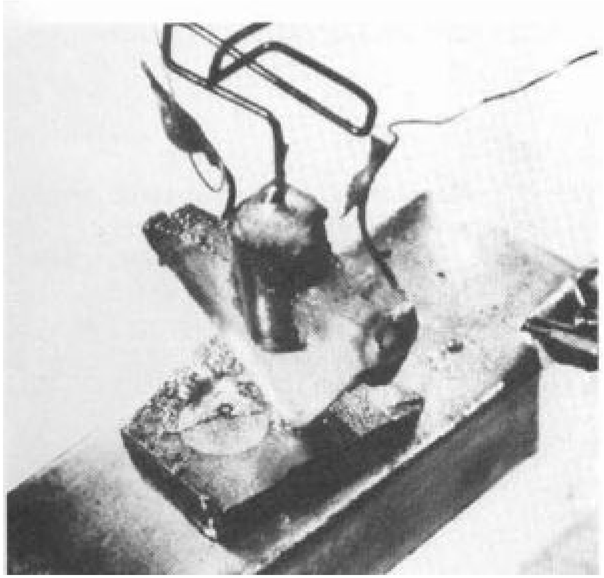
Introduction:
The weird world of quantum information

What would you do with a 1000 qubits?

Fantastic story of classical computing

1947



1981

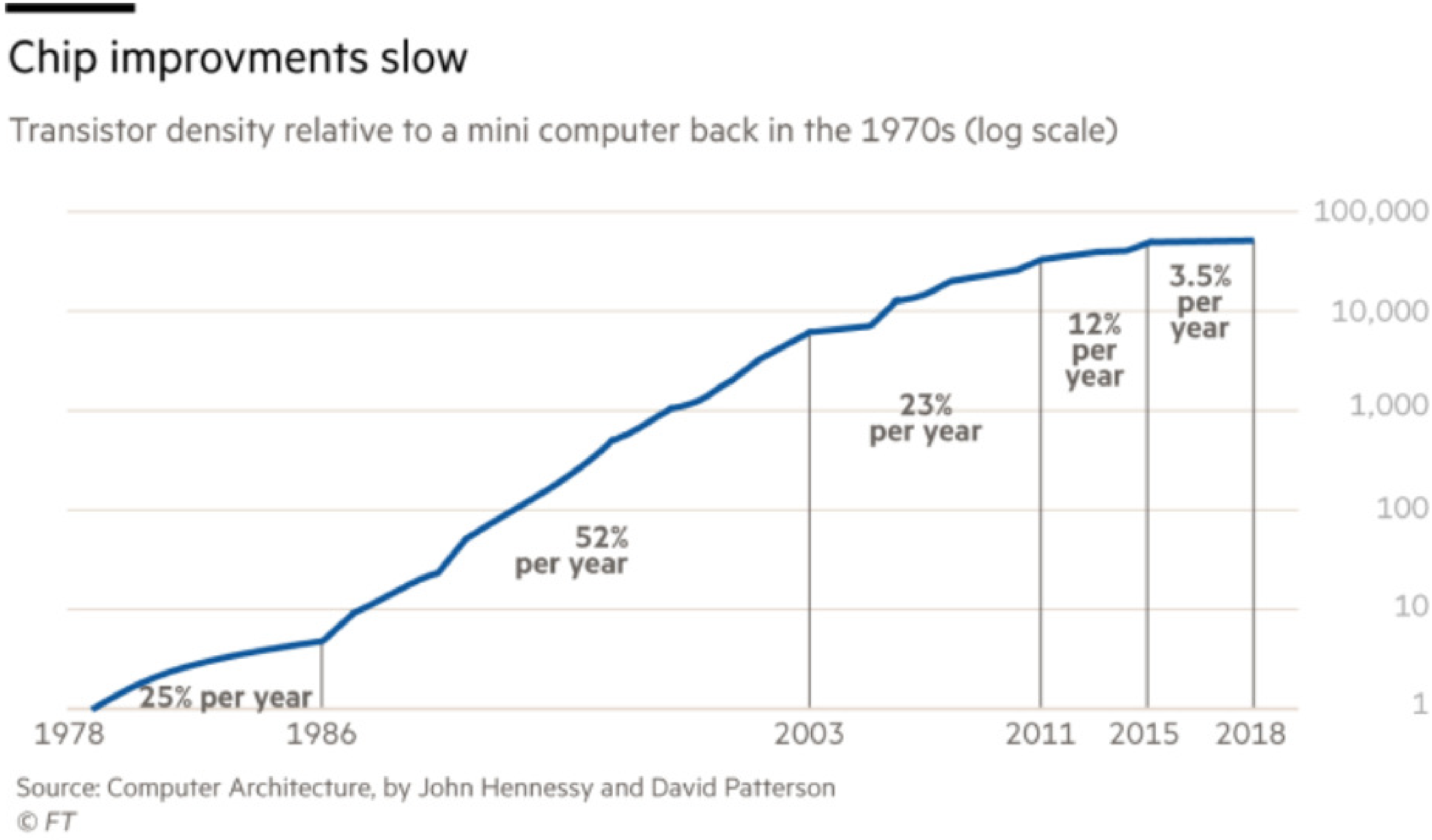
2010s

Picture sources: ethw.org/Transistors, wiki/IBM_Personal_Computer, wiki/Floppy_disk, wiki/ThinkPad, wiki/Supercomputer, realtechexperts.com/advantages-of-internet-in-entertainment/

The end of Moore's law

Moore's law: the number of transistors in a dense integrated circuit doubles about every two years

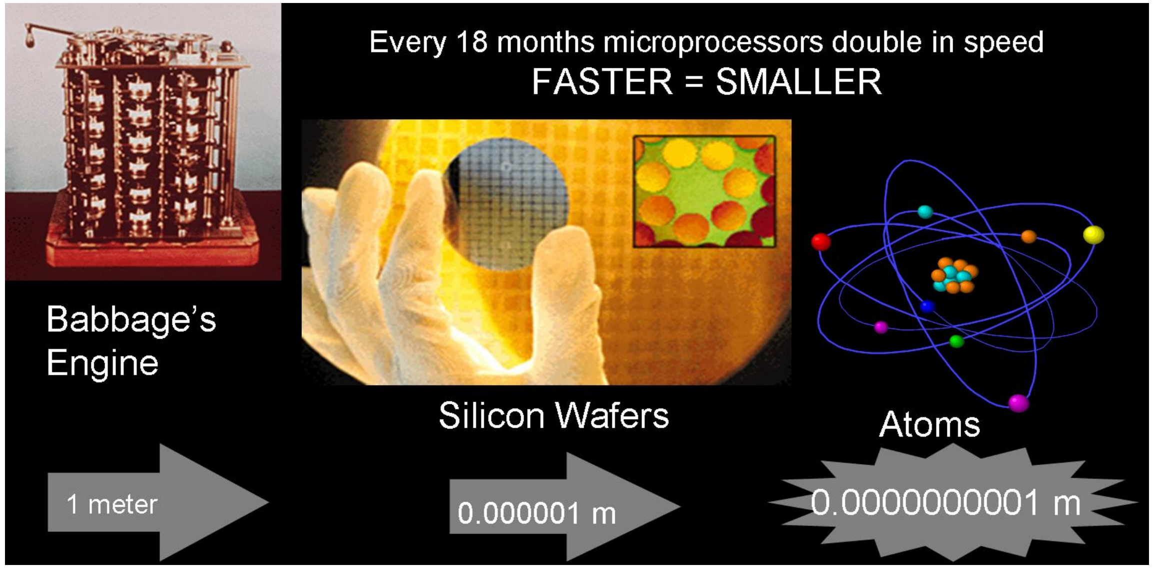
Gordon Moore, 1965



Transistor density: average number of transistors per unit area

Information is physical

Any processing of information
is always performed by physical means



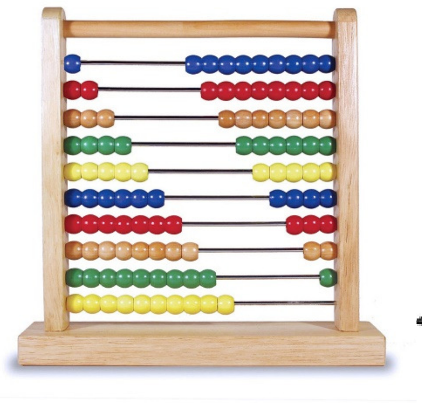
Bits of information obey laws of classical physics.

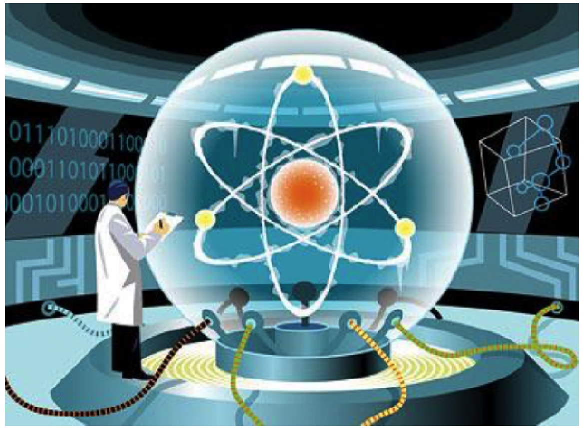
The nearest neighbor distance in Si lattice is 0.235 nm – gate size of 2 nm means 10 Si atoms.

