从Beacon Chain到Beam Chain 速读Justin的以太坊共识层新提案

撰文：Tia，Techub News

在昨日泰国 Devcon 的 Mainstage 中，以太坊研究员 Justin Drake 以演讲的形式完成了对 Beam Chain 提案的首发。Beam Chain 是 Justin 对以太坊共识层进行重新设计的提案，该提案为对 Beacon Chain 的进一步升级，以进一步迈向以太坊最终愿景。本文将带大家速览 Beam Chain 提案改进的目标和与其相关的技术实现。

虽为共识层的重新设计，Beam Chain 将依旧沿用以太坊代币，不会发行新的代币也不会发行新的网络。

## 为什么提议 Beam Chain？

以太坊有三个层级：执行层、blob 数据层、以及共识层。执行层是以太坊中处理交易和执行智能合约的部分，直接管理应用的状态和逻辑。blob 数据层负责存储大量数据，涉及到应用所需的长期数据存储。这两层属于直接和应用交互的层级，任何更改都会直接影响这些层的兼容性。

而共识层主要负责确保整个网络节点间的数据共识，不直接处理应用的状态或数据。这种间接性使得它相对更容易引入创新和升级，不会对应用带来直接影响。因此，像 Beam Chain 提案这样的共识层改进，能够提供创新空间，而不破坏前端应用层的兼容性。

并且，Beacon Chain 是 5 年前的设计，已经非常老旧。经过 5 年时间，市场对 Beacon Chain 的一些错误有了充分认识，对于 MEV 的理解也进一步深入。恰逢 SNARK 技术也有了突破，因此，乘着突破的东风，对以太坊共识层进行一系列修复。

## Beam Chain 计划实现的目标

可以将目标分为三个部分：区块生产、质押、密码学。

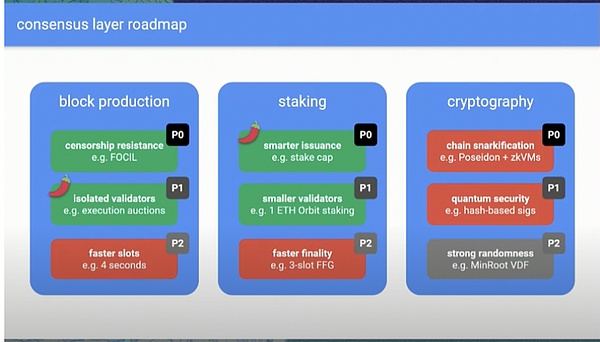
区块生产的目标有三个，主要和 MEV 有关：一是计划用 inclusion list 等增加抗审查性；二是采用 Attester Proposer Seperation 以及执行拍卖等方式将验证者从区块生产中隔离出来；三是实现更快速的 slot，将 slot 时间缩短至 4 秒。

质押部分的目标为对目前的发行曲线进行改进、将质押门槛从 32 ETH 降低到 1 ETH、实现快速最终性 single slot finality。

密码学部分的目标是，使用 zkVM 等实现链的 snarkification；维护以太坊密码学的安全性，使其能够延续数十年甚至数百年；以及使用 MinRoot VDF 等保持强随机性。

对于这些目标的实现方式，Justin 将这类目标进行了两类划分。绿色的部分，以逐步分叉的形式完成，红色的部分应该以整体的方式同时完成。

以 snarkifacation （使用 zk-SNARKs 技术来对数据或计算进行证明）为例，如果想实现 real time proving（实时证明），就必须在系统中做一些结构性调整，包括哈希函数、签名方式、以及序列化和默克尔化（Merkleization）等方面的改变。签名方式需要能够快速生成并完成验证，并且需要序列化使得复杂的数据结构能够在节点之间传输并存储，并将将序列化后的数据进行默克尔树（Merkle Tree）处理，以此满足零知识证明需要对数据进行可验证的格式化和转化，以及对状态的高效验证。



ZK 化的 Beam Chain

过去，以太坊共识经历了从 POW 到 POS 的变更，而在 Beam Chain 的机制里，共识将会有更进一步的更新——完全 ZK 化，即把 snark 应用到整个共识层。

## Chain snarkification

需要强调的是，被 snarkified 的部分只存在于状态转换，但一些基础层面的计算（共识机制在处理事务或状态转换之前所做的逻辑计算）、网络层（节点之间的通信和数据传递）、缓存管理和性能优化则保持不变，不受到 ZK 的影响。

Beam Chain 的实现代码（例如使用 Go 或 Rust 编写的 Beam Chain 的核心逻辑和共识算法代码）需要做的工作就是将代码转换为 zkVM 能理解的格式。Beam Chain 的实现代码被编译为 zkVM 的代码格式后，zkVM 可以执行这些代码，读取区块链外部输入，验证状态转换过程的合法性，并生成零知识证明。

zkVM 是一个执行零知识虚拟机的环境，它能理解特定格式的代码，以便进行零知识证明的验证。将代码编译成 zkVM 可执行的格式的这一过程可能包括将高层语言（如 Go 或 Rust）转换为一个底层的、中间的格式（如 RISC-V 指令集），然后在 zkVM 中执行。

目前，RISC-V 已成为 zkVM 的行业标准。目前有七家公司提供 Risc-v zkVM。

## Attestationsnarkification

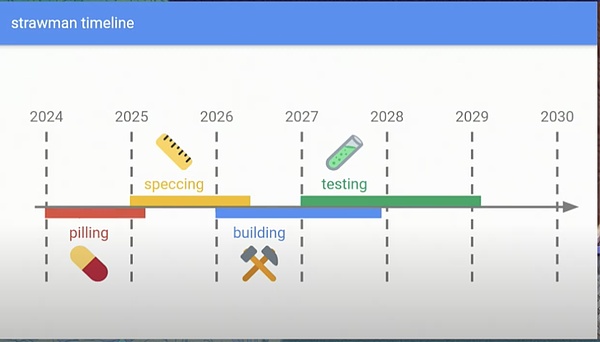
另一个使用到 snark 的部分是聚合签名（aggregatable signatures），即将多个验证者和见证者（attesters）签名的压缩过程，把大量签名聚合成一个单独的、可验证的证明。

我们希望有后量子聚合签名安全性（能抵御量子攻击），因此预计在这里会使用哈希函数。哈希函数具备后量子安全级别，可以用它作为密码学系统的基本组件或基础模块来构建密码学。使用 hash-based snarks，可以将数以千计的签名压缩为一个 proof。这就是后量子聚合签名。并且，这种后量子聚合签名是无限递归的，你可以不断地叠加，将多个聚合签名再度聚合，达到更高的压缩效率，相较于传统 BLS 签名聚合实现了极大的提升。

去几个月里，snark 化的哈希函数技术获得了显著提升，通过笔记本电脑就可快速生成证明，并且每秒可完成约 200 万次哈希操作的证明。这种性能突破让后量子安全的聚合签名方案在现实中变得更为实用，为高效的、量子抗性的加密提供了可能。

不仅如此，snark 化后的 Beam Chain 让原本复杂的验证、存储、计算过程得到压缩，这使得一系列原本不能直接用于 Beacon Chain 的如 libp2p、ssz、pyspec、protocolguild 等基础设施得以实现。

## 时间线规划



时间线的规划上，Justin 计划在 2025 年制定规格，2026 年构建，并在 2027 年进行测试。目前，有两家团队愿意开发 Beam Chain 共识客户端，一家为来自印度的 Zeam lambda，另一家为位于南美的 Lambda。