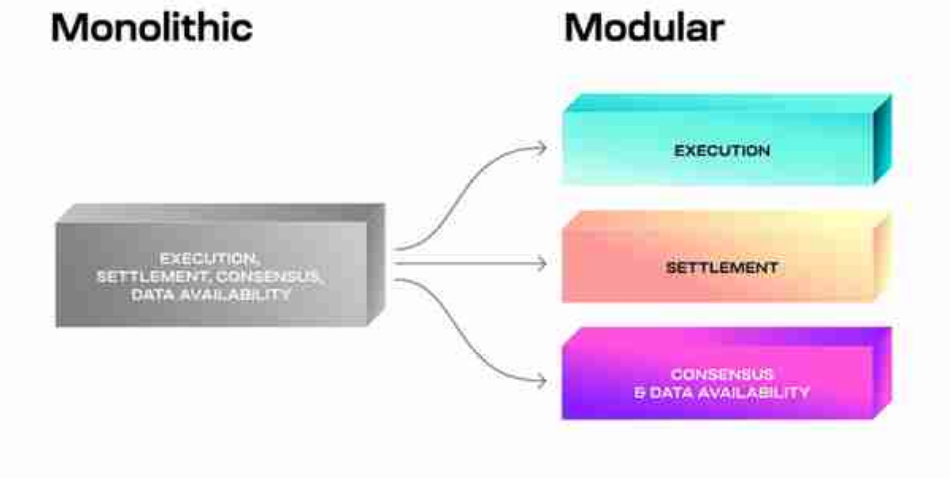
一、单链（Monolithic blockchains）单链包含四个组件执行层：确保所执行的交易进行正确的状态更新。执行层必须确保被执行的交易是有效的，即交易的结果是有效的状态机转换。结算层：确保有一个使得执行层能够验证证明、解决欺诈纠纷的环境，并作为执行层之间的桥梁。共识层：确保交易的顺序达成一致。数据可用性层：确保交易数据的可用性。

单片区块链在单个层上同时完成上述的所有事情。

单链的限制低效的交易验证：节点必须重新执行交易以检查有效性。资源约束：区块链受单个节点的资源容量约束。可扩展性：为了提高吞吐量，必须在一定程度上牺牲安全性或去中心化。



单链和模块化区块链的对比

二、模块化区块链基础知识(1) 模块化区块链是什么

指将「执行层、结算层、共识层、数据可用性层」四个组件中至少一个组件完全外包给外部链的区块链。

由于在单片链上为数百万或数十亿用户提供服务过于复杂且解决能力有限，人们提出了分片和Layer2 解决方案，后来逐渐演变成模块化区块链。模块化的实现最初方案是rollups，后来这个概念进一步扩大成模块化区块链。

模块化区块链能够最大限度地降低运行节点的成本。

(2) 模块化区块链的第一原则去中心化：模块化区块链通过降低用户操作节点和验证网络的成本来优先考虑网络安全。安全：在存在恶意验证者的情况下，去中心化的用户网络最终负责维护区块链的安全性。可扩展：扩展使模块化区块链能够增加

容量，而不会增加用户验证和保护网络的成本。如果区块链可以增加它处理的交易数量，而不会增加节点验证交易的成本，那么它就是可扩展的。模块化区块链堆栈中使用的欺诈证明、有效性证明和数据可用性采样等技术使节点能够比完整节点更有效地验证交易，同时保持同等的安全性。

可扩展性公式定义

(3) 模块化区块链的优势具有主权：尽管使用了其他层，但新的模块化区块链可以像Layer1 一样具有主权。这允许区块链在未经任何底层许可的情况下响应黑客攻击并推送升级。主权（Sovereignty）：在代币、协议的功能和升级、网络和协议的治理、生态系统的建设和基础设施具有更高的主动权方便推出新的区块链：由于模块化区块链不需要处理所有功能，新区块链可以简单地将现有的模块化区块链用于他们希望卸载的组件。像Optimint 这样的Rollups “SDK”与Cosmos SDK 相结合将有助于促进新区块链的创建，而无需引导安全验证器集提高可扩展性：通过模块化可以在不牺牲安全性或去中心化的情况下实现扩展。

