

Quantum Computing and Quantum-Safe Security

François Varchon
Global Leader - IBM Quantum Support
IBM Quantum

Bring useful quantum
computing to the world

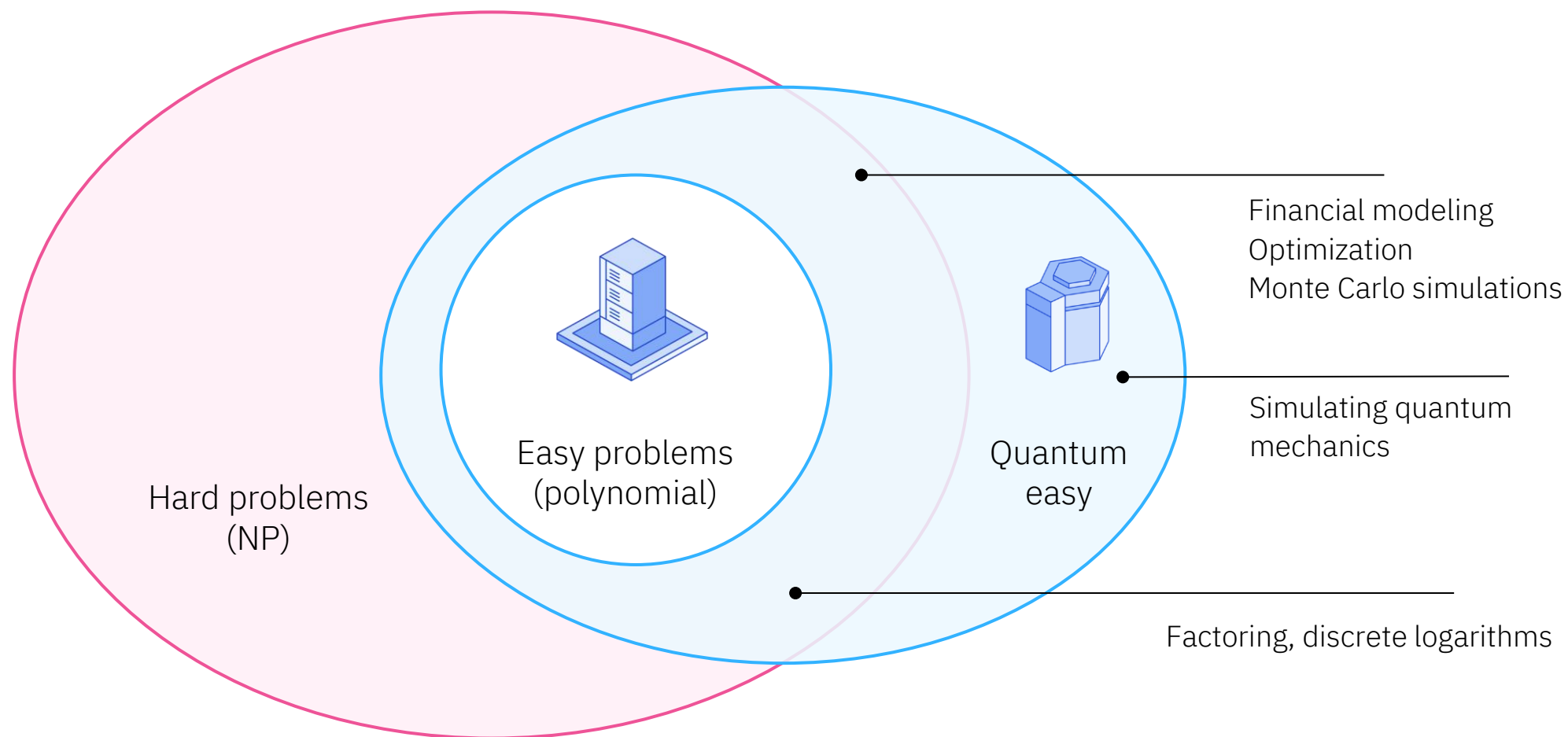
Make the world
quantum safe

Our IBM mission

Bring useful quantum
computing to the world

Make the world
quantum safe

Why quantum?



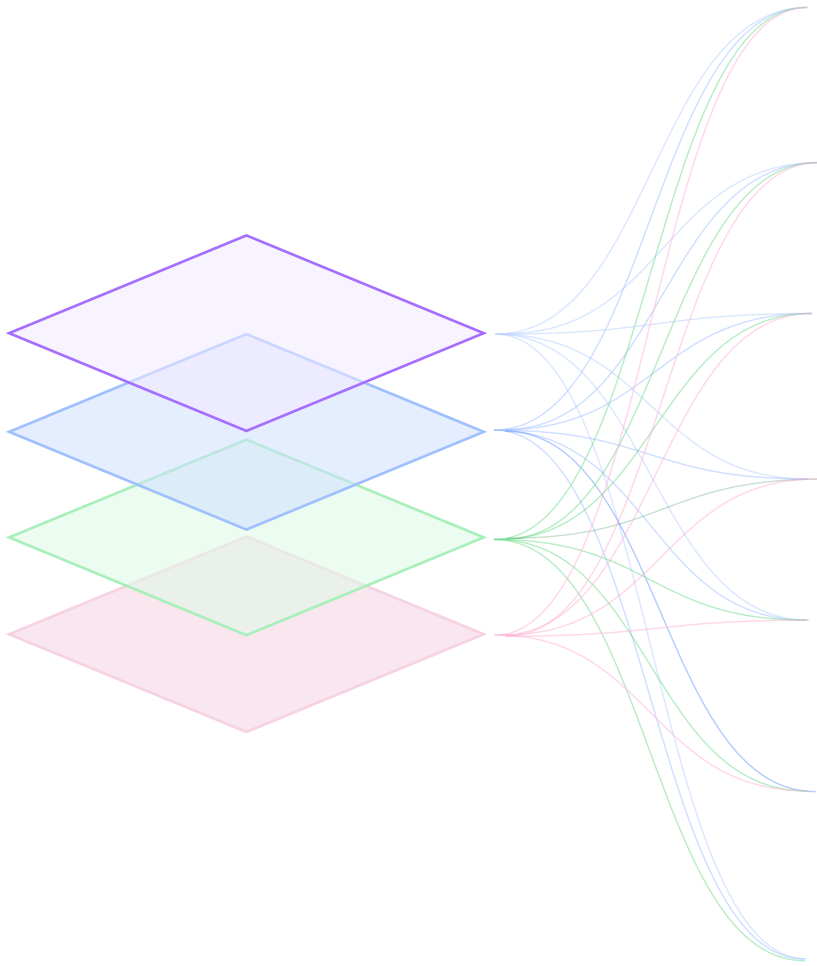
Quantum computing is expected to have impact across industries

Hamiltonian simulation

Optimization

Quantum machine learning

Partial differential equations (PDEs)



- Aerospace
 - High strength-to-weight materials development
 - Wing ply-composite design optimization
 - Aircraft computational fluid dynamics
- Automotive
 - Advanced batteries
 - Multi-objective vehicle routing optimization
 - Auto design and simulation
- Chemicals
 - Lower energy fertilizer manufacturing
 - Efficient catalysts
 - Accelerated product development
- Electronics & semiconductors
 - Placement and routing optimization
 - Deposition/etch process modeling
 - Multi-domain simulation
- Energy
 - Grid management
 - Grid optimization with EVs
 - Carbon sequestration
- Financial services
 - Portfolio optimization
 - Derivatives/options pricing
 - Anti-money laundering
- Healthcare & life sciences
 - Drug discovery and drug design optimization
 - mRNA & protein structure predictions
 - Disease target & biomarker discovery

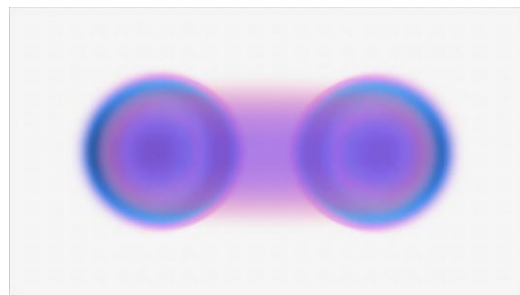
Uniquely quantum

Some problems are classically intractable and will never be solvable with traditional computers



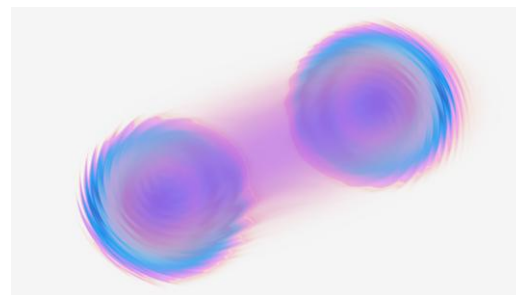
Superposition

A quantum system existing in a complex linear combination of two states until it is measured



Entanglement

Information shared jointly between entangled pairs or groups



Interference

Interaction that affects likelihood of solutions

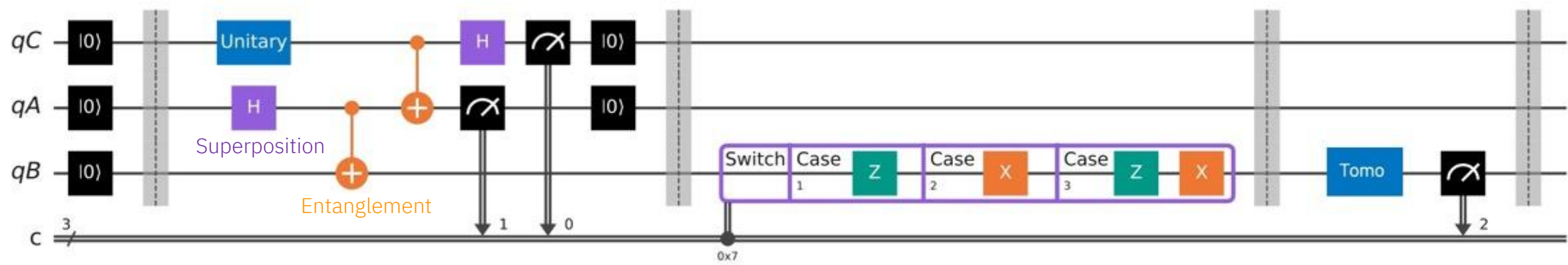
Moore's law: the number of transistors in a classical integrated circuit doubles about every two years ... but we are approaching the end due to physical limitations

