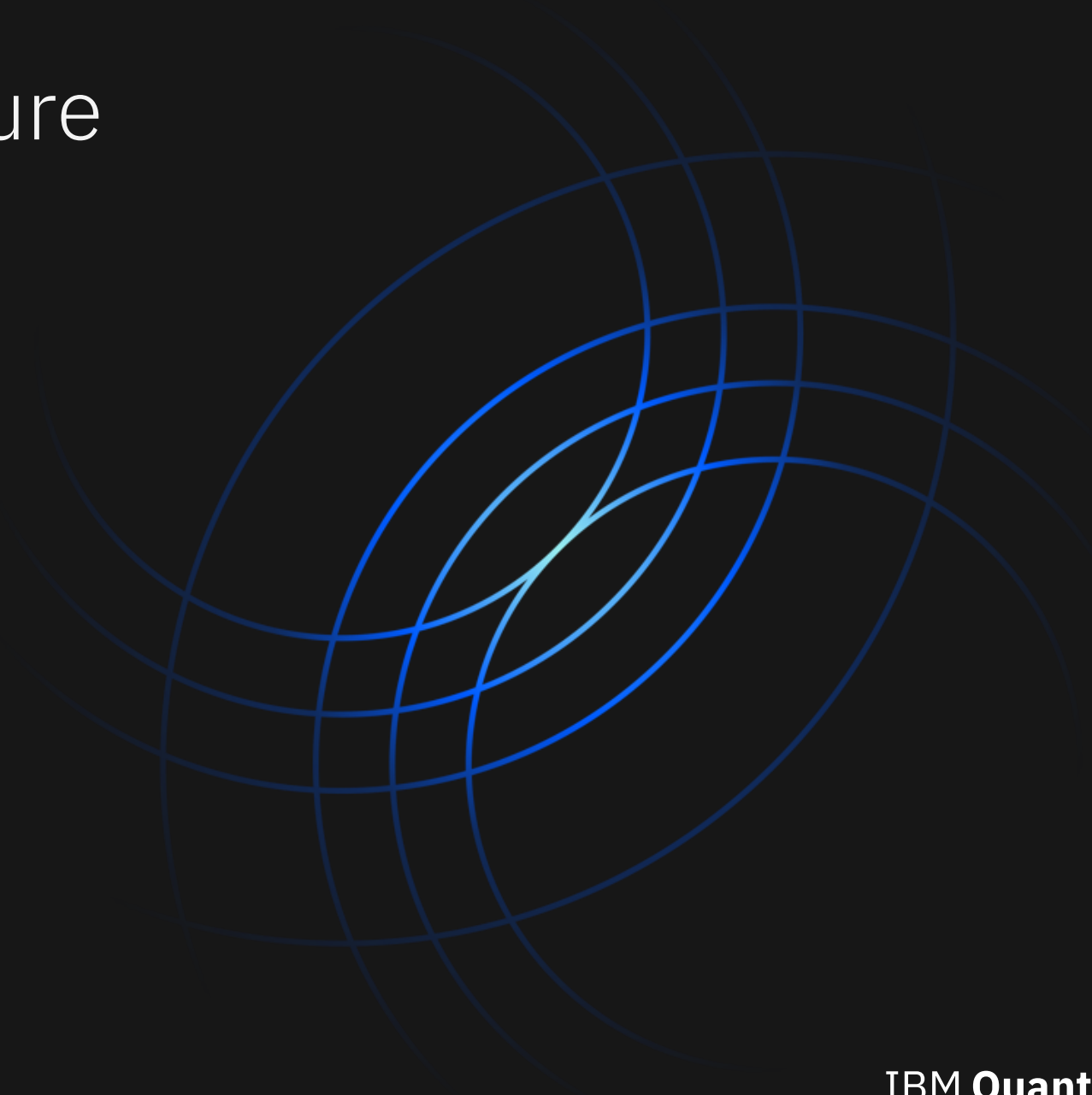
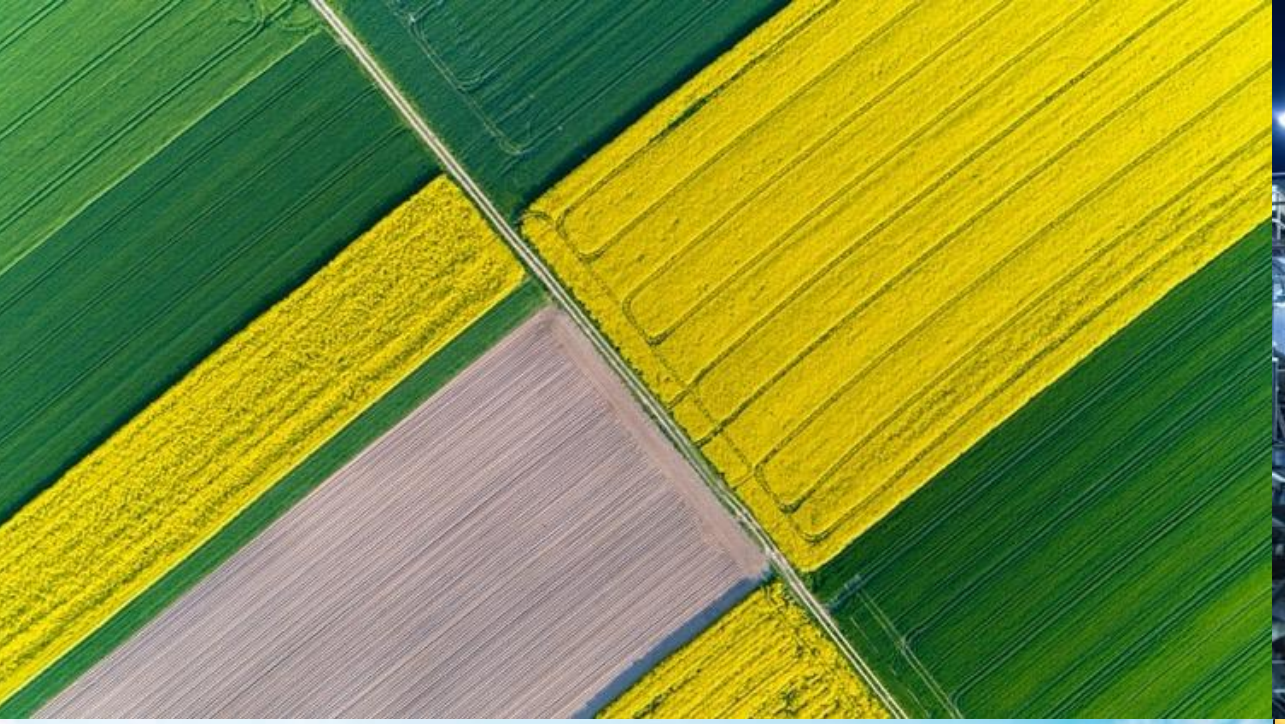
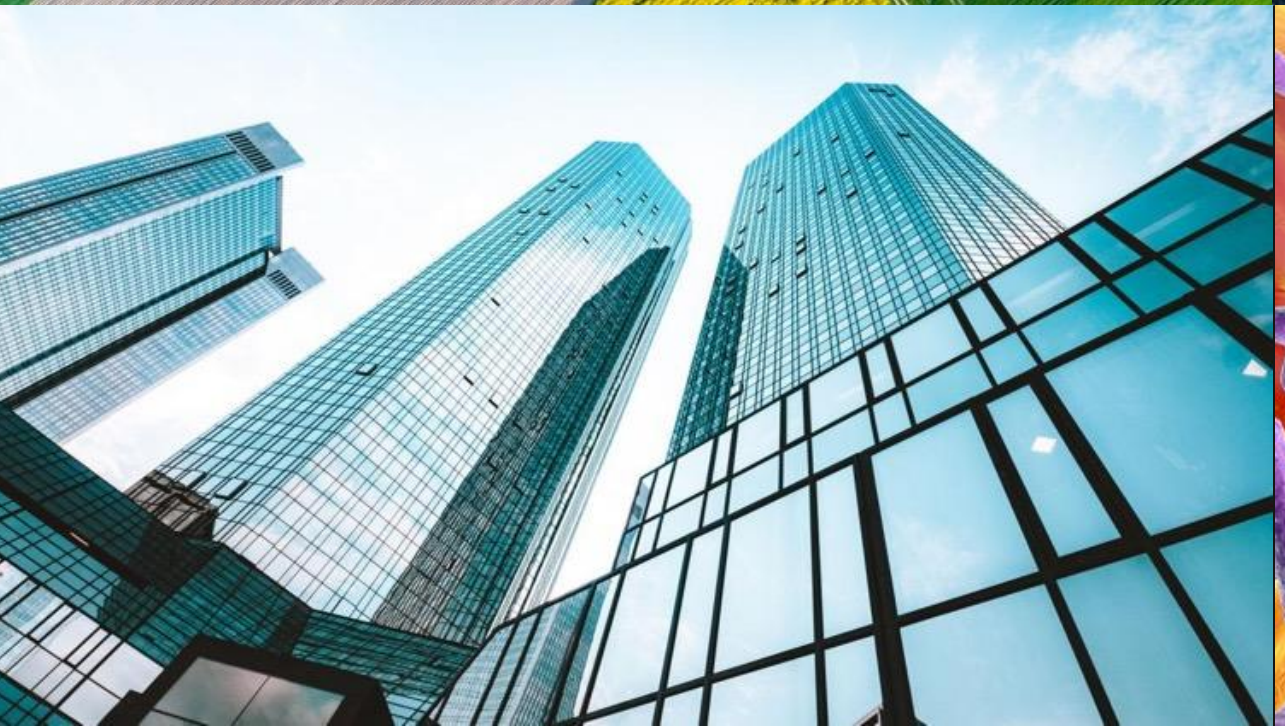
The Quantum Decade: India’s Leap into the Future