Why Quantum Computers?

Computer technology is making devices smaller and smaller…

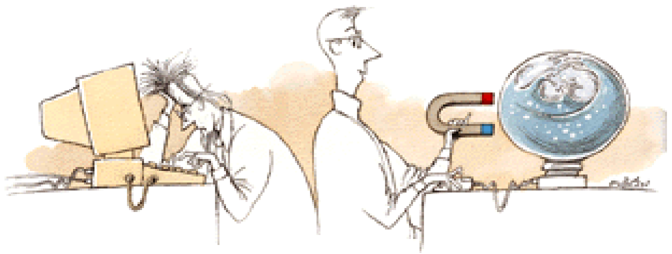
…reaching a point where classical physics is no longer a suitable model for the laws of physics.





- Many problems are intractable on classical computers (no efficient algorithms to solve them).
- Quantum simulation

Bits & Qubits



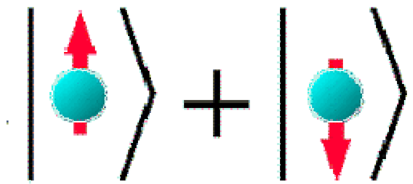
Fundamental building blocks of classical computers:

BITS

STATE:
Definitely
0 or 1

Fundamental building blocks of quantum computers:

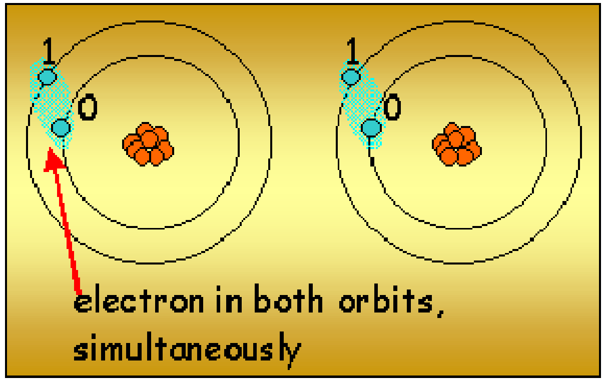
Quantum bits
or
QUBITS



Basis states: $|0\rangle$ and $|1\rangle$

Superposition:

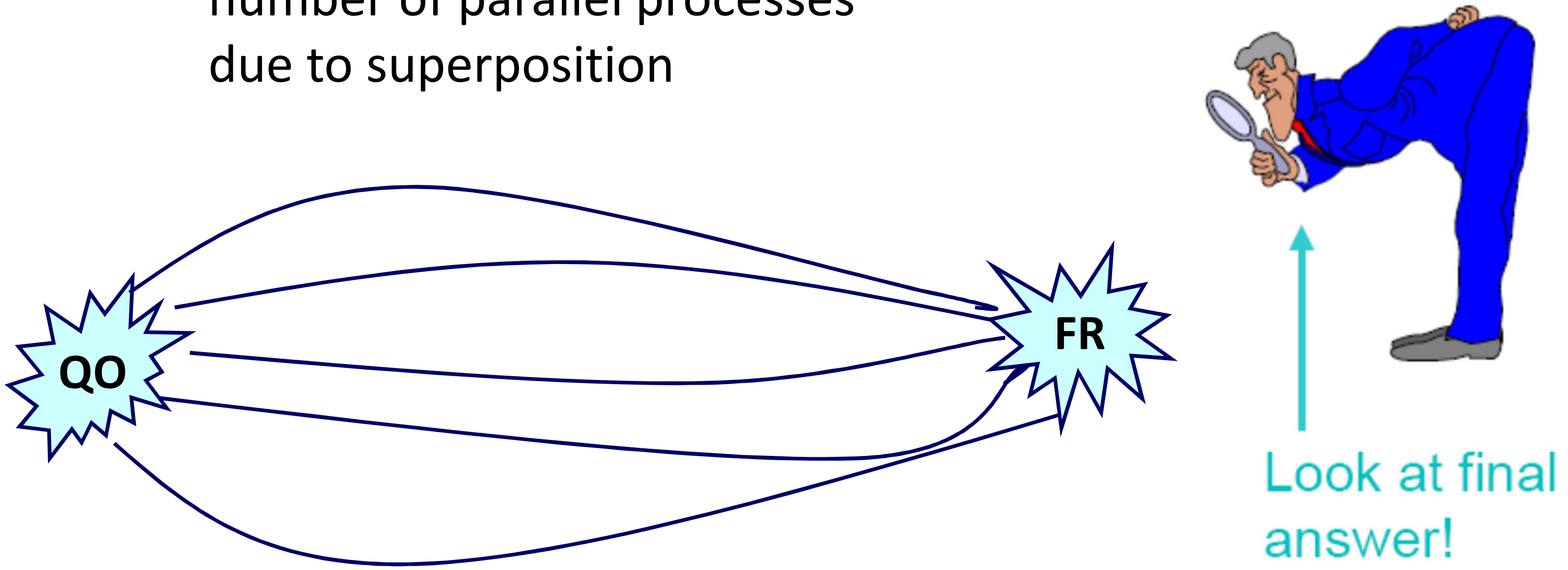
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$



Qubits: measurement

Measurement

- Classical bit: we can find out if it is in state 0 or 1 and the measurement will not change the state of the bit.
- Qubit: Quantum calculation:
  number of parallel processes
  due to superposition



Bits & Qubits: primary differences

- **Superposition**

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

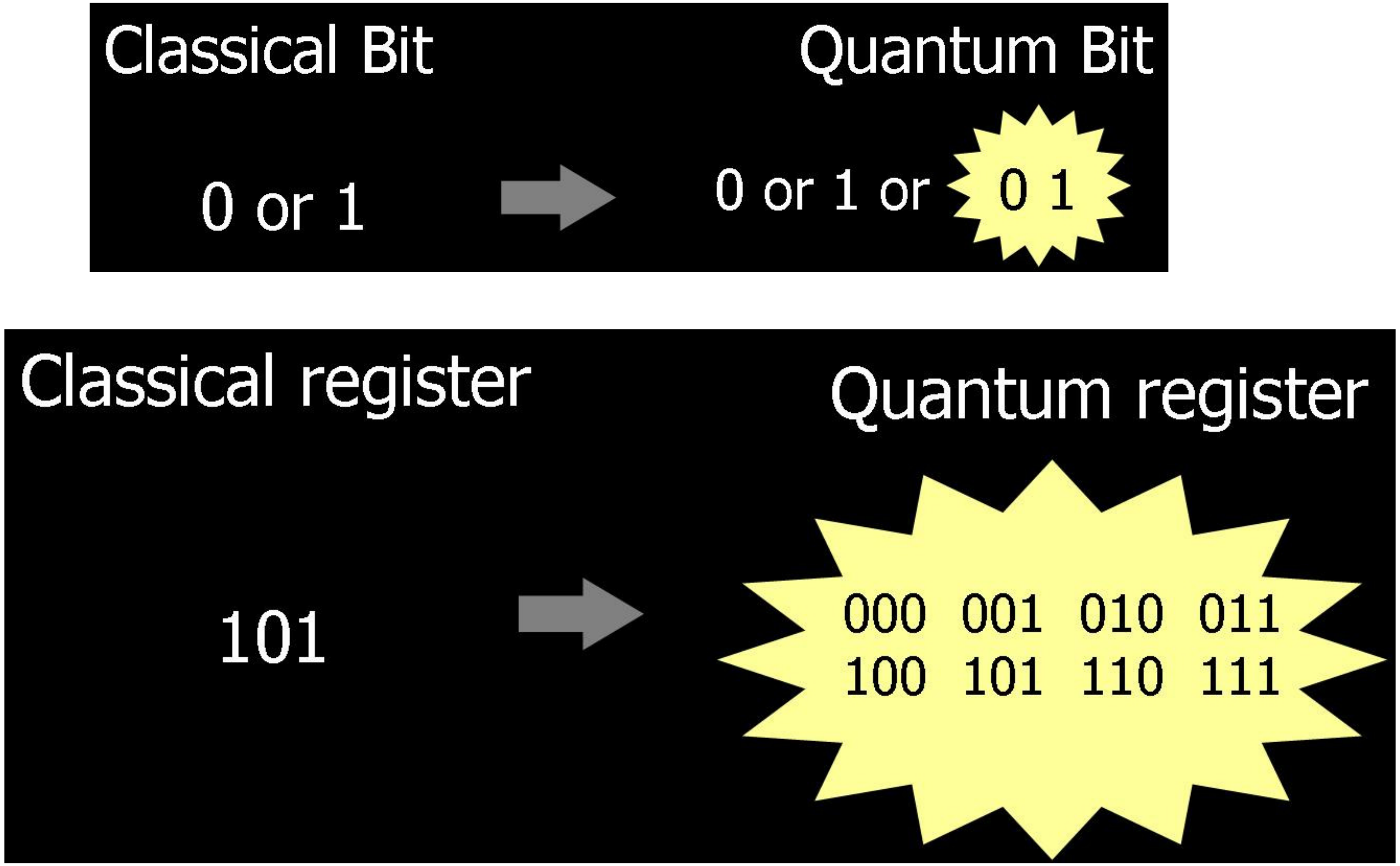
- **Measurement**

  - Classical bit: we can find out if it is in state 0 or 1 and the measurement will not change the state of the bit.
  - Qubit: we cannot just measure α and β and thus determine its state! We get either $|0\rangle$ or $|1\rangle$ with corresponding probabilities $|\alpha|^2$ and $|\beta|^2$.
  - The measurement changes the state of the qubit!

$$|\alpha|^2 + |\beta|^2 = 1$$

Multiple qubits

Hilbert space is a big place!
- Carlton Caves



Multiple qubits

Hilbert space is a big place!
- Carlton Caves

- Two bits with states 0 and 1 form four definite states 00, 01, 10, and 11.
- Two qubits: can be in superposition of four computational basis set states.

