Chicago Chapter
Association of Information Technology Professionals

Quantum Engineering in 2024

Arunava (Ron) Majumdar
Advisory Solution Architect
Head, Center for Advanced Studies US
IBM Cloud and Cognitive Platform
https://www.linkedin.com/in/arunava-majumdar/

IBM Center for Advanced Studies

IBM Center for Advanced Studies (CAS) provides high-touch collaborations with Universities and Research organizations to work with faculty and students on a regular basis on agreed upon project initiatives. We provide a flexible plan to orient closely with the university programs like Senior Design Projects, Capstone Projects, etc. to align with the goals and objectives of the university as well as IBM initiatives. This provides a hands-on exposure to industry standards and processes to work on innovative ideas.

CAS centers are located around the world to work with academia at a locally and coordinate with international leaders.

https://arunava.com

Arunava (Ron) Majumdar

arunava@us.ibm.com

ADVISORY SOLUTION ARCHITECT

IBM Application Modernization Portfolio,
Telecommunication Signature Accounts,
Head, Center for Advanced Studies (USA)

IBM Watson Cloud Platform

in https://www.linkedin.com/in/arunava-majumdar/

Arunava (Ron) Majumdar is an Advisory Solution Architect with more than 28 years of software design, architecture and development (23 in IBM). He leads the IBM Application Modernization portfolio for Signature Telecommunication Accounts. He also heads the Center for Advanced Studies (CAS) for the USA and the coordinator for CAS India and CAS Africa.

He has been working on Telecommunication Client Use Cases and Academic Research projects with various universities in diverse fields of Astronomy, Automobiles, Healthcare and others. His focus areas are Integration, Artificial Intelligence and Pattern Engineering and holds several patents in these fields. He is involved with automated deployment strategies to the Cloud and Kubernetes environments.

Ron is in the leadership board for IBM Open Innovation Community (OIC) for the Chicago Chapter, Chicago Chapter Leader for AI Camp, Host for the Future Tech SIG at AITP Chicago and the Lead for the Developer Advocacy program in Chicago in collaboration with AI Alliance.

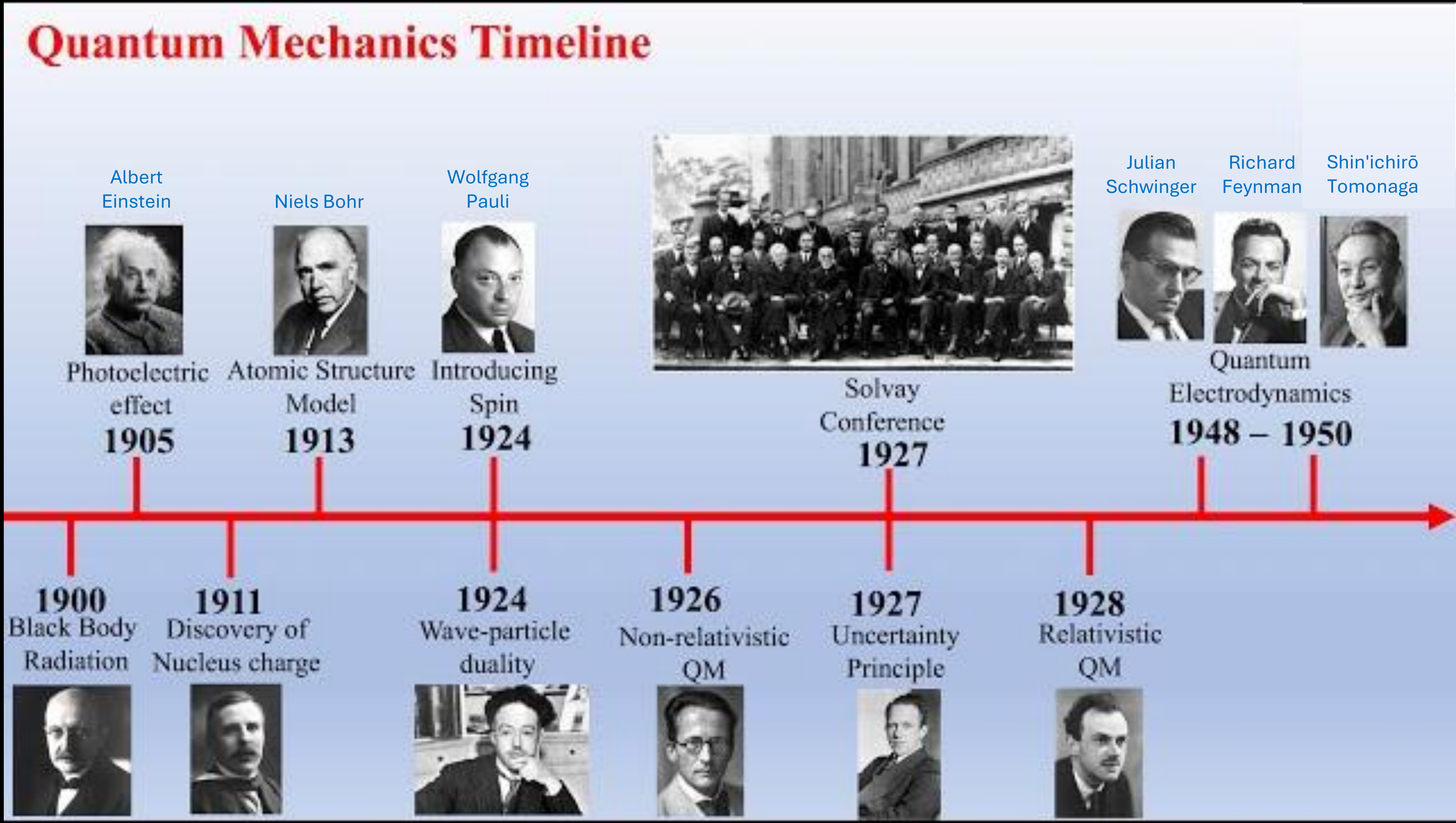
Titles: • Founder, IBM Services Asset Community • Founder, Open Development Platform • Lead, IBM Asset Strategy • Member, IBM Academy of Technology • Host, Future Tech SIG, AITP Chicago • President, Chicago Emerging Leaders • Board, IdeazShack Innovation Center • Chapter Lead, AI Camp • Founder, Chicago Panthers • Life Member, Poet's Foundation • Content Creator and Editor, Open Development, Developerworks TV • Mentor, Polsky Center, University of Chicago • Lead, Developer Advocacy in Chicago, AI Alliance

HISTORY OF QUANTUM MECHANICS

Perhaps the most famous conference was the fifth Solvay Conference on Physics, which was held from 24 to 29 October 1927. The subject was *Electrons and Photons* and the world's most notable physicists met to discuss the newly formulated quantum theory. The leading figures were Albert Einstein and Niels Bohr.

1927 Solvay Conference: Bottom Row: I. Langmuir, M. Plank, M. Curie, H. A. Lorentz, A. Einstein, P. Langevin, C. E. Guye, C. T. R. Wilson, O. W. Richardson, Middle Row: P. Debye, M. Knudsen, W. L. Bragg, H. A. Kramers, P. A. M. Dirac, A. H. Compton, L. V. de Broglie, M. Born, N. Bohr, Top Row: A. Piccard, E. Henriot, P. Ehrenfest, E. Herzen, T. de Donder, E. Schrodinger, E. Verschaffelt, W. Pauli, W. Heisenberg, R. H. Fowler, L. Brillouin

