Introduction to Quantum Computing

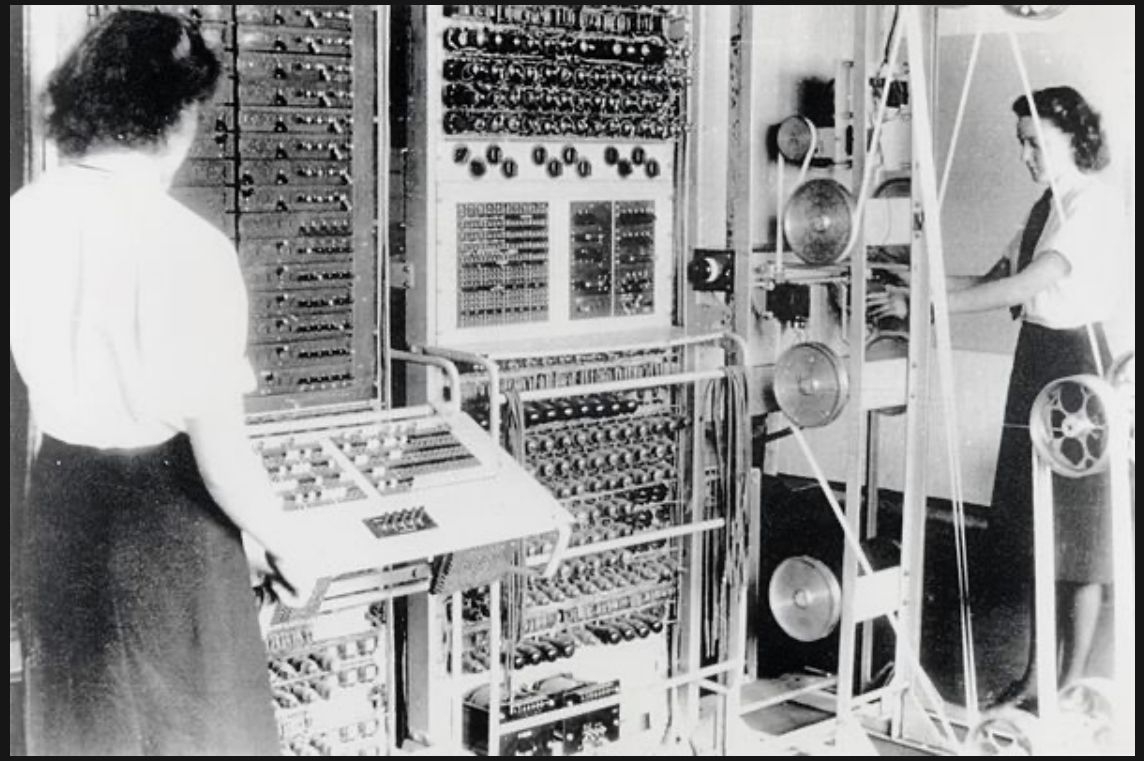
Adam Jollans FBCS
Program Director, IBM Systems

29th September 2022

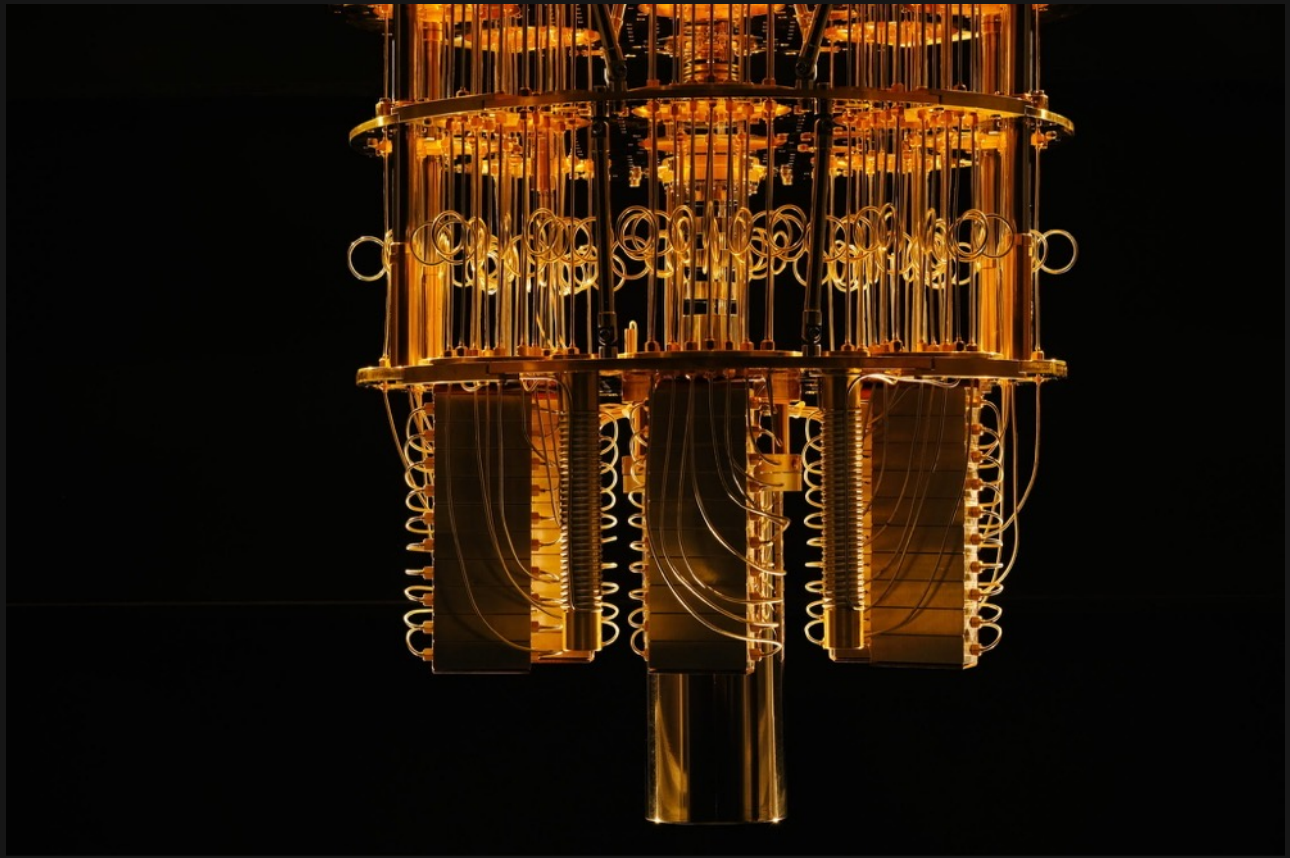
IBM Quantum / © 2021 IBM Corporation

IBM **Quantum**

The world is changing…



Introducing Quantum Computing



Improved nitrogen-fixation process for creating ammonia-based fertilizer

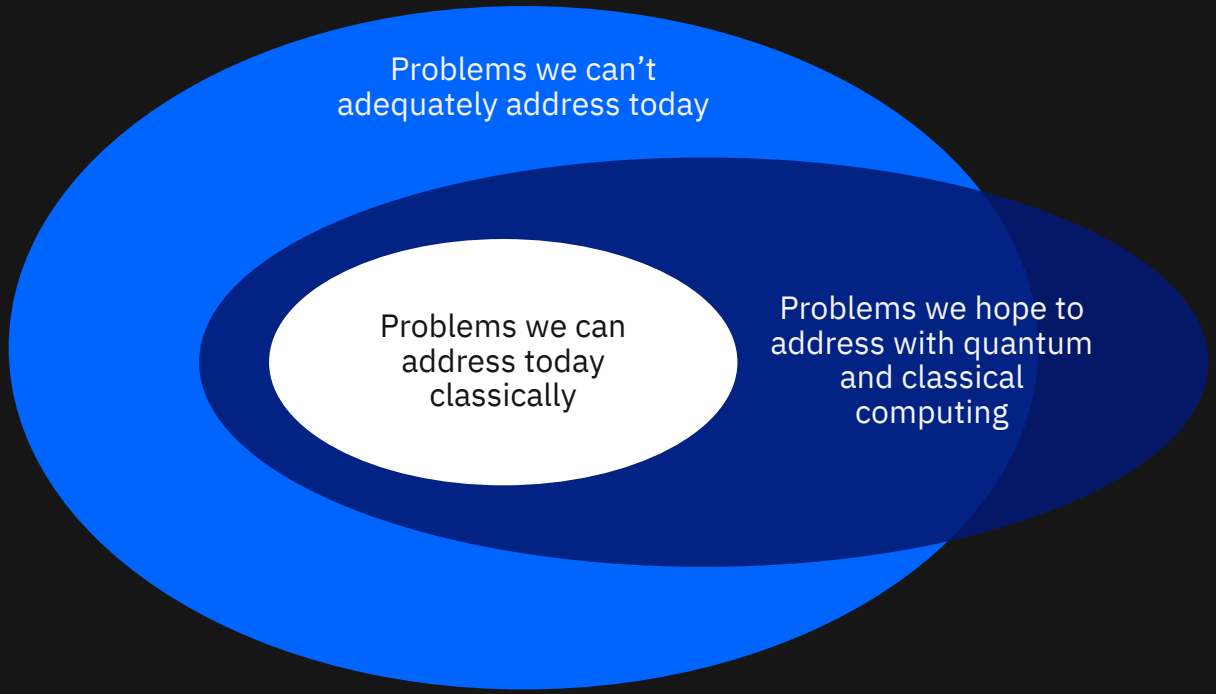
New catalysts to make CO_2 conversion into hydrocarbons more efficient and selective

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

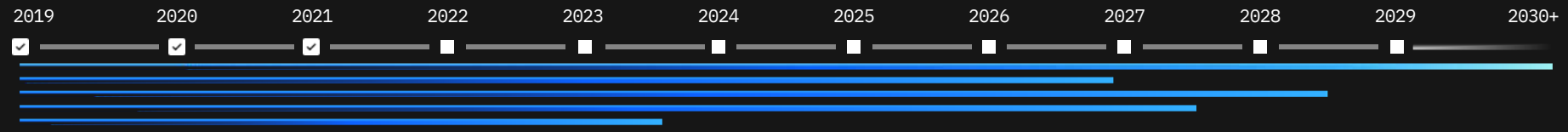
New classes of antibiotics to counter the emergence of multidrug-resistant bacterial strains

Why quantum?

