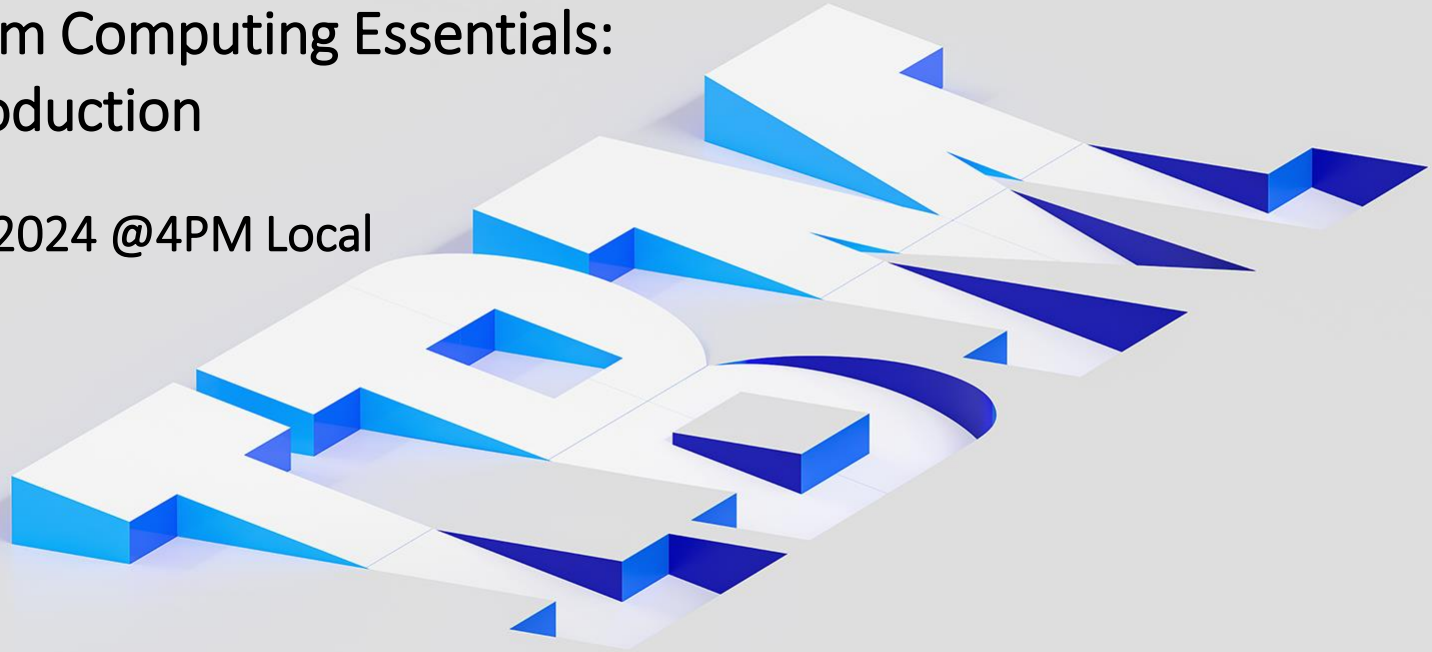
# DAFITC 2024 – Montgomery, AL

## Quantum Computing Essentials: An Introduction

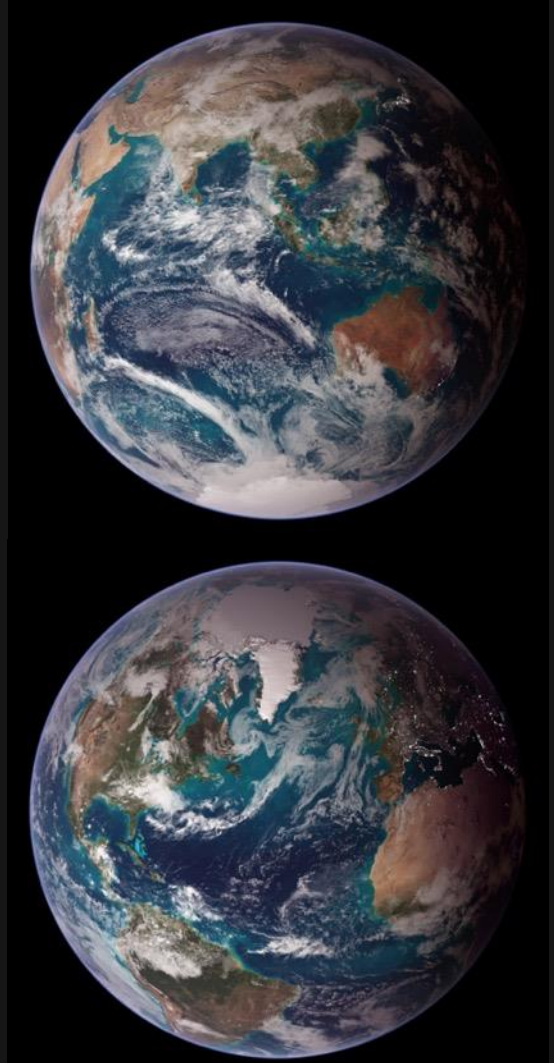
Aug 27, 2024 @4PM Local



Gabe Chang, Account Technical Leader
IBM Quantum Ambassador
changg@us.ibm.com

IBM

We are a small planet ...