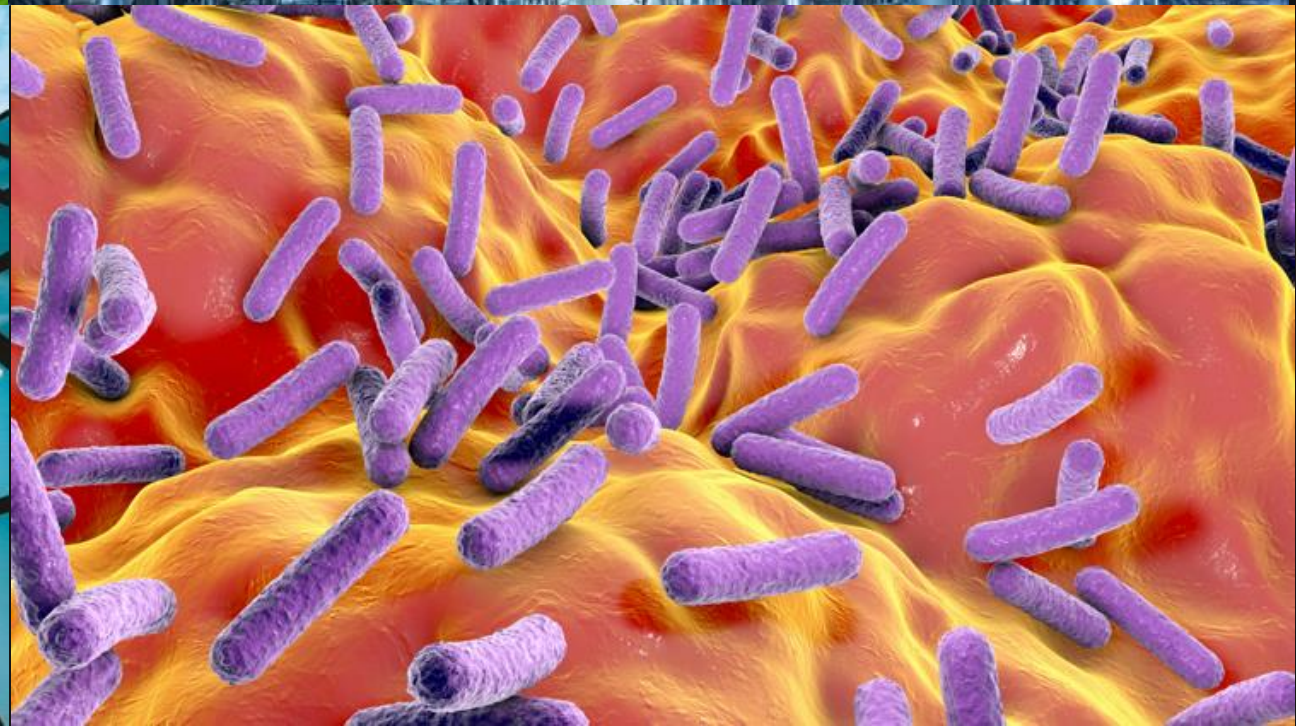
L Venkata Subramaniam
IBM Quantum India Lead



IBM **Quantum**







Improved nitrogen-fixation process for creating ammonia-based fertilizer

New catalysts to make CO_2 conversion into hydrocarbons more efficient and selective

Better financial models to improve stability, predictability and growth of world economies

New classes of antibiotics to counter the emergence of multidrug-resistant bacterial strains

One of the world's most powerful supercomputer

Oak Ridge National Laboratory
US Department of Energy

Summit supercomputer specs

200 quadrillion calculations per second

9216 IBM Power 9 processors

27,648 NVIDIA GPUs

250 PB File System

IBM Red Hat Enterprise Linux (RHEL) v 7.4 Operating System

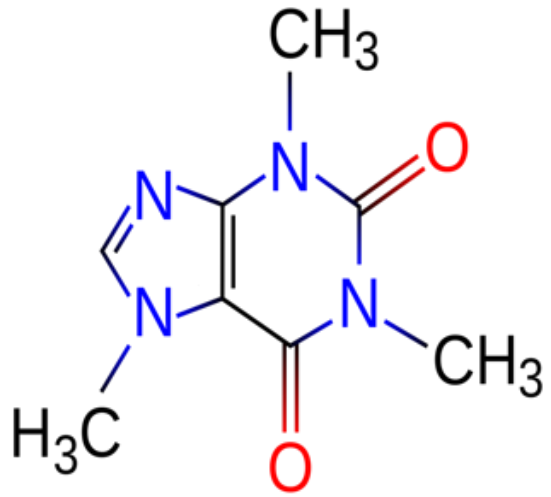
https://www.ibm.com/thought-leadership/summit-supercomputer/

Computing with caffeine

If our best classical computers are so powerful, shouldn’t we be able to perfectly simulate molecules and chemical reactions?

This would allow us to accelerate discovery of new compounds and processes for healthcare, materials, alloys, and sustainable energy creation.

Let’s consider caffeine …



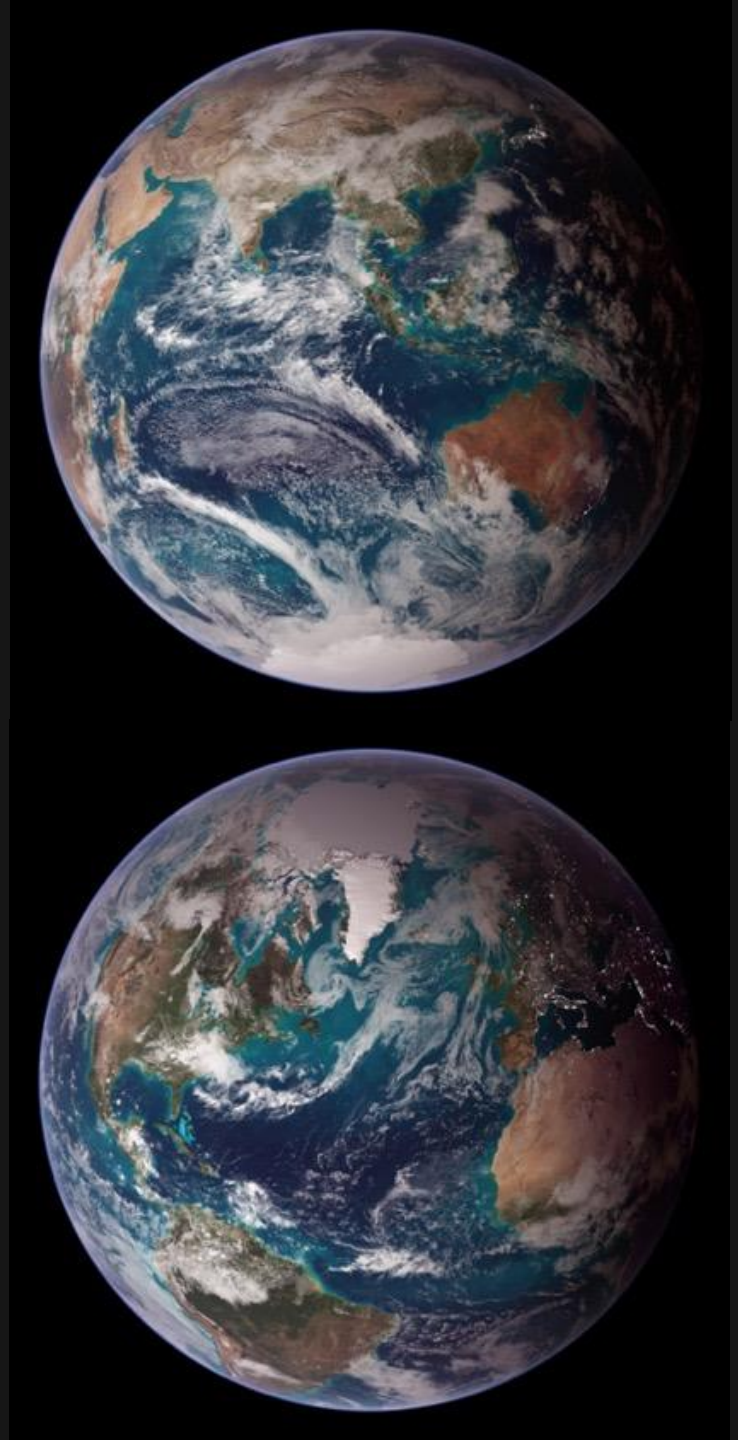
Computing with caffeine

We would need approximately 10^{48} bits to represent the energy configuration of a single caffeine molecule at a single instant in a classical computer.

This is 1 to 10% of the total number of atoms in the Earth.