(4) 关于Celestia

Celestia 与之前的区块链设计不同，后者将执行作为核心功能，但Celestia 设计者认为执行是新链的工作（指基于Celestia 创建的新链来负责处理执行），而Celestia 专注于基础层（共识和数据可用性），这样可以从基础层缓解单片链的最大瓶颈：吞吐量和状态膨胀。

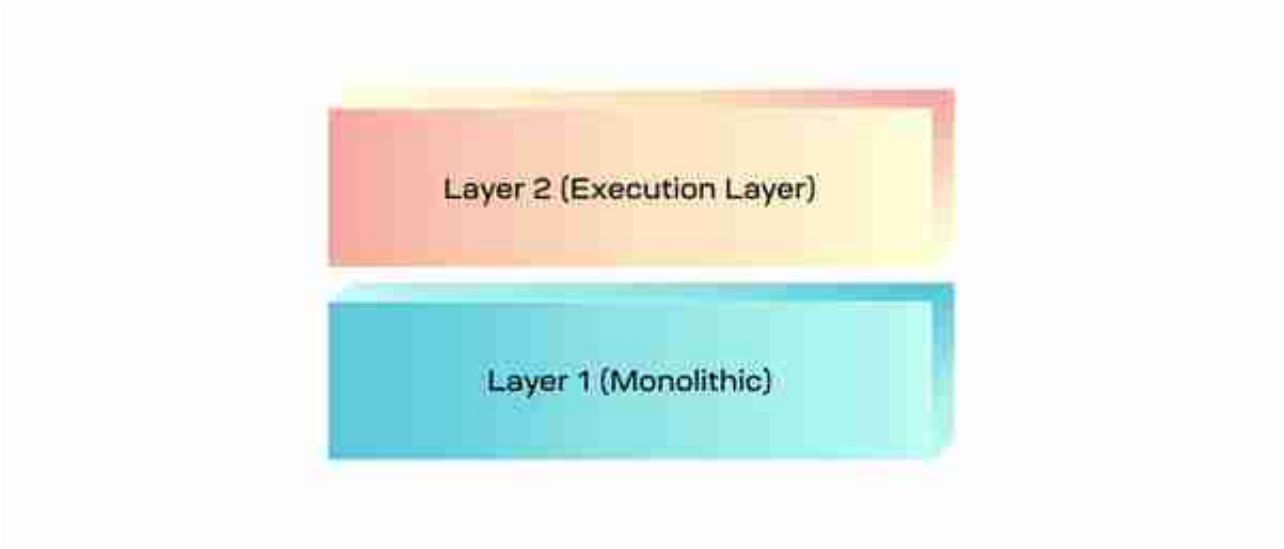
Rollups 和Celestia 的区别在于Rollups 专注于执行（无结算、共识和数据可用性层），Celestia 专注于共识和数据可用性（无执行和结算）。

数据可用性层对吞吐量的重要性：吞吐量分为数据吞吐量和交易吞吐量，数据吞吐量与数据可用性层密切相关，因为它们的主要工作是为数据提供高容量。状态膨胀：指支付一次GAS费会让你的数据在以太坊区块链上永久保存，从而导致一个无限的、不断增长的状态，其中甚至有很多无用数据。

三、模块化区块链的三种架构(1) Layer 1 & Layer 2

最初构建朴素的模块化堆栈是为了向Layer1 提供可扩展性。在这个堆栈中，Layer1 提供所有关键功能，包括执行，而Layer2 只专注于执行。Layer1 允许Layer2 发布区块，同时充当连接Layer2 的枢纽。