... with big problems to solve

# One of the world's most powerful supercomputers



**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

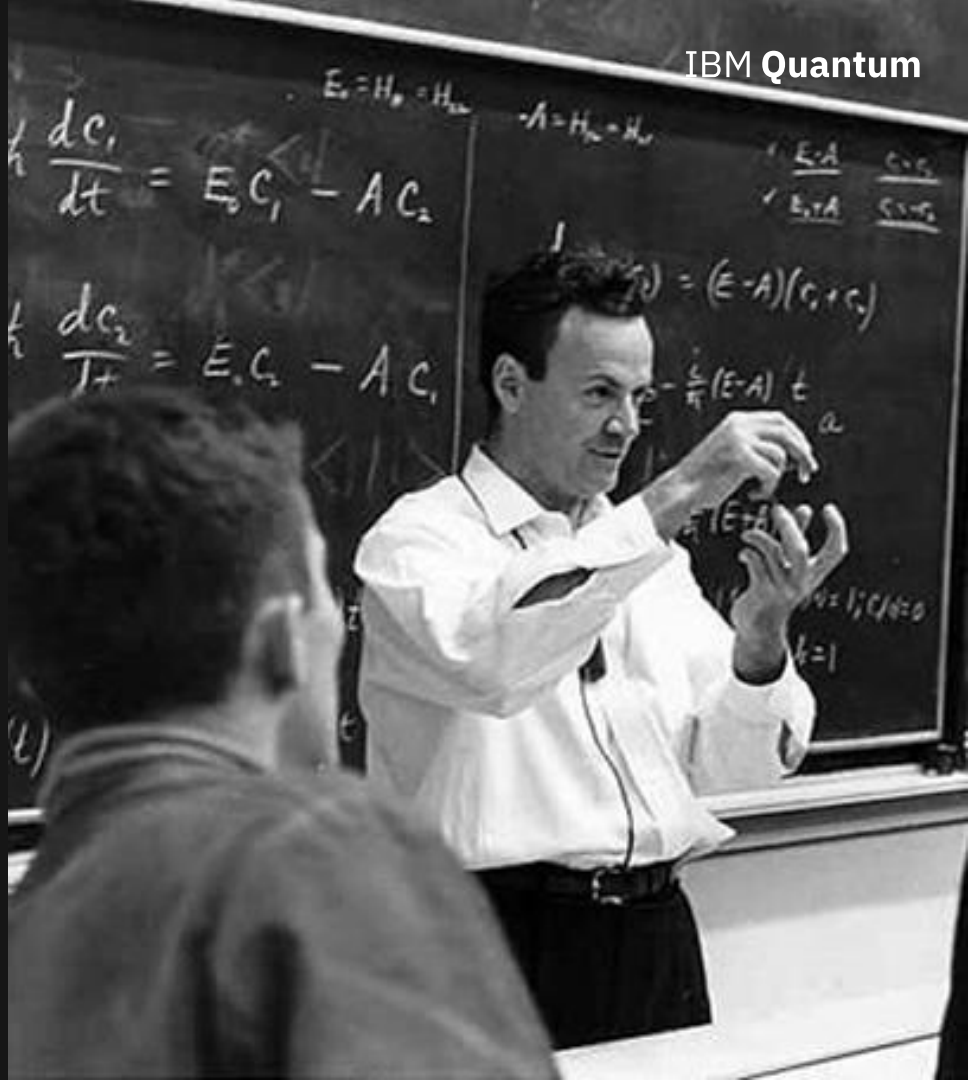
IBM Red Hat Enterprise Linux (RHEL) v 7.4 Operating System


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

“I’m not happy with all the analyses that go with just the classical theory, because nature isn’t classical, dammit, and if you want to make a simulation of nature, you’d better make it quantum mechanical …”

Richard P. Feynman
Department of Physics,
California Institute of Technology

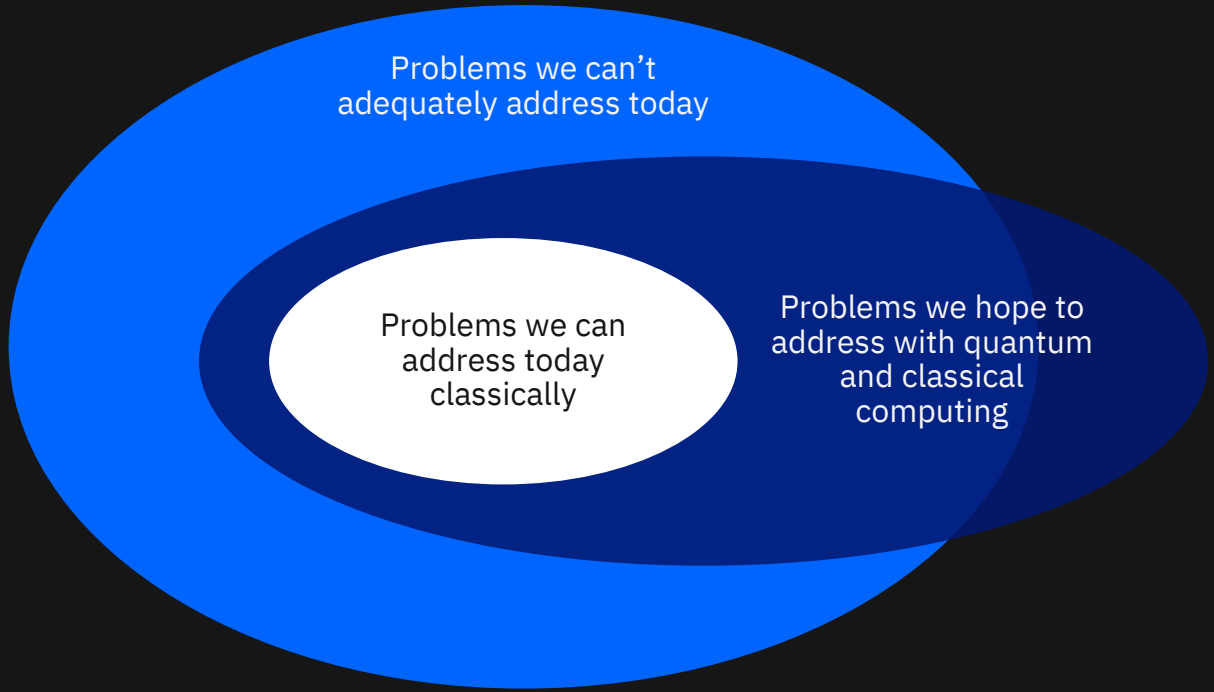
International Journal of Theoretical Physics,
Vol 21, Nos. 6/7, 1982