IBM **Quantum**



Despite how sophisticated digital "classical " computing has become, there are many scientific and business problems for which we've barely scratched the surface.



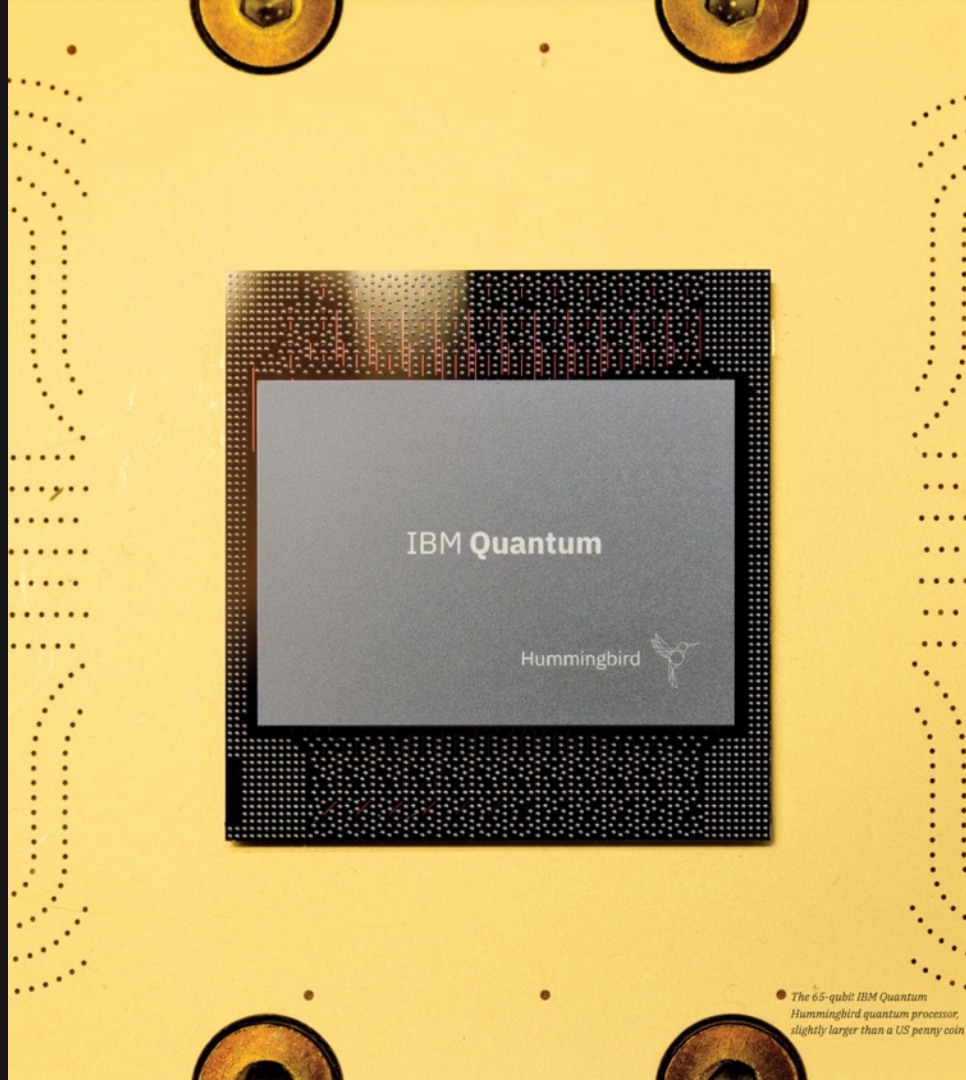
The Quantum Decade

There is a closing window to become quantum-ready and prepare to capitalize on new innovations that quantum computing will make possible.

We are in the Quantum Decade, and as we accelerate the pace of discovery, enterprises of all kinds need to pay close attention.

Quantum Awareness

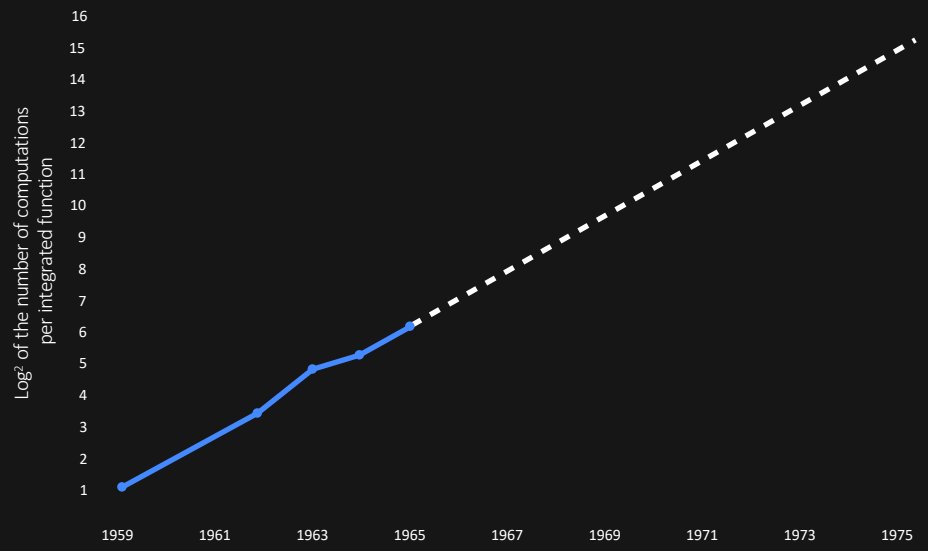
Computing paradigm evolving from an age of analytics to an age of discovery

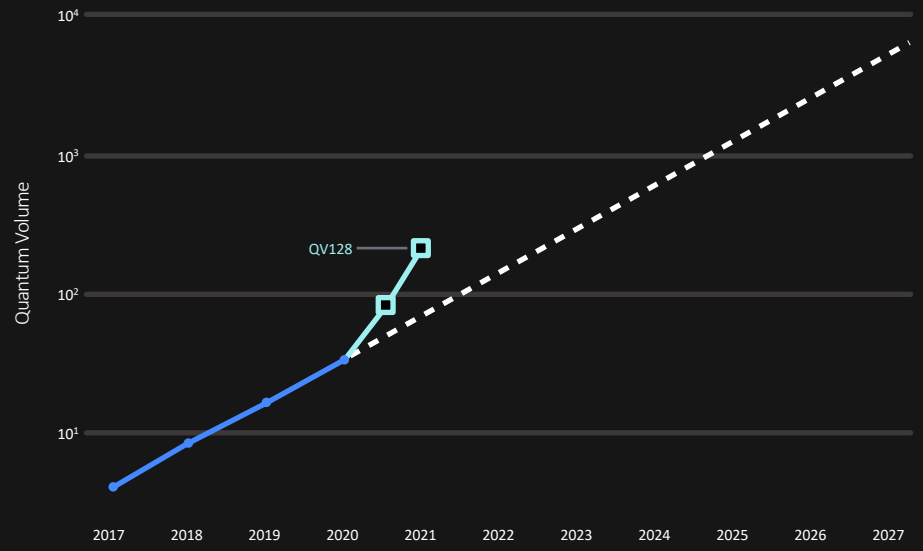


The 65-qubit IBM Quantum Hummingbird quantum processor, slightly larger than a US penny coin

IBM Quantum / © 2021 IBM Corporation

"Moore's Law is coming to an end and classical computing is reaching its limits just as our demand is starting to surge."





IBM Quantum / © 2021 IBM Corporation

Quantum computing can help expedite solutions to complex computational problems that face business and society.

What makes this the Quantum Decade?