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

2 qubits	4 amplitudes
3 qubits	8 amplitudes
10 qubits	1024 amplitudes
20 qubits	1 048 576 amplitudes
30 qubits	1 073 741 824 amplitudes
500 qubits	More amplitudes than our estimate of number of atoms in the Universe!!!

Entanglement

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

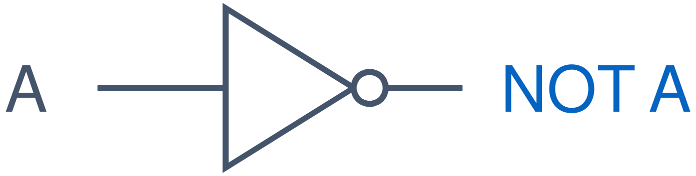
Results of the measurement			
First	qubit	0	1
Second	qubit	0	1

$$|\psi\rangle \neq |\alpha\rangle \otimes |\beta\rangle \longrightarrow$$

Entangled states

Logic gates

Classical NOT gate



A	NOT A
0	1
1	0

The only non-trivial single bit gate

Quantum NOT gate (X gate)

Matrix form representation

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

More single qubit gates

Any unitary matrix U will produce a quantum gate!

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\alpha|0\rangle + \beta|1\rangle \;\text{—}\boxed{Z}\text{—}\; \alpha|0\rangle - \beta|1\rangle$$

Hadamard gate:

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

$$\alpha|0\rangle + \beta|1\rangle \;\text{—}\boxed{H}\text{—}\; \alpha\frac{|0\rangle + |1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Universality: quantum computation

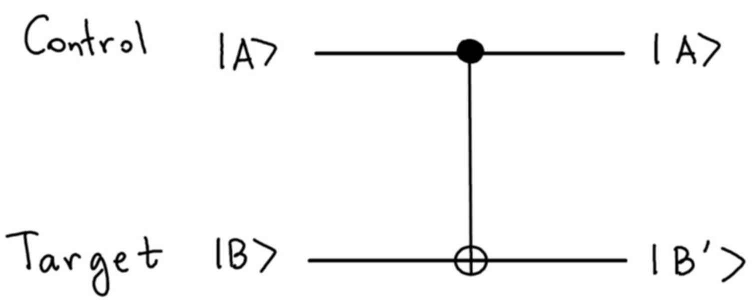
How many quantum gates do we need to build any quantum gate?

Any n-qubit gate can be made from 2-qubit gates.

(Since any unitary n x n matrix can be decomposed to product of two-level matrices.)

Only one two-qubit gate is needed!

Controlled-NOT (CNOT) gate



$\vert AB\rangle$	$\vert AB'\rangle$
$\vert 00\rangle$	$\vert 00\rangle$
$\vert 01\rangle$	$\vert 01\rangle$
$\vert 10\rangle$	$\vert 11\rangle$
$\vert 11\rangle$	$\vert 10\rangle$

Gate operations: if control qubit is $|1\rangle$, then flip the target qubit.

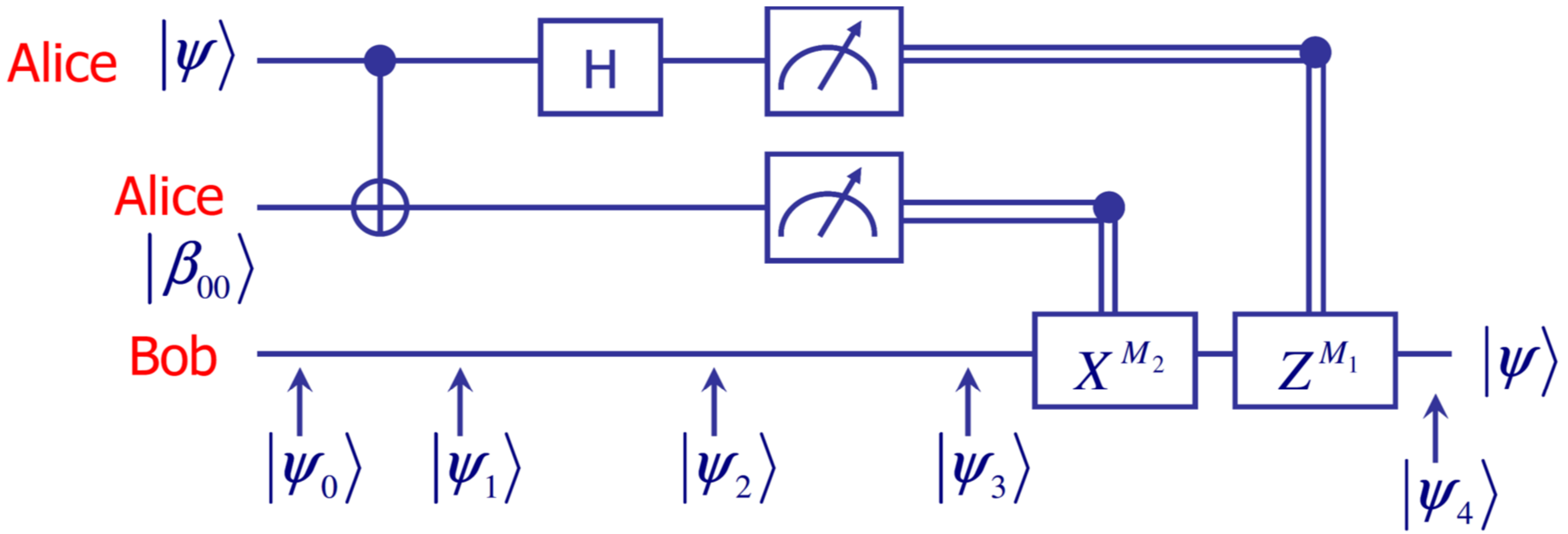
Quantum circuits: quantum teleportation

QT: Technique for moving quantum states around, even in an absence of quantum communication channel.

<u>The problem:</u>

Alice must deliver qubit $|\psi\rangle$ to Bob

- She does not know the state of the qubit
- She can use only classical channels



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

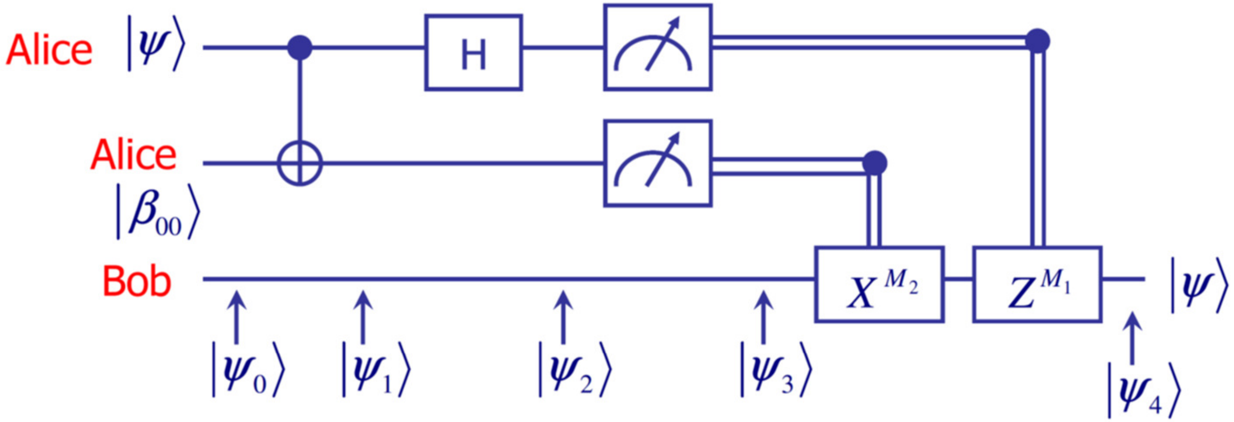
Quantum circuits: quantum teleportation

The problem:

Alice must deliver qubit $|\psi\rangle$ to Bob

- She does not know the state of the qubit
- She can use only classical channels

Teleportation scheme



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

How does it work?

- Alice and Bob generate an EPR pair together.

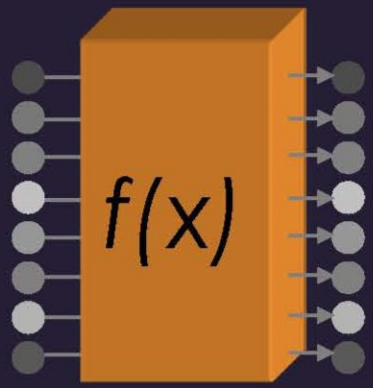
  EPR pair: two entangled qubits in the state $|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

- The moved to different places and each took one qubit of the EPR pair.
- Alice interacts qubit $|\psi\rangle$ to be teleported with half of her EPR pair and then makes a measurement on two qubits which she has.
- She can get one out of four possible results: **00, 01, 10, and 11.**
- Alice reports this information to Bob.
- Bob performs one of four operations on his half of the EPR pair.
- Amazingly, he can recover the original state $|\psi\rangle$!