Dawn of Quantum Mechanics



Max Plank

Ernest Rutherford

Louis de Broglie

Erwin Schrödinger

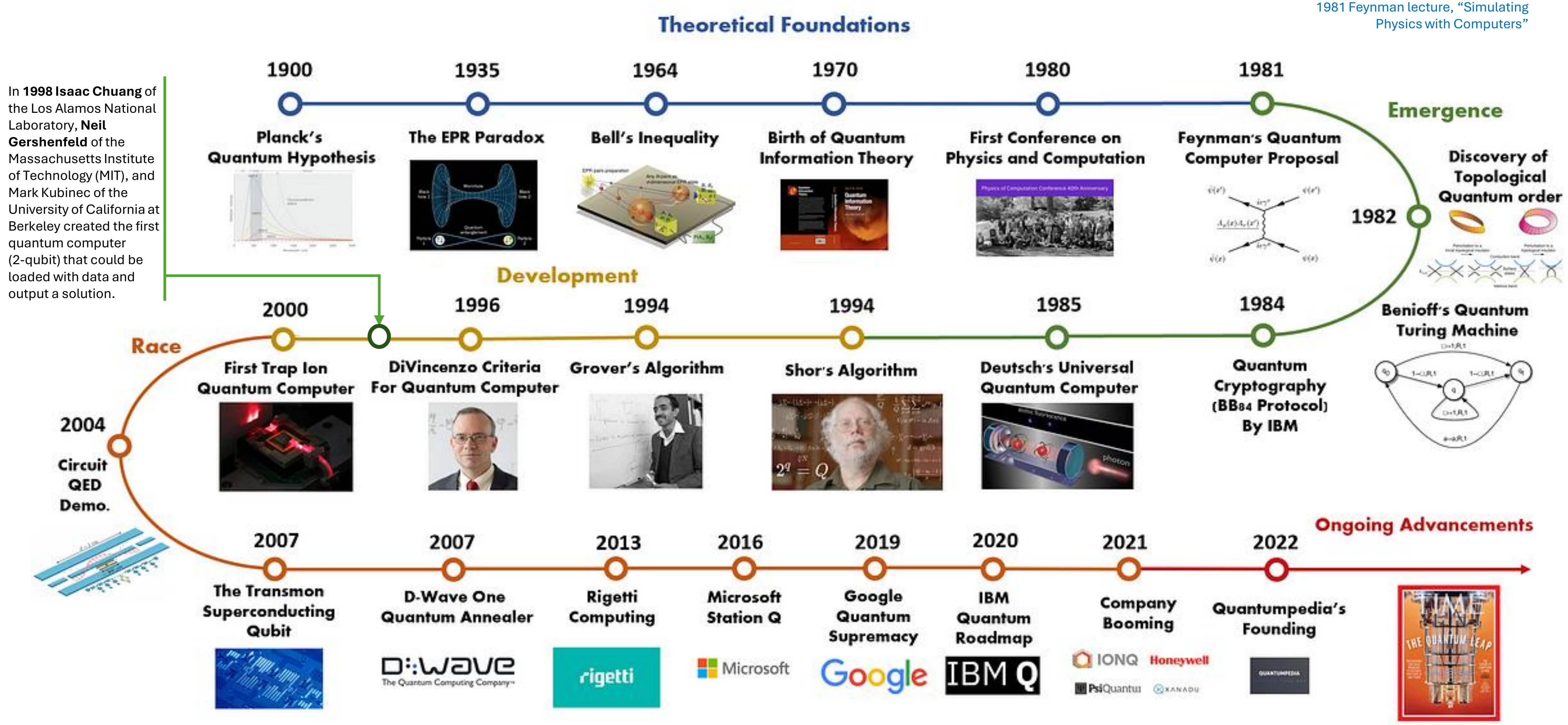
Werner Heisenberg

Paul Dirac

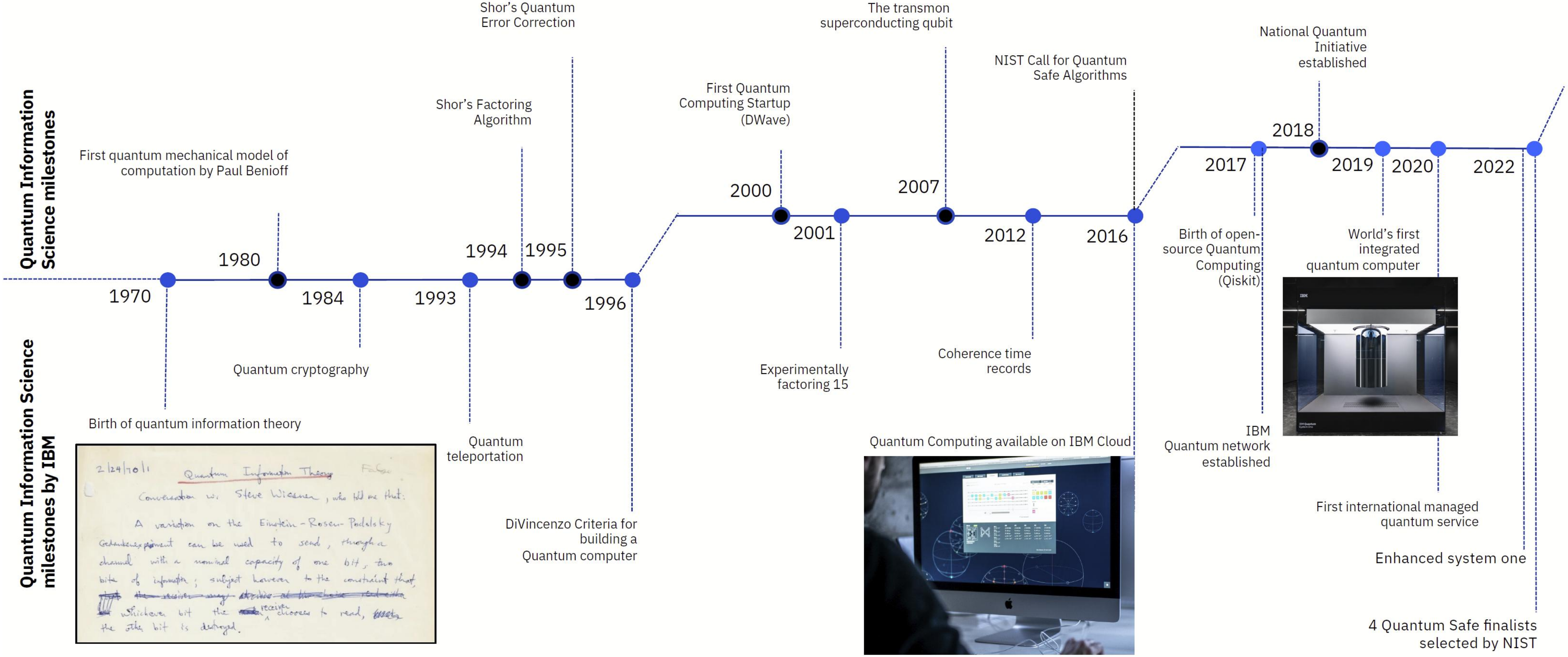
Pathway to Quantum Computers

“Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical.”

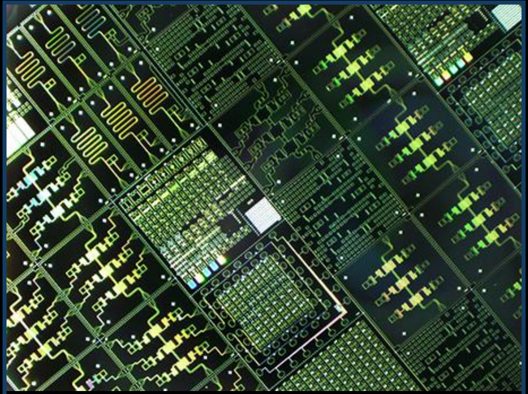
1981 Feynman lecture, “Simulating Physics with Computers”



IBM Research into Quantum Computing

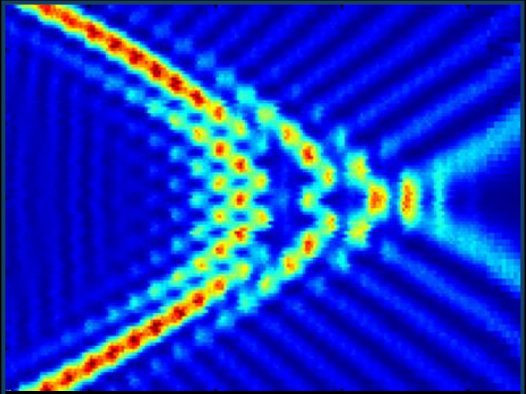


QUANTUM ENGINEERING RESEARCH



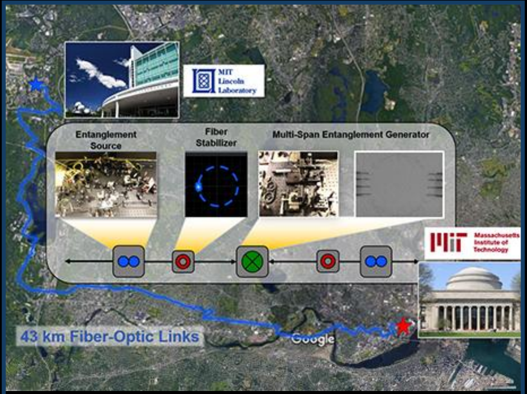
Quantum Computing

Quantum computing with superconducting qubits, trapped ions, cold atoms, NV centers, and more. Vertically integrated research efforts span hardware, control, and error mitigation methods, to software, architecture, and algorithm design. Image shows aluminum superconducting qubit circuits fabricated on a silicon wafer.



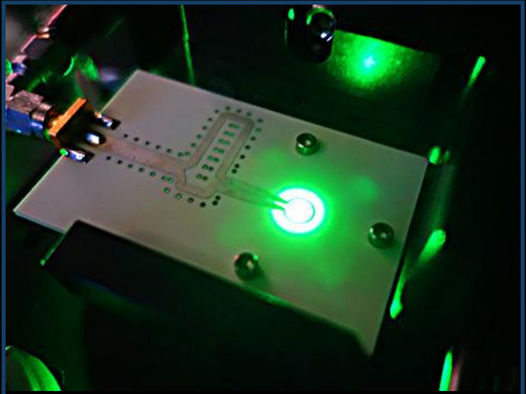
Quantum Simulation

Simulation and emulation of quantum systems using superconducting qubits, trapped ions, cold atoms, and more. The image shows the emulation of coherent backscattering and universal conductance fluctuations using a strongly driven superconducting qubit.



Quantum Networks

Quantum networking with microwave and optical photons. Image shows the quantum communication test bed link connecting MIT Lincoln Laboratory and MIT campus. The link also extends to Harvard and Raytheon BBN Technologies.

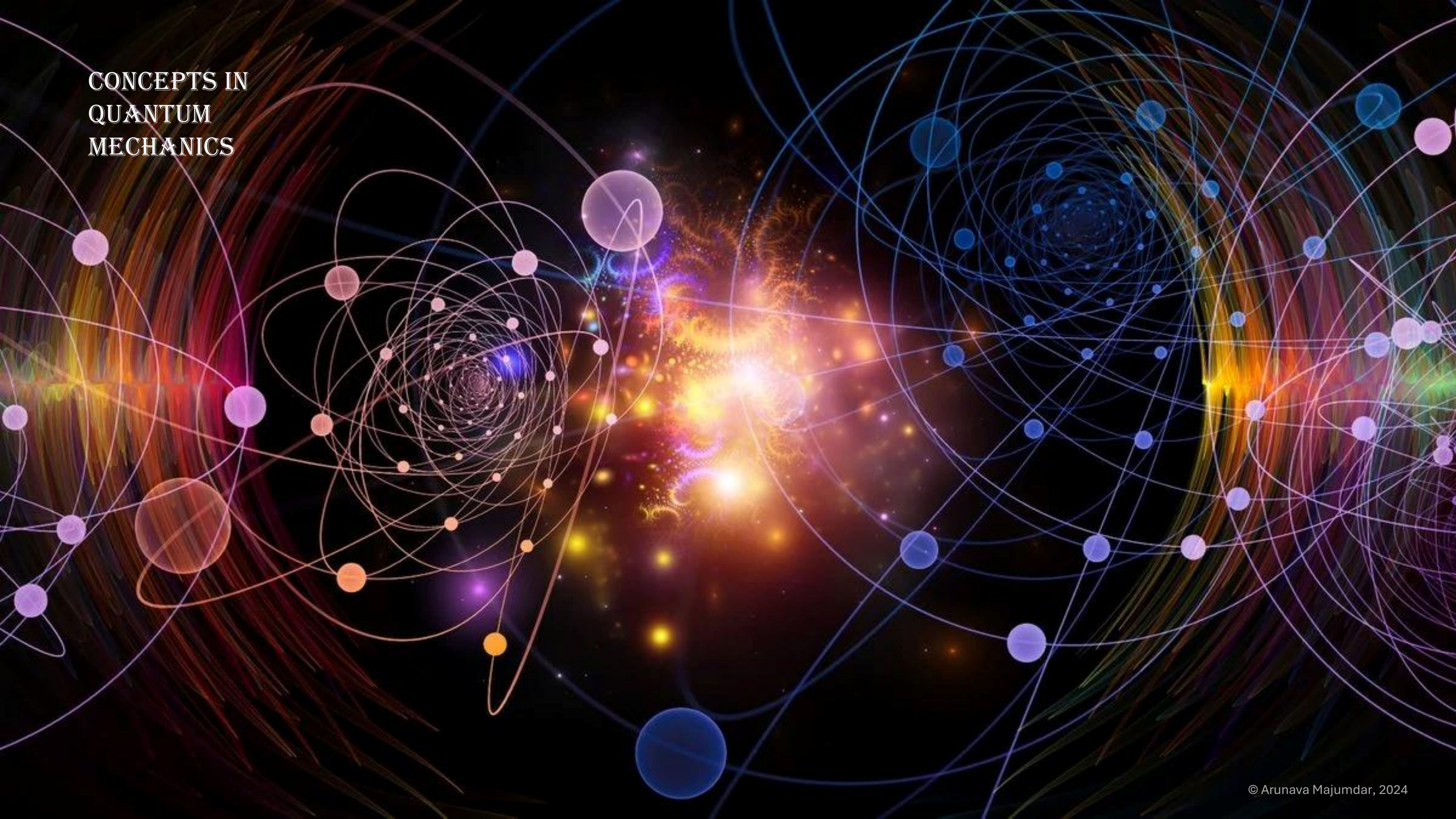


Quantum Sensing

Precision quantum sensing and metrology using cold atoms, ions, quantum defect centers, non-classical states of light, and more, with application to magnetic sensing, inertial measurement, precision clocks, microscopy, and more. Image shows nitrogen-vacancy diamond on a split-loop resonator.

Source: https://cqe.mit.edu/research/

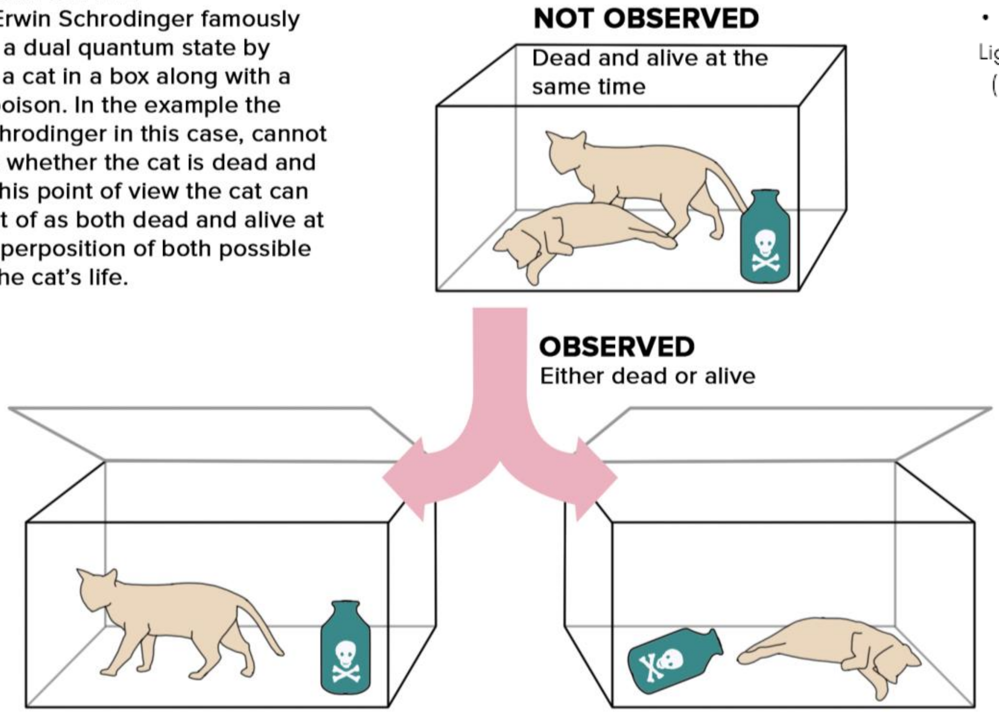
CONCEPTS IN QUANTUM MECHANICS



Superposition

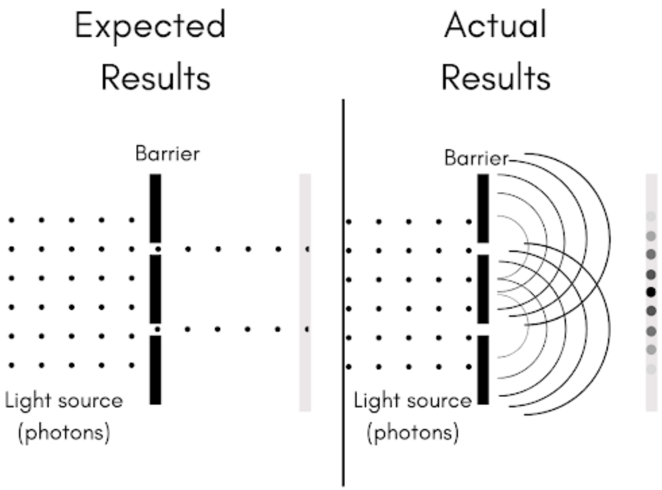
Schrodinger's Cat

QUANTUM STATE
Physicist Erwin Schrodinger famously illustrated a dual quantum state by imagining a cat in a box along with a bottle of poison. In the example the viewer, Schrodinger in this case, cannot determine whether the cat is dead and thus from his point of view the cat can be thought of as both dead and alive at once, a superposition of both possible states of the cat's life.



$$i\hbar \frac{d}{dt}|\Psi\rangle = \hat{H}|\Psi\rangle$$

Schrödinger equation



Copenhagen Interpretation of Quantum Mechanics

The Copenhagen interpretation is a collection of views about the meaning of quantum mechanics, stemming from the work of Niels Bohr, Werner Heisenberg, Max Born, and others. The idea that quantum mechanics is intrinsically indeterministic, with probabilities calculated using the Born rule, and the principle of complementarity, which states that objects have certain pairs of complementary properties that cannot all be observed or measured simultaneously Moreover, the act of "observing" or "measuring" an object is irreversible, and no truth can be attributed to an object except according to the results of its measurement.

