

Quantum Computing

First steps...

Didier Guillevic

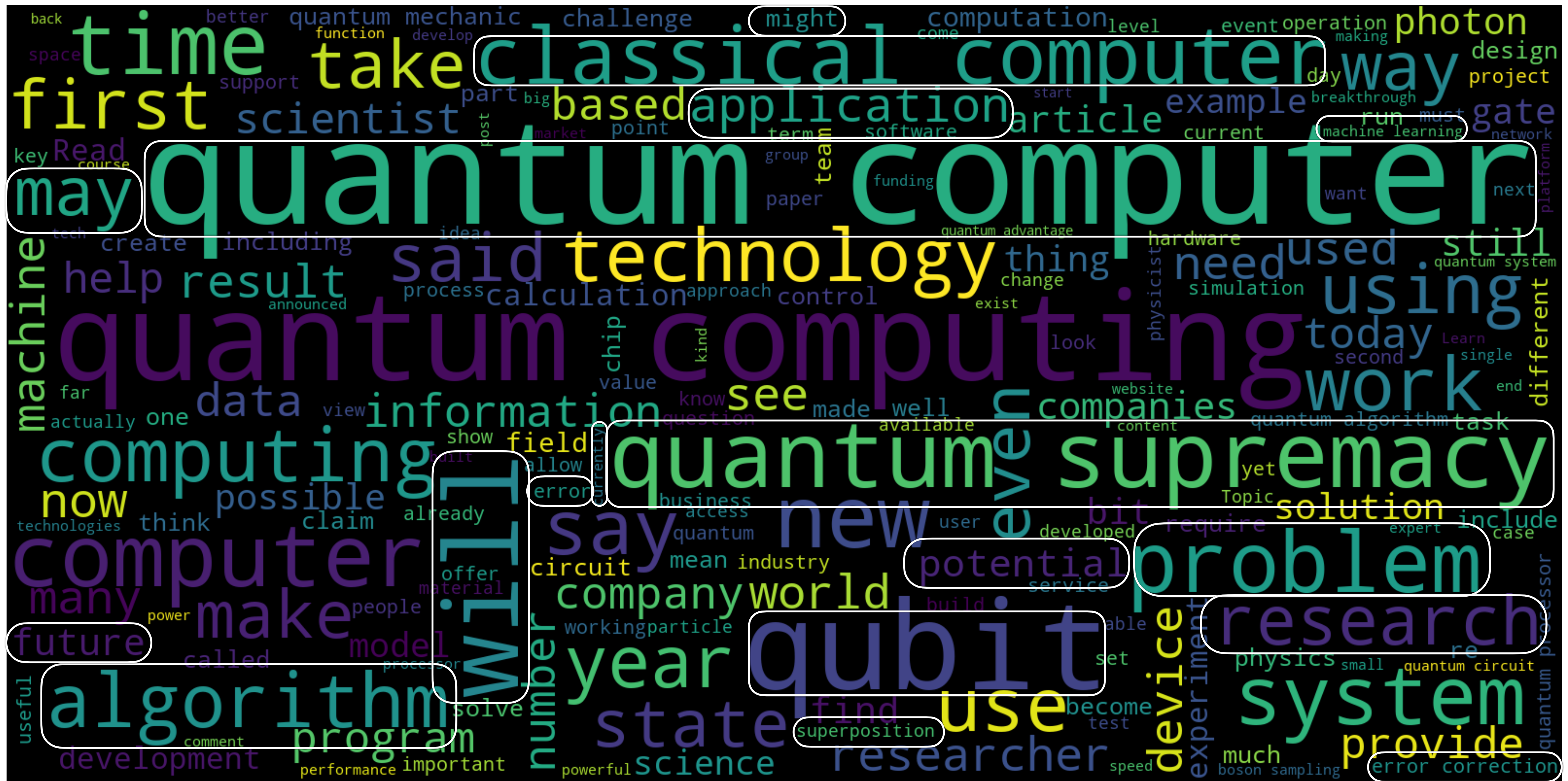
didier.guillevic.net



0. What is it ?
1. Why should we care ?
2. How does it work ?
3. What are the problems ?
4. Potential future applications
5. People / organizations involved ?
6. Coding, playing, learning...
7. Where can I learn more ?

0. What is it ?

Some potential - A lot of hype - Probable “winter”



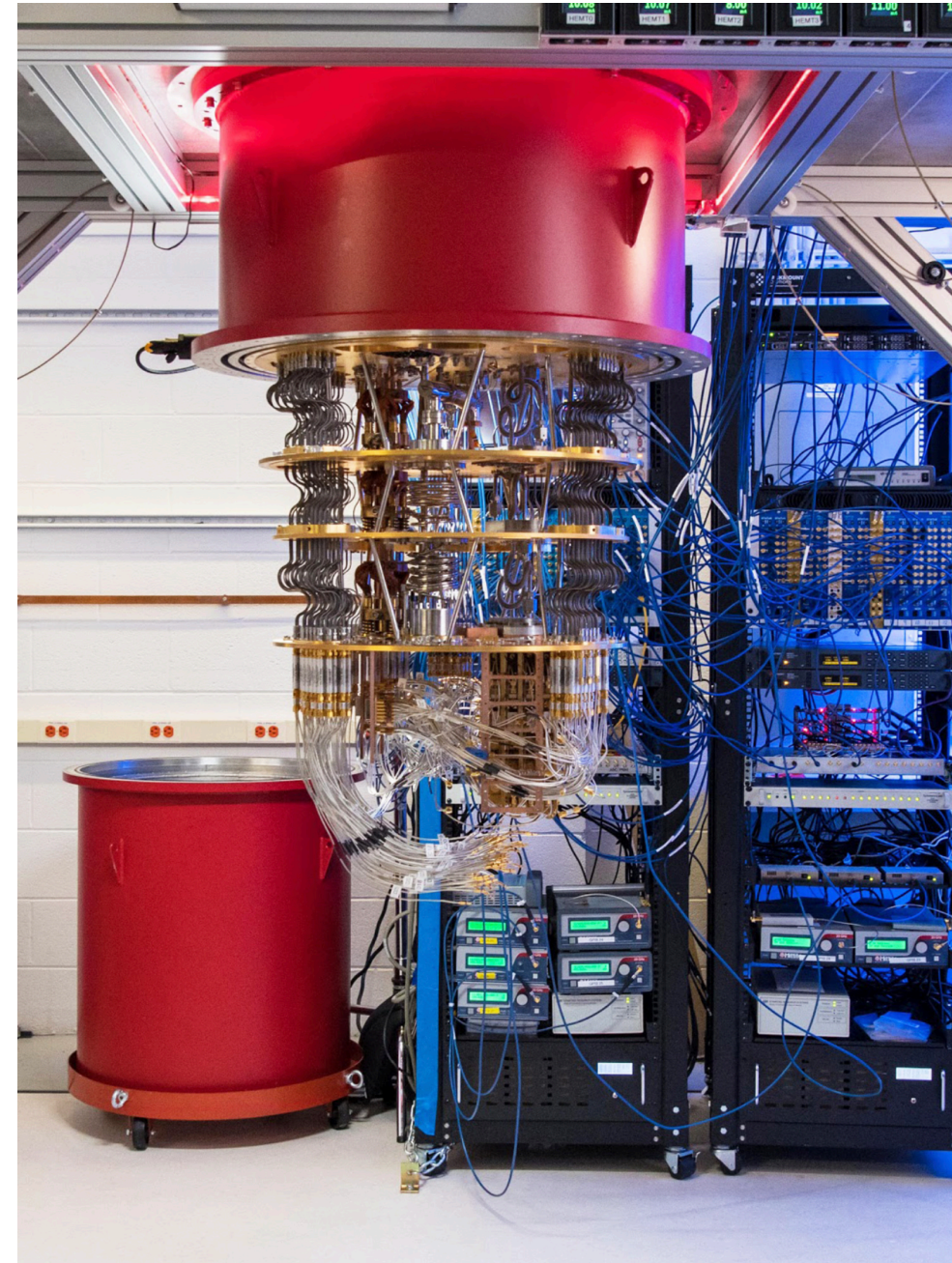
Most frequent words in a few hundred web documents mentioning Quantum Computing

Noisy Intermediate-Scale Quantum (NISQ) computer processor

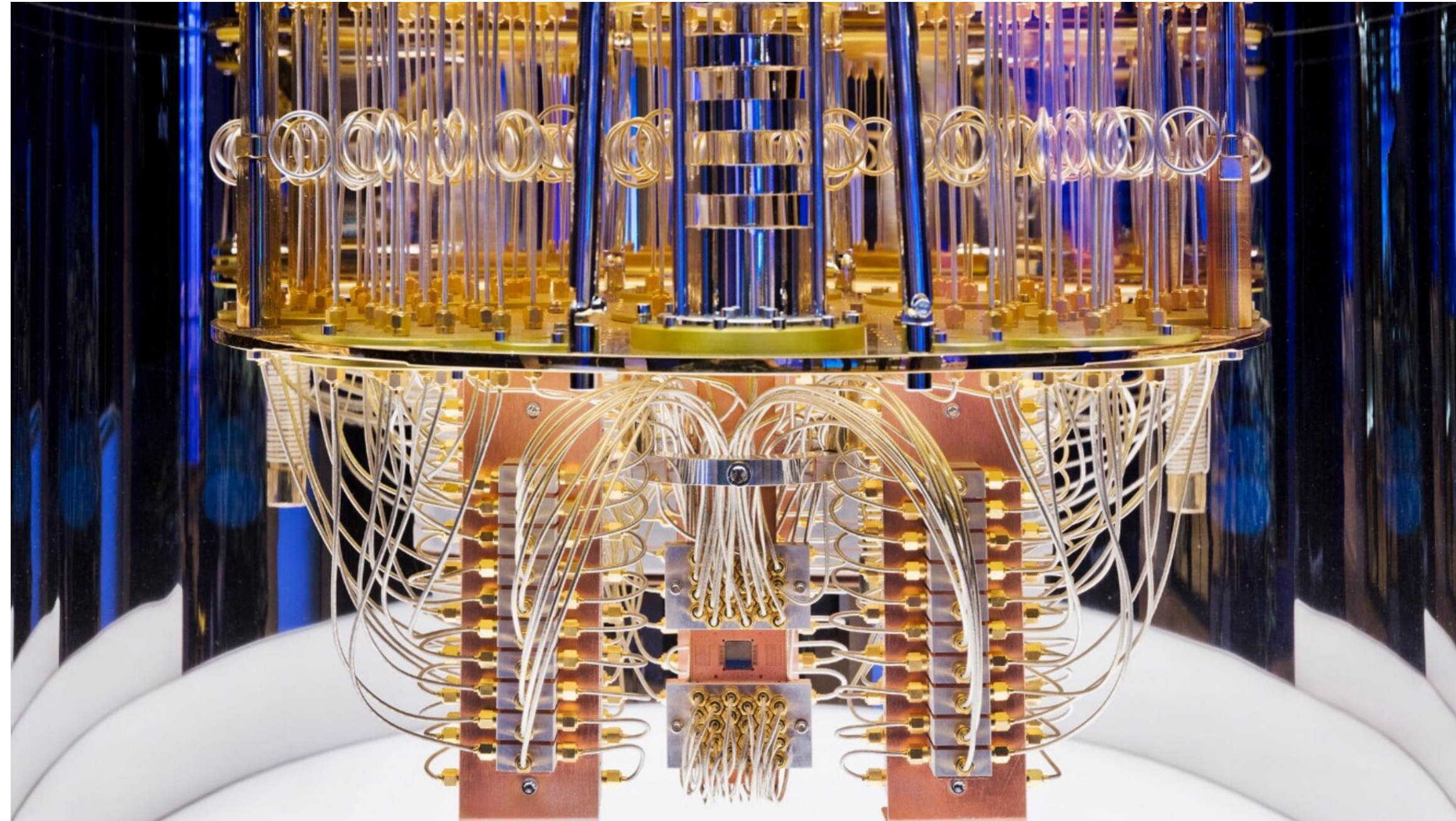
superconducting processor: operating at close to absolute 0 temperature (0 Kelvin / -273 Celsius) at which particle motion ceases



