Auth-and-Integrity

方法

本文通过将 **搜索验证与完整性审计统一到一个证明中** 的技巧性结构设计，将原本需要分别进行的两类验证操作合并，大幅降低 DSN 场景下的链上开销与节点计算成本，实现加密条件下的高效可验证搜索与完整性审计。

主要贡献

1. **统一证明机制**：将搜索结果正确性与文件完整性验证融合为一个证明，避免分别生成两个证明带来的昂贵链上存储开销。
2. **无需新增第三方仲裁节点**：通过文件状态链式链接 + 关键字关联标签实现可验证搜索，不破坏去中心化原则。
3. **支持前向安全的动态更新**：提出状态链（state-chain）与 pointer 结构，使得新插入文件不会与历史查询关联。
4. **高效率、低开销**：相比将搜索与审计分离实现的方案，本方案在不增加证明大小的情况下，实现更低的链上 gas 开销与更快的验证速度。

主要问题

1. **仅支持单关键词搜索**：当前仅支持 single-keyword，复杂查询（如相似性检索、多条件搜索）无法直接扩展。
2. **依赖链式状态结构**：搜索时必须遍历状态链，若同一关键词关联文件过多，检索延迟会增长；
3. **未处理访问模式泄露问题**：仍需引入 dummy 技术才能应对频率分析与访问模式攻击；
4. **需要节点额外执行搜索证明**：相比传统 PoS 仅验证完整性，本方案对资源较弱的节点仍存在一定额外负担。