AR-ACE：基于 ACE-GF 的后量子密码学（PQC）证明中继——无需在传播路径上携带证明的轻量级内存池传播

Jian Sheng
Wang Yeah LLC
jason@yeah.app

2026年3月9日

arXiv:2603.07982v1 [cs.CR] 9 Mar 2026

摘要

在后量子区块链环境中，需要有效性证明的对象（例如 Blob 根、执行层或共识层签名聚合值）必须通过内存池和中继网络进行广播。人们提出使用递归 STARK 将此类证明聚合起来，使每个节点每个时隙转发一个证明以及不带证明的对象，从而将每个节点的证明带宽限制在每个时隙约 128 KB $\times$ 度。我们观察到，传播本身并不要求在路径上携带有效性证明——只需提供对象有资格进行中继的轻量级保证即可。我们提出 **AR-ACE**（基于 ACE-GF 的后量子密码学证明中继），在该方案中，中继节点转发对象及紧凑证明（例如身份绑定签名或承诺），且不生成、持有或转发任何完整有效性证明。只有构建者（或最终验证者）会针对其纳入的对象集合执行一次聚合有效性证明。这种证明脱离传播路径的设计彻底消除了传播路径上的证明开销；与携带证明的传播相比，可将证明相关的中继带宽降低一个数量级。采用源自 ACE-GF 的证明密钥后，AR-ACE 通过链上授权保持统一身份体系，并支持后量子密码学。我们规定了协议模型，阐述设计目标和安全考量，定义安全性游戏，并与基于递归 STARK 的传播方案进行结构带宽比较。

关键词。 后量子密码学、内存池传播、带宽效率、证明中继、ACE-GF、证明脱离传播路径、确定性身份。

1 引言

1.1 后量子内存池中的带宽问题

在分布式区块构建中，大量对象——例如 Blob 根（具备纠删码正确性）、执行层交易或共识层签名聚合——必须被广播，以便构建器能够发现并纳入它们。在后量子环境中，椭圆曲线 SNARK 可能被视为不适用；STARK[5] 是证明这些对象有效性的自然替代方案。然而，即便在经过体积优化的实现中，单个 STARK 证明的大小也在 128 KB 量级。如果每个对象都连同其完整的 STARK 证明一起传播，中间内存池节点以及构建者的带宽需求将随对象数量线性增长，很快变得难以承受。

Buterin [1] 提出通过递归 *STARK*来解决这一问题：每个内存池节点定期生成一个递归 STARK，证明其当前持有的所有对象均有效，并且

向每个对等节点转发这一份证明，以及尚未发送给该对等节点的任何对象（不附带证明）。关键结果是，每个节点的证明带宽不再随对象数量增加而增长，而是保持恒定：大致每个时隙向每个对等节点发送一份 STARK（例如，每个节点每 0.5 s ≈ 2发送 128 KB $\times 8$，即 MB/s），而对象载荷仍按现状传输。这解决了证明流量激增的问题，是一种有效且优雅的解决方案。

1.2 关键观察：传播路径上必须证明什么？

我们提出一个更根本的问题：传播路径上究竟一定要有有效性证明吗？

中继节点需要决定是否接受并转发对象。这个决定可以基于：

- 对象的<纳style id='2'>完整有效性证明（例如 STARK）——这是携带证明和递归 STARK 传播方法的基础；或者
- 能够证明对象符合中继条件的轻量级凭证（例如，提交者或证明服务认证该对象格式正确且值得中继），而无需在传播路径上证明其完整有效性。

如果我们采用第二种观点，那么只有在构建者纳入对象时才会证明其有效性——例如，构建者针对其选定的对象集合运行一个聚合 STARK（或等效证明）。传播只需携带对象和一份小型证明（签名、承诺或保证金引用）。我们称之为证明脱离传播路径传播：证明不经过中继路径，只有构建者会看到或生成这些证明。

其基本原则具有普适性：当某个重量级密码学凭证（证明、签名）必须在最终阶段验证时，就不必让它经过每一个中间跳。相反，中间节点只需验证足以确认中继资格的轻量级凭证，并将重量级验证推迟到端点（此处为构建者）。我们不在中继路径上携带有效性证明，而是携带证明，并将证明验证推迟到构建者处。

