从 LRT 协议到去中心化基础设施供应商：Puffer 如何对齐以太坊生态？

作者：LindaBell 来源：chainfeeds

根据 Puffer Finance 最新发布的战略路线图，该平台已经从原生流动性再质押协议扩展为以太坊去中心化基础设施供应商。其产品架构也进行了调整，除了 Puffer LRT，还新增了 Based Rollup Puffer UniFi 和预确认解决方案 UniFi AVS。针对这些调整，Puffer 表示，「Puffer 的战略路线图代表了团队在构建支持以太坊增长和弹性所需的基础设施的承诺。从 UniFi AVS 到 PUFI TGE，都经过精心设计以符合以太坊的核心原则。」



### Puffer 的诞生

2023 年 11 月 29 日，Puffer 联创Jason Vranek在 EigenLayer 主办的「Restaking Summit: Istanbul Devconnect」峰会上展示了 Puffer 的 Demo。Puffer 是一个原生流动性再质押协议，其目标是通过设计一个无需许可、降低 Slash 风险的流动性再质押方案，并缓解当前质押市场中存在的中心化和准入门槛过高的问题。

Puffer 创始团队最初的目标是利用可验证技术来降低流动性质押协议中可能存在的罚没（Slash）风险。但受到以太坊基金会研究员 Justin Drake 2022 年在论文「Liquid solo validating」中提出的通过硬件技术降低单独验证者 Slash 风险的方案的启发，Puffer 团队在 2022 年底开发了 Secure Signer 安全签名技术。该技术利用 Intel SGX 将验证者私钥存储在 enclave 中，防止验证者因密钥泄漏或操作失误的 Slash 风险。Secure Signer 的开发获还获得了以太坊基金会 2022 年第四季度的资助。

当然，Puffer 也获得了很多投资机构和天使投资者的关注。截至目前，Puffer Finance 已经完成了 4 轮融资，累计融资金额已经达到了 2415 万美元。2022 年 6 月，Puffer Finance 完成了 Jump Crypto 领投的 65 万美元 Pre-Seed 轮投资。随后于 2023 年 8 月，Puffer Finance 又完成了由 Lemniscap 和 Lightspeed Faction 领投的 550 万美元种子轮融资，Brevan Howard Digital、Bankless Ventures 等参投。此轮融资资金被用于进一步开发 Secure-Signer。而在今年 4 月，Puffer Finance 再度完成1800 万美元 A 轮融资，Brevan Howard Digital 和 Electric Capital 领投，Coinbase Ventures、Kraken Ventures、Consensys、Animoca 和 GSR 等参投。这一轮的融资主要用于推进主网发布。

### Puffer LRT 协议：原生流动性质押协议

流动性再质押代币（LRT）是一种围绕 EigenLayer 生态发展起来的资产类别，旨在通过再质押机制进一步提升以太坊质押资产的资本利用效率。其运作原理是将已经质押在以太坊 PoS 网络上的 ETH 或流动性质押代币（LST）通过 EigenLayer 再质押到其他网络中，以获取以太坊主网质押奖励之外的额外收益。

自以太坊转向 PoS 机制以来，越来越多的质押产品涌现，推动了质押市场的发展。然而，部分平台如 Lido 在质押市场中占据了较大份额，这引发了人们对网络中心化风险的担忧。回顾 2023 年 9 月，在流动性质押领域，Lido 在流动性质押市场的份额一度达到 33%。然而，随着流动性再质押协议的兴起，Lido 的市场份额开始逐步下降，目前已降至 28% 左右。以太坊贡献者Anthony Sasson表示，Puffer 发起的吸血鬼攻击对 Lido 造成了重大冲击，涉及超过 10 亿美元的资金流动。



作为无需许可的去中心化原生流动性再质押协议，Puffer 结合了流动性质押和流动性再质押的双重策略，利用 Secure Signer 安全签名技术和 Validator Tickets（VT）等设计，帮助独立验证者有效参与以太坊质押和再质押过程，从而在提升收益的同时维护以太坊网络的去中心化水平。

此外，为了防止 Puffer 在网络中形成过度中心化的情况，该协议严格限制其验证节点数量，不允许其占据以太坊总网络节点数量的 22% 以上，以确保对以太坊的可信中立性不构成威胁。