Source: https://en.wikipedia.org/wiki/Copenhagen_interpretation

Source: https://plato.stanford.edu/entries/qm-copenhagen/

The Bohr and Einstein debate: Copenhagen Interpretation challenged

The Bohr Einstein debate on the meaning of quantum physics involved Einstein inventing a series of thought experiments to challenge the Copenhagen Interpretation of quantum physics. Einstein disliked many aspects of the Copenhagen Interpretation especially its idea of an observer dependent universe. Bohr was able to answer all Einstein's objections to the Copenhagen Interpretation and so is usually considered as winning the debate.

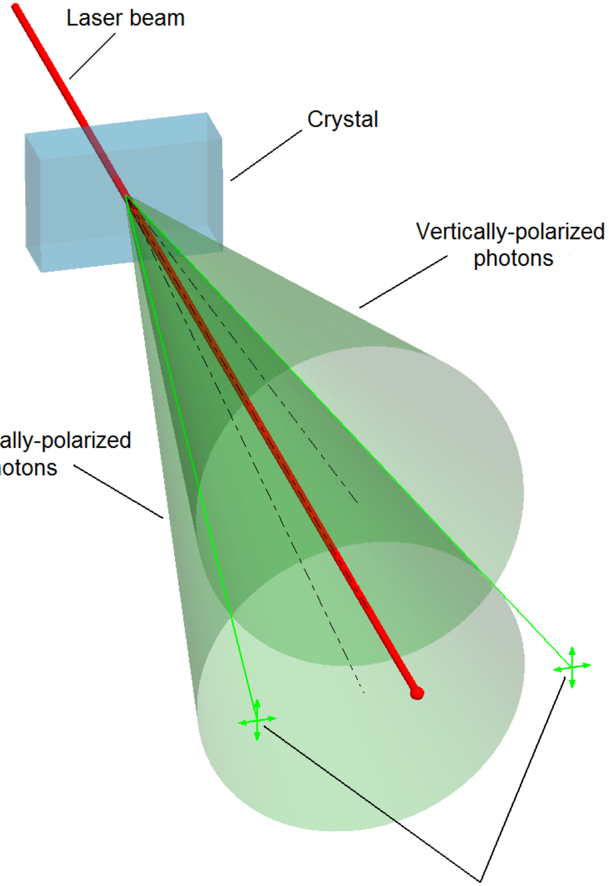
Source: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3221514

Gerard 't Hooft, Nobel Prize 1999

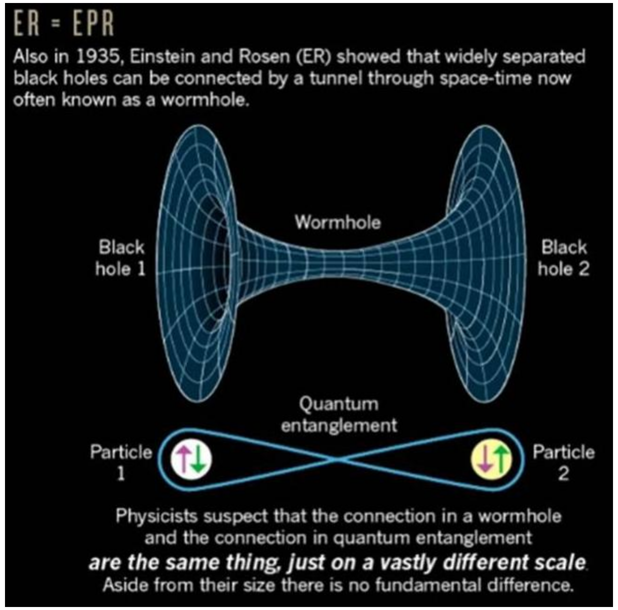
The Cellular Automaton Interpretation of Quantum Mechanics

Source: https://arxiv.org/abs/1405.1548

Entanglement



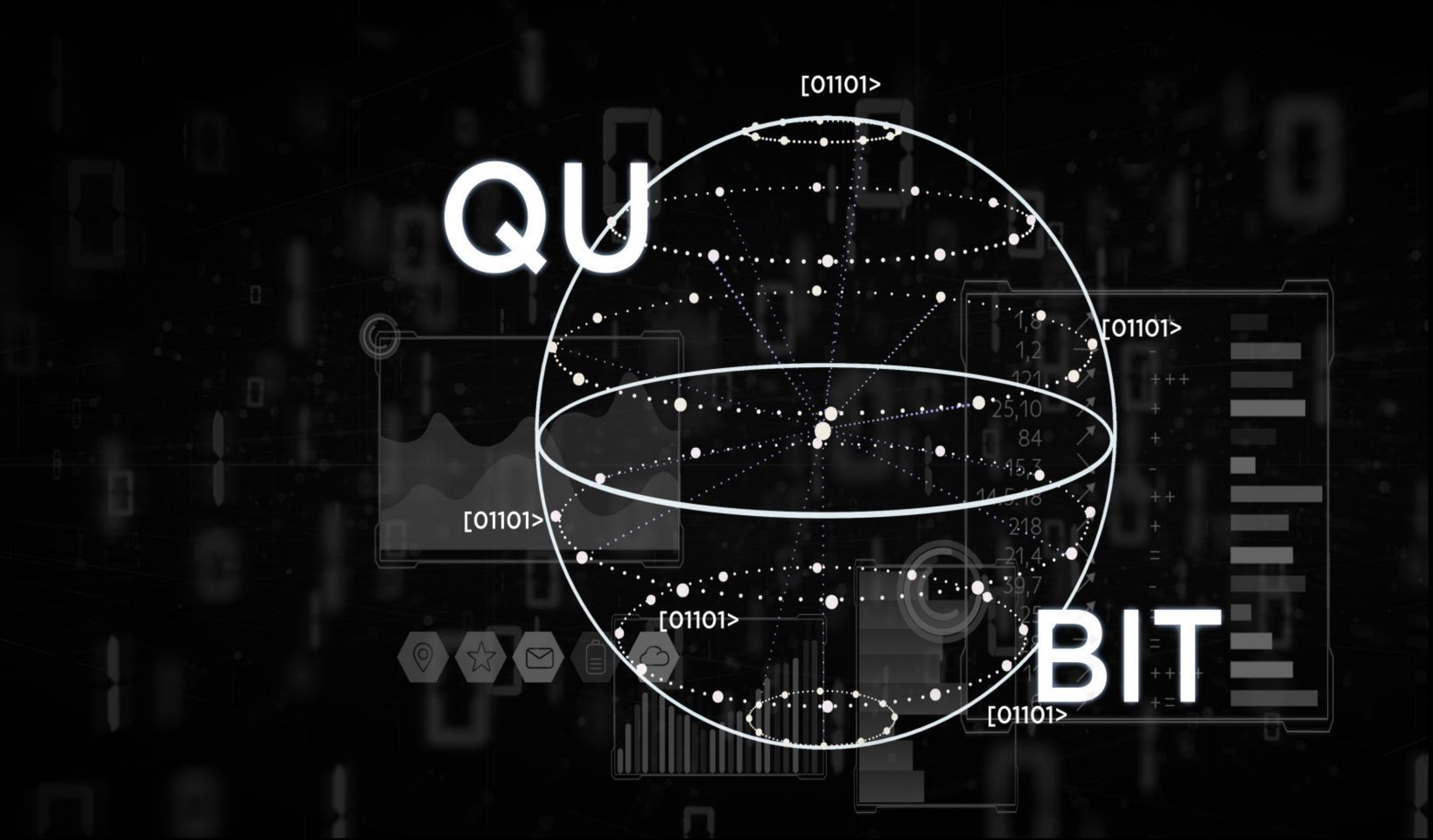
Quantum entanglement is the phenomenon of a group of particles being generated, interacting, or sharing spatial proximity in such a way that the quantum state of each particle of the group cannot be described independently of the state of the others, including when the particles are separated by a large distance. The topic of quantum entanglement is at the heart of the disparity between classical and quantum physics: entanglement is a primary feature of quantum mechanics not present in classical mechanics

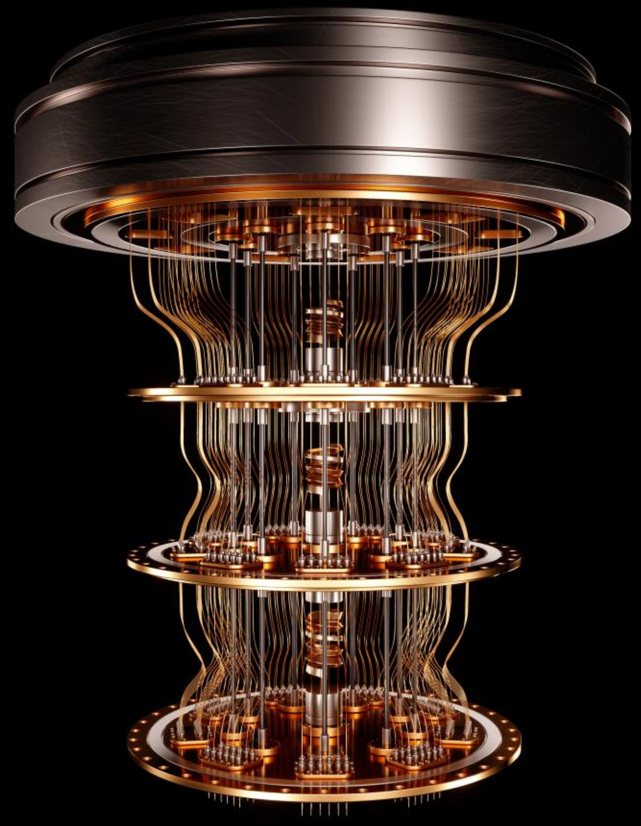


Spooky interaction at a distance

The phenomena were the subject of a 1935 paper by Albert Einstein, Boris Podolsky, and Nathan Rosen, and several papers by Erwin Schrödinger shortly thereafter, describing what came to be known as the EPR paradox. Einstein and others considered such behavior impossible, as it violated the local realism view of causality (Einstein referring to it as "spooky action at a distance") and argued that the accepted formulation of quantum mechanics must therefore be incomplete.

Einstein Podolsky Rosen





- Traditionally, a bit is either a 0 or a 1

  There are two possible values

- A Qubit can be all possible values, at the same time

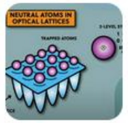
- For a bit wise value, it can be both a 0 AND a 1

Two Qubits can be 00, 01, 10, and 11- all at the same time

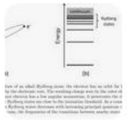
The IBM 127 Qubit system, can have 2^{127} possible bit combinations – all at the same time!

Types of quantum circuits


Superconducting qubit


Quantum dots

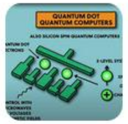

Nuclear magnetic resona...