1.3 贡献

1. 我们提出 AR-ACE（基于 ACE-GF 的后量子密码学证明中继），这是一种传播设计：中继节点转发对象及其紧凑证明，且不生成、持有或转发完整有效性证明。2. 我们规范了证明脱离传播路径的协议模型：其中定义了各角色（提交者、中继节点、构建者）和证明凭证，并规定只有构建者执行聚合有效性验证。3. 我们阐述设计目标（带宽效率、垃圾信息抵抗，以及证明与对象和身份的绑定），定义安全游戏（证明伪造、重放、准入绕过），并讨论基于证明的中继所涉及的安全考量。4. 我们提供结构带宽比较，表明 AR-ACE 完全从传播路径中移除证明流量；相较于携带证明的传播方式，这使证明相关的中继带宽减少了一个数量级，同时仍兼容由构建者生成单个聚合证明。5. 我们介绍了使用 ACE-GF 实例化证明凭证的优势：通过链上授权实现统一身份、上下文隔离、面向后量子密码学的派生，以及将授权与中继证明共用单一根。

1.4 与 ACE-GF 的关系

AR-ACE 不要求ACE-GF：路径外证明架构可以通过任何提供紧凑证明的机制来实例化（例如 BLS签名、Ed25519、保证金引用）。当使用 ACE-GF派生密钥[2] 进行证明时，我们获得了一个统一的叙述：

支持链上授权的同一身份根可以为内存池中继派生专用证明密钥，同时实现上下文隔离和面向后量子密码学的流。本文将 AR-ACE 作为通用设计，并强调 ACE-GF 实例化是实现身份一致性和后量子一致性的首选方案。

1.5 论文结构

第 2 节综述相关工作。第 3 节给出符号和假设。第 4 节阐述问题和设计目标。第 5 节介绍 AR-ACE 设计。第 6 节讨论安全性，包括威胁模型和安全游戏。第 7 节比较带宽并概述实用优化方向。第 8 节总结 ACE-GF 的优势。第 9 节总结全文。

2 相关工作

递归 STARK 内存池。 Buterin [1] 提出了递归 STARK [5]，使每个节点每个时隙生成一个证明，以证明其所知的所有对象均有效；对象则在不附带证明的情况下发送。这项技术基于递归证明组合 [7, 6]。它限制了每个节点的证明带宽，但仍要求每个节点生成并转发 STARK。我们的方法彻底移除传输路径上的证明；仅由构建者生成（或验证）聚合证明。

以身份为中心的授权。 一种新兴的后量子区块链授权方法以身份绑定零知识证明取代大型链上签名对象，以证明授权语义，从而将链上数据量减少一个数量级。AR-ACE 将同一原则应用于中继层：我们不压缩庞大的证明对象，而是改变传输路径上验证的内容 （资格证明，而非有效性证明），并将繁重的验证工作推迟到构建者执行。

数据可用性与 Blob。 EIP-4844 [3]引入了 Blob 交易和数据可用性采样（DAS）。Blob 根及其有效性的传播（例如纠删码正确性），是递归 STARK 传播和 AR-ACE 的一种应用场景。我们的设计不依赖于具体的有效性谓词；我们只要求构建者最终能够在单个聚合证明中验证纳入情况。

点对点 Gossip 与中继网络。 </style}现代区块链内存池传播依赖结构化 Gossip 协议，例如 GossipSub [13], 。该协议基于 Kademlia [14] 等分布式哈希表（DHT），在非结构化覆盖网络上实现具备抗攻击能力的消息传播。AR-ACE 不依赖于底层 Gossip 拓扑；它只要求中继节点在转发前验证证明。

账户抽象与中继者。 ERC-4337 [4] 和中继者/打包器架构将签名或授权的实体与提交交易的实体分离。AR-ACE 兼容这种分离：证明可以由提交者生成，也可以由持有专用证明密钥的中继者生成（例如，该密钥可在中继专用上下文中从 ACE-GF 派生）。

3 预备知识与假设

3.1 符号说明

- λ：安全参数。

- objHash：使用抗碰撞哈希对对象（Blob 根、交易或聚合值）计算得到的哈希。
- 证明：证明凭证（例如，对 objHash 的签名，或将对象与身份绑定的承诺）。
- 域：域分隔符（链、内存池实例或应用）。
- REV：根熵值（ACE-GF 身份根）；使用 ACE-GF 时，会基于 REV 在中继专用上下文中派生证明密钥。
- 中继路径：从提交者到构建者的节点序列。路径上指位于此路径上；路径外指不在此路径上（例如，仅位于构建者处）。