Mounting pressure to solve exponential problems

Discovery of new materials

Managing complex financial risk

Re-engineering supply chains for resilience

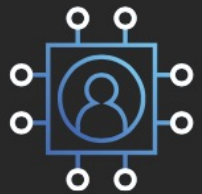
Quantum technology at a tipping point

Hardware scaling from 127 qubits in 2021 to 1,000 qubits in 2023

Software developments for frictionless quantum computing

Algorithmic improvements and greater circuit quality, capacity, and variety

Quantum ecosystems scaling



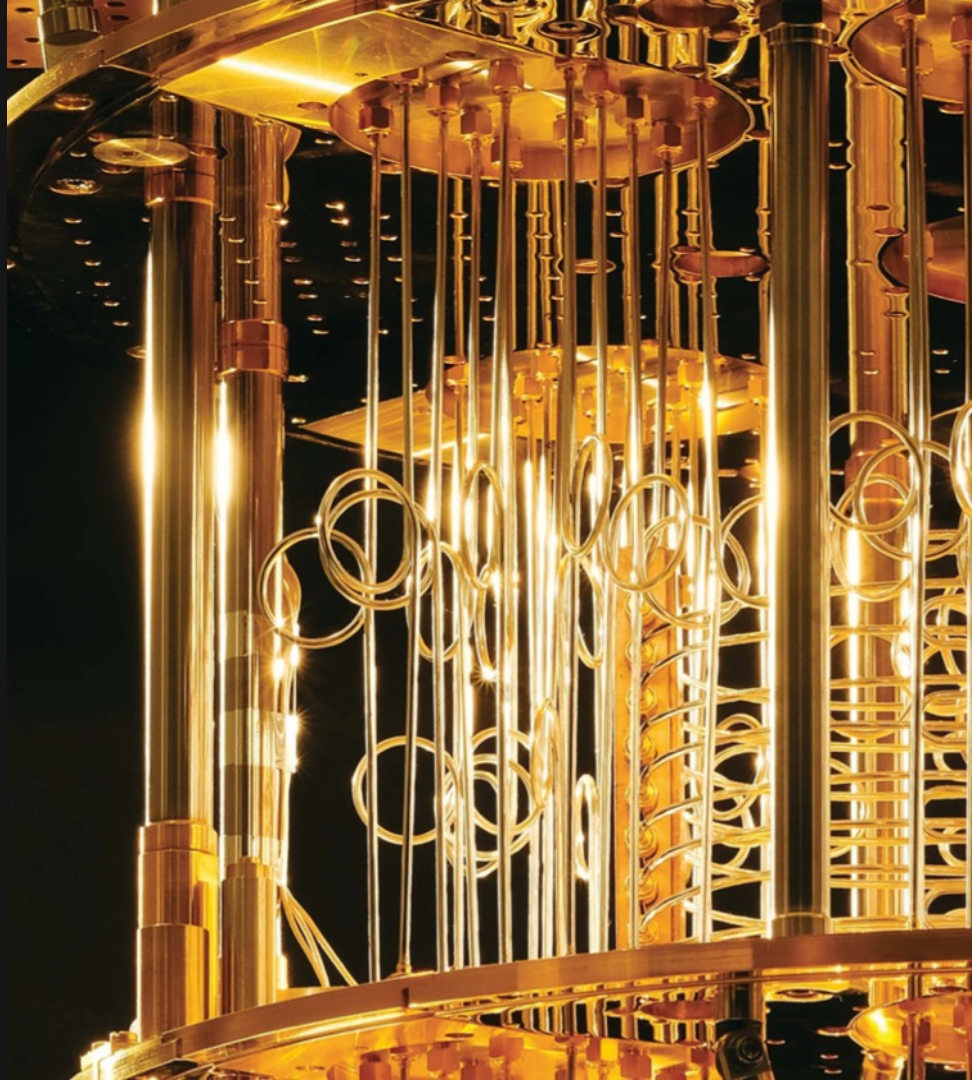
Open innovation fosters collaborative learning

Users trained to apply quantum computing to real-world problems

>2 billion circuits on IBM Quantum Services per day

Quantum Readiness

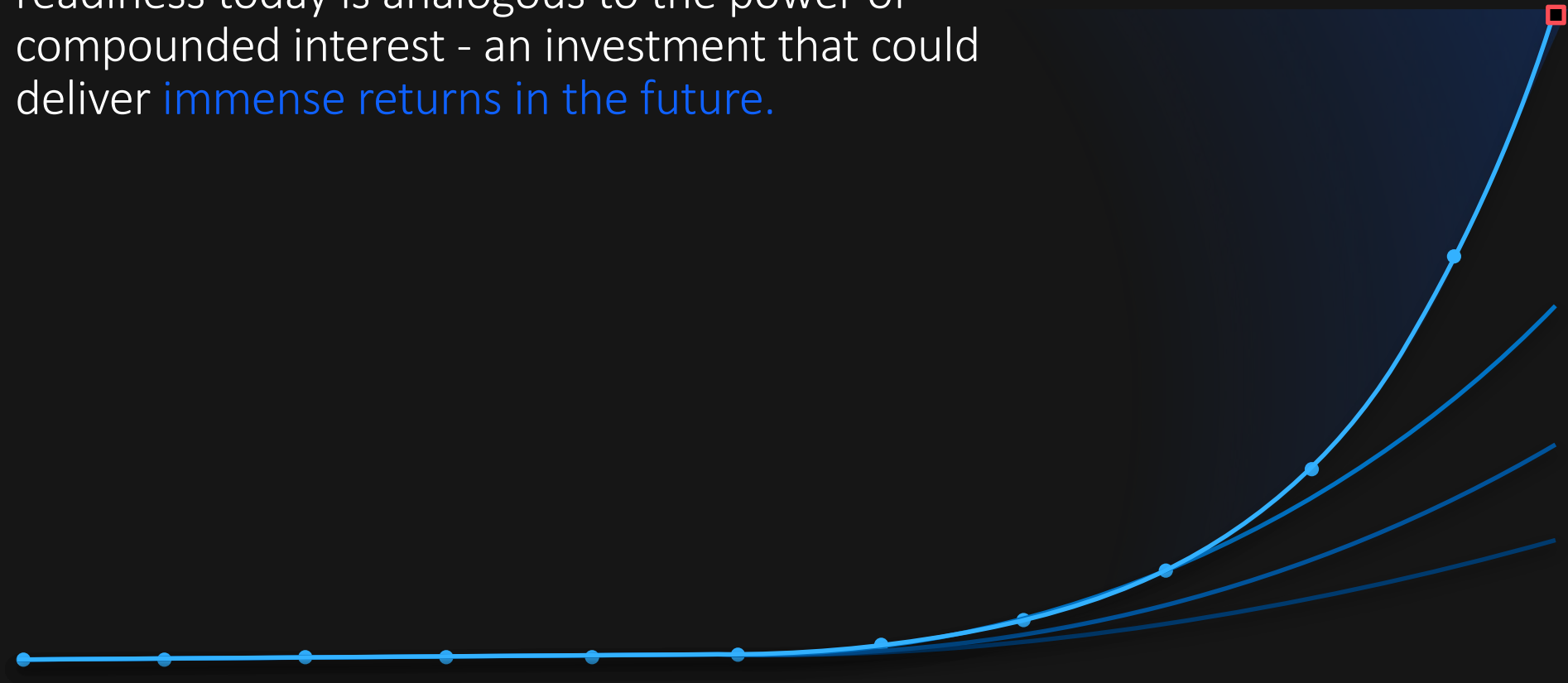
Accelerating digital transformation in the context of preparing for quantum computing



IBM Quantum / © 2021 IBM Corporation

A relatively small investment in quantum readiness today is analogous to the power of compounded interest - an investment that could deliver immense returns in the future.

IBM **Quantum**



Talent & transformation for the quantum age

IBM **Quantum**

Quantum computing is going to require new skills that will be some of the most in-demand skills in the world.

Quantum stack components	Skills required
Technical services	General technology expertise
Applications	Application architecture and development
Use case-specific libraries	Industry/domain knowledge
Performance libraries	Quantum computing system algorithms
Compilers, optimizers, simulators	Advanced math, quantum computing system expertise
Assembly language and drivers	Quantum physics, quantum computing system expertise
Quantum computing hardware	Quantum physics, chemistry, engineering

What components and skills can help you achieve quantum computing literacy?

Quantum Advantage

Where quantum computers plus classical systems can do significantly better than classical systems alone

IBM Quantum / © 2021 IBM Corporation

The realized business value of quantum computing will come in waves

IBM **Quantum**

Wave 1
Low tide

Low key murmurs in some research corners

Wave 2
High tide

Breakthroughs are more structured and commonplace

Wave 3
Tsunami

Breakthroughs grow more complex and revolutionary

Quantum Advantage occurs when a computing task of interest to business or science can be performed more efficiently, more cost effectively, or with better quality using quantum computers.

In the near-to-medium term, quantum computing can be applied to problems in three areas

IBM **Quantum**

Simulation
Such as modeling processes and systems that occur in nature

- Chemistry
- Pharmaceuticals
- Materials
- Electric batteries

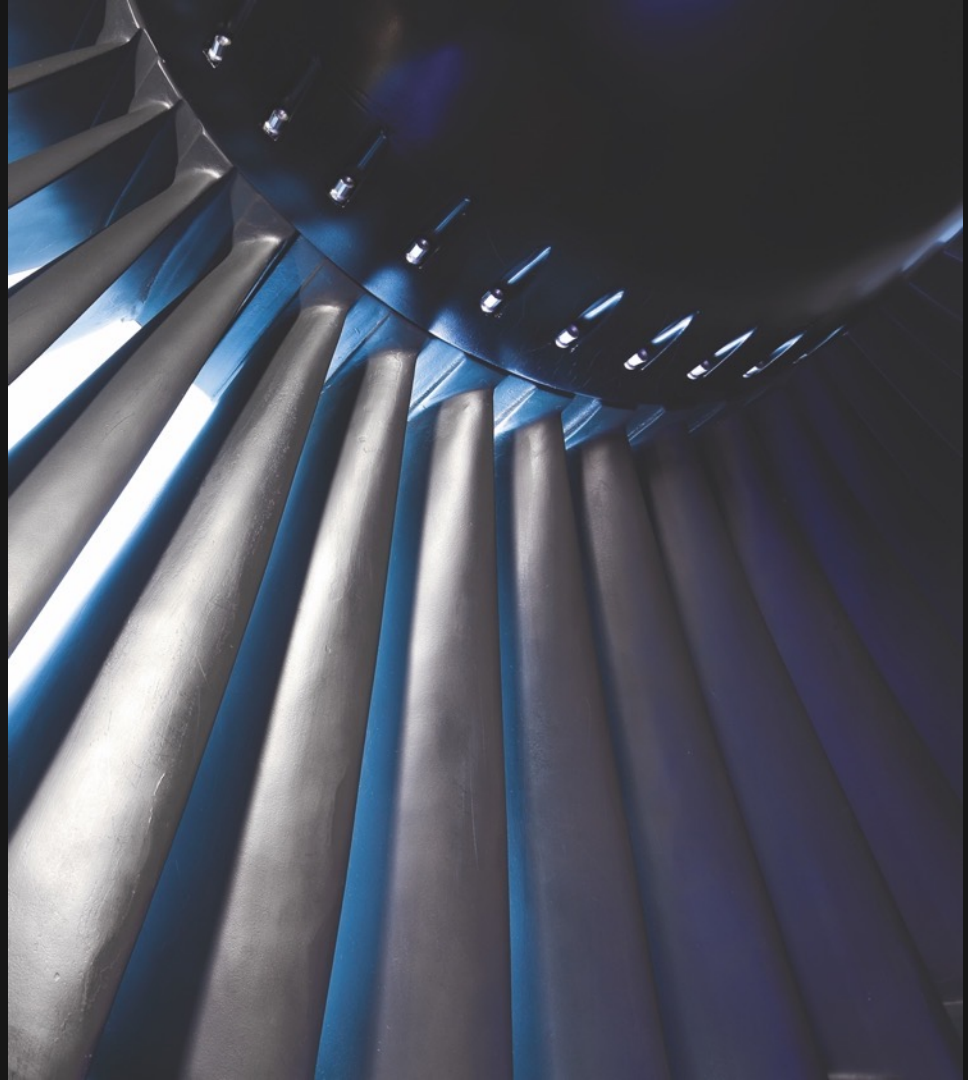
Search and graph
Involving searching for the best or "optimal" solution in a situation with many possible answers