[Approaching the physical limit: IBM created the world's first 2 nm node chip in 2021, with transistors as small as 10 silicon atoms](#)

These Quantum concepts can reduce the number of computational steps required for certain algorithms &

At a ~100 qubit scale, with sufficient circuit depth and complexity, classical computers can no longer simulate exactly

Quantum circuits - The fundamental unit of quantum computation



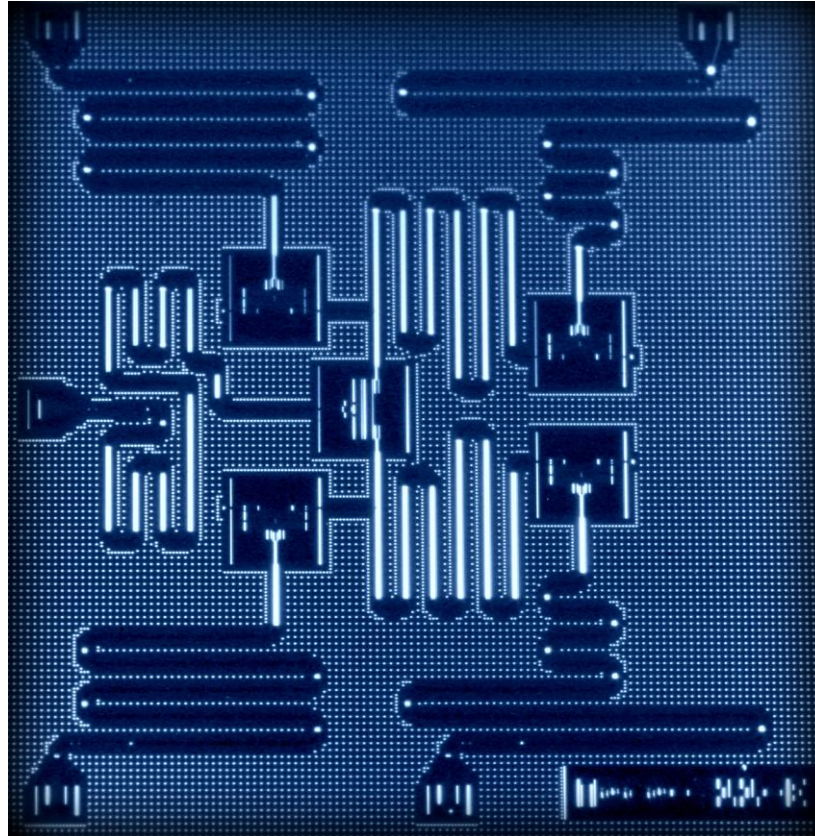
Quantum circuit:

An ordered sequence of **coherent** (reversible) **quantum gates** and **irreversible operations** that form a quantum computation

A quantum circuit can represent **any** computation provided that the quantum gates in the circuit are taken from a ‘universal’ set

— 2016

First quantum computer
on the cloud



— 2016

Mermin inequalities on a 5-qubit quantum computer

The screenshot shows the arXiv web interface for the paper 'Experimental test of Mermin inequalities on a 5-qubit quantum computer' by Daniel Alsina and José Ignacio Latorre. The page is categorized under 'Quantum Physics' and 'quant-ph'. It includes a search bar at the top right, a submission history section, and a sidebar with links to access the paper (PDF, TeX Source) and browse context (quant-ph, 2016-05). The main text describes the experimental test of Mermin inequalities on a 5-qubit IBM quantum computer, showing violation of all Mermin inequalities with a clear degradation of results in the 5-qubit case. The page also features a 'Bibliographic Tools' section with options for Bibliographic Explorer, Connected Papers, Litmaps, and scite Smart Citations.

arXiv > quant-ph > arXiv:1605.04220

Search... All fields Search

Help | Advanced Search

Quantum Physics

[Submitted on 13 May 2016 (v1), last revised 12 Jul 2016 (this version, v2)]

Experimental test of Mermin inequalities on a 5-qubit quantum computer

Daniel Alsina, José Ignacio Latorre

Violation of Mermin inequalities is tested on the 5-qubit IBM quantum computer. For 3, 4 and 5 parties, quantum states that violate the corresponding Mermin inequalities are constructed using quantum circuits on superconducting qubits. Measurements on different basis are included as additional final gates in the circuits. The experimental results obtained using the quantum computer show violation of all Mermin inequalities, with a clear degradation of the results in the 5 qubit case. Though this quantum computer is not competitive to test Mermin inequalities as compared to other techniques when applied to few qubits, it does offer the opportunity to explore multipartite entanglement for four and five qubits beyond the reach of other alternative technologies.

Comments: 4 pages
Subjects: Quantum Physics (quant-ph); Superconductivity (cond-mat.supr-con)
Cite as: arXiv:1605.04220 [quant-ph]
(or arXiv:1605.04220v2 [quant-ph] for this version)
<https://doi.org/10.48550/arXiv.1605.04220>
Journal reference: Phys. Rev. A 94, 012314 (2016)
Related DOI: <https://doi.org/10.1103/PhysRevA.94.012314>

Submission history

From: Daniel Alsina [view email]
[v1] Fri, 13 May 2016 15:43:31 UTC (463 KB)
[v2] Tue, 12 Jul 2016 16:22:38 UTC (464 KB)

Access Paper:

[View PDF](#)
[TeX Source](#)
[view license](#)

Current browse context:
quant-ph
< prev | next >
[new](#) | [recent](#) | [2016-05](#)
Change to browse by:
[cond-mat](#)
[cond-mat.supr-con](#)

References & Citations

[INSPIRE HEP](#)
[NASA ADS](#)
[Google Scholar](#)
[Semantic Scholar](#)

[Export BibTeX Citation](#)

Bookmark

[Bibliographic Tools](#) [Code, Data, Media](#) [Demos](#) [Related Papers](#) [About arXivLabs](#)

Bibliographic and Citation Tools

☐ Bibliographic Explorer ([What is the Explorer?](#))
☐ Connected Papers ([What is Connected Papers?](#))
☐ Litmaps ([What is Litmaps?](#))
☐ scite Smart Citations ([What are Smart Citations?](#))

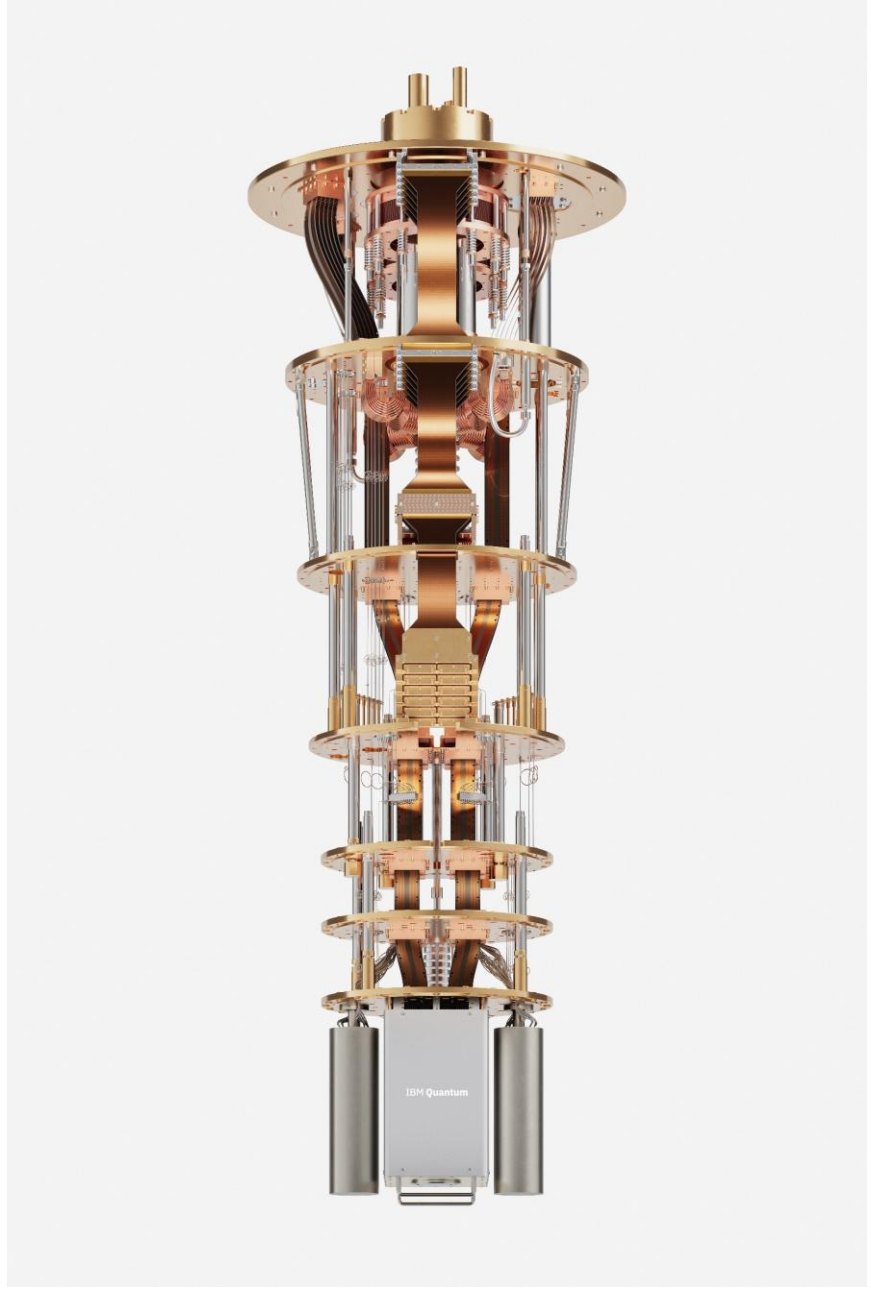
— 2026

Even before fault tolerance
useful quantum computing
is here











IBM

IBM Quantum
System Two

IBM

Q100

Q100

Q100

Q100

IBM leads in quantum computer deployments

- 60 quantum devices (<100 qubits)
- 29 quantum computers (>100 qubits) that can run circuits with >5000 two-qubit gates
- Average 97% availability across fleet
- 99% availability of at least one Heron R2+
- Job success rate >99.5%