3.2 假定的 ACE-GF 接口（使用时）

将 AR-ACE 与 ACE-GF [2], 实例化时，我们假定其提供以下黑盒接口：具有上下文隔离的确定性密钥派生 Key $\leftarrow$ Derive(REV，Ctx)。证明时，我们使用专用上下文，例如 $\text{Ctx}^{\text{relay}}$ =(算法标识符，MEMPOOL-ATTEST，域)，从而使证明密钥与签名、加密或链上授权密钥隔离。无需持久化存储 REV；生成证明时临时派生证明密钥。

3.3 网络与角色模型

- **提交者**：生成对象（例如 Blob 根、交易）以及将自身（或其身份承诺）绑定到 objHash（以及可选的域、随机数）的证明。将（obj，证明）发送至内存池。
- **中继节点**：从对等节点或提交者处接收（obj，证明）。验证证明对于 objHash（以及域）是否有效，并确认对象尚未过期或被丢弃。它们不验证完整有效性（例如纠删码、签名聚合正确性）。将（obj，证明）转发给其对等节点。它们不会生成或转发任何 STARK 或其他有效性证明。
- **构建者**：从网络收集（obj，证明）。选择一组要纳入的对象。针对所纳入的对象集生成或验证一个聚合有效性证明（例如递归 STARK）。将区块（或批次）与这一份证明一同发布。

4 问题陈述与设计目标

4.1 带宽问题

我们要解决的带宽问题如下：许多对象必须进行广播，以便构建者能够将其纳入。每个对象都关联一个有效性谓词（例如，纠删码正确、签名有效）。在后量子环境中，可以使用 STARK 证明有效性；单个 STARK 大小为 $\approx$128KB。如果每个对象都连同其证明一起传播，中继带宽将随对象数量增长至 O(#objects $\times$ 128KB)。递归 STARK 聚合 [1] 可将每个节点每个时隙的证明流量降至 O(1)（每个对等节点每个时隙一个证明），但每个节点仍必须生成并发送 STARK。我们的目标是在保留仅有效对象才能被构建者纳入这一保证的同时，彻底消除中继路径上的证明流量。

4.2 设计目标

- **带宽效率**。 中继节点不得发送或接收完整有效性证明。路径上仅传输对象和紧凑证明（例如，每个对象几十到几百字节）。
- **垃圾信息抵抗**。 证明必须具有足够高的成本（或受到速率限制），以使匿名垃圾信息难以实施。可选方案包括：将证明密钥绑定到身份或质押、为每次证明缴纳少量保证金，或对每个证明密钥实施速率限制。

- **绑定**。 证明必须绑定到对象哈希（并可选择绑定到域），以防止证明在不同对象或域上被重放。

- **纳入时有效性**。 构建者通过单个聚合证明验证纳入对象的有效性。无需考虑任何没有有效证明的对象；构建者还可以要求证明来自合格密钥或承诺。

- **兼容性**。 该设计应与现有的有效性谓词（纠删码、签名聚合）以及构建者处的单个聚合证明（例如递归 STARK）兼容。

最小准入策略模型（针对本文）。 为明确垃圾信息防护假设，我们假设中继采用最小准入策略：(i) 仅准入来自合格密钥（已注册或已提供保证金）的证明；(ii) 每个合格密钥拥有每纪元配额；(iii) 策略违规将触发丢弃，并暂时列入拒绝列表。本文不优化策略经济学；仅要求准入策略可执行，且成本足够高，使大规模垃圾信息发送并非零成本。

5 AR-ACE 设计

5.1 证明凭证

证明 Attest 是一种紧凑凭证，用于将证明者（例如身份或公钥）绑定至对象哈希 objHash，并可选择绑定至域以及随机数或重放令牌。具体而言，Attest 可以是：

- 使用具备 EUF-CMA 安全性的标准签名方案，对消息 $m = \text{objHash}\|\text{domain}\|\text{nonce}$（或其规范编码）使用密钥 pk 进行签名 σ [11]。路径上的验证会检查 Verify(pk m， σ)，并可选择检查 pk 是否属于允许集合，或是否派生自已承诺身份。