# Are there still intractable problems?

# Why quantum?

IBM **Quantum**



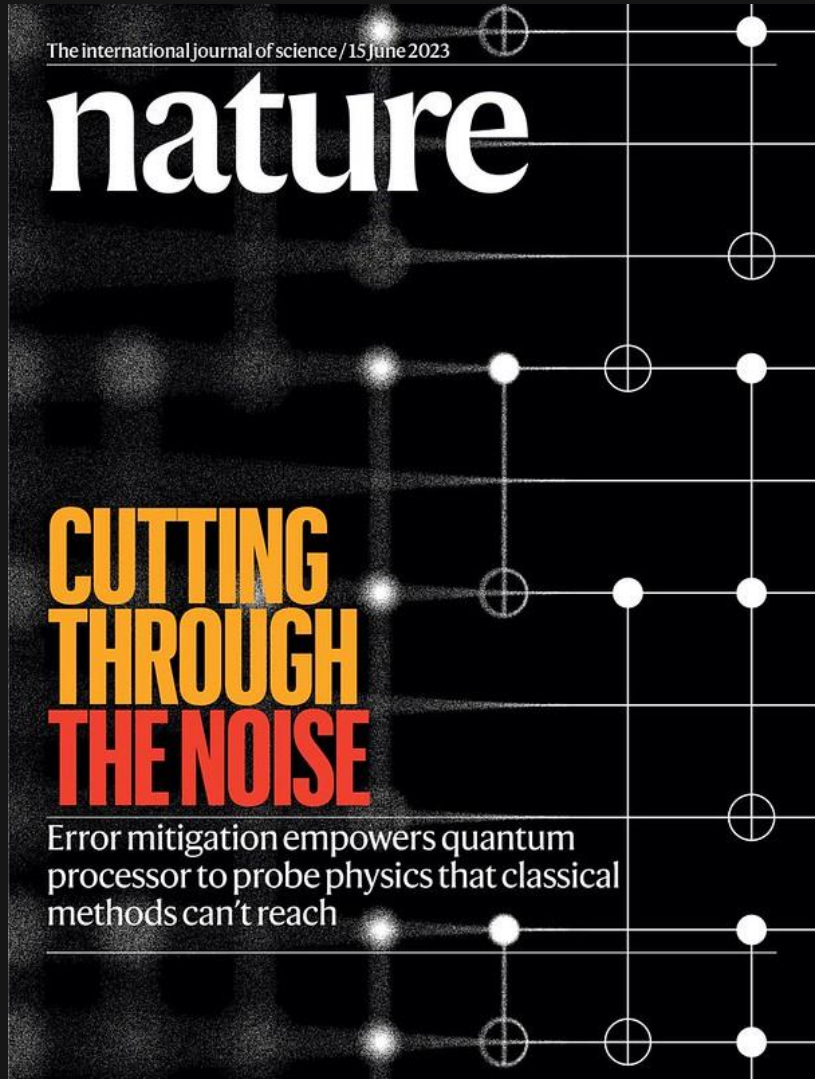

Despite how sophisticated digital "classical " computing has become, there are many scientific and business problems for which we've barely scratched the surface.

# Nature 2023: Quantum Utility

A noisy quantum computer is able to produce accurate expectation values in regimes beyond brute force classical computation

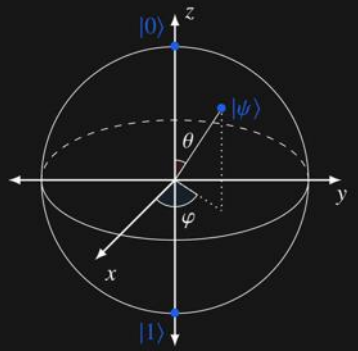
This serves as evidence for the utility of quantum computing before fault tolerance

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



# Quantum computing uses essential ideas from quantum mechanics

## Measurement




Measurement is forcing the qubit's state

$$a\,|0\rangle + b\,|1\rangle$$

to $|0\rangle$ or $|1\rangle$ by observing it, where

- $|a|^2$ is the probability we will get $|0\rangle$ when we measure
- $|b|^2$ is the probability we will get $|1\rangle$ when we measure

For example,

$$\frac{\sqrt{2}}{2}\,|0\rangle + \frac{\sqrt{2}}{2}\,|1\rangle$$

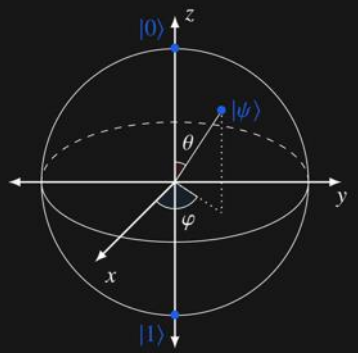
has an equal probability of becoming $|0\rangle$ or $|1\rangle$, and

$$\frac{\sqrt{3}}{2}\,|0\rangle - \frac{1}{2}\,i\,|1\rangle$$

has a 75% chance of becoming $|0\rangle$.