#### 将质押准入门槛从 32 枚以太坊降至最低 1 枚

以太坊成为节点需要 32 枚 ETH，这对于独立用户而言无疑是一个较高的门槛。而 Puffer 通过一种称为 Validator Tickets (VT) 的机制，降低了参与质押的准入门槛，使得节点操作者只需提供 2 枚 ETH 的保证金（如果使用 SGX，只需要 1 枚 ETH）即可运行验证节点。VT 是一种 ERC20 代币，代表节点操作者运行以太坊验证器的一天权利，而 VT 的价格则是根据运行验证器的预期每日收益设定。也就是说，节点操作者需要锁定一定数量的 VT 才能参与质押，并在质押期间逐渐释放给流动性提供者，同时验证者可以获得 PoS 产生的全部奖励。

举个简单的例子，类似于加盟餐厅时，用户可以选择按月支付收益或提前一次性支付未来一年内的预期收益来获得运营权，而 Puffer 的 VT 机制便是后者的模式。同时，节点运营者可以获得 100% 的 PoS 奖励，从而避免传统质押模式中因收益不足而导致的「懒惰节点」现象（即在收益不理想时选择消极参与或退出共识）。此外，VT 作为一种权益票据，不仅能够补充质押资金，还具有流动性，可以在二级市场上进行交易。



#### 通过 EigenLayer 实现双重收益

Puffer 是一个原生流动性质押协议。这里的「原生」指的是用户除了参与以太坊 PoS 共识外，还可以直接将 ETH 用于再质押。这意味着质押者不仅能够从以太坊 PoS 中获得验证奖励，还能够通过再质押机制获得额外的收益，实现双重回报。此外，与传统流动性再质押产品不同，Puffer 不依赖第三方流动性提供者，而是直接使用原生验证者的 ETH 进行再质押，避免了由少数大型质押实体主导可能带来的中心化问题。通过这一方式，Puffer 不仅提升了收益率，还增强了网络的去中心化。目前，Puffer 的总锁仓价值已达到 8.596 亿美元，年化收益率为 3%。



#### 借助 Secure-signer 与 RAVe 防范 Slash 风险

Puffer 通过 Secure-signer 及 RAVe（Remote Attestation Verification） 远程证明技术来有效防范验证者因操作错误而导致的 Slash 处罚。其中，Secure-Signer 基于 Intel SGX 硬件安全技术的远程签名工具，能够在 enclave 中生成、存储和执行签名操作，从而防止验证者因双重签名或其他签名错误而遭受 Slash 处罚。而 RAVe 技术的作用是为了验证这些 Intel SGX 生成的远程证明报告，确保节点确实在运行经过验证的 Secure-Signer 程序。通过验证后，系统会在链上记录其验证者密钥状态，从而防止恶意节点使用未经验证的代码或替换关键操作逻辑。

值得一提的是，作为一种公共物品，Secure Signer 代码已经开源，目前可以在Github上查看。

Puffer 已于今年 5 月 9 日启动了主网。而为了进一步提升以太坊网络的去中心化，Puffer 计划在今年第四季度发布 V2 版本。此次升级侧重于增强用户体验，并引入了几个关键功能：

快速路径奖励 (FPR)：允许用户直接从 L2 提取共识层奖励，避免了在 EigenPod 提取过程中因 Gas 费用过高而导致的成本的问题。

全局强制反 Slash：Puffer V2 将实施协议范围内的抗 Slash 机制，进一步提升网络的安全性和去中心化水平

降低保证金要求：Puffer V2 还降低了 NoOps（非运营节点）对保证金的要求，仅需少量的 pufETH 抵押品来应对因不活跃而导致的 Slash 风险。

### Puffer UniFi：通过 UniFi AVS 实现 100 毫秒交易确认

今年 7 月 6 日，Puffer 发布了其 Based Rollup 方案 Puffer UniFi 的 Litepaper。作为 Based Rollup，UniFi 通过利用以太坊验证者进行交易排序，同时将交易价值回馈给 L1，从而提升了以太坊网络的安全性和去中心化水平。

自从以太坊推行「以 Rollup 为中心」的路线图以来，市场上涌现了大量 L2 解决方案。据 L2Beat 数据显示，目前市场上 Rollup 数量已经超过 100 个。然而，这些扩展方案虽然在一定程度上提升了以太坊的扩展性和用户体验，但同时也带来了流动性割裂和中心化排序器等问题。首先是流动性割裂问题，由于不同 Rollup 之间缺乏互操作性，流动性和用户被分散在各个独立的 L2 网络中，导致整体生态难以形成有效的协同效应。而且用户在不同 Rollup 之间进行资产转移时需要依赖跨链桥，不仅增加了操作成本，还存在一定的安全风险。此外，当前大部分 Rollup 使用的是中心化排序器，这些排序器通过 MEV 从用户交易中提取额外租金，也会对用户交易体验产生影响。