- 使用 ACE-GF 时：pk 是与 Derive(REV，上下文$_{\text{中继}}$) 对应的公钥。为链上身份承诺提供支持的同一 REV 会在独立上下文中派生中继密钥，因此，仅用于中继的密钥遭到泄露不会暴露授权密钥。

大小：一个签名（例如，Ed25519 [9] 64 字节；若证明采用后量子密码学，则 ML-DSA [8] 级别为 2 ≈2.4 KB），外加可选的 pk 或承诺。

部署配置。配置 A（混合性能）： 路径上的证明采用较短的经典签名（例如 Ed25519 [9] 或 BLS [10]），以尽量减少带宽和中继 CPU 开销；后量子密码学安全性则由纳入和最终验证层保障。

配置 B（全后量子密码）： 链路上的证明使用后量子密码签名（例如 ML-DSA [8]），这会增加每个对象的字节数，但能确保中继路径完全符合后量子密码学。

5.2 传播协议

1. 提交者计算对象哈希 $= H(\text{obj})$，生成证明（签名或承诺），将对象哈希、域和可选随机数绑定在一起。将 (obj,Attest) 发送给一个或多个中继节点。 2. 中继节点：收到 (obj,Attest) 后，验证对象哈希和域对应的证明；检查重放/过期情况。不 验证完整有效性（不验证 STARK，也不进行纠删码检查）。将 (obj,Attest) 转发给尚未收到该对象的对等节点。 3. 构建者：订阅或从网络拉取对象（及其证明）。选择一组S 要纳入的对象。可选择丢弃不再符合纳入条件的对象。为 S 生成一个聚合有效性证明 Π （例如，递归 STARK：“ S中的所有对象都满足有效性谓词”）。发布包含 S 和 Π的区块/批次。区块验证会检查 Π；链上不会验证每个对象的证明。

算法 1 对这三个角色进行了形式化定义。

算法 1 AR-ACE 传播协议

参数：签名方案（密钥生成，签名，验证），哈希 H，域 domain，合格密钥集合 $\mathcal{E}$，每键配额 Q

提交者(obj，sk)1：objHash $\leftarrow H$(obj)2：nonce $\leftarrow$ 新鲜的重放令牌3：$m \leftarrow$ objHash$\|$域$\|$nonce4：证明 $\leftarrow$ 签名(sk m)5：**发送** (obj，证明，pk，nonce) 给中继节点

中继（收到 (obj, 证明, pk, nonce)）6：objHash $\leftarrow H$**(obj) 7：** $m \leftarrow$**objHash**$\|$**域**$\|$**nonce 8：如果 pk** $\notin \mathcal{E}$ **则丢弃并返回 9：结束 if 10：如果配额[pk** $] \geq Q$ **则丢弃并返回 11：结束 if 12：如果 nonce 之前已出现，则丢弃并返回 13：结束 if 14：如果验证(pk** m**, 证明)** $= 0$ **则丢弃并返回 15：结束 if 16：配额[pk]** $\leftarrow$ **配额[pk]** $+ 1$**17：记录 nonce 18：将 (obj, 证明, pk, nonce) 转发给尚未服务过的对等节点**

构建者（对象池 $\mathcal{P}$）19：$S \leftarrow$ 从 $\mathcal{P}$ 按策略选择对象20：$\Pi \leftarrow$ 聚合证明($\{$(对象，有效性谓词)：对象 $\in S\}$）21：**如果** Π 有效**，则发布**区块(S，Π)22：**结束 if**

5.3 路径上的流量

在中继路径的每条链路上：

- **传输内容：**对象（保持不变）和证明（大小固定）。没有 STARK，也没有递归证明。
- **不传输：**任何有效性证明。证明仅存在于构建者处（聚合值的输出）以及已发布区块中。

因此具有证明脱离传播路径这一属性：有效性证明不在传播路径上。

5.4 ACE-GF 实例化（摘要）

当通过 ACE-GF 派生证明密钥时：

- 使用 Ctx$_{\text{中继}}$ =(算法标识符，MEMPOOL-ATTEST，域)，使中继证明位于独立的流中。

- 同一个 REV（由密封工件和凭证重建）既可支持链上身份承诺，也可派生 sk$_{\text{中继}}$。一个根，一份备份；无需额外的密钥管理。
- 可选：在用于证明的上下文$_{\text{中继}}$中使用后量子密码算法（例如 ML-DSA），使整个路径保持后量子密码一致；这样证明会更大，但仍远小于 STARK，并且路径上不会传输证明。