Atomic qubits


Photonic qubits

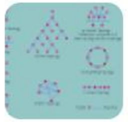

Neutral atoms


Photons


Optical quantum comput...


Trapped ions

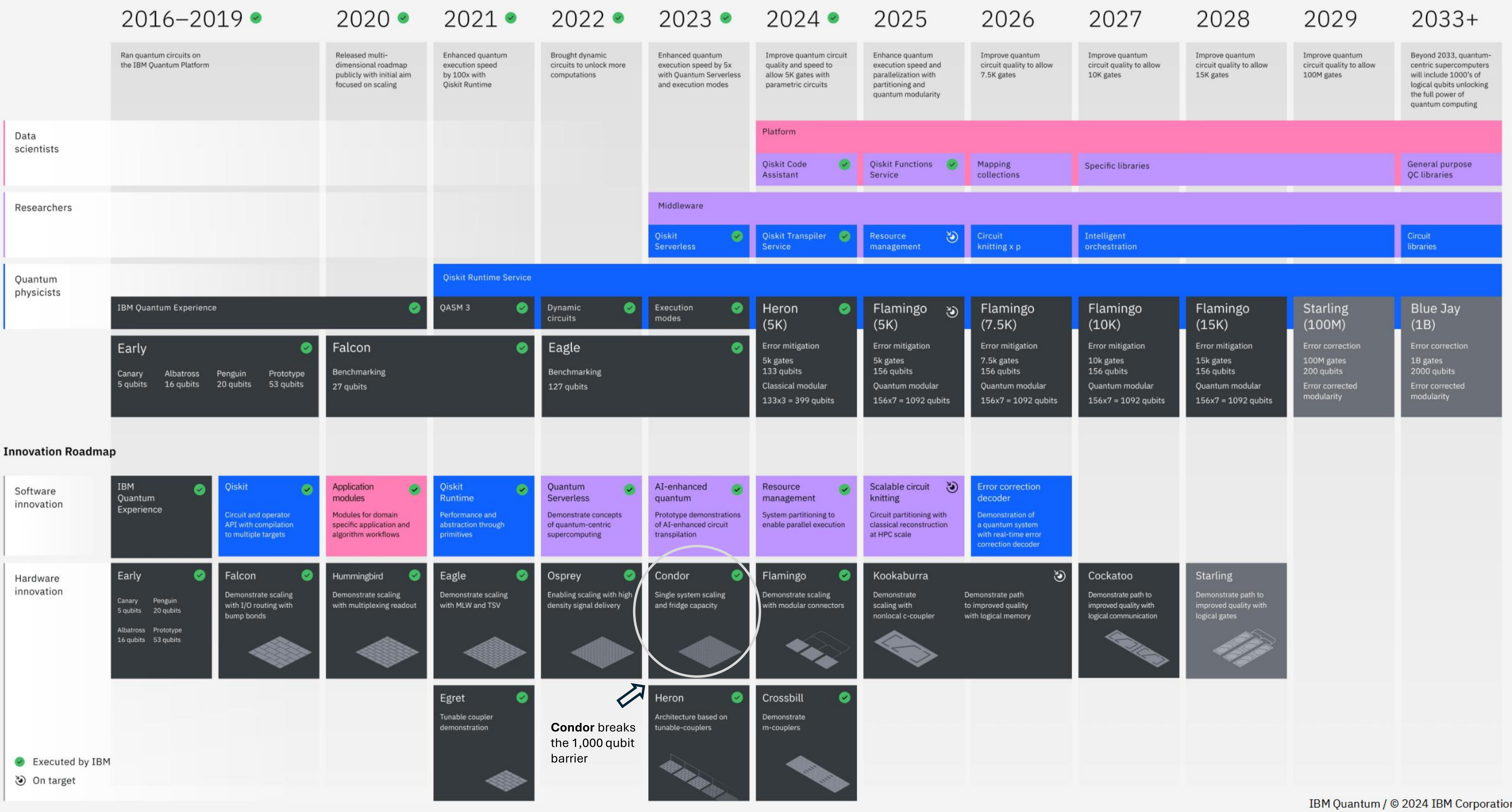

Photonics


Topological qubits


Silicon based qubits

A **superconducting qubit** is a quantum bit (or qubit) that utilizes the properties of superconductivity to store quantum information, essentially acting as a tiny circuit made from superconducting materials where the quantum state is controlled by manipulating electrical currents with minimal resistance, allowing for **superposition** and **entanglement** states crucial for quantum computing; they are often considered the most common type of qubit used in current quantum computing systems.

Josephson junction:
A key component of a superconducting qubit is the Josephson junction, which allows for controlled flow of supercurrent without resistance, enabling manipulation of the qubit's quantum state.

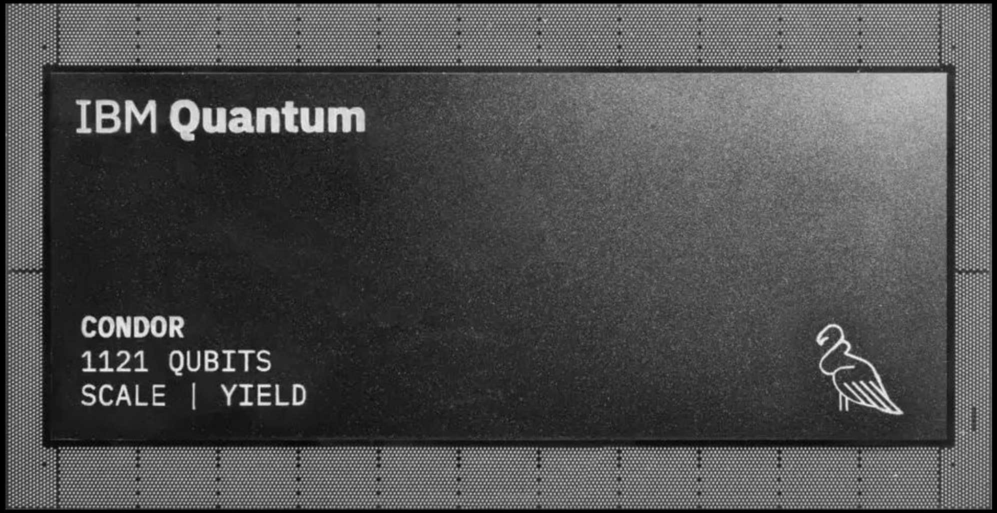

2016–2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2033+
Ran quantum circuits on the IBM Quantum Platform
Released multi-dimensional roadmap publicly with initial aim focused on scaling
Enhanced quantum execution speed by 100x with Qiskit Runtime
Brought dynamic circuits to unlock more computations
Enhanced quantum execution speed by 5x with Quantum Serverless and execution modes
Improve quantum circuit quality and speed to allow 5K gates with parametric circuits
Enhance quantum execution speed and parallelization with partitioning and quantum modularity
Improve quantum circuit quality to allow 7.5K gates
Improve quantum circuit quality to allow 10K gates
Improve quantum circuit quality to allow 15K gates
Improve quantum circuit quality to allow 100M gates
Beyond 2033, quantum-centric supercomputers will include 1000's of logical qubits unlocking the full power of quantum computing
Data scientists
Platform
Qiskit Code Assistant
Qiskit Functions Service
Mapping collections
Specific libraries
General purpose QC libraries
Researchers
Middleware
Qiskit Serverless
Qiskit Transpiler Service
Resource management
Circuit knitting x p
Intelligent orchestration
Circuit libraries
Quantum physicists
Qiskit Runtime Service
IBM Quantum Experience
QASM 3
Dynamic circuits
Execution modes
Heron (5K)
Error mitigation
5k gates
133 qubits
Classical modular
133x3 = 399 qubits
Flamingo (5K)
Error mitigation
5k gates
156 qubits
Quantum modular
156x7 = 1092 qubits
Flamingo (7.5K)
Error mitigation
7.5k gates
156 qubits
Quantum modular
156x7 = 1092 qubits
Flamingo (10K)
Error mitigation
10k gates
156 qubits
Quantum modular
156x7 = 1092 qubits
Flamingo (15K)
Error mitigation
15k gates
156 qubits
Quantum modular
156x7 = 1092 qubits
Starling (100M)
Error correction
100M gates
200 qubits
Error corrected modularity
Blue Jay (1B)
Error correction
1B gates
2000 qubits
Error corrected modularity
Early
Canary 5 qubits
Albatross 16 qubits
Penguin 20 qubits
Prototype 53 qubits
Falcon
Benchmarking
27 qubits
Eagle
Benchmarking
127 qubits
Innovation Roadmap
Software innovation
IBM Quantum Experience
Qiskit
Circuit and operator API with compilation to multiple targets
Application modules
Modules for domain specific application and algorithm workflows
Qiskit Runtime
Performance and abstraction through primitives
Quantum Serverless
Demonstrate concepts of quantum-centric supercomputing
AI-enhanced quantum
Prototype demonstrations of AI-enhanced circuit transpilation
Resource management
System partitioning to enable parallel execution
Scalable circuit knitting
Circuit partitioning with classical reconstruction at HPC scale
Error correction decoder
Demonstration of a quantum system with real-time error correction decoder
Hardware innovation
Early
Canary 5 qubits
Penguin 20 qubits
Albatross 16 qubits
Prototype 53 qubits
Falcon
Demonstrate scaling with I/O routing with bump bonds
Hummingbird
Demonstrate scaling with multiplexing readout
Eagle
Demonstrate scaling with MLW and TSV
Osprey
Enabling scaling with high density signal delivery
Condor
Single system scaling and fridge capacity
Flamingo
Demonstrate scaling with modular connectors
Kookaburra
Demonstrate scaling with nonlocal c-coupler
Demonstrate path to improved quality with logical memory
Cockatoo
Demonstrate path to improved quality with logical communication
Starling
Demonstrate path to improved quality with logical gates
Egret
Tunable coupler demonstration
Heron
Architecture based on tunable-couplers
Crossbill
Demonstrate m-couplers
Condor breaks the 1,000 qubit barrier
Executed by IBM
On target

At IBM Quantum Summit 2023, IBM Quantum System Two was debuted as the company's first modular quantum computer and cornerstone of IBM's quantum-centric supercomputing architecture. (Credit: Ryan Lavine for IBM)

Source: https://newsroom.ibm.com/2023-12-04-IBM-Debuts-Next-Generation-Quantum-Processor-IBM-Quantum-System-Two,-Extends-Roadmap-to-Advance-Era-of-Quantum-Utility

IBM Quantum Summit 2023

IBM Quantum Heron features 133 fixed-frequency qubits with tunable couplers, yielding a 3-5x improvement in device performance over our previous flagship 127-qubit Eagle processors, and virtually eliminates cross-talk.

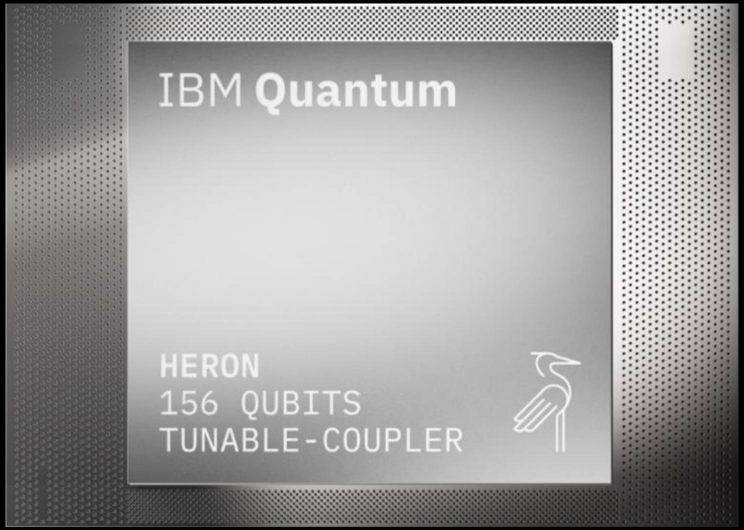


IBM Condor is a 1,121-qubit quantum processor created by IBM, unveiled during the IBM Quantum Summit 2023, which occurred on December 4, 2023. It is the 2nd largest quantum processor (in terms of qubits), just shy of the 1,125-qubit quantum processor by the company Atom, created in October 2023. It has a similar performance to its predecessor, the IBM Osprey. It has a 50% increase in qubit density compared to the IBM Osprey, and over a mile of high-density cryogenic flex IO wiring.

