



Navigating the Quantum threat: ensuring encryption security

Derya Kali, Sirius Quantum Solutions

10 June 2025



Did you know?

ICAEW's revised Continuing Professional Development (CPD) Regulations brought in new CPD requirements, including a minimum number of hours and an ethics requirement.

This webinar could contribute to up to 1 hour of verifiable CPD, so long as you can demonstrate that the content is relevant to your role.

Find out more about how these changes affect you at icaew.com/cpdchanges.



Ask a question



The screenshot shows a Q&A interface. At the top, it says 'Q&A'. Below that, it shows a question: 'You asked: What happens when I raise my hand?' with a timestamp of '18:03'. Below the question, it shows an answer: 'Molly Parker answered: I can take you off of mute.' with a timestamp of '18:04'. Below the answer, there is a large text input field with the placeholder text 'Please input your question'. At the bottom left of the input field, there is a checkbox labeled 'Send Anonymously'. At the bottom right of the input field, there is a blue button labeled 'Send'.

To ask a question

Click on the **Q&A** button in the bottom toolbar to open the submit question prompt.

Type your question and click send

NOTE: If you wish to ask your question anonymously check the **send anonymously** box shown on the illustration.

Meet the speakers



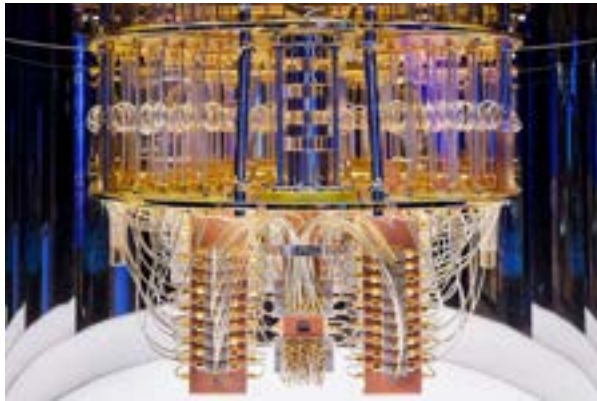
Derya Kali, Founder, Sirius Quantum Solutions



Polly Tsang, Senior Manager,
Financial Services Faculty, ICAEW

Jargon - Decoder

QC



Quantum Computers

PQC



Post Quantum Cryptography

QKD

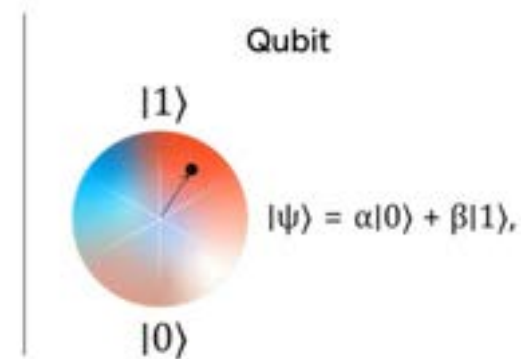
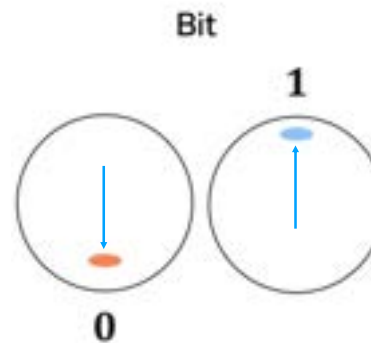


Quantum Key Distrubution

NIST: National Institute of Standards and Technology

NISQ: Noisy Intermediate-Scale Quantum (10-1000 Qubit)

