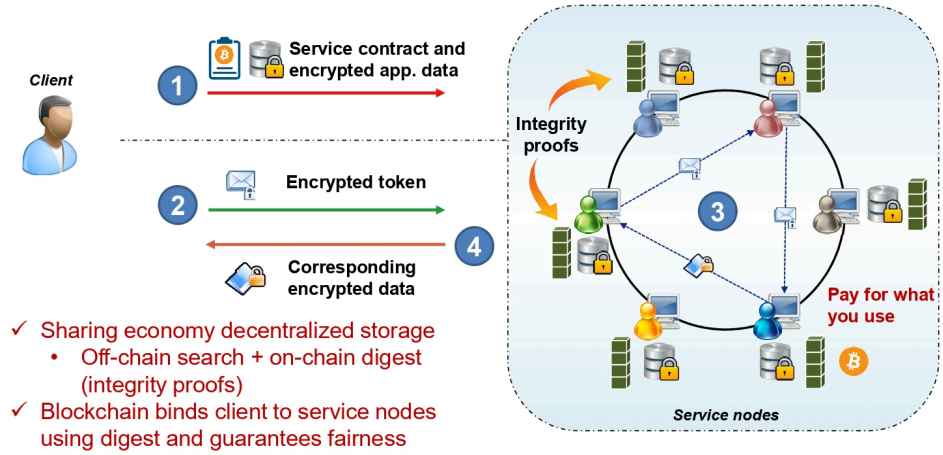
Knowledge Transfer Office
香港城市大學
City University of Hong Kong

通过区块链进行加密去中心化存储中可信与私密关键词搜索的方法

信息和通信

计算机/人工智能/数据处理和信息技术



IP状态
专利已授权

技术成熟度等级 (TRL) 8

发明人
王聪教授
Dr. Xingliang YUAN
蔡承均
询问: kto@cityu.edu.hk

机会

区块链引领了去中心化应用的趋势，并在加密货币以外展示了巨大用途。去中心化存储如Storj和Sia利用区块链建立了一个共享经济的开放平台，提供私密且可靠的文件外包服务。与中心化云存储相比，去中心化存储依赖于个人服务节点提供的租赁存储空间，并通过区块链确保服务的完整性，例如，通过在节点间锚定存储合约和通过区块链处理服务支付。为了保护用户隐私，一个有前途的方法是采用端到端加密来保障数据内容的安全，并实施访问控制，使得只有拥有私钥的授权用户能够解密数据，但数据加密却导致无法搜索和计算加密数据，这不可避免地降低了用户体验。

技术

在这项发明中，我们提出了一种支持可信和私密关键词搜索功能的加密去中心化存储架构。为了实现这一功能，我们首先将可搜索加密技术应用于去中心化环境中。然而，仅有这一原始技术难以保证服务完整性。这是因为去中心化存储通常面临来自客户端和服务节点的严重威胁。服务节点可能返回部分或不正确的结果，而客户端可能故意诋毁服务节点以避免支付。为了解决这些威胁，我们利用智能合约在区块链上记录加密搜索的日志（亦称为证据），并设计了一种公平协议来解决争议和发布公平支付，从而激励服务节点进行真实努力，共同保证服务的可靠性。我们在Python和Solidity中实现了我们的方案，并在以太坊上测试其搜索性能和交易成本。

优势

- 支持私密和可信关键词搜索功能的首个加密去中心化存储设计
- 通过新颖协议的动态高效可搜索加密方案，适当调整去中心化存储结构，确保恶意环境中的公平性

- 用于区块链成本优化的集成链下-链上协议
- 对可搜索加密方案的公共可验证性

应用

- 具有加密搜索功能的新型去中心化存储架构
- 个体服务节点和用户客户端之间的便捷且公平的支付
- 对外包加密数据的动态和公开可验证的搜索