10^{48} =

1,000,000,000,000,000,
000,000,000,000,000,000,
000,000,000,000,000



IBM **Quantum**

Computing with caffeine

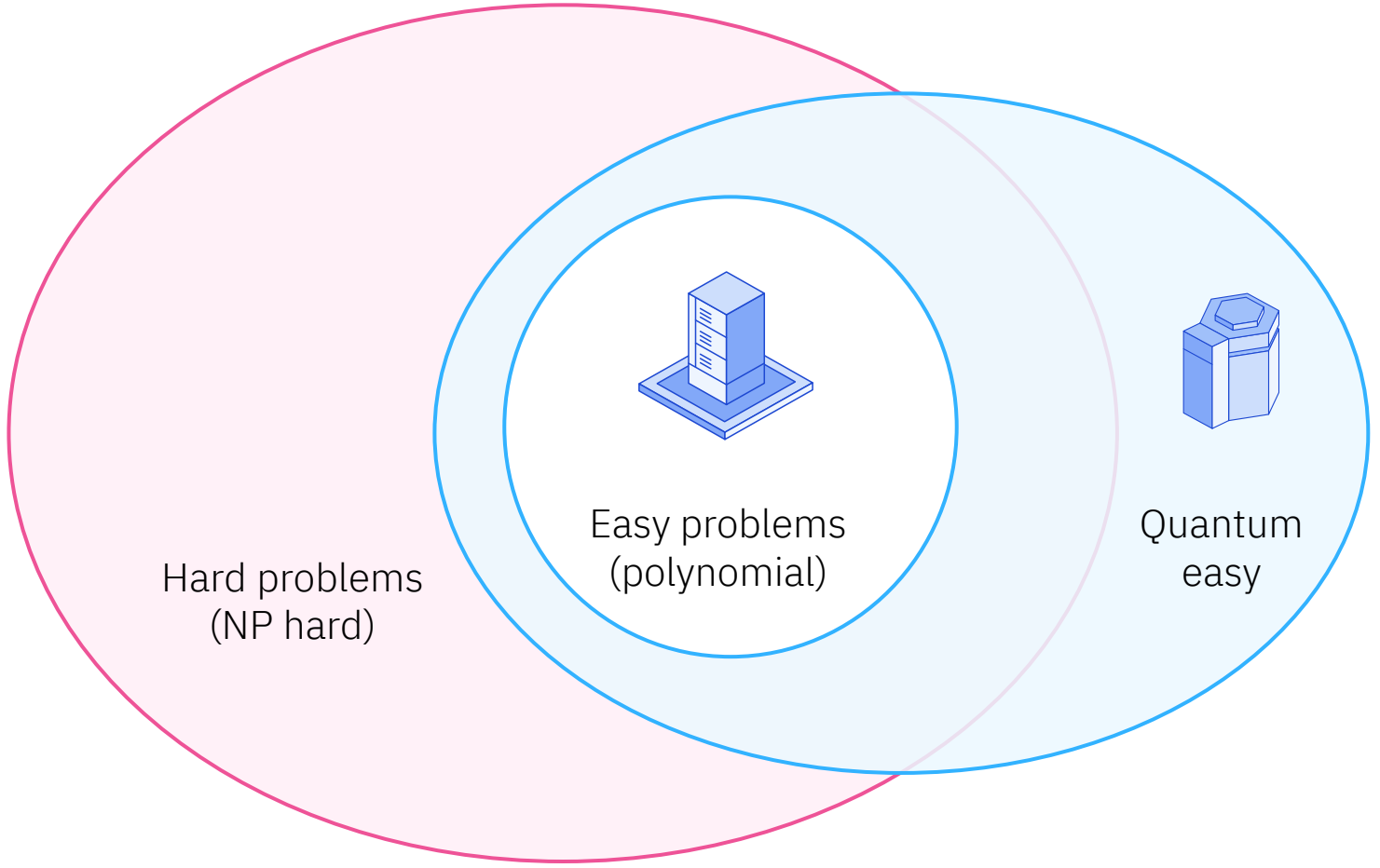
Although it’s impossible to completely represent the molecular configuration of caffeine on today’s most powerful super computers, we could represent it using 160 logical qubits.

Quantum computers are the only novel hardware that changes the game

Quantum computing is not just a faster or better version of classical systems. It is an entirely new branch of computing.

Quantum computing follows the laws of nature to represent data in ways that mimic the randomness and unpredictability of the natural world.

Ultimately, GPUs and classical hardware are not built for this.



Why quantum?

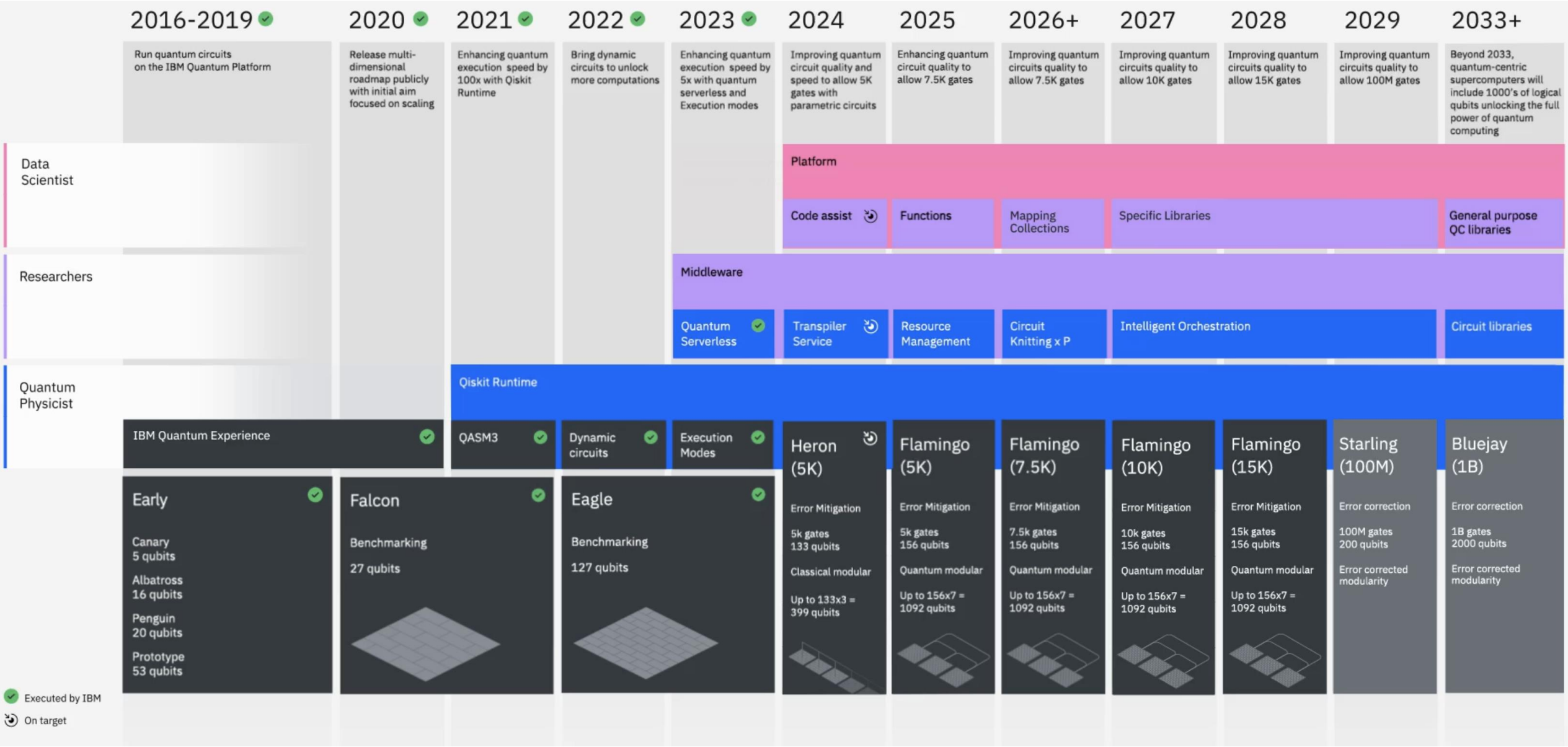
Graphics processing units (GPUs)

- Apply principles of classical physics
- Bits are either 0 or 1
- Rely on quantum-inspired methods to obtain expected answers
- Struggles to simulate utility-scale quantum systems and large problems with many gates
- Effective at tackling hard AI problems and driving advances in quantum computing

Quantum processing units (QPUs)

- Apply principles of quantum mechanics
- Qubits can be in more states than 0 and 1
- Use new computational paradigm to obtain answers to previously intractable problems
- Error mitigation lets us run larger, longer circuits
- Computational advantages expected in simulations, search and optimization, and processing data with complex structure

Development Roadmap



IBM **Quantum** – On the cloud since May 2016

Over 460,000 registered users have run …

over 2 TRILLION hardware quantum circuits in total, and users run …

over 4 BILLION hardware quantum circuits on a typical day on …

more than 25 quantum computing systems on the IBM Cloud, and written over

1750+ scientific and research papers.

Quantum applications span three general areas

IBM **Quantum**

Simulating Quantum Systems	Artificial Intelligence	Optimization / Monte Carlo
Quantum chemistry Material science High energy physics	Better model training Pattern recognition Fraud detection	Portfolio optimization Risk analysis Loans & credit scoring Monte Carlo-like applications

IBM Quantum Network

Use Cases

Cleveland Clinic

Creating a new quantum computing ecosystem in Ohio focused on advancing skills in the region and fundamentally advancing the pace of discovery in healthcare and life sciences.

Woodside

Improve petrophysical analysis and gain better insights on oil exploration and rock type predictions

ExxonMobile

Exploring more accurate thermodynamical and chemical simulations, and ways to optimize logistics in resource and energy distribution.

Boeing

Exploring quantum computing's potential to deliver the advanced and computation and communications increasingly at the heart of aerospace innovation.

Air Force Research Lab

Providing access to real quantum computing hardware to accelerate the development of DOE and DOD mission-critical applications and drive transformational advancements in science and research.

Arizona State University

Creating a workforce and development pipeline for a quantum-enabled community with the aim to promote understanding of the technology and forge partnerships with industry and academia.

IBM Quantum Network

Use Cases

E.ON

Providing access to the most advanced quantum computing hardware to accelerate E.ONs aim to drive the transformation of the energy industry with Quantum Computing to implement quantum solutions for their critical workflow.

Arxiv: 2304.10385

Crédit Mutuel

As the first enterprise in France to join the IBM Quantum Network, Crédit Mutuel identified specific use cases, among many areas of interest in financial services, including: research into customer experience, fraud management and risk management,

Erste Bank

Erste Digital will gain access to IBM’s premium plan for quantum computer systems, including the recently announced 127-Qubit Eagle processor, as well as to IBM’s quantum expertise. The aim is to investigate, validate and promote concrete quantum application cases relevant to banks.

Bosch

With its activities in the field of electromobility, Bosch brings in a concrete application in which quantum computers may soon offer a significant advantage over conventional computers in discovering and designing new materials. Fuel cells, batteries, electric engines, or advanced sensors contain strongly correlated electrons.

CERN

The mission of the CERN hub is to explore promising applications of quantum computing for high-energy physics and other sciences together with academia and research institutes in CERN Member States. These also include areas in quantum machine learning.