- Sampling
- Travel and transportation
- Logistics / supply chain
- Network infrastructure
- Air traffic control
- Work scheduling

Algebraic problems
Including applications for machine learning

- Adaptive vendor / customer interactions
- Decision support
- Training

Industry Guides



IBM Quantum / © 2021 IBM Corporation

Airlines

Untangling operational disruption for airlines (IROPS)

Enhancing contextual personalized services for airline customers

Optimizing airline network planning globally

© Copyright 2020 IBM Corporation

Banking and financial markets

Targeting and prediction

Risk profiling

Trading optimization

IBM Quantum / © 2021 IBM Corporation

Chemicals and petroleum

Developing chemical products,

including catalysts and surfactants

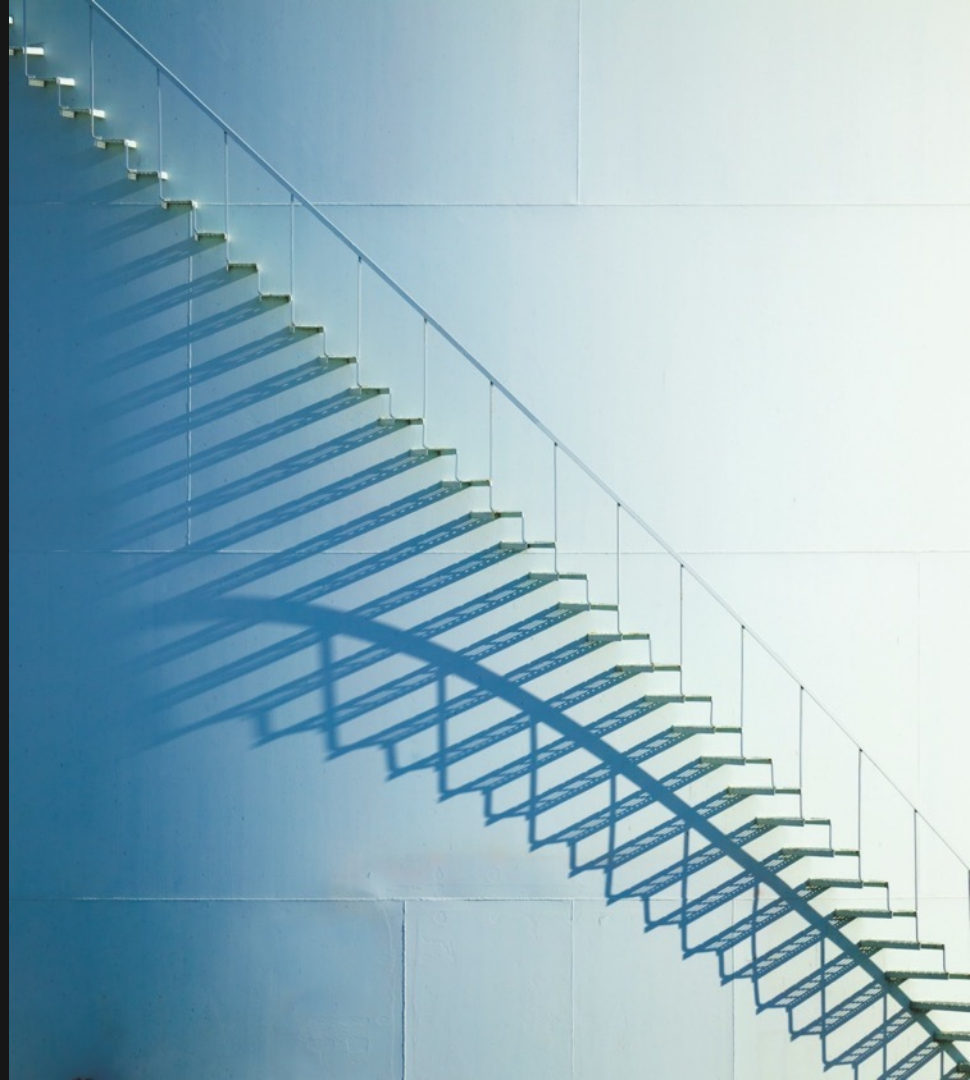
Optimizing feed-stock routing,

refining, and taking product to market

Expanding reservoir

production

IBM Quantum / © 2021 IBM Corporation



Healthcare

Diagnostic assistance

Insurance premiums and pricing

Precision medicine

IBM Quantum / © 2021 IBM Corporation

Life sciences

Creating precision medicine therapies by linking genomes and outcomes

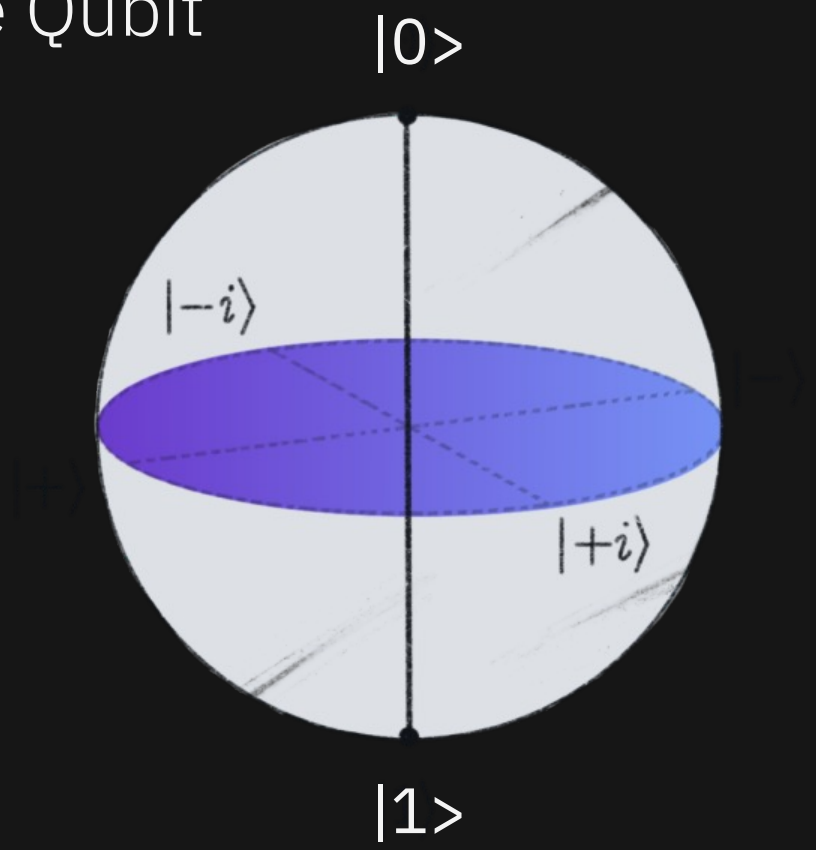
Improving patient outcomes by enhancing the efficiency of small-molecule drug discovery