Absolute zero is the lowest limit of the thermodynamic temperature scale; a state at which the enthalpy and entropy of a cooled ideal gas reach their minimum value. The fundamental particles of nature have minimum vibrational motion, retaining only quantum mechanical, zero-point energy-induced particle motion. The theoretical temperature is determined by extrapolating the ideal gas law; by international agreement, absolute zero is taken as 0 kelvin (International System of Units), which is −273.15 degrees on the Celsius scale, and equals −459.67 degrees on the Fahrenheit scale (United States customary units or imperial units). The Kelvin and Rankine temperature scales set their zero points at absolute zero by definition.

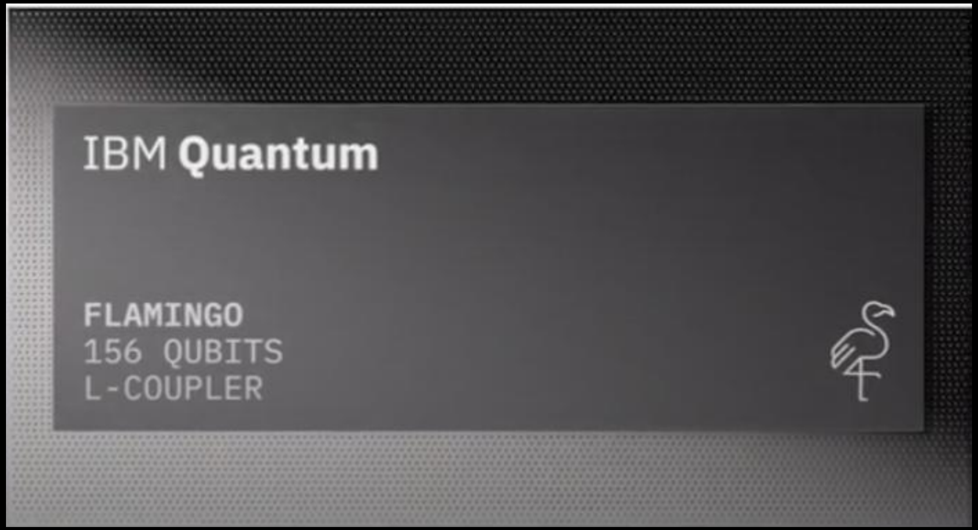
IBM Condor quantum computer is extremely low, near absolute zero, specifically around 10-20 millikelvins (mK), which translates to roughly -273.13°C (-459.6°F). This is because the superconducting qubits used in IBM's quantum processors require such frigid temperatures to function properly.

IBM Quantum Developer Conference 2024



156-qubit quantum processing unit (QPU) called **R2 IBM Heron** (the second generation of a chip launched last year); and Qiskit — a collection of software tools and algorithms designed to optimize quantum computing performance.

The result is a new system that can perform tasks up to 50 times faster than previous efforts, according to benchmarking data. For reference, in IBM's 2023 quantum utility experiment, published in the journal Nature, its most powerful quantum computer at the time took 122 hours to run workloads in the benchmark. The new system, fitted with the R2 Heron QPU, took just 2.4 hours.



IBM's Flamingo is a quantum processor system that will be made up of multiple chips and processors. The goal of the Flamingo system is to scale quantum systems while maintaining performance and error rates.

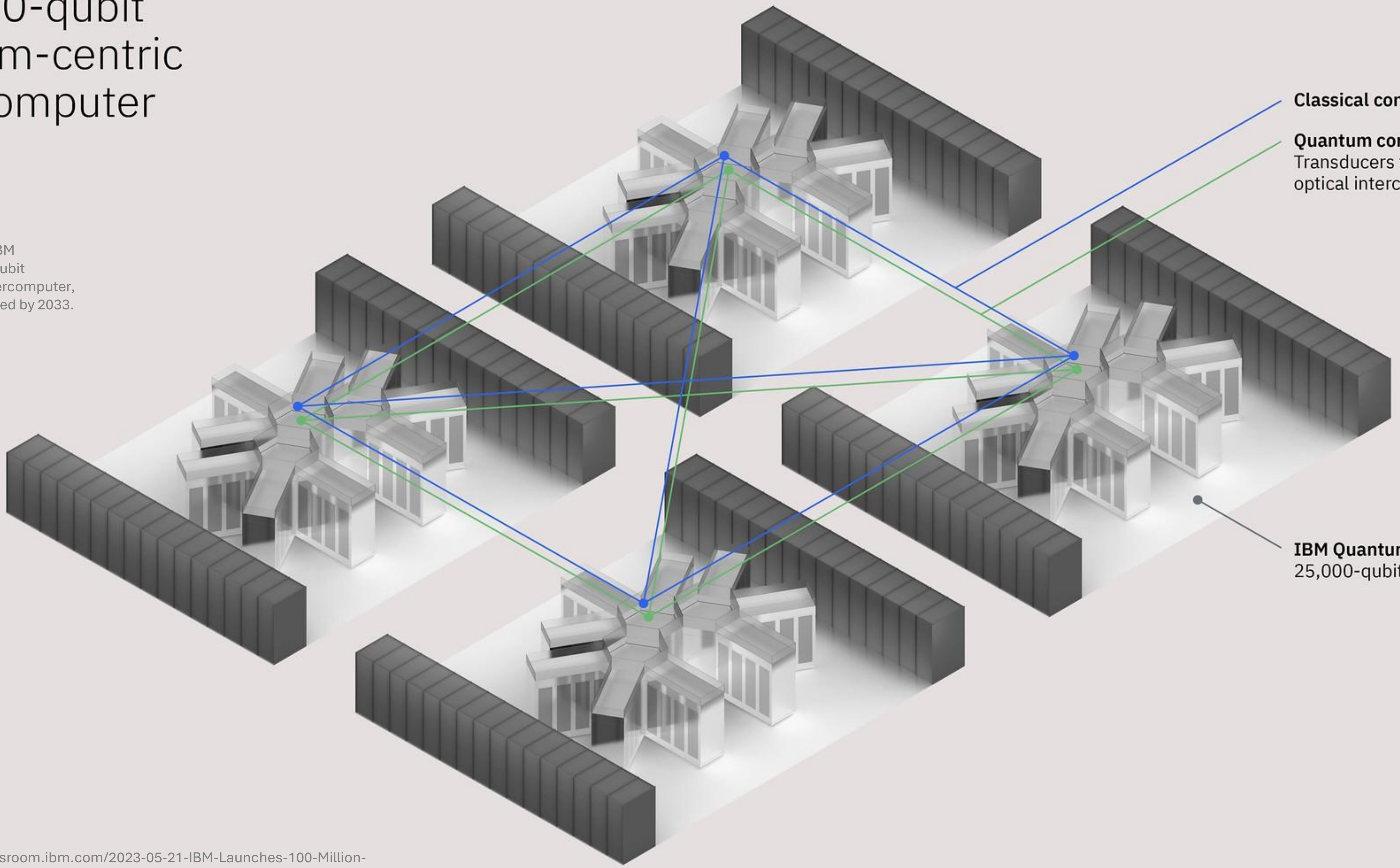
The Flamingo has 156 qubits. The number of gates will increase from 5,000 in 2024 to 15,000 in 2028. The Flamingo will eventually support cluster sizes of up to seven QPUs, totaling 1,092 qubits.

100,000-qubit quantum-centric supercomputer

—

2033

A visual rendering of IBM Quantum's 100,000-qubit quantum-centric supercomputer, expected to be deployed by 2033.



Classical connections

Quantum connections
Transducers to optical interconnects

IBM Quantum System Two
25,000-qubit cluster

Source: https://newsroom.ibm.com/2023-05-21-IBM-Launches-100-Million-Partnership-with-Global-Universities-to-Develop-Novel-Technologies-Towards-a-100,000-Qubit-Quantum-Centric-Supercomputer

IBM **Quantum**

The future of computing

Algorithm accuracy depends on quantum subroutine accuracy
Quantum subroutine accuracy depends on circuit depth

All quantum algorithms depend on classical plus quantum

```
for _ in loop:
    qc,matrix,… = do_classical(param)
    A,… = SGESVD(matrix)
    job = sampler.run([qc])
    do_classical(job.result(), A, …)
    …
```

Thesis

The future of computing is mapping all problems to matrices, and/or quantum circuits

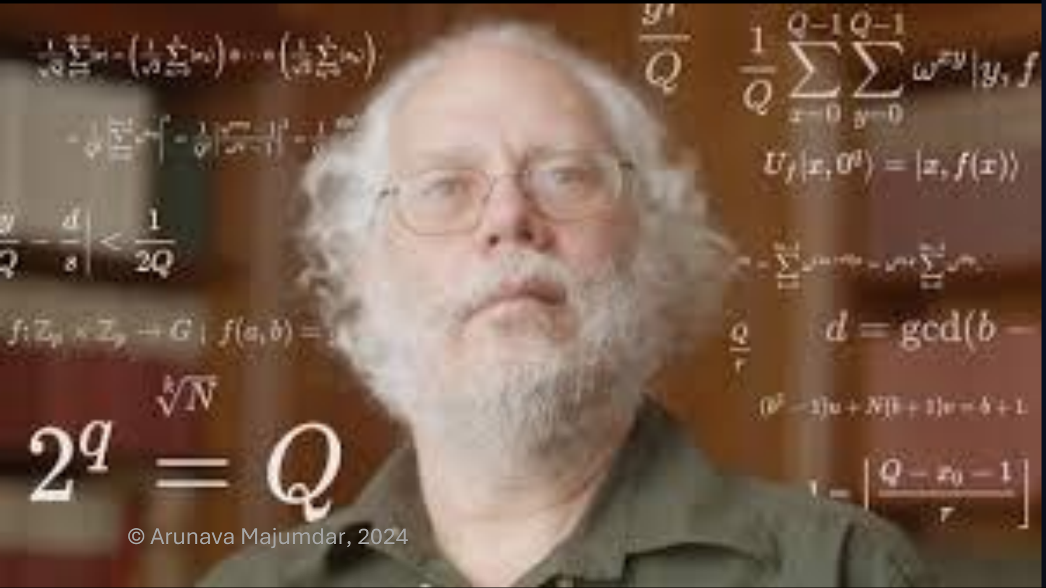
---

Quantum-centric supercomputing = CPU + GPU + QPU

Source: IBM Quantum Developer Conference 2024
https://learning.quantum.ibm.com/course/qdc2024/day-1-wednesday-nov-13

Breaking 2048 bit encryption in 8 hours…

- In 1994 Peter Shor created a quantum algorithm that efficiently solves integer factorization problems, all it needs is a powerful enough quantum computer to run it



Standards (First 3 post-quantum algorithms finalized)

- Critical to begin planning for the replacement of hardware, software, and services that use public-key algorithms now
- Be ready to adopt and implement the new algorithms at the end of the standardization process
- 5 to 15 or more years following, standardization to replace most of the vulnerable public-key systems currently in use

https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography

Bundesamt für Sicherheit in der Informationstechnik

- The protection of long-lasting secrets makes it urgent that actions be taken now or as soon as possible
- Federal Office for Information Security (BSI) is not waiting for NIST to come out with a standard to issue technical guidance
- In high security applications, hybrid schemes (use classical algorithms + quantum-safe algorithm) are required by BSI

https://www.bsi.bund.de/EN/Home/home_node.html

FIPS 186-5: Digital Signature Standard (DSS)

This standard specifies a suite of algorithms that can be used to generate a digital signature. Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation since the signatory cannot easily repudiate the signature at a later time.

NIST SP 800-56A Rev. 3 Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography

This Recommendation specifies key-establishment schemes based on the discrete logarithm problem over finite fields and elliptic curves, including several variations of Diffie-Hellman and Menezes-Qu-Vanstone (MQV) key establishment schemes.

NIST SP 800-56B Rev. 2 Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography

This Recommendation specifies key-establishment schemes using integer factorization cryptography (in particular, RSA). Both key-agreement and key transport schemes are specified for pairs of entities, and methods for key confirmation are included to provide assurance that both parties share the same keying material. In addition, the security properties associated with each scheme are provided.

FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard

A key-encapsulation mechanism (KEM) is a set of algorithms that, under certain conditions, can be used by two parties to establish a shared secret key over a public channel. A shared secret key that is securely established using a KEM can then be used with symmetric-key cryptographic algorithms to perform basic tasks in secure communications, such as encryption and authentication. This standard specifies a key-encapsulation mechanism called ML-KEM. The security of ML-KEM is related to the computational difficulty of the Module Learning with Errors problem. At present, ML-KEM is believed to be secure, even against adversaries who possess a quantum computer. This standard specifies three parameter sets for ML-KEM. In order of increasing security strength and decreasing performance, these are ML-KEM-512, ML-KEM-768, and ML-KEM-1024. The standard is based on the CRYSTALS-Kyber algorithm.