2 Quantum Data Centers



IBM US Quantum Data Center
Poughkeepsie, USA
August 2019

Currently operating 6 quantum computers with 100+ qubits

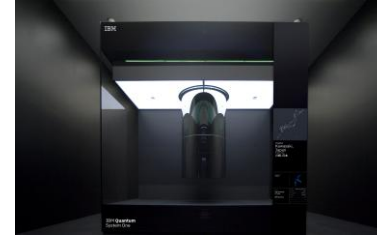


IBM EU Quantum Data Center
Ehningen, Germany
October 2024

Currently operating 3 quantum computers with 100+ qubits

9 Quantum Computers On-Site

Quantum Computational Center
University of Tokyo
Shin-Kawasaki, Japan
June 2021



Quantum Computational Center
Rensselaer Polytechnic
Troy, New York
April 2024



IBM-Euskadi Quantum Computational Center
San Sebastián, Spain
October 2025



Discovery Accelerator
Cleveland Clinic
Ohio, USA
March 2023



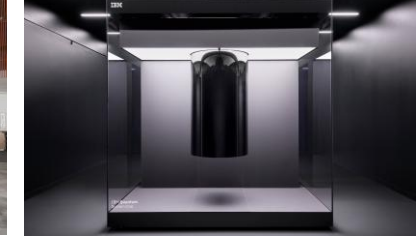
Quantum Computational Center
Yonsei University
Seoul, South Korea
September 2024



National Quantum Algorithm Center
Chicago, USA
Projected 2026



Discovery Accelerator
PINQ²
Bromont, Canada
September 2023



JHPC-quantum Riken
Kobe, Japan
May 2025



Quantum Valley Tech Park
Andhra Pradesh, India
Projected 2026



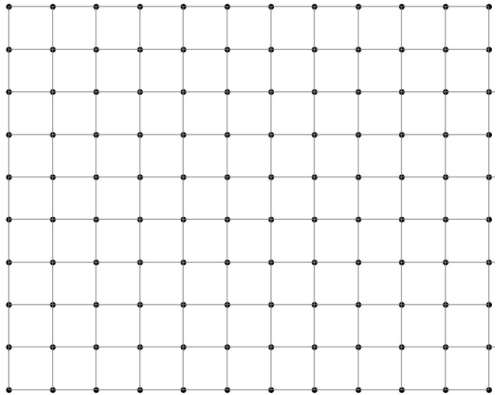
Nighthawk r2

120 programmable qubits with square connectivity

458 physical qubits

On-chip reset critical for error correction

Coming August 2026



100,000

Max circuits per second

25x

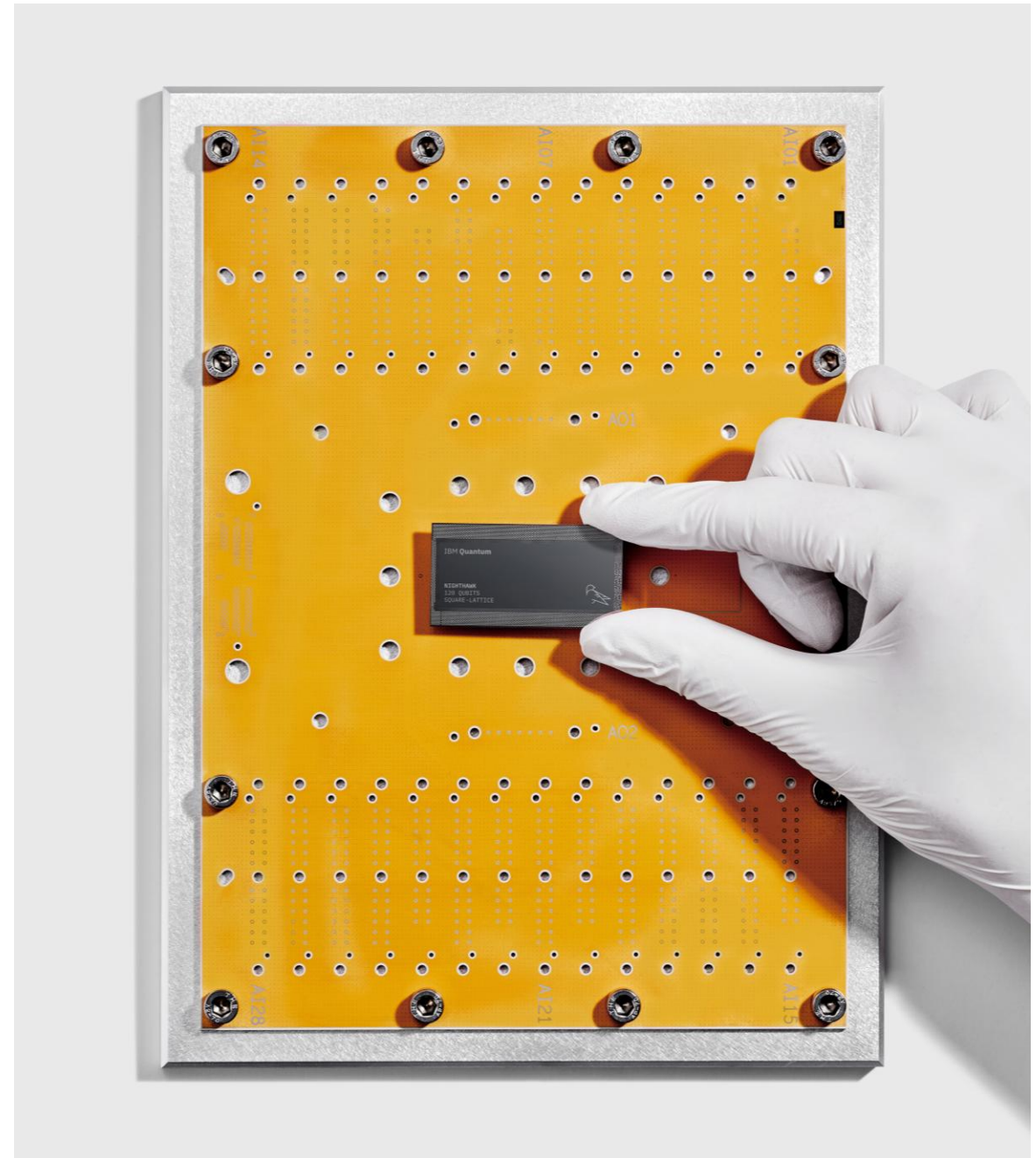
Speedup in circuits per second compared to Heron

11x

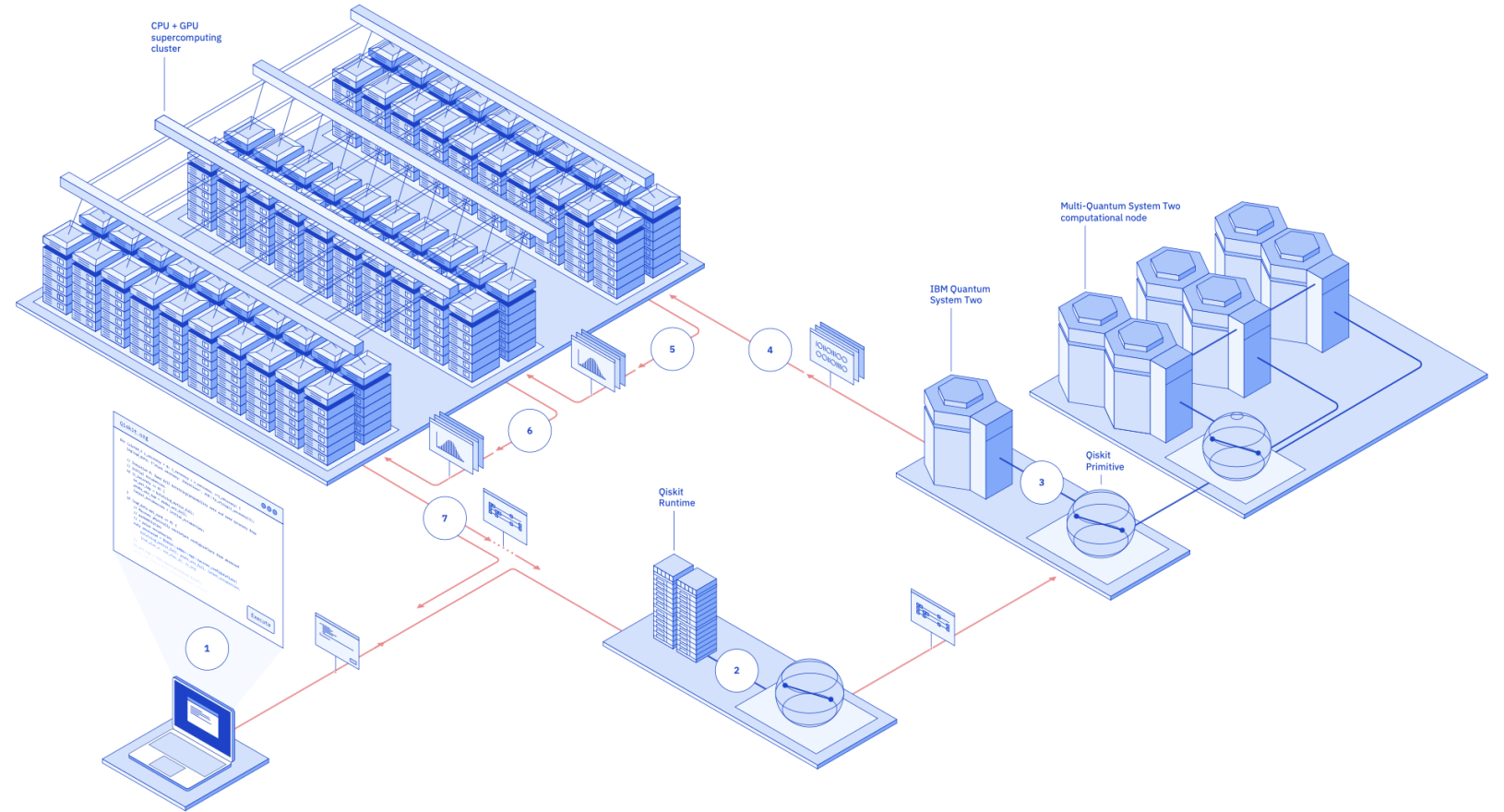
Improvement in initialization error compared to Heron