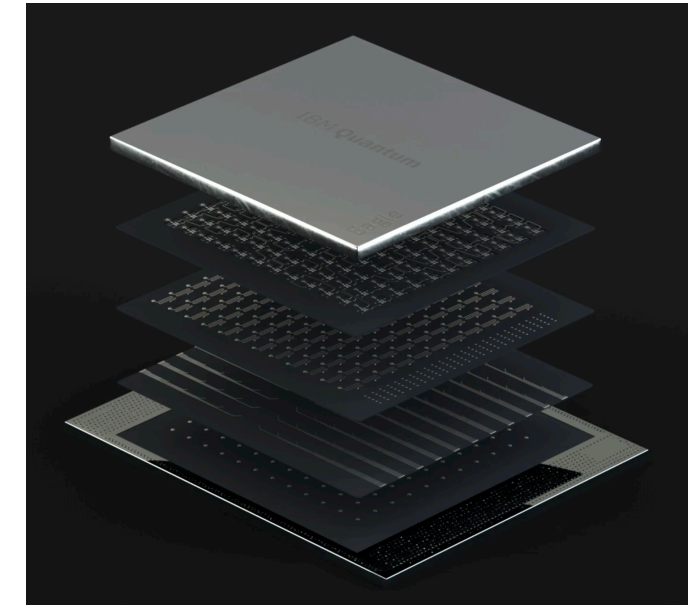
Source: IBM



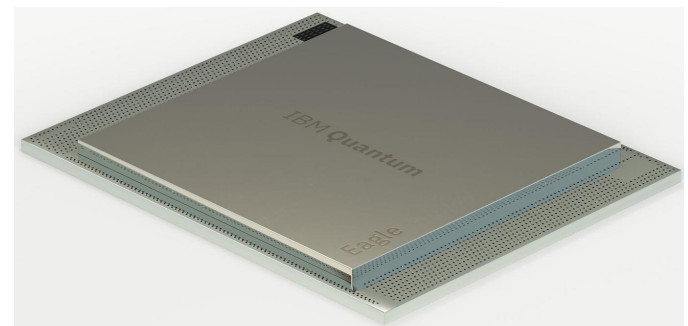
Source: Google



Source: IBM

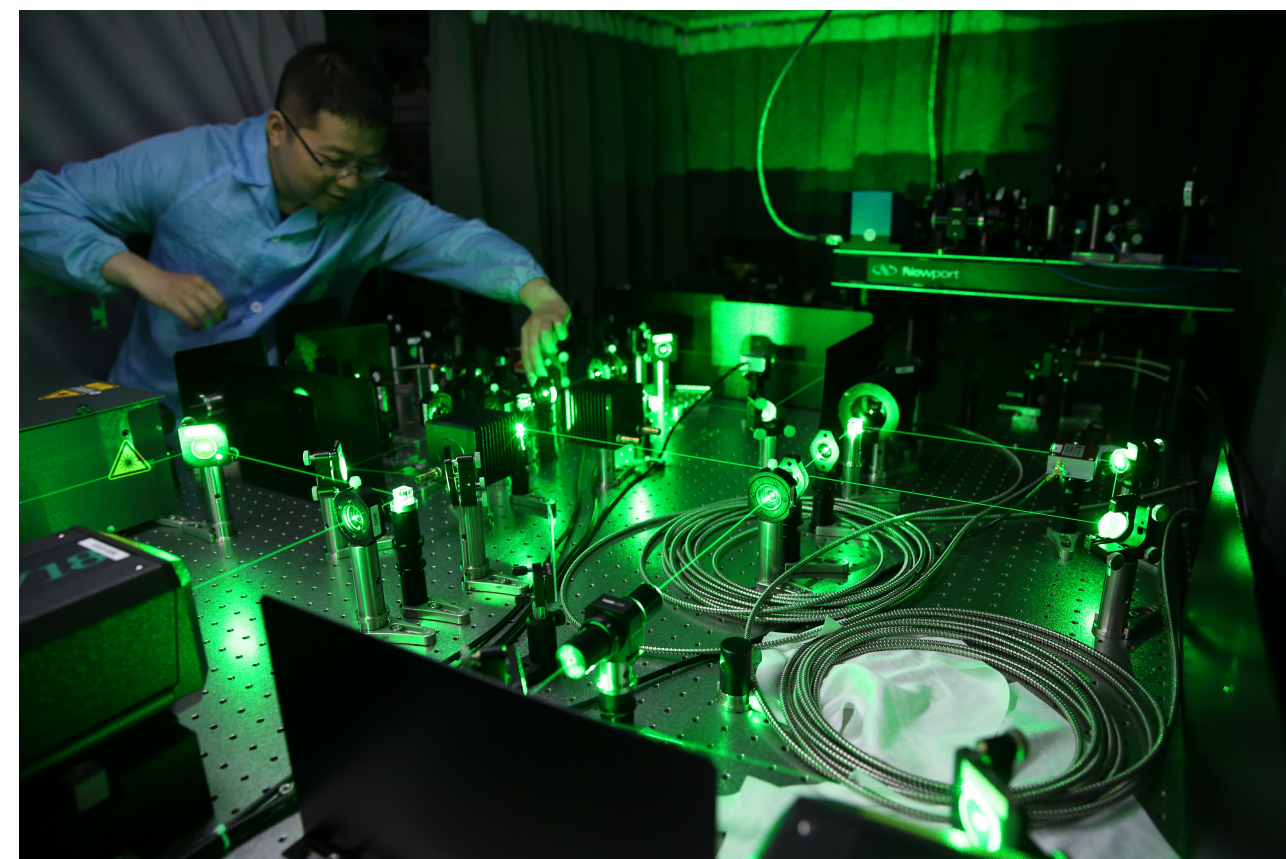


Source: IBM

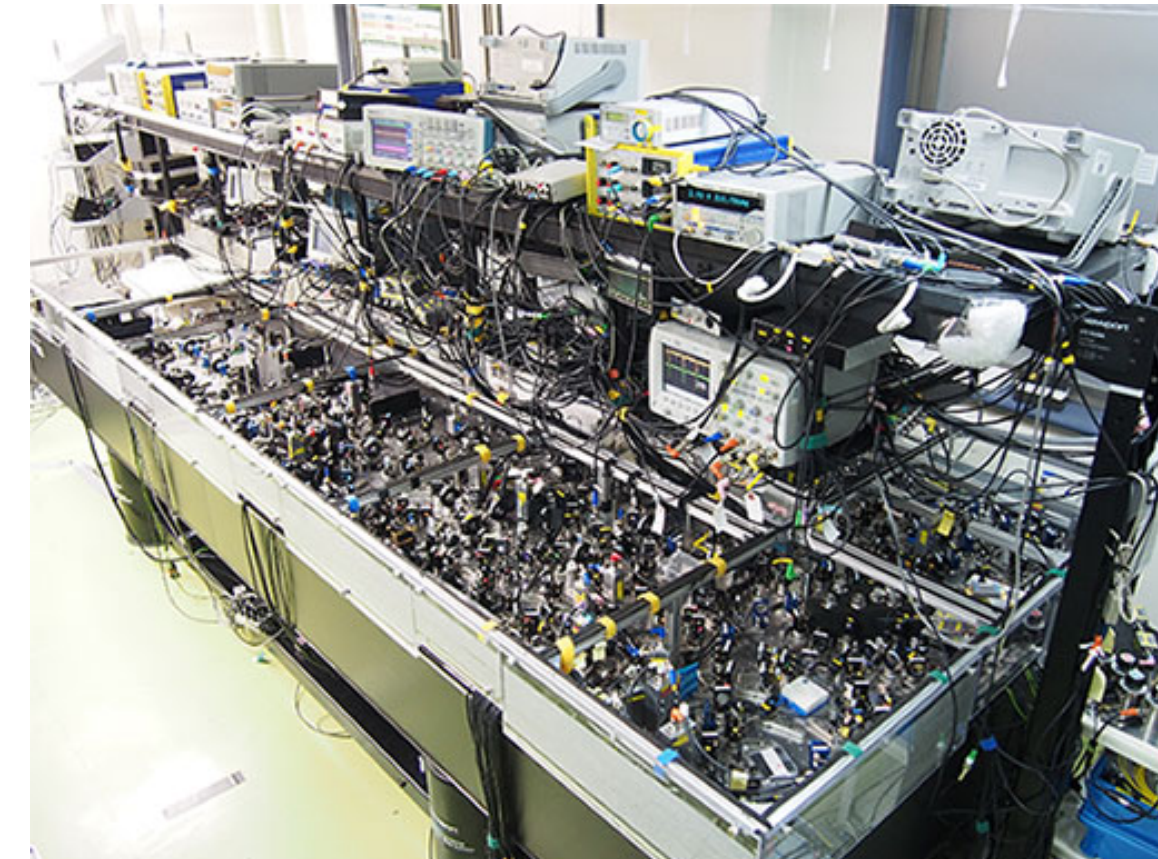


Source: IBM

photonics processor



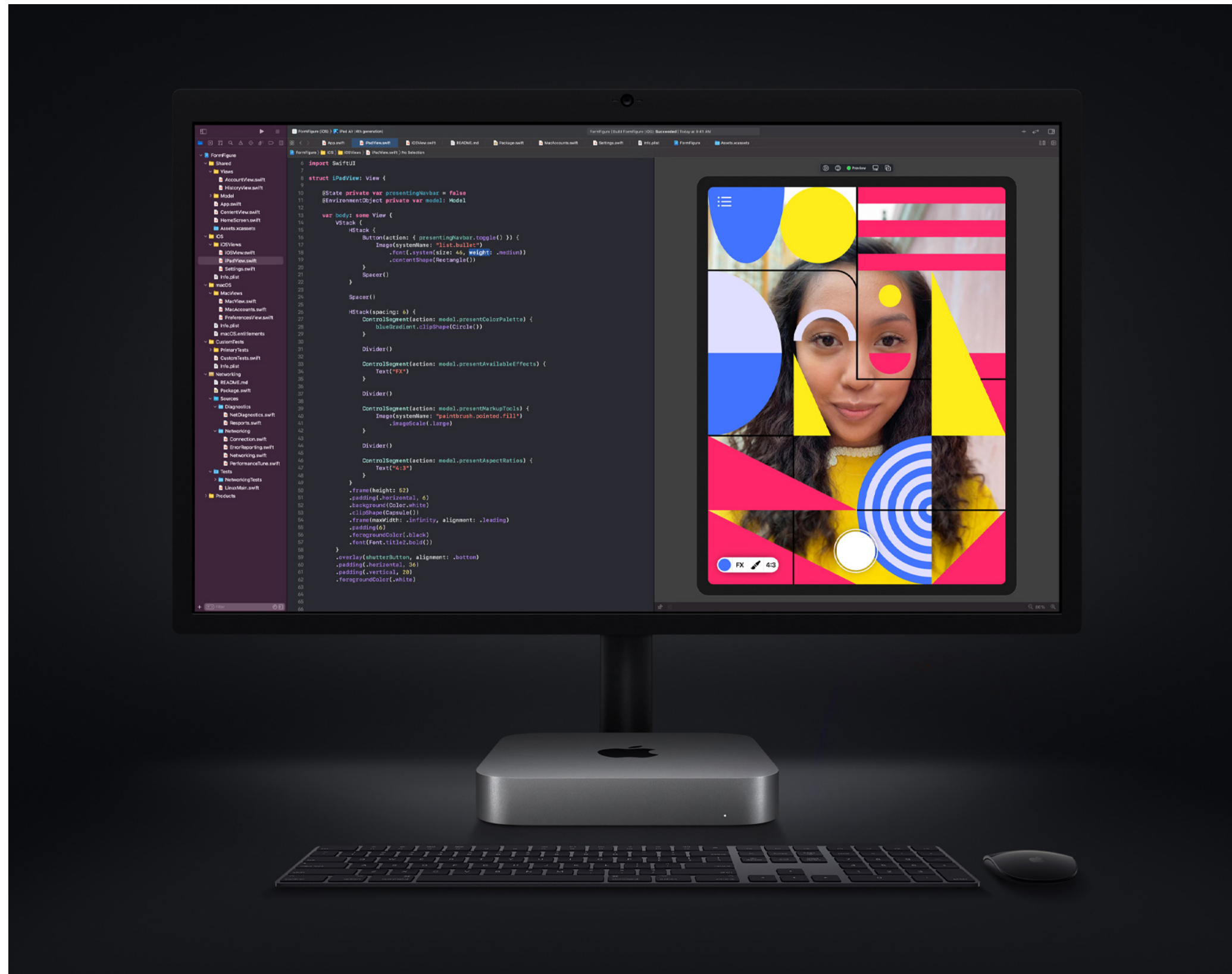
Source: CAS-Alibaba Quantum Computing Laboratory



Source: U. of Tokyo

Computer versus Processor

Master: classical computer

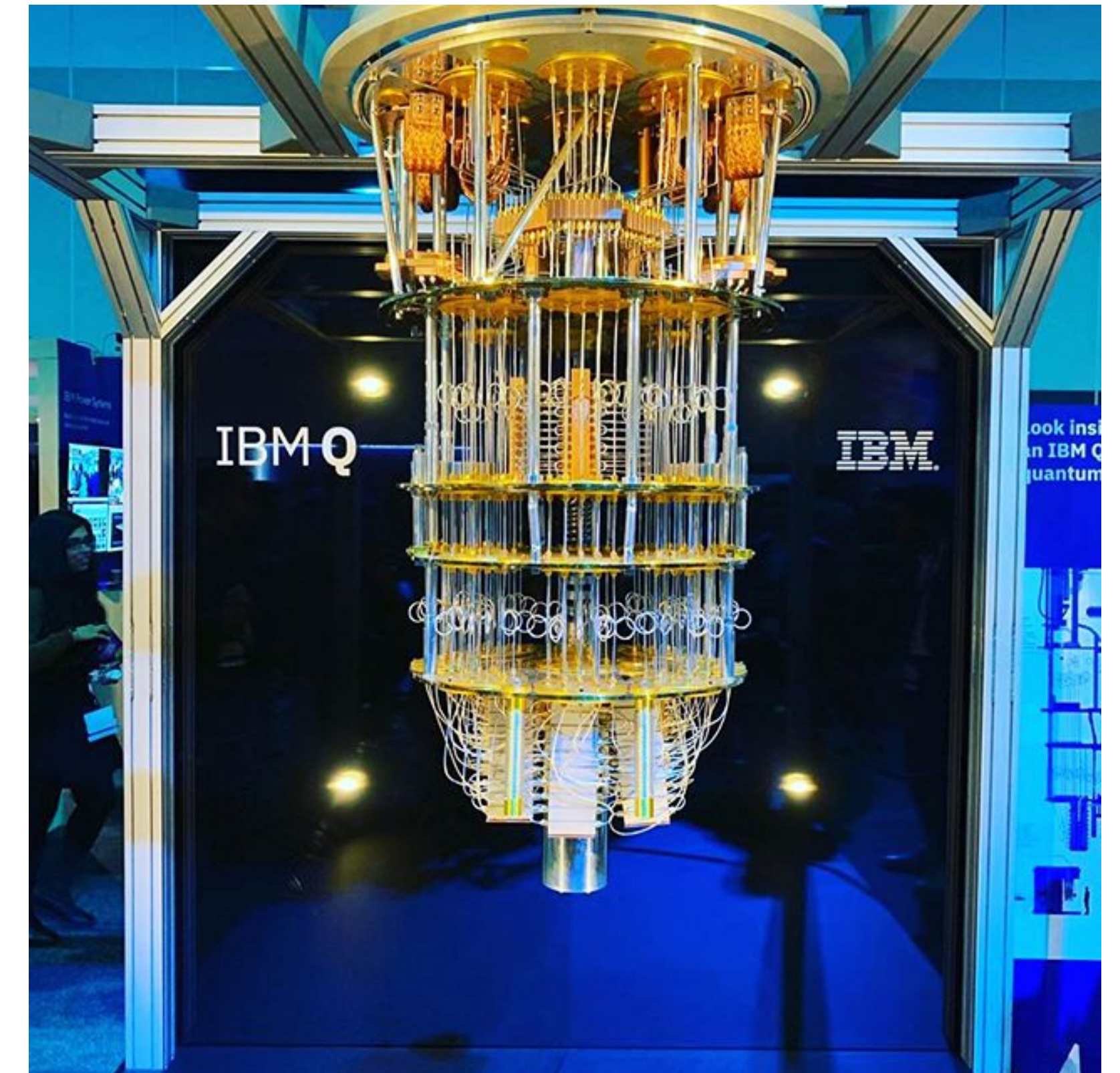


Source: Apple

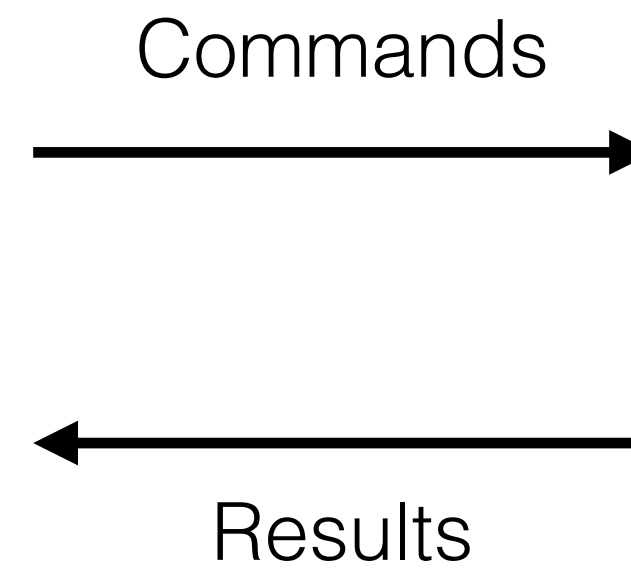
(Relatively) vast amount of storage

Code

Slave: quantum processor



Source: IBM



NO storage space

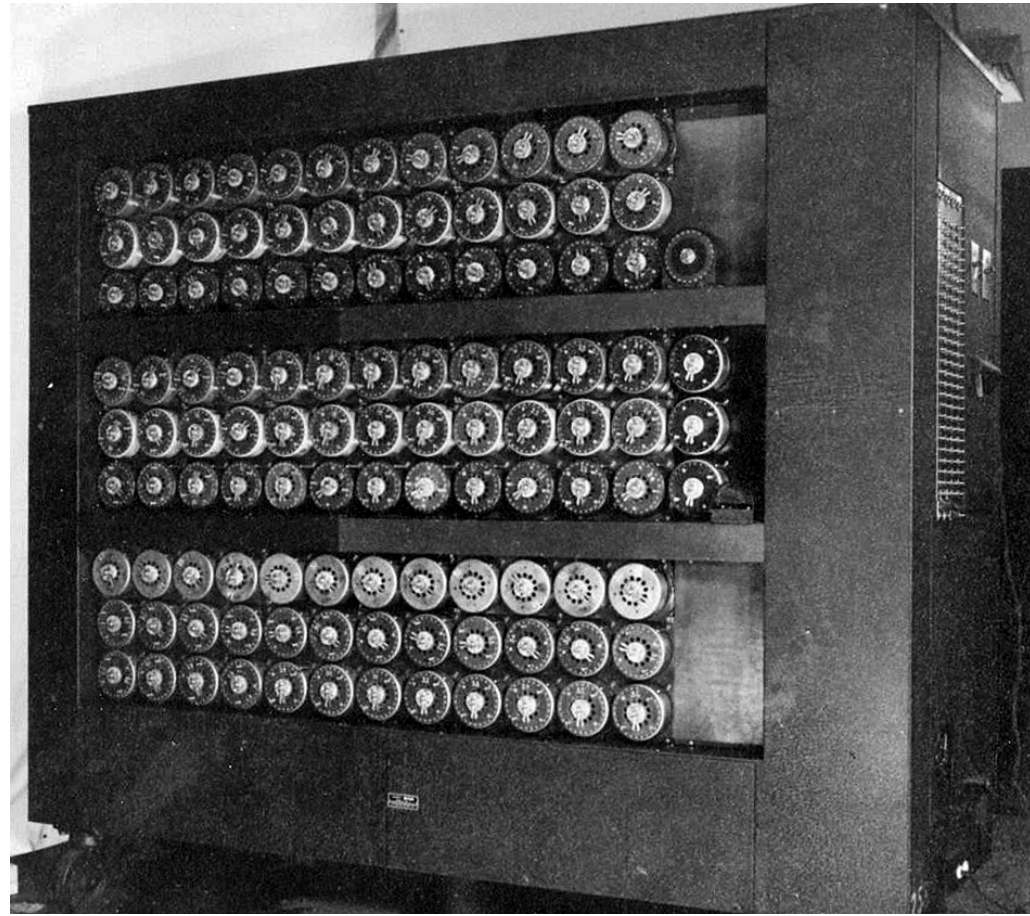
NO code

ONLY 100 qubits holding *little information* for a *very short time*

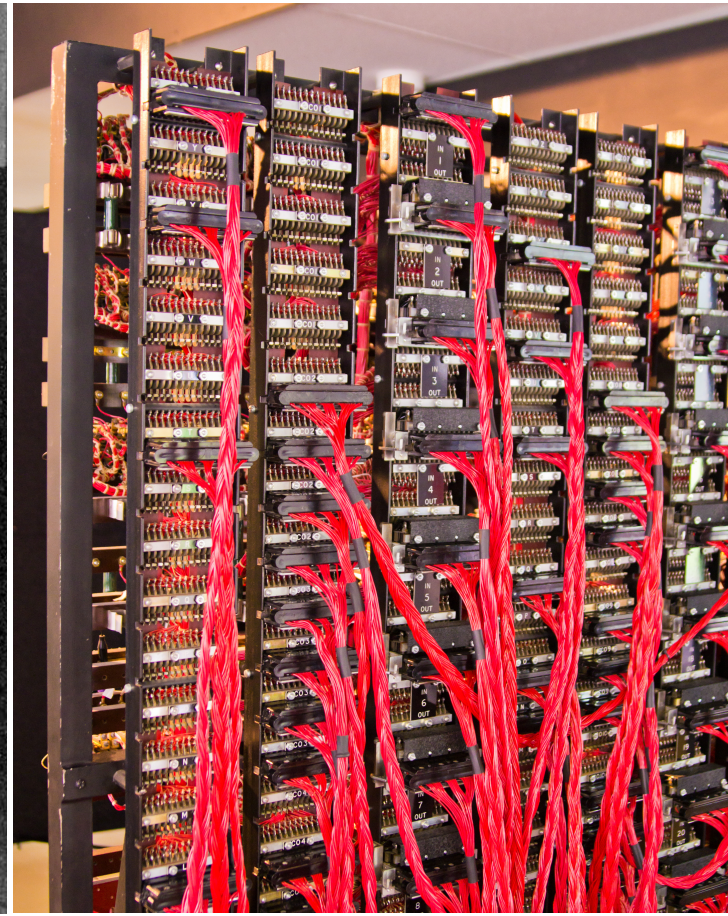
Classical computing (1939-1960)

1939: Electro-mechanical: The Bombe

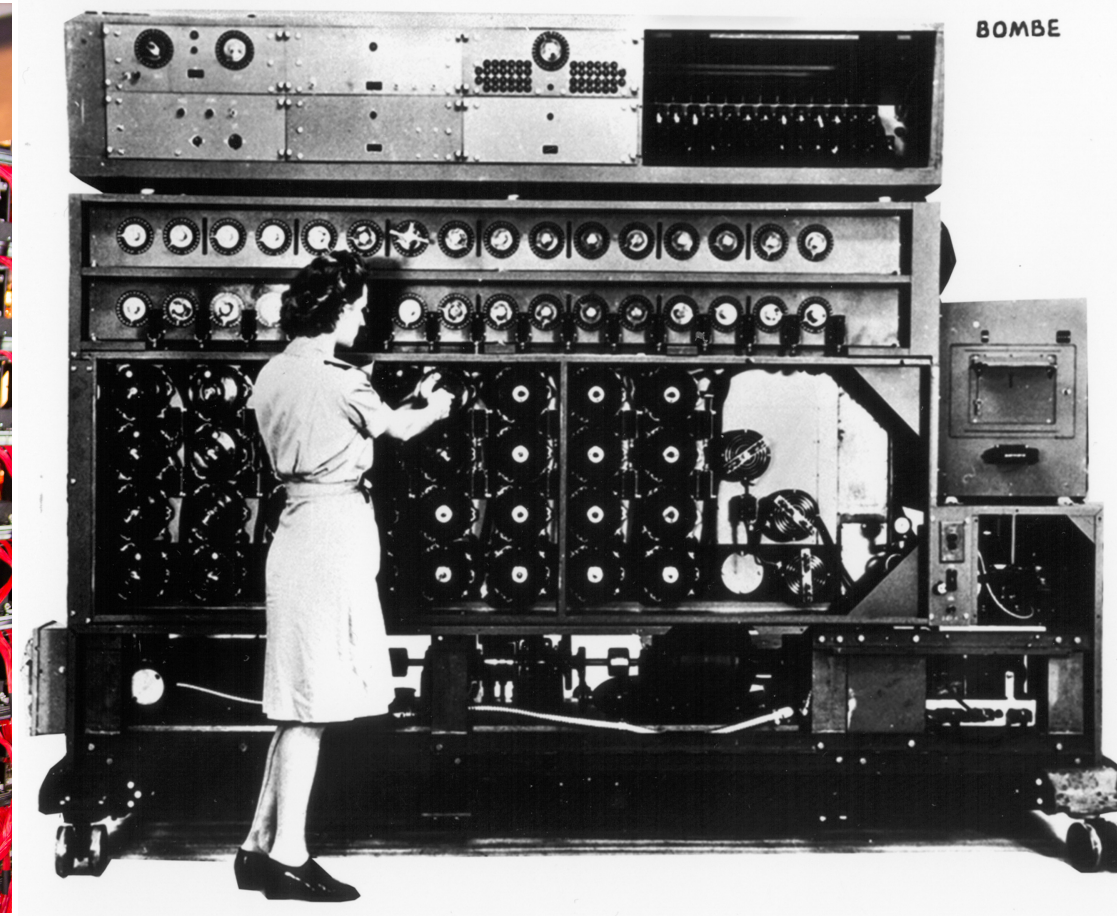
Application: deciphering German encrypted messages during WWII



(Source: Wikipedia)



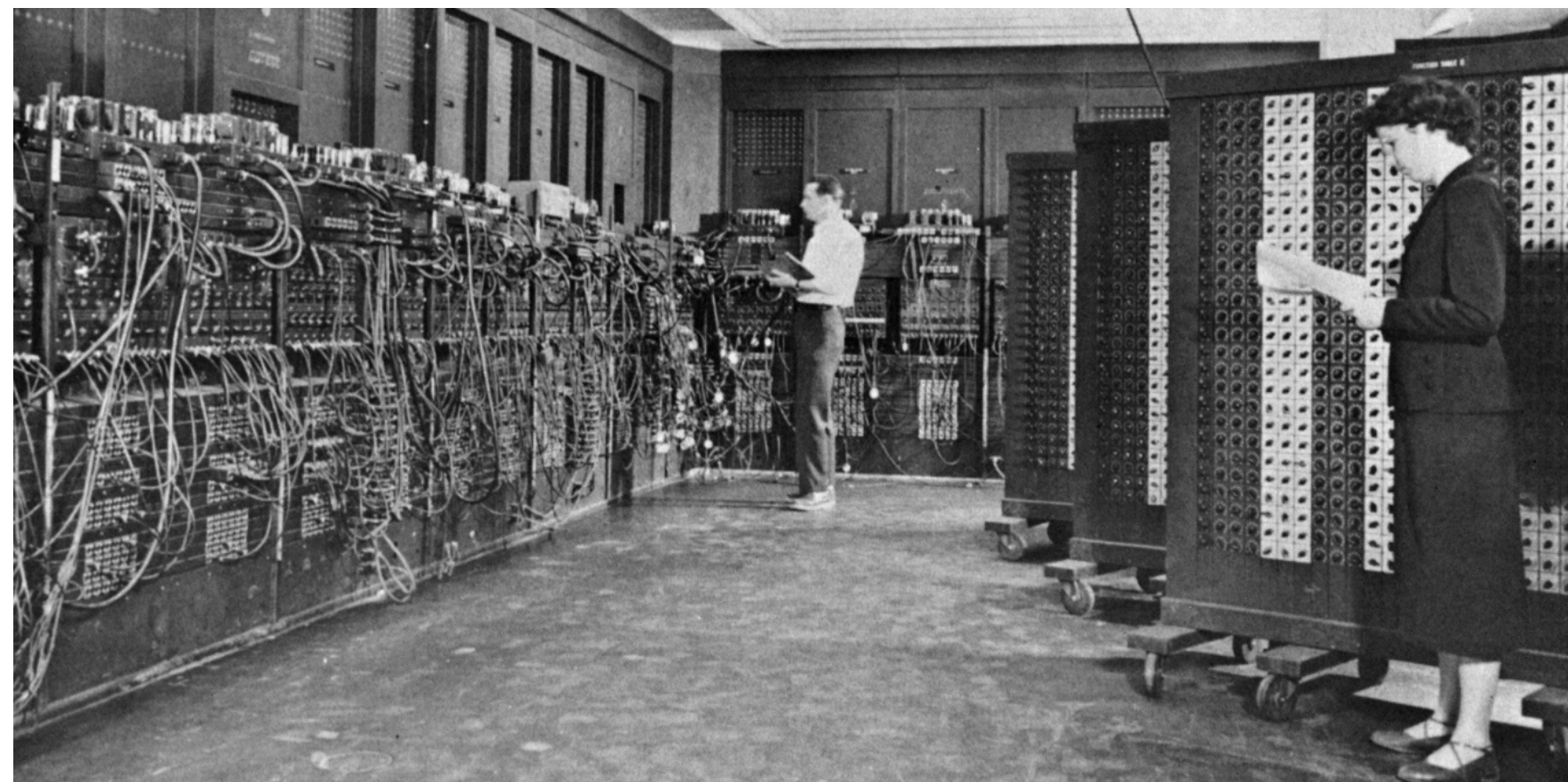
(Source: Wikipedia)



(Source: Wikipedia)

1945: Electronic Numerical Integrator and Computer (ENIAC): first programmable digital computer

Application: solving numerical problems: artillery firing tables, feasibility of thermonuclear weapons



(Source: Wikipedia)