在大多数情况下， Layer2 的容量也取决于Layer1 的容量。因此， Layer1 和Layer2 堆栈的这种实现对于可扩展性来说不是最理想的。

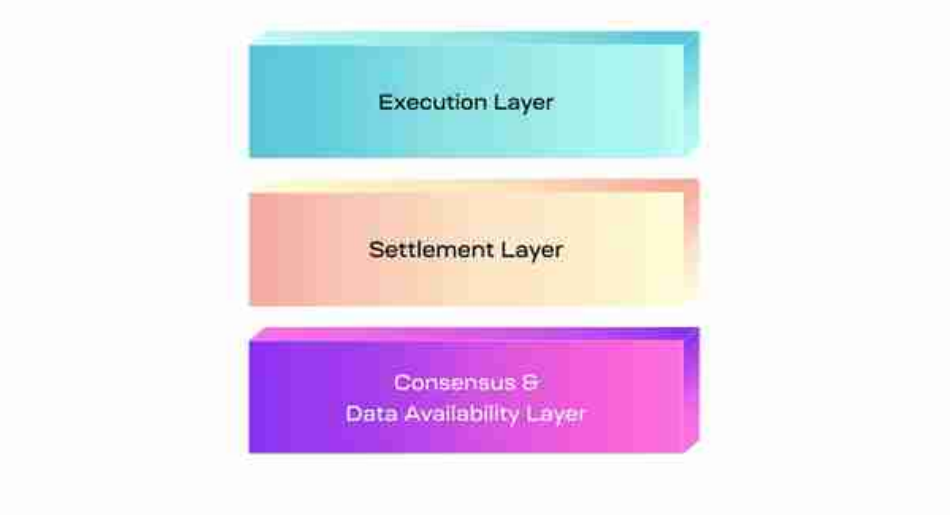


(2) 执行、结算和数据可用性

优化模块化区块链堆栈可以提供的更多好处，通过模块化区块链将各个功能解耦：

执行层应用程序所在的环境和执行状态更改的环境，位于模块化堆栈的顶部，其作用与Layer2 相同。结算层执行层的可选中心，用于验证证明、解决欺诈纠纷。用于在执行层和结算层之间建立信任最小化桥梁，并提供了一种执行层之间相互连接的方式。执行层可以选择将其完整的区块发布到结算层，之后结算层将构建自己的区块，包括来自执行层的交易，并将交易数据发布到共识和数据可用性层。这只是结

算层在模块化堆栈中发挥作用的多种方式之一。因为没有执行功能，所以结算层只发布交易数据，而不是整个区块的内容。信任最小化桥梁：两个区块链之间的桥梁不需要中间人、委员会或诚实的多数假设来确保资金不会被盗。例子是以太坊和建立在其之上的Rollups 之间的桥梁。共识和数据可用性层共识就交易顺序达成一致，数据可用性验证交易数据是否可供下载。在多数情况下这两层之间互相协作，例如专门研究数据可用性的模块化区块链需要达成共识才能对数据进行排序，否则无法确定数据的历史记录。



(3) 执行和数据可用性

在前两个模块化堆栈中，执行层只专注于执行，并将剩余的功能卸载到其他层。然而，由于模块化区块链的用途很灵活，因此执行层不仅限于将其块发布到结算层。例如，可以创建一个不涉及结算层的模块化堆栈，只涉及共识和数据可用性层之上的执行层。

由于不涉及结算层，因此只有数据可用性层负责为交易排序和数据可用性提供安全性。这使执行层能够获得将共识与执行分离的全部可扩展性优势，因为没有中间层将交易数据转发到基础层（共识和数据可用性层）。