Good News…

parallel processing on 2^N inputs

e.g., N=3 qubits

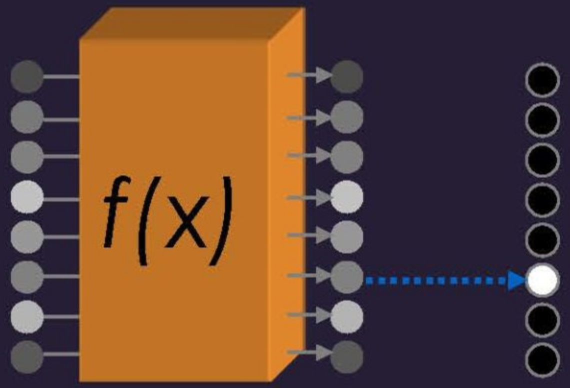


$$a_0|000\rangle + a_1|001\rangle + a_2|010\rangle + a_3|011\rangle$$
$$a_4|100\rangle + a_5|101\rangle + a_6|110\rangle + a_7|111\rangle$$

N=300 qubits have more configurations than there are particles in the universe!

…Bad News…

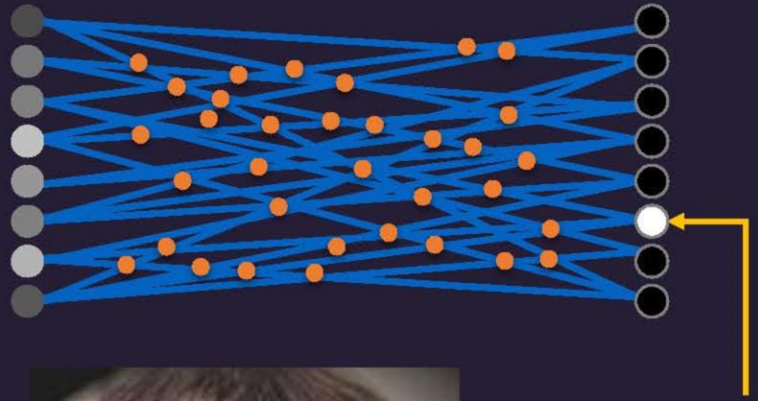
measurement gives random result



…Good News!

quantum interference

Need smart algorithms!



depends on *all* inputs

David Deutsch (early 1990s)

Slide credit: Chris Monroe, from Patrick Kennedy, https://www.servethehome.com/ionq-quantum-computing-at-hot-chips-33/

Application: Factoring Numbers

A quantum computer can factor numbers **exponentially faster** than classical computers

P. Shor (1994)

39 = 3 × 13 (…easy)
38647884621009387621432325631 = **?** × **?**

Key generation	N = P * Q d * e = 1mod Φ(N)
Encryption	c = m^e mod N Public Key(N,e)
Decryption	m = c^d mod N private key (d)

Practical applications: need millions of qubits and billions of gates

Factor N (n bits)

Best classical algorithm: $time \sim e^{n^{1/3}(log n)^{2/3}}$

Shor's quantum algorithm: $time \sim (log log n)(log n) n^2$

Slide credit: Chris Monroe, from Patrick Kennedy, https://www.servethehome.com/ionq-quantum-computing-at-hot-chips-33/

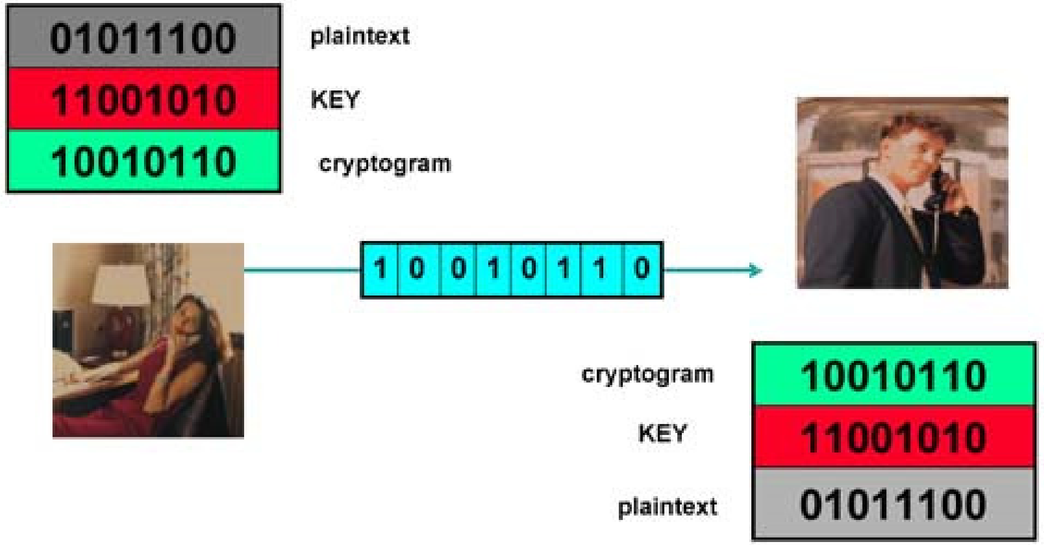
Quantum cryptography

Classical cryptography

Scytale – the first known mechanical device to implement permutation of characters for cryptographic purposes

Classical cryptography

Private key cryptography



How to securely transmit a private key?

Key distribution

A central problem in cryptography:

the key distribution problem.

1) Mathematics solution: public key cryptography.
2) Physics solution: quantum cryptography.

One can not copy a qubit!!!

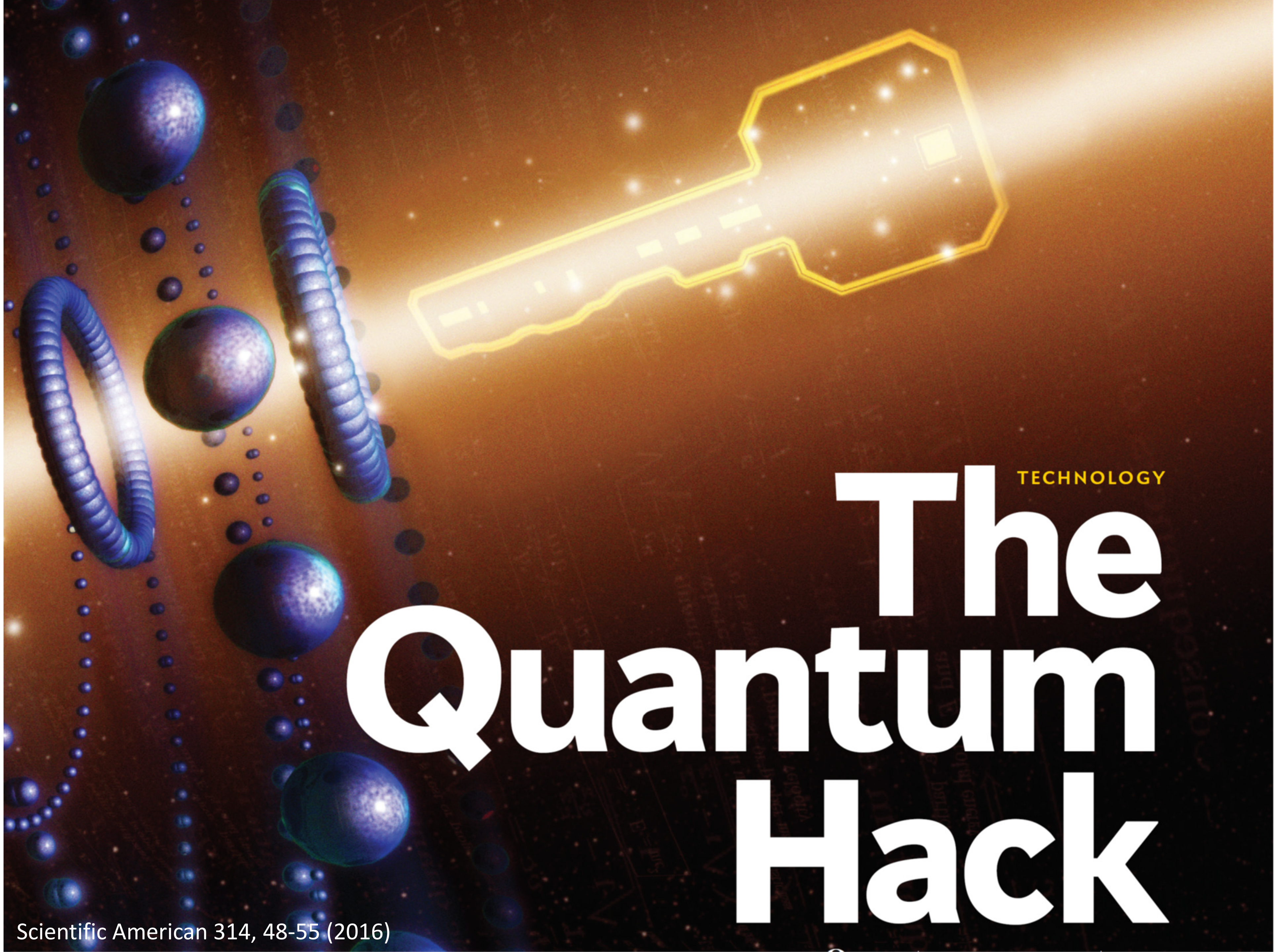
Public-key cryptography relies on the computational difficulty of certain hard mathematical problem (computational security)

Quantum cryptography relies on the laws of quantum mechanics (information-theoretical security).

