BRITISH GOLD TRUST

Quantum-Secured Gold Custody

Preparing the Gold Standard for the Quantum Age

1. The Quantum Threat to Financial Security

Emerging Risks:

- **Blockchain Vulnerabilities**: Shor's algorithm will break RSA and ECC encryption, compromising Bitcoin/ETH wallets and smart contracts.
- **Gold Audit Risks**: Quantum spoofing could falsify reserve proofs in "secured" digital gold systems.
- **Timeline**:
    - *2025*: NIST finalizes post-quantum standards (CRYSTALS-Dilithium/Kyber).
    - *2029-2032*: First practical attacks on RSA-2048 (MITRE forecast).

2. GoldTech's Quantum Shield

Three-Layer Architecture:

Layer	Technology	Purpose
Quantum Key Generation	CRYSTALS-Dilithium (NIST PQC winner)	Unhackable digital signatures
Entanglement Auditing	QRNG + Photon Entanglement	Tamper-proof reserve verification
Institutional Gateway	YubiHSM 2 + FIPS 140-3	Military-grade key storage

Key Advantages:

- 256-bit security against quantum brute-force attacks.
- Real-time audit trails via quantum-secure ZK proofs.
- GDPR/ISO 27001 compliant data pipelines.

3. Institutional Benefits

For Central Banks:

- Future-proof gold reserves against quantum theft.
- Interoperability with CBDC networks.

For Hedge Funds:

- First quantum-resistant gold ETF infrastructure.
- Cross-border settlements with 10-minute finality.

For Family Offices:

- Multi-generational wealth preservation.
- Off-balance-sheet asset shielding.

4. Technical Specifications

- **Encryption**: XMSS (stateful hash-based signatures).
- **Consensus**: Modified PBFT with lattice-based thresholds.
- **Compliance**: NIST SP 800-208, FATF Travel Rule.