1966: Apollo Guidance Computer

Application: Landing on the moon



(Source: Wikipedia)

Quantum computing (1981-2023)



IBM Quantum lab in Yorktown Heights, NY

Source: IBM

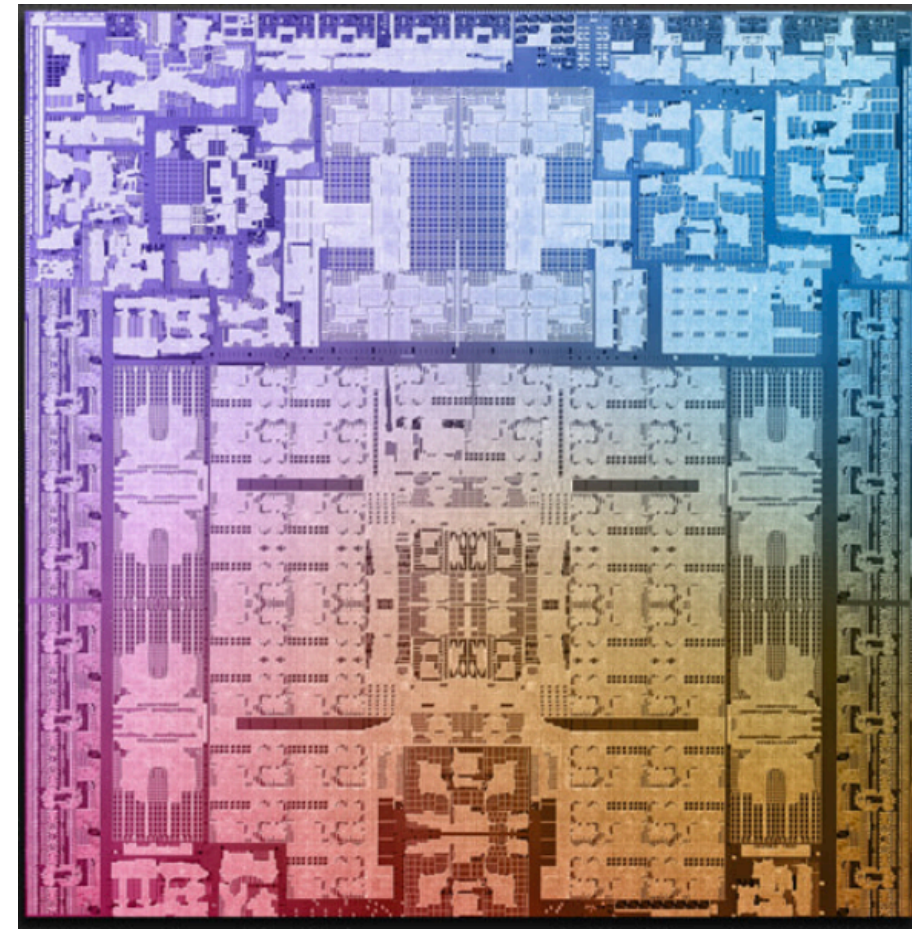
Classical computing (2022)

2022: iPhone 14 Pro



(Source: Apple)

Apple's M2 chip

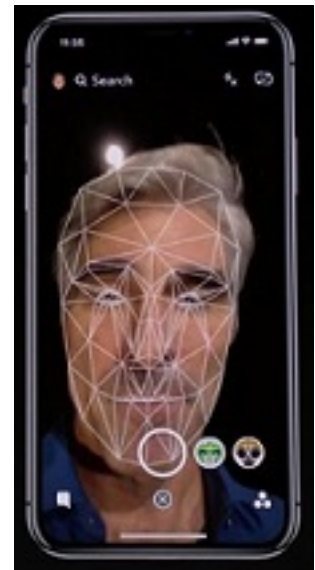


67 billion transistors

(Source: Apple)

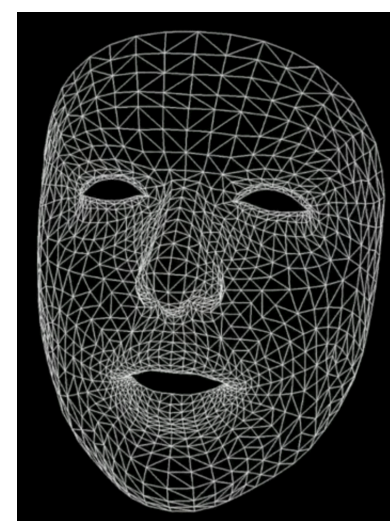
Applications: ...

Facial recognition



(Source: Apple)

Face tracking



Object detection



Image classification



LIDAR 3D scene Modelling and understanding

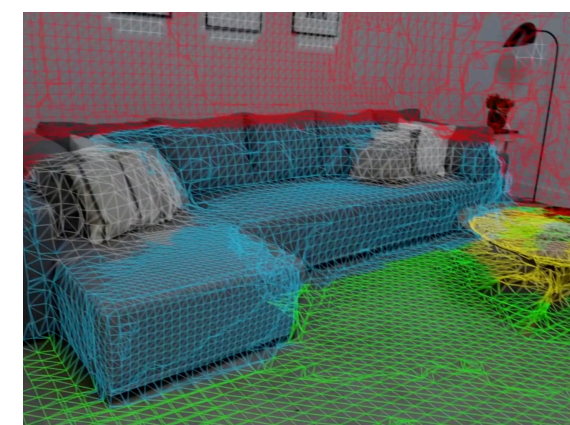
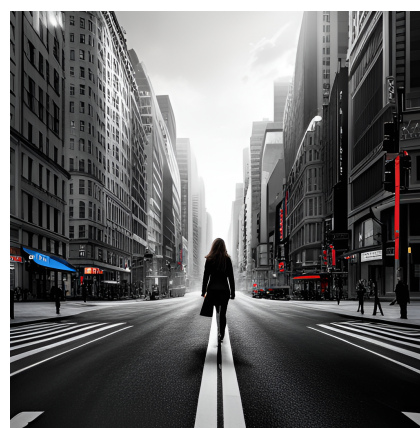


Photo artistry



Generated with Stable Diffusion



Quantum computing (2070-2100)



Applications (probable)

modelling molecules interactions

chemistry, material design, drug development

finance, agriculture

1. Why should we care ?

A. Potential to break current encryption schemes



Source: Midjourney

RSA cryptosystem relies on the practical difficulty of **factoring** the product of two large **prime numbers** (source: Wikipedia)

The world economy (on-line) depends on cryptography: information, traffic encrypted while sent over the web

RSA-250 has 250 decimal digits (829 bits)

```
RSA-250 = 2140324650240744961264423072839333563008614715144755017797754920881418023447
1401366433455190958046796109928518724709145876873962619215573630474547705208
0511905649310668769159001975940569345745223058932597669747168173806936489469
9871578494975937497937
```

```
RSA-250 = 6413528947707158027879019017057738908482501474294344720811685963202453234463
0238623598752668347708737661925585694639798853367
× 3337202759497815655622601060535511422794076034476755466678452098702384172921
0037080257448673296881877565718986258036932062711
```

factored in February 2020 by

Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger,
Emmanuel Thomé, and Paul Zimmermann.

Using approximately 2700 CPU core-years

RSA-2048 has 617 decimal digits (2,048 bits)

```
RSA-2048 = 2519590847565789349402718324004839857142928212620403202777713783604366202070
7595556264018525880784406918290641249515082189298559149176184502808489120072
8449926873928072877767359714183472702618963750149718246911650776133798590957
0009733045974880842840179742910064245869181719511874612151517265463228221686
9987549182422433637259085141865462043576798423387184774447920739934236584823
8242811981638150106748104516603773060562016196762561338441436038339044149526
3443219011465754445417842402092461651572335077870774981712577246796292638635
6373289912154831438167899885040445364023527381951378636564391212010397122822
120720357
```

?

Source: [Wikipedia RSA numbers](#)

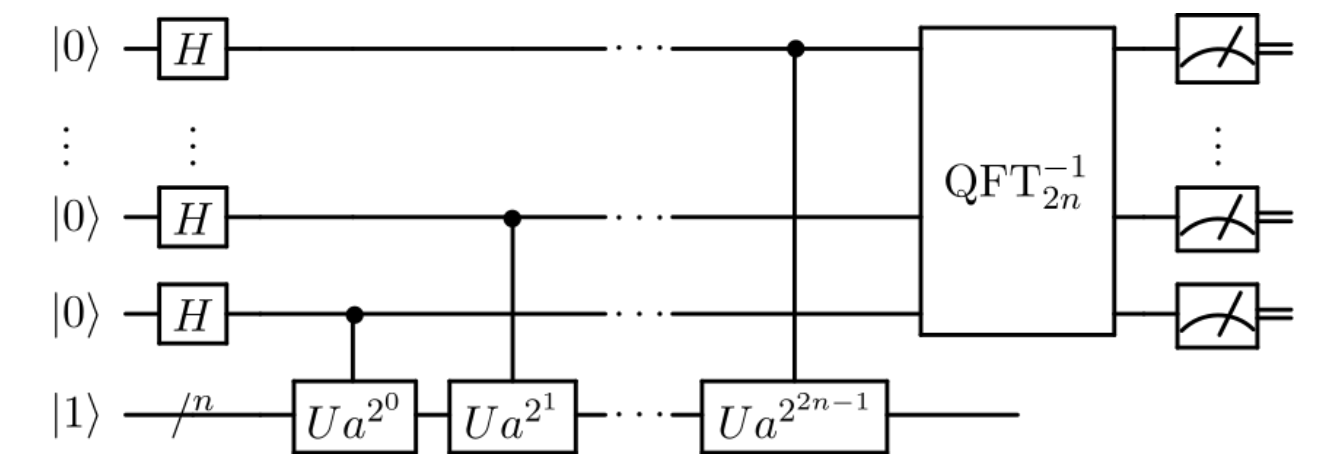
1994 - Shor's algorithm



Peter Shor, professor of Applied mathematics at MIT

“Shor's algorithm is a quantum algorithm for factoring the prime factors of an integer” (source: [Wikipedia](#)) ([semiprime](#))

Fourier transform on a quantum processor...



Practical implementation

Factoring a 2,048 bit integer would require approx. 4,000 perfect qubits and about 1,000,000,000 gates... (MIT 2017 - Quantum Computational Supremacy)

Today's Noisy Intermediate Scale Quantum (NISQ) processor have about 100 “imperfect” (noisy) qubits... Coherence time of qubits is around milli- to micro-second

With today's technology and knowledge, one would need approximately:

4,000,000 qubits that would not negatively interfere too much with each other and stay coherent for a significant amount of time...

Breaking current encryption schemes

A 2,048 bit integer might *never* be factored on a quantum processor...

Not very likely in the next half century...



Generated with dreamstudio.ai

Impact of Shor's algorithm

Post-quantum cryptography

Development of post-quantum cryptography (quantum-proof / quantum-resistant schemes)

NIST Post-Quantum Cryptography Standardization

Competition started in 2016: lattice, code-based, hash-based algorithms...

2022-07-05: First winners for standardization: lattice based (CRYSTALS-Kyber) and hash-based (SPHINCS+)



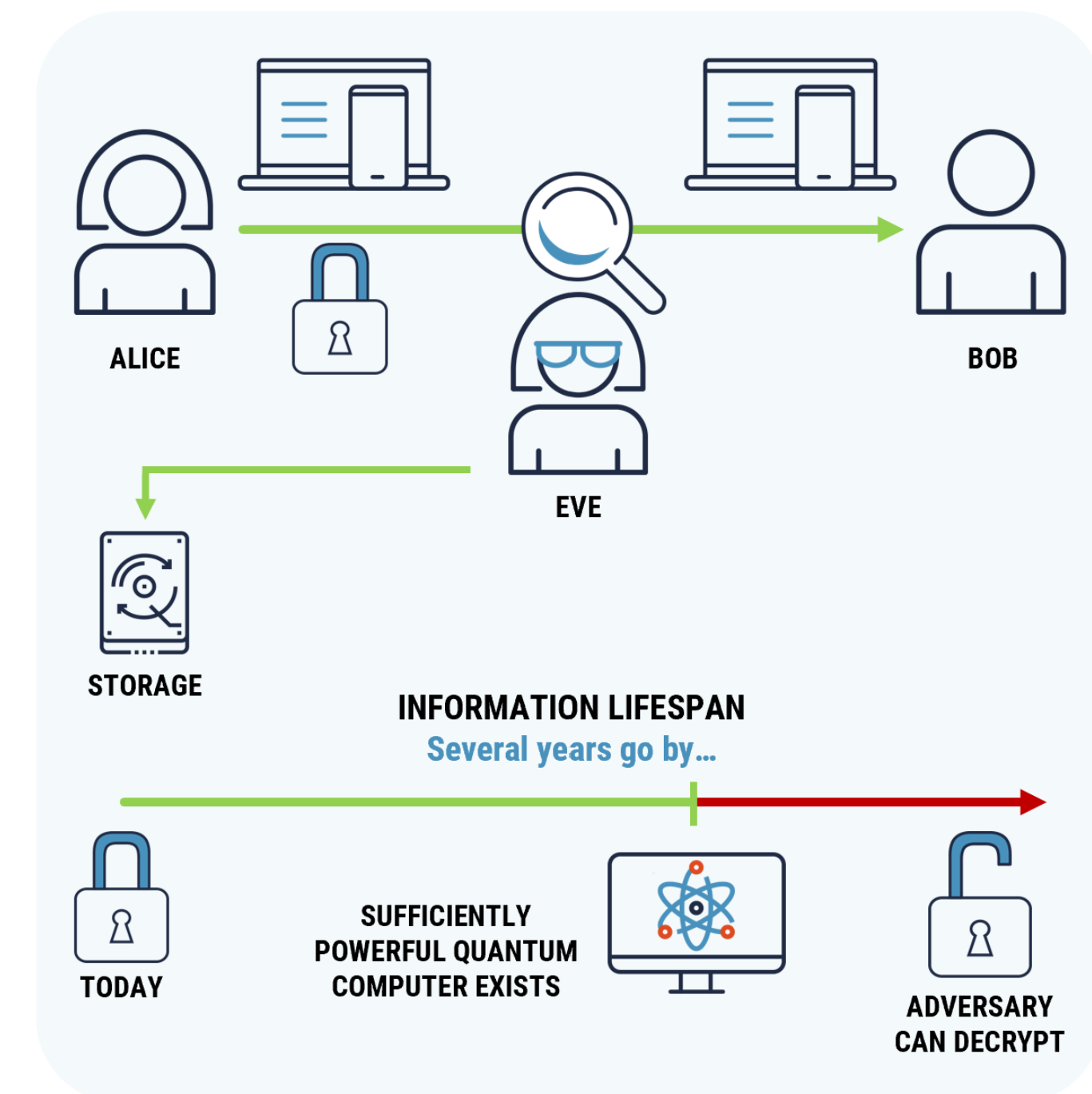
(Source: Midjourney)

Quantum key distribution

Governments / companies transition to quantum safe encryption

Stashing other countries' encrypted secrets to decrypt later (e.g. Forbes 2023-01)

National defence is getting ready; e.g. Gov. Of Canada Quantum 2030



Source: cyber.gc.ca

B. Feeding the world (“ending world hunger”)



Fritz Haber (wikipedia)

Haber–Bosch process, a method used in industry to synthesize ammonia from nitrogen gas and hydrogen gas. (Source: Wikipedia) (1909)

“Solving one of the biggest problem humanity has ever faced” (feeding billions of people) (source: Veritasium)

The Green Revolution (third agricultural revolution)



Fertilizer made using ammonia: Haber-Bosch process $N_2 + 3H_2 \rightarrow 2NH_3$

The Haber-Bosch process “consumes 1% of the world’s total energy production.” (Nature 2019)

The process requires high temperatures (500 degree C) and pressures.

Finding a better way (less energy requirement) to produce ammonia

Some plants can synthesize ammonia directly from air and water at room temperature (Nature)

Using quantum processors to simulate quantum processes (molecules interactions)

Quantum Chemistry :

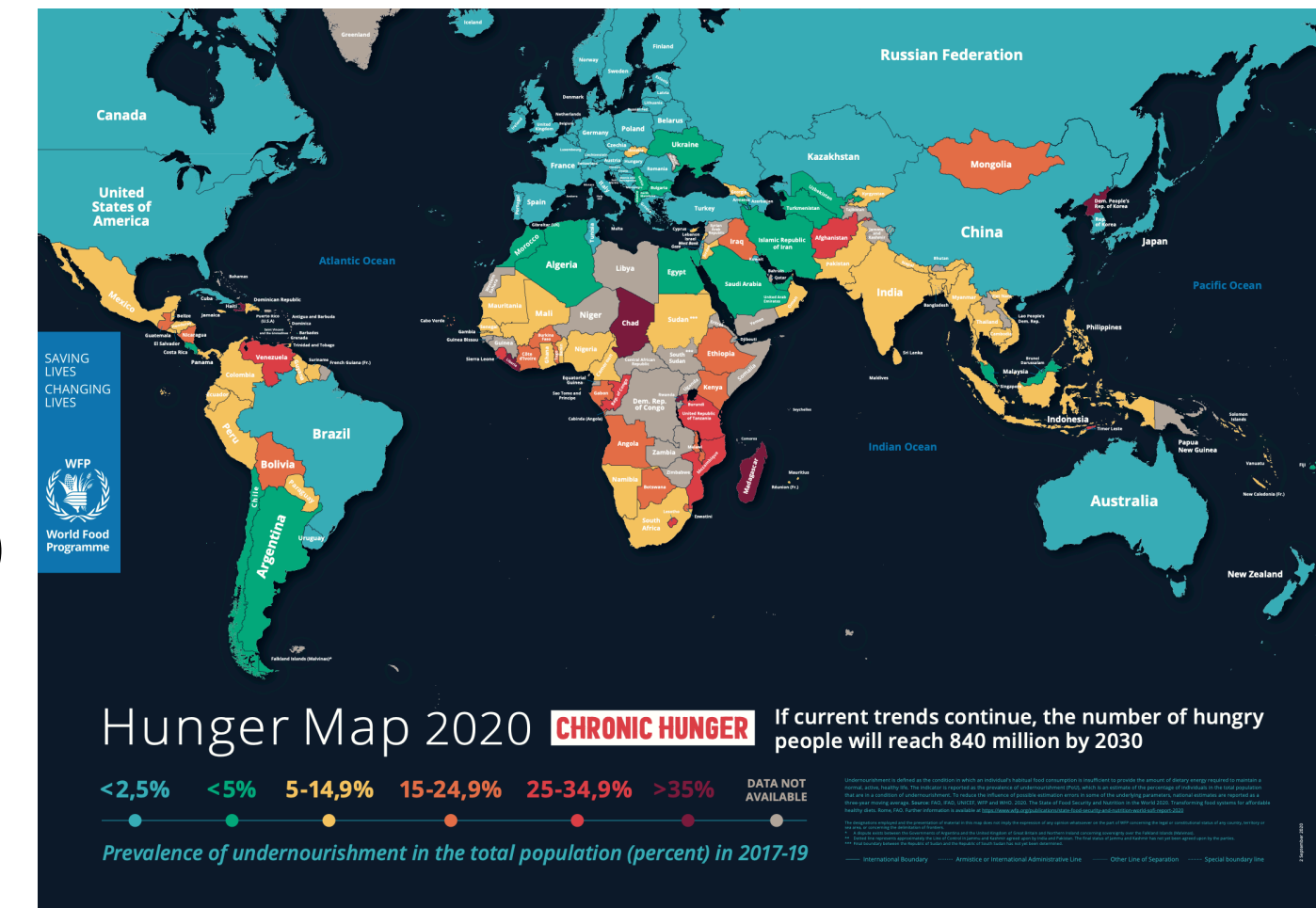
$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = \hat{H} |\psi(t)\rangle$$

“Understanding **electronic structure** and **molecular dynamics** using the **Schrödinger equations** are central topics in quantum chemistry.”