Sirius Quantum Solutions Ltd Propriety



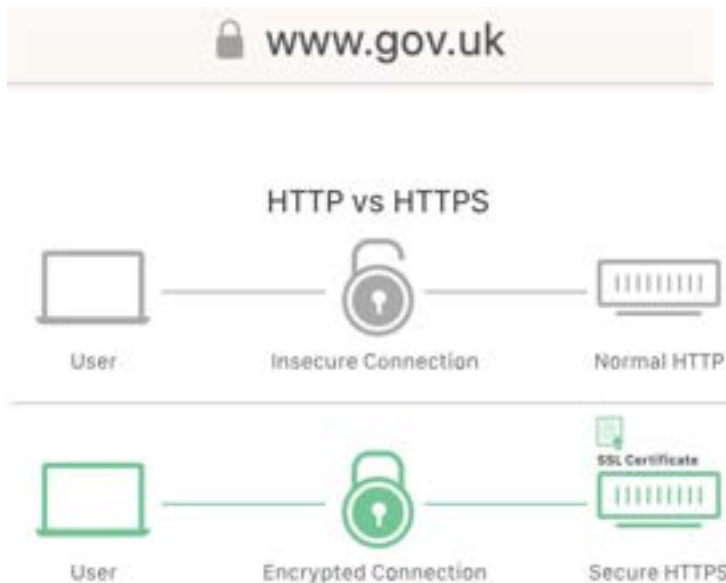
Quantum Threat: What is at Risk?



30% of Global Encrypted Data, including financial records, is at risk of “harvest now, decrypt later” (HNDL) attacks, per the U.S. National Security Agency (NSA) 2023 Cybersecurity Advisory.