6 安全考量

6.1 威胁模型与安全博弈

我们考虑一个能够完全查看内存池流量，并且可以提交、重放和重新排序中继对象的概率多项式时间敌手。安全性通过遵循基于代码的博弈证明框架 [12] 的三个博弈来表述。

博弈 $\mathsf{G}_{\mathsf{forge}}$ **（证明伪造）**。挑战者公开资格元数据，并提供针对合格密钥有效证明的预言机访问。若对手输出的 (obj，Attest) 通过了针对某个合格密钥的中继验证，且对手未查询过该消息，则对手获胜。优势为

$$\mathsf{Adv}^{\mathsf{forge}}_{AR-ACE}(\lambda) = \Pr[\mathsf{G}_{\mathsf{forge}} = 1].$$

博弈 $\mathsf{G}_{\mathsf{replay}}$ **（跨域／重放滥用）**。对手观察有效证明；若其在不同的 (objHash，域，随机数) 元组上重用某个证明，且仍通过中继检查，则对手获胜。优势为

$$\mathsf{Adv}^{\mathsf{replay}}_{AR-ACE}(\lambda) = \Pr[\mathsf{G}_{\mathsf{replay}} = 1].$$

博弈 $\mathsf{G}_{\mathsf{admit}}$ **（违反策略的准入绕过）**。根据第 4.2 节的准入策略，若对手输出的 (obj，Attest) 被诚实中继接受并转发，尽管违反了该策略（使用不合格密钥、违反配额或使用拒绝名单密钥），则对手获胜。优势为

$$\mathsf{Adv}^{\mathsf{admit}}_{AR-ACE}(\lambda) = \Pr[\mathsf{G}_{\mathsf{admit}} = 1].$$

准入假设的可执行接口。为使准入界限在模型层面可由机器检查，我们通过明确的实验定义这三个术语：

- $\mathsf{Adv}_{\mathsf{meta}}(\lambda)$：在 $\mathsf{G}_{\mathsf{meta}}$ 中的优势，即敌手输出被诚实中继接受、但在同一纪元内未经元数据根/签名机构授权的资格元数据（或更新记录）。
- $\mathsf{Adv}_{\mathsf{state}}(\lambda)$：在 $\mathsf{G}_{\mathsf{state}}$ 中，诚实中继状态转移在可接纳事件轨迹下违反指定准入状态机（配额计数器、临时数集合、纪元重置）的概率。
- $\mathsf{Adv}_{\mathsf{net}}(\lambda)$：在 $\mathsf{G}_{\mathsf{net}}$ 中的优势，即在途消息修改改变了与准入相关的字段（密钥标识、随机数、域、纪元标签），但仍通过端点完整性检查。

这三者均由具体的中继实现与网络信道假设加以参数化；它们可以直接在仿真或模型检测框架中实例化。

定理 6.1（中继路径认证与抗重放）**.** 假设证明签名方案的 *EUF-CMA* 安全性 *[11]*、 H的抗碰撞性，以及签名消息中严格的域与临时数绑定。则

$$\mathsf{Adv}^{\mathsf{forge}}_{AR-ACE}(\lambda) + \mathsf{Adv}^{\mathsf{replay}}_{AR-ACE}(\lambda) \le \mathsf{negl}(\lambda).$$

证明概要。 成功的伪造意味着对该签名方案发起了一次 EUF-CMA 伪造。若在 (objHash，域，随机数) 元组之间成功重放或替换，则意味着要么在不同消息上重复使用了有效签名（同样构成 EUF-CMA 攻击），要么发生了哈希碰撞或域绑定失败。根据标准归约和并集界，这两种优势均可忽略。形式化地，$\mathsf{Adv}^{\mathsf{forge}}_{AR-ACE}(\lambda) + \mathsf{Adv}^{\mathsf{replay}}_{AR-ACE}(\lambda)$ 的上界为针对证明签名方案的 EUF-CMA 优势与针对 H 的寻找碰撞优势之和；二者在 λ 中均可忽略。