FIPS 204: Module-Lattice-Based Digital Signature Standard

Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation since the signatory cannot easily repudiate the signature at a later time. This standard specifies ML-DSA, a set of algorithms that can be used to generate and verify digital signatures. ML-DSA is believed to be secure, even against adversaries in possession of a large-scale quantum computer. The standard uses the CRYSTALS-Dilithium algorithm.

FIPS 205: Stateless Hash-Based Digital Signature Standard

This standard specifies the stateless hash-based digital signature algorithm (SLH-DSA). Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation since the signatory cannot easily repudiate the signature at a later time. SLH-DSA is based on SPHINCS+, which was selected for standardization as part of the NIST Post-Quantum Cryptography Standardization process.

Milestones on the way to Quantum-Safe Cryptography

1

Discover and classify data

- Identify locations of all data
- Classify the value of all data and identify the “Crown Jewels”
- Understand compliance requirements
- Create and manage all data inventory with defined ownership

2

Crypto inventory

- Identify how the data is encrypted
- Create a cryptography inventory (containing certificates, encryption protocols, algorithms, key lengths, etc.)
- Manage the cryptography inventory and the lifecycle of certificates, encryption keys, etc.

3

Crypto agility

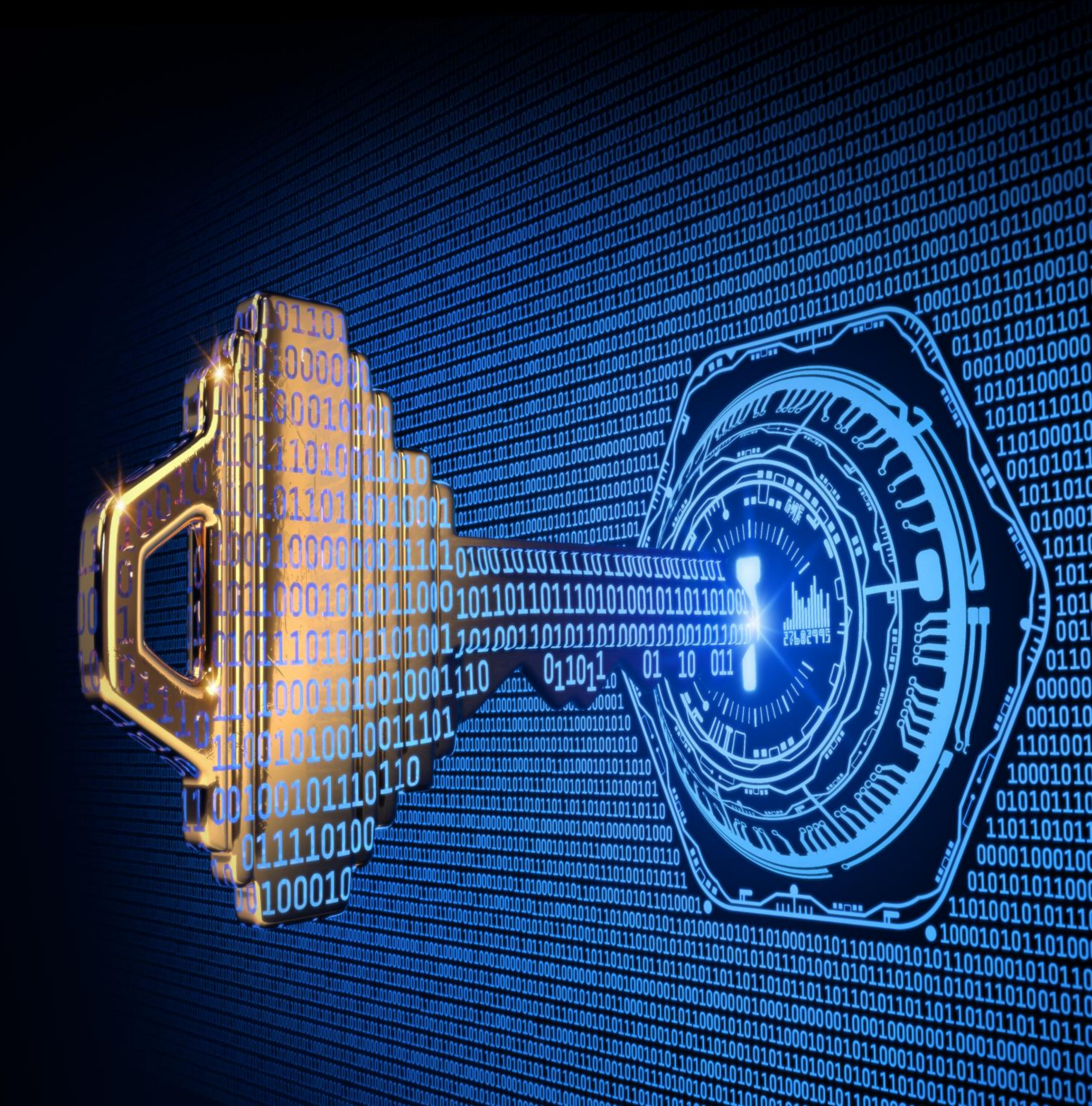
- Define and implement processes to update/replace cryptography with well defined lead-times
- Take all dimensions of crypto agility into account
- Test the crypto agility

4

Quantum-safe

- Implement quantum- safe cryptography algorithms
- Understand the performance impact of Quantum-safe crypto on the business

A quantum-safe future for everyone



IBM Power10 Security

Design, architecture, and integration

Security is architected into Power for all types of threats: traditional, new, and emerging

- Processor
- Firmware
- Hypervisors
- Management

- Network
- Operating systems
- Containers

- Applications
- Middleware
- AI

Base Platform Security & Integrity

Continuously protect platform integrity across main processor, service processor and peripherals

End to End Hybrid Cloud Security

Offer all platform capabilities with the highest level of security from enterprise through Cloud

Workload Security Enablement

Provide features to secure customer workloads: HW, firmware, and OS support for isolation, integrity, encryption, event monitoring, …

Simplified Security Management

Automated security management to simplify security operations and compliance: patching, integrity monitoring, health checking, …

IBM **Quantum** Safe Roadmap

✔ First generation available ◉ On target ○ Planned

	2022	2023	2024	2025	2026+
Regulatory milestones	NIST selects algorithms for standardization	Federal agencies plan for PQC adoption	NIST publishes PQC standards	CNSA 2.0: preference to PQC-compliant vendors	Vendors complete transition to PQC
Consortia	✔ Open Quantum Safe (OQS) ✔ Post-Quantum Telco Network	✔ NCCoE ✔ PQC Coalition (MITRE)	◉ Payments (EPAA, NACHA) ◉ PQC Alliance (Linux Foundation)	○ Critical Infrastructure Protection Coalition	
IBM services		✔ Quantum-safe preparation & advisory	◉ Application modernization ◉ Platform modernization	○ Security platform modernization	○ Quantum-safe talent transformation
IBM Quantum Safe technology: IBM Quantum Safe Remediator — *Transform*			◉ Adaptive Proxy ◉ TLS, VPN, SSH ◉ Performance benchmarking	◉ Crypto-agility framework ◉ Encryption ◉ Key/certificate management	○ Automated remediation ○ LLM-based recommendation
Quantum Safe Posture Management — *Observe*			◉ Dynamic scan ◉ Cryptographic inventory ◉ Cryptographic posture mgmt	◉ Risk-based prioritization ◉ Enriched metadata	○ AI-driven risk analysis
IBM Quantum Safe Explorer — *Discover*		✔ Static scan ✔ CBOM generation ✔ CI/CD integration	◉ Custom library support ◉ Remediation recommendation	○ LLM-assisted scanning	
Algorithms, protocols, standards, libraries	✔ Key encryption: CRYSTALS - Kyber ✔ Digital signature: CRYSTALS - Dilithium, FALCON	✔ Cryptography Bill of Materials (CBOM)	◉ MAYO, UOV, SQISign ◉ OpenSSL		
IBM infrastructure		✔ IBM z16, IBM Hyper Protect Crypto Services, IBM Tape Storage, Hardware Security Modules (HSM)	◉ IBM Cloud, IBM Software, Red Hat, IBM Storage, IBM Power		

IBM Guardium Quantum Safe

https://www.ibm.com/quantum/quantum-safe

LEADERS IN QUANTUM COMPUTING

1 IBM

IBM, the current leader in quantum computing, last year launched its Quantum System Two, a modular quantum computer powered by an IBM-made chip called the Heron. The chip improves “error correction,” combatting decoherence, a phenomenon that leads to the loss of quantum states in a quantum system. More recently, IBM unveiled Condor, a 1,121 superconducting qubit quantum processor based on the company's cross-resonance gate technology. IBM hopes to produce a 100,000 quibit quantum system by 2033.

2 Google AI Quantum

Google Quantum AI announced in 2019 that it had achieved “quantum supremacy,” with its quantum computer, Sycamore, by sampling the output of a random quantum circuit faster than it claimed a supercomputer could do. (IBM quickly countered that its supercomputers could do the task faster.) Google aims to build a quantum system with 1 million qubits within a decade. Google Quantum AI’s open-source framework, Cirq, meanwhile, is designed to develop novel quantum algorithms for near-term quantum computers.

3 aws

In 2019, Amazon Web Services established a center for quantum computing on a campus at Caltech, where Richard Feynman first proposed the idea of building a quantum computer in the early 1980s. It’s Amazon Braket is a fully-managed quantum computing service that provides access to quantum hardware from various vendors, including IonQ, Rigetti, Oxford Quantum Circuits, QuEra, and its own Amazon Braket Quantum Simulator. This allows users to experiment with different hardware architectures and find the best fit for their specific needs. Recently, AWS unveiled a custom-designed chip fabricated in house that can suppress errors by a factor of 100 using a passive error correction approach.

4 Azure Quantum

Microsoft Azure provides a comprehensive set of tools and resources for quantum computing, and is actively working on developing a scalable and fault-tolerant quantum computer. The Azure Quantum platform provides access to quantum hardware, simulators, and development tools, allowing users to experiment with quantum algorithms and explore the potential of quantum computing.

5 intel

Intel has been working towards delivering a full-stack commercial quantum system. It recently released a 12-qubit silicon chip, named Tunnel Falls, aimed at advancing silicon spin qubit research. The company plans integrate the chip into its full quantum stack with the Intel Quantum Software Development Kit. It plans to release its next-generation quantum chip in 2024 and has announced a partnership with the University of Chicago and the University of Tokyo to advance the development of a fault-tolerant quantum computer.

6 D:Wave

A leader in quantum computing systems, software, and services, D-Wave uses a process called quantum annealing and its systems are employed by some of the world's most sophisticated enterprises, including Google, NASA Ames, and Volkswagen. Quantum annealing is different from the gate-based quantum computing pursued by most other players in the space but shows promise in solving complex optimization problems at scale. The company focuses on optimization problems to deliver business value.

7 QUANTINUUM

Formed by the merger of Cambridge Quantum Computing and Honeywell Quantum Solutions, Quantinuum's H-Series trapped ion quantum computers support all-to-all qubit connectivity, allowing entangled states to be created between all qubits, and enables a high fidelity of quantum states. Quantinuum has developed middleware and software products that run on trapped-ion and other quantum computing platforms for quantum chemistry, quantum machine learning, and quantum artificial intelligence.

8 rigetti

Rigetti Computing builds and deploys integrated quantum computing systems leveraging superconducting qubit technology. It also offers a cloud platform called Forest that enables programmers to write quantum algorithms.

Source: https://www.forbes.com/sites/technology/article/top-quantum-computing-companies/

LEADERS IN QUANTUM COMPUTING…

9 XANADU

Xanadu is a full-stack photonic quantum computing company that builds quantum computers and provides quantum cloud services. The company's systems are based on photonic technology and are designed to enable the development of practical quantum applications.

10 Atos

Atos Quantum is a global leader in digital transformation. Its Quantum Learning Machine (QLM) is a powerful dedicated hardware infrastructure that enables researchers, engineers, and students to develop and experiment with quantum software.

