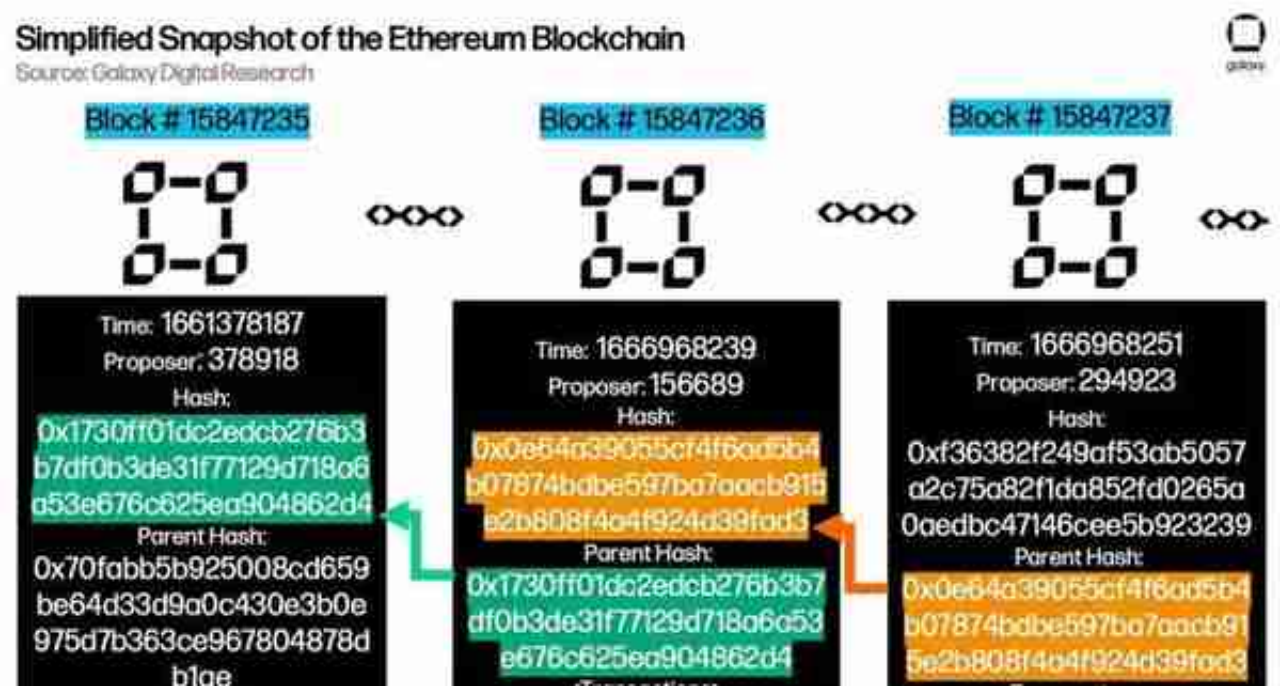


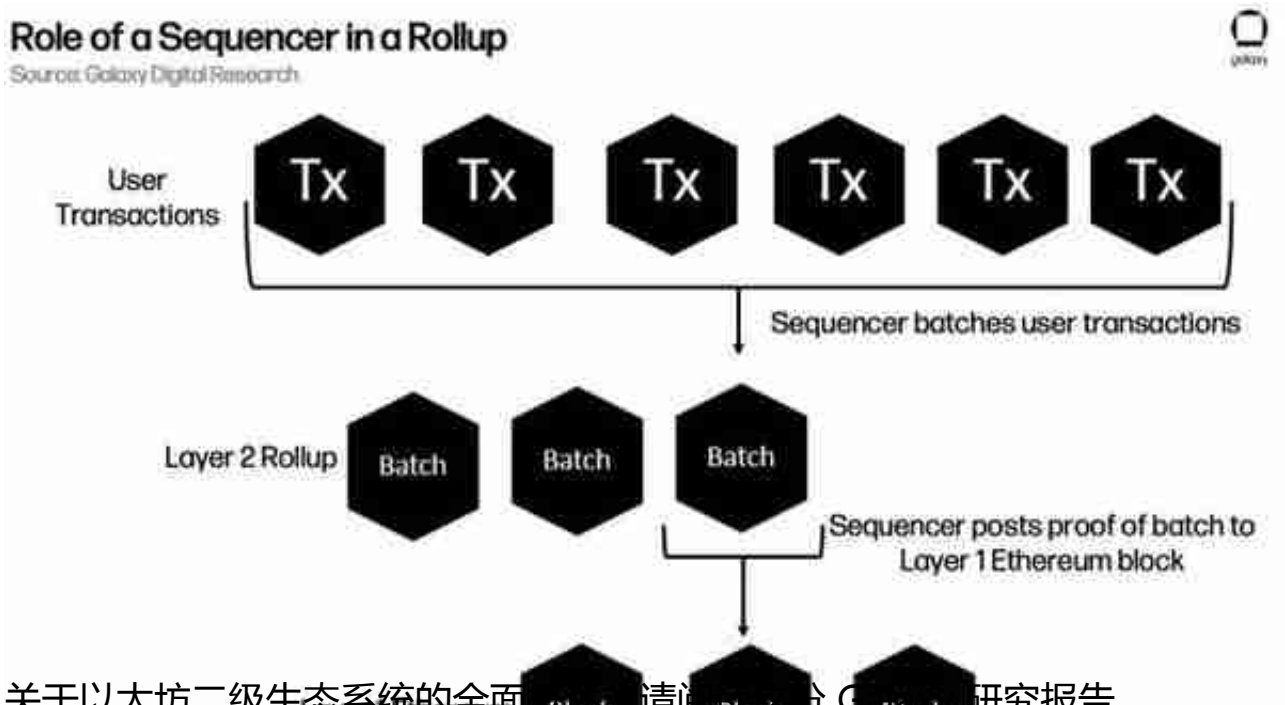
直到 2022 年 9 月 15 日，以太坊依靠工作证明（PoW）共识机制，矿工不是验证者，而是负责区块生产，矿工不是消耗大量资本，而是需要消耗大量电力来处理用户交易。关于 PoS 对以太坊的影响的全面分析，请在这里阅读 Galaxy 的 Merge 研究汇编。

谈到以太坊区块链在 PoW 和 PoS 共识协议下缺乏可扩展性，其根源在于区块空间有限的问题。区块空间在以太坊上是以 gas
为单位衡量的。需要更多计算努力才能执行的交易通常以较高的 gas
单位定价，而计算成本较低（即资源密集度较低）的交易的 gas 成本较低。gas
通过以太坊网络自动设置的动态gas 费率（称为基本费）转换成 ETH.
以太坊协议限制了区块，因此它们最多只能包含 3000 万单位的 gas.
这种最大的区块 gas 限制保留了快速的区块传播时间，并减少了链分裂的风险。关于以太坊的收费动态的更多信息，请阅读这份 Galaxy 研究报告。

以太坊虚拟机

一旦交易被包含在以太坊的区块中，这些交易就会通过一个被称为以太坊虚拟机（EVM）的自定义运行环境来执行。EVM 被设计用来在以太坊上部署任意复杂度的代码。这基本上是使以太坊成为通用区块链的原因，有时也被称为[图灵完备](https://en.wikipedia.org/wiki/Turing_completeness#:~:text=In colloquial usage%2C the terms,purpose computer or computer language.)系统。

EVM 执行事务的方式是有规则的。首先，EVM 将人类可读的编程语言如 Solidity 和 Yul 编译成面向机器的或“低级”的语言，称为 EVM 字节码。然后，EVM 将字节码解析成一系列被称为“操作码”的连续指令。每个操作码命令 EVM 执行一个不同的任务，在 EVM 字节码中以十六进制的形式表示。例如，当智能合约在链上执行时，命令 EVM 保持瞬时数据的操作码在记忆上表示为“MSTORE”，在十六进制形式中表示为“0x52”。为了帮助读者了解操作码的概念，以下是以太坊黄皮书中定义的简单操作码的快照：

