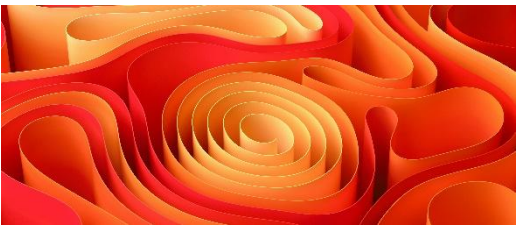
Pills
Regulatory/Supervisory Pills | N.13 January 2025



TOPICS:
Technology

SOURCE
Bank of Italy

Bankit - The Quantum Challenge: Implications and Strategies for a Secure Financial System

- The Bankit paper outlines the emerging risks and opportunities associated with quantum computing (QC) in the financial sector. It addresses how QC can **enhance computational capabilities**, potentially solving complex problems in areas such as risk management, capital allocation, and optimization. However, QC also poses **significant threats**, particularly to cryptographic systems, which underpin the security of communication channels and digital assets like central bank digital currencies (CBDCs).
- The paper emphasizes that current **encryption methods could be vulnerable to QC-powered attacks**, which might retroactively compromise past communications ("harvest now, decrypt later"). Although fully functioning quantum computers are still years away from commercialization, hybrid systems combining quantum capabilities with classical high-performance computing (HPC) are already in development. These systems offer the potential for financial firms to harness QC's benefits, but they also increase the risk landscape, requiring a strategic approach to secure systems against future quantum threats.
- **To mitigate these risks**, the paper advocates for **the development of quantum-safe technologies and migration strategies**, including post-quantum cryptography (PQC) and quantum key distribution (QKD). It calls for international cooperation to establish shared standards and secure frameworks, as the global nature of the financial system means that even small vulnerabilities can have far-reaching consequences. Key forums like the G7 and IMF are identified as critical players in coordinating these efforts.