$2.7e-3$

Median 2Q error rates



CPU
+ GPU
+ QPU



Quantum-centric supercomputing

for accelerated scientific discovery

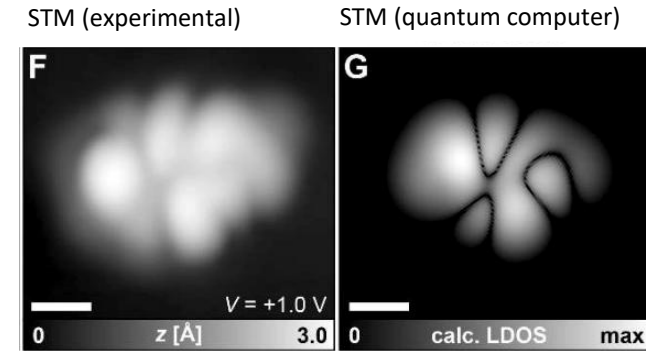
Enabling Feynman's vision with quantum-centric supercomputing

“ I’m **not happy** with all the analysis that go with just **classical theory**, because **nature isn’t classical**... And if you want to make a **simulation of nature**, you’d better **make it quantum** mechanical, and, by golly, it’s a wonderful problem because it doesn’t look so easy.

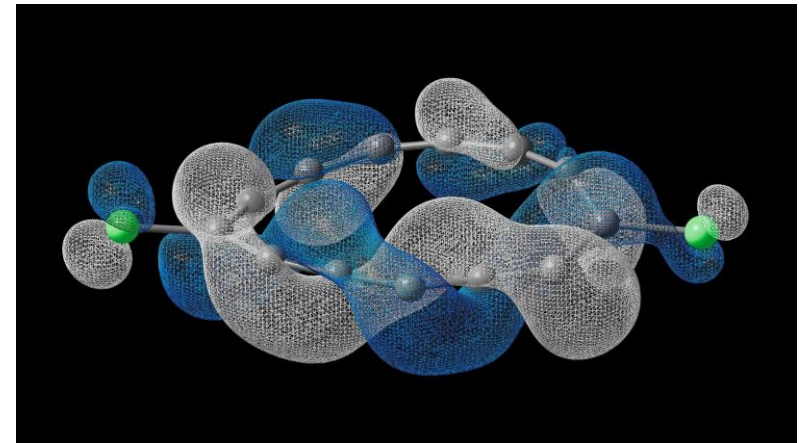
”

Richard P. Feynman
1982

SqDRIFT application to the half-Möbius molecule created by atomic manipulation in IBM laboratories



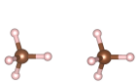
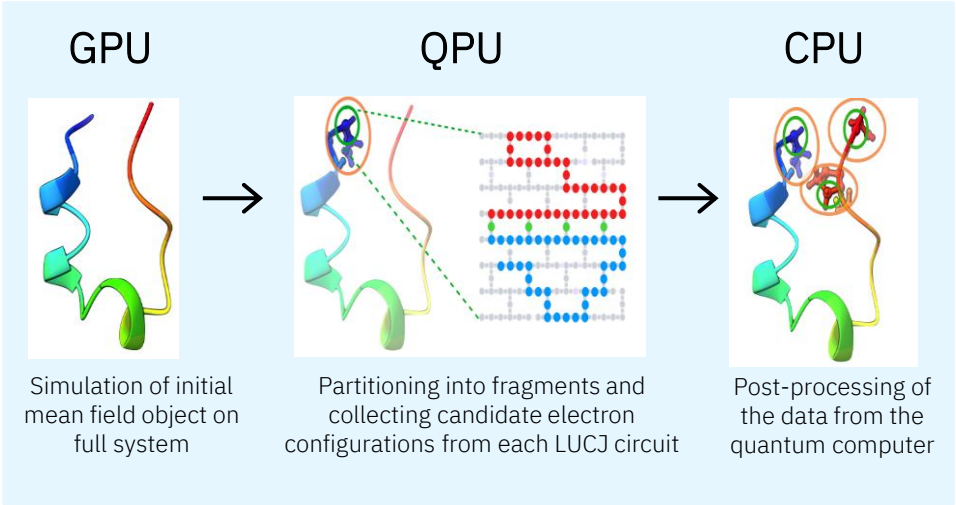
STM images of the Dyson orbital



Dyson orbital computed with SqDRIFT on 72 qubits

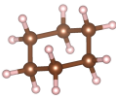
Rončević et al., Science (5 March 2026)
and arXiv:2507.03516