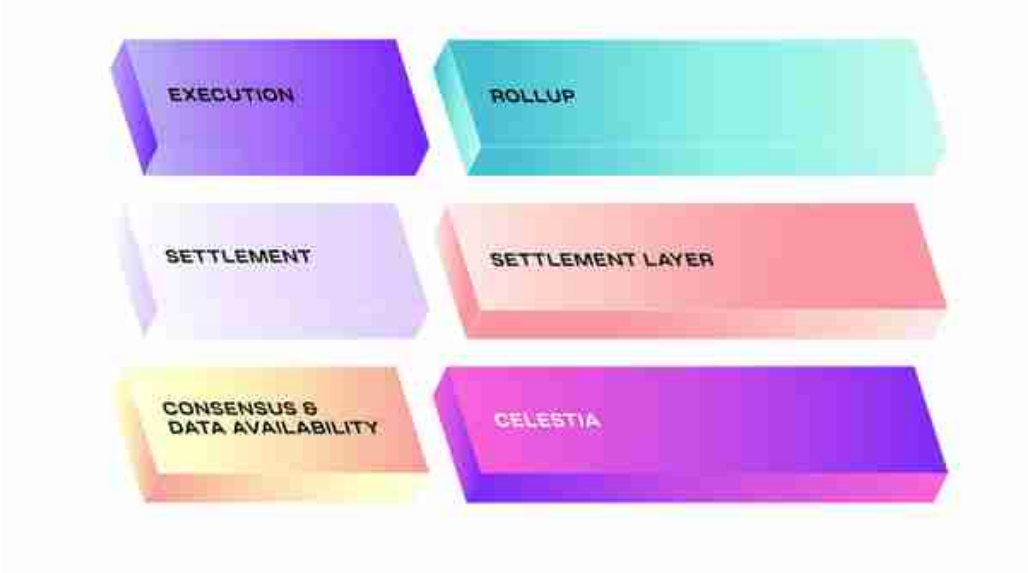
四、模块化结算层

由于模块化区块链仅处理一部分功能，因此可以进行更多的解耦，比如解耦出结算层，可以通过模块化区块链进行结算层的优化和专业化。

模块化堆栈中的结算层可以专注于结算，同时将其余组件（如共识和数据可用性）外包给其他模块化区块链。通过引入欺诈或有效性证明，结算层可以增强轻客户端的安全性，允许他们验证有效或无效块。

结算层为rollups 提供的功能Proof Verification 和Dispute Resolution：rollups 发布其证明以供外部验证的地方，这对于依赖交互式欺诈证明的OP-Rollups 特别有用。促进桥接的中心：如果rollups 通过一个共同的结算层，它们可以相互桥接。流动性来源：存在于同一个结算层的流动性可以被顶部的所有rollups 使用。

模块化堆栈中的结算



五、模块化可扩展性

站在可扩展性的角度，可以进行执行层、数据可用性层、结算层的模块化划分。

1. 执行层

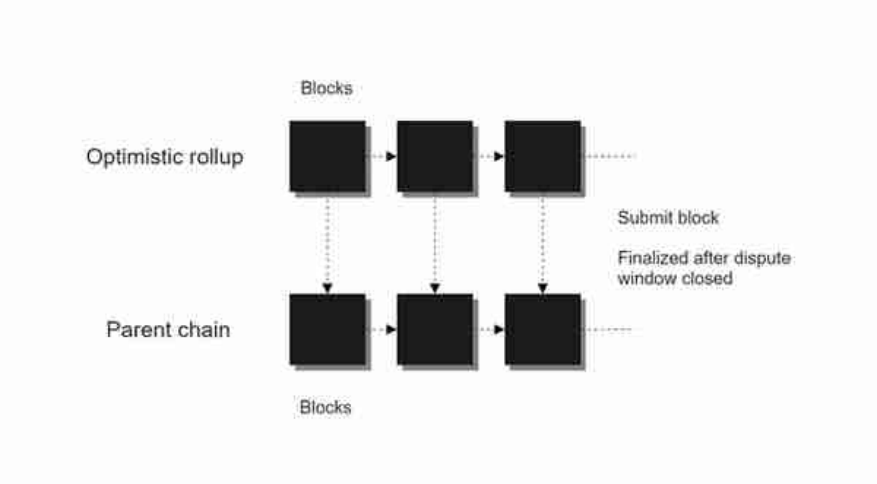
Rollups 本身就是一种区块链，将其块发布到基础层以确保有效性和数据可用性。随着时间的推移，出现了两种主要的Rollup 设计，optimistic 和zk-rollups。