(1925)

(Source: Wikipedia)



World Food Program hunger map (840 million by 2030)

2. How does it work ?

Classical computing

High level language

Software packages

Algorithms

Compilers

Machine code

Assembler

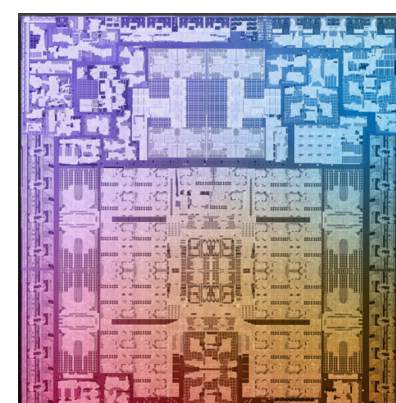
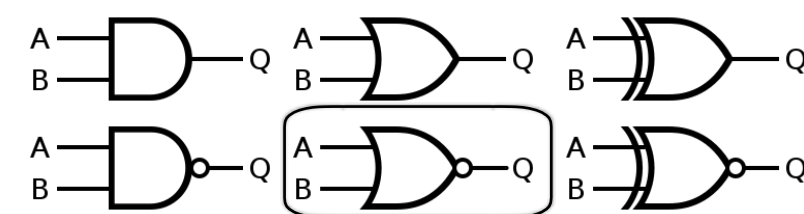
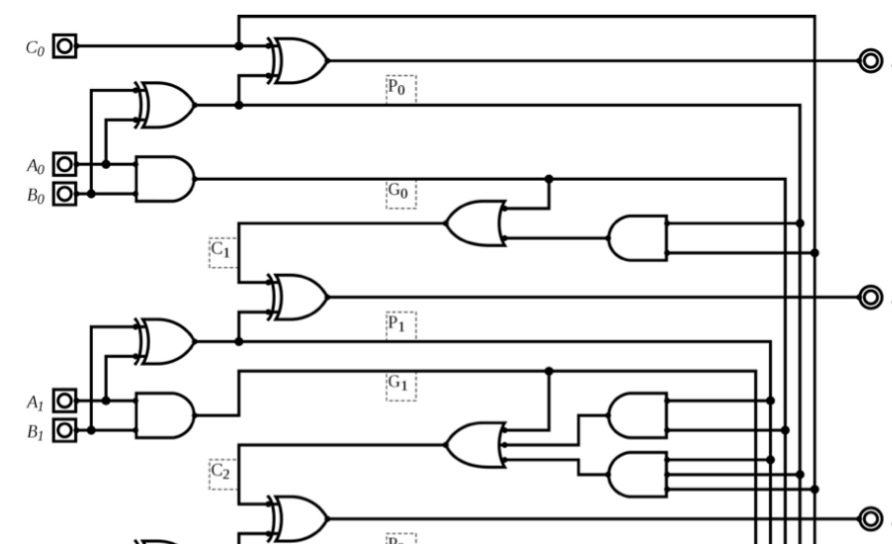
Circuits

Gates

Processor



Fourier transform, sorting algorithms, balanced search trees, Hash tables, minimum spanning trees, linear programming, Maximum flow / minimum cut, ... (Algorithms - Princeton [part 1](#), [part 2](#))

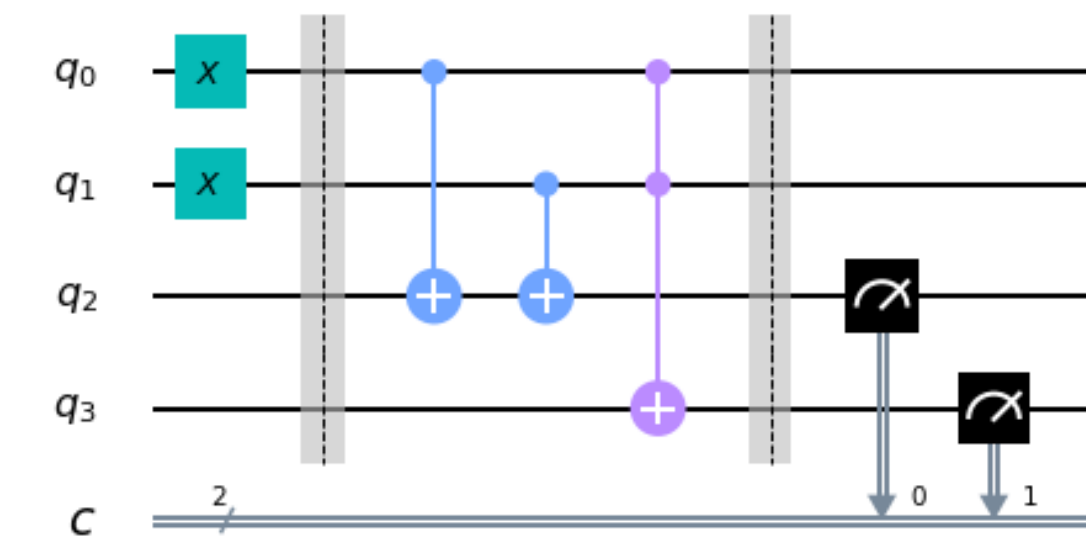


(Source: Apple)

Quantum computing



Quantum Fourier transform, quantum phase estimation algorithm, Shor's algorithm, Grover's algorithm, quantum optimization algorithms, Eigensolver, ... (Qiskit [Algorithms](#))



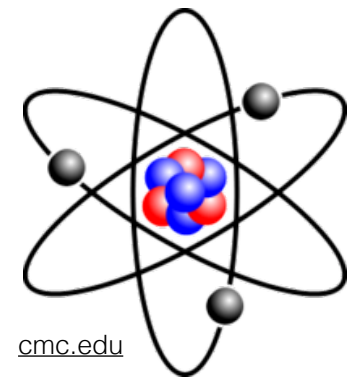
Source: IBM

Classical mechanics | Quantum mechanics

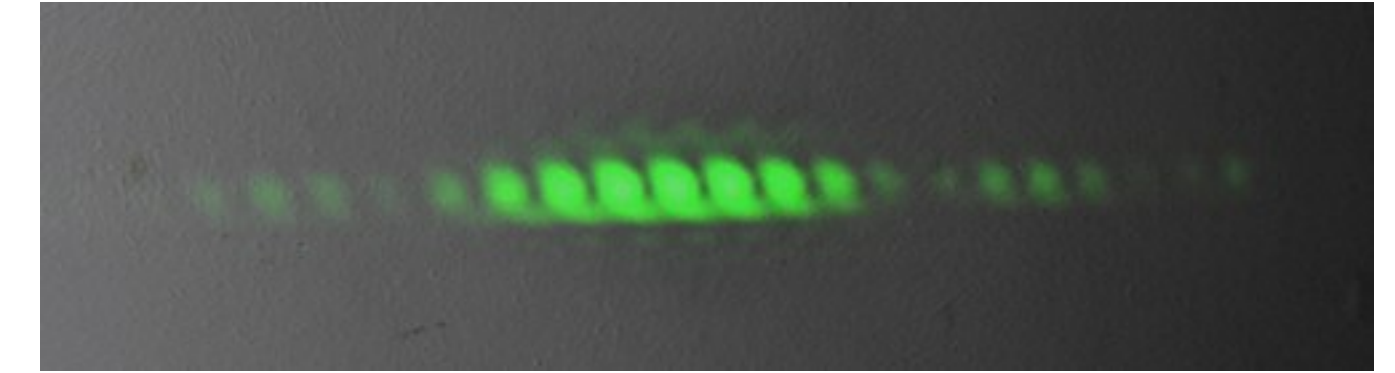
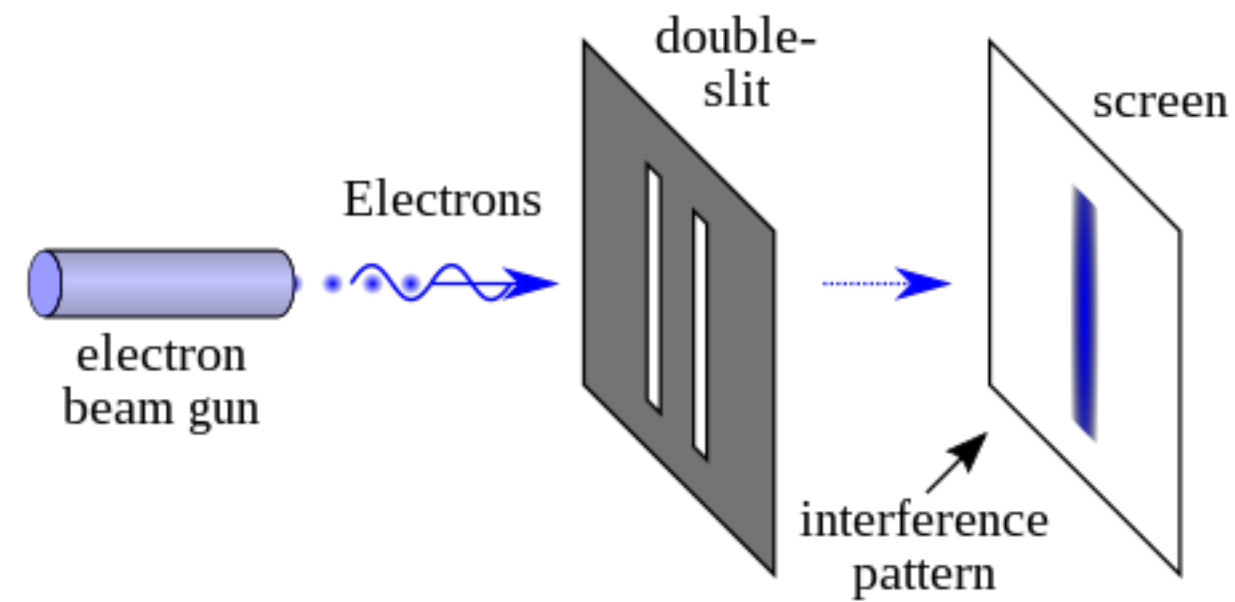
	Classical	Quantum
Scale	Applies to <i>macroscopic</i> objects (planets and everyday objects)	Applies to <i>microscopic</i> objects (atoms and subatomic particles)
Math framework	Newton's equations, <i>deterministic</i> , position, velocity, acceleration	Schroedinger's equation, wave function, β distribution
Behaviour	Particles have definite properties (position, momentum) <i>Deterministic</i> , position, trajectories can be predicted precisely.	<i>Wave-particle duality</i> . Behaviour <i>probabilistic</i> . Impossible to know both position and momentum.
Measurement	Precise and not disturbing system being measured	Affect system being measured. Exact state cannot be measured.
Energy levels	Energy levels are continuous, can have any values	Energy is quantized. Can only have certain values.
Superposition	Objects can only be in one place (state) at a given time	Objects can be in multiple states at once.
Entanglement	Non existent	Objects properties (states) can be correlated even when far away

Theories in physics that describe the behaviour of **matter and energy**

Wave particle duality



Double-slit experiment



(Source: [wikipedia](#))

is

behaves

An electron

e^{-}

(Also applies
photons, atoms
and molecules)

not a particle

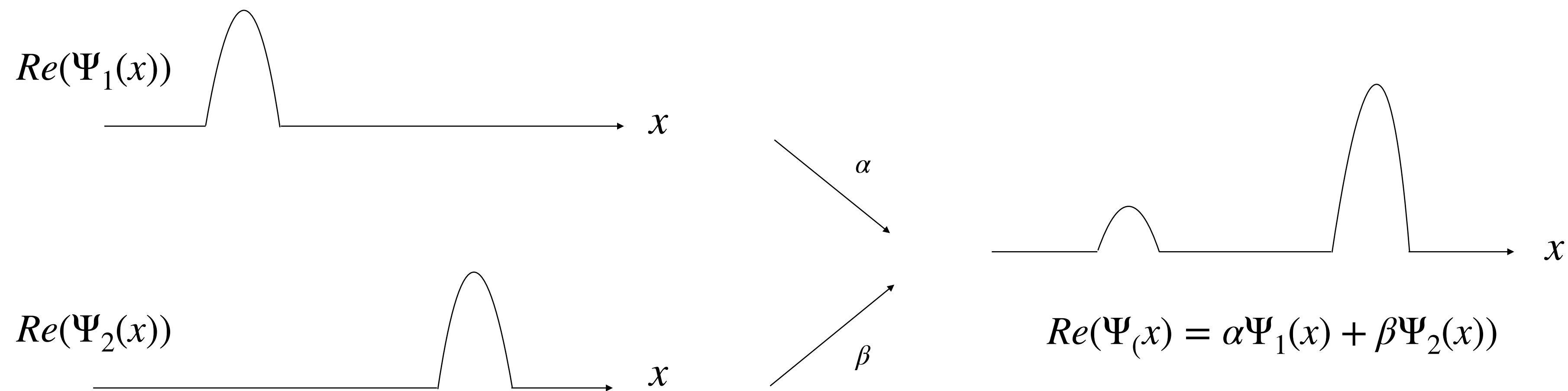
not a wave

like a particle

like a wave

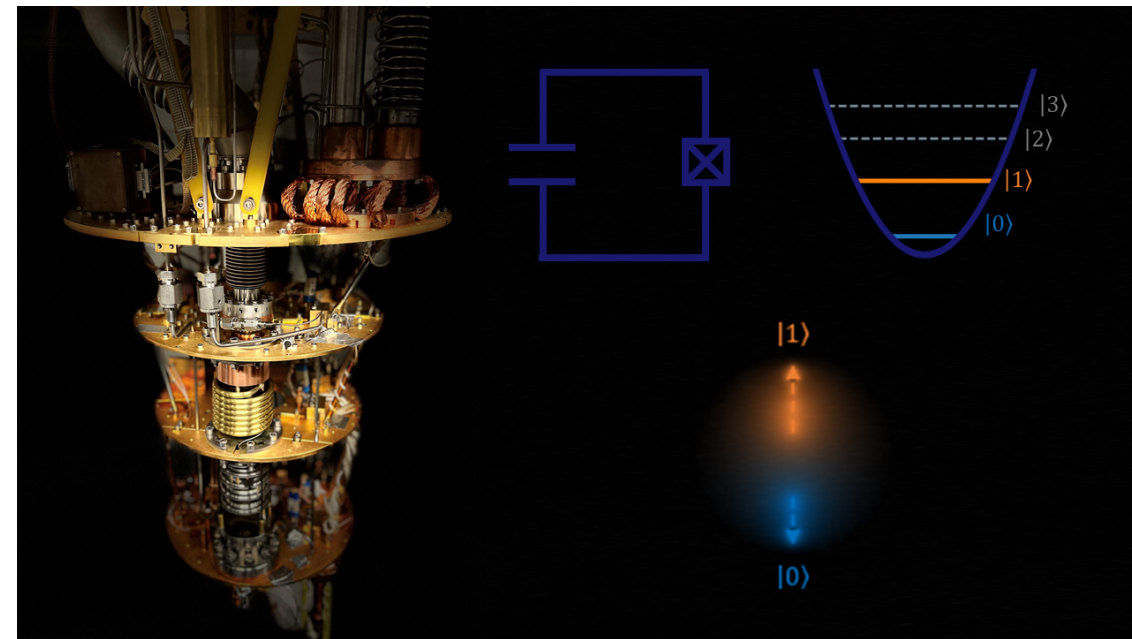
Three postulates of quantum mechanics

1. Configuration of a quantum object is described by a complex wave function $\Psi(x)$
2. $|\Psi(x)|^2$ is the probability density of finding the object at position x
3. Superposition principle: given $\Psi_1(x)$ and $\Psi_2(x)$, it is possible to have $\Psi(x) = \alpha\Psi_1(x) + \beta\Psi_2(x)$



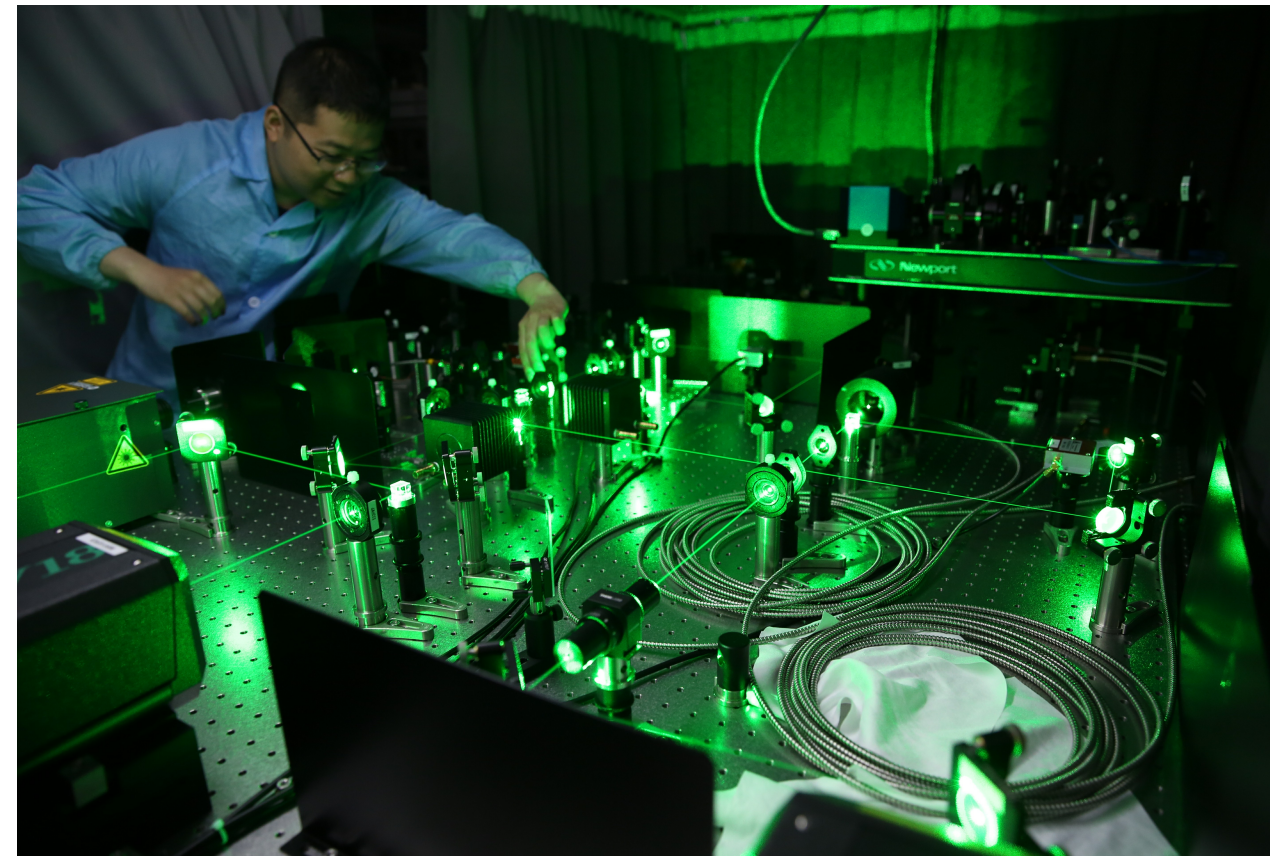
Qubit (physical)

Superconductor



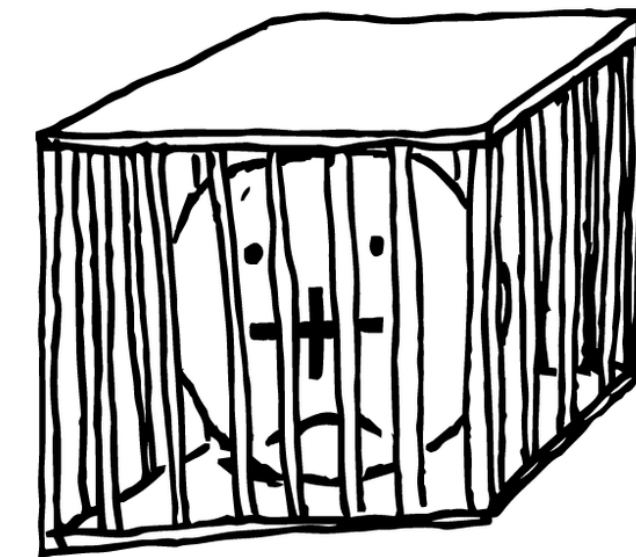
Source: [QST @ Naples](#)

Photons

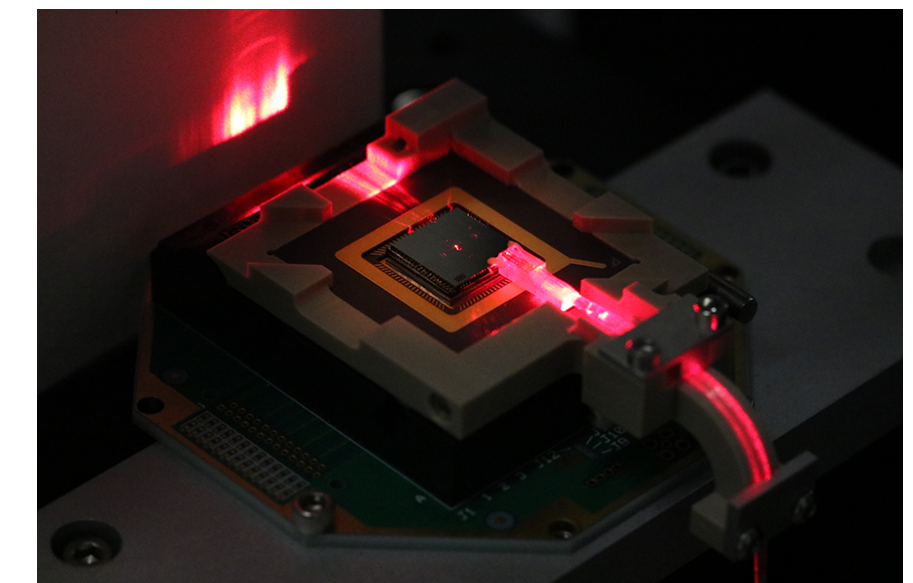


Source: [CAS-Alibaba Quantum Computing Laboratory](#)

Trapped ions



Source: [U. Chicago](#)



Source: [MIT News](#)

Qubit (intuition)

Head or Tail



Spinning coin



Classical bit (binary digit) vs Quantum bit (qubit)

