Criptografía Post-Cuántica

Guía de Implementación de Seguridad

Descripción General

QuantPayChain implementa criptografía post-cuántica para proteger contra futuras amenazas de computación cuántica. Nuestra implementación sigue algoritmos aprobados por NIST asegurando seguridad a largo plazo para activos tokenizados.

Amenaza Cuántica

Las computadoras cuánticas representan una amenaza significativa para los sistemas criptográficos actuales. Algoritmos como RSA y ECC, que aseguran la mayoría de las redes blockchain hoy, podrían ser quebrados por computadoras cuánticas suficientemente potentes.

Algoritmos Aprobados por NIST

Implementamos los siguientes algoritmos post-cuánticos aprobados por NIST: - CRYSTALS-Kyber para encapsulación de claves - CRYSTALS-Dilithium para firmas digitales - SPHINCS+ como esquema de firma de respaldo

Implementación

Nuestra implementación post-cuántica incluye: 1. Enfoque criptográfico híbrido combinando algoritmos clásicos y post-cuánticos 2. Sistema de gestión segura de claves 3. Auditorías de seguridad y actualizaciones regulares 4. Compatibilidad retroactiva con sistemas existentes

Beneficios

La seguridad post-cuántica proporciona: - Protección contra ataques cuánticos futuros - Cumplimiento con estándares de seguridad emergentes - Confianza a largo plazo para inversores institucionales - Liderazgo en innovación tecnológica