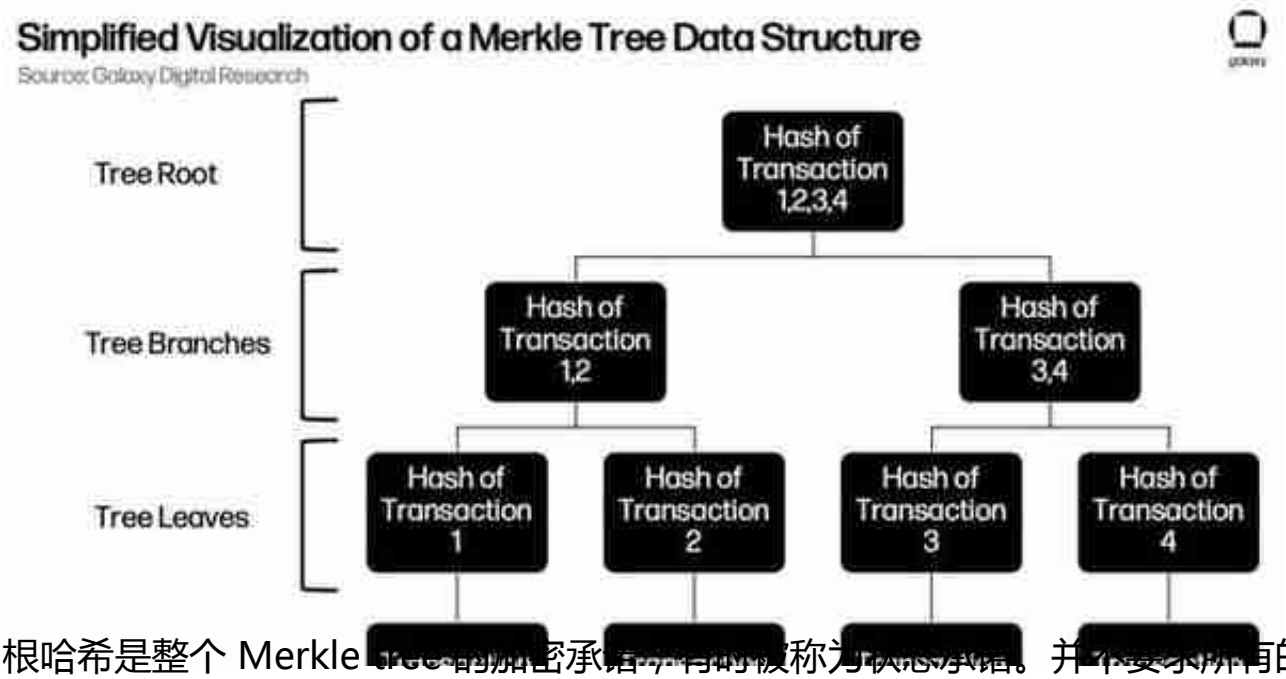


关于以太坊二级生态系统的全面概述，请阅读这份 Galaxy 研究报告。

Rollup 不同于以太坊上的其他扩展解决方案，如等离子体和状态通道，在以太坊的历史过程中，核心开发人员对以太坊的可扩展性路线图进行了研究和废除。主要有两种类型的 rollup：optimistic 和零知识（ZK）。optimistic rollup 依赖于欺诈证明，这意味着对 L2 网络状态的改变被发布到以太坊，而不需要直接证明其有效性。只要至少有一个诚实的行为者在观察 optimistic rollup 的状态转换，无效的状态转换就可以被发现并取消。在 Arbitrum 和 Optimism 的情况下，可以提交欺诈证明的”挑战窗口"持续一个星期。一旦挑战窗口结束，optimistic rollup 的状态转换被认为是最终和有效的。

另一方面，ZK rollup 依靠 ZKP，每次在 L2 上处理一个交易批次时，ZKP 都会生成有效性证明并发布到以太坊。所有交易批次的有效性证明的自动生成增加了 ZK rollup 的安全保障。这也意味着每次新的有效性证明被提交到以太坊时，ZK rollup 的资金就可以被提取，而对于 optimistic rollup，通常有 7 天左右的等待期，以允许争议和欺诈证明的生成。ZK rollup 还提供比 optimistic

rollup 更优越的数据压缩。下面的表格总结了 optimistic rollup 和 ZK rollup 之间的高层区别：



根哈希是整个 Merkle tree 的加密承诺，有时被称为状态承诺。并不要求所有的 ZK rollup
向以太坊提交根哈希值，但为了方便使用以太坊上发布的数据重建和验证 rollup 上执行的交易，他们通常会这样做。