Developing novel biological products based on protein folding predictions

IBM Quantum / © 2021 IBM Corporation

Fundamentals of Quantum Computing

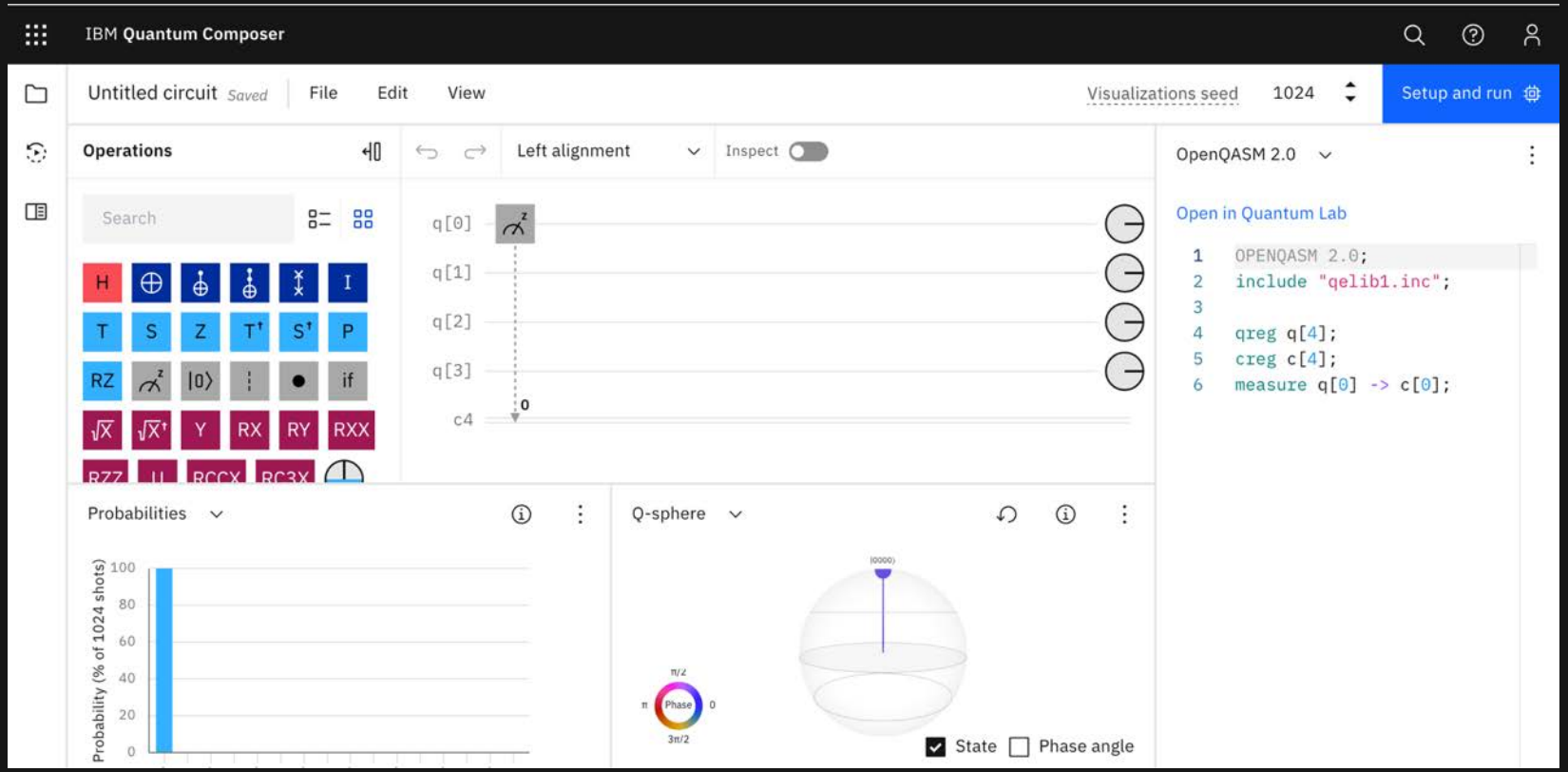
Introducing the Qubit



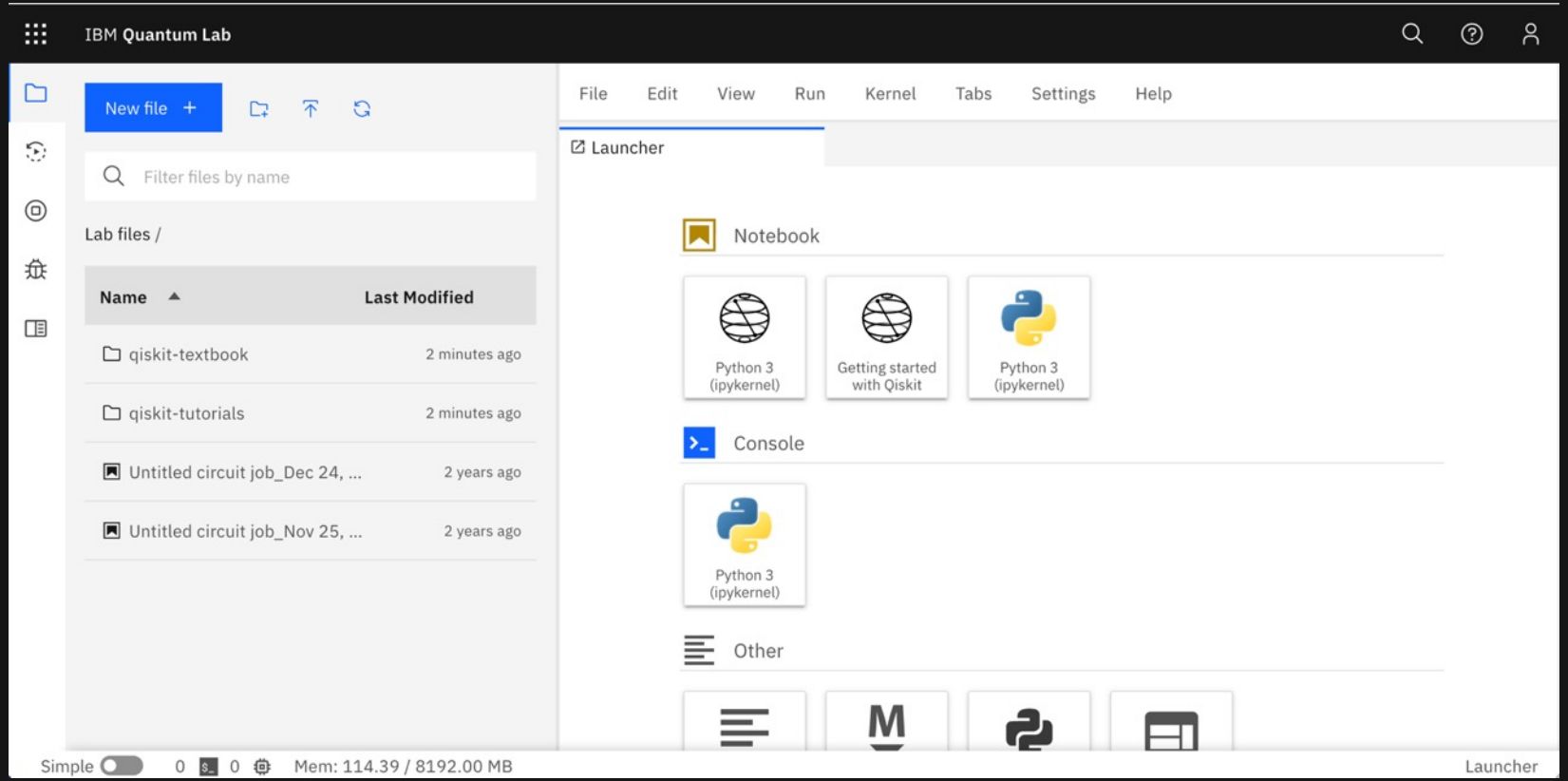
Three Key Quantum Phenomena

- Superposition
- Entanglement
- Interference

IBM Quantum Composer



IBM Quantum Lab



The Road to Quantum Advantage

The road to Quantum Advantage

Quantum science

Create the fundamental theoretical and physical building blocks of quantum computing.

Quantum ready

Engage the world to prepare for the quantum computing era.

Launch of the IBM Q Network

Quantum advantage

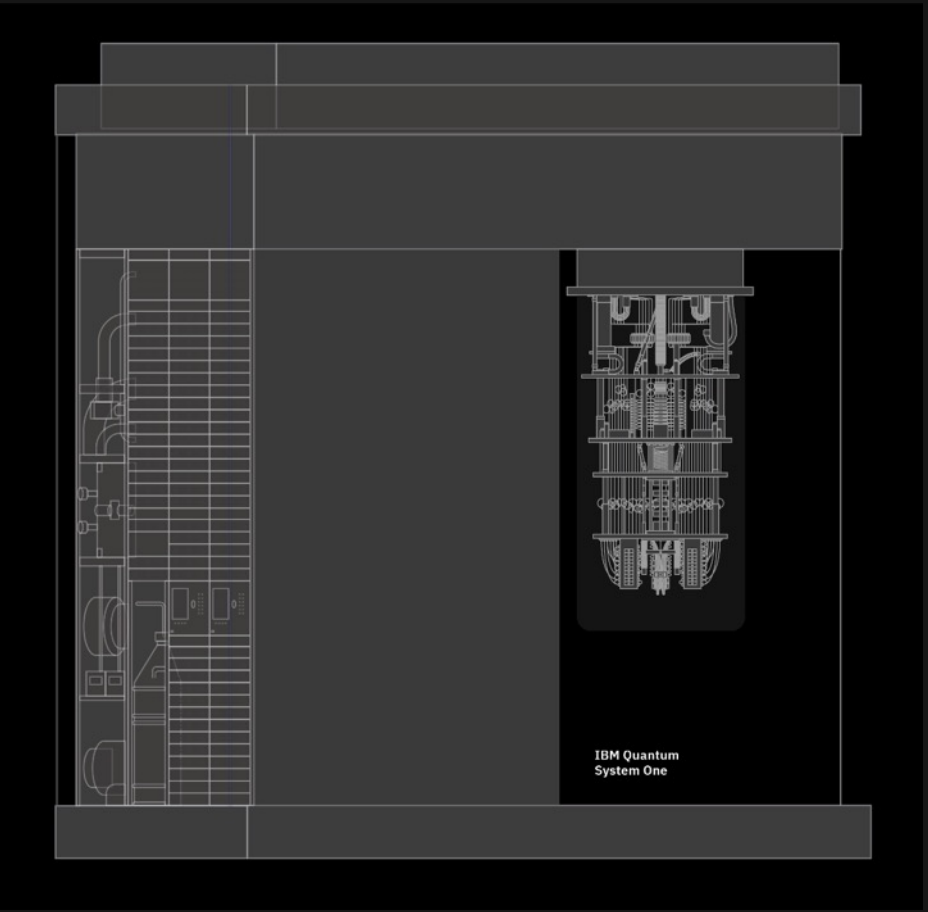
Commercial advantage to solving real world problems with quantum computing systems.