11 IONQ

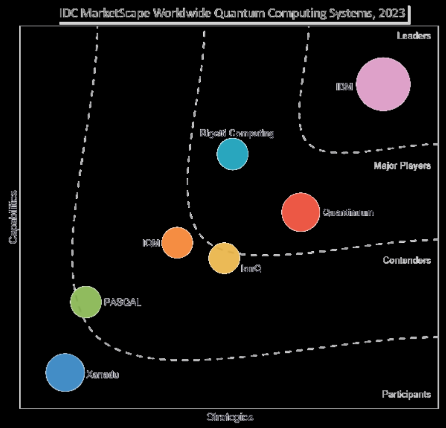
The most important part of any quantum computer are its quantum bits, or qubits. IonQ's qubits are ionized ytterbium atoms, a silvery rare-earth metal. Each ytterbium atom is perfectly identical to every other ytterbium atom in the universe.

Moreover, once prepared in a particular stable quantum state, they can remain in that state for very long periods of time — they're so consistent they're used in one of the most accurate atomic clocks ever built.

12 Infleqtion

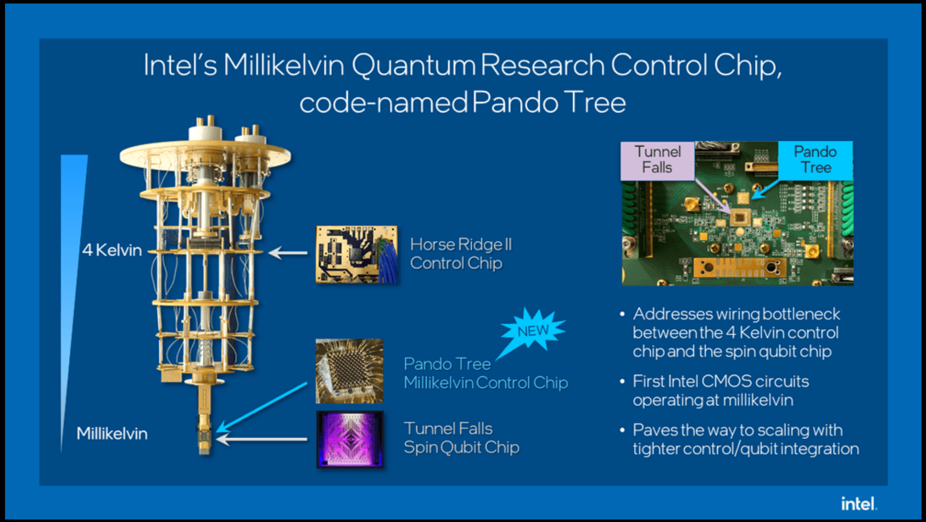
Infleqtion's approach centers on neutral atom quantum computing, a platform that enables large qubit arrays and high-fidelity gate operations. By accelerating gate fidelity and scaling to larger qubit systems, we are developing a robust framework for error correction, ensuring reliability and scalability for diverse quantum applications.

Gate Fidelity Improvement: Our advancements in gate fidelity bring us closer to a reliable error-corrected system, with a fidelity of F=0.9977 across a 1,600-site qubit array.



https://idcdocserv.com/download/US49607923e_IBM.pdf

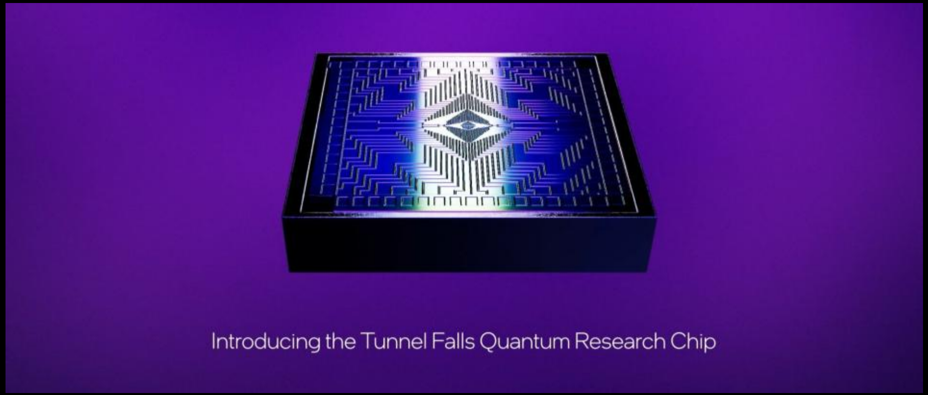
Source: https://www.forbes.com/sites/technology/article/top-quantum-computing-companies/



Intel is focused on **silicon spin qubits** that resemble single electron transistors and leverage the company's 50+ years of semiconductor manufacturing expertise. The quantum research team uses Intel's most advanced transistor fabrication capabilities including extreme ultraviolet lithography (EUV) and materials processing techniques such as standard complementary metal oxide semiconductor (CMOS) logic processing. To control these advanced devices, Intel has developed the **Horse Ridge II cryogenic** control chip. The customized control chip is based on Intel 16 technology, which operates at 4 Kelvin to control qubits.

https://www.intel.com/content/www/us/en/research/quantum-computing.html

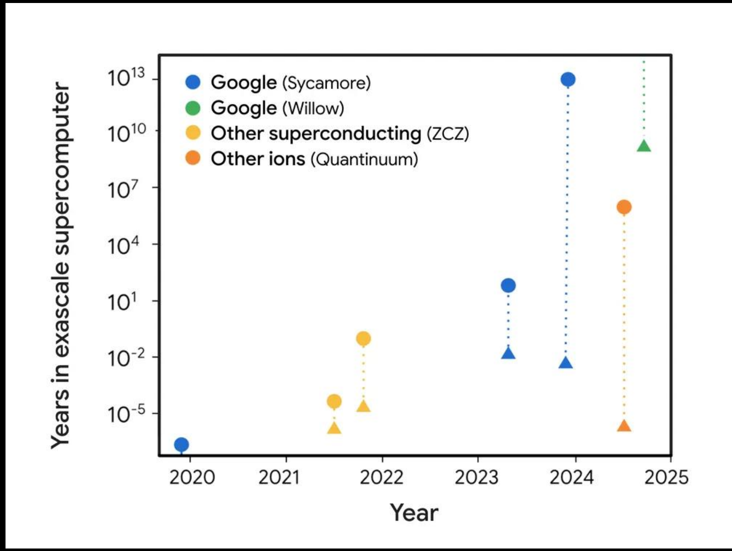
Intel has unveiled version 1.1 of its Quantum Software Development Kit (SDK). Designed to interface with Intel's quantum hardware, including the Horse Ridge II control chip and Tunnel Falls quantum dot spin qubit research chip, the SDK offers seamless integration with C/C++ and Python applications.

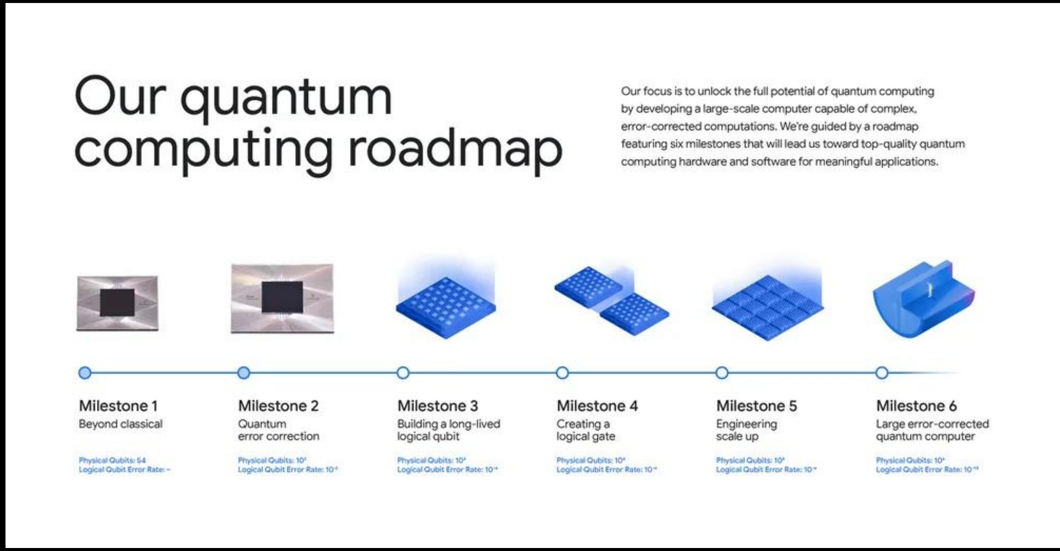


Google AI Quantum

Willow System Metrics	
Number of qubits	105
Average connectivity	3.47 (4-way typical)
Quantum Error Correction (Chip 1)	
Single-qubit gate error[1] (mean, simultaneous)	0.035% ± 0.029%
Two-qubit gate error[1] (mean, simultaneous)	0.33% ± 0.18% (CZ)
Measurement error (mean, simultaneous)	0.77% ± 0.21% (repetitive, measure qubits)
Reset options	Multi-level reset (|1⟩ state and above) Leakage removal (|2⟩ state only)
T_1 time (mean)	68 µs ± 13 µs[2]
Error correction cycles per second	909,000 (surface code cycle = 1.1 µs)
Application performance	$\Lambda_{3,5,7}$ = 2.14 ± 0.02
Random Circuit Sampling (Chip 2)	
Single-qubit gate error[1] (mean, simultaneous)	0.036% ± 0.013%
Two-qubit gate error[1] (mean, simultaneous)	0.14% ± 0.052% (swap-like)
Measurement error (mean, simultaneous)	0.67% ± 0.51% (terminal, all qubits)
Reset options	Multi-level reset (|1⟩ state and above) Leakage removal (|2⟩ state only)
T_1 time (mean)	98 µs ± 32 µs[2]
Circuit repetitions per second	63,000
Application performance	XEB fidelity depth 40 = 0.1%
Estimated time on Willow vs classical supercomputer	5 minutes vs. 10^{25} years

[1] Operation errors measured with randomized benchmarking techniques and reported as "average error"
[2] Chip 1 and 2 exhibit different T_1 due to a tradeoff between optimizing qubit geometry for electromagnetic shielding and maximizing coherence



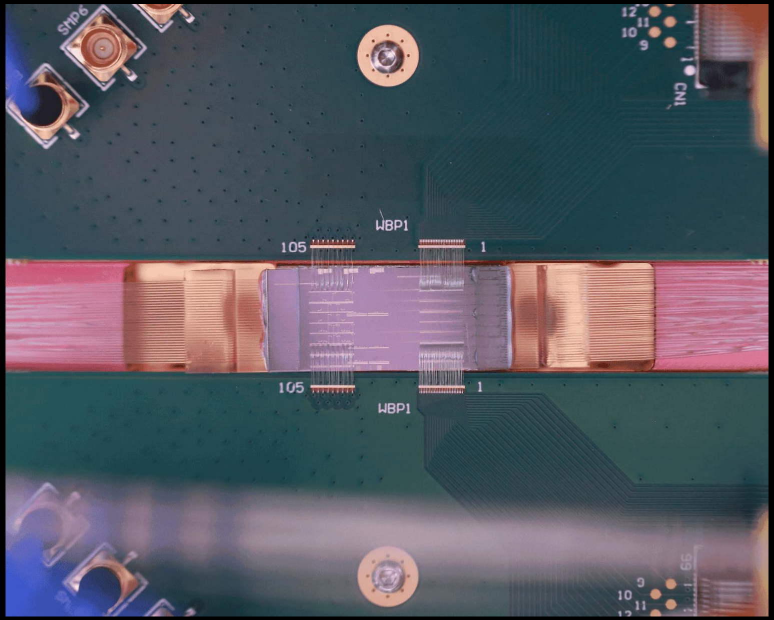


Dec 09, 2024, Nature: Google published results showing that the more qubits they use in Willow, the more they reduce errors, and the more quantum the system becomes. Google engineers tested ever-larger arrays of physical qubits, scaling up from a grid of 3x3 encoded qubits, to a grid of 5x5, to a grid of 7x7 — and each time, using their latest advances in quantum error correction, they were able to cut the error rate in half. In other words, they achieved an exponential reduction in the error rate. This historic accomplishment is known in the field as "below threshold" — being able to drive errors down while scaling up the number of qubits. You must demonstrate being below threshold to show real progress on error correction, and this has been an outstanding challenge since quantum error correction was introduced by Peter Shor in 1995.