高级根哈希值除了确认第二层区块链的新状态外，还在以太坊上记录了一个加密证明。这个证明可以是 ZKP，或者在 optimistic rollup
的情况下是一个欺诈证明。它可以通过 STARK 或 SNARK
算法生成。最后，除了这两个数据之外，ZK rollup
还向以太坊发布了一个压缩版的分批交易，也称为状态 delta. 状态 delta
是一种具有成本效益的方式，将大量的交易数据提交给以太坊，这是 ZK rollup 所特有的。Optimistic rollup
代替了状态三角洲，使用其他数据压缩技术来批量交易并在链上提交。

（作为一个附带说明，某些 ZK rollup 项目，如 Scroll
团队，实际上并不依赖于向以太坊发布状态 delta 的额外数据压缩收益。在 Scroll 开发者的心目中，即将到来的代码修改，如 Ethereum Improvement Proposal 4844和danksharding将大大降低向以太坊提交交易数据的成本，以至于相对于其他数据压缩技巧，状态延迟的效率提升可以忽略不计。）

使用 Merkle tree 最低层的数据，也就是树上的叶子，并将其与 Merkle tree 最高层的根部哈希值相结合，任何人都可以重建和验证在链上提交的交易批次的内容。大多数滚动的一个决定性特征是能够使用在链上提交给以太坊的数据重新创建在第

二层网络上执行的交易。然而，某些 rollup 避免向以太坊提交状态 delta 或其他压缩的交易数据，而是将数据发布到其他地方，以减少运营成本并提高网络可扩展性。某些开发者会认为，避免向以太坊提交交易数据，从而破坏交易重建的保证的Layer 2 网络不应该被归类为 rollup.

Rollup 处理状态 delta 的方式决定了网络是否可以被归类为有效的或自愿的。

- Validium
  最好理解为只在链上提交有效性证明和根哈希，而在链外的独立网络上存储状态 delta 的 rollup. 这在理论上增加了 rollup 的交易吞吐量至 9000 TPS，因为 rollup
  不再依赖以太坊的数据可用性和受网络的块空间限制。Validium 的缺点是安全性。发布链外数据的独立网络并没有继承与以太坊相同的安全保障。
- Volition 将在链外或链上发布状态 delta
  的决定权交给了用户。它们首先是由以太坊扩展创业公司 Starkware 开创的。这是一种新颖的方式，让用户决定他们的交易是否需要通过直接在链上确认到以太坊或到链外网络（如 Starkware 的可信数据可用性委员会 DAC）来加强安全，也许成本更高。

EVM 等效性的 4 个主要层

给出上述理解以太坊上的交易执行、EVM 和 ZK rollup
的框架，我们现在可以讨论 zkEVM. zkEVM 是 ZK rollup
的一种类型，模拟与主网以太坊相同的交易执行环境。zkEVM
的实施在其证明算法以及数据可用性策略方面有所不同。zkEVM 在其 EVM
等价水平方面也有所不同。有四个主要的 EVM
等价水平。以下是对不同级别的高层次总结：

zkEVM Projects on Ethereum at a Glance

Source: Galaxy Digital Research

	Level of EVM Equivalence	ZK Proving Algorithm	Volition	Smart Contract Language	Open Sourced	Expected Mainnet Launch
zkSync 2.0	Language	SNARK	Yes	Solidity Zinc Compiler	No	EOY 2022
StarkNet + Warp	Language	STARK	Yes	Solidity Cairo Compiler	No	Already available*
Polygon zkEVM	Bytecode (Partial)	SNARK+STARK	TBD	Solidity	Yes**	H1 2023
Scroll	Bytecode (Partial)	SNARK	No	Solidity	Yes	TBD
Privacy Scaling Explorations (Ethereum	Consensus	SNARK	TBD	Solidity	Yes	TBD