# Quantum computing uses essential ideas from quantum mechanics

## Superposition




Superposition is creating a quantum state that is a combination of |0⟩ and |1⟩

$$a\,|0\rangle + b\,|1\rangle$$

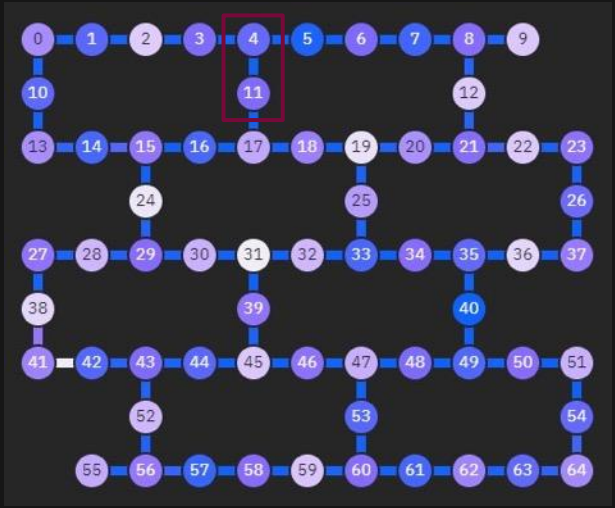
These conditions allow us to map the qubit onto the *Bloch Sphere*.

Note that if $a$ and $b$ are non-zero, then the qubit's state contains both |0⟩ and |1⟩.

This is what people mean when they say that a qubit can be "0 and 1 at the same time."

# Quantum computing uses essential ideas from quantum mechanics

## Entanglement




We can write

$$\frac{\sqrt{2}}{2}|00\rangle + \frac{\sqrt{2}}{2}|01\rangle$$

as

$$|0\rangle \left(\frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle\right)$$

but we cannot write

$$\frac{\sqrt{2}}{2}|00\rangle + \frac{\sqrt{2}}{2}|11\rangle$$

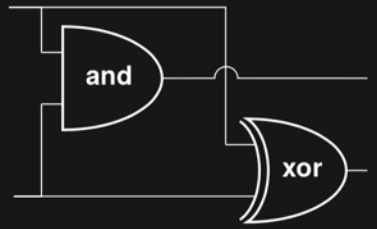
as the “product” of two single qubit states.

They are entangled!

Once you measure the first qubit, the second is uniquely determined.

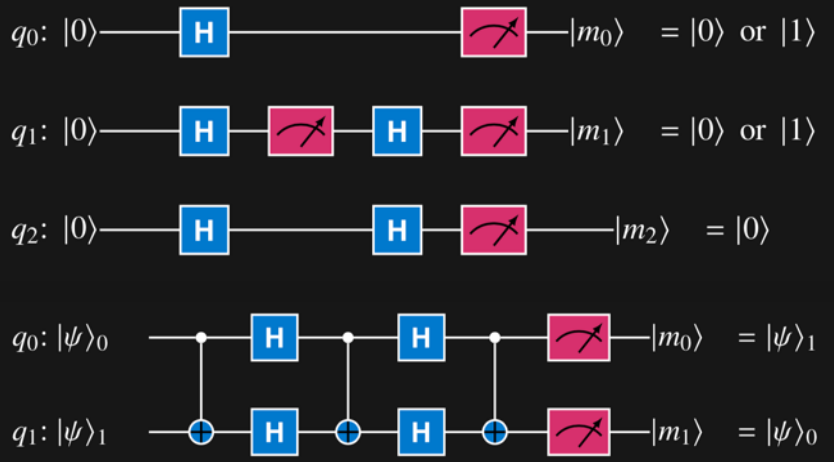
# Quantum computing uses essential ideas from quantum mechanics

## Gates / operations




Classical logical circuits use operations like and, or, not, nand, and xor. We also call these gates.

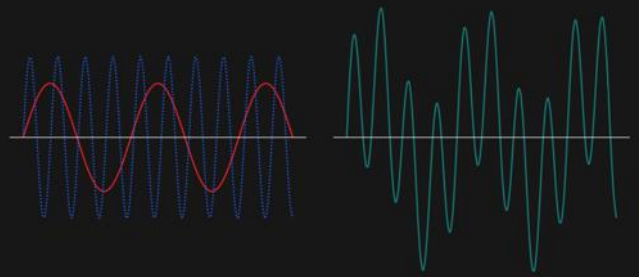
Quantum circuits use reversible gates that change the quantum states of one, two , or more qubits.