Quantum key distribution

A quantum communication channel:
physical system capable delivering quantum systems
more or less intact from one place to another (photons).

- Quantum mechanics: quantum bits cannot be copied or monitored.
- Any attempt to do so will result in altering it that can not be corrected.
- Problems
  - Authentication
  - Noisy channels

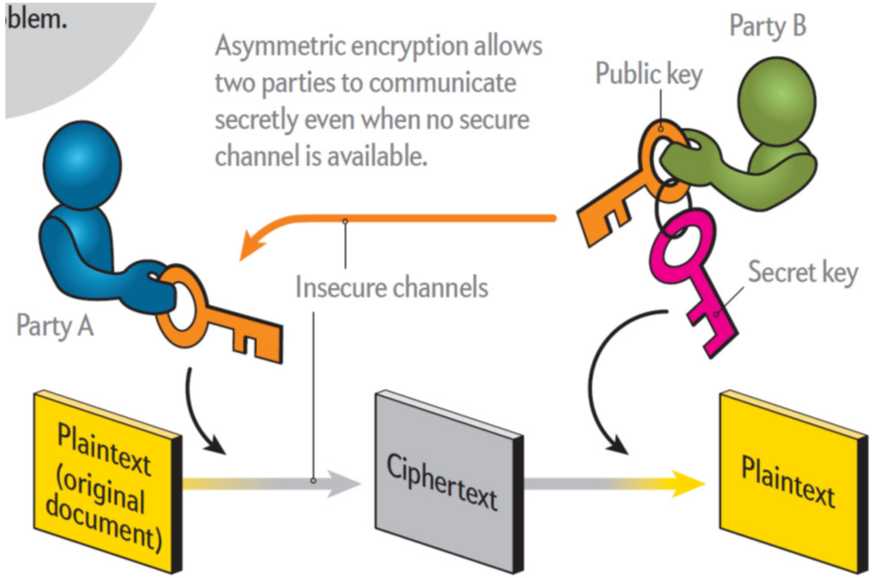


Scientific American 314, 48-55 (2016)

A central problem in cryptography: the key distribution problem.

Mathematics solution:
public key cryptography.

Public–key cryptography relies on the computational difficulty of certain hard mathematical problems (for example factoring)



Security problems with public key cryptography:

(1) The is no proof that there is no "easy" solution to factoring: somebody can come up with new much quicker algorithm!

(2) Quantum computer, if build, can break public key encryption – fast quantum algorithm is already knows (Shor's algorithm)

Another solution to the key distribution problem: Quantum key distribution

Use quantum communication channel:
physical system capable delivering quantum systems more or less intact from one place to another.

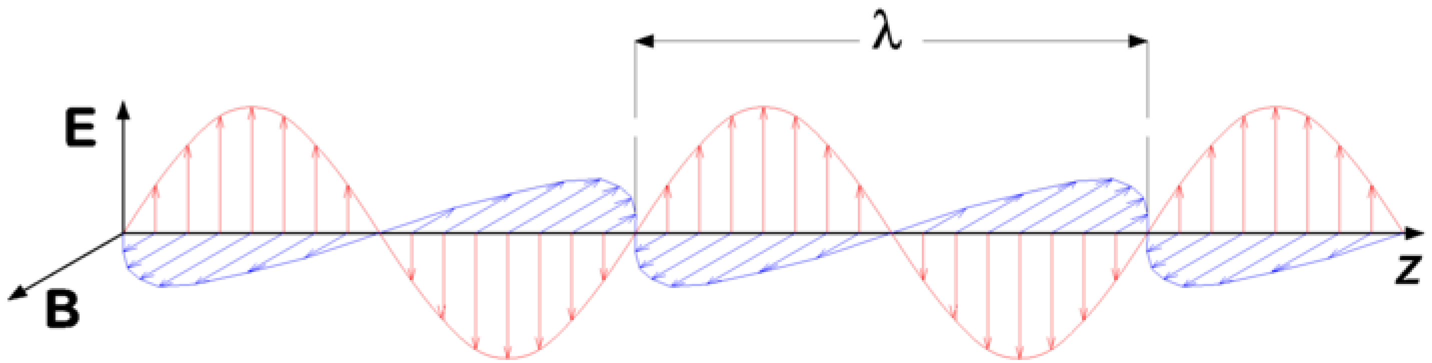
What is this quantum system? Photons!

Why is this secure:
Quantum mechanics: quantum bits cannot be copied or monitored.

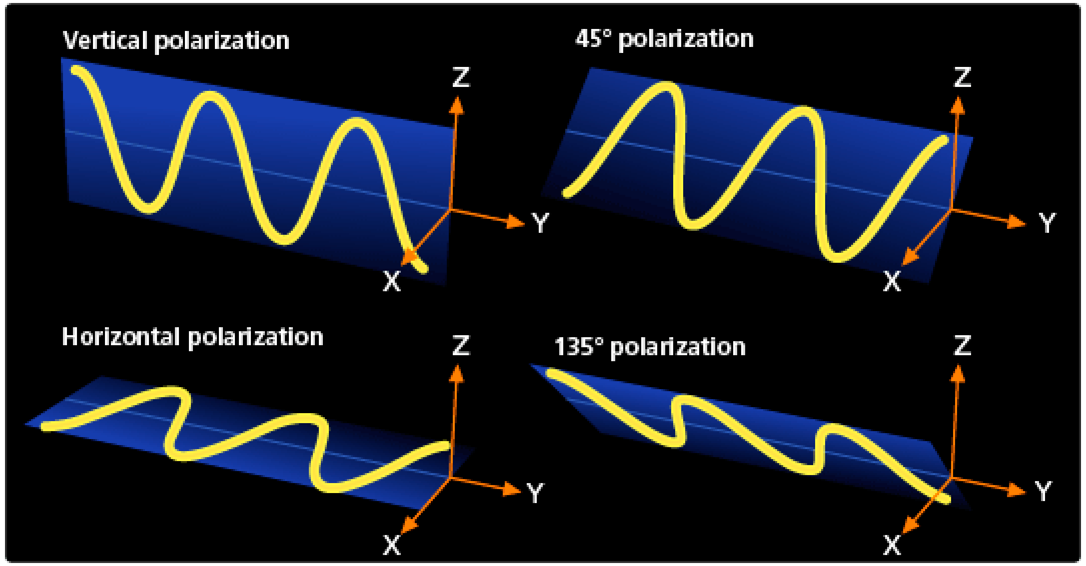
Any attempt to do so will result in altering it that can not be corrected.

How to use photons as qubits?
Use polarization of photons to encode 0 and 1.

Electromagnetic waves



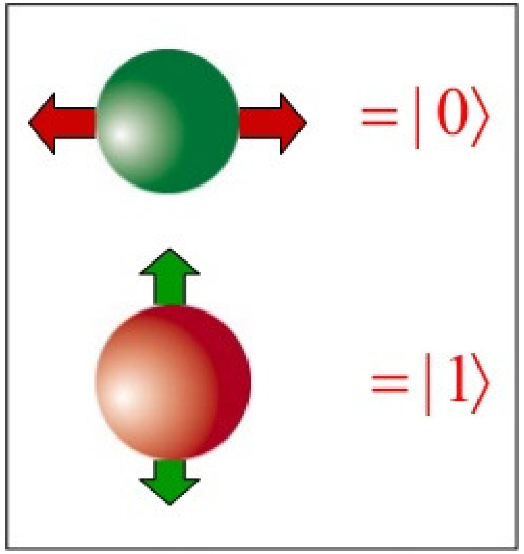
A "vertically polarized" electromagnetic wave of wavelength λ has its electric field vector **E** (red) oscillating in the vertical direction. The magnetic field **B** (or **H**) is always at right angles to it (blue), and both are perpendicular to the direction of propagation (**z**).