STFC

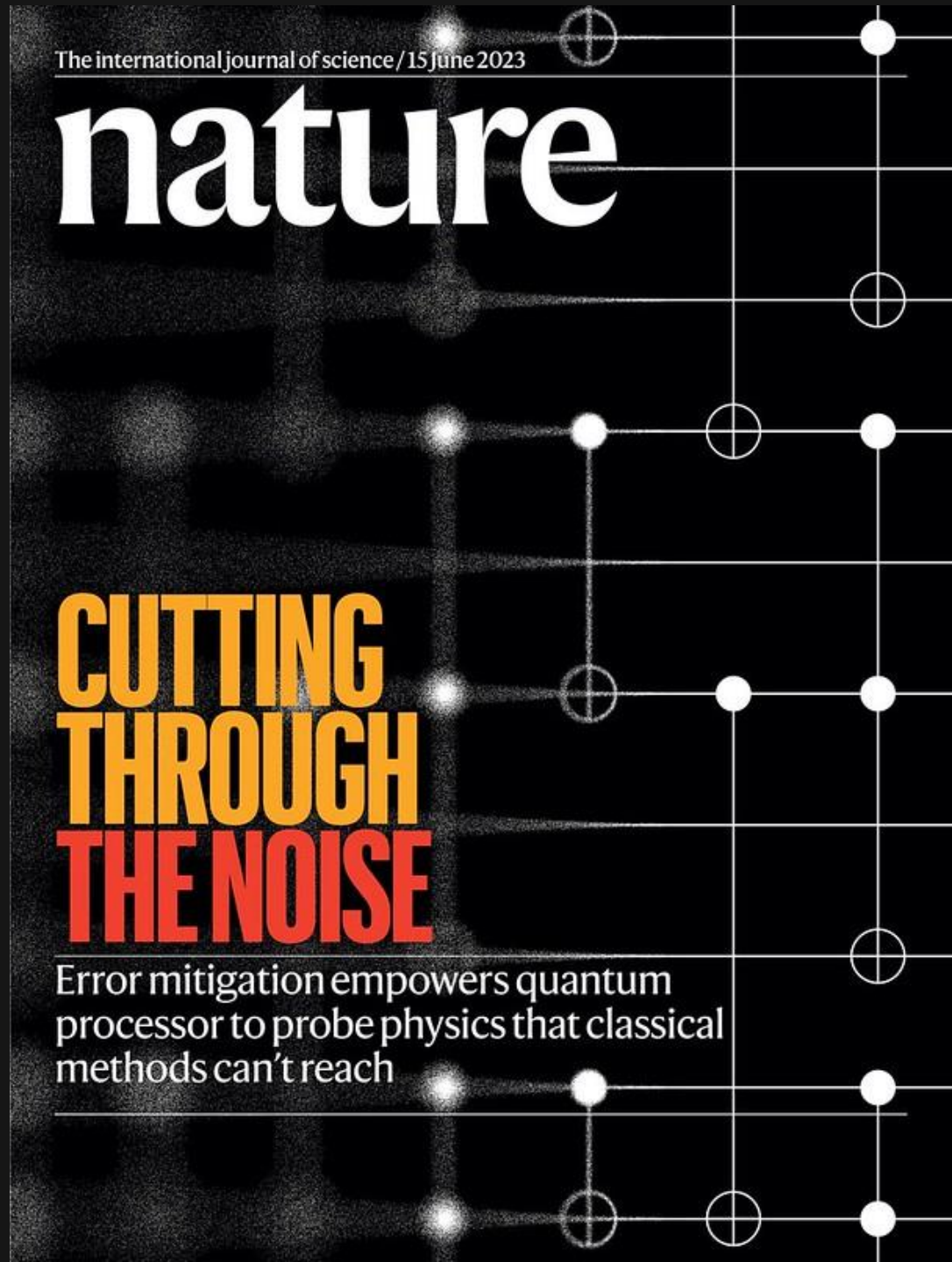
Hartree Centre at the UK Research and Innovation's Science and Technology Facilities Council (STFC) will work together over the next five years to apply artificial intelligence and quantum computing to produce innovations in materials, life sciences, climate, agriculture, and manufacturing.

Nature 2023: Quantum Utility

A noisy quantum computer is able to produce accurate expectation values in regimes beyond brute force computation and where leading classical approximations struggle

This serves as evidence for the utility of quantum computing before fault tolerance

https://www.nature.com/articles/s41586-023-06096-3



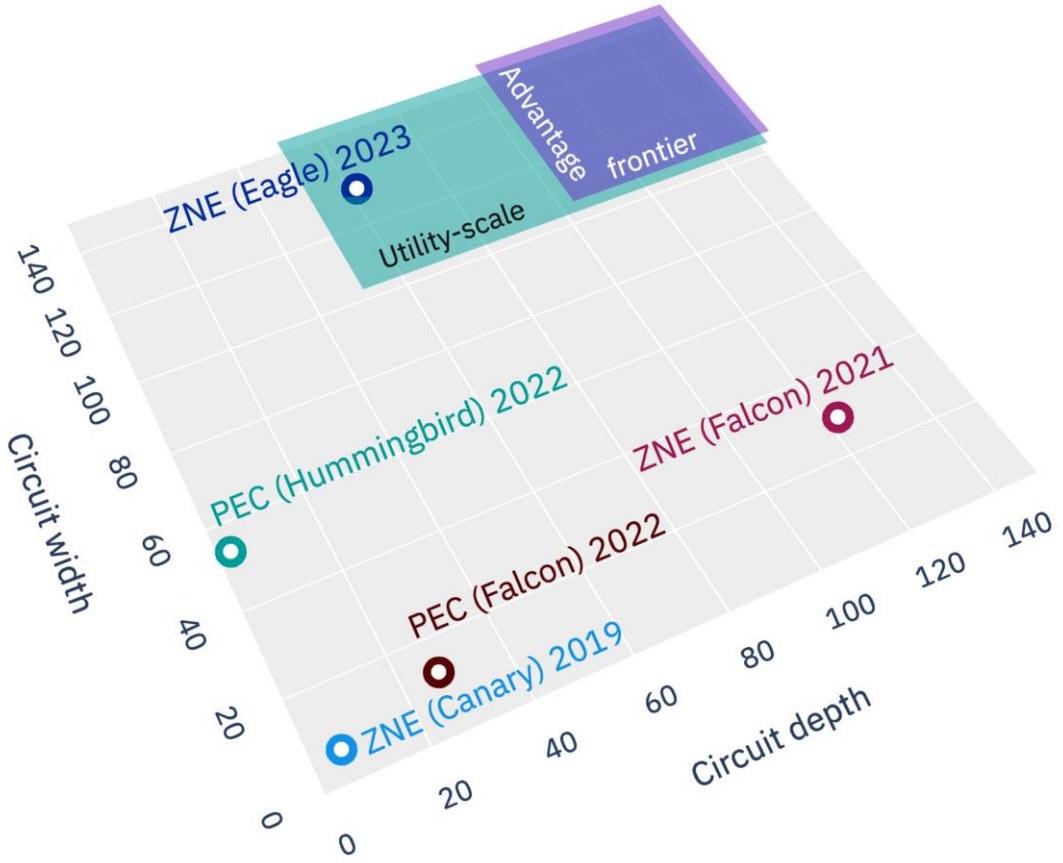
Definition of quantum utility

High-fidelity quantum computation outside the reach of exact classical simulation methods

It is the first major milestone on the path to Quantum Advantage.

Useful quantum computation requires utility-scale hardware and co-designed scalable software capabilities.

This means systems larger than 100 qubits, where simulations are not a viable alternative.



Application use cases

The tools of utility – requirement 4

IBM Quantum is not in this alone. Working groups bring together the best industry pioneers and scientists in their field to accelerate our path to achieving Quantum Advantage by 2025 across several domain areas:

Optimization

July 19–20, Zurich

UKRI:STFC
E.On
Fraunhofer
Los Alamos

Quantum Optimization: Potential, Challenges, and the Path Forward: https://arxiv.org/abs/2312.02279

Materials and HPC

April 17–18, Chicago

Riken
Univ. Tokyo
Univ. Chicago
Oak Ridge Nat. Labs

Quantum-centric Supercomputing for Materials Science: A Perspective on Challenges and Future Directions
https://arxiv.org/abs/2312.09733

High energy physics

November 2–3, Geneva

CERN
DESY
PSNC
Univ. Tokyo

Quantum Computing for High-Energy Physics: State of the Art and Challenges. Summary of the QC4HEP Working Group
arXiv:2307.03236

Healthcare and life sciences

April 13–14, Cleveland

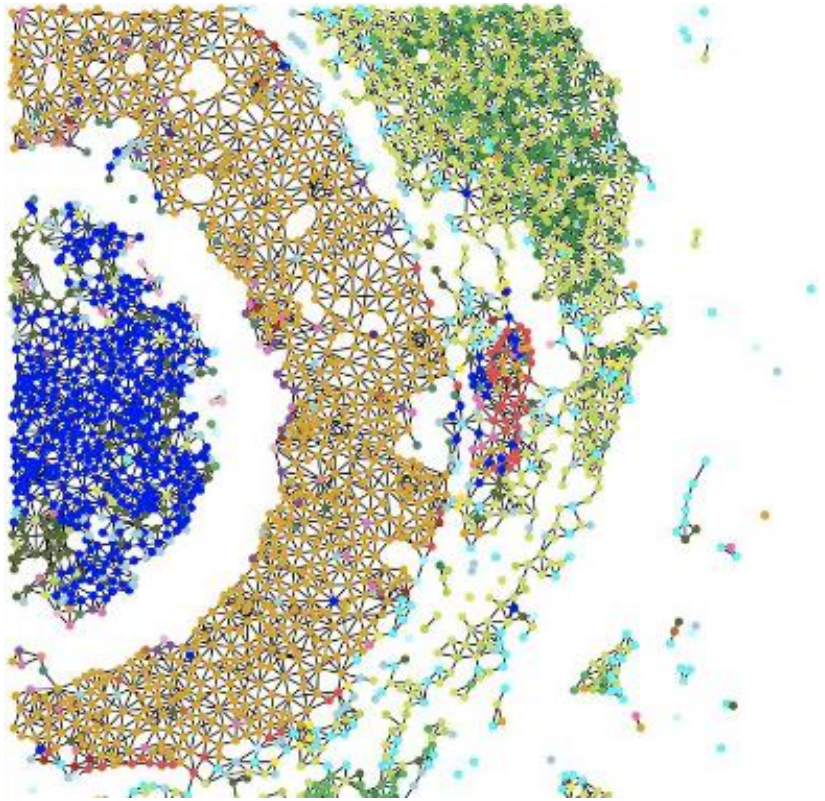
Cleveland Clinic
Univ. Toronto
Univ. Chicago
Yonsei Univ

Towards quantum-enabled cell-centric therapeutics
arXiv:2307.05734

Cleveland Clinic

Advancing Discovery in Healthcare and Life Sciences

Building a robust research and clinical infrastructure for empowering medical research in ethical, privacy preserving ways leading to discoveries for patient care and novel approaches to public health threats like Covid-19 pandemic



Transforming Drug Discovery with Quantum Computing - White paper released on Quantum-enabled cell-centric therapeutics from the QML for Omics theme, involved the efforts of IBM, Cleveland Clinic, Algorithmiq, Athos, and Purdue University.