(1) Optimistic Rollups

Optimistic Rollups 将其区块发布到基础层，基础层接收区块并乐观地假设交易是正确的。为了允许在怀疑区块无效的情况下挑战Rollups
块，提供了一个争议窗口（dispute
window），如果一个块受到挑战，则使用欺诈证明（fraud
proof）来验证它是否无效。一旦争议窗口关闭，就不能对区块提出挑战。

Optimistic Rollups 提供的可扩展性：

将执行从Layer1 移走，一旦交易在Optimistic Rollups 上执行， Layer1
就不需要重新执行它们，因为它们自动被假定为正确的，从而减轻了Layer1
执行的负担。减轻Layer1 的状态增加。通过将应用程序和交易转移到不同的链上，Layer1 可以降低其状态增长的速度。大量的状态增加会增加对节点的硬件要求，这会对去中心化产生负面影响。

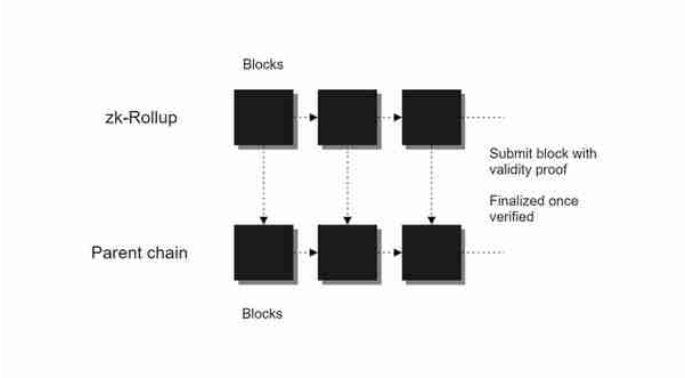


(2) ZK-Rollups

对于发布到Layer1 的每个Rollups 区块都会附带一个有效性证明（validity proof），以证明该区块的正确性。一旦验证了有效性证明，交易就被认为是最终的，不需要争议窗口来判断Rollups 区块的有效性。