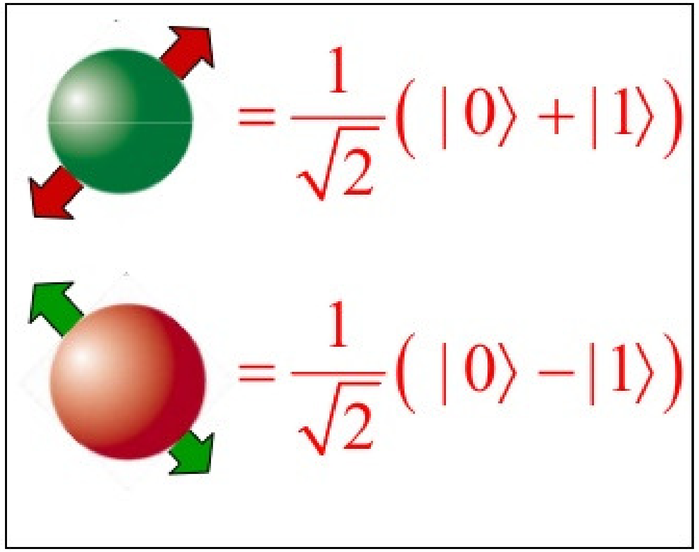


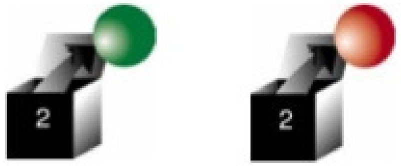
http://www.nikon.com/about/feelnikon/light/chap04/sec01.htm

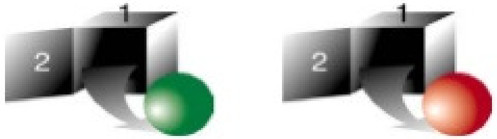
https://en.wikipedia.org/wiki/Polarization_(waves)

Photon polarization as a qubit

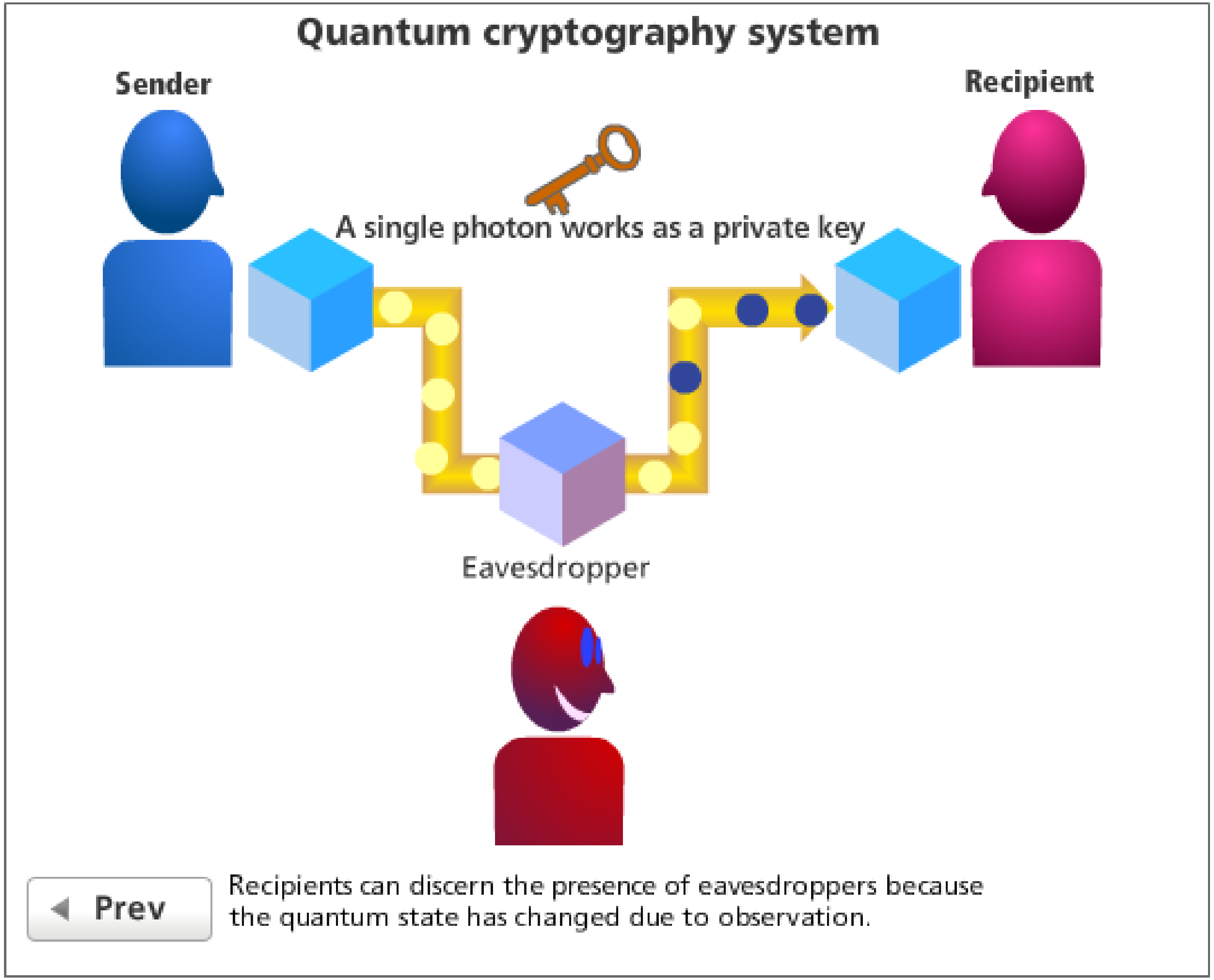








Quantum key distribution

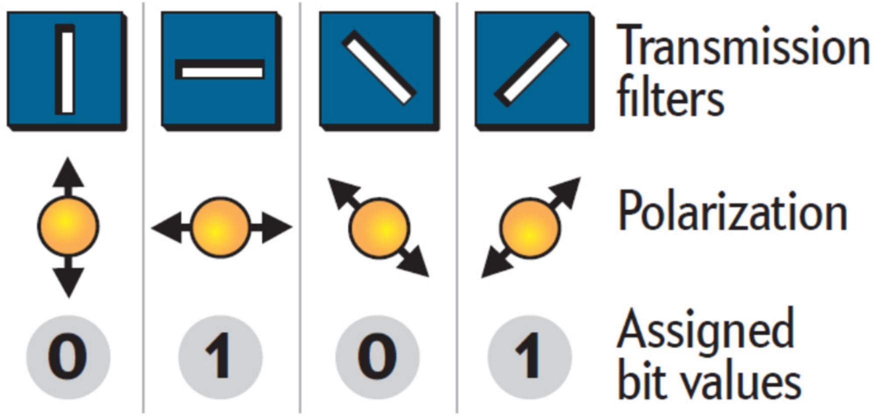


The Quantum Future of Cryptography

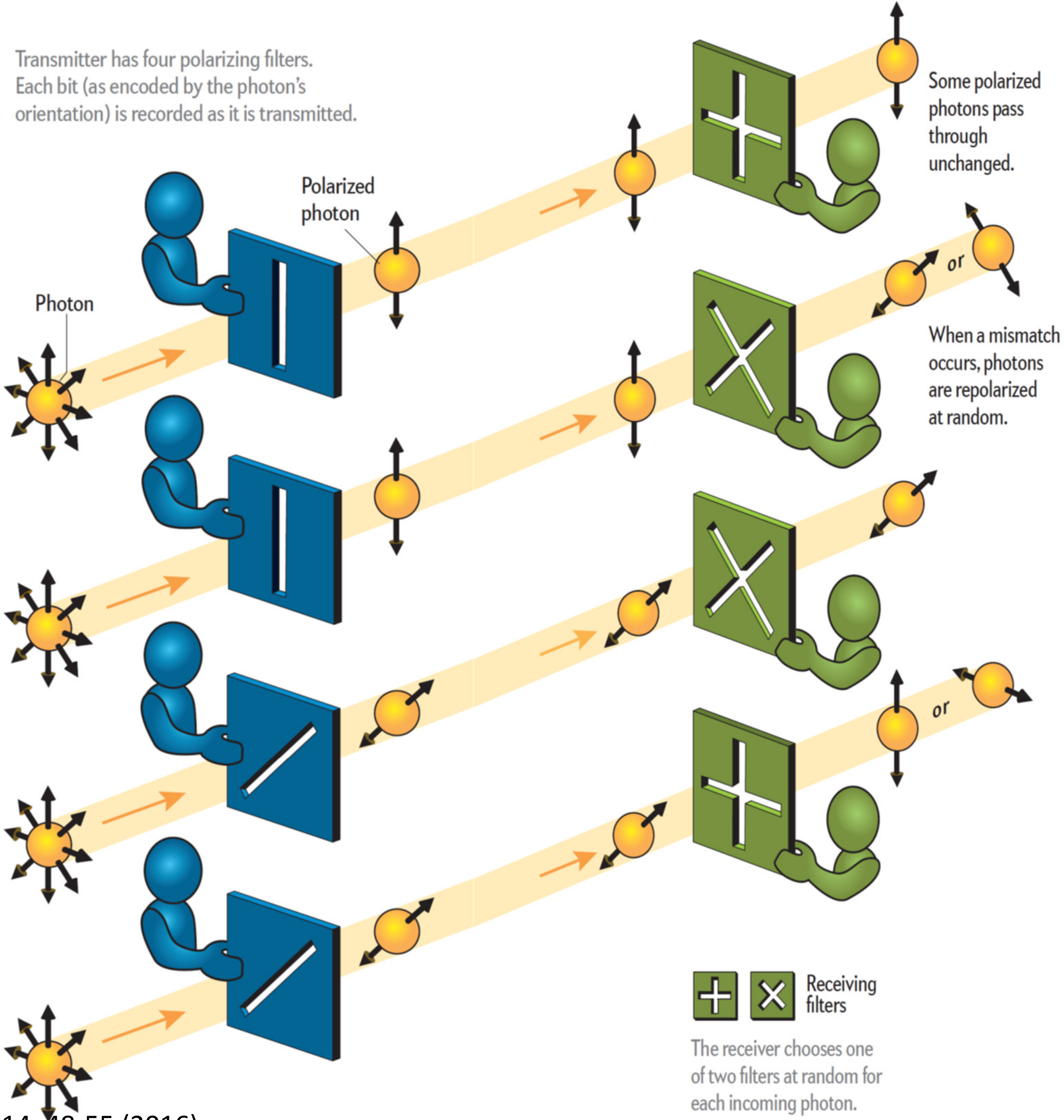
Quantum-key distribution is a way of securely sharing a cryptographic key using a stream of light particles, or photons, that are polarized. If an eavesdropper measures those photons while they are in transit, the act of measurement will change the polarization of some of those photons, and the sender and recipient will know that their message has been tampered with.