1900s | 2016 | ~2020s | 2050+

© 2019 IBM Corporation #IBMQ

IBM Quantum System One

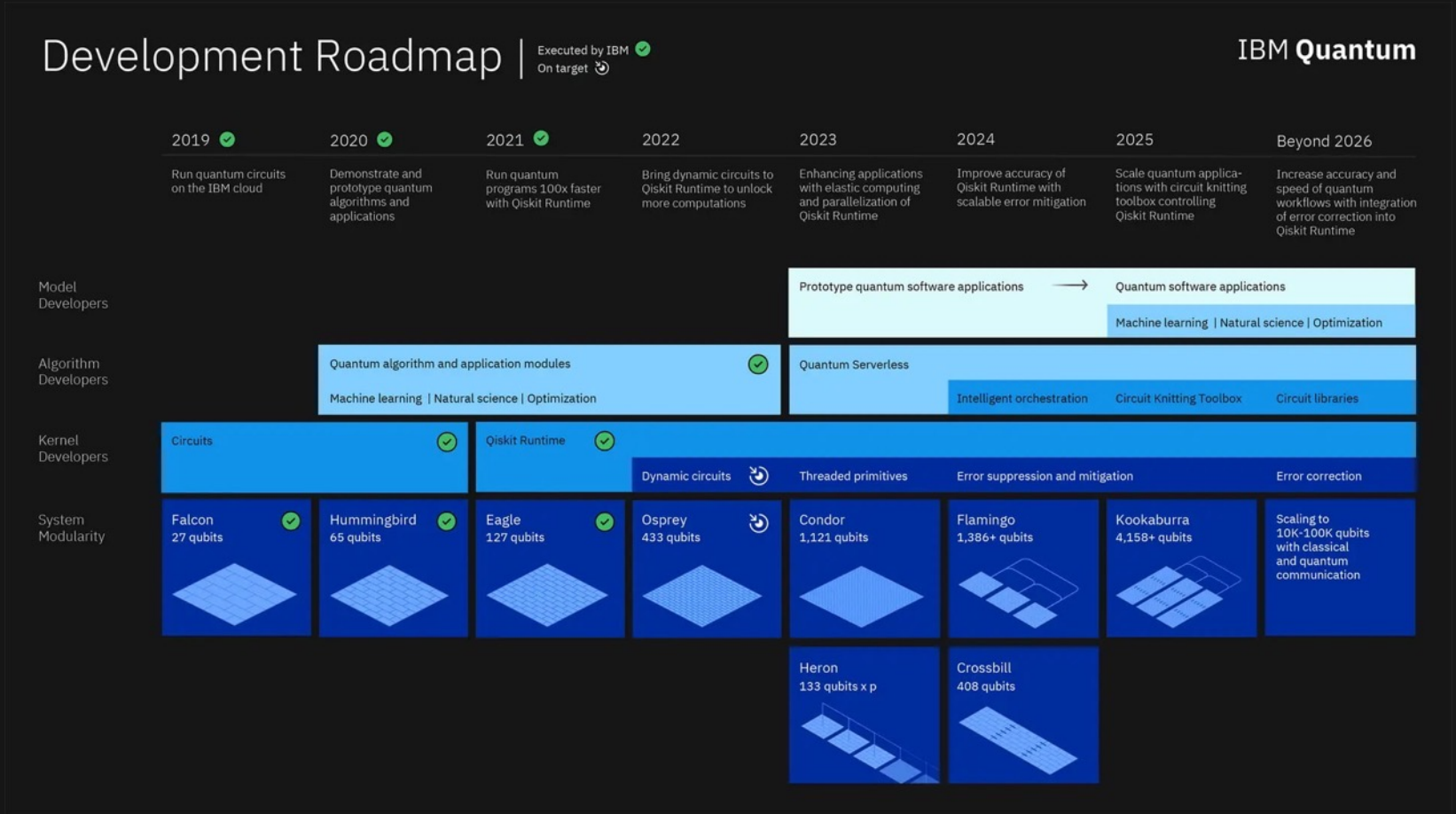
IBM **Quantum**



Current generation of technologies includes the Eagle processor at 127 qubits with state of the art:

- Processor
- Components & wiring
- Cryogenic Platform
- Control electronics
- Cloud Platform

IBM Quantum Development Roadmap



IBM Quantum System One – Strategic partnerships

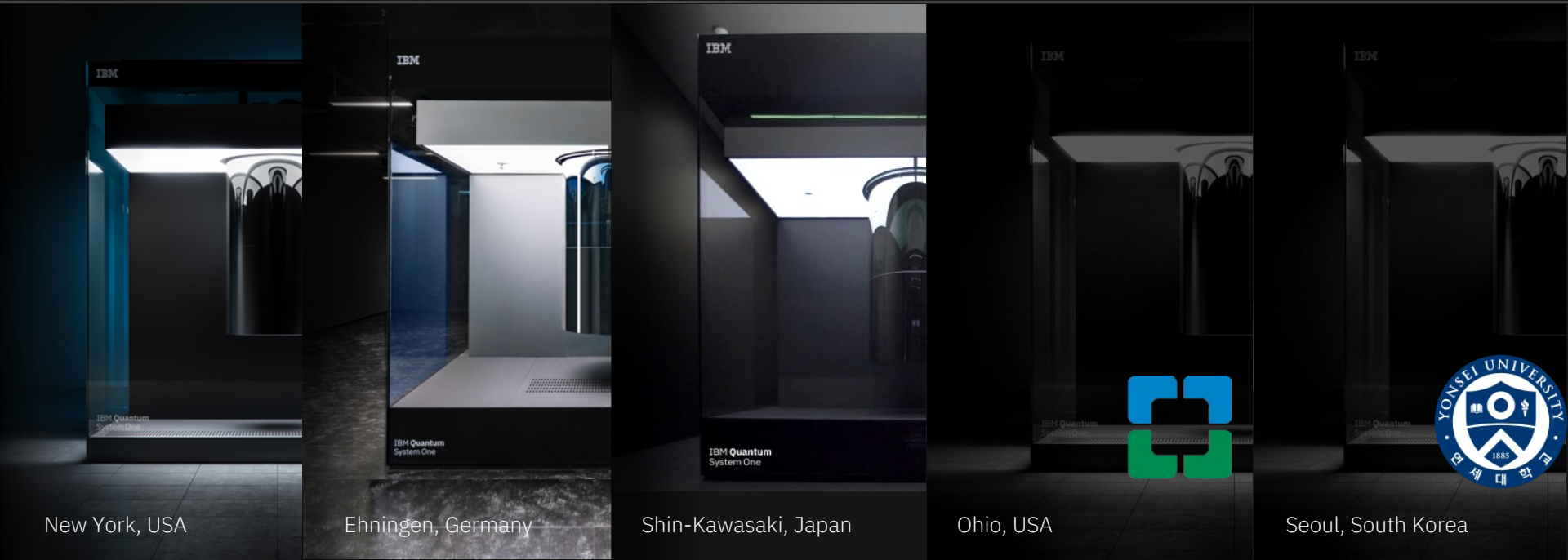
IBM Quantum datacenter with 20+ systems deployed

