Post-Quantum Cryptography

Security Implementation Guide

Overview

QuantPayChain implements post-quantum cryptography to protect against future quantum computing threats. Our implementation follows NIST-approved algorithms ensuring long-term security for tokenized assets.

Quantum Threat

Quantum computers pose a significant threat to current cryptographic systems. Algorithms like RSA and ECC, which secure most blockchain networks today, could be broken by sufficiently powerful quantum computers.

NIST-Approved Algorithms

We implement the following NIST-approved post-quantum algorithms: - CRYSTALS-Kyber for key encapsulation - CRYSTALS-Dilithium for digital signatures - SPHINCS+ as backup signature scheme

Implementation

Our post-quantum implementation includes: 1. Hybrid cryptographic approach combining classical and post-quantum algorithms 2. Secure key management system 3. Regular security audits and updates 4. Backward compatibility with existing systems