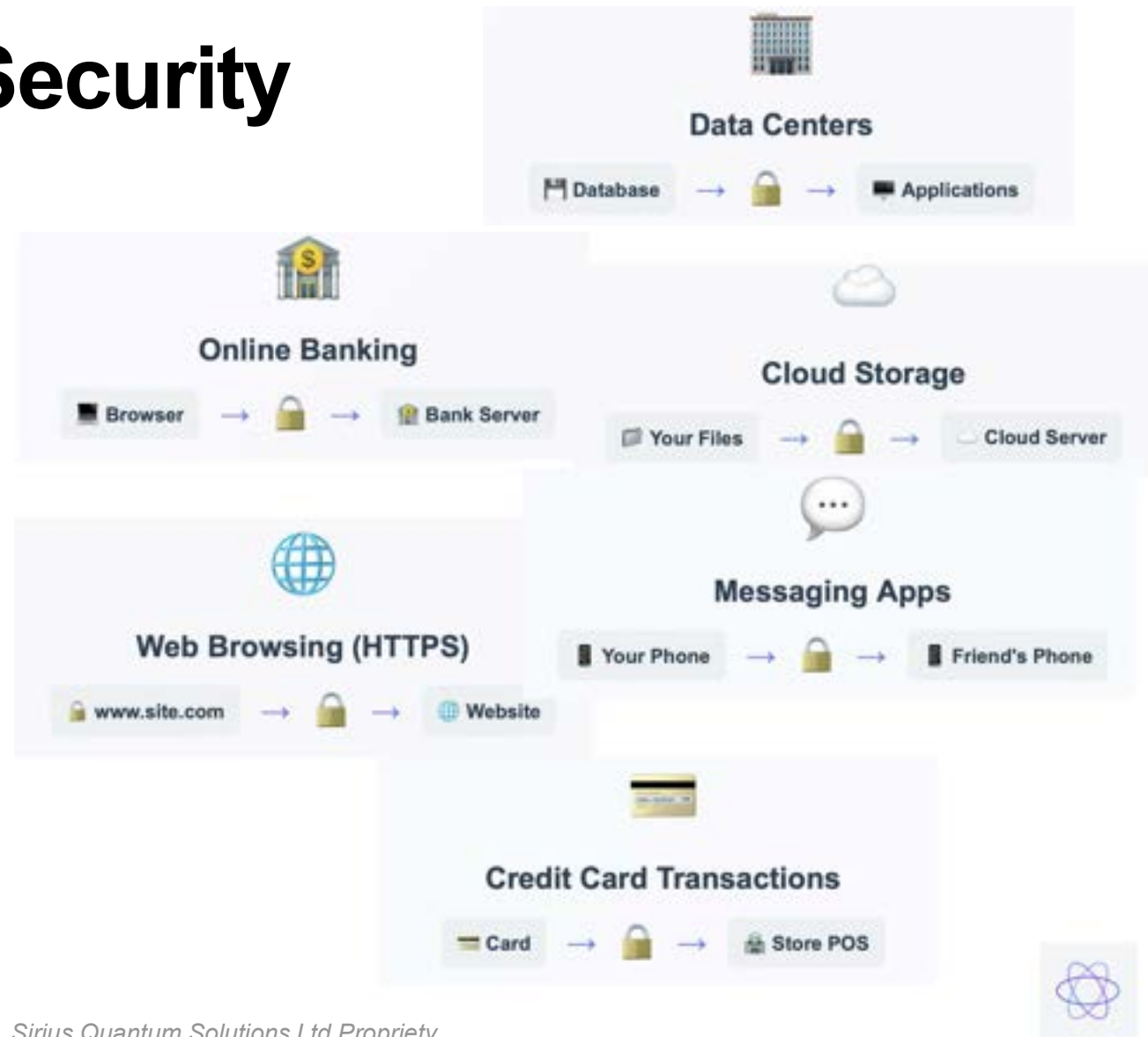


Data Encryption Security



Banks and merchants must use TLS 1.2 or 1.3 to comply with PCI DSS (Payment Card Industry Data Security Standard) security requirements.

TLS/SSL : Transport Layer Security/ Secure Socket Layer



Sirius Quantum Solutions Ltd Propriety

What PKI Secures Now?

Banks

SWIFT Transaction Services

Payment Services

ATM

Internet Banking

Private and Public Cloud

Blockchains

Wallet Address & Ownership

Transaction Signatures

Smart Contract Permission

Consensus (PoW/ PoS)

Cross-chain Bridges

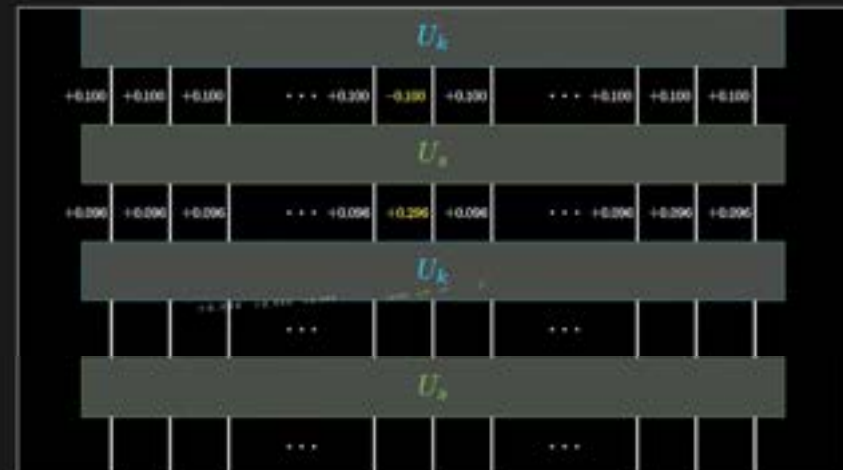


How does Quantum break encryption?

Classical Search



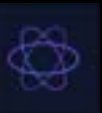
Quantum Search



Grover's algorithm searches an unsorted database in \sqrt{n} steps instead of n .

For a 1-million-entry database,
that's 1,000 steps vs. 1,000,000. That's a quantum advantage! It can find the private key in one go!

Sirius Quantum Solutions Ltd Propriety



Quantum Readiness Imperatives

“1 in 3 banks have no quantum migration plan,” despite 78% of central banks labeling it a “systemic risk”
(Accenture, 2024 Financial Quantum Resilience Survey)



Risk Assessment Table

Cryptographic Security Risk Analysis

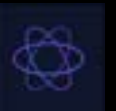
Dimension	Use Case	Time	Ext. Avail.	Sens.	Risk
Confidentiality	Public websites TLS encryption	1	5	5	25 (Medium)
	Internal SSH server access	2	1	3	6 (Low)
	Teleworking VPNs	3	3	5	45 (High)
	Site-to-site IPSEC VPNs	5	3	5	75 (Very High)
	Data at rest encryption (premises)	5	2	3	30 (Medium)
	Data at rest encryption (cloud)	5	3	5	75 (Very High)
Authentication	Public digital certificates	2	5	5	50 (High)
	Internal digital certificates	2	1	4	8 (Low)
Legal History	Digital contract signatures	5	4	5	100 (Critical)

Time: Duration for which the security measure remains effective (1=short term, 5=long term)

External availability: Accessibility to external entities (1=internal only, 5=publicly accessible)

Sensibility: Sensitivity level of data/process protected

Sirius Quantum Solutions Ltd Propriety



Regulatory and Compliance Drivers

PCI DSS 4.0

(effective March 2024) requires disabling **TLS 1.0** and **TLS 1.1** for all payment systems.