Pushing the scale of chemistry applications with quantum-centric supercomputing



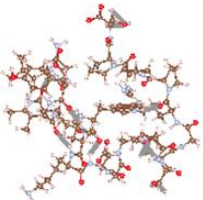
10 atoms

2024
October
arXiv:2410.09209



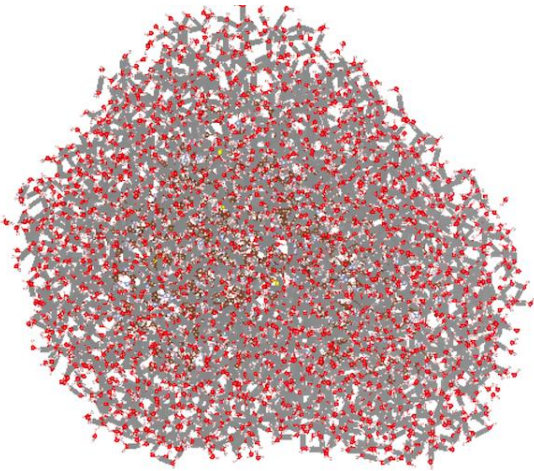
36 atoms

2024
November
arXiv:2411.09861



303 atoms

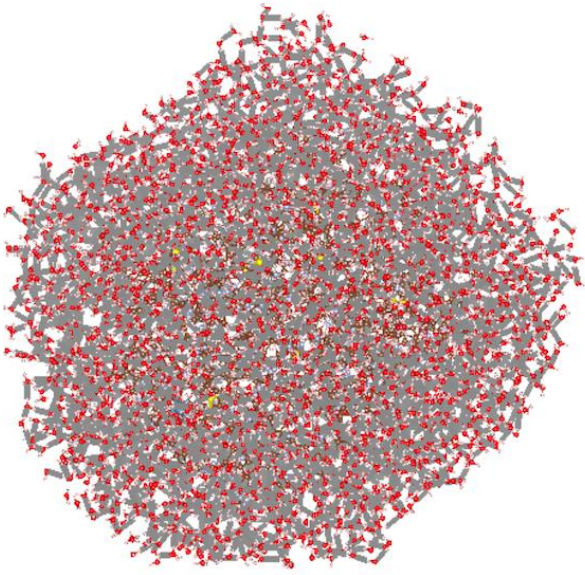
2025
December
arXiv:2512.17130



11,608 atoms

2026
April
arXiv:2605.01138

In collaboration with:
RIKEN



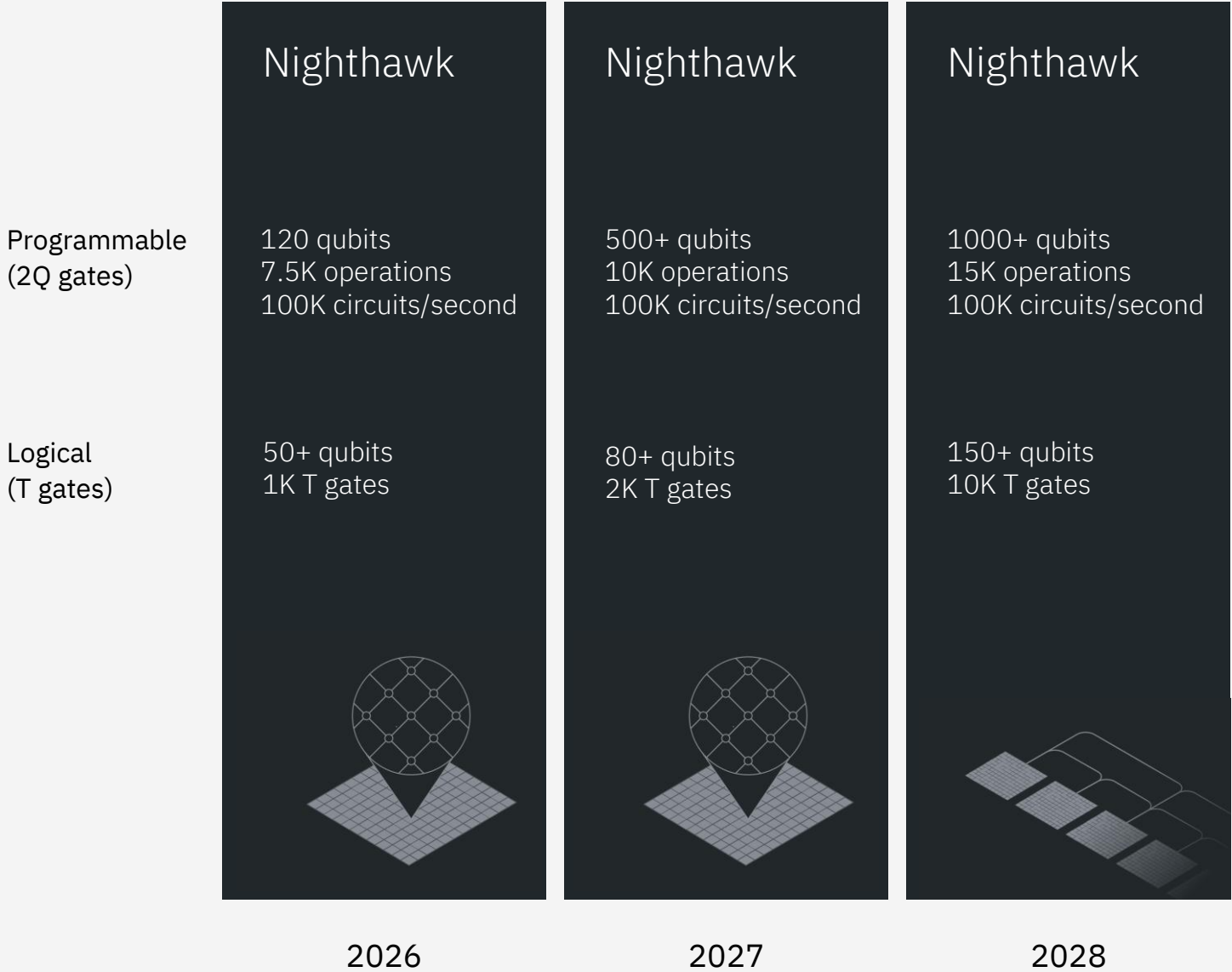
12,635 atoms

2026
April
arXiv:2605.01138

Quantum computational performance

- Key performance metrics:
- Number of programmable qubits
 - Number of qubit operations
 - Throughput (Max circuits per second)

IBM Quantum Nighthawk: Outlook on client-accessible IBM quantum systems



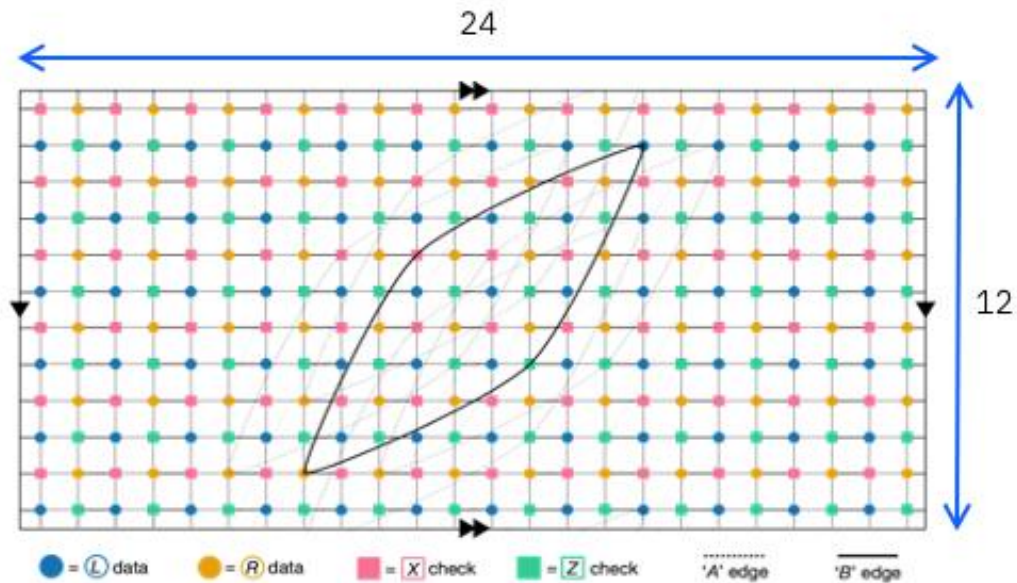
— 2029

Starling



Why do we have confidence in 2029 to deliver fault-tolerant quantum computing?

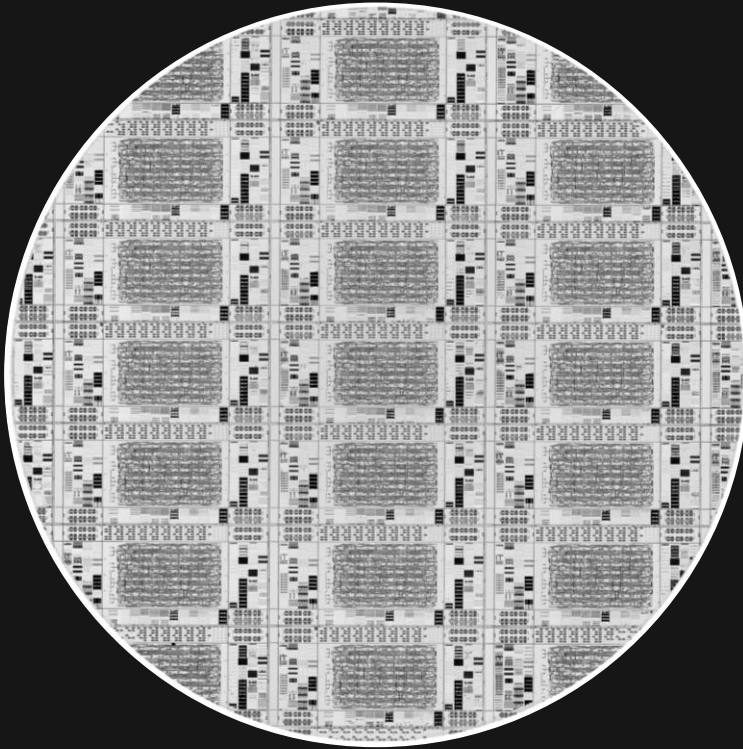
We have developed a more efficient error correction code and demonstrated the ability to run the decoder software on relatively low-cost electronics



The gross code is 10x more efficient than the surface code



Building the first large-scale, fault-tolerant quantum computer



IBM Quantum Loon

2025

Loon



Demonstrate c-couplers and next-generation packaging for FTQC

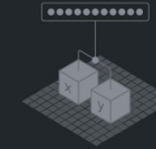


2026

Kookaburra



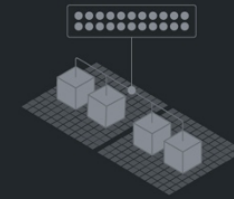
Demonstrate a complete module consisting of a logical processing unit and quantum memory



2027

Cockatoo

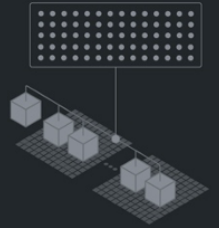
Demonstrate entanglement of modules using a universal adapter



2028

Starling

Demonstrate multiple modules and magic state distillation

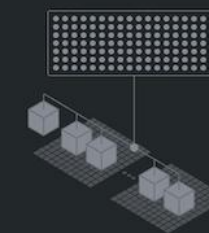


2029

Starling (100M)