Mercedes-Benz

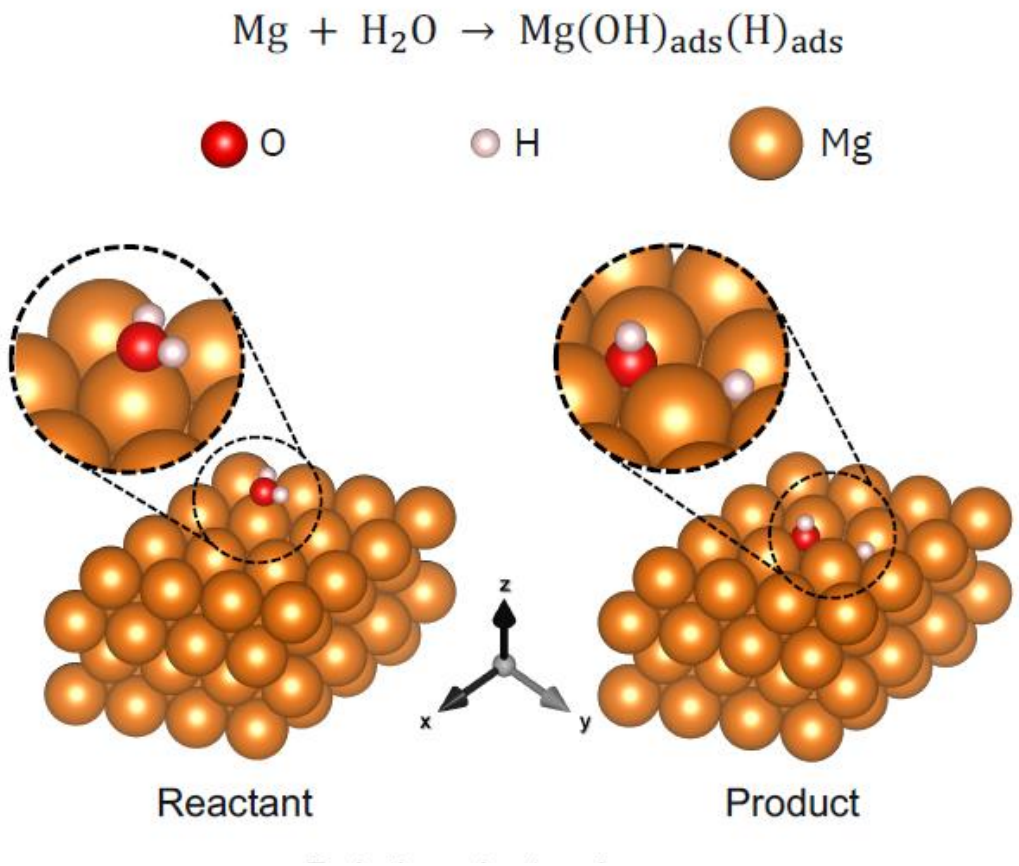
Quantum Computing for Materials Discovery and Manufacturing Optimization

Mercedes-Benz and IBM have recently published a series of papers demonstrating progress toward using quantum computers to model material systems including Lithium-sulfur that are relevant to advancing the performance of batteries. The teams have also demonstrated applications in manufacturing defect analysis and product recommendation.

“Developing and perfecting these hypothetical batteries could unlock a billion-dollar opportunity.”

Benjamin Boeser
[Former] Director of Innovation Management, Silicon Valley at Mercedes-Benz R&D North America

- Boeing and IBM are using quantum computers to model corrosion processes in structural aircraft materials
- Their approach employs Quantum Embedding to simulate a large chemical scenario on today's quantum computers



Gujarati, Tanvi P., et al. "Quantum Computation of Reactions on Surfaces Using Local Embedding." *arXiv preprint arXiv:2203.07536* (2022).

Mitsubishi Chemical, JSR and Keio University

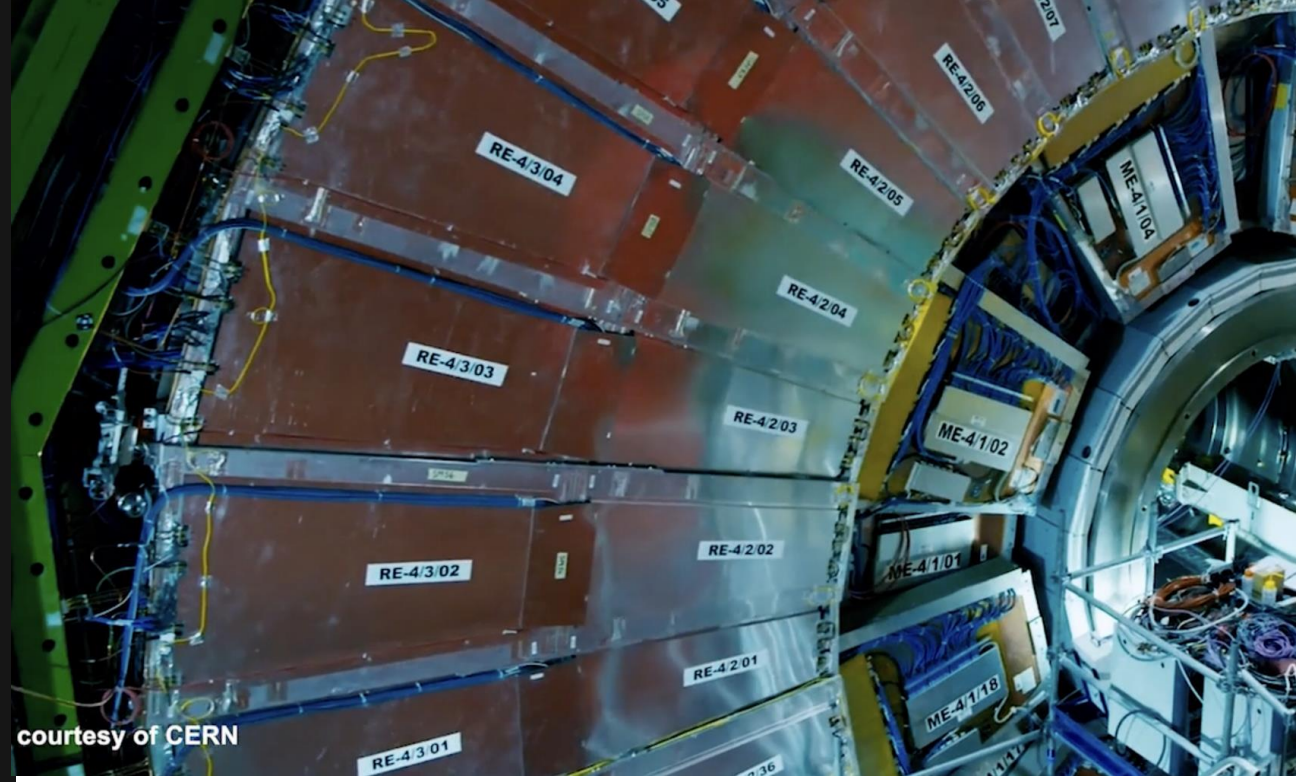
Exploring new forms of light with Quantum Computing

A Japanese research partnership comprising corporate teams from industrial chemists Mitsubishi Chemical and JSR Corporation, and academics from Keio University, have joined the IBM Quantum Network. Their mission is to collaborate with IBM scientists to create a new breed of disruptively efficient OLED materials — flexible, scalable and able to produce more (and more visually appealing) light with far less energy.

CERN

Quantum Machine Learning to understand what sews the universe together

CERN’s partnership with IBM Quantum seeks new ways of finding patterns in data of the Large Hadron Collider. A recent collaboration with IBM scientists involves the detection and analysis of the Higgs boson, a recently discovered particle that helps explain the origin of mass. Sifting through raw data to find occurrences of Higgs behavior is a knotty problem that stretches classical computers to their limit.



“Quantum computing may play a significant role in (...) exploring the many open questions related to issues such as dark matter, dark energy, (...) and more.”