IBM Quantum | Fraunhofer

IBM Quantum | University of Tokyo

IBM Quantum | Cleveland Clinic

IBM Quantum | Yonsei University



New York, USA

Ehningen, Germany

Shin-Kawasaki, Japan

Ohio, USA

Seoul, South Korea

IBM Quantum Network

A collaborative community of discovery

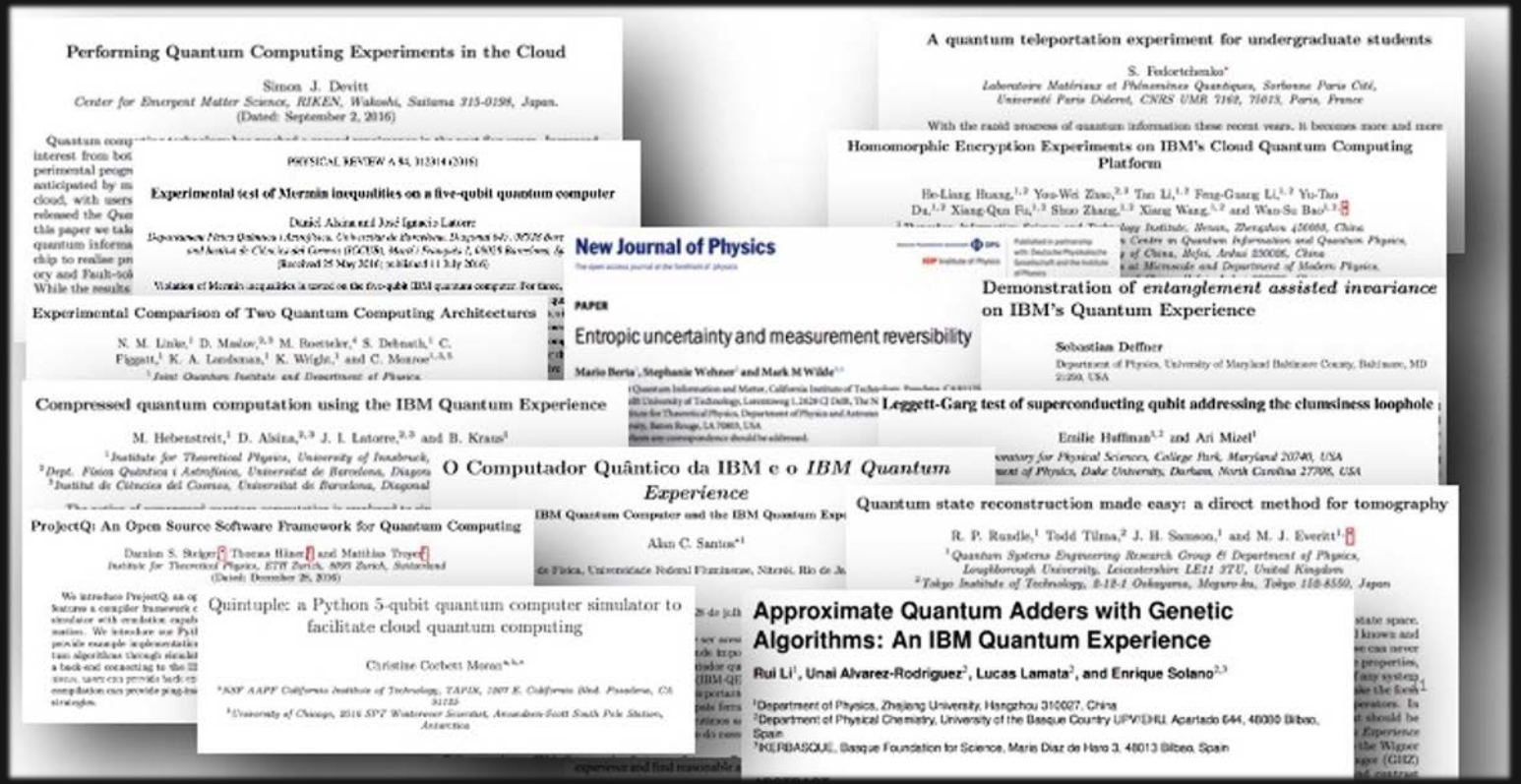
Educate and Train

Accelerate Research

Develop Applications

Enabling Research: 700+ papers and counting

IBM **Quantum**



Quantum Safe Cryptography

IBM Quantum / © 2022 IBM Corporation

Our modern digital world depends on cryptography

IBM Quantum / © 2022 IBM Corporation

Understanding the Quantum Threat

Exponential speedup for some algorithms

IBM **Quantum**

A quantum computer can solve certain problems much faster

2048-bit composite integer

2519590847565789349402718324004839857142928212620403202777713783604366202070759555626401852588078440691829064124951508218929855914917618450280848912007284499268739280728777673597141834727026189637501497182469116507761337985909570009733045974880842840179742910064245869181719511874612151517265463228221686998754918242243363725908514186546204357679842338718477444792073993423658482382428119816381501067481045166037730605620161967625613384414360383390441495263443219011465754445417842402092461651572335077870774981712577246796292638635637328991215483143816789988504044536402352738195137863656439212010397122822120720357

Problem: find prime factors

$= p \times q$

Expected computation time

Most powerful computer today

millions of years

Shor's Quantum Algorithm

some hours

IBM Quantum / © 2022 IBM Corporation

Scalable Fault-Tolerant Quantum Computers...

IBM Quantum

- will crack most Public Key schemas (due to Shor's Algorithm)
  - Public Key Encryption
  - Digital Signatures
  - Key Exchange Algorithms

  RSA | DSA | ECC | ECDSA | DH

- will weaken (halved) symmetrical crypto algorithms (due to Grover's Algorithm)
  - Hashing
  - Symmetric Encryption
  - Password derivation

  SHA2 | SHA3 | TDES | AES

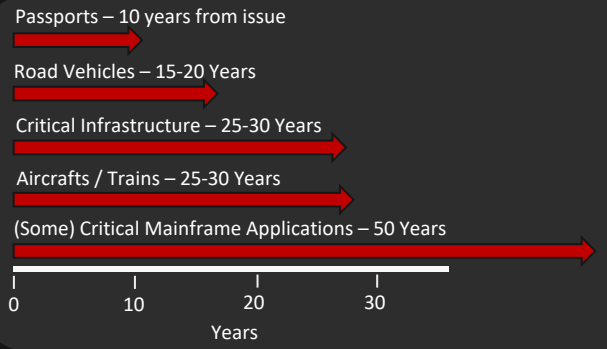
Why is that a problem today?

IBM Quantum / © 2022 IBM Corporation

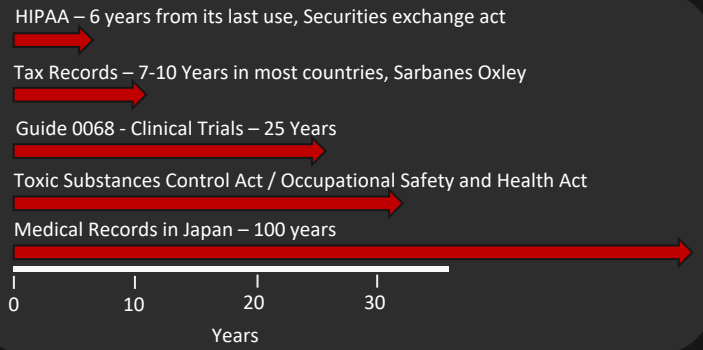
Long Security Horizons

IBM **Quantum**

Infrastructure Update Cycles



Security Time Value of Data



How long do we have?

The National Institute of Standards and Technology predicts it may be possible to break 2048-bit RSA by 2030
- NIST report on Post Quantum Cryptography

"There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031"
- Dr. Michele Mosca, Institute of Quantum Computing, University of Waterloo

"60% fewer cryptographically related security breaches and application failures experienced by organizations with crypto-agility plans in place by 2021, than organizations without a plan"
- Gartner Group

IBM Quantum / © 2021 IBM Corporation
IBM Quantum / © 2022 IBM Corporation

Quantum Threats

IBM **Quantum**

What threats would a future 'quantum attacker' impose?

Threat 1: Loss of data confidentiality

Decryption of communicated or stored data and disclosure of confidential data.

Threat 2: Fraudulent Authentication

Gaining unauthorized access, manipulating systems or stealing company secrets.

Threat 3: Loss of data integrity & legal history

Modifying digitally signed data and forging signatures and contracts.

IBM Quantum / © 2022 IBM Corporation

IBM Quantum Safe / IBM CONFIDENTIAL / © 2022 IBM Corporation

Quantum Safe Cryptographic Algorithms

NIST Standards

- NIST (the National Institute of Standards and Technology in the US) started a program to identify and standardize algorithms for Post-Quantum Cryptography (PQC) in 2015.
- The NIST PQC program followed best practice in the cryptography community with submission, and public analysis of candidates by academia, industry and government.
- After 82 submissions, and three rounds of analysis, July 5th, 2022 NIST announced the four candidate algorithms to be standardized 2022-2024, based on security, cost/performance and algorithm and implementation characteristics.
- None of the new algorithms can be attacked by a classical or quantum computer

Purpose	Algorithm
Public-key Encryption and Key establishment Algorithms	**CRYSTALS-Kyber**
Digital Signature Algorithms	**CRYSTALS-DILITHIUM**
	Falcon
	SPHINCS+

NIST Selected Algorithms, 05 July 2022. NIST will recommend two primary algorithms to be implemented for most use cases: CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures).

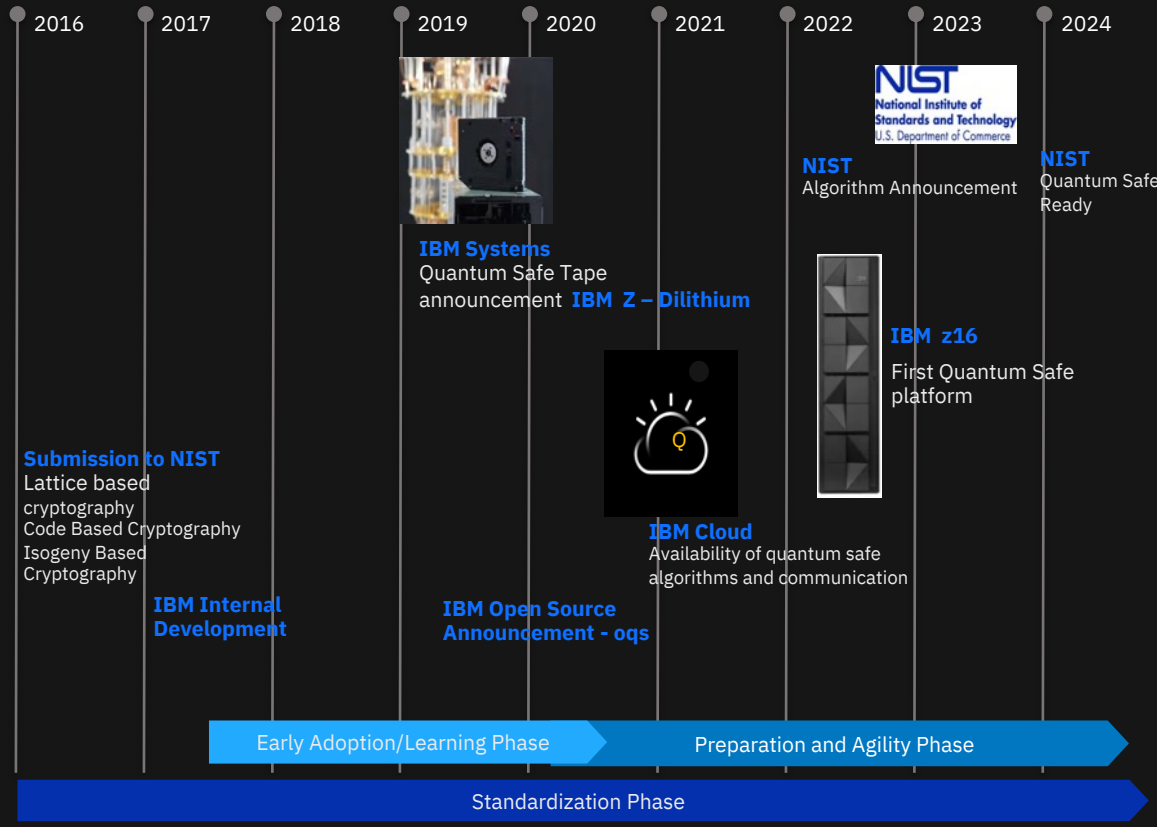
https://csrc.nist.gov/projects/post-quantum-cryptography