Fault-tolerant

100M gates
200 qubits

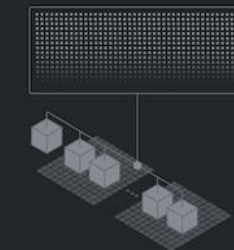


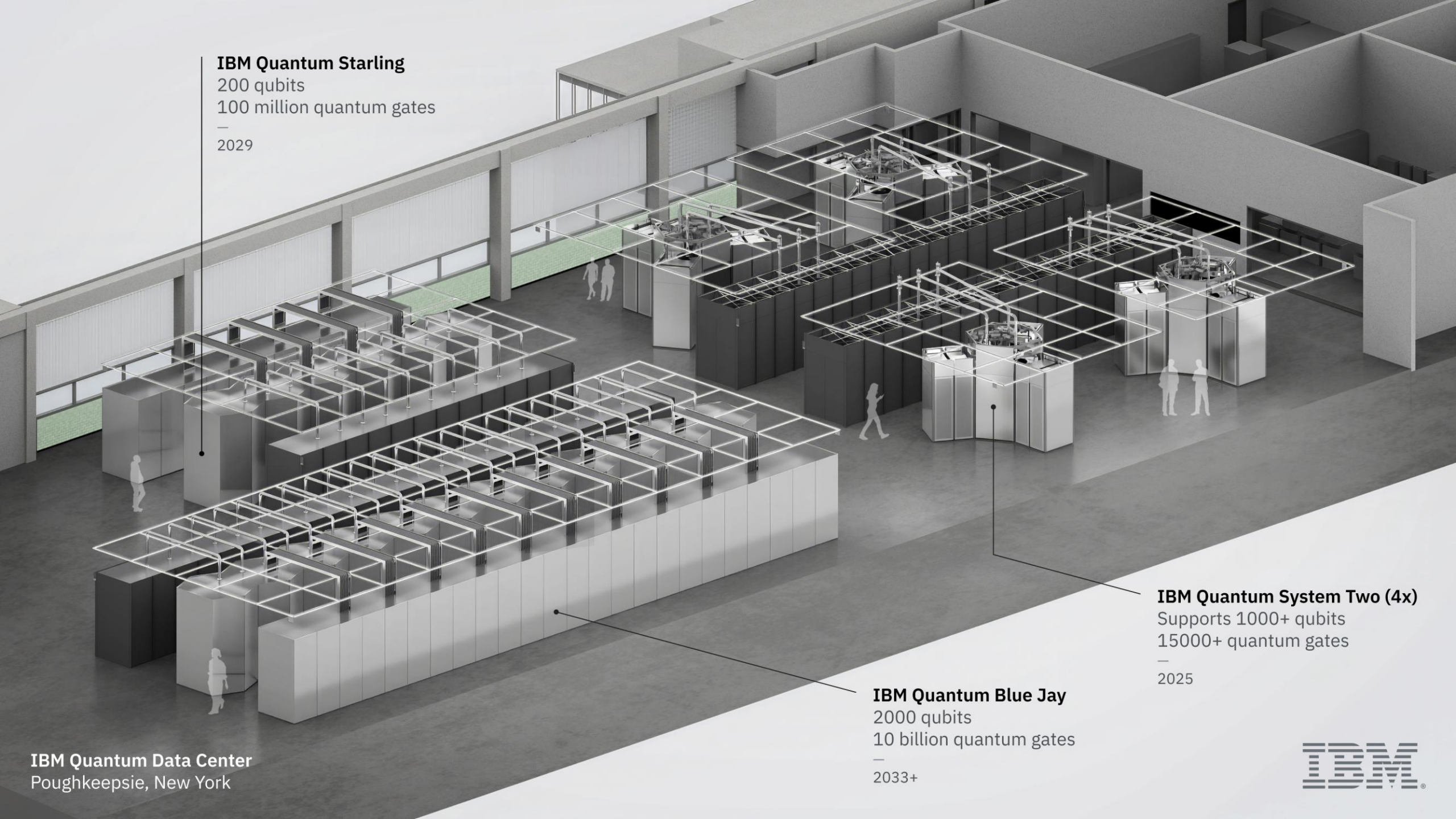
2033+

Blue Jay (10B)

Fault-tolerant

10B gates
2000 qubits





The image is an isometric architectural rendering of the IBM Quantum Data Center in Poughkeepsie, New York. It depicts a large, modern facility with multiple levels and a complex network of server racks and quantum computing hardware. The rendering is in a grayscale style with some green accents on the walls. Several human figures are placed throughout the space to provide a sense of scale. Three specific quantum computing systems are highlighted with callout lines and text boxes: IBM Quantum Starling, IBM Quantum System Two (4x), and IBM Quantum Blue Jay. The IBM logo is located in the bottom right corner.

IBM Quantum Starling

200 qubits

100 million quantum gates

—

2029

IBM Quantum System Two (4x)

Supports 1000+ qubits

15000+ quantum gates

—

2025

IBM Quantum Blue Jay

2000 qubits

10 billion quantum gates

—

2033+

IBM Quantum Data Center
Poughkeepsie, New York



Ecosystem

IBM has the largest and most advanced network advancing quantum computing

The IBM Quantum Network has 325+ members

Industry members	70+
Commercial partners and startups	70+
Academic and research institutions	170+

Oak Ridge National Laboratory and the oak leaf symbol are registered trademarks of the U.S. Department of Energy. Use of this mark does not constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors.



IBM Quantum offerings

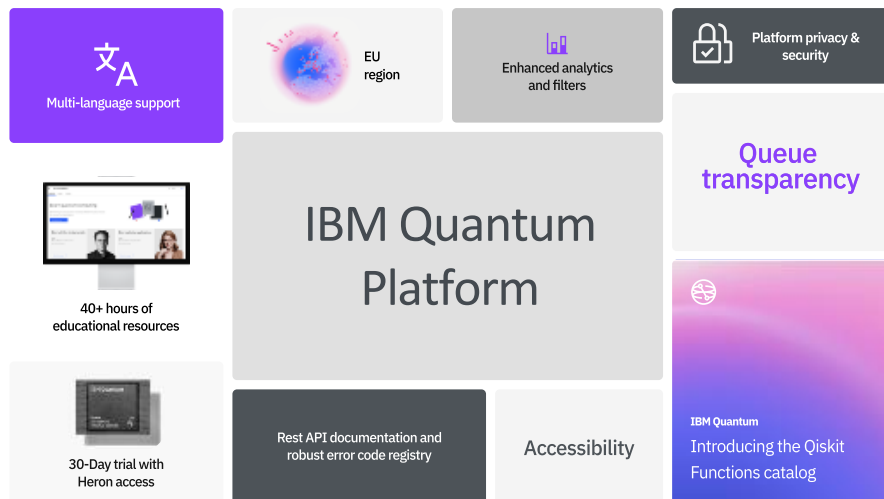
Access quantum computing

Provided pricing assumes use of
<200 qubit quantum computers

Open Plan	Pay-as-you-go Plan	Flex Plan	Premium Plan	On-Prem Plan
		Subscription required	Subscription required	Subscription required
Best for Learning quantum computing and exploring IBM quantum technology.	Best for Discovering quantum utility through proof-of-concept and business model validation.	Best for Performing quantum utility research projects and prototyping with flexible access.	Best for Executing a strategic quantum roadmap and developing quantum algorithms and applications at scale.	Best for Exploring quantum algorithms and applications with high control over your resources and data.
✓ Access to IBM Quantum Compute service ✓ Access to 100+ qubit utility-scale quantum computers	✓ Access to IBM Quantum Compute service ✓ Access to 100+ qubit utility-scale quantum computers ✓ IBM Quantum™ technical support	✓ Access to IBM Quantum Compute service ✓ Access to 100+ qubit utility-scale quantum computers ✓ IBM Quantum technical support ✓ IBM Quantum Network membership¹ ✓ Optional access to our Quantum Accelerator offering ✓ Advanced software features ✓ Early access to new features <u>Purchased in Resource Units (RUs)</u> 1 RU = 1 min. of usage on <200 qubit computer 0.5 min. on 200 to <500 qubit computer ¹: 3,500 RU minimum purchase required	✓ Access to IBM Quantum Compute service ✓ Access to 100+ qubit utility-scale quantum computers ✓ IBM Quantum technical support ✓ IBM Quantum Network membership ✓ Optional access to our Quantum Accelerator offering ✓ Advanced software features ✓ Early access to new features <u>Purchased in Quantum Allocation Units (QAUs)</u> 1 QAU = up to 1600 RUs per 28-day period 1 RU = 1 min. of usage on <200 qubit computer 0.5 min. on 200 to <500 qubit computer	✓ Access to IBM Quantum Compute service ✓ Access to 100+ qubit utility-scale quantum computers ✓ IBM Quantum technical support ✓ IBM Quantum Network membership ✓ Optional access to our Quantum Accelerator offering ✓ Advanced software features ✓ Full computer capacity purchased as a service ✓ Quantum system location on client site
Free Access to utility scale quantum computers for up to 10 minutes of runtime per month.	Starting at \$96 USD / minute Pay for what you use. Billed per second of usage via IBM Cloud.	Starting at \$72 USD / minute* Purchase the capacity you need with Resource Units and use them throughout the contract period. *Based on list price for 1 RU (Resource Unit) purchase with min. of 400 RUs	Equivalent to \$48 USD / minute* Reserve the capacity you need for the year with Quantum Allocation Units and use up to 1600 minutes per QAU every 28-day rolling time-window. *Based on list price for 1 QAU (Quantum Allocation Unit) purchased with min. of ¼ QAU	Price requires quote Access to an entirely on-prem quantum system that is serviced and maintained by IBM.

A PLATFORM for quantum computing

IBM Quantum Platform

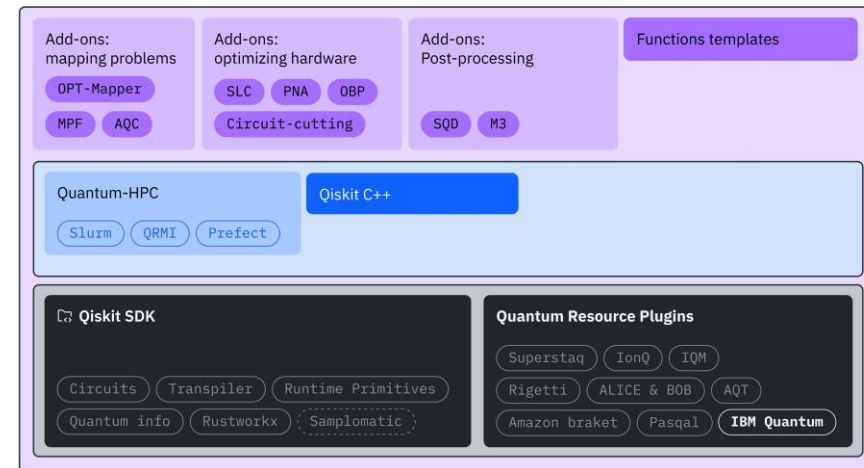


A cloud platform that allows us to deliver the most performant 100Q+ quantum computers for global distribution

A set of runtime and application services that enable you to unlock advantage on today's systems

Qiskit

- Qiskit for:
 - Algorithm research
- Qiskit for:
 - High Performance Computing
- Qiskit for:
 - Quantum information science research



