错的，他们改进了 ZKP 算法，显著提高了集群中机器资源的利用率，进一步加快了 ZKP 计算。成功将平均交易确认时间从大约 5-6 分钟缩短到约 3 分钟，将 ZKP 生成效率提高了约 80% 。

Lumoz 还引入了 ZK-PoW 的概念，邀请矿工参与维护 zkEVM 并计算 ZKP。Lumoz 的目标是简化 ZK-Rollup 的使用，并促进其更广泛的采用，从而促进基于 zkEVM 的应用链的大规模部署。

说到这里大家是不是感觉Lumoz这个项目很厉害呢？

没错，他们的实力在加密行业也是很受认可的，据说目前已经支持了Merlin Chain、Hashkey Chain、Ultiverse、Matr1x等20多个Layer2链。



是不是很炸裂？

要知道，现在市面上绝大多少Raas服务商都只能提供OP roll ups服务，而Lumoz的横空出世，竟然让zk rollups也可以一键发链了。

如果你撸空投被zkSync伤到了，这个lumoz就可以帮你报仇雪恨，十分钟就能复制一个zkSync出来。