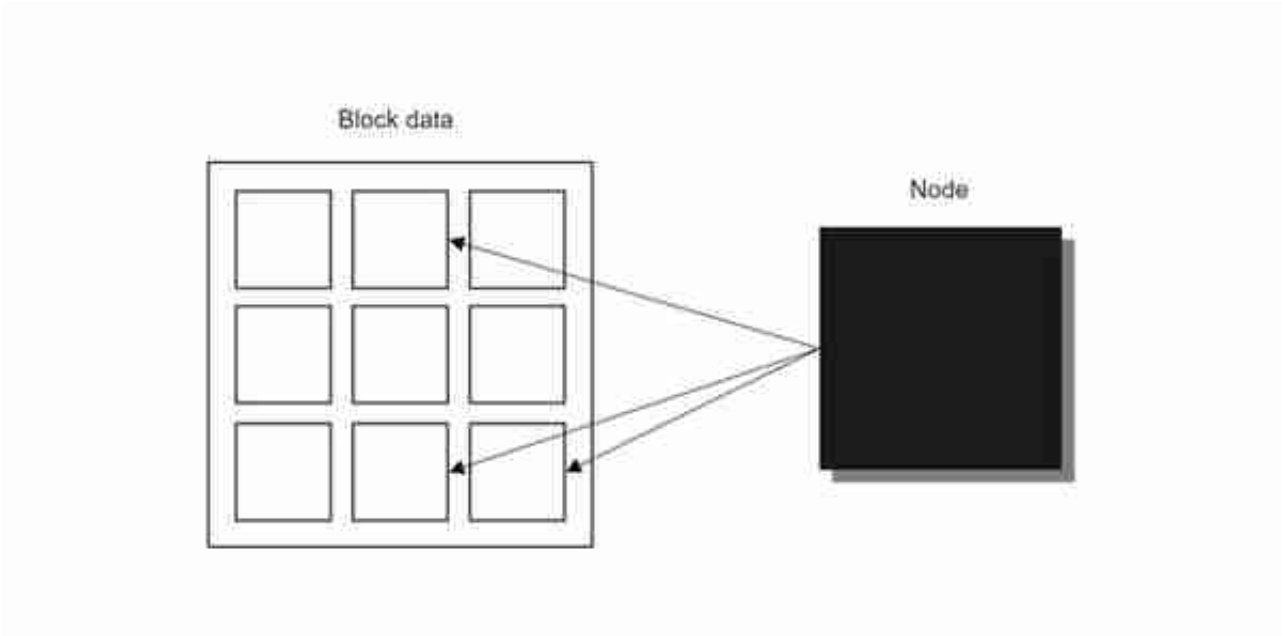
ZK-Rollups 提供的可扩展性：

减轻Layer1 的执行瓶颈和状态增长，提供与Optimistic rollups 类似的可扩展性优势。此外，ZK-Rollups 还通过使用有效性证明为计算验证提供可扩展性。在大多数区块链中，区块生产者执行交易并将它们放入一个区块中，随后由节点重新执行以验证正确性。有效性证明允许节点有效地验证交易而无需重新执行它们——它们只需验证有效性证明。



2. 数据可用性层

通过分离共识和执行，数据可用性层也可以进行可扩展性优化，而不受提供结算层功能的限制。关键技术是数据可用性采样，通过多轮抽样小随机块，它允许节点无需下载整个块来验证可用，从而减少轻节点的带宽。



3. 结算层

现在的结算层仍然承受着应用程序及其相应的基于用户的交易活动的负担，这导致结算层挤满了来自个人用户和执行层的交易。结算层可以使用与执行层和数据可用性层相同的技术进行扩展，但目前结算层的扩展效果还不理想。

