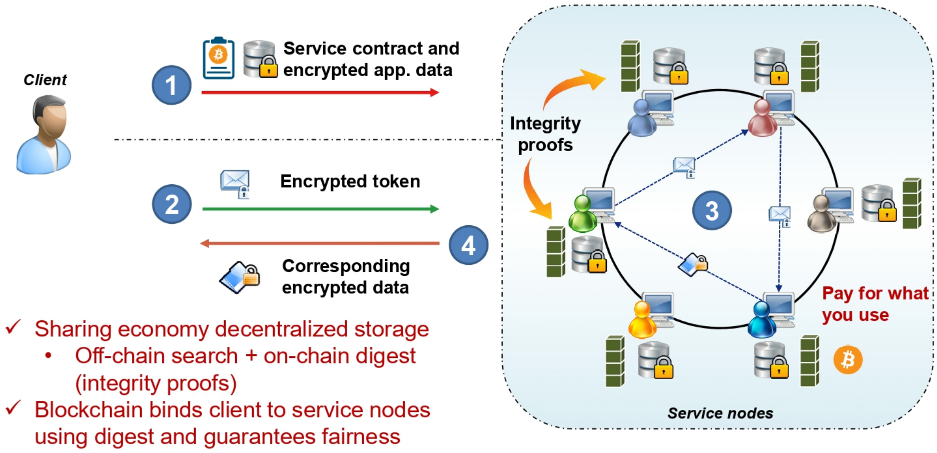
Methods for Trustworthy and Private Keyword Search in Encrypted Decentralized Storage via Blockchain

Communications & Information

Computer/AI/Data Processing and Information Technology



- ✓ Sharing economy decentralized storage
  - Off-chain search + on-chain digest (integrity proofs)
- ✓ Blockchain binds client to service nodes using digest and guarantees fairness

IP Status
Patent granted

Technology Readiness Level (TRL) ?
8

Inventor(s)
Prof. WANG Cong
Dr. YUAN Xingliang
Mr. CAI Chengjun
Enquiry: kto@cityu.edu.hk

Opportunity

Blockchain has led the trend of decentralized applications and shown great use beyond cryptocurrencies. Decentralized storage such as Storj and Sia leverages blockchain to establish an open platform for sharing economy, which provides private and reliable file-outsourcing services. Compared to centralized cloud storages, decentralized storage relies on individual service peers to provide the leasing storage volume and the blockchain to enforce service integrity, e.g., by anchoring storage contracts between peers and handing service payments via the blockchain.

To protect user privacy, one promising approach is to adopt end-to-end encryption to secure data content and enforce access control in such a way that only authorized users with private keys are able to decrypt the data, but data encryption prohibits from searching and computing over encrypted data, which inevitably degrades the user experience.

Technology

In this invention, we propose an encrypted decentralized storage architecture that can support trustworthy and private keyword search functions. To enable this function, we first apply searchable encryption techniques to the decentralized setting. But this primitive can hardly ensure the service integrity. The reason is that decentralized storage commonly faces severe threats from both clients and service peers. Service peers may return partial or incorrect results, while clients may intentionally slander the service peers to avoid payments.

To address these threats, we utilize the smart contract to record the logs of encrypted search (aka evidence) on the blockchain, and devise a fair protocol to handle disputes and issue fair payments, so that service peers are incentivized to make real efforts and jointly guarantee service reliability. We implement our scheme in Python and Solidity, and test its search performance and transaction costs on Ethereum.

Advantages

- First encrypted decentralized storage design that supports private and trustworthy keyword search function
- Dynamic efficient searchable encryption scheme with novel protocol that properly adjusts the decentralized storage structure and ensures fairness in a malicious setting
- Integrated off-chain on-chain protocol for blockchain cost optimizations
- Public verifiability for searchable encryption schemes

Applications

- A new decentralized storage architecture with encrypted search functions
- Faciliated and fair payment among individual service peers and user clients
- Dynamic and publicly verifiable search over outsourced encrypted data