TLS 1.2 and 1.3 are permitted, but TLS 1.3 is **recommended** for its stronger encryption (e.g., ChaCha20, AES-GCM) and forward secrecy.

NIST Guidelines (U.S Federal Standards)

NIST SP 800-52 Rev. 2 (2019) states that TLS 1.3 **should be used** where possible, and TLS 1.2 is acceptable only with strict cipher suite configurations

GDPR (EU General Data Protection Rules)

While GDPR does not explicitly mandate TLS versions, it requires "appropriate security" for data in transit.

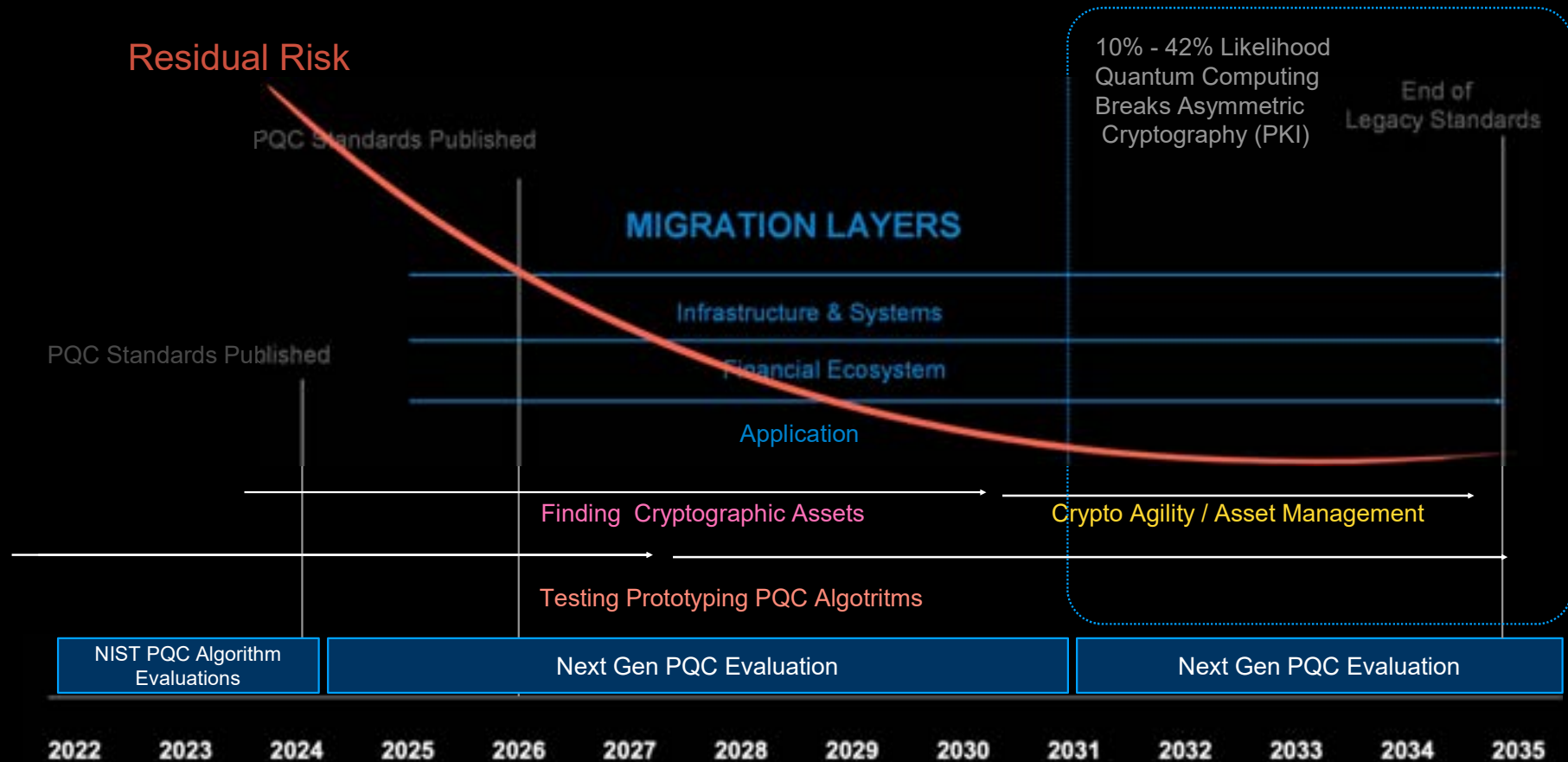
Financial Sector Regulations (e.g FFIEC, FCA)