□

定理 6.2 (准入策略可靠性**)**。 假设：*(i)* 资格元数据（合格密钥集合、拒绝列表、纪元参数）经过认证，其遭篡改的优势为 $\mathsf{Adv}^{\mathsf{meta}}(\lambda)$；*(ii)* 诚实中继正确执行配额/随机数状态，且不一致概率为 $\mathsf{Adv}^{\mathsf{state}}(\lambda)$；以及 *(iii)* 网络完整性可抵御传输中的准入字段篡改，其优势为 $\mathsf{Adv}^{\mathsf{net}}(\lambda)$。则

$$\mathsf{Adv}^{\mathsf{admit}}_{AR-ACE}(\lambda) \le \mathsf{Adv}^{\mathsf{meta}}(\lambda) + \mathsf{Adv}^{\mathsf{state}}(\lambda) + \mathsf{Adv}^{\mathsf{net}}(\lambda).$$

特别是，如果这三个项在 λ 中均可忽略，则 $\mathsf{Adv}^{\mathsf{admit}}_{AR-ACE}(\lambda) \le \mathsf{negl}(\lambda)$。

证明概要。 只有在以下至少一种情况发生时，才可能出现准入绕过：元数据遭到伪造或过期，导致不合格密钥看似符合资格；中继状态不一致，导致配额或随机数检查被跳过；或者传输过程中准入相关字段被修改而未被检测到。这些事件通过并集界给出 $\mathsf{G}_{\mathsf{admit}}$ 的上界，从而得到所述不等式。 □

命题 6.1 (证明脱离传播路径下的纳入安全性**)**。 如果共识会拒绝包含无效聚合证明 Π 的区块，那么无论中继路径准入结果如何，任何不满足有效性谓词的对象都无法被最终确定。

证明概要。 中继准入影响传播，而非最终有效性。最终确定要求对纳入对象的 Π 有效。任何无效对象都会使 Π 无效，从而导致共识拒绝。 □

6.2 中继完整性

中继节点只转发 (obj，证明)。它们无需信任提交者来保证有效性；只需验证证明格式正确，且与对象哈希和域绑定。无效或格式错误的对象仍可能被转发；构建者会在构建聚合证明时拒绝这些对象（只有有效对象才能纳入有效的 Π）。因此，中继节点不会成为有效性检查的瓶颈，纳入安全性则由构建者的证明来保障。

6.3 垃圾信息与拒绝服务攻击

如果证明的成本很低（例如，任何人都能创建密钥并进行签名），那么垃圾信息（obj，证明）可能会淹没网络。缓解措施包括：(i) 将证明密钥与质押或身份承诺关联（例如，仅允许已注册或已抵押的密钥）；(ii) 按密钥或承诺进行速率限制；(iii) 为每次证明收取少量保证金或费用。这些属于协议层面的选择；AR-ACE 只要求证明内容简洁且可验证。

6.4 绑定与重放

证明必须绑定到对象哈希（以及域），以防针对一个对象的证明被用于另一个对象。签名消息中的随机数或序列号可防止在不同时间或上下文中重复使用同一对象的同一证明。域分离可防止跨链或跨内存池重放。

6.5 构建者安全性

假设构建者会针对其纳入的集合生成正确的聚合证明 Π。构建者激励和罚没（例如，在权益证明或构建者市场中）不在本文讨论范围内；我们假设构建者的输出由共识层验证，且无效的 Π 会被拒绝。

7 结构带宽比较

令 n 为对象数量， d 为中继节点度数（对等节点数量）， T 为时钟周期（例如 0.5 秒）。假设一个 STARK [5] $\approx$ 128KB，一个证明 $\approx$ 64–256 字节（经典签名，例如 Ed25519 [9]）或 $\approx$2.5KB（后量子密码签名，例如 ML-DSA [8]）。

递归 STARK 传播 [1]。 每个节点在每个时隙生成一个递归 STARK，并将其发送给每个对等节点。每节点证明带宽（出站）： 128 KB $\times\, d/T$。入站情况类似。因此 $\approx 2\times 128\,\text{KB}\times d/T$（例如， $\approx$2 MB/s，针对 $d=8$， $T=0.5\,\text{s}$）。对象载荷： n对象$\times$ 对象大小，与现状相同。路径上的证明流量： $O\,(d/T)$ 每节点，在 n 中为常数。

AR-ACE（证明脱离传播路径）。 路径上不发送任何证明。对于每个对象，每条链路携带 obj 与证明。因此，每节点用于与证明相关的 数据的带宽为零。对于证明：随时间最多$n\times|$证明|（对象与证明一同流动）。若证明为 64–256 字节，总证明开销为 $n\times 64$–256 字节，与当今的每对象元数据（例如，非后量子密码情形中的签名）处于同一数量级。路径上的证明流量：0。有效性证明仅存在于构建者处（区块中包含一个聚合证明）。