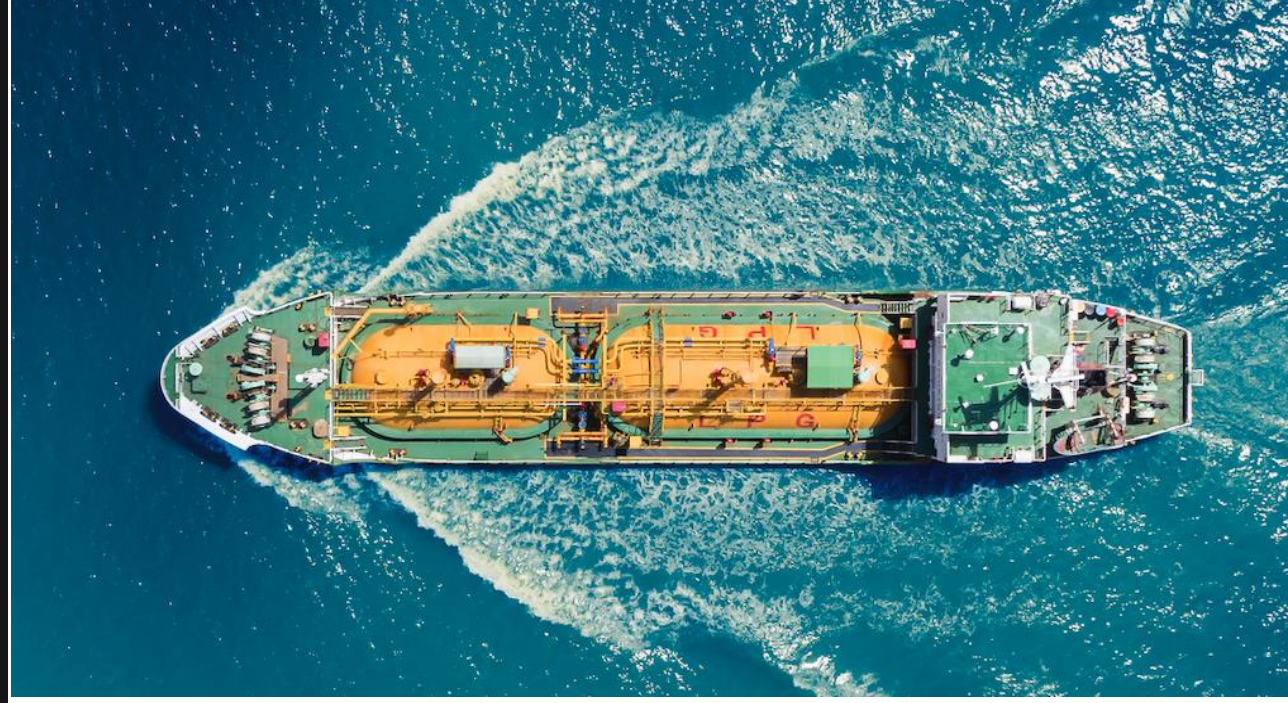
Alberto Di Meglio
Head of CERN openlab

ExxonMobil

Maritime Routing's Mind-Boggling Math

In 2021 more than 500 LNG (liquified natural gas) ships are used to transport critical fuel supplies across the oceans. Together, they make thousands of journeys per year to destination ports where the LNG is deployed to power critical infrastructure.

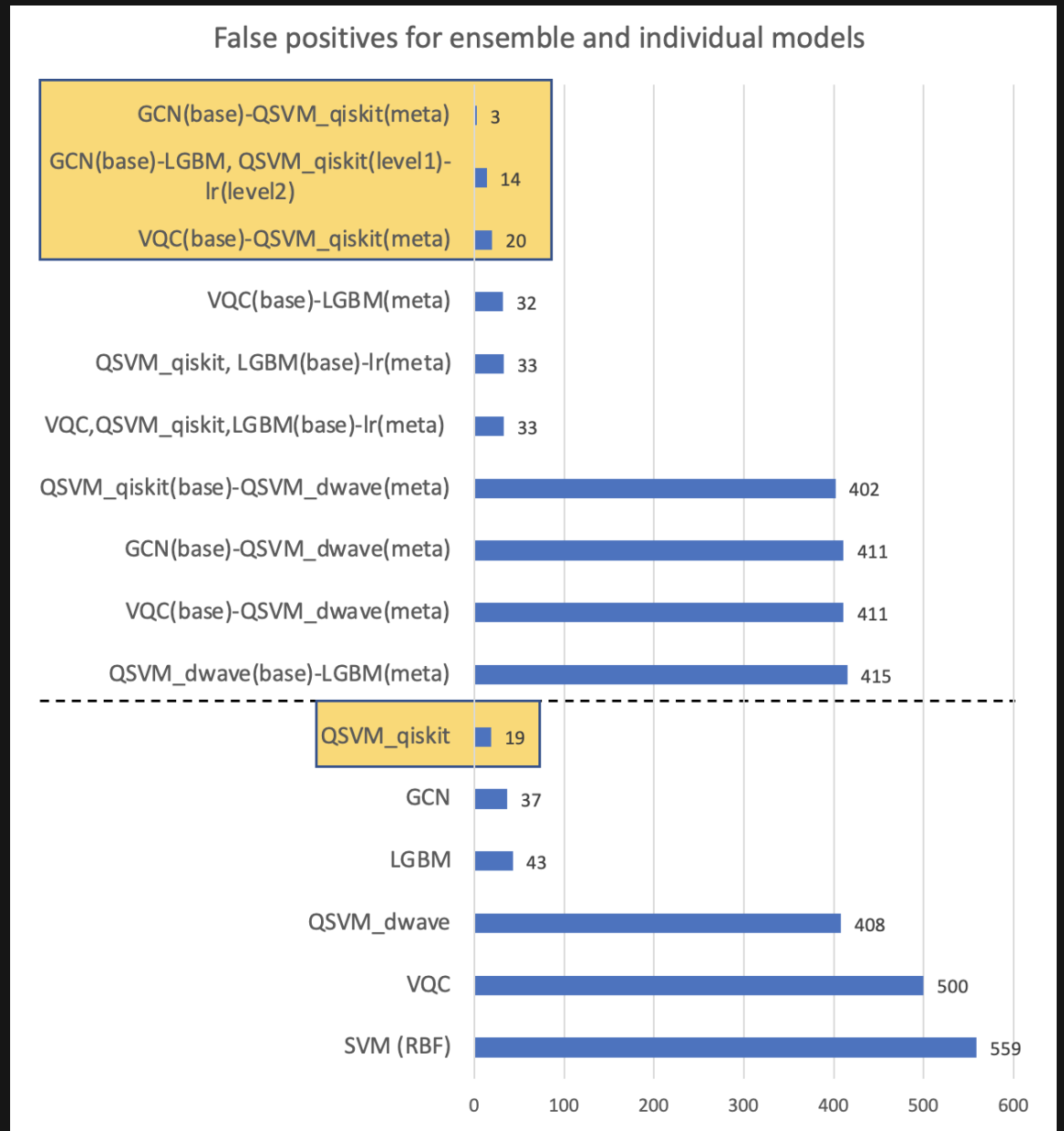
Finding optimal routes for a fleet of such ships can be a mind-bendingly complex optimization problem.



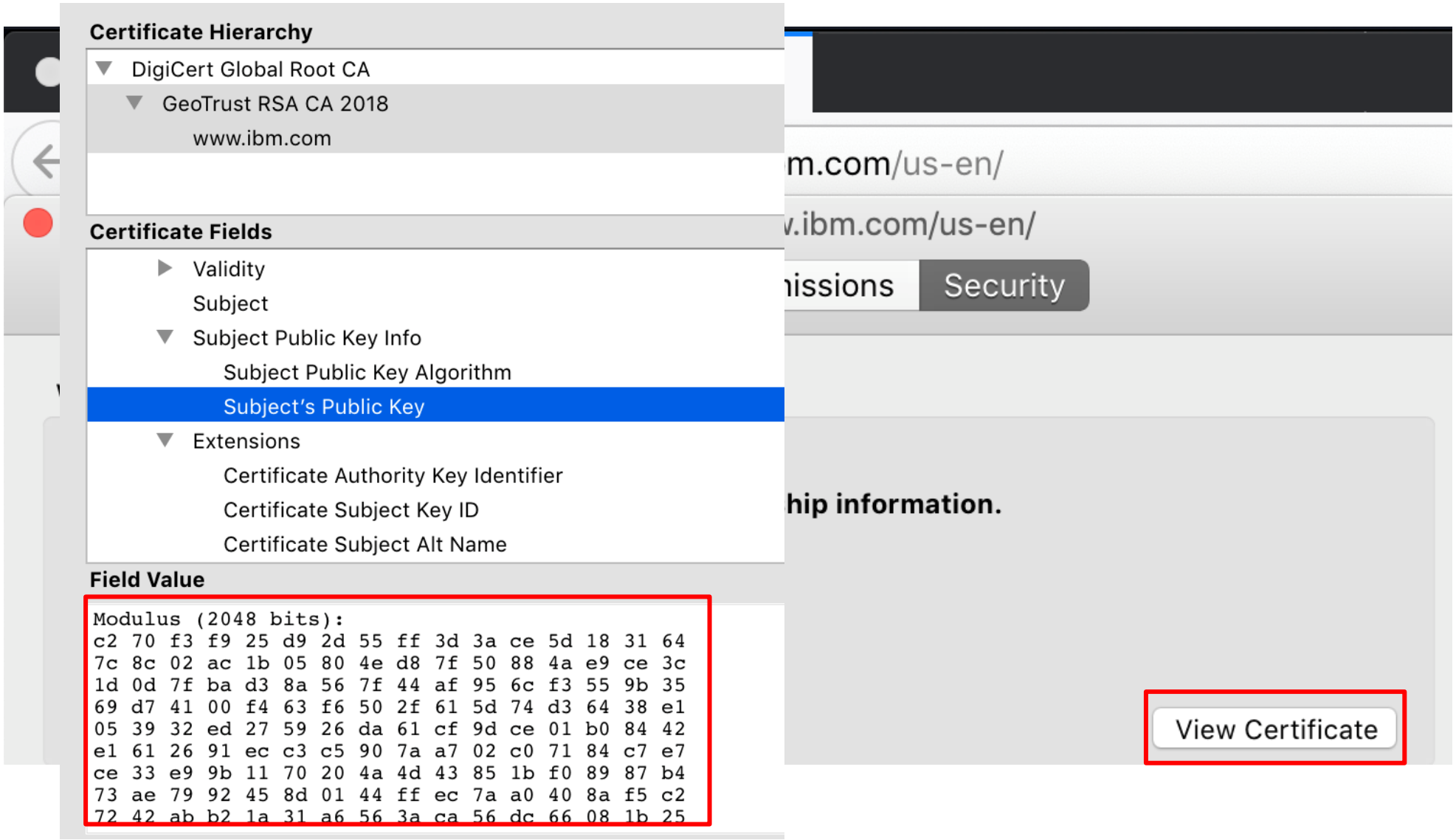
Quantum computers take a new approach to addressing this sort of complexity, with the potential to find solutions that classical supercomputer alone cannot handle. Industry leaders like Exxon are getting involved now to explore how blending classical and quantum computing techniques might solve big, complex, pressing global challenges.

