5分钟了解以太坊“终局设计”Beam Chain

整理：Karen，Foresight News

以太坊基金会研究员 Justin Drake 在今日 Devcon 大会上提议以太坊的最终设计，其核心在于对以太坊共识层的大规模重新设计。他将这一提议的设计与分叉命名为「Beam」 。那么，Beam Chain 究竟承载着怎样的愿景？其技术架构与实施计划又是如何铺展的呢？

### Beam 愿景

为何要对共识层进行大规模重新设计？Justin Drake 认为，当前的信标链已经过时，其规范在五年前被冻结，加之近年来，在 MEV 缓解、SNARKS（零知识简洁非交互论证）、zKVMs（零知识虚拟机）等领域取得了诸多突破性进展，因此，共识层的重新设计显得尤为迫切。



首先需要指出的是，自 2020 年信标链启动以来，以太坊每年都会迎来一次重要的分叉升级。从 2021 年的同步委员会增加，到 2022 年的合并完成，再到 2023 年的质押提款支持，以及 2024 年的 proto-danksharding，每一步都见证了以太坊的成长与蜕变。而在 2025 年以太坊将实施 Electra 分叉，包括实施 EIP-7251（MaxEB）。在接下来的几年里，以太坊也将进行一些渐进式的分叉。

然而，在这些渐进式分叉之后，Justin Drake 认为，我们或将面临一个前所未有的挑战——Beam 分叉。这是一次共识层的「量子飞跃」，它能够将多个升级整合（batch）到一个单一的分叉中。



值得一提的是，Beam 专门针对共识层，将 blob 和执行层（包含 EVM）排除在外，这是因为修改 blob 和执行层的机会相当有限，另一方面，共识层并不直接被应用程序使用，有比较大的机会进行设计和改变。

在 Beam Chain 共识层路线图中，包括区块生产、质押和密码学三个类别。区块生产方面，通过引入 inclusion lists 实现抵抗审查，将验证者和区块生产流程解耦，还有像执行拍卖这样的想法，另外，也许可以缩短当前的 12 秒 slots 时间。

质押方面，目前研究人员广泛认为，优化当前的发行曲线有机会改善以太坊的整体健康状况。此外，降低成为验证者所需的以太坊质押量，以及实现更快的确定性（finality）也是研究的重点。而在密码学方面，主要是链抽象、量子安全以及 strong randomness 等。



### Beam Chain 技术层

Justin Drake 认为，「PoW、PoS 之后，我们可能正在进入以太坊共识的零知识证明时代。在 ZK 时代，在这个时代，SNARKS 将成为一项不可或缺的技术。整个 Beam Chain，乃至整个共识层都可以进行 SNARK 化处理。这正是 zKVM 大显身手之时。」

值得注意的是，需要进行 SNARK 处理的部分主要是状态转换函数，这是共识客户端的核心所在。而围绕状态转换函数的所有基础设施，如网络、syncing、缓存优化或分叉选择规则等，则无需进行 SNARK 处理。最终，状态转移函数只是整个系统中的一个子集。



在 Beam Chain 中大量使用 SNARKS 的另一个地方是聚合签名——使用哈希函数实现后量子聚合签名（post quantum aggregatable signatures）。Justin Drake 解释称，可以收集成千上万的签名，并将他们压缩成一个证明，结合起来就得到一个基于哈希的后量子可聚合方案，还可以对聚合再进行多次聚合。

除此之外，以太坊还将继续沿用现有的基础设施，包括 libp2p、SimpleSerialiZe、PySpec 以及 Protocol Guild。



### Beam Chain 路线图

Justin Drake 为 Beam Chain 的启动制定了详细的计划，从 2025 年开始会启动相关规格制定过程，2026 年开始构建，而在 2027 年开始，就会启动相关测试，以确保 Beam Chain 达到生产级标准，并且可以安全部署到主网。从下面的路线图来看，主网部署时间可能会在 2029 年、2030 年以后上线。



Justin Drake 打算下一步开始撰写可执行规范，这个规范最终将精简至大约 1000 行 Python 代码。



此外，已有两家客户端开发团队（印度的 Zeam 团队和南美的 Lambda 团队）表示了对 Beam Chain 客户端开发的兴趣。