Sending and Receiving Polarized Photons

The sender (*blue*) transmits a series of photons; each passes through one of four polarizing filters. Each filter—and therefore polarization direction—is assigned a bit value of 0 or 1 (*below*). The sender writes down the bit value of each photon. The recipient (*green*) can only determine the bit value of each photon after it has passed through a receiving filter.

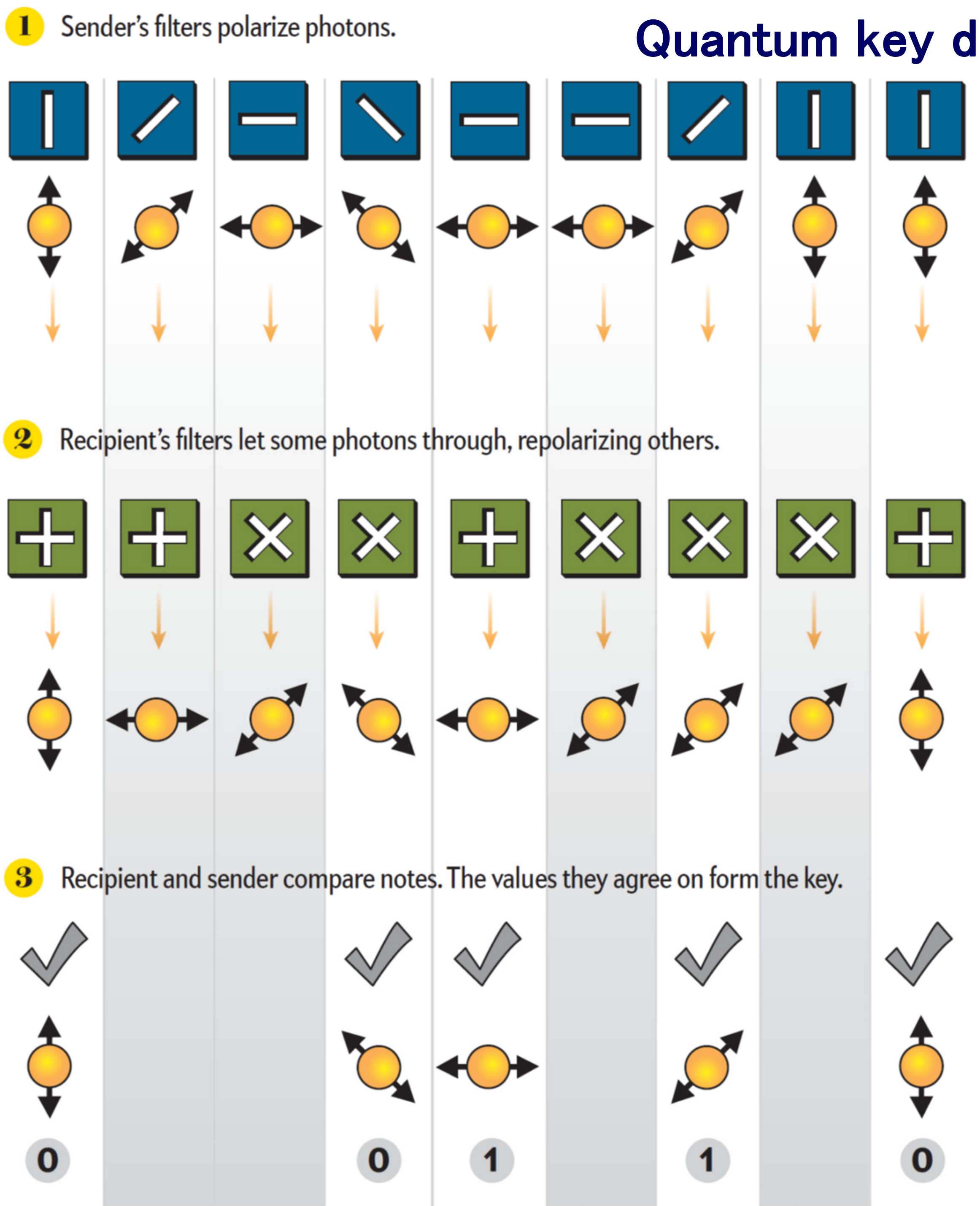


Scientific American 314, 48-55 (2016)



Scientific American 314, 48-55 (2016)

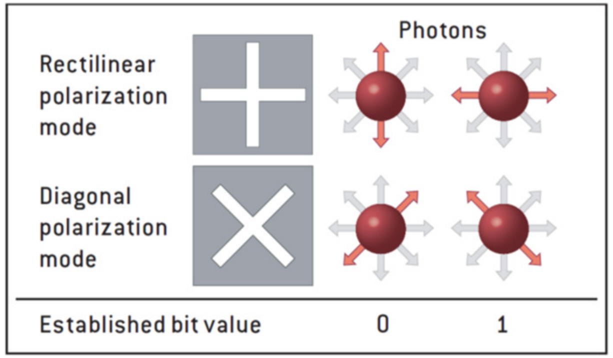
Quantum key distribution



Scientific American 314, 48-55 (2016)

Scientific American 292, 78 (2005)

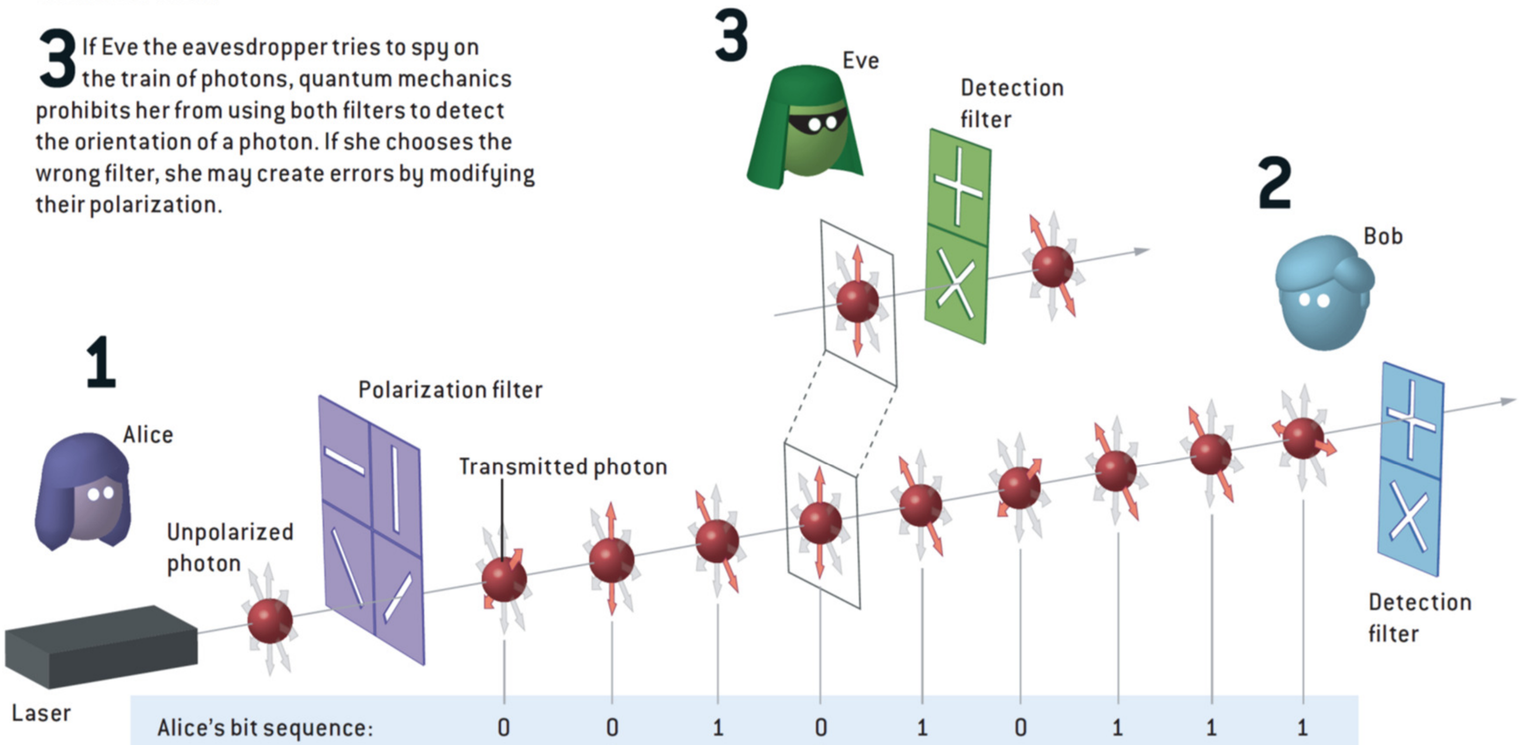
Alice and Bob try to keep a quantum-cryptographic key secret by transmitting it in the form of polarized photons, a scheme invented by Charles Bennett of IBM and Gilles Brassard of the University of Montreal during the 1980s and now implemented in a number of commercial products.