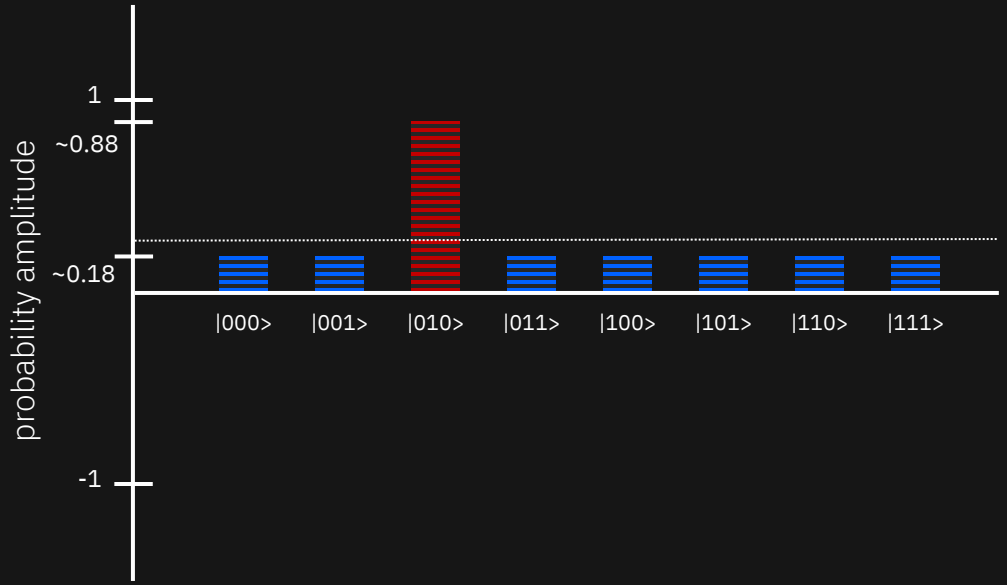


# Quantum computing uses essential ideas from quantum mechanics

Interference allows us to increase the probability of getting the right answer and decrease the chance of getting the wrong one.

## Interference





# Developer ecosystem

IBM **Quantum**

## Model developers

Makes circuits and algorithms accessible to non-experts by allowing developers to describe their problem rather than the solution methodology.

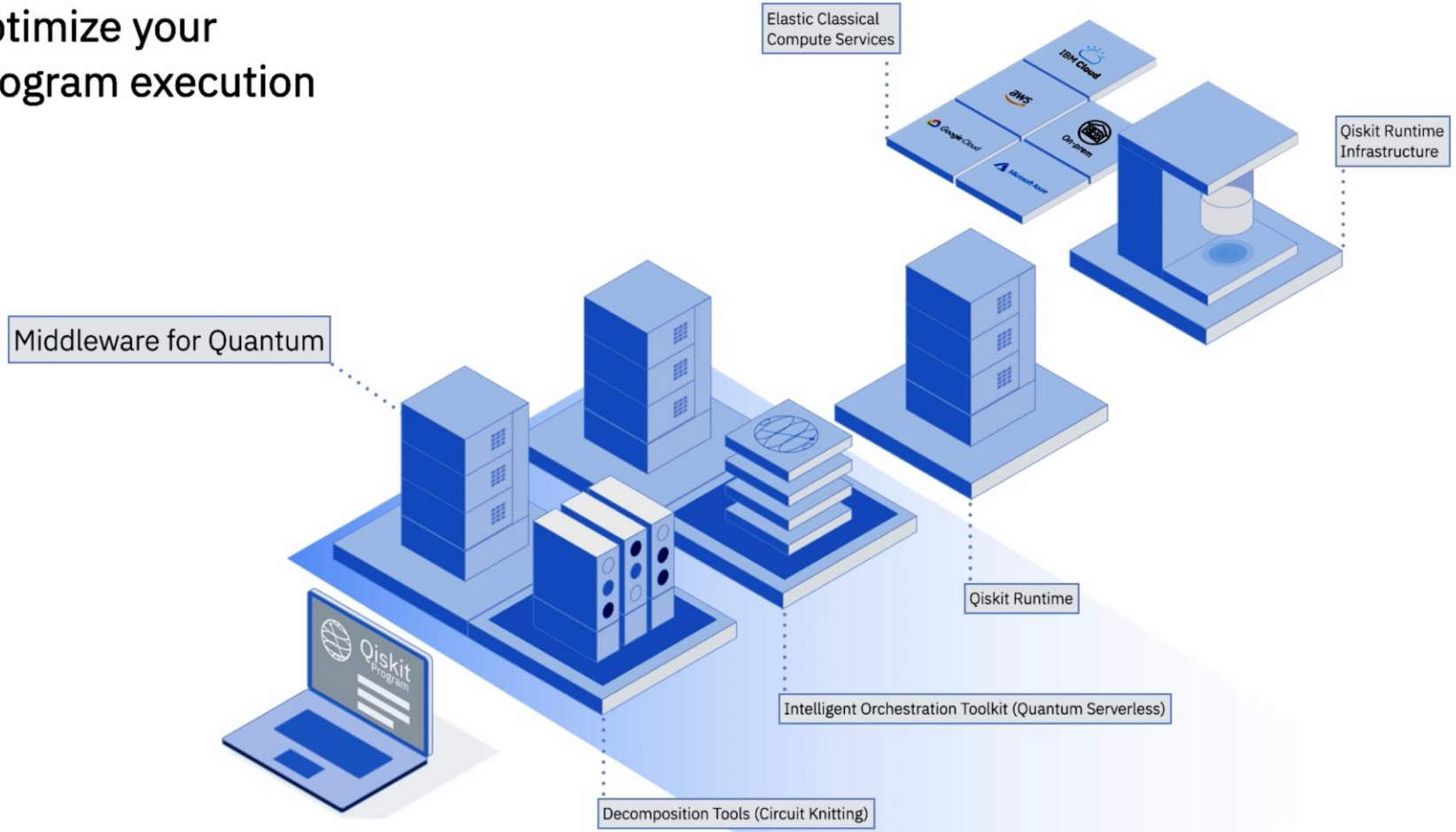
## Algorithm developers

Uses higher level building blocks like state prep, operators and oracles to help them construct algorithms.