Many financial institutions (e.g., EU banks under PSD2) require **TLS 1.2 or higher** for APIs and customer-facing services.

Using TLS to protect data https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data#section_5



Enterprise Quantum Readiness Strategy

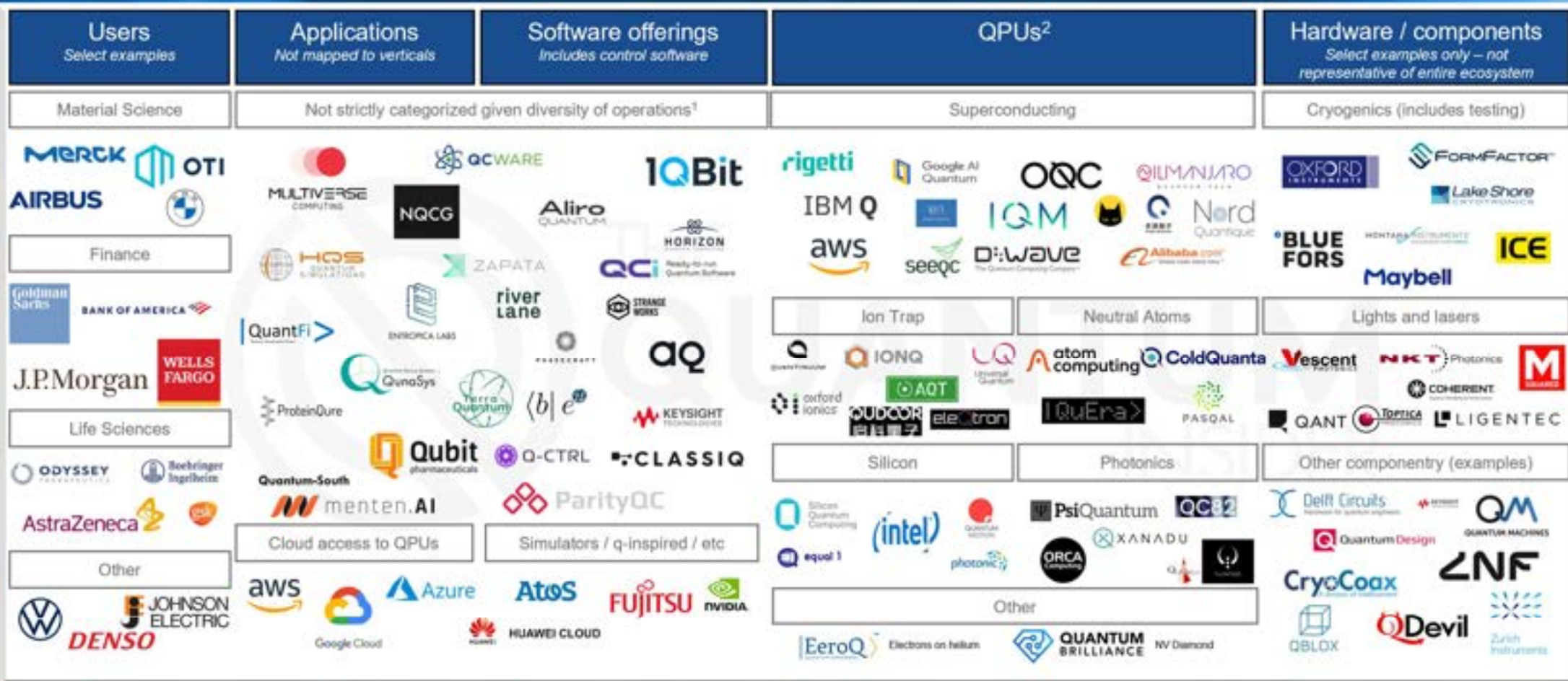


Global Quantum Playbook



Quantum Computing Market Map

