
# Crypto-Asset Vulnerabilities in the Quantum Era


- Juan Díez González
- Spanish National Cybersecurity Institute - INCIBE

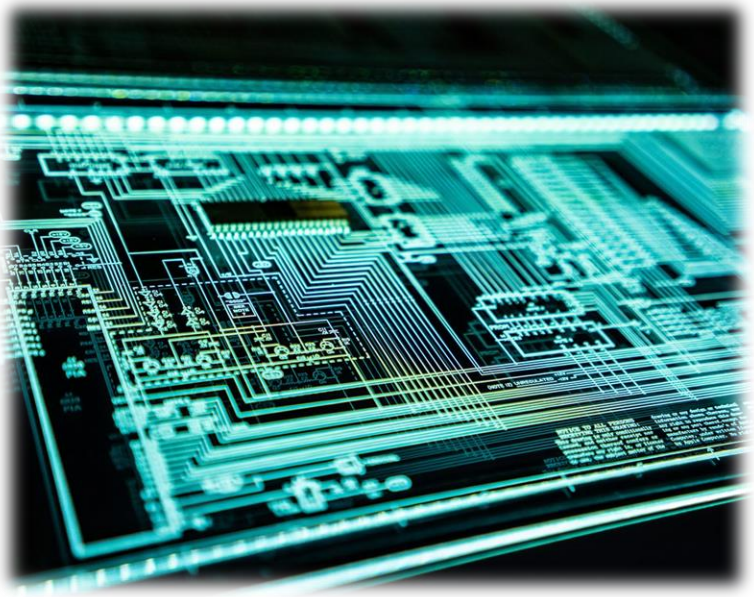

**Juan Díez González**

# Why This Matters Now

- MiCA introduces harmonised EU oversight
- Quantum computing is becoming a strategic issue
- Public blockchains rely on vulnerable cryptographic assumptions
- Supervisors need measurable resilience strategies

# The Cryptographic Foundations of Crypto-Assets

- Public-key cryptography secures wallets and signatures
- Hash functions protect integrity and consensus
- ECC dominates Bitcoin and Ethereum
- Current trust assumes classical computing limits



# What Changes with Quantum Computing?

- Shor’s algorithm threatens RSA and ECC
- Grover’s algorithm weakens hash security
- Dormant wallets become exposed
- Harvest-now, decrypt-later strategies increase urgency

# Potential Impact on Crypto Markets

- Compromise of legacy wallets
- Custody providers become systemic targets
- Potential liquidity and valuation shocks
- Smart contracts add new attack surfaces

# MiCA and the Quantum Risk Landscape

- MiCA requires transparency and operational resilience
- White papers must disclose technology risks
- CASPs need robust ICT controls
- Quantum resilience may become supervisory expectation

# Key Supervisory Challenges

- Assessing quantum readiness consistently
- Lack of standardised disclosure metrics
- Cross-border migration complexity
- Balancing innovation and security

# Transitioning to Post-Quantum Cryptography

- Protocol upgrades will be required
- Hybrid cryptographic models likely
- Backward compatibility remains difficult
- NIST standards becoming reference points

# Digital Reporting and Structured Disclosure

- Structured reporting improves supervisory visibility
- Machine-readable disclosures enable monitoring at scale
- XBRL supports MiCA transparency goals
- Quantum disclosures may enter future frameworks

# Open-Source XBRL Generator for Crypto-Asset White Papers

- Implementation-oriented digital reporting
- Supports MiCA-aligned structured disclosures
- Open standards enhance transparency
- Benefits for regulators, academia an tech providers.

# Strategic Recommendations

- Start quantum risk assessments now
- Promote EU-wide supervisory coordination
- Encourage migration roadmaps
- Invest in auditable reporting infrastructures

# Conclusions & Call to Action

- Quantum threats are a governance issue
- Crypto resilience must join supervisory dialogue
- MiCA enables future-proof transparency standards
- Europe can lead through regulation and innovation

# Thank you

**Juan Díez González**
Project Leader
INCIBE| Instituto Nacional de Ciberseguridad
juan.diez@incibe.es
https://www.linkedin.com/in/juandiez/