## Kernel developers

Creates high performance circuits using pulse level and timing controls

# How to use services to optimize your program execution



# Multicloud workflows

IBM **Quantum**

```
service = QiskitRuntimeService(...)
backends = ["ibmq_kolkata", "ibm_auckland"]

from circuit_knitting_toolbox.circuit_cutting
import WireCutter
cutter = WireCutter(circuit, service, backends)
```

```
# cut (decompose) the circuit on Azure
with serverless.provider('azure'):
    cuts = cutter.decompose("automatic", ...)
```

```
# execute subcircuits using Qiskit Runtime
Primitives
with serverless.provider('ibm'):
    subcircuit_results = cutter.evaluate(cuts)
```

```
# reconstruct probabilities on AWS
with serverless.provider('aws'):
    reconstructed_result =
cutter.recompose(subcircuit_results, cuts)
```

Reconstructed result


Multi-cloud

# Building an *industry*

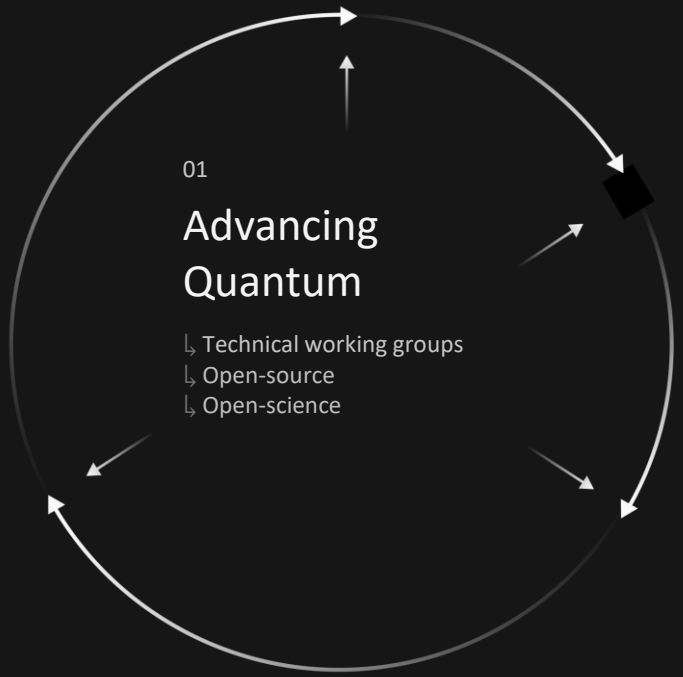
# Building a Quantum Computing *Industry*

IBM **Quantum**

03

## Industry Adoption

- Direct client interactions
- Scaling solutions with partner engagements



01

## Advancing Quantum

- Technical working groups
- Open-source
- Open-science

04

## Application Services

- Access compute resellers
- Software providers
- Application integration

02

## Quantum Innovation Centers

- Access to leading-edge quantum compute services
- Research and development
- Education and workforce development
- Economic development

05

## Quantum Safe

- Direct client interactions
  - Prepare & Discover
  - Assess & Plan Transformation
  - Transform & Ongoing Observability