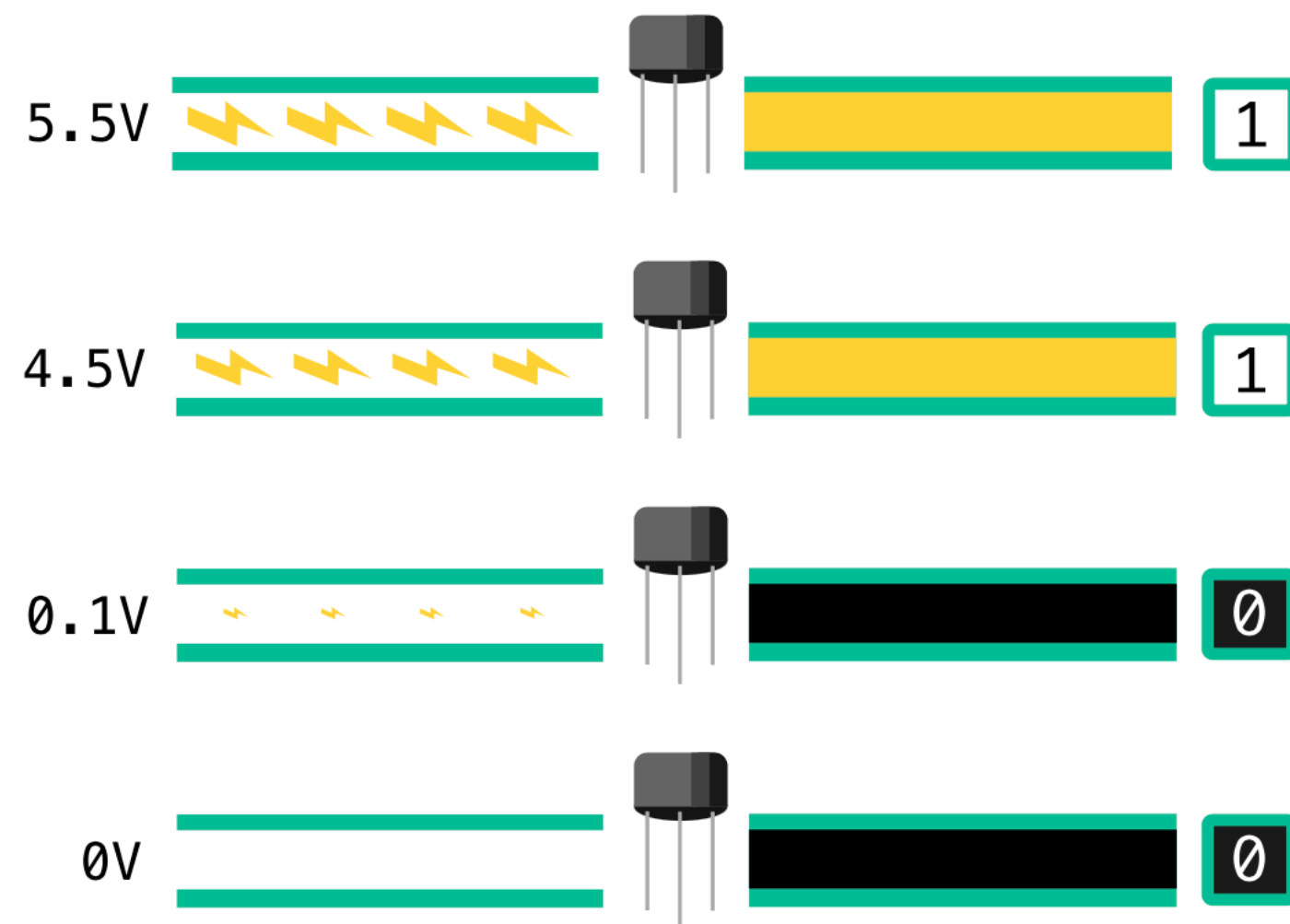
Bit

0 (1) dimension - 2 discrete values

Two distinct values: 0 or 1

Can be represented as two different voltage levels

Show voltage diagram



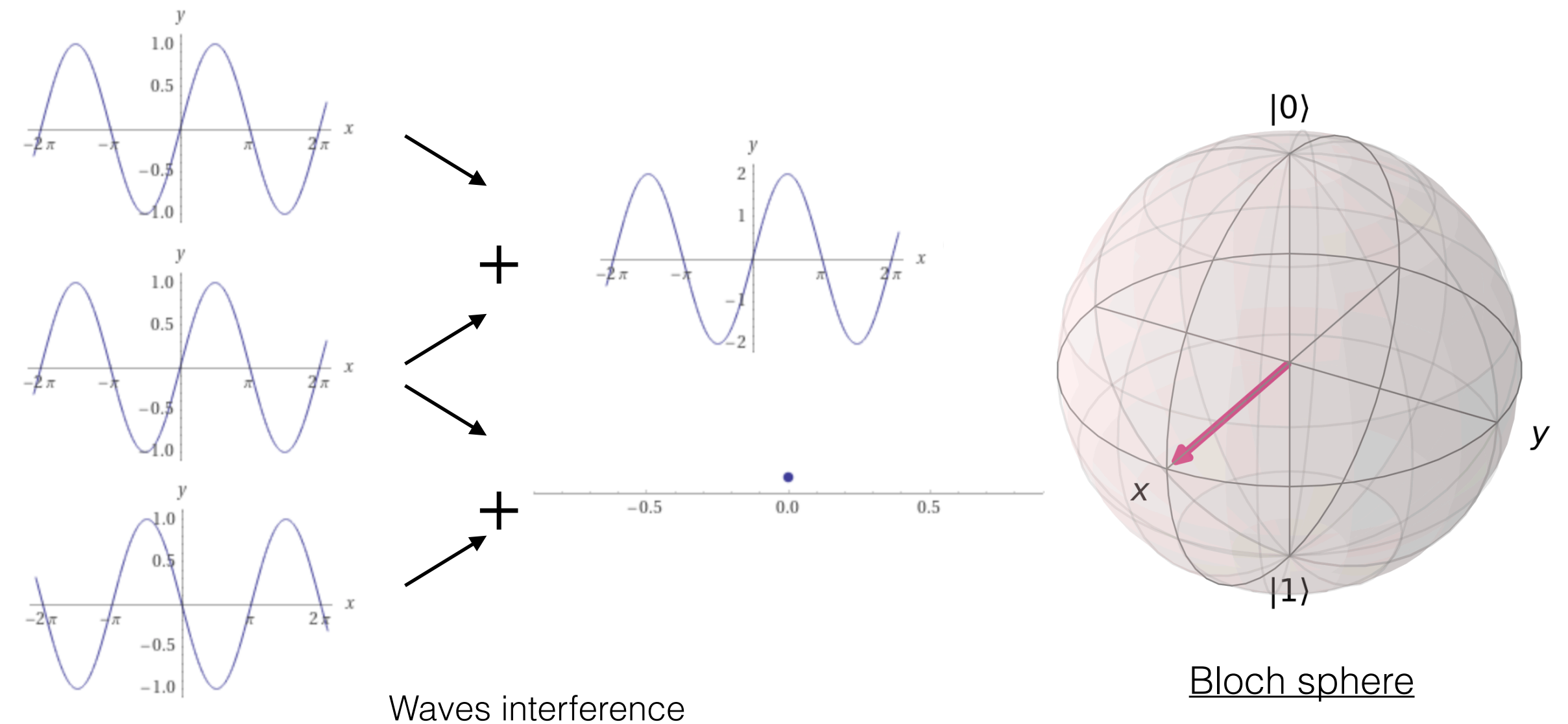
Source: KhanAcademy.org

Qubit

Unobservable: **2 dimensions - complex continuous values**

Observable: Either 0 or 1 (classical bit)

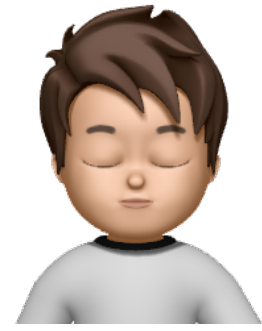
Particle / wave duality



Waves interference

Bloch sphere

Key concept 1: superposition



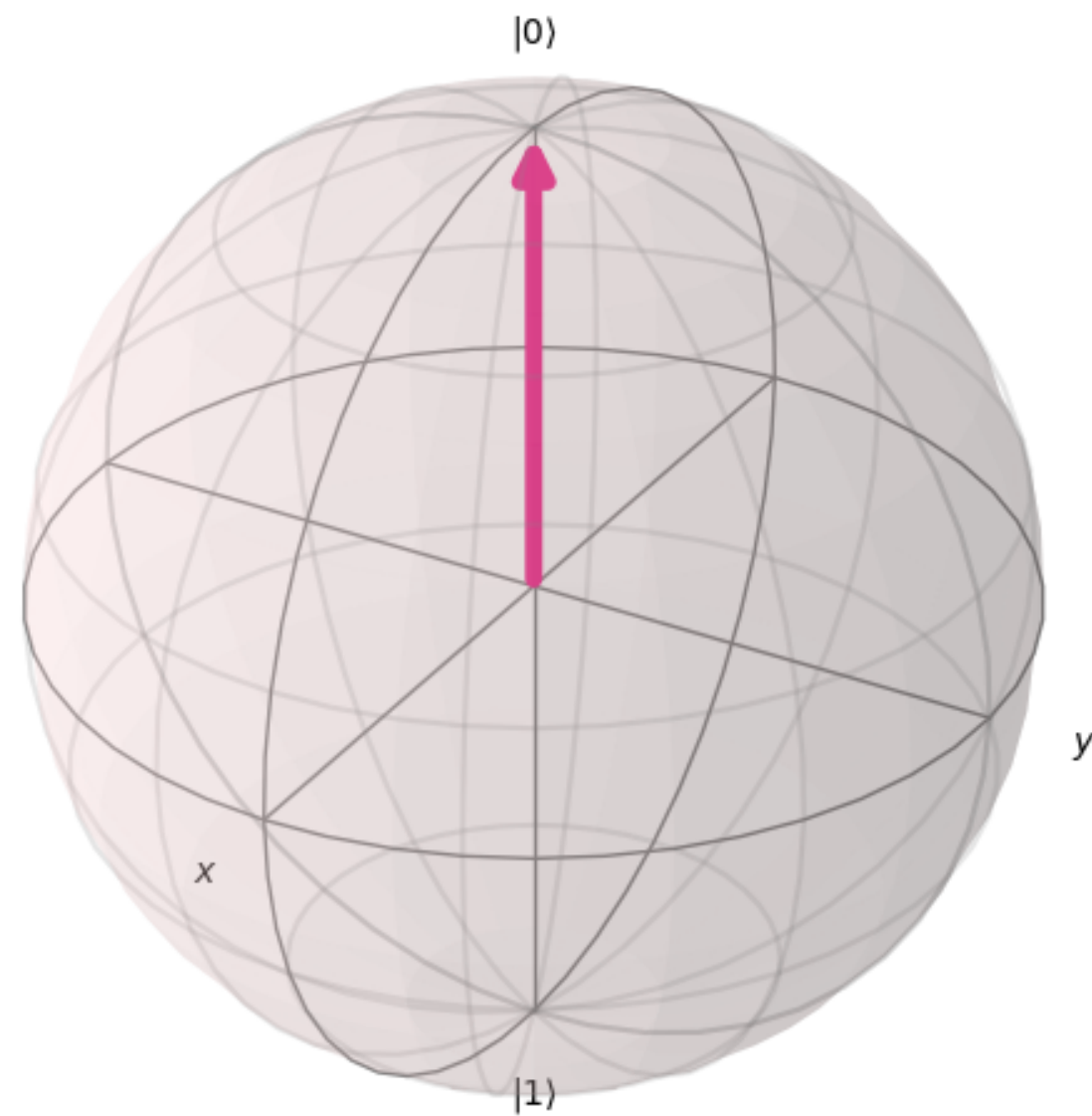
Unobservable (quantum)

"Schrödinger's cat"

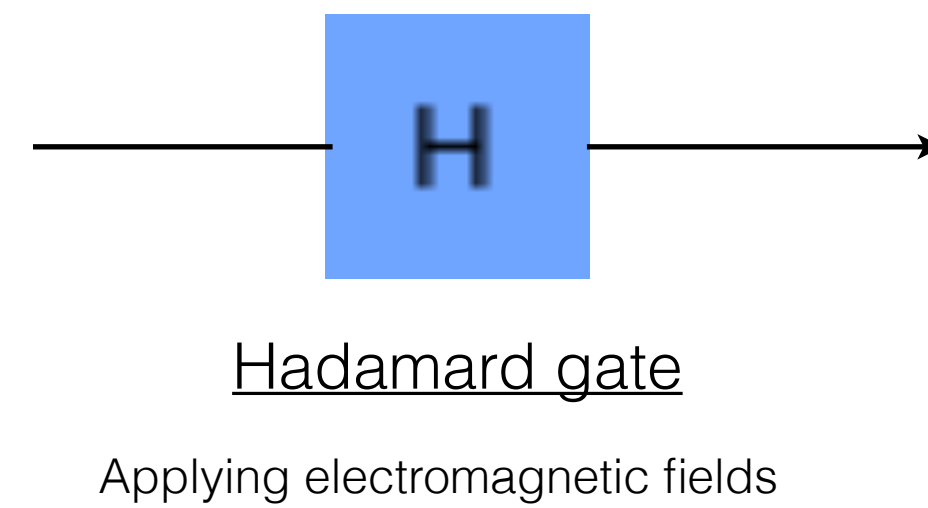


Observable (classical)

Initial (zero) state

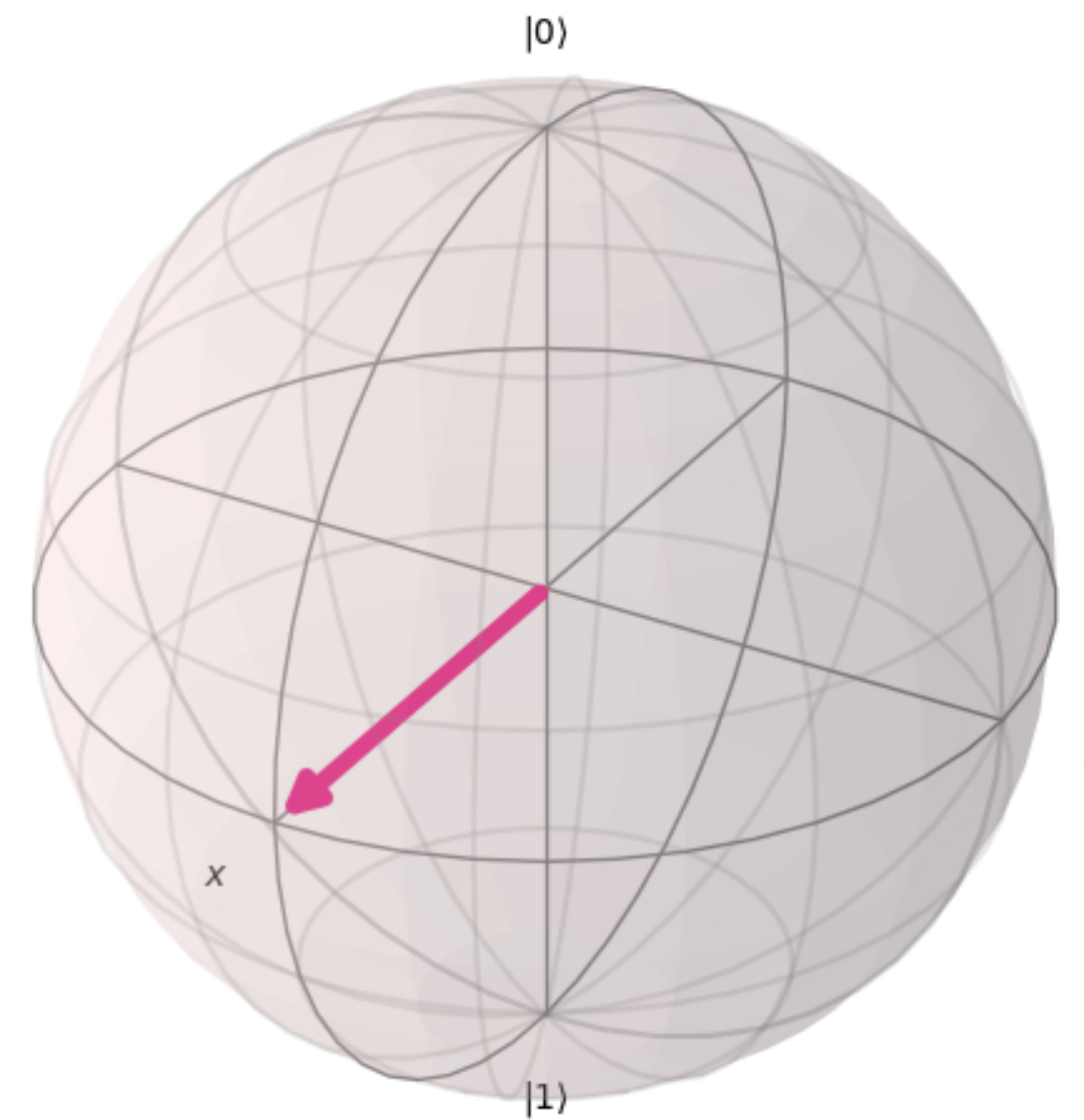


$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{matrix} |0\rangle \\ |1\rangle \end{matrix}$$

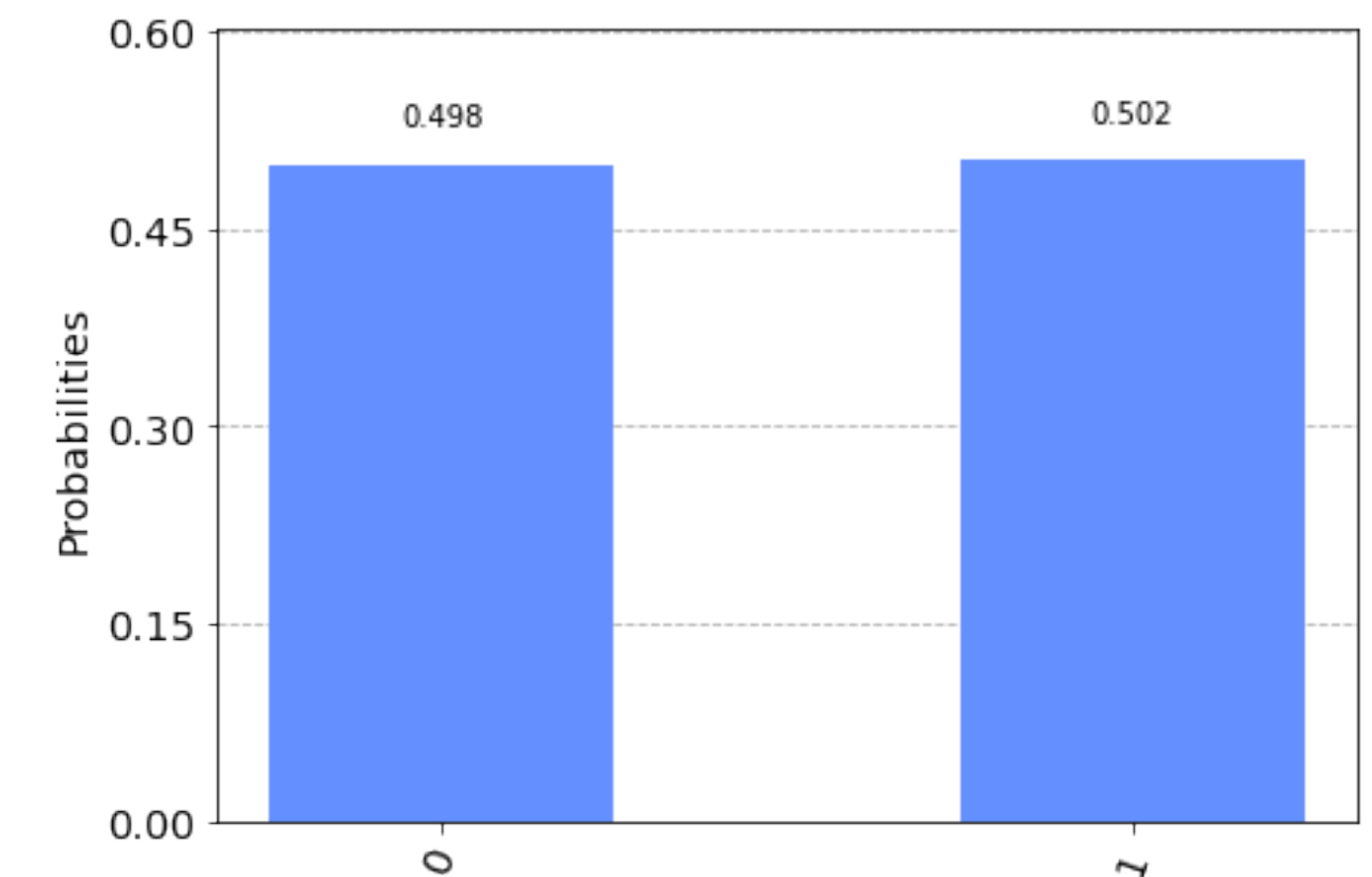
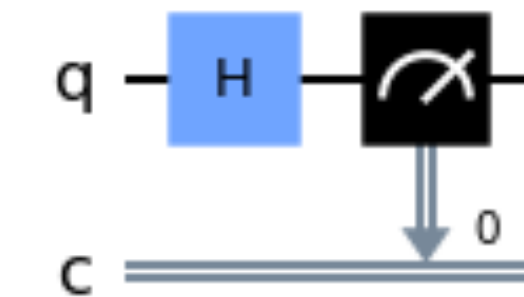