Non exhaustive and in no particular order. Excludes details on control systems, assembly languages, circuit design, etc.



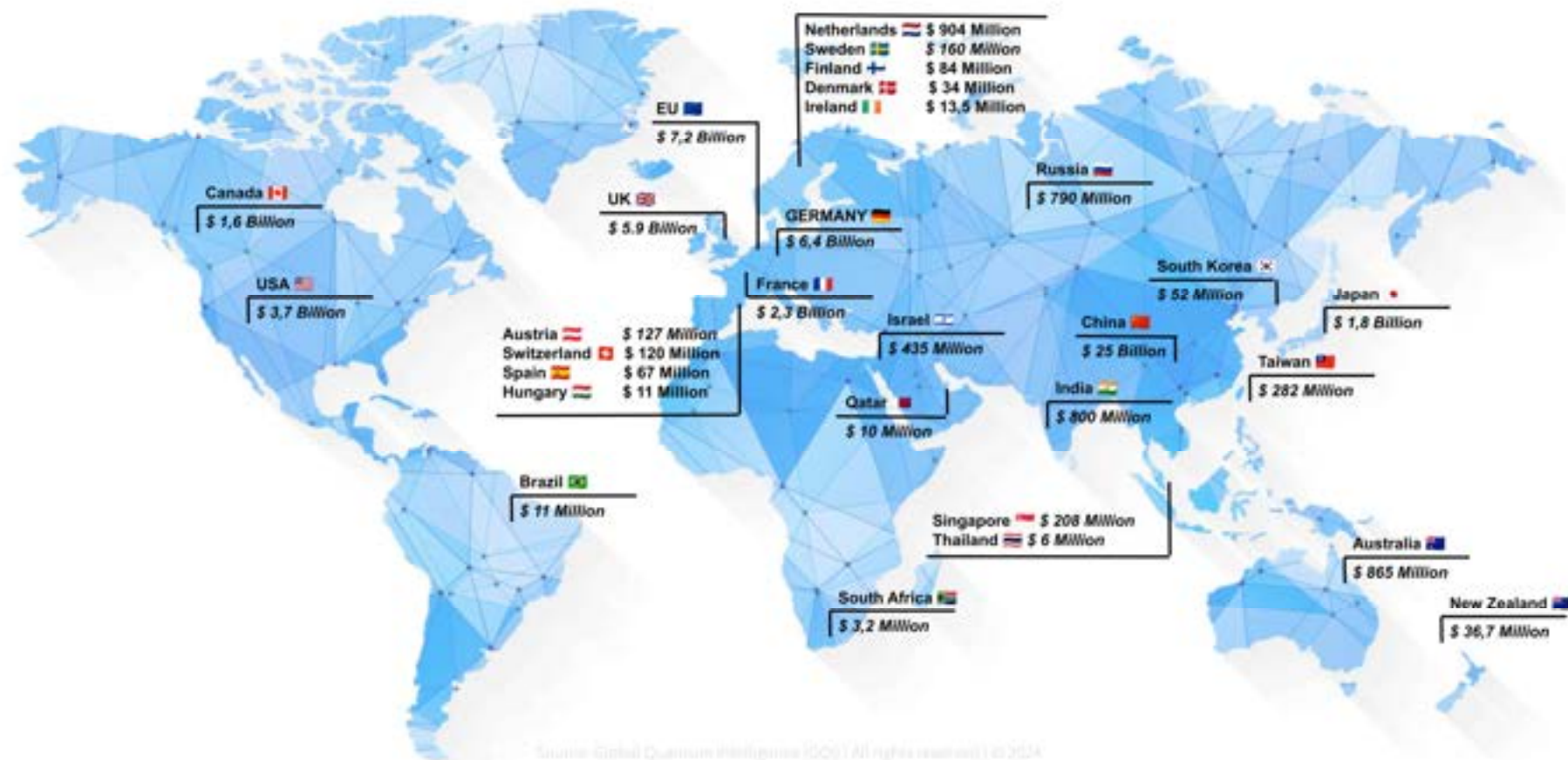
¹ Software offerings can be further classified into SDKs, firmware / enablers, algorithms / applications, simulators etc. but many companies are offering a mixture across the stack