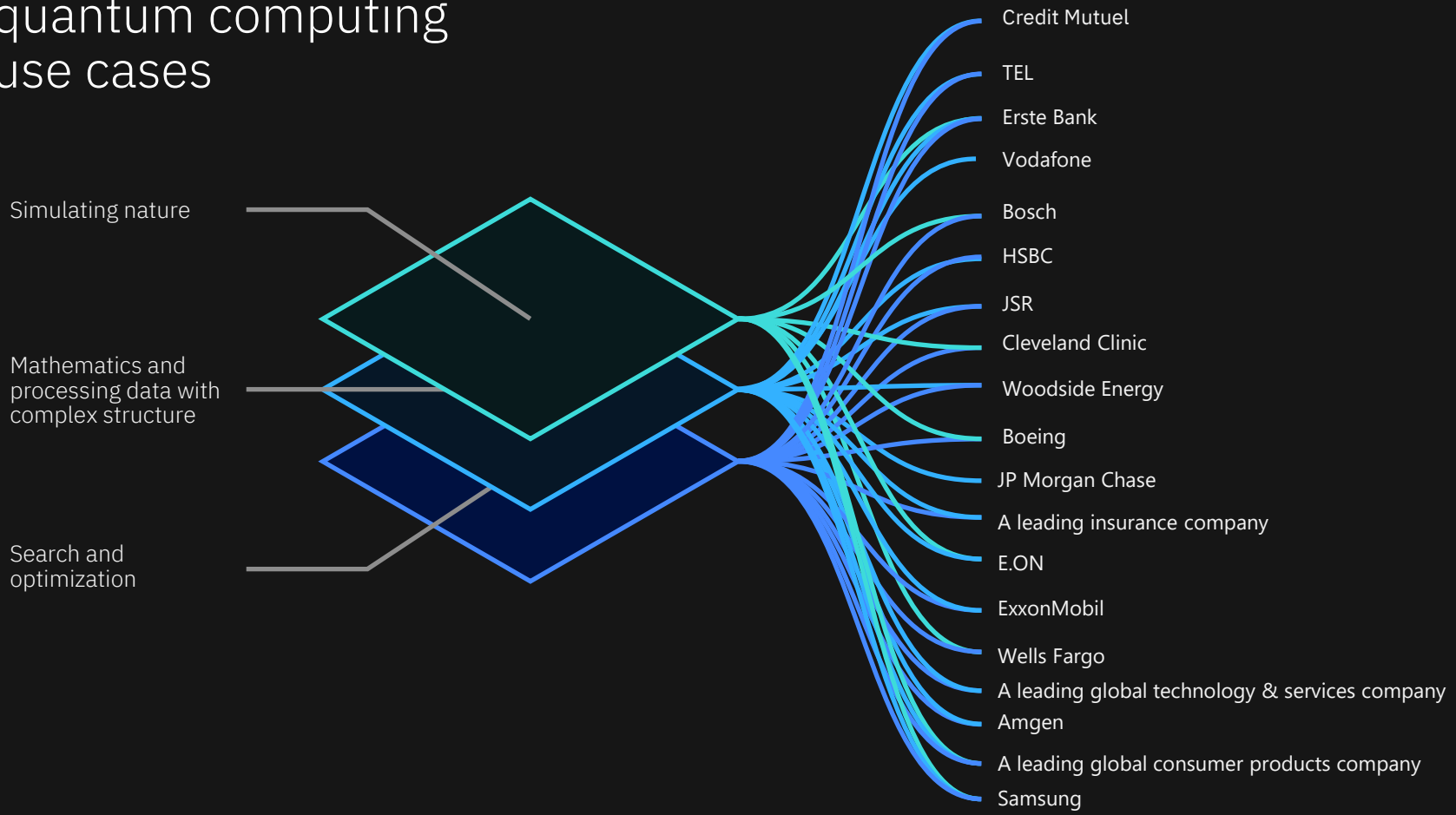
# Quantum applications span three general areas

IBM **Quantum**

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

# Connecting industry clients with quantum computing use cases

IBM **Quantum**

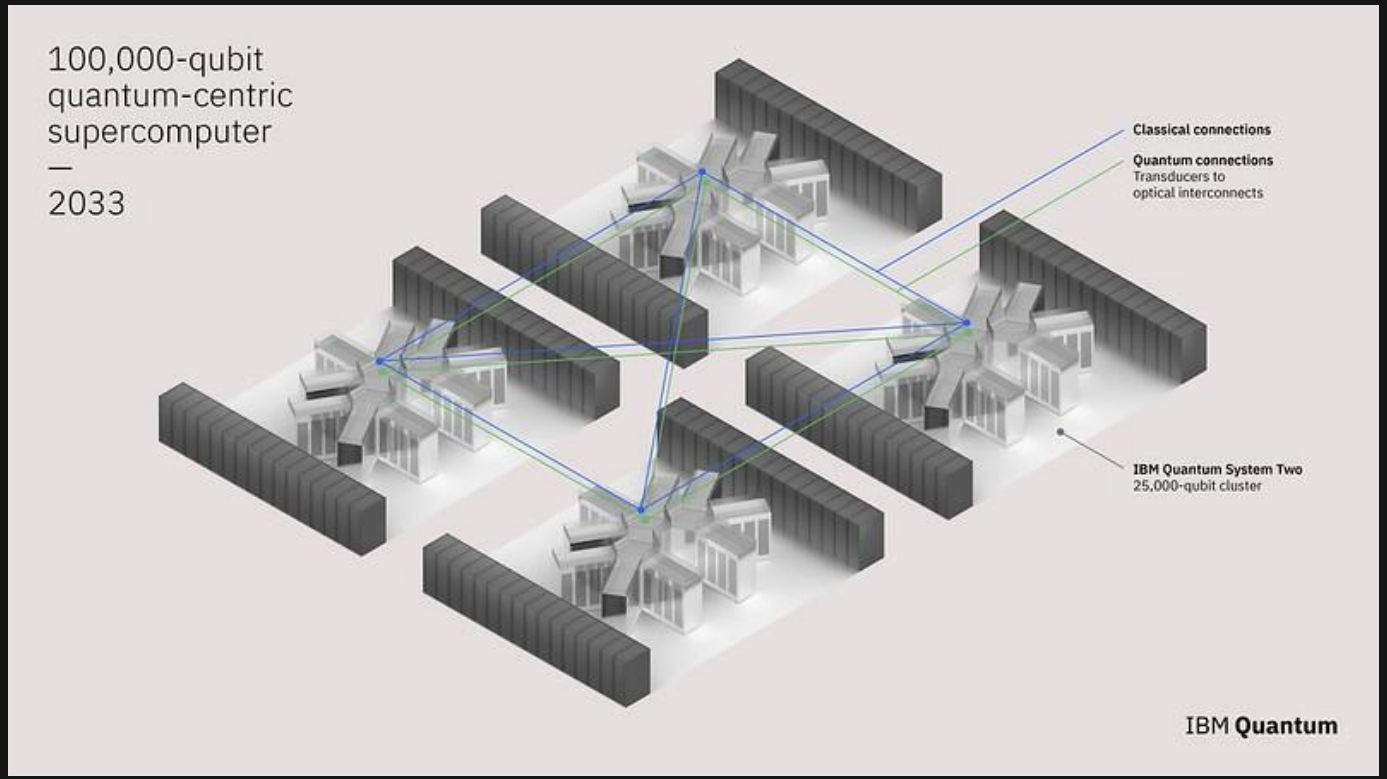


# IBM launches partnership with the University of Chicago and the University of Tokyo to develop a 100,000-qubit Quantum-Centric Supercomputer

IBM **Quantum**

The 10-year, $100 million initiative is a global collaboration and an activation of talent and resources across industries and research institutions is being initiated.