六、创建新的区块链

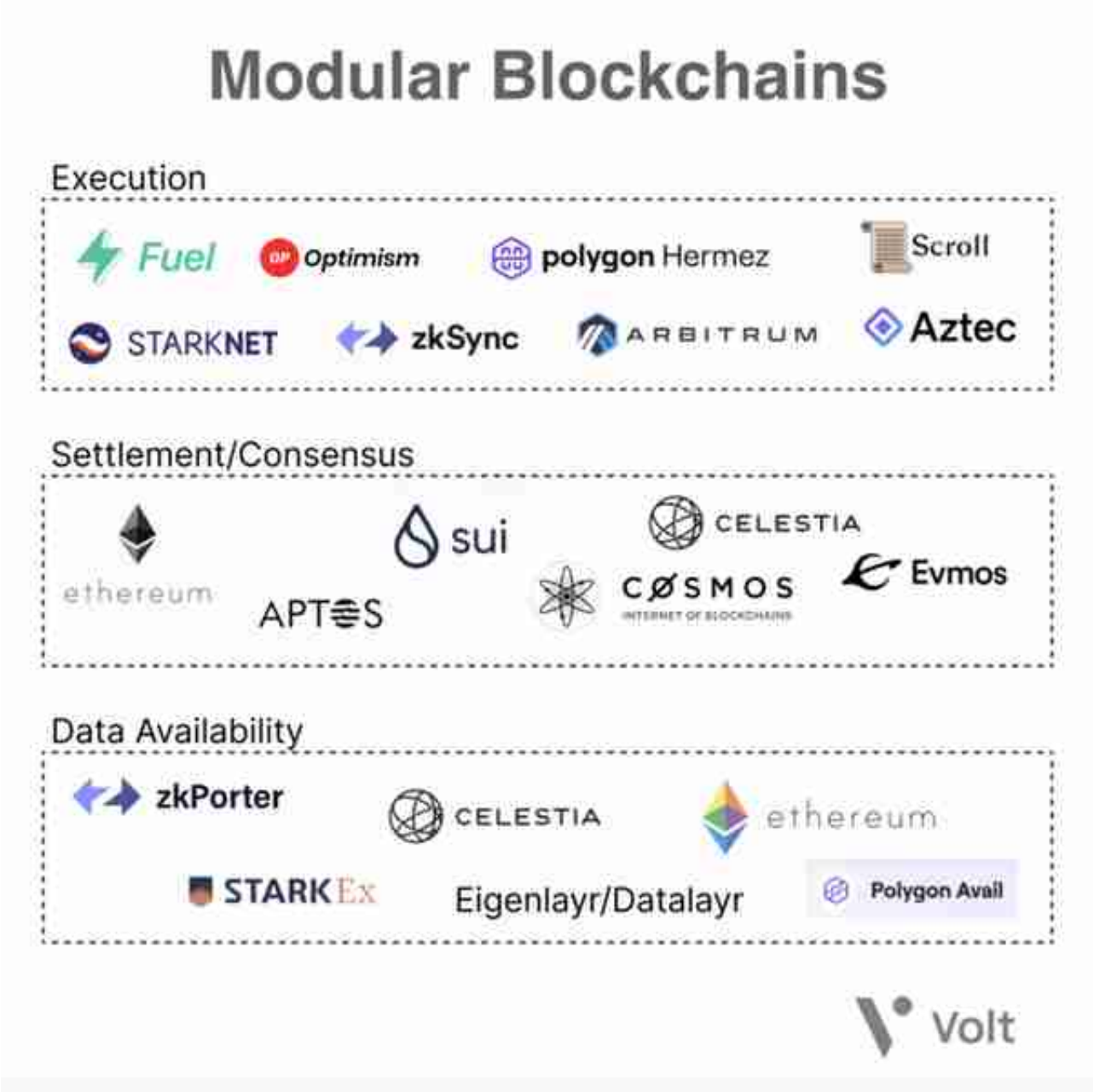
随着Cosmos SDK 及其相应的共识引擎Tendermint 等SDK 的兴起，与之前的区块链相比，现在已经可以更轻松地创建新的区块链，而区块链创建的下一次演变将由模块化架构实现。例如，一个新的区块链将能够使用SDK 创建，并且能够立即使用现有的模块化区块链。新的区块链可以使用在数据可用性层之上启动的结算层，由于执行层不需要共识机制，因此它们不需要大量的验证集或进行代币分配。新的区块链将能够毫不费力地启动，而无需花费大量时间或金钱成本。

在数据可用性层上启动结算层的区块链像独立的区块链一样具有主权，而结算层之上的Rollups 不具有主权，它们依赖结算层来验证他们的交易。

原始的Rollups 类型的执行层在部署到结算层时，需要对以太坊虚拟机进行兼容。而现在解耦了数据可用性层，可以不处理来自执行层的任何交易或状态更新，仅发布原始交易数据，使得新的Rollups
可以很快地部署到没有兼容限制的数据可用性层。

主权区块链（Sovereign blockchain）：通过社会共识对自身及其应用进行独立控制的区块链。主权链有能力应对黑客攻击并推动升级。

附录


Modular Blockchains
Execution
Fuel
Optimism
polygon Hermez
Scroll
STARKNET
zkSync
ARBITRUM
Aztec
Settlement/Consensus
ethereum
sui
CELESTIA
APTOS
COSMOS
Evmos
Data Availability
zkPorter
CELESTIA
ethereum
STARKEx
Eigenlayr/Datalayr
Polygon Avail
Volt