数量级缩减。 与随附证明的 传播方式（每个对象都附带自己的 128 KB STARK）相比，AR-ACE 从传播路径中移除了 $n\times 128$KB。与递归 STARK 传播相比，AR-ACE 每个节点每个时隙从传播路径中移除了 128 KB $\times\, d/T$。这两种情况下，传播路径均不携带有效性证明；只有构建者持有并发布一份证明。因此，对于证明相关的 带宽问题，AR-ACE 实现了数量级缩减（实际上消除了传播路径上的此类问题）。此结论仅适用于特定指标：它并不声称，在面对对抗性无效对象压力或策略控制流量时，中继总流量也会有相同幅度的缩减。

7.1 参数化计算范围（解析性，非实证）

免责声明。 本小节给出的是硬件无关的解析关系，而非基准测试结论。

对于一个 10 分钟的分析窗口，设 N 为观测到的对象数， N_{ticks} 为中继时隙数， K 为中继节点数， c_h 为每时隙的重型验证成本（递归证明路径）， c_l 为每个对象的轻量证明验证成本。非构建者中继 CPU 的比率为

$$\frac{\text{AR-ACE CPU}}{\text{Recursive-on-path CPU}} = \frac{N\cdot c_l}{N_{\text{ticks}}\cdot c_h}.$$

当且仅当以下条件成立时，AR-ACE 才会产生更低的中继验证 CPU

$$\frac{c_h}{c_l} > \frac{N}{N_{\text{ticks}}}.$$

对于工作负载对 $(N, N_{\text{ticks}}) = (50{,}000, 1{,}200)$，该阈值为

$$\frac{c_h}{c_l} > 41.67.$$

因此，任何重检查成本比轻量证明检查成本高出$41.67\times$ 以上的部署均可实现中继侧 CPU 节省；确切百分比随后由目标实现/硬件上测得的 (c_h, c_l) 得出。

全网中继 CPU 按相同比率扩展：

$$\frac{K\cdot N\cdot c_l}{K\cdot N_{\text{ticks}}\cdot c_h} = \frac{N\cdot c_l}{N_{\text{ticks}}\cdot c_h}.$$

解释。 该结果与配置无关：繁重的验证工作从中继跳转移，并集中到纳入时间，而实际获得的增益取决于测得的平台参数。

7.2 实用优化方向

除分析基线外，实施层面的优化还可进一步提升吞吐量并降低延迟：

- **证明批次验证**。 中继节点可以一次验证多份证明，从而降低逐对象验证的开销。
- **两阶段传播（先传播哈希+标签，再按需获取）**。 节点首先中继精简的元数据，并按需获取完整对象，从而减少在无效或低优先级对象上浪费的带宽。
- **自适应准入控制**。 可根据拥塞状态调整每键配额、费用和保证金参数，以控制垃圾信息压力。
- **构建器端并行预检流水线**。 构建器可以在聚合证明之前并行执行轻量级筛选和分桶，从而缩短繁重的关键路径。
- **配置切换（混合与全后量子密码）**。部署可以在常规情况下运行低开销的混合证明，并在威胁假设提高时切换为全后量子密码证明。

优化方向及其主要影响指标。量化收益取决于实现和工作负载；本表仅展示其结构性关系。

优化	主要指标	机制
批量证明验证	中继 CPU	将验证开销分摊至多个认证的每批中
两阶段传播（哈希+标签）	中继带宽	延后完整对象获取；避免传输无效或低优先级对象
自适应准入控制	对抗性开销	限制不符合条件或超出中继处的配额提交者条目
构建者并行预检	构建器延迟	并行化轻量级 filtering 之前 聚合的证明
混合配置文件运行	中继 CPU + 带宽	使用紧凑型经典证明-tations 当后量子密码威胁模型允许