By partnering with the University of Chicago, the University of Tokyo, and IBM's broader global ecosystem, IBM will work over the next decade to advance the underlying technologies for this system, as well as to design and build the necessary components at scale [1].



# Bring useful quantum computing to the world

## A path towards quantum computing

*„IBM's point of view and goal is a computational quantum advantage, where a computational task of business or* **scientific** *relevance can be performed more efficiently, cost-effectively, or accurately using a quantum computer than with classical computations alone.“*

# Our modern digital world depends on public key *cryptography*

IBM **Quantum**

This is now a problem

# Cryptography impacts everything



## Cryptography touches every corner of the digital world

**Internet**
Domain Name Service(DNS), Hyper-text Transfer Protocol (HTTP), Telnet, File-Transfer Protocol (FTP)

**Digital Signatures**
eIDAS – PDF Advanced Electronic Signature – (PAdES), Advanced Electronic Signatures (AES), ...

**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, ...

## Upgrading digital infrastructure takes a long time

Passports – 10 years from issue

Road Vehicles – 15-20 Years

Critical Infrastructure – 25-30 Years

Aircrafts / Trains – 25-30 Years

(Some) Critical Mainframe Applications – 50 Years

## Data needs to stay secure for a long time

HIPAA – 6 years from its last use, Securities exchange act

Tax Records – 7-10 Years in most countries, Sarbanes Oxley

Guide 0068 - Clinical Trials – 25 Years

Toxic Substances Control Act / Occupational Safety and Health Act

Medical Records in Japan – 100 years

# OUR MODERN DIGITAL WORLD
# DEPENDS ON CRYPTOGRAPHY

*Cryptography is the last line of defense*

## Prime factors

= p x q

## 2048-bit composite integer

```
25195908475657893494027183240048398571429282126204032
02777713783604366202070759555626401852588078440691829
06412495150821892985591491761845028084891200728449926
87392807287776735971418347270261896375014971824691165
07761337985909570009733045974880842840179742910064245
86918171951187461215151726546322822168699875491824224
33637259085141865462043576798423387184774447920739934
23658482382428119816381501067481045166037730605620161
96762561338441436038339044149526344321901146575444541
78424020924616515723350778707749817125772467962926386
35637328991215483143816789988504044536402352738195137
86365643921201039712282212072035 7
```

## Expected computation time

The most powerful computer ***today:***

*Millions of years*

Shor's Quantum Algorithm:

***Hours***

Shor's algorithm will crack our asymmetric form of cryptography

- Public Key Encryption
- Digital Signatures
- Key Exchange Algorithms

- RSA
- DSA
- ECC

- ECDSA
- DH

# 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

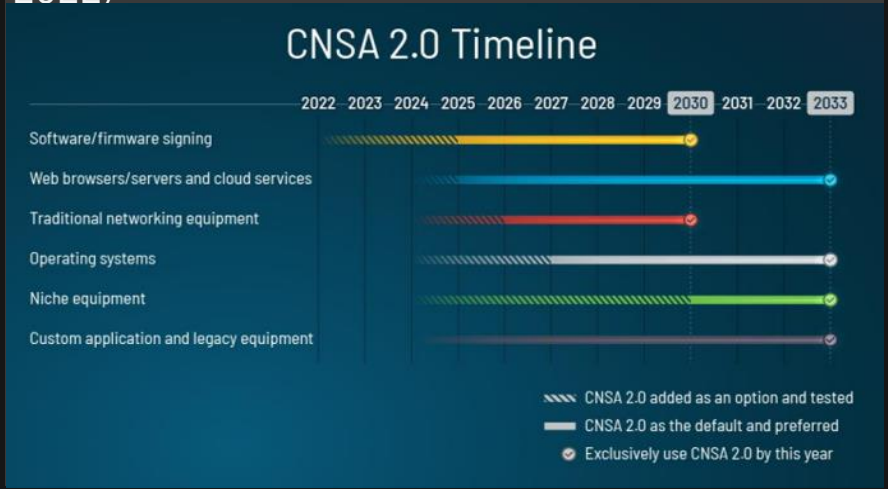
**IBM Quantum Safe**

Support client transition to quantum-safe cryptography

# CNSA 2.0 calls for national security systems to be fully compliant with quantum-resistant algorithms in the early 2030s



National Security Agency (NSA): Commercial National Security Algorithm Suite (CNSA) 2.0 (Sep 2022) [1)]




White House Memorandum - Migrating to Post-Quantum Cryptography (Nov 2022) [2)]

- "By May 4, 2023, [...] agencies are directed to submit a prioritized inventory of information systems and assets, excluding national security systems"
- "Testing of pre-standardized PQC in agency environments will help to ensure that PQC will work in practice before NIST completes PQC standards and commercial implementations are finalized."

1) https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
2) https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

# IBM **Quantum**