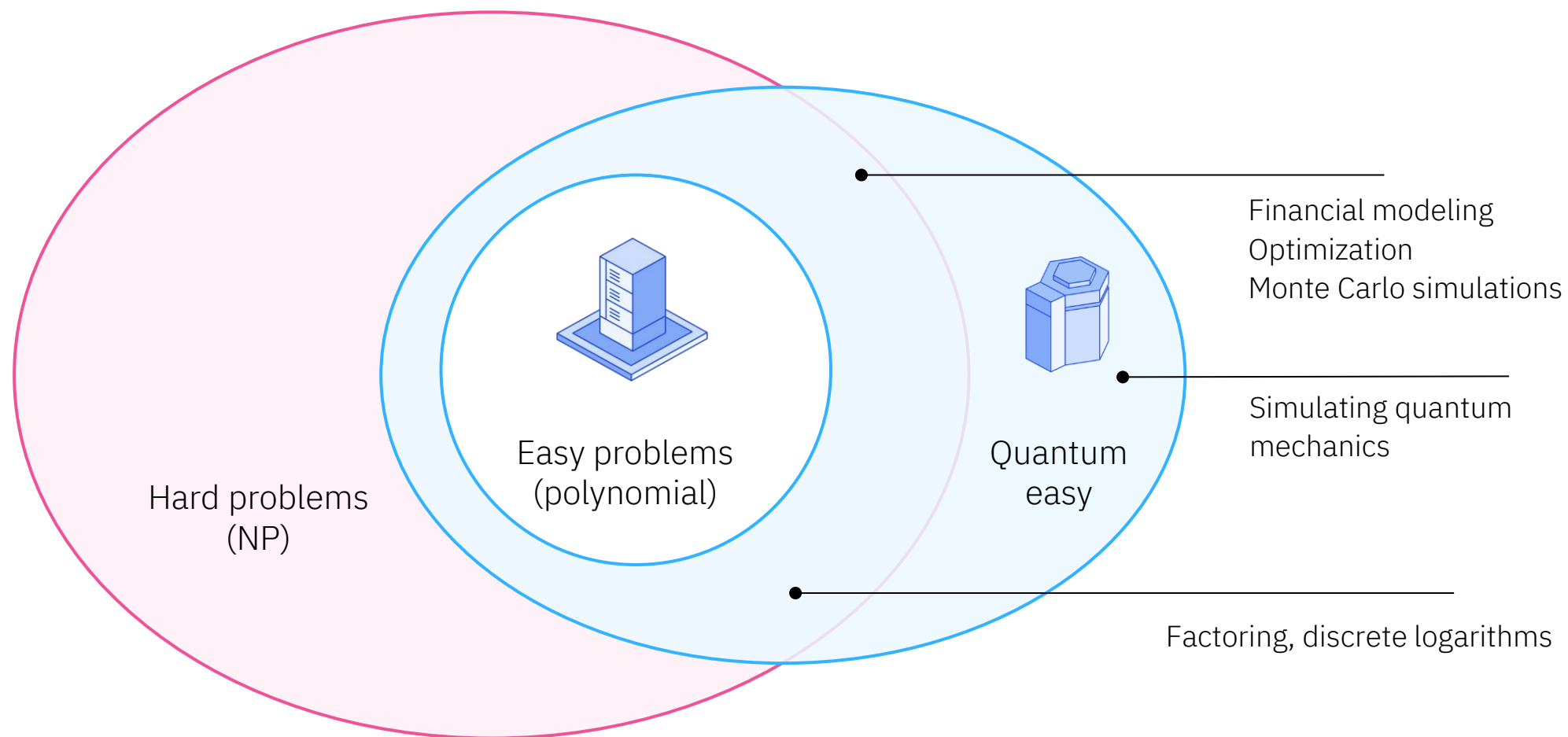
An open SDK that provides flexible and comprehensive interfaces for building, optimizing, and executing quantum circuits at scale

A collection of open science tools for designing QCS and developing novel algorithms

Bring useful quantum
computing to the world

Make the world
quantum safe

Why quantum?



Today’s classical security protocols
will be obsolete tomorrow

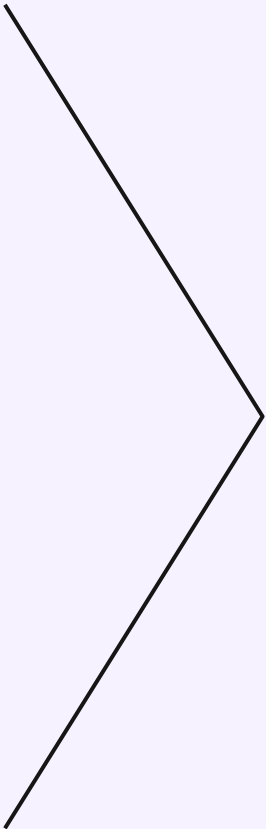
Prime factors = p x q	2048-bit composite integer 251959084756578934940271832400483985714292821262040320 277771378360436620207075955562640185258807844069182906 412495150821892985591491761845028084891200728449926873 928072877767359714183472702618963750149718246911650776 133798590957000973304597488084284017974291006424586918 171951187461215151726546322822168699875491824224336372 590851418654620435767984233871847744479207399342365848 238242811981638150106748104516603773060562016196762561 338441436038339044149526344321901146575444541784240209 246165157233507787077498171257724679629263863563732899 121548314381678998850404453640235273819513786365643921 2010397122822120720357	Expected computation time The most powerful computer today: Millions of years Shor’s quantum algorithm: Hours
---	--	--

Public key encryption • Digital signatures • Key exchange algorithms

RSA • DSA • ECC • ECDSA • DH

Our digital world depends on cryptography, which is used in trillions of transactions on billions of devices

- Internet**
Domain name system (DNS), Hypertext Transfer Protocol (HTTPS), Telnet, file transfer protocol (FTPS)
- Digital signatures**
Electronic identification and trust services (eIDAS), PDF advanced electronic signature (PAdES), advanced electronic signatures
- Critical infrastructure**
Code updates, control systems, car systems
- Financial systems**
Payment systems: EMV, CHAPS, Fedwire, TARGET2, EURO1; SWIFT; settlement systems
- Blockchain**
Wallets, transactions, authentication
- Enterprise**
Email: PGP, identity management, PKI, LDAP; virus scanning patterns; PKI services; bespoke applications



- Systems have long update cycles**
 - Passports: 10 years from issue
 - Road vehicles: 15–20 years
 - Aircraft/rail: 25–30 years
 - Some critical infrastructure: 50+ years
- Data needs to stay secure for a long time**
 - HIPAA: 6 years from last use per Security Rule
 - Tax records: 7–10 years in most countries; Sarbanes-Oxley Act set the precedent in the US
 - Legitimate interest under GDPR: 20+ years
 - Toxic Substances Control Act/Occupational Safety and Health Act: up to 30 years

What can a cybercriminal do?

Harvest now, decrypt later

Before



Harvest confidential data to decrypt later

Availability of “cryptographically relevant” quantum computers

After



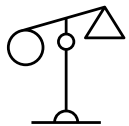
Decrypt lost or harvested confidential data by breaking encryption

Launch extortion attacks by threatening to disclose harvested data



Disrupt business with manipulation through fraudulent authentication

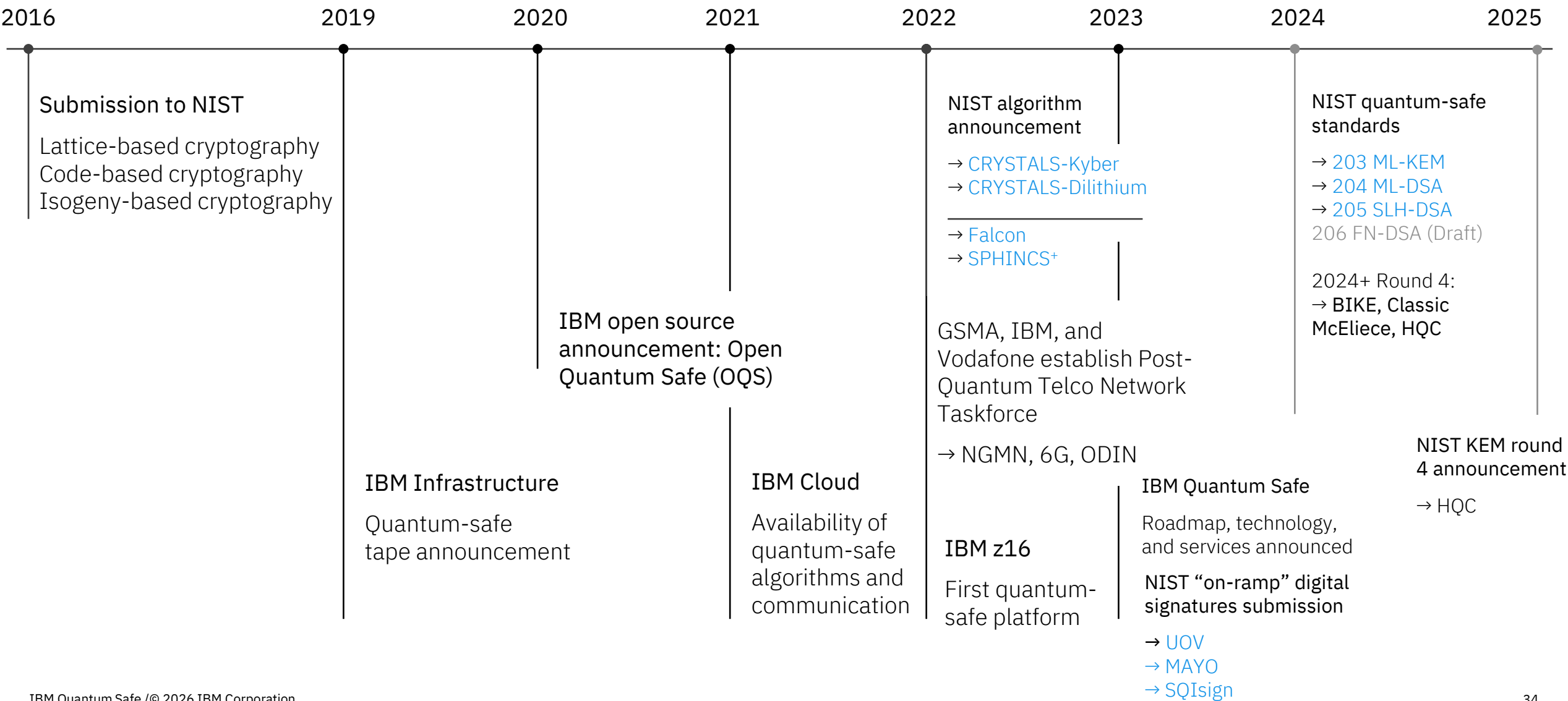
Create fake identities for websites or system administrators



Manipulate digitally signed contracts and legal history by forging digital signatures

Create fake software downloads and software updates, create indistinguishable fraudulent land records or lease documents

Launching the era of quantum safe in IBM



NIST standardization for Quantum-Safe Cryptography

NIST Standards

NIST published in August 2024 the **final Standards** for 3 out of the 4 quantum-safe algorithms selected.