各项优化的幅度取决于工作负载和实现。在真实内存池条件下的实证评估留待未来工作。

8 ACE-GF 实例化的优势

使用 ACE-GF 派生证明密钥可得到：

- **统一身份**。 支持链上身份承诺和钱包密钥的同一根（REV）派生出中继证明密钥。一个助记词，一份备份；无需管理单独的证明密钥。

- **上下文隔离**。 证明密钥位于专用的派生上下文中。中继者或遭到泄露的仅用于中继的密钥不会暴露授权密钥或签名密钥。ACE-GF 通过上下文隔离来确保隔离。

- **后量子密码学就绪性**。 后量子密码学流（例如 ML-DSA）可用于证明，使整个处理流程保持后量子密码一致。迁移到后量子密码学证明无需新的身份或备份。

- **确定性与可审计性**。 相同的身份与上下文始终产生相同的证明密钥。恢复与审计（哪一把密钥进行了证明）都很直接。
- **叙事一致性**。 同一身份层（ACE-GF）同时用于链上授权与中继证明（AR-ACE），从而简化协议与产品叙事。

这些优势并非证明离路径传播所严格必需；当身份连贯性与后量子密码一致性成为设计目标时，它们使基于 ACE-GF 的实例化成为首选方案。

9 结论

我们提出了 AR-ACE，一种面向后量子内存池的证明离路径传播设计。通过在中继路径上仅携带轻量证明，并在构建者处执行一次聚合有效性证明，我们彻底将证明流量移出该路径，并实现证明相关带宽的数量级缩减。安全性通过三个博弈（证明伪造、重放与准入绕过）加以形式化，并在标准假设下给出基于归约的论证。该设计与现有有效性谓词及聚合证明系统（例如构建者处的递归 STARK）兼容。当使用由 ACE-GF 派生的证明密钥进行实例化时，AR-ACE 与链上授权保持统一身份叙事，并具备后量子密码学就绪性。我们将具体参数设定、实现，以及与特定内存池和构建者实现的集成留待未来工作。

参考文献

[1]V. Buterin. 基于递归 STARK 的高带宽效率内存池。以太坊研究，2025年1月。 https://ethresear.ch/t/recursive-stark-based-bandwidth-efficient-mempool/23838.[2] J. S. Wang. ACE-GF：原子密码实体生成框架。*arXiv* 预印本 *arXiv:2511.20505*，2025年。[3] V. Buterin、D. Feist、D. Loerakker、G. Kadianakis、M. Garnett、M. Taiwo Adeniyi 和 A. Schoedon。EIP-4844：分片 Blob 交易。以太坊改进提案，2022年。[4] V. Buterin、Y. Weiss、D. Kristjansson、N. Luca、T. Silberstein 和 M. Tirosh。ERC-4337：使用替代内存池的账户抽象。以太坊改进提案，2021年。[5] E. Ben-Sasson、I. Bentov、Y. Horesh 和 M. Riabzev。可扩展、透明且抗后量子攻击的计算完整性。*IACR* 电子预印本 2018/046，2018年。[6] A. Kothapalli、S. Setty 和 I. Tzialla。Nova：基于折叠方案的递归零知识论证。载于$CRYPTO$，LNCS 13510，第359–388页，2022年。[7] S. Bowe、J. Grigg 和 D. Hopwood。无需可信设置的递归证明组合。*IACR* 电子预印本 2019/1021，2019年。[8] 美国国家标准与技术研究院。模格数字签名标准。联邦信息处理标准出版物 FIPS 204，2024年。

[9] D. J. Bernstein、N. Duif、T. Lange、P. Schwabe 和 B.-Y. Yang。高速高安全性签名。《密码工程杂志》，2(2):77–89，2012年。[10] D. Boneh、B. Lynn 和 H. Shacham。基于 Weil 配对的短签名。载于*ASI-ACRYPT*，LNCS 2248，第514–532页，2001年。[11] S. Goldwasser、S. Micali 和 R. L. Rivest。一种可抵御自适应选择消息攻击的数字签名方案。《*SIAM* 计算杂志》，17(2):281–308，1988年。[12] M. Bellare 和 P. Rogaway。三重加密的安全性及基于代码的博弈证明框架。载于*EUROCRYPT*，LNCS 4004，第409–426页，2006年。[13] D. Vyzovitis、Y. Napora、D. McCormick、D. Dias 和 Y. Psaras。GossipSub：Filecoin 和 ETH2.0 网络中具有攻击韧性的消息传播。arXiv 预印本 arXiv:2007.02754，2020年。[14] P. Maymounkov 和 D. Mazières。Kademlia：基于异或度量的点对点信息系统。载于*IPTPS*，LNCS 2429，第53–65页，2002年。