$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Initial (superposition) state

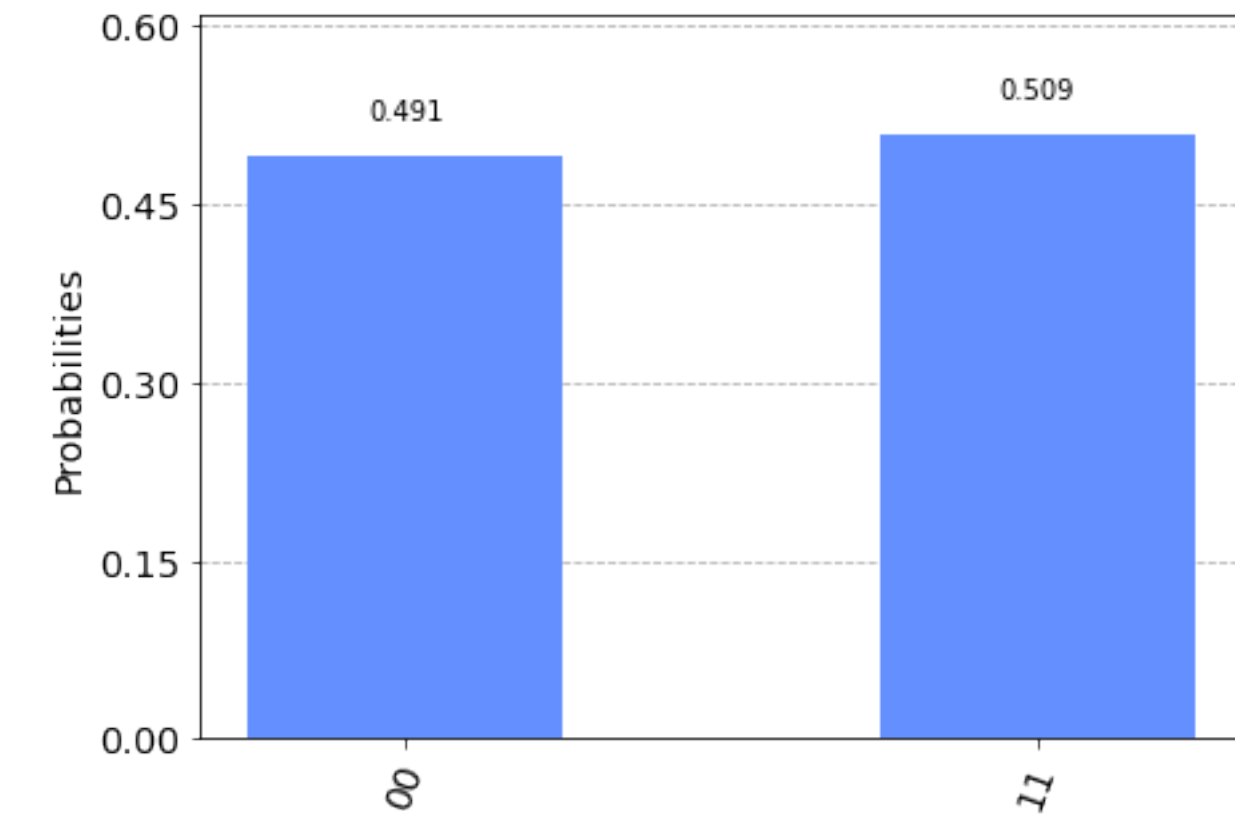
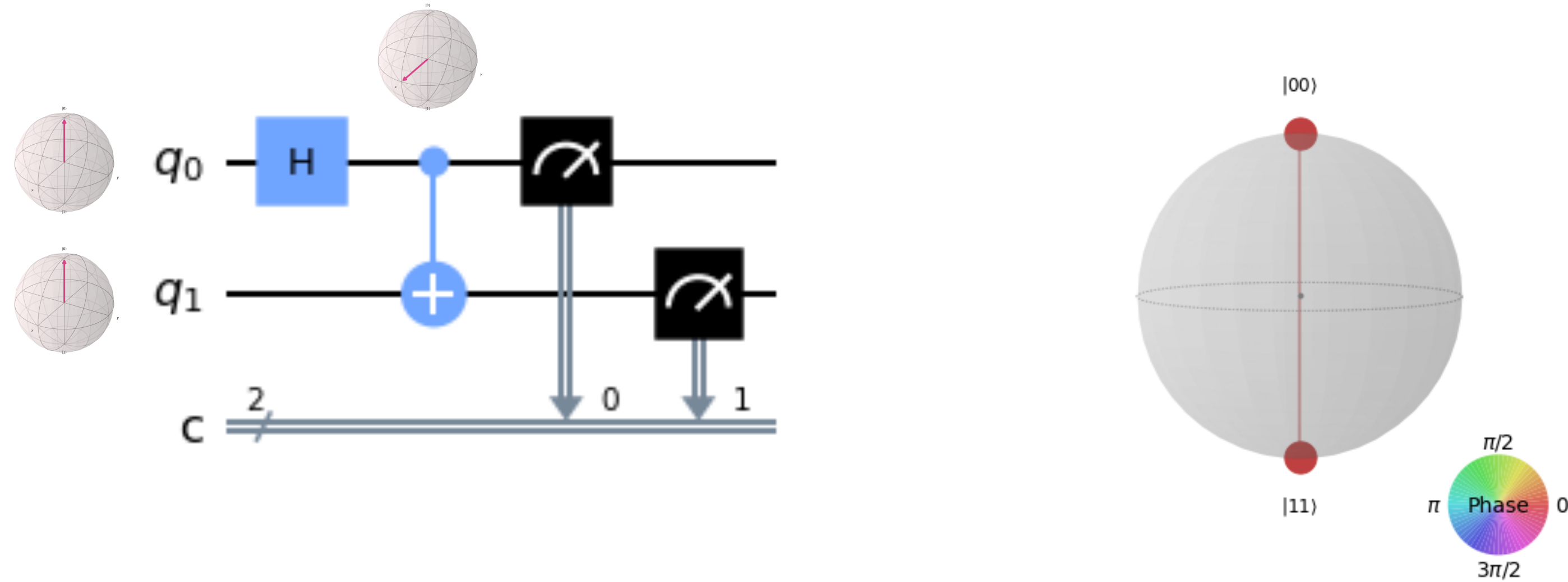


$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{matrix} |0\rangle \\ |1\rangle \end{matrix}$$



Superposition = "we have no clue what is going on ... superposition is really weird, but true" (MIT Quantum Physics 8.04)

Key concept 2: entanglement



$$C \left(H \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) = C \left(\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{matrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{matrix}$$

Quantum leaps
China's Micius satellite, launched in August 2016, has now validated across a record 1200 kilometers the "spooky action" that Albert Einstein abhorred (1). The team is planning other quantum tricks (2-4).

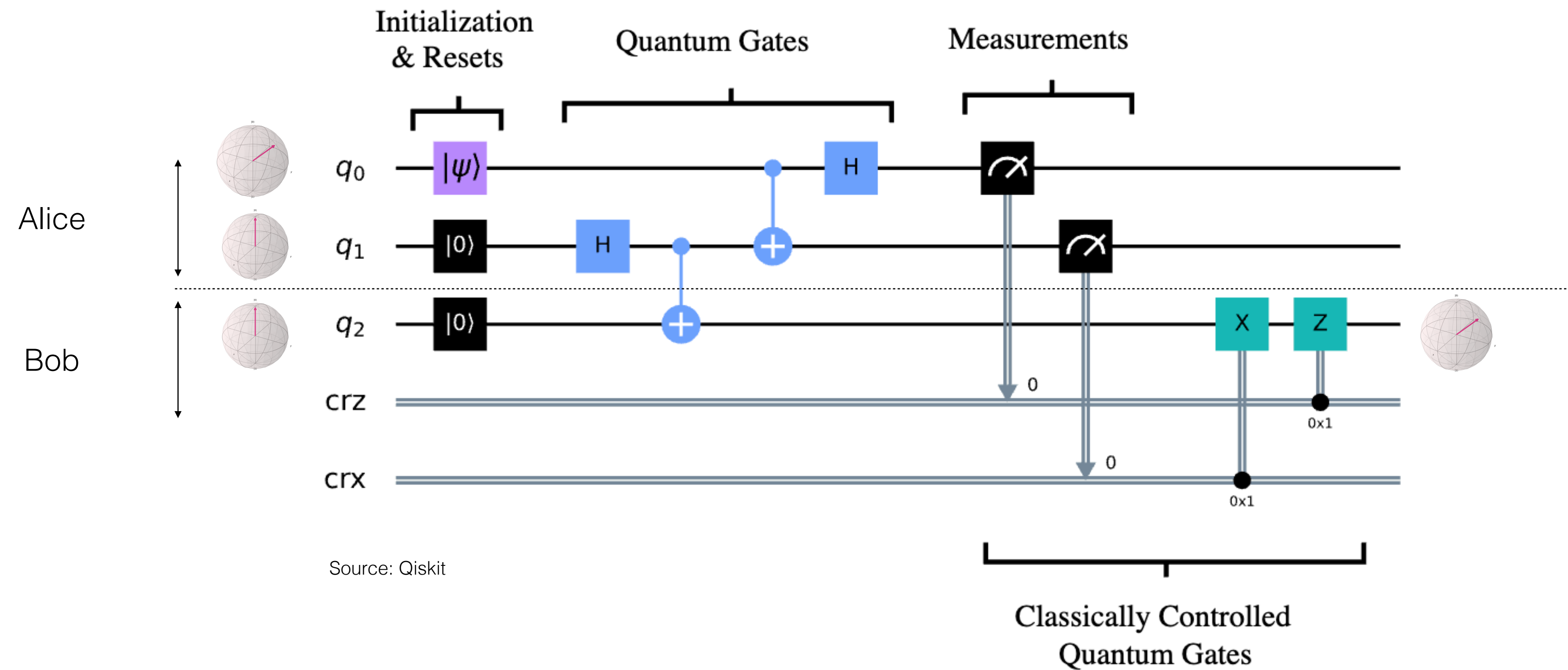
- 1. Spooky action**
Entangled photons were sent to separate stations. Measuring one photon's quantum state instantly determines the other's, no matter how far away.
- 2. Quantum key distribution**
Micius will send strings of entangled photons to the stations, creating a key for eavesdrop-proof communications.
- 3. Quantum teleportation**
Micius will send one entangled photon to Earth while keeping its mate on board. When a third photon with an unknown state is entangled with the one on Earth, and their states jointly measured, the properties of the last photon are instantly teleported up to Micius.
- 4. Global network**
Future satellites and ground stations could enable a quantum internet.

Labels in diagram: Light-altering crystal creates entangled photon pairs, Micius (500 km altitude), India, Ali observatory, Deilingha ground-station, Ejiang groundstation, China, Indian ocean.

"Spooky action at a distance" Einstein (source: [Wikipedia](https://en.wikipedia.org/wiki/Spooky_action_at_a_distance))

Source: [science.org](https://www.science.org)

Quantum teleportation



Code: [quantum teleportation Qiskit tutorial \(lecture video\)](#)

3. What are the problems ?

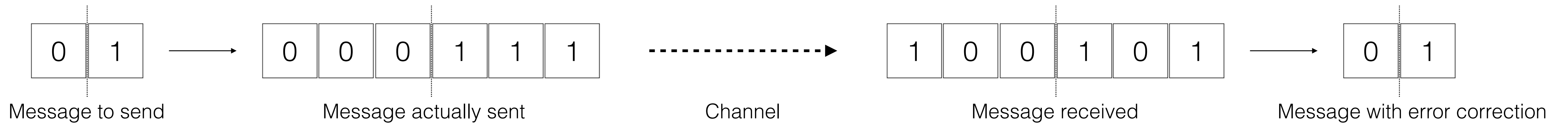
1. Noise (need for error correction)
2. Quantum decoherence
3. Scaling up

1. Noise / Error correction

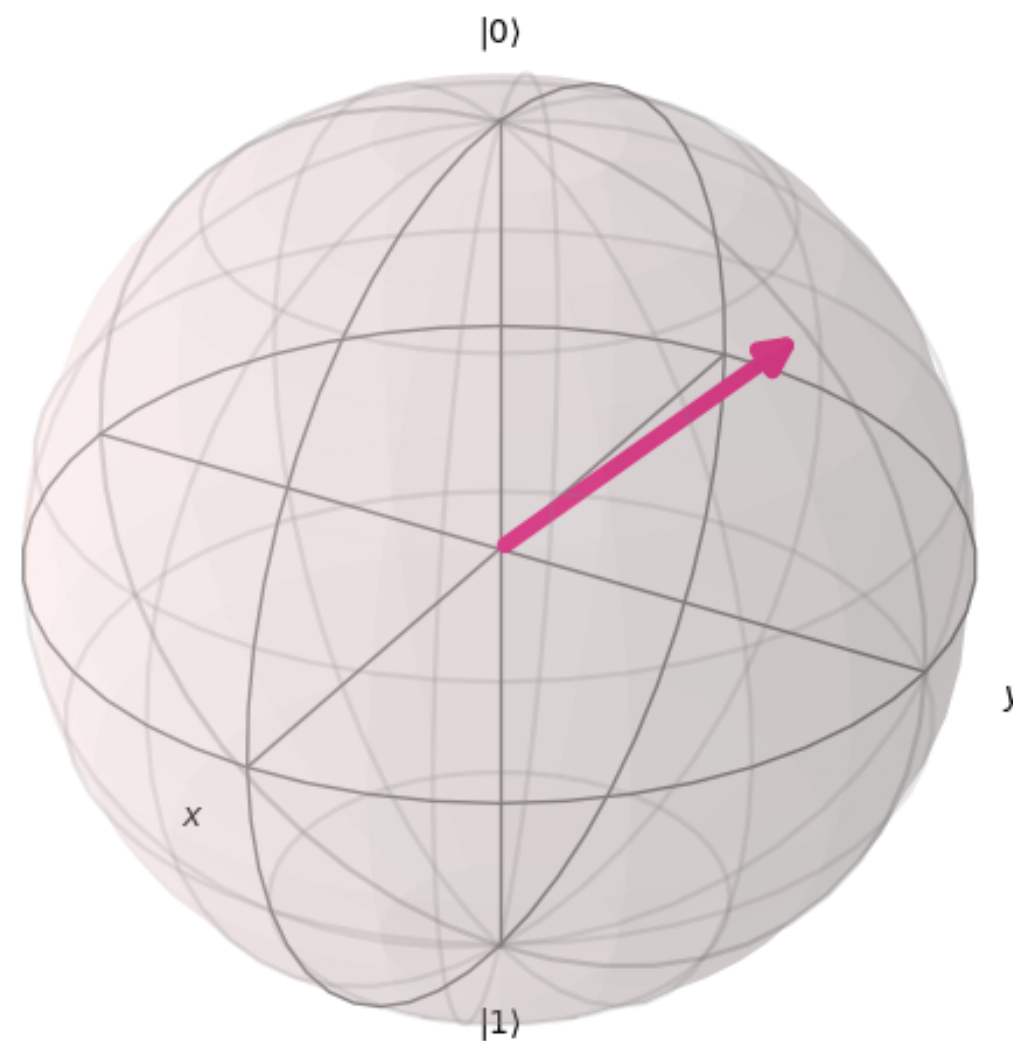
Classical computing (classical bit)

Basic error correction scheme:

3 physical bits sent for 1 logical bit of information



Quantum computing (quantum bit)

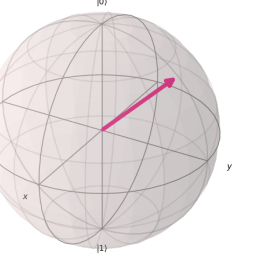


Vector of 2 complex values

Currently approx. 1,000 physical qubits for 1 logical qubit

Need for: Work on error correction schemes

2. Decoherence



Issue

After a very short time (milli to micro-seconds in a superconducting processor), qubits *lose* their coherence (*state*).

Impact

Circuits can only have a *limited number of gates* for a computation to remain meaningful

Find algorithms that require less gates.

Limit use of complex gates that need to be expressed (compiled into) multiple basis gates.

Need for

Limiting external noise (cryogenics / low temperature physics)

Limiting noise among qubits

...

3. Scaling up

Issue / fact

Today's quantum processors have in the order of *100* qubits

Factoring a 2,048 bit integer (Shor's algorithm / RSA cryptosystem) requires 4,000 logical (perfect) qubits,
Or approximately *4,000,000* of today's noisy (imperfect) physical qubits.

Each qubit adds noise for the other qubits

Each qubit is controlled by a co-axial cable (electromagnetic field)

Need for

Work on quantum error correction (needing less physical qubits to implement a logical qubit)

Architecture (how to arrange the qubits), limit noise from neighbouring qubits

...

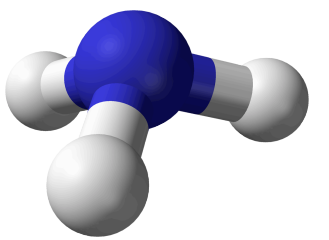
4. Potential future applications

Potential future applications

1. Cryptography: breaking encryption schemes (unlikely), quantum key distribution, ...
2. Chemistry & material science: simulating molecule behaviours, new drugs, materials, cheaper process for ammonia
3. Optimization: logistics, finance
4. Machine learning
5. Energy production

		Type of Algorithm	
		<i>classical</i>	<i>quantum</i>
Type of Data	<i>classical</i>	CC	CQ
	<i>quantum</i>	QC	QQ

Source: [Wikipedia](#)



Source: [Wikipedia](#)

Applied Quantum Computing Challenge program

Algorithms and simulations: advanced materials, biological systems, ...

Enabling technologies: efficient use and scaling, error correction, compiling, ...

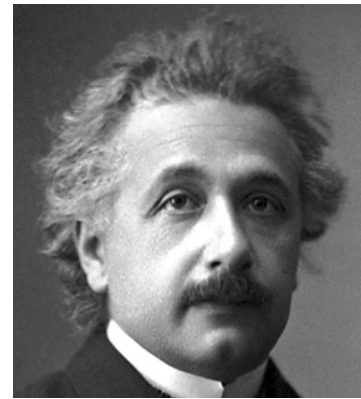
Canada's National Quantum Strategy: research, talent, commercialization

5. People / organizations involved ?

People involved in Quantum Computing

Theory

Theoretical physicist



Albert Einstein



Richard Feynman

Hardware

Quantum experimentalists

Cryogenics

Photonics

Superconductor

Engineer

Software

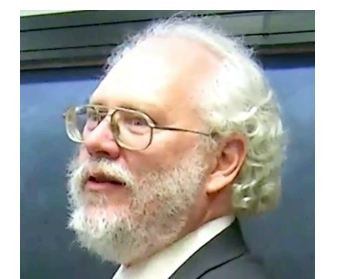
Computer scientist

Compiler, software packages

Domain expert (e.g. chemistry)

Algorithm development

Applied Mathematics



Peter Shor

All groups are working in parallel...

Canadian Universities



Institut Quantique



Computer Science and Operations Research



Cryptography and quantum information laboratory



Institute for quantum computing



Center for Quantum Information and Quantum Control



Institute for quantum science and technology



Silicon Quantum Technology Lab

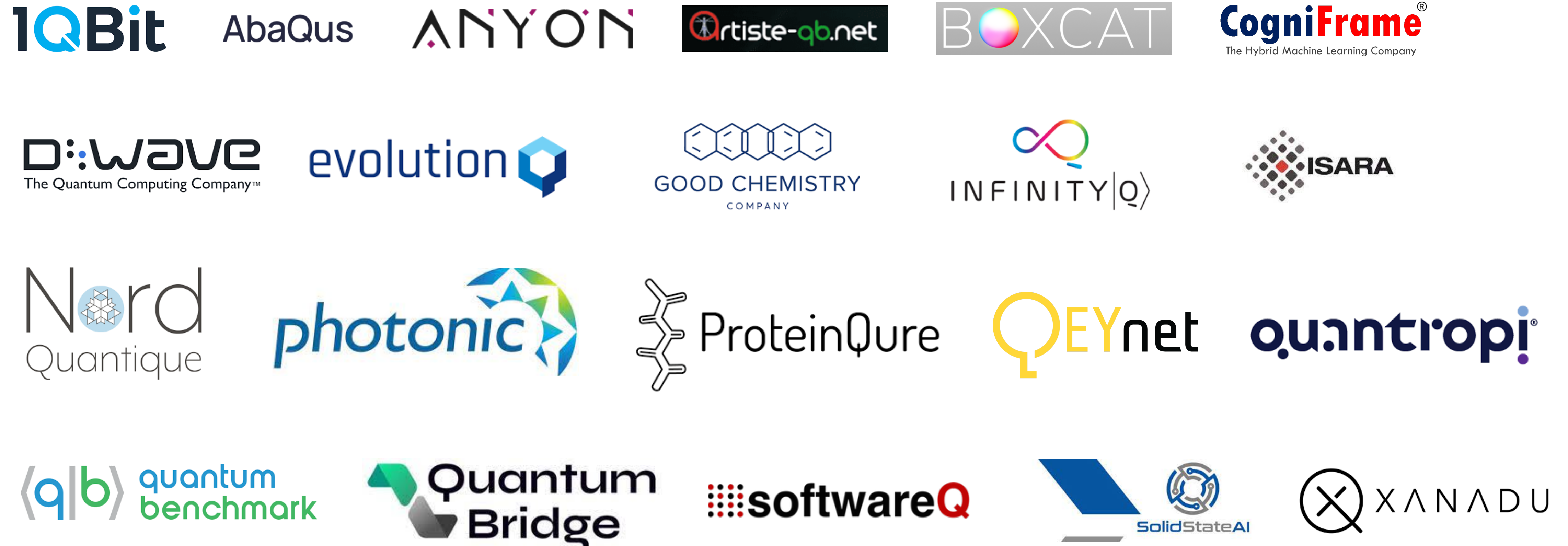


Quantum Information Theory

...