QML Application for Anomaly Detection (IBM + IITM)

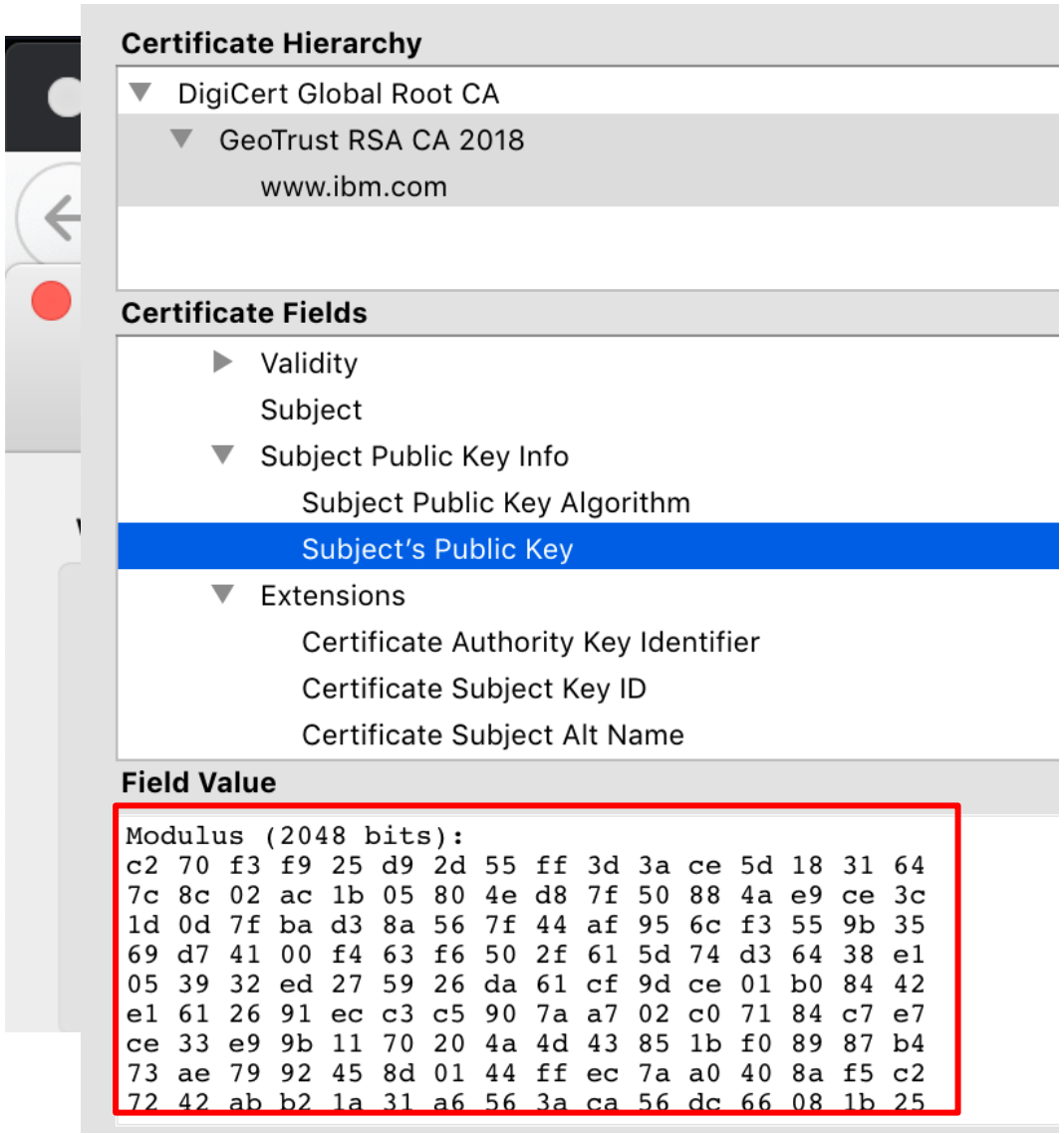
- Goal: Improve Phishing detection in Ethereum transaction networks using Quantum ML algorithms
- Core Idea : Created classical ensemble of Quantum-classical ML models. Achieved least false positives with QSVM and ensembles created with QSVM.
- Buisness Impact – Banks and other financial institutions are interested in fraud detection, anti-money laundering and other anomaly detection problems.
- The overall code is generic for any classification and regression task, thus these algorithms can be used to create other QML applications.



Example: Web Traffic Encryption via TLS



Example: Web Traffic Encryption via TLS



1) Server presents signed **public key** (=certificate) to client
2) Agreement on **session key**
3) Channel encrypted using **symmetric encryption**

Cryptography today

- Key distribution with **public key cryptography:**

Public key =  Private key = 

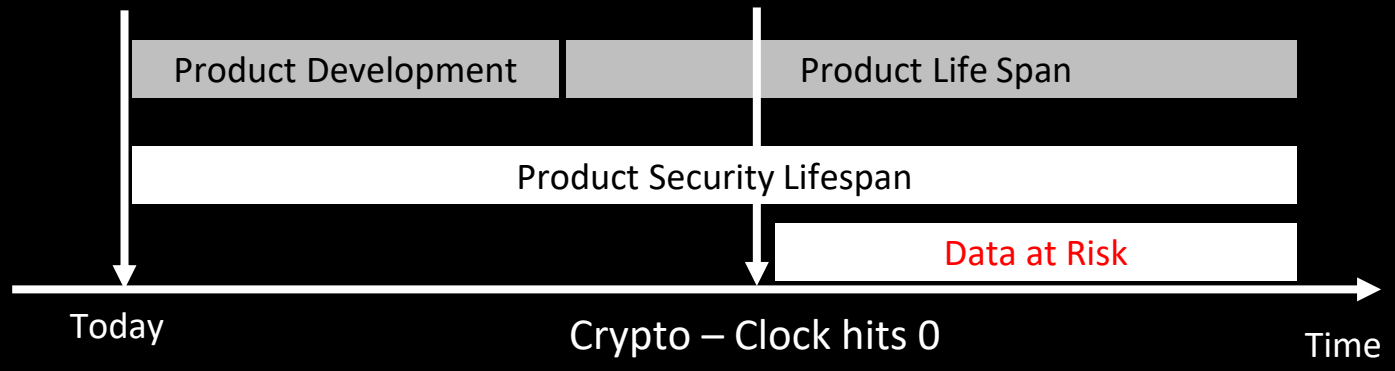
- Examples: Web traffic, Email, Virtual Private Networks, Remote Connections …

- Currently used “best-practice” public key algorithms, e.g. RSA, Diffie-Hellman, Elliptic Curve Crypto (ECC)…, rely on **three mathematical problems**:

1. Integer Factorization
2. Discrete Logarithm
3. Elliptic Curve Discrete Logarithm

…recognized to be hard problems for a **classical computer** but could be solved **efficiently on a quantum computer (Peter Shor, 1994)**

Security time value of data – the Risk Timeline



Cryptography that is resistant against a quantum attacker

Quantum Key Distribution ("Quantum Cryptography")

- Key distribution exploiting quantum physics (e.g. use of 'single photons')
- Provably secure against (quantum) eavesdropper
- Requires special infrastructure: optical fibers/satellites
- Range limitations & low bitrate

Quantum-Safe Cryptography ("Post-Quantum Cryptography")

- Classical algorithms based on 'hard' mathematical problems
- Considered secure against quantum attacker
- Can be implemented on todays infrastructure (e.g. update of TLS)
- No range limitation / limitation in bitrate

Journey to Quantum Safe

U.S. National Institute of Standards and Technology announced the first quantum-safe cryptography protocol standards for cybersecurity (July 2022), three of which were created by IBM in collaboration with industry and academic partners.

Purpose	Algorithm
Public-key Encryption and Key establishment Algorithms	CRYSTALS-Kyber
Digital Signature Algorithms	CRYSTALS-DILITHIUM
DSA (alternate)	Falcon
DSA (alternate)	SPHINCS+
NIST Selected Algorithms, July 5th 2022. NIST recommended two primary algorithms to be implemented for most use cases: CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures).	NIST National Institute of Standards and Technology U.S. Department of Commerce

US Government
establishes timeline for transition to CNSA 2.0-compliant algorithms