A draft standard for *FN-DSA*, a further lattice-based algorithm for digital signatures is expected in 2026.

A final standard for a further KEM, based on **HQC** can be expected approximately in 2027.

FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

ML-KEM: Primary algorithm for Key encapsulation (to be used for key exchange)

FIPS 204

Federal Information Processing Standards Publication

Module-Lattice-Based Digital Signature Standard

ML-DSA: Primary algorithm for digital signatures

FIPS 205

Federal Information Processing Standards Publication

Stateless Hash-Based Digital Signature Standard

SLH-DSA: Stateless hash-based algorithm for digital signatures

When will Cryptographically Relevant Quantum computers be available?

Governments and industry associations all over the world urge for a complete transition in the early 2030s

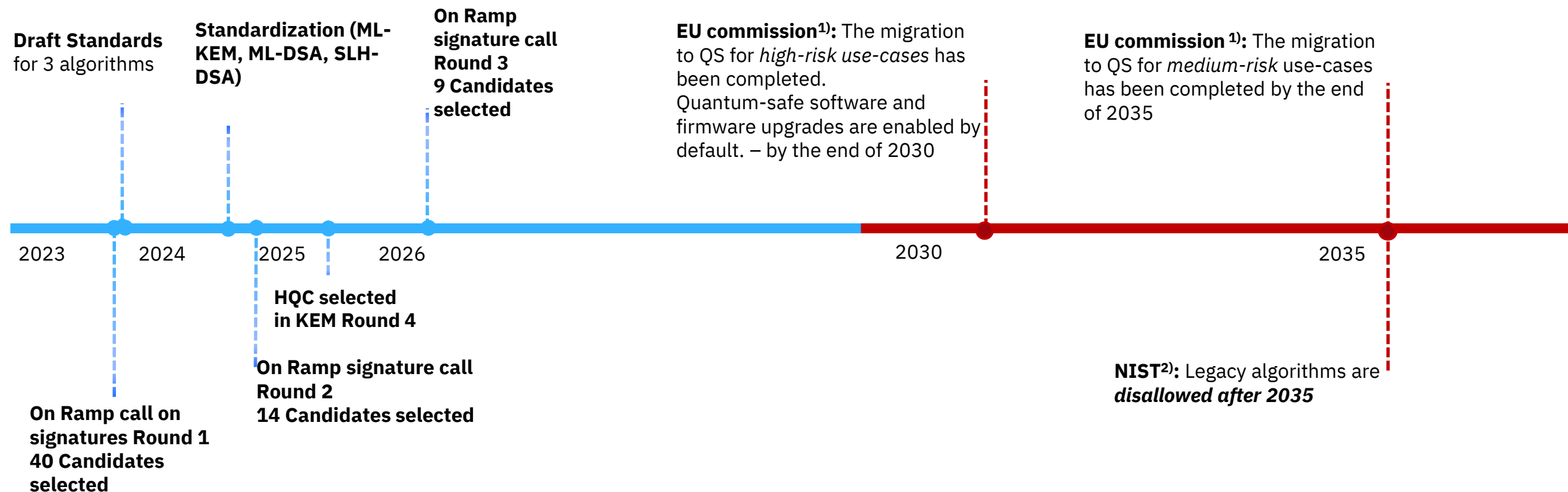
The exact date of the development of a CRQC cannot be foreseen with certainty

Organizations should monitor advancements in Quantum hardware, error correction & Quantum algorithms, and align to **guidance** given by international regulators

NIST: Expected date of deprecation of legacy cryptography - **2035**



Quantum-safe cryptography timeline



1. <https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography>
2. <https://csrc.nist.gov/pubs/ir/8547/ipd> (Draft)

There will be differences ...



Enter text to sign: baanana weise signed

Signing data with key: DSA

Signature is:

```
290153D9DC848796B849E2F39379D99977A3A95F56D2F5DD7AB797D11158E54343406061B393E850E0562AF5E81DA039EBA009C022446EA722552B7E24297D93
```

DSA signature is 64 bytes

Enter text to sign: baanana weise signed

Signing data with key: RSA

Signature is:

```
11926725C407AE1A0DDAB1AB7377675235C6A0D07BBE5BCA9C0C88EA02A5F7383784BA8339CEA2752EB1F92531133BD6045E7B615B7ECA8357CD7CD308704C8DF6F225D4DAAB0F7794F2EB11E38940FBE63  
AFDD326A43B01ECBFA8870F52B349D06E82851A8391B799C178A07A1B60008EC91CB3C88A1996F69F3B49F1BB284C34D90602FC28EEA678D20B279301562163851B11EDB0C5B8426CA1DE94B83B16BC4B81  
FB94043B04A654842ED4E0091CA02A9B91A0F1C40660C09F6B71D45A121F963A7A70DF3A6F8445D768686F4B5CCFAE09941A3AACD69F450FB681E5FBA598A7A8D1A0957B85975EA08C739D36F76C25380CE9  
A6035C4074CA64B5E519F0
```

RSA signature is 256 bytes

Signature is:

PQC signature is 3293 bytes !!

The new algorithms are not drop-in replacements.

Planning for a
quantum-safe future

How do we [protect our data](#)—now and in the future?

How do we understand our [cryptography usage](#)?

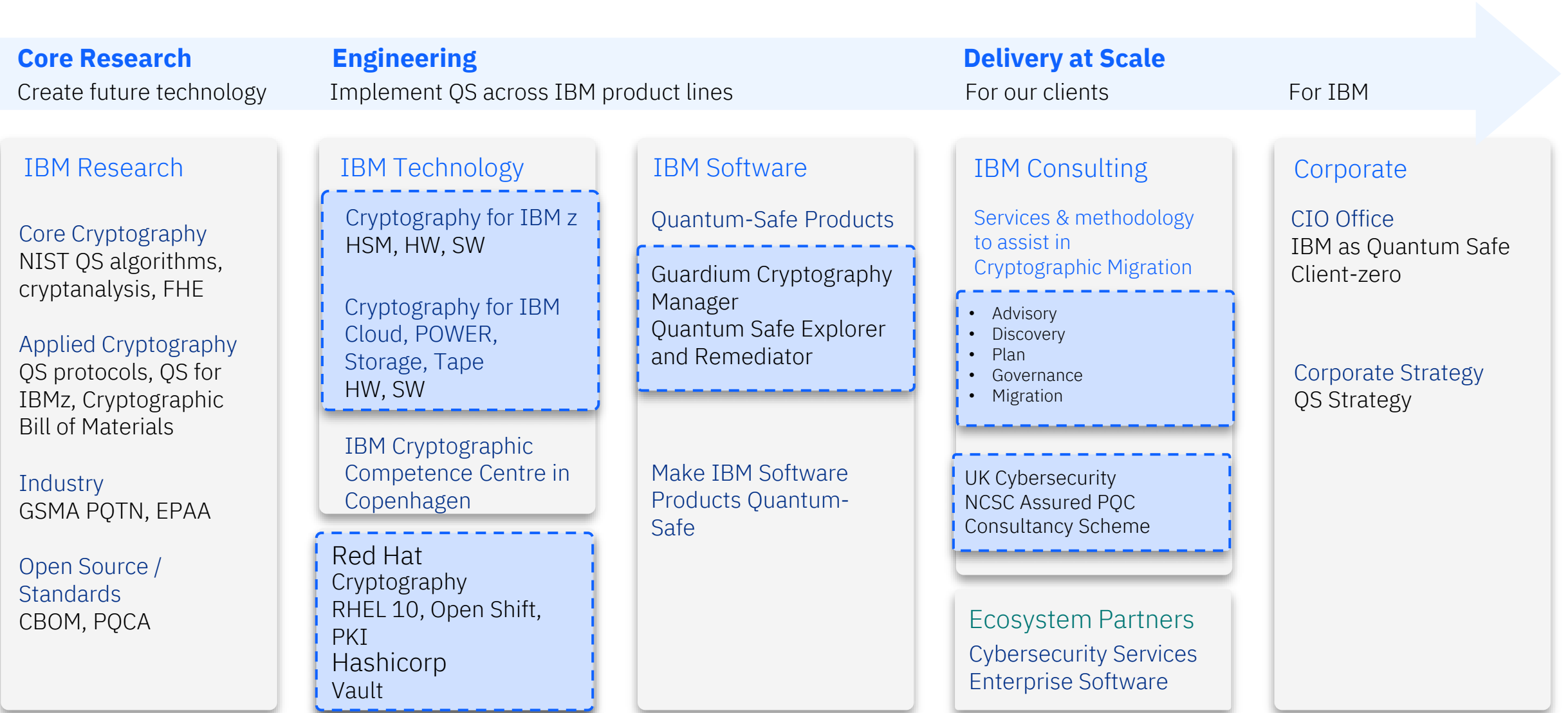
What is our current [risk exposure](#)?

When—and how—do we begin our [quantum-safe transition](#)?



IBM and Quantum Safe

A Global Mission



The time to start is now

Understand
quantum risks and
quantum-safe
priorities



Identify risk &
dependencies and
prioritize actions



Initiate and
implement a
quantum-safe
program



Next step : reach us !

IBM Quantum technology



Pierre Jaeger
Quantum Strategic Partnership Executive
pierre.jaeger@fr.ibm.com
+33-6-8909-4131

Save Pierre contact



IBM Quantum-safe technologies



Zineddine Gherari
Advisory Data & AI Technical Specialist
zineddine.gherari@fr.ibm.com
+33-6-08-10-66-79

Save Zineddine contact