Canadian Companies

Companies involved in various aspects of quantum computing or proposing classical solutions to prepare for potential “quantum threat”.



...

State Of Canada Quantum Computing [2022]

6. Coding, playing, learning...

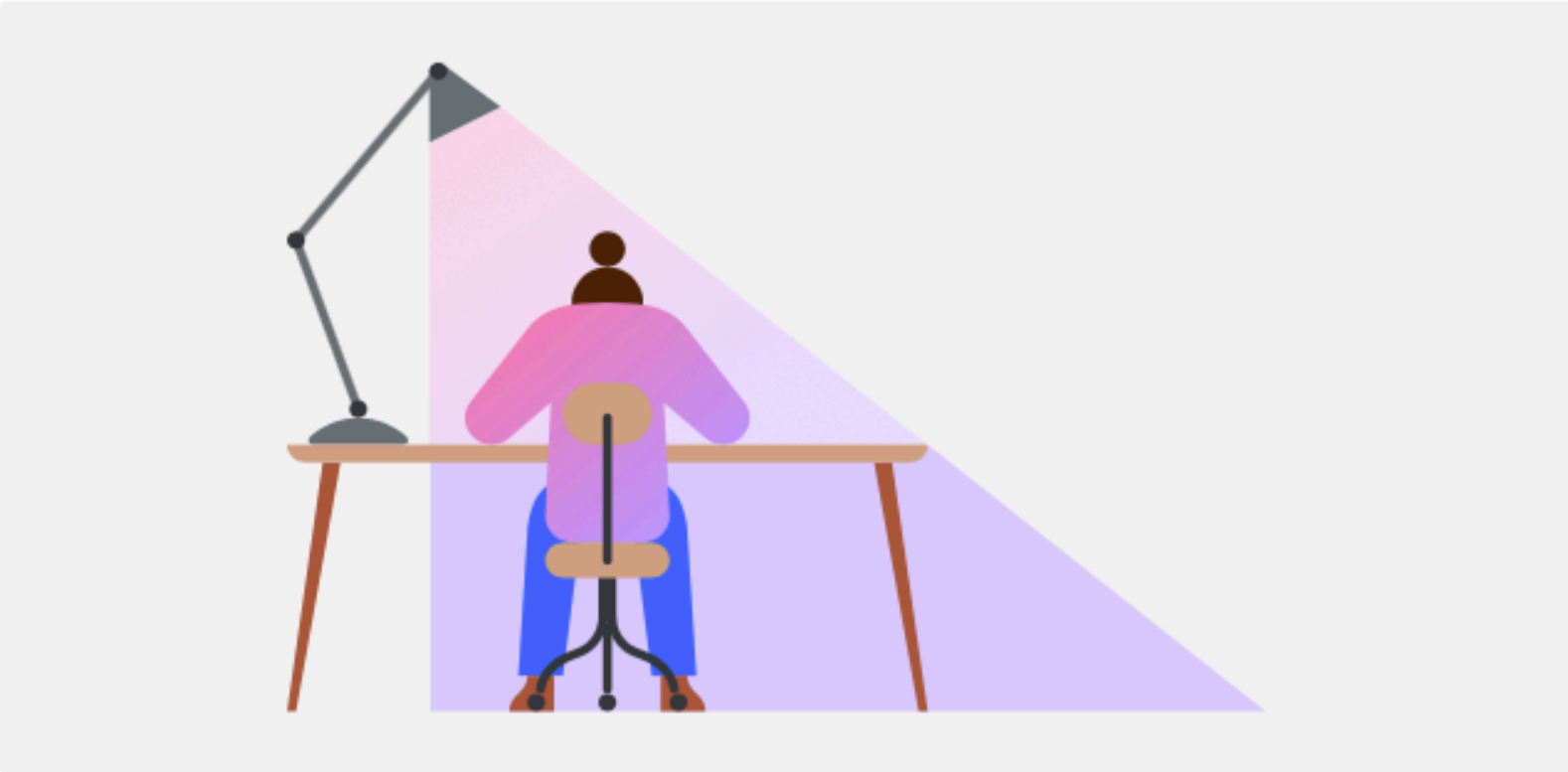
IBM Quantum Platform: learning, coding, testing

IBM Quantum Learning | Home Catalog Composer Lab

IBM Quantum Learning

Learn the basics of quantum computing, and how to use IBM Quantum services and systems to solve real-world problems.

Explore the latest course



Fundamentals of quantum algorithms

New

Use quantum computers to solve problems more efficiently, including problems with real-world relevance such as searching and factoring.

Lessons	Your progress
4	0%

Start course →

Courses

Learn about key concepts, algorithms, and their applications

[View all](#)

Basics of quantum information	Variational algorithm design	Practical introduction to quantum-safe cryptography
A detailed course covering mathematical aspects of quantum computing, comparable to an advanced undergraduate or introducto...	Today's hardware is delicate and error-prone. This course covers variational algorithms, which play to the strengths of these...	An introduction to quantum-safe cryptography, and how quantum computing poses a risk to existing cryptography.
Lessons 4	Lessons 7	Lessons 7
Start course →	Start course →	Start course →

<https://learning.quantum-computing.ibm.com>

IBM Quantum Platform - Compute Resources

Compute resources

Access IBM Quantum systems and simulators via our available access plans.

Your resources

All systems

All simulators

Card | Table

Search by system name

Sort, Filter icons

ibm_sherbrooke

System status ● Online - Queue paused maintenance

Processor type Eagle r3

Qubits QV CLOPS
127 32 904



ibm_kyiv

System status ● Online
Processor type Eagle r3

Qubits
127



ibm_brisbane

System status ● Online
Processor type Eagle r3

Qubits
127



ibm_nazca

System status ● Online
Processor type Eagle r3

Qubits
127



ibm_cusco

System status ● Online
Processor type Eagle r3

Qubits
127



ibm_ithaca

Exploratory

System status ● Online - Queue paused maintenance
Processor type Hummingbird r3

Qubits
65



ibm_prague

Exploratory

System status ● Offline internal
Processor type Egret r1

Qubits
33



ibm_algiers

System status ● Online
Processor type Falcon r5.11

Qubits QV CLOPS
27 128 2.2K



ibmq_kolkata

System status ● Online
Processor type Falcon r5.11

ibmq_mumbai

System status ● Online
Processor type Falcon r5.10

ibmq_cairo

System status ● Online
Processor type Falcon r5.11

ibmq_auckland

Exploratory

System status ● Online
Processor type Falcon r5.11

IBM Quantum Platform - Free compute resources

Compute resources

Access IBM Quantum systems and simulators via our available access plans.

Your resources

All systems

All simulators

You have access to the following systems with your IBM Quantum account.

Card | Table

Search by system or simulator name

Your systems & simulators (13)

Sort, Filter icons

ibm_perth

System status: Online
Processor type: Falcon r5.11H

Qubits: 7
QV: 32
CLOPS: 2.9K



ibm_lagos

System status: Online
Processor type: Falcon r5.11H

Qubits: 7
QV: 32
CLOPS: 2.7K



ibm_nairobi

System status: Online
Processor type: Falcon r5.11H

Qubits: 7
QV: 32
CLOPS: 2.6K



ibmq_jakarta

System status: Online
Processor type: Falcon r5.11H

Qubits: 7
QV: 16
CLOPS: 2.4K



ibmq_manila

System status: Online
Processor type: Falcon r5.11L

Qubits: 5
QV: 32
CLOPS: 2.8K



ibmq_quito

System status: Online
Processor type: Falcon r4T

Qubits: 5
QV: 16
CLOPS: 2.5K



ibmq_belem

System status: Online
Processor type: Falcon r4T

Qubits: 5
QV: 16
CLOPS: 2.5K



ibmq_lima

System status: Online
Processor type: Falcon r4T

Qubits: 5
QV: 8
CLOPS: 2.7K



simulator_stabilizer

Simulator status: Online
Simulator type: Clifford simulator

Qubits: 5000

simulator_mps

Simulator status: Online
Simulator type: Matrix Product State

Qubits: 100

simulator_extended_stabilizer

Simulator status: Online
Simulator type: Extended Clifford (e.g. Clifford+T)

Qubits: 63

ibmq_qasm_simulator

Simulator status: Online
Simulator type: General, context-aware

Qubits: 32

IBM quantum machines

ibmq_lima

Details

5 Qubits	Status: ● Online	Median CNOT error: 1.077e-2
8 QV	Total pending jobs: 224 jobs	Median SX error: 5.307e-4
2.7K CLOPS	Processor type ⓘ: Falcon r4T	Median readout error: 2.430e-2
	Version: 1.0.52	Median T1: 91.28 us
	Basis gates: CX, ID, RZ, SX, X	Median T2: 102.82 us
	Your usage: 0 jobs	Instances with access: 1 Instances ↓

Your upcoming reservations 0

Calibration data

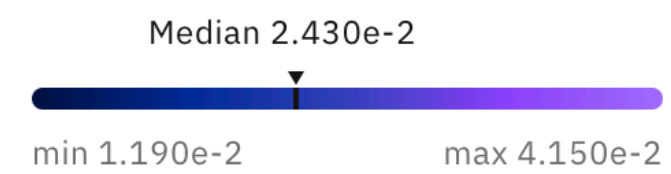
Last calibrated: about 24 hours ago

Map view | Graph view | Table view

[Collapse map view](#)

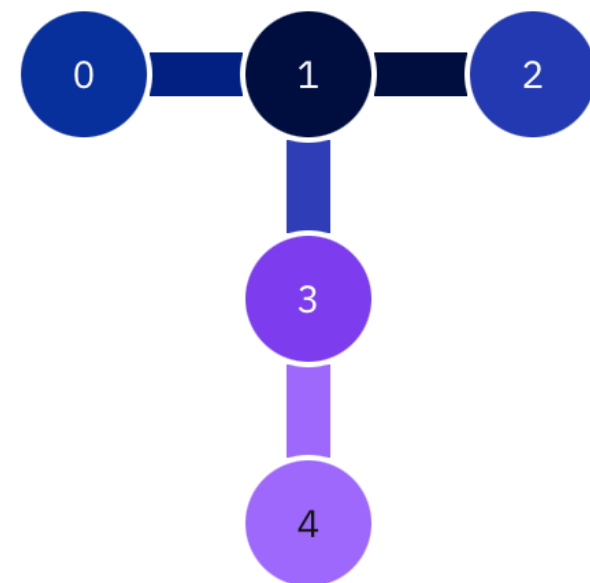
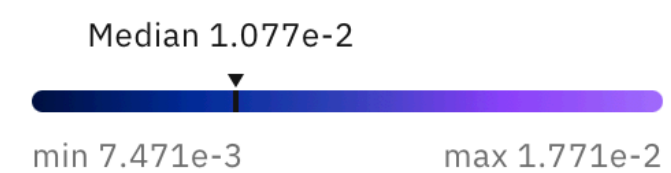
Qubit:

Readout assignment error



Connection:

CNOT error



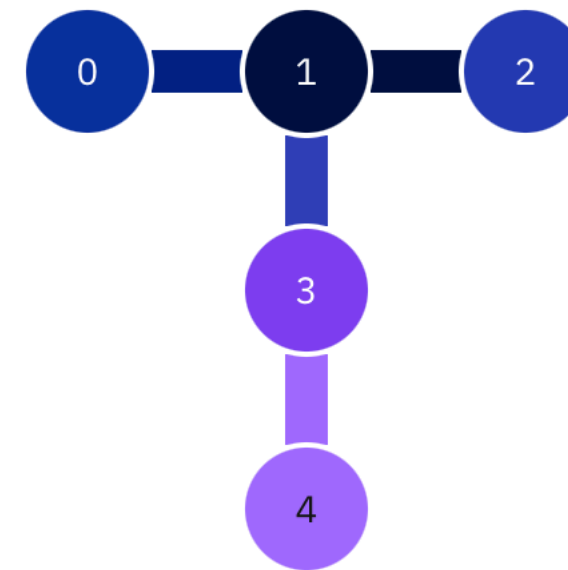
Available systems

- ✓ 7-qubit and 5-qubit QPUs ⓘ
- ✓ Simulators

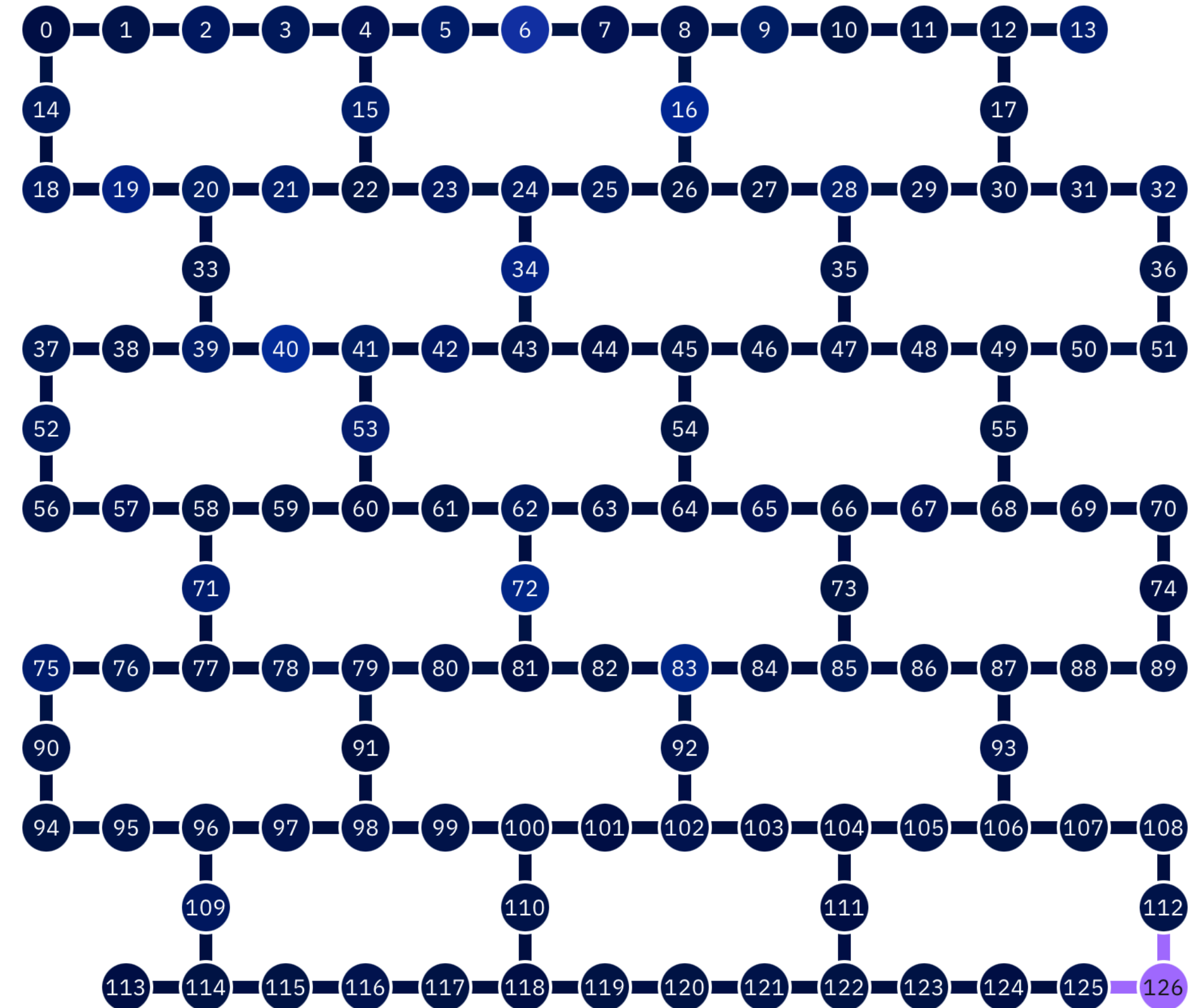
Available systems

- ✓ 433-qubit Osprey systems (coming soon) ⓘ
- ✓ 127-qubit Eagle systems ⓘ
- ✓ 27-qubit Falcon systems ⓘ
- ✓ Exploratory systems ⓘ
- ✓ Simulators

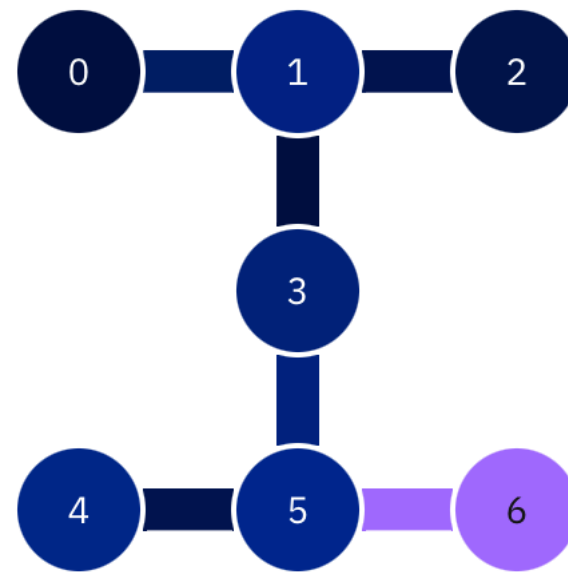
ibmq_lima (5 qubits)



ibmq_sherbrooke (127 qubits)



ibmq_lagos (7 qubits)



Sending jobs on a real quantum processor

The screenshot displays the IBM Quantum Learning interface. The top navigation bar includes 'Home', 'Catalog', 'Composer', and 'Lab'. The main workspace is titled 'entanglement Saved' and contains a quantum circuit with two qubits, q[0] and q[1], and a classical register c2. The circuit includes an H gate on q[0], a CNOT gate with q[0] as control and q[1] as target, and Z gates on both qubits. The circuit is visualized in the 'Operations' panel and the 'Q-sphere' panel. The 'Probabilities' panel shows a bar chart with two bars at 50% for states 00 and 11. The 'Status timeline' on the left shows the job is 'Queued'. The 'Details' section on the left provides information about the job, including the compute resource 'ibm_perth', the instance 'ibm-q/open/main', and the program 'sampler'. The 'Code' panel on the right shows the Qiskit code for the circuit.