z16

First Quantum-safe platform

GSMA Telco Consortium

Support industry transition to quantum-safe cryptography

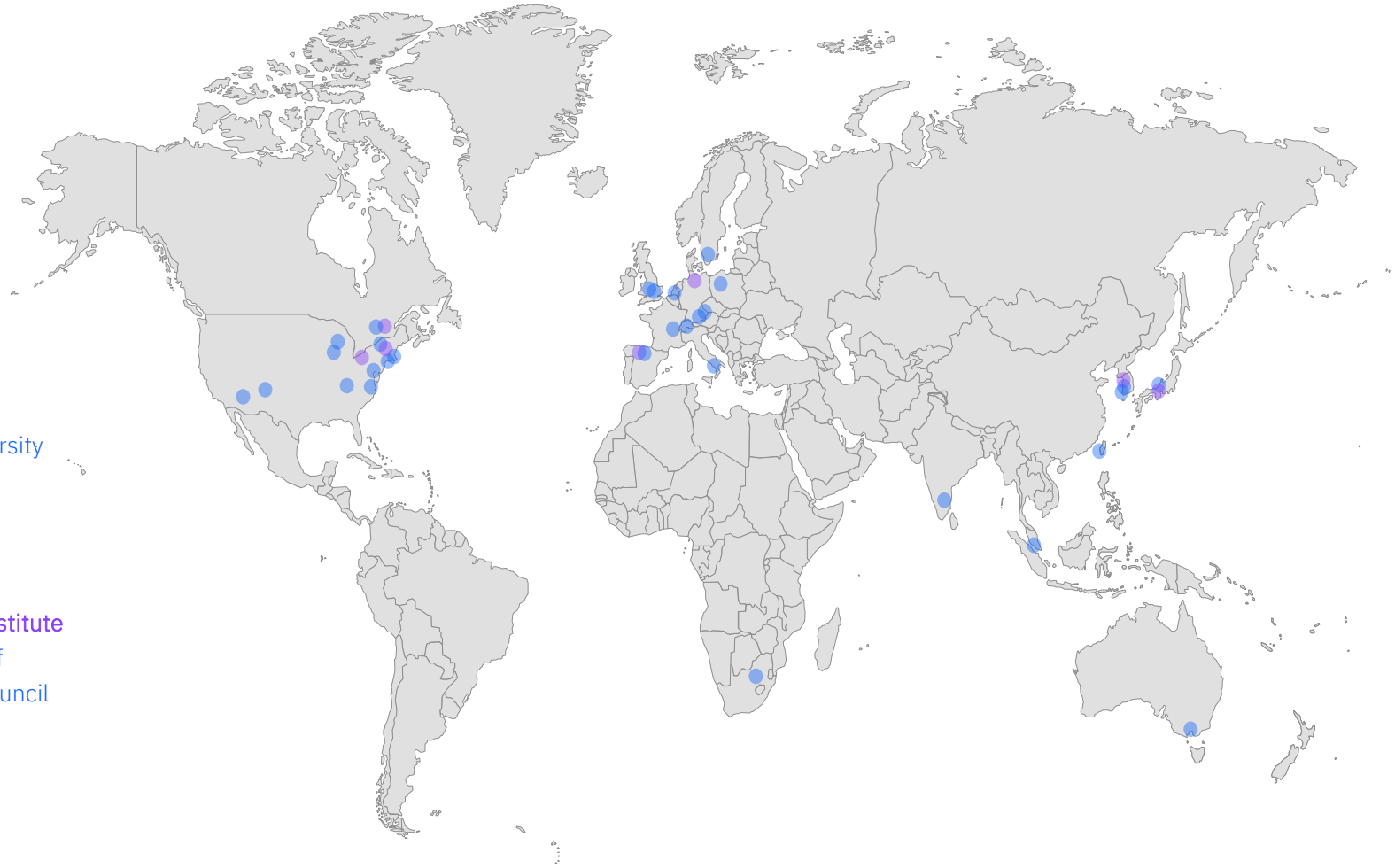
vodafone

GSMA Taps IBM, Vodafone for Post-Quantum Taskforce

IBM Quantum Safe

Support client transition to quantum-safe cryptography

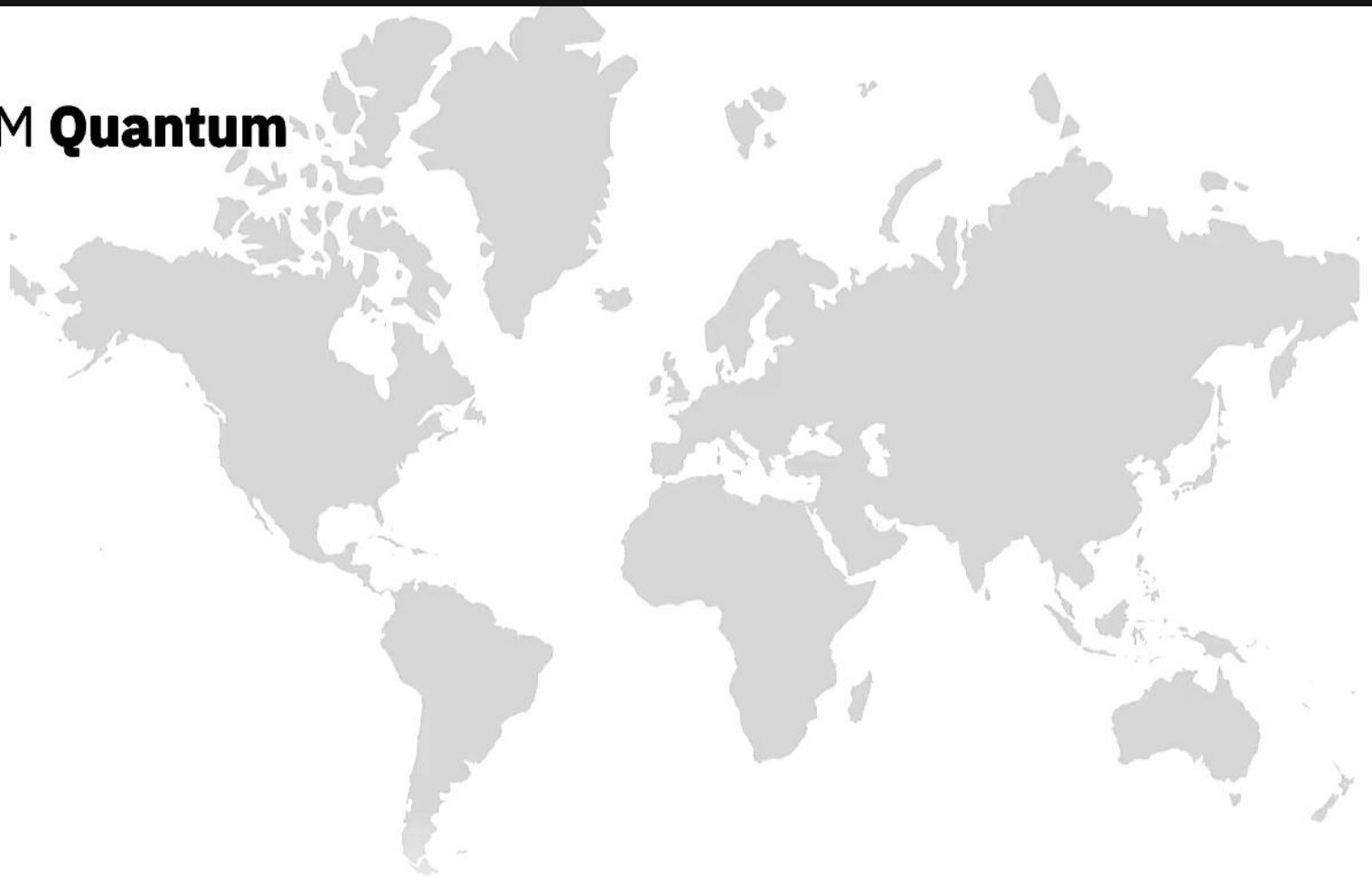
37 Quantum Innovation and Computation Centers



Air Force Research Laboratory
Arizona State University
BasQ (Ikerbasque)
Brookhaven National Laboratory
CERN
Chicago Quantum Exchange
Cleveland Clinic Foundation
Consiglio Nazionale delle Richerche
Copenhagen, University of
DESY
Fraunhofer
IBM-HBCU Quantum Center
IBM-Illinois DA Inst - UIUC
IIT Madras
Keio University
Korea Quantum Computing
Lantik
Los Alamos National Lab
Melbourne, University of
National Quantum Computing Centre
National Taiwan University
National University of Singapore
North Carolina State University
Oak Ridge National Lab
PINQ^2
Poznan SNC
Quantum Application Lab
Rensselaer Polytechnic Institute
Rhode Island, University of
Sci. and Tech. Facilities Council
Sherbrooke, Université de
Sungkyunkwan University
Tokyo, University of
UniBWM
uptownBasel
Witwatersrand, University of
Yonsei University

* QCC
* QIC

IBM **Quantum**



140k
130k
120k
110k
100k
90k
80k
70k

Circuits executed in

Quantum Hardware

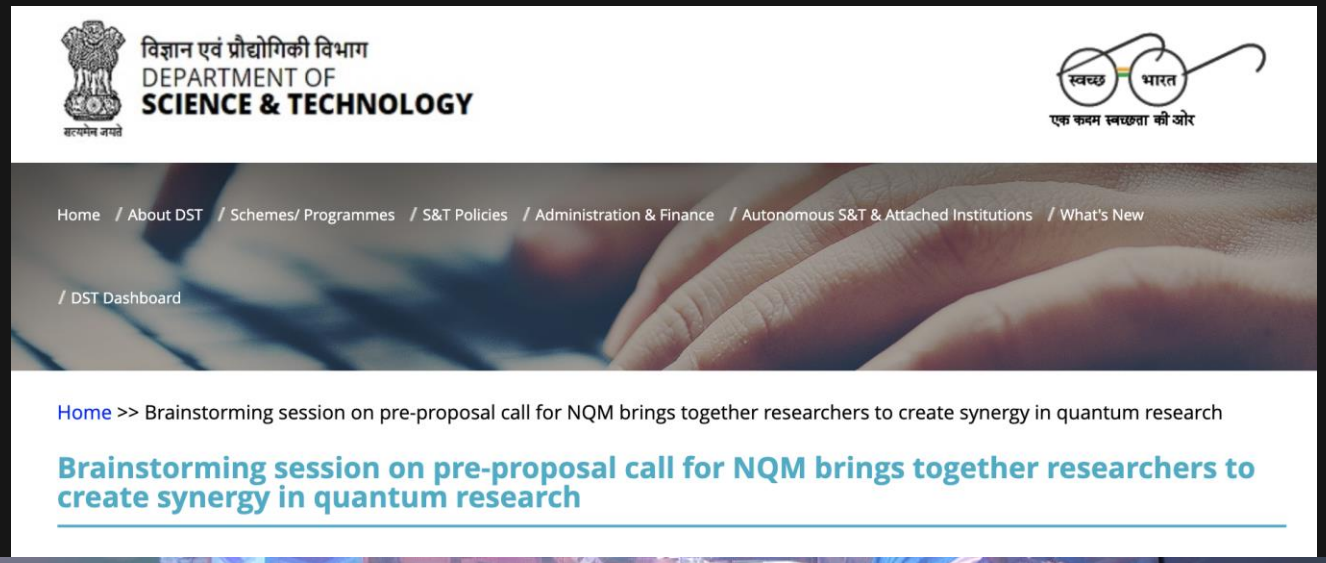
130k

Users

0.0

India’s National Quantum Mission

Call for pre proposals closed on April 12, 2024
4 Thematic Hubs likely to be in place by September-October 2024



IBM **Quantum**