IBM Submission

IBM Quantum / © 2022 IBM Corporation

IBM and Quantum Safe

IBM **Quantum**



1. World leading research group on quantum safe algorithms
2. Production Quantum Safe libraries
3. Clear roadmap to quantum safe platforms
4. Commitment to opensource
5. Commitment to Quantum Safe industry standards
6. Clear understanding of cryptographic agility
7. Rapidly developing understanding in quantum safe migration
8. Research and development of approaches, tools, processes

IBM Quantum / © 2022 IBM Corporation

Migrating to a Quantum Safe future

IBM **Quantum**

Understand the threat

Understand the risk

Re-design crypto for agility

Migrate to agile and quantum safe

1. Better governance to manage cryptography

2. Better ways to consume cryptography

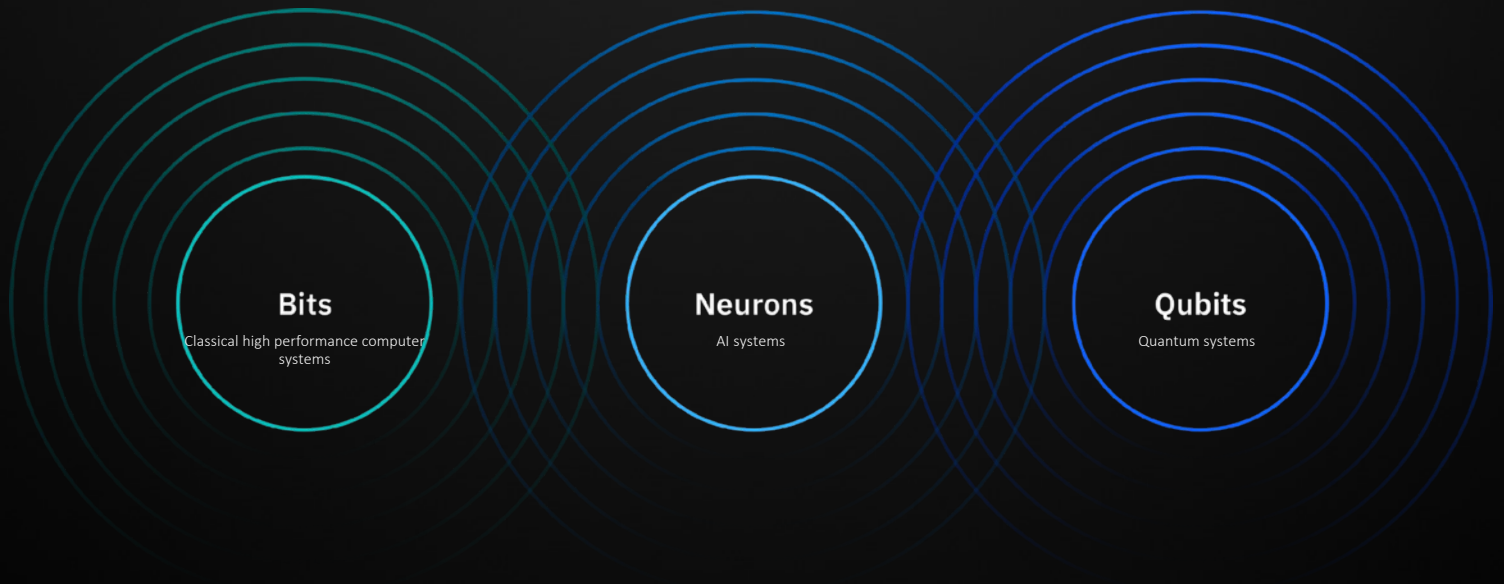
3. Automation to simplify the migration to new cryptography

Agility needs to be applied across these phases

Quantum computing completes a trinity of technologies

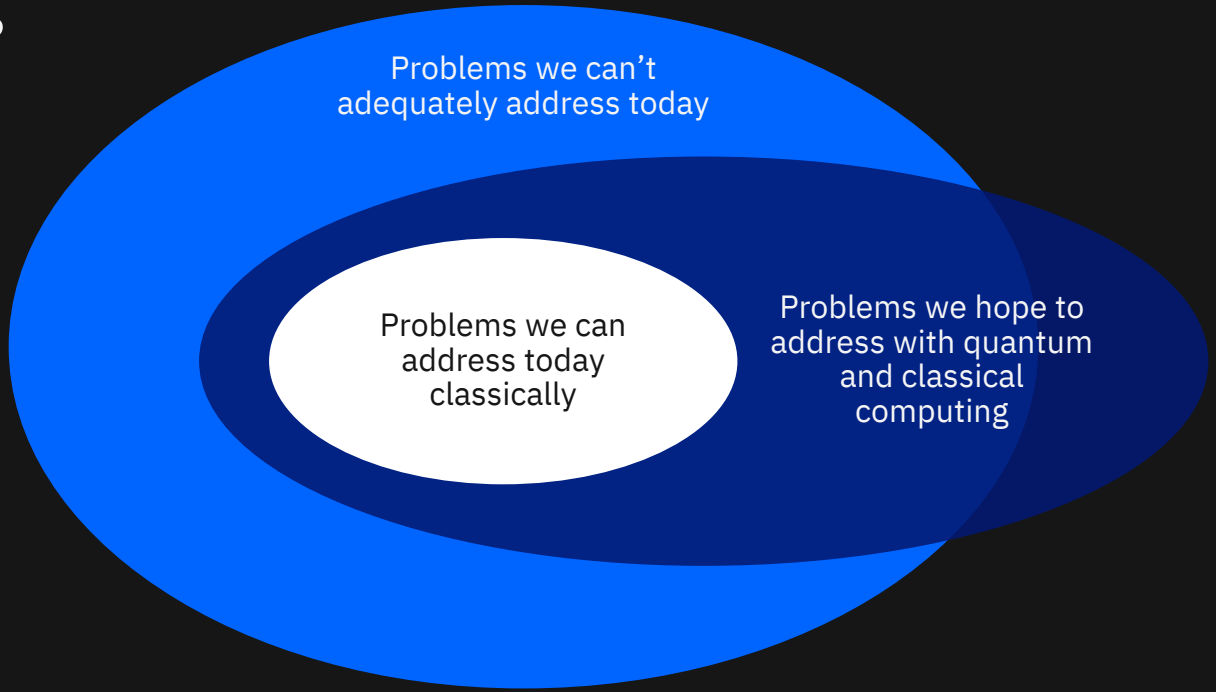
IBM **Quantum**

The synergies created by this triad, not quantum computing alone, are driving the future of computing.



Quantum + Classical is the future of computing

IBM **Quantum**



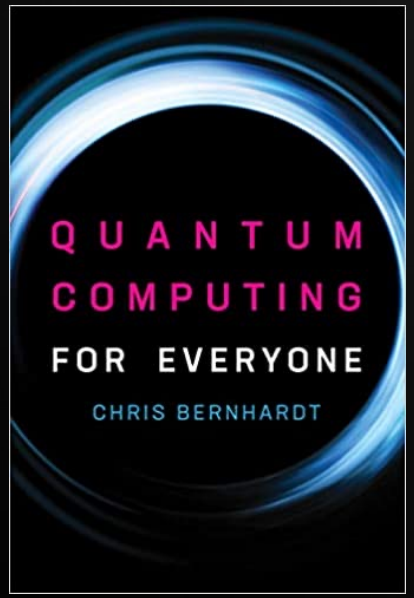
Quantum Computing Resources

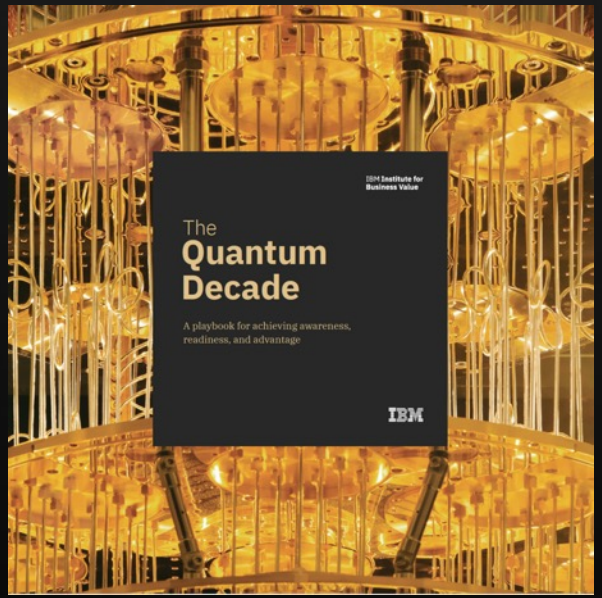
IBM Quantum

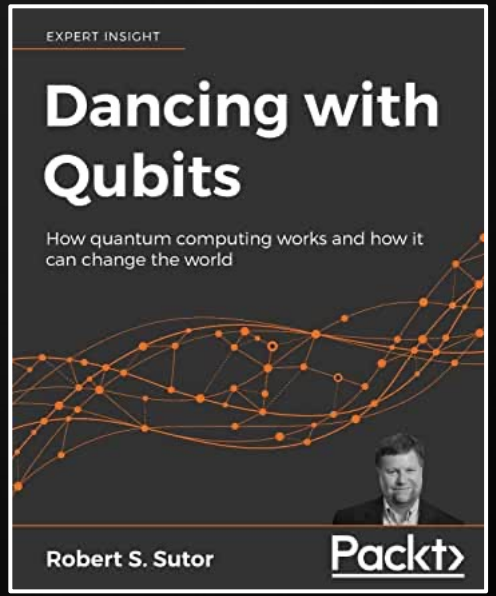
IBM Quantum Composer & IBM Quantum Lab

- https://quantum-computing.ibm.com/

Quantum Computing Books







IBM **Quantum**

© Copyright IBM Corporation 20221. All rights reserved.

The information contained in these materials is provided for informational purposes only and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and ibm.com are trademarks of IBM Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available at Copyright and trademark information.