² Many QPU providers are offering full stack services (e.g. Pasqal acquired Qu&Co, Quantinuum was originally QQC prior to merger with HQS, etc.

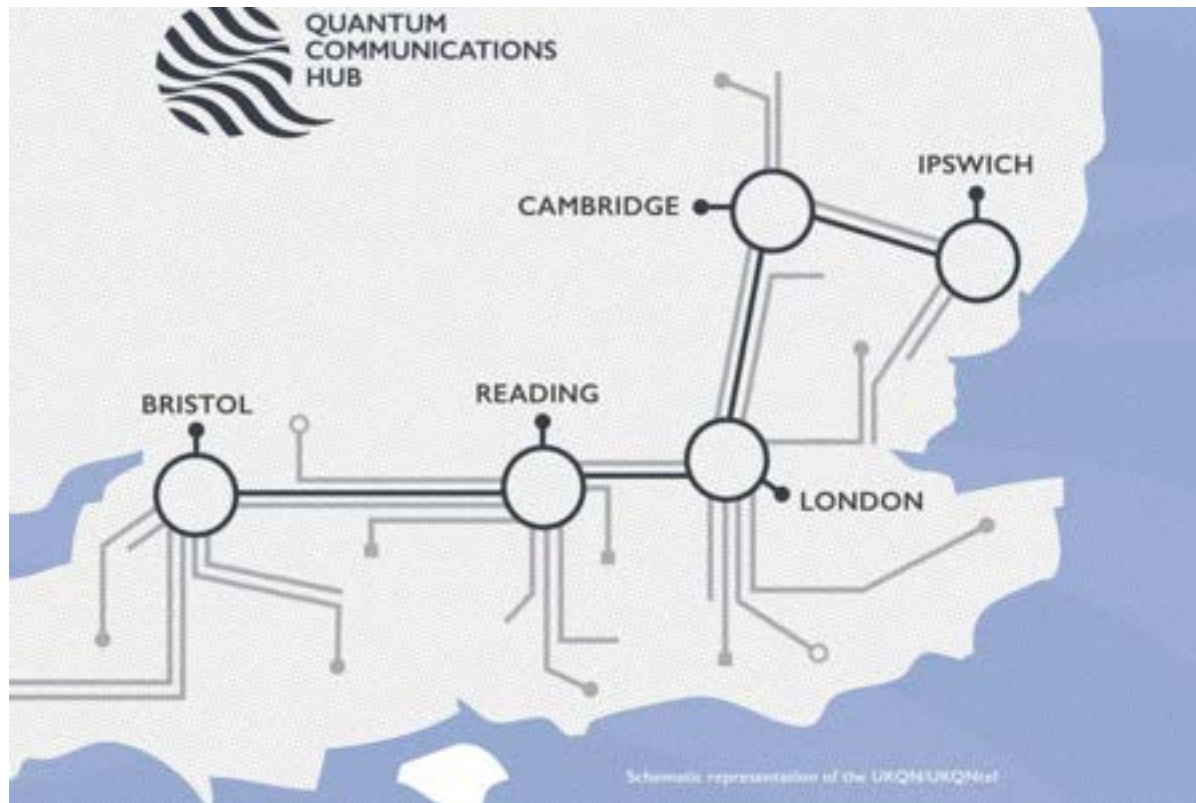
Quantum Race is “Geopolitical”



Government driven funding of quantum initiatives



UK National Quantum Strategy



The Hub is funded through the UK National Quantum Technologies Programme, a ten-year £1 billion public and private investment underpinned by the UK government

Sirius Quantum Solutions Ltd Propriety

Press release

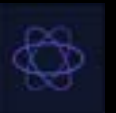
£121 million boost for quantum technology set to tackle fraud, prevent money laundering and drive growth



Crypto-Agility Roadmap

90% of Public-Key Cryptography:

Current standards (RSA, ECDSA) securing banks and blockchains will be broken by quantum computers, confirms **NIST's 2023 Post-Quantum Cryptography Report**.