Puffer 的 UniFi 方案则希望通过基于验证者的去中心化交易排序来解决这些问题。与传统的中心化排序方案不同，UniFi 的交易虽然是由 Puffer 节点处理，但这些节点本身是以太坊的原生质押节点，因此 UniFi 方案将交易排序权利分配给去中心化的验证者，充分利用了以太坊的安全性和去中心化特性。



延伸阅读「能继承以太坊活性的 Based Rollup 是什么？」

此外，UniFi 还通过同步可组合性（Synchronous Composability）和原子可组合性（Atomic Composability）来应对流动性割裂的问题。基于 UniFi 的应用可以依赖其提供的排序和预确认机制，因此能够与其他同样 Based L1 排序的 Rollup 或应用链实现无缝互操作。同时，通过使用 Puffer 的 TEE-multiprover 技术，UniFi 还能够实现与 L1 的原子级别组合性，即 UniFi 允许即时 L1 结算，并且可以直接访问 L1 流动性，以提升跨层交易和应用的效率，方便开发者构建更高效的应用。

然而，虽然 Based Rollup 将交易排序交由 L1 验证者避免了中心化排序器带来的风险。但其交易确认速度依然受限于 L1 的出块时间（约 12 秒），导致无法实现快速确认。为解决这个问题，Puffer 引入了基于 EigenLayer 的 AVS 服务，为 UniFi 提供了预确认机制，实现了 100 毫秒的交易确认时间。

延伸阅读「为什么 Based Rollup 需要预确认（Preconfs）技术？」

在 Puffer UniFi AVS 中，通过 EigenLayer 的再质押机制，验证者能够将他们在以太坊主网质押的 ETH 同时用于 UniFi 的预确认验证服务，而无需额外质押新资金。这在一定程度上提高了资金的利用效率，并降低了参与的门槛。且 UniFi AVS 利用了以太坊主网的经济安全性。如果参与预确认的验证者不遵守承诺，自然会面临其在主网上质押的 ETH 被罚没的风险，因此无需为 Puffer 的预确认机制再设计额外的罚没措施。

要参与 Puffer UniFi AVS 的验证者必须具备 EigenPod 所有权，以确保 UniFi AVS 服务可以执行 Slash 惩罚，从而约束违反预确认承诺的验证节点行为。此外，节点运营商需在其验证者客户端所在的服务器或环境中运行 Commit-Boost，负责处理验证者和预确认供应链之间的通信。

上线短短两周内，UniFi AVS 平台已经获得了 105 万枚 ETH的质押，并且有超过 32,000 名验证者参与其中。未来，Puffer 还计划结合以太坊基金会的中立注册合约机制，允许任何 L1 提议者自愿注册为预确认验证节点。这意味着，以太坊主网上的每个验证者都可以选择成为预确认验证者，从而进一步扩展系统的去中心化程度。



### 总结

随着以太坊生态的逐渐壮大，如何确保各项目和参与者朝着同一目标努力成为了社区长期关注的核心问题。这种一致性（Ethereum alignment）被认为是以太坊网络长期成功的关键。早期，社区将其分解为「文化对齐」、「技术对齐」和「经济对齐」三个维度，而 Vitalik Buterin 在其近期文章「Making Ethereum Alignment Legible」中又提出了一套新的衡量标准，包括开源性、开放标准、去中心化与安全性、以及「正和效应」。当然，无论采用何种标准，其核心目标都是确保协议、社区和项目能够与以太坊的整体发展方向保持一致，从而为生态系统的可持续发展提供正向支持。

值得肯定的是，Puffer 在设计和产品演进中始终践行了与以太坊一致的原则，并展现了对以太坊长期愿景的支持。通过与 EigenLayer 的集成，Puffer 使得更多的独立验证者能够参与质押网络，从而提升了以太坊去中心化水平。而 Puffer 的 UniFi 方案将交易排序权交还给以太坊原生质押节点，在安全性及去中心化等方面对齐了以太坊。

目前，Puffer Finance 已经发布了其代币经济学，其中 7500 万枚 PUFFER 代币（占总供应量的 7.5%）将用于 Crunchy Carrot Quest 第一季的空投活动。第一季空投的资格快照已于 2024 年 10 月 5 日完成，用户可在 2024 年 10 月 14 日至 2025 年 1 月 14 日期间通过代币申领门户进行领取。随着 PUFFER 代币的正式推出，Puffer 能否在推进其与以太坊保持一致性目标的同时，实现进一步的去中心化和用户增长，值得持续关注。