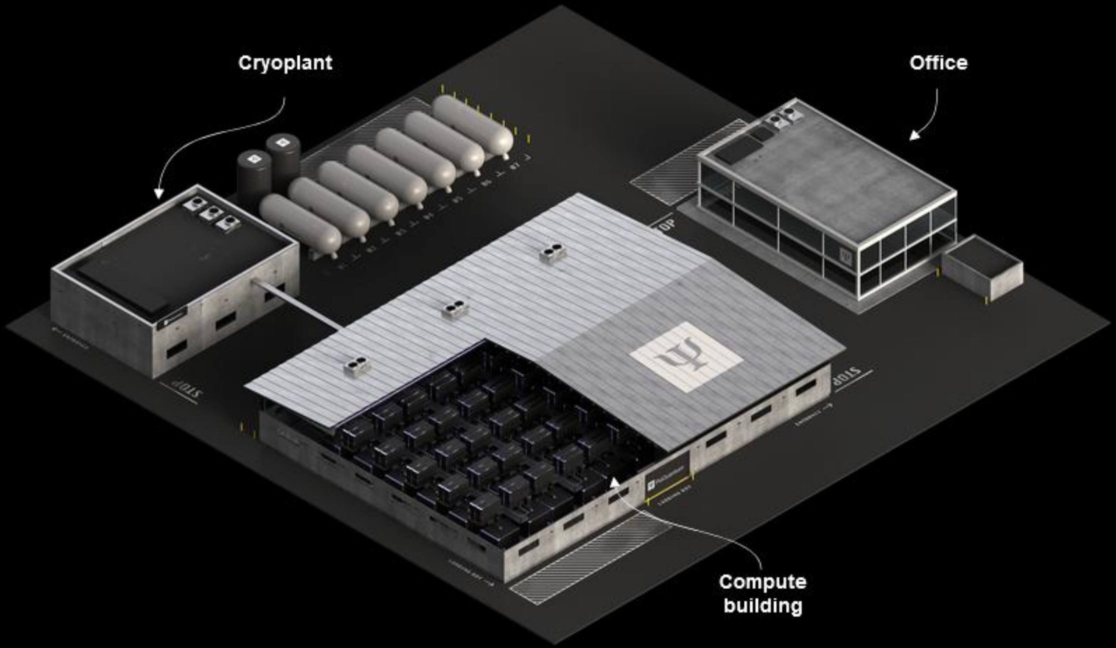
https://quantumai.google/

PsiQuantum

PsiQuantum is planning to build utility-scale, fault-tolerant quantum computer involving photonics-based architecture and it leverages existing infrastructure to build and scale these systems as fast as possible.



Photonic qubits are implemented by repurposing integrated photonics technology, originally developed for telecom and datacenter networking applications. Entangled states — specially designed to implement quantum error-correcting codes — are created and measured using fusion gates. Nondeterministic photon sources and gate operations are made scalable via a combination of multiplexing and loss-tolerant error correcting codes
~99.99% for single-qubit fidelity [5]
>99% for two-qubit fidelity [6]

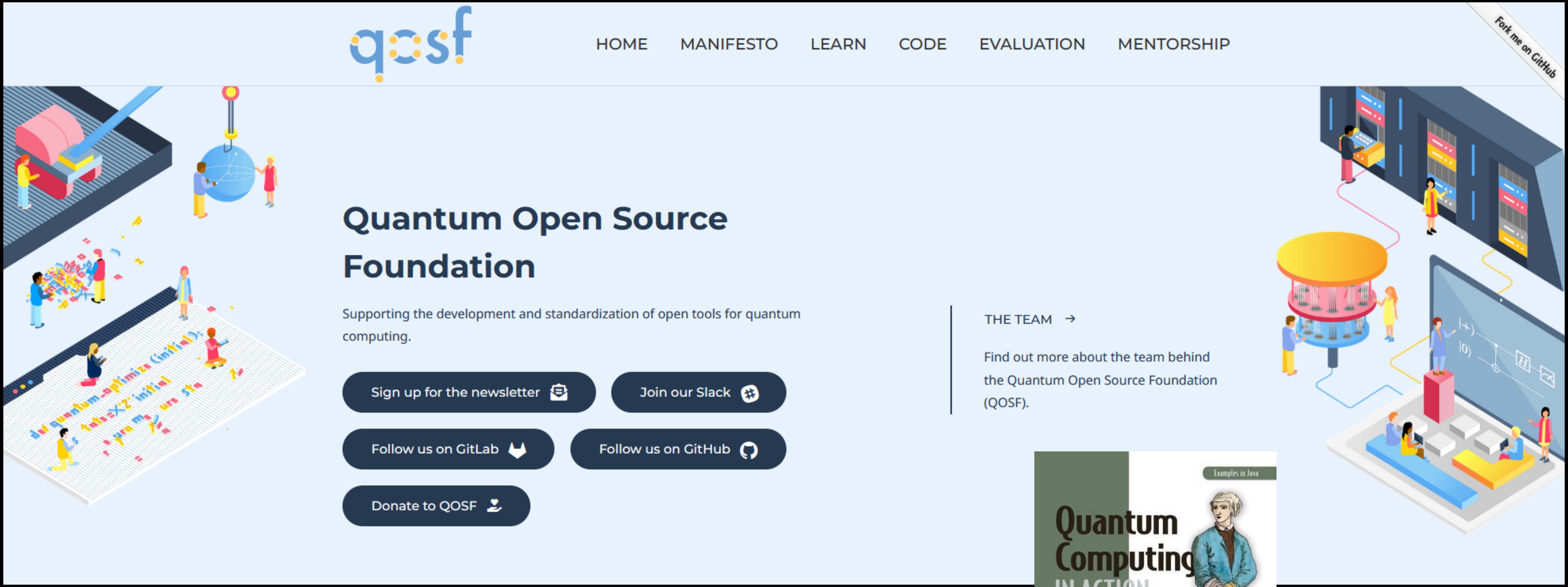


The University of Queensland Australia
Griffith University
QUT Queensland University of Technology
University of Southern Queensland
University of the Sunshine Coast Australia

Collaborations in Australia and scaling at Queensland.

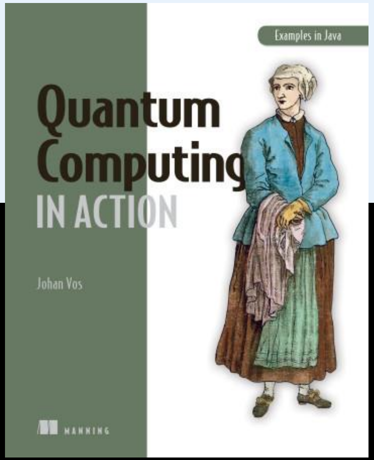
https://www.psiquantum.com/

OPEN SOURCE DEVELOPMENT IN QUANTUM COMPUTING

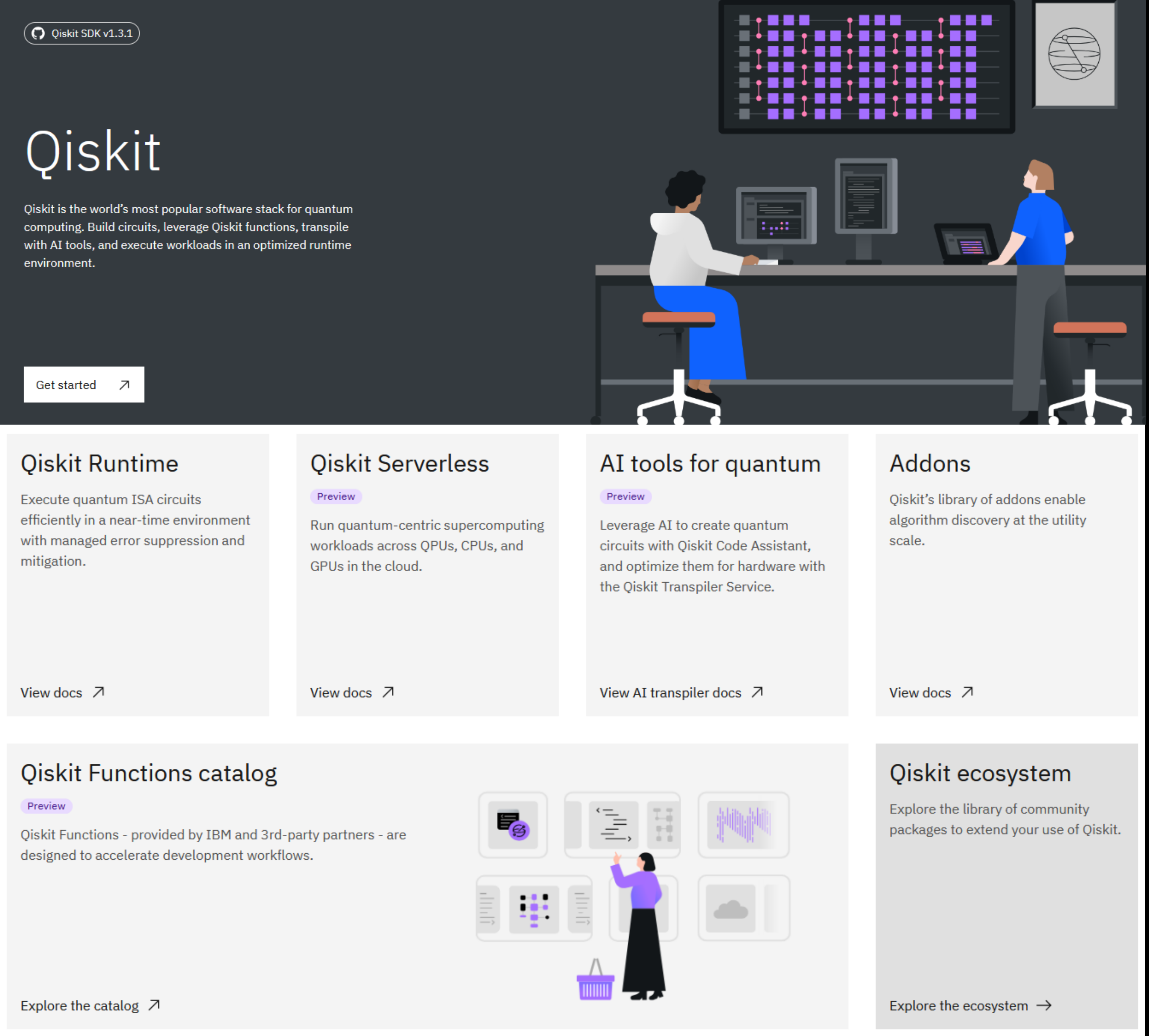


https://qosf.org/

https://github.com/qosf/awesome-quantum-software



https://github.com/johanvos/quantumjava



https://qiskit.org/

The Quantum Information Science Kit (Qiskit) first hit the ecosystem five years ago, in March 2017. It came as an answer to the need for a software development kit that could program the milestone cloud-based Quantum processors that were developed just a year before.

4 Dec 2024: Qiskit SDK v1.3 released. Qiskit's core data model re-written in Rust. C library will be introduced in 2.x

```
from qiskit.circuit.library import EfficientSU2
from qiskit_ibm_transpiler.transpiler_service import TranspilerService

circuit = EfficientSU2(101, entanglement="circular", reps=1).decompose()

cloud_transpiler_service = TranspilerService(
    backend_name="ibm_sherbrooke",
    ai='true',
    optimization_level=1,
)
transpiled_circuit = cloud_transpiler_service.run(circuit)
```

QISKIT CODE ASSISTANT CELL 0001

Introducing Qiskit Code Assistant

Qiskit Code Assistant combines the sophisticated large language models (LLMs) of IBM® watsonx™ with the collective expertise of Qiskit users all across the quantum community to help you write better Qiskit code with less effort. Its quantum code-generation capabilities serve not only to make quantum computing more accessible and efficient, but also provide users with a new, hands-on way of learning to write Qiskit code.

LATEST QUANTUM NEWS

https://www.ibm.com/quantum/blog/nature-qldpc-error-correction

Landmark IBM error correction paper published on the cover of Nature

IBM has created a quantum error-correcting code about 10 times more efficient than prior methods — a milestone in quantum computing research.

IBM and State of Illinois to Build National Quantum Algorithm Center in Chicago with Universities and Industries

Dec 12, 2024

Anchored by next-generation IBM Quantum System Two in Illinois Quantum and Microelectronics Park, new initiative will advance useful quantum applications as industries move towards quantum-centric supercomputing

"We're making Illinois the global quantum capital and the center for job growth in the quantum industry – a true center of innovation with the power to solve the world's most pressing and complex challenges and create jobs and investment for our state," said **Governor JB Pritzker.**

Gov. Pritzker Announces Location and PsiQuantum as Anchor Tenant of New Quantum Park

July 26, 2024

https://www.intersectillinois.org/illinois-quantum-park/

https://gov-pritzker-newsroom.prezly.com/gov-pritzker-announces-location-and-psiquantum-as-anchor-tenant-of-new-quantum-park