When QDay?

The results for the resource estimates are in the table below:

Bit length of ECC key	Bit length of equivalent RSA key	Logical qubits to break ECC key	Number of Toffoli gates to break ECC key	Super-conducting qubits needed*	Execution time on a super-conducting device*	Interleaving modules needed*	Execution time on a photonic device using Active Volume*
163	1024	2125	$1.37 \cdot 10^6$	$2.45 \cdot 10^6$	2.4 min	188	1.2 min
233	2048	3035	$3.52 \cdot 10^6$	$3.79 \cdot 10^6$	6.5 min	294	3.1 min
283	3072	3685	$5.62 \cdot 10^6$	$4.98 \cdot 10^6$	10.8 min	390	5.1 min
571	15360	7429	$2.71 \cdot 10^7$	$1.16 \cdot 10^7$	56.2 min	929	23.4 min

* The results listed here are excerpts from the full list of results in Tables VI, VII, and VIII from the text of the article representing realistic conditions for comparison between matter-based qubits and PsiQuantum's photonic devices.

<https://www.psiquantum.com/featured-news/binary-ecc>


<https://quantumdoomclock.com/explanation>

Sirius Quantum Solutions Ltd Propriety



Don't wait - Act Now

Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	≥ 128 bits of security strength	Disallowed after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	Disallowed after 2035
RSA [FIPS186]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	≥ 128 bits of security strength	Disallowed after 2035

First Migration: Key Agreement (TLS)

Second Migration: Signature/Certificates (RSA, ECC, X.509)

Sirius Quantum Solutions Ltd Propriety



Quantum Risk Mitigation Roadmap

1 TECHNOLOGY ASSESSMENT

Key Activities:

- Audit cryptographic infrastructure
- Hardware: HSMs, network appliances, IoT
- Software: OpenSSL, APIs, frameworks
- Legacy: mainframes, core banking, SWIFT

Timeline: 3-6 months

Priority: Complete vulnerability mapping

2 CRITICAL DATA INVENTORY

Key Activities:

- Customer: PII, accounts, KYC, biometrics
- Financial: transactions, audit trails, compliance
- Internal: credentials, API keys, certificates
- Classify by quantum threat exposure

Timeline: 2-4 months

Priority: Highest-value data first

3 CRYPTOGRAPHY MAPPING

Key Activities:

- Network: TLS/SSL, VPNs, IPSec, SWIFT
- Application: signatures, tokens, APIs
- Storage: database, backup, cloud encryption
- Document dependencies & interconnections

Timeline: 4-6 months

Priority: Map all crypto implementations

4 HYBRID ENCRYPTION STRATEGY

Key Activities:

- NIST PQC: Kyber, Dilithium, FALCON
- Dual-layer: classical + quantum-resistant
- Pilot programs & stress testing
- Gradual rollout with compatibility

Timeline: 12-18 months

Priority: Highest-risk systems first

5 VENDOR COORDINATION

Key Activities:

- Core Banking: Temenos, FIS, Oracle, SAP
- Security: HSM providers, CAs, cyber partners
- Cloud: AWS, Azure, GCP roadmaps
- Joint testing & upgrade schedules

Timeline: Ongoing

Priority: Regular communication channels

6 REGULATORY COLLABORATION

Key Activities:

- European: EBA, ECB, national authorities
- International: BIS, NIST, ISO standards
- Industry: banking associations, ISACA
- Proactive participation in guidance

Timeline: Continuous

Priority: Stay ahead of requirements



Thank You!

Contact us: info@siriusquantum.com



Q&A

Visit : <https://siriusquantum.vercel.app/>

