ABSTRACT

In an era where quantum computing threatens to compromise traditional encryption, secure data storage is essential. This project is a decentralized storage solution leveraging blockchain technology and post-quantum cryptography to create a quantum-safe environment for storing documents and files. It addresses growing concerns around data privacy, integrity, and resilience with advanced quantum-resistant algorithms—Crystal Kyber for key exchange, Crystal Dilithium for digital signatures, and AES-256 encryption—to protect against both current and future computational threats.

The Project's architecture decentralizes data storage across multiple nodes, eliminating single points of failure and enhancing data availability and redundancy. This blockchain-based structure inherently supports immutability and security, distributing encrypted data across the network to mitigate the risks of tampering, loss, or unauthorized access. Smart contract protocols further manage data access control and permissions, ensuring an immutable audit trail for every transaction and storage operation.

The Project offers a seamless user experience that supports secure file encryption, storage, retrieval, and management. Its design layers quantum-safe cryptographic algorithms for robust data protection against classical and quantum attacks, creating a resilient and traceable storage solution. This quantum-safe, blockchain-based storage system is scalable and suitable for industries requiring high levels of data security, such as finance, healthcare, and government. It provides a forward-looking solution to current cybersecurity vulnerabilities, establishing a robust foundation that can adapt to the evolving landscape of quantum computing threats.