Jobs / cm70m6gbxrbg0089hqq0

Compute resource: [ibm_perth](#)

Status timeline: Queued

- Created: Sep 22, 2023 5:41 PM
- In queue
- Running
- Estimated usage: 7.6s
- Completed

Details

Sent from: [entanglement](#)

Created on: Sep 22, 2023 5:41 PM

Instance: [ibm-q/open/main](#)

Program: [sampler](#)

Operations

Search

q[0] H CNOT Z

q[1] CNOT Z

c2

Probabilities

Computational basis states	Probability (% of 1024 shots)
00	50
01	0
10	0
11	50

Q-sphere

Phase

State Phase angle

```
1 from qiskit import QuantumRegister, ClassicalRegister, QuantumCircuit
2 from numpy import pi
3
4 qreg_q = QuantumRegister(2, 'q')
5 creg_c = ClassicalRegister(2, 'c')
6 circuit = QuantumCircuit(qreg_q, creg_c)
7
8 circuit.h(qreg_q[0])
9 circuit.cx(qreg_q[0], qreg_q[1])
10 circuit.measure(qreg_q[0], creg_c[0])
11 circuit.measure(qreg_q[1], creg_c[1])
```

Experiment sent to ibm_perth

ibm_perth

OpenQASM 3

32

QV

2.9K

CLOPS

Processor type: Falcon r5.11H

Version: 1.2.8

Basis gates: CX, ID, RZ, SX, X

Your usage: 1 job

Median readout error: 2.770e-2

Median T1: 154.74 us

Median T2: 112.25 us

Instances with access: 1 Instances ↓

Your upcoming reservations 0

Calibration data

Last calibrated: 30 minutes ago

Map view

Graph view

Table view

Expand map view

Qubit:

Readout assignment error

Median 2.770e-2

min 1.300e-2

max 3.120e-2

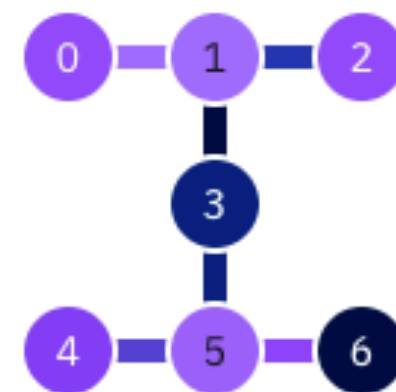
Connection:

CNOT error

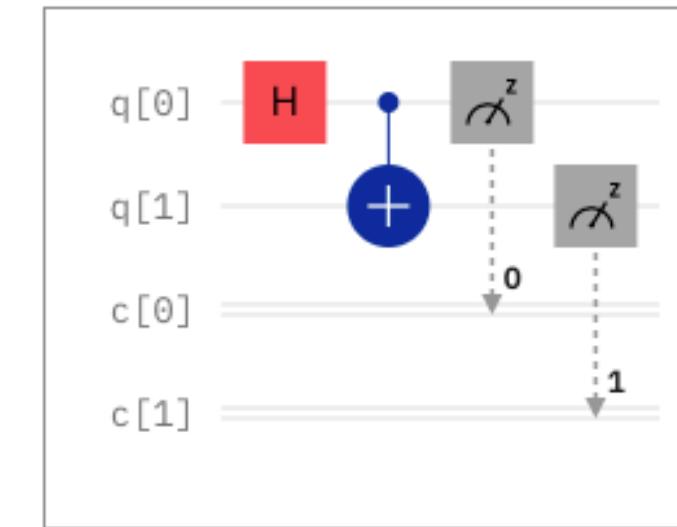
Median 1.151e-2

min 4.424e-3

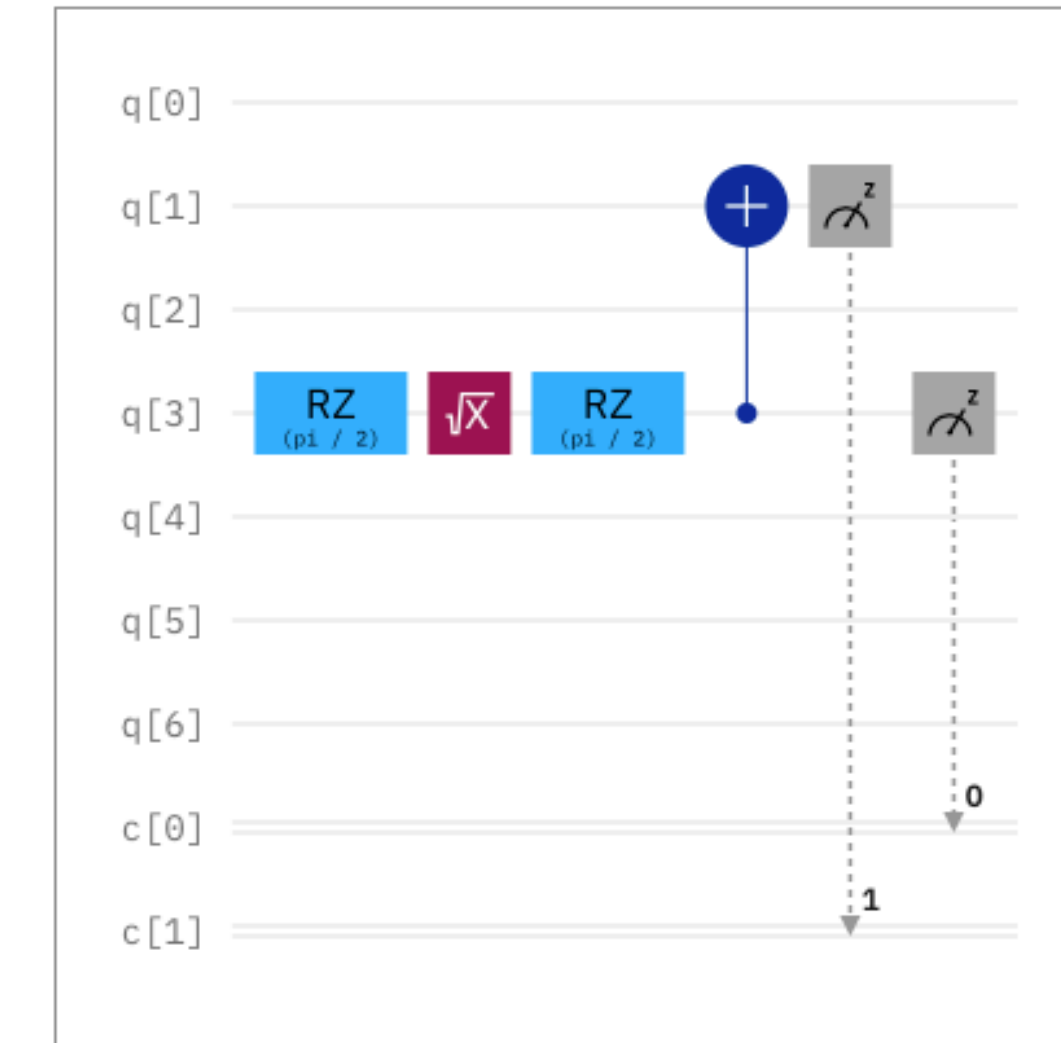
max 1.857e-2



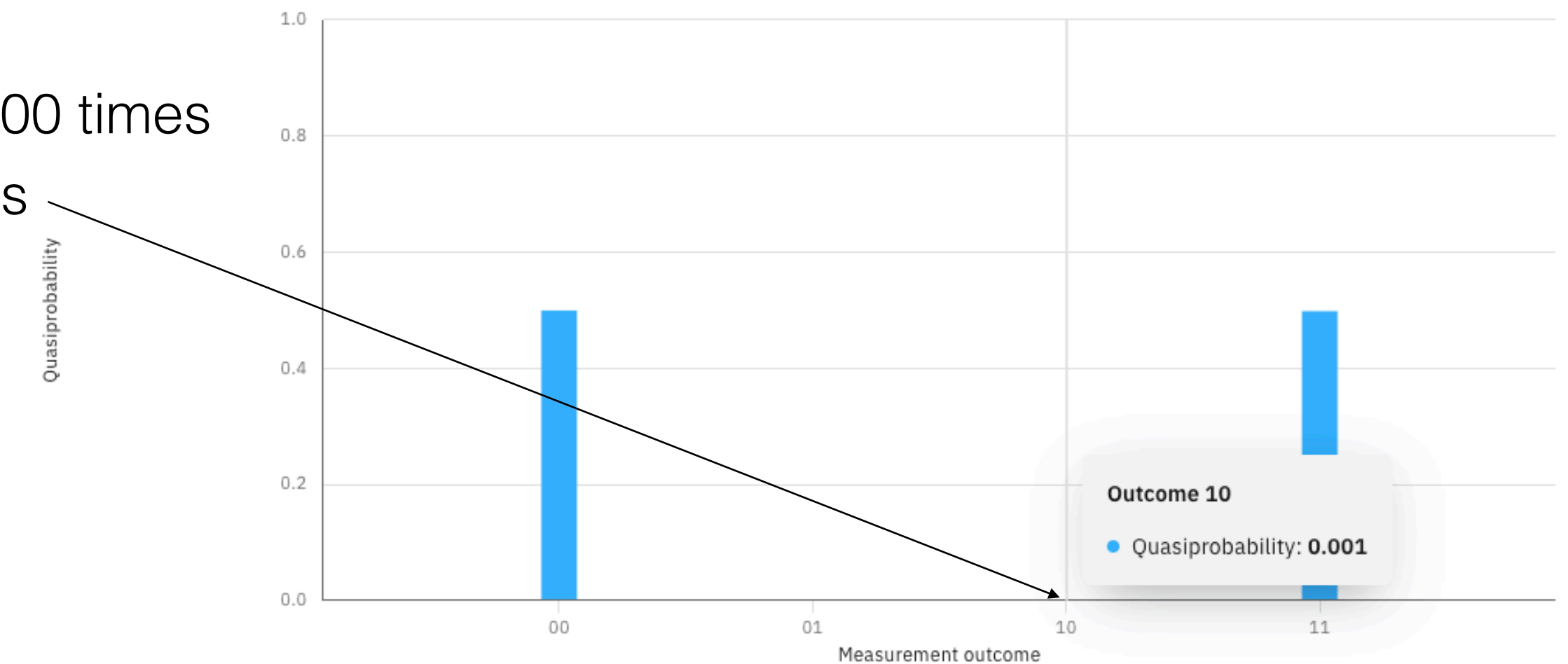
Original circuit



Transpiled circuit



Quasiprobability distribution



Experiment (circuit) run 1,000 times
1 error out of 1,000 trials

7. Where can I learn more ?

IBM Quantum Learning [Courses, tutorials, videos \(YouTube channel\), summer schools, challenges, ...](#) IBM Quantum **Platform**

 **Qiskit** “open-source software development kit (SDK) for working with quantum computers” ([wikipedia](#))



 **MIT OPEN COURSEWARE** Quantum physics I (8.04)
MASSACHUSETTS INSTITUTE OF TECHNOLOGY



[1 year quantum course](#) for high school students & above (course created by researchers @ Berkeley, MIT, Oxford)



“nonprofit striving to connect and teach young individuals about quantum computing”



Numerous university courses from Stanford, UofT, UBC, Purdue, EPFL, X, ...

[Looking Glass Universe \(Youtube channel\)](#)

[Quantum Computing Expert Explains One Concept in 5 Levels of Difficulty](#)

Summary

A quantum processor will *never* replace a classical computer

“any computational problem that can be solved by a quantum computer can also be solved by a classical computer” (IBM)

“*might provide faster solutions to some computational problems*” (IBM); e.g. modelling molecules (quantum chemistry)

Still very early stage... quantum mechanics (100 years old), idea to build a quantum processor (40 years old)

Governments are preparing: education, research, commercialization

Preparing for quantum resistant encryption algorithms (just in case, better be prepared than sorry)

Large companies, banks, governments are experimenting / learning on potential use cases with current error prone quantum processors

Notation, varia, ...

IBM fundamentals of quantum computing

“might provide *faster* solutions to some computational problems”

“may allow us to solve certain computational problems that classical computers are too slow to solve”

“any computational problem that can be solved by a quantum computer can also be solved by a classical computer”

States of a classical bit

X : system being considered e.g. a bit

$\Sigma = \{0,1\}$ possible states assumed by the bit

Probabilistic state: Assume we believe X is in state 0 with probability $3/4$ (resp. in state 1 with prob. $1/4$)

$$\begin{pmatrix} \frac{3}{4} \\ \frac{1}{4} \end{pmatrix} \begin{matrix} 0 \\ 1 \end{matrix}$$

Measuring probabilistic states

“we can never “see” a system in a probabilistic state” (source: [IBM Quantum learning](#))

“a measurement will yield exactly one of the allowed classical states” (source: [IBM Quantum learning](#))

We see either state 0 and state 1 (standard basis vector)

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} \frac{3}{4} \\ \frac{1}{4} \end{pmatrix} = \frac{3}{4} |0\rangle + \frac{1}{4} |1\rangle$$

Flip of a fair coin

Example: a flip of a fair coin has equal probability to fall on heads and tails

Original probabilistic state: $\begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix} = \frac{1}{2} \text{heads}\rangle + \frac{1}{2} \text{tails}\rangle$

State set of a coin: $\Sigma = \{\text{heads}, \text{tails}\}$

Observed state: either $\text{heads}\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ or $\text{tails}\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Quantum systems behave in an analogous way: observed states are one of the basic states (not a combination)

Deterministic operations (matrix vector multiplication)

Deterministic operations on probabilistic states can be represented as a *matrix vector multiplication*.

$$\text{E.g. NOT operation: } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{If applied on state } \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{Results in } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Bra notation: $\langle a$ for **row vectors**

$\langle a$ is the row vector having a 1 in entry corresponding to a and 0 elsewhere

For $\Sigma = \{0,1\}$, we have $\langle 0 = (1 \ 0)$ and $\langle 1 = (0 \ 1)$

Ket notation: $|a\rangle$ for **column vectors**

$|a\rangle$ is the column vector having a 1 in entry corresponding to a and 0 elsewhere

For $\Sigma = \{0,1\}$, we have $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Quantum state vectors

Indices label the classical states of the system; e.g. for 3-bit system:

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \\ \alpha_5 \\ \alpha_6 \\ \alpha_7 \end{pmatrix} \begin{matrix} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{matrix}$$

1. **The entries α_i are complex numbers**

2. The sum of absolute values squared of entries α_i equals 1: $\sum_i |\alpha_i|^2 = 1$

Quantum state vectors are unit vectors (Euclidean norm of 1.0)

Example of a qubit state

$$|\psi\rangle = \begin{pmatrix} \frac{1+2i}{3} \\ \frac{-2}{3} \end{pmatrix} = \frac{1+2i}{3} |0\rangle - \frac{2}{3} |1\rangle$$

Measuring quantum states (*standard basis* measurement)

“measurements act as the interface between quantum and classical information” (source: [IBM learning](#))

each classical state results with probability equal to absolute value squared of the entry

E.g. a 3 bit quantum state: the classical state **010** appears with probability α_2^2

$$\psi = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \\ \alpha_5 \\ \alpha_6 \\ \alpha_7 \end{pmatrix} \begin{matrix} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{matrix}$$

Unitary matrix operations (reversible) on a single qubit

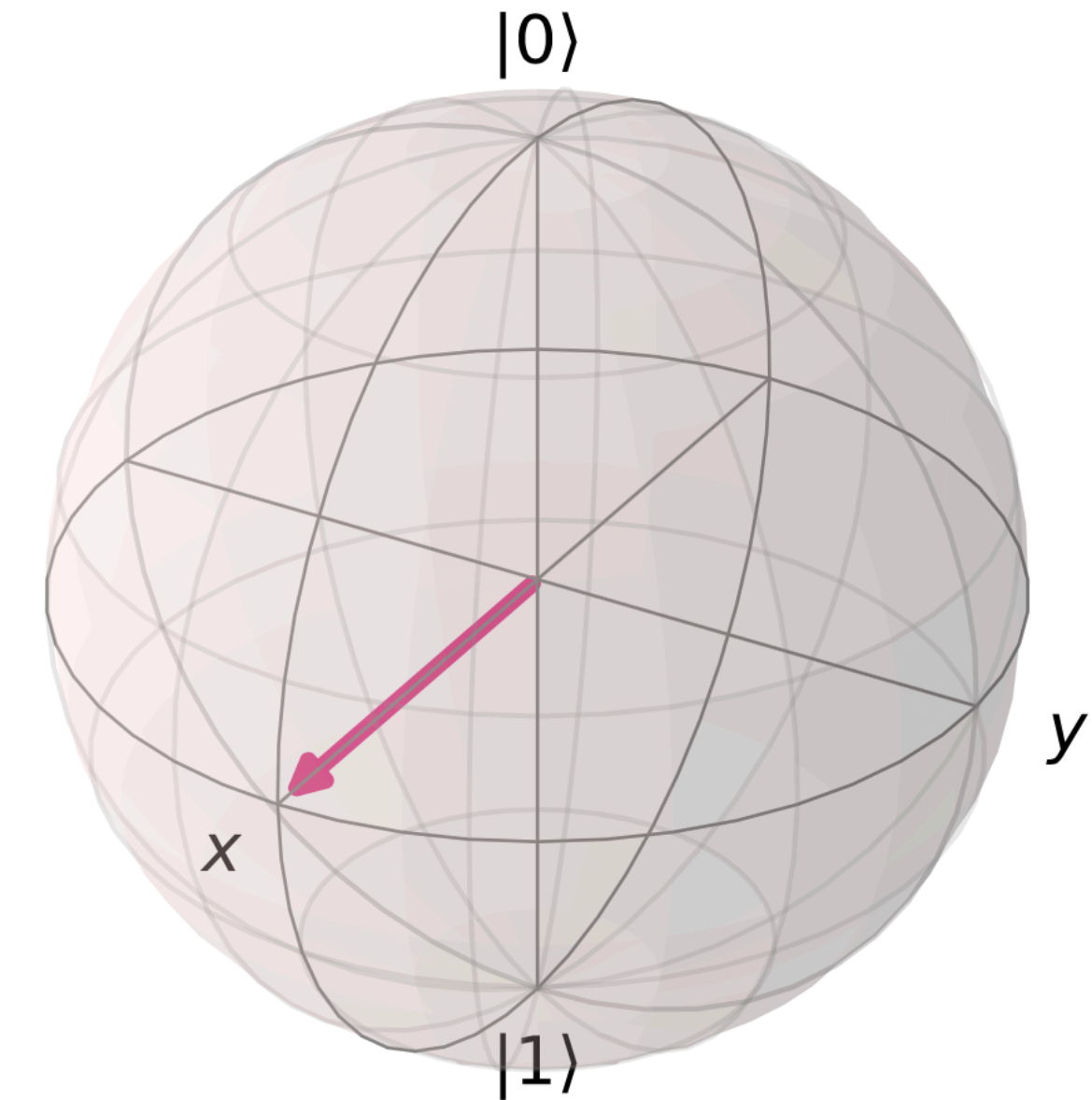
Pauli operations

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_x/X = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_y/Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z/Z = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$$

identity

NOT (bit flip)

phase flip



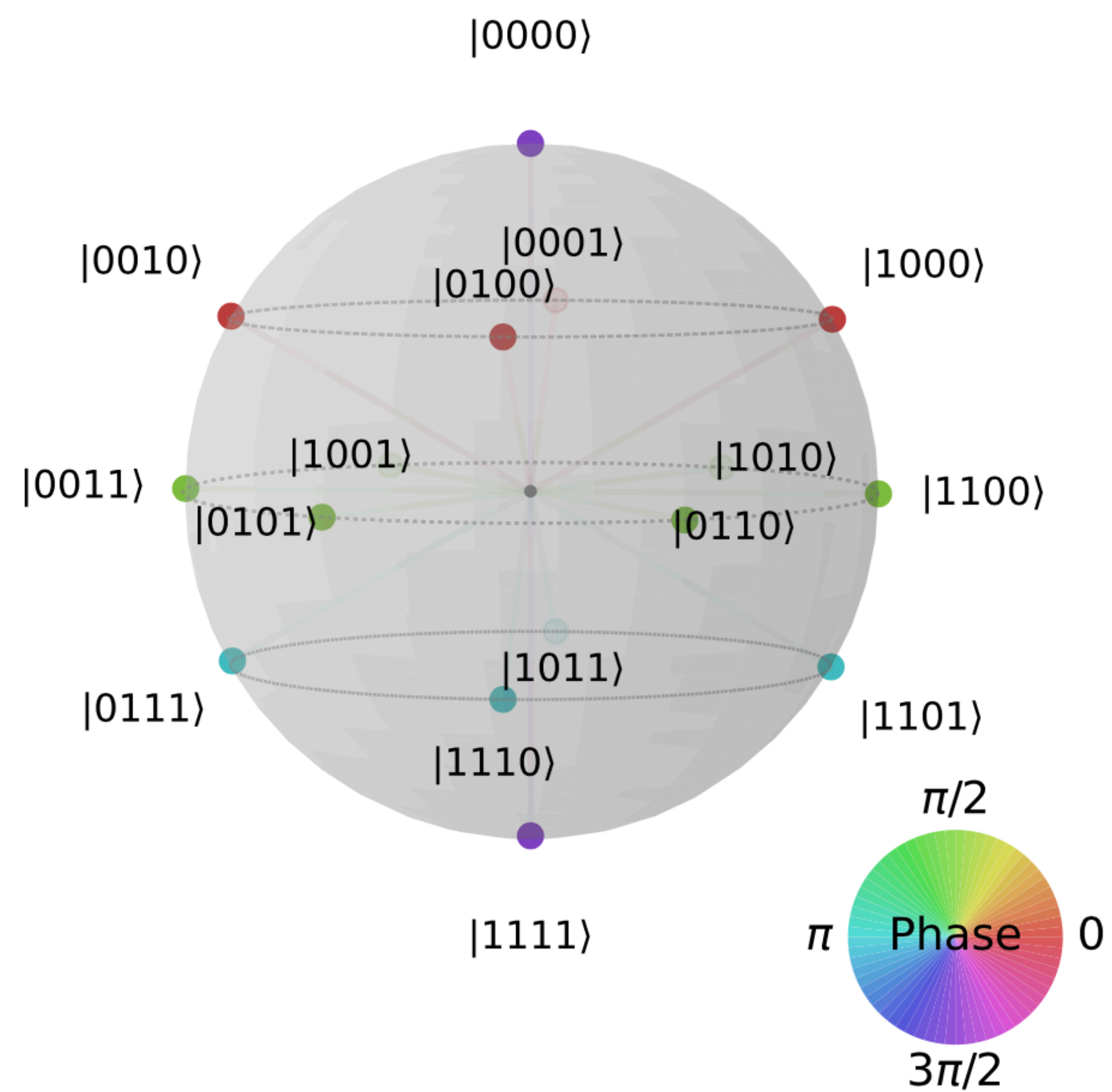
Hadamard operation

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Phase operations

$$P_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \quad \text{e.g.} \quad S = P_{\pi/2} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad T = P_{\pi/4} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{pmatrix}$$

Representation of multi qubit states using Bloch sphere



A tautology, obviously true, proved with logic and integers

$$N(A, \bar{B}) + N(B, \bar{C}) \geq N(A, \bar{C})$$

$$N(A, \bar{B}, C) + N(A, \bar{B}, \bar{C}) + N(A, B, \bar{C}) + N(\bar{A}, B, \bar{C}) \geq N(A, B, \bar{C}) + N(A, \bar{B}, \bar{C})$$