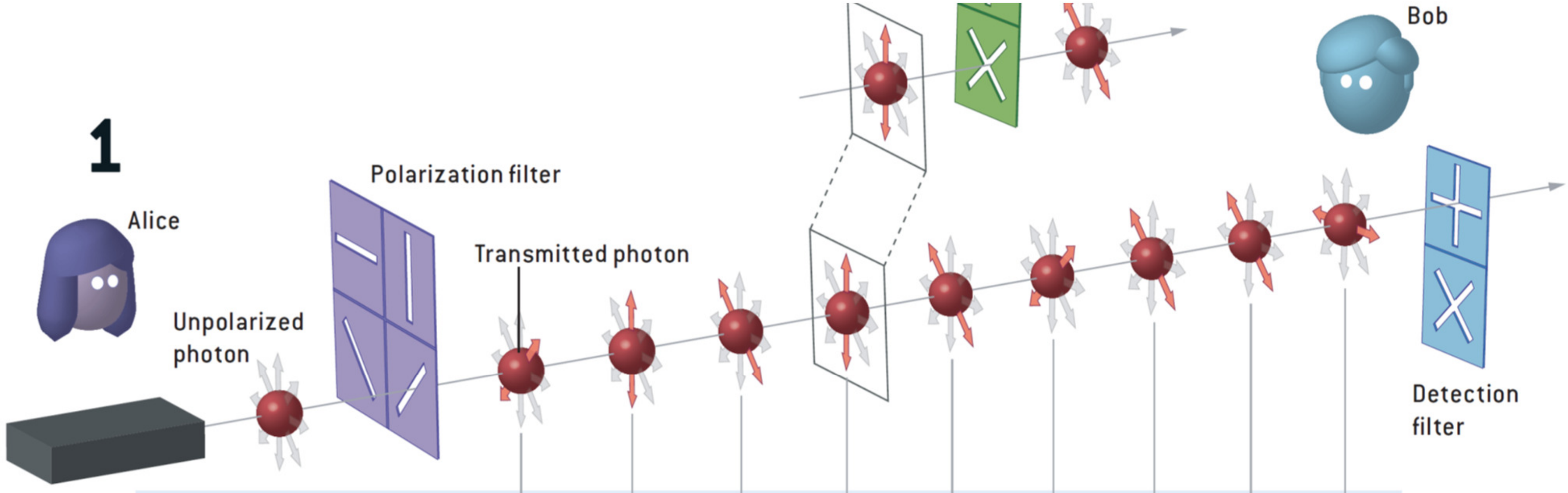
1 To begin creating a key, Alice sends a photon through either the 0 or 1 slot of the rectilinear or diagonal polarizing filters, while making a record of the various orientations.

2 For each incoming bit, Bob chooses randomly which filter slot he uses for detection and writes down both the polarization and the bit value.

3 If Eve the eavesdropper tries to spy on the train of photons, quantum mechanics prohibits her from using both filters to detect the orientation of a photon. If she chooses the wrong filter, she may create errors by modifying their polarization.



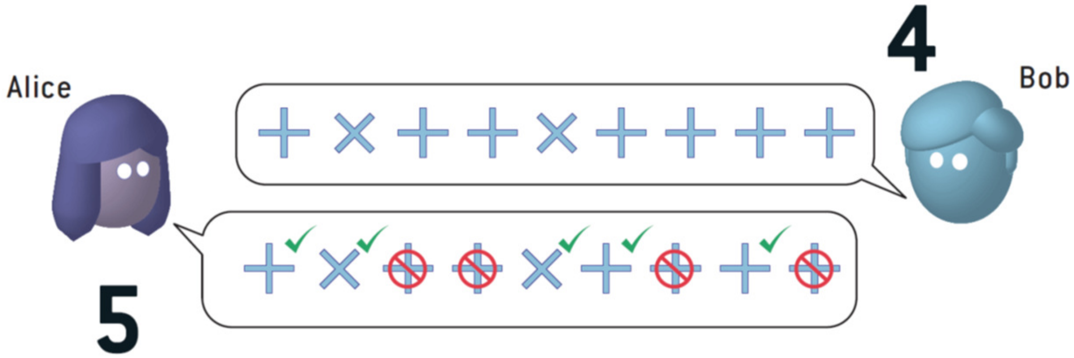
Alice's bit sequence:	0	0	1	0	1	0	1	1	1
Alice's filter scheme:	/	|	\	|	\	/	\	\	—
Bob's detection scheme:	+	+	+	+	×	+	+	×	+
Bob's bit measurements:	1	0	1	0	1	0	0	1	1
Retained bit sequence (key):	—	0	—	0	1	—	—	1	1



Alice's bit sequence:	0	0	1	0	1	0	1	1	1
Alice's filter scheme:	/	|	\	|	\	/	\	\	—
Bob's detection scheme:	+	+	+	+	×	+	+	×	+
Bob's bit measurements:	1	0	1	0	1	0	0	1	1
Retained bit sequence (key):	—	0	—	0	1	—	—	1	1

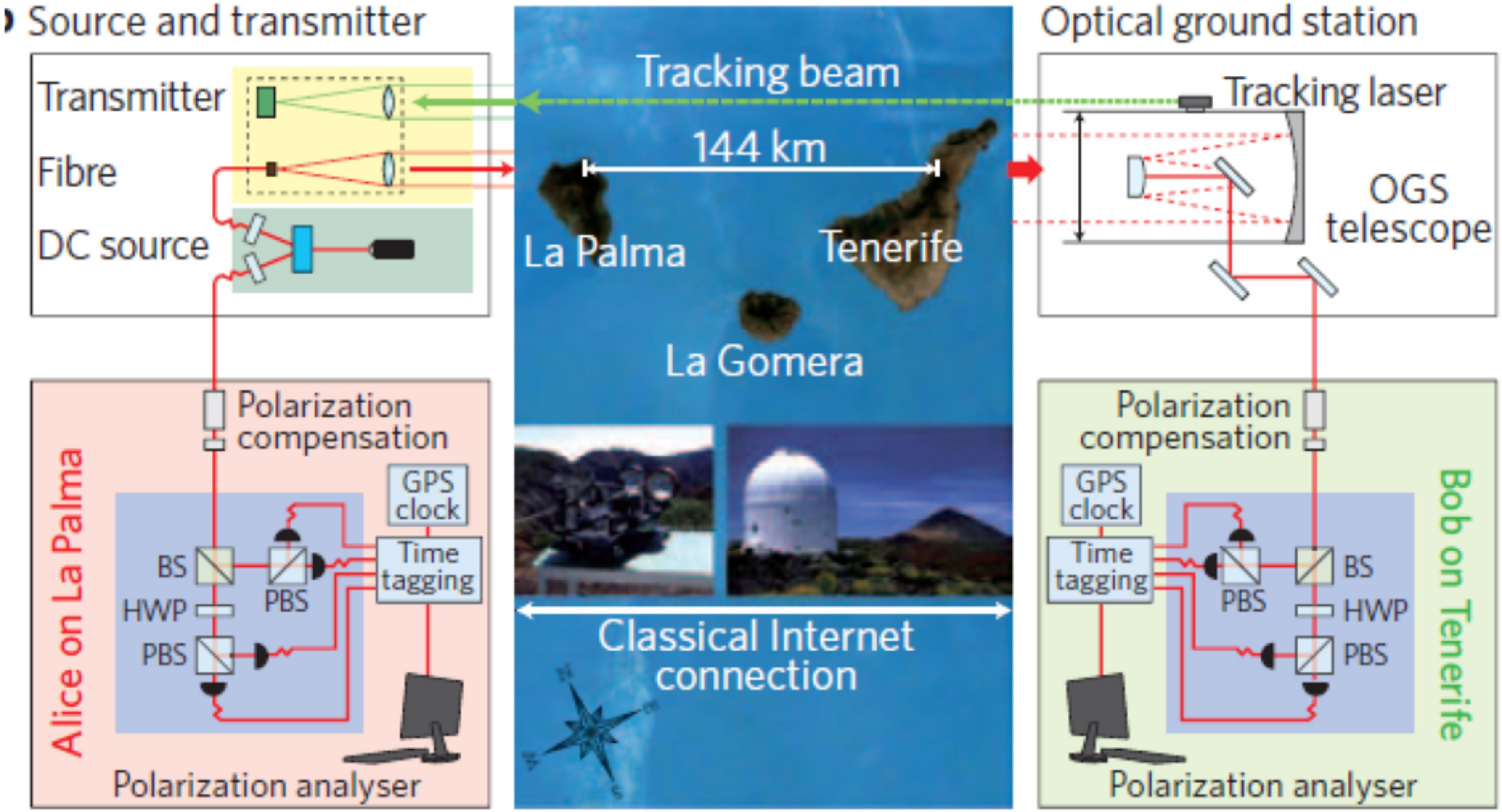
4 After all the photons have reached Bob, he tells Alice over a public channel, perhaps by telephone or an e-mail, the sequence of filters he used for the incoming photons, but not the bit value of the photons.

5 Alice tells Bob during the same conversation which filters he chose correctly. Those instances constitute the bits that Alice and Bob will use to form the key that they will use to encrypt messages.



Scientific American 292, 78 (2005)

Entanglement-based Quantum Key Distribution set-up connecting the two Canary Islands La Palma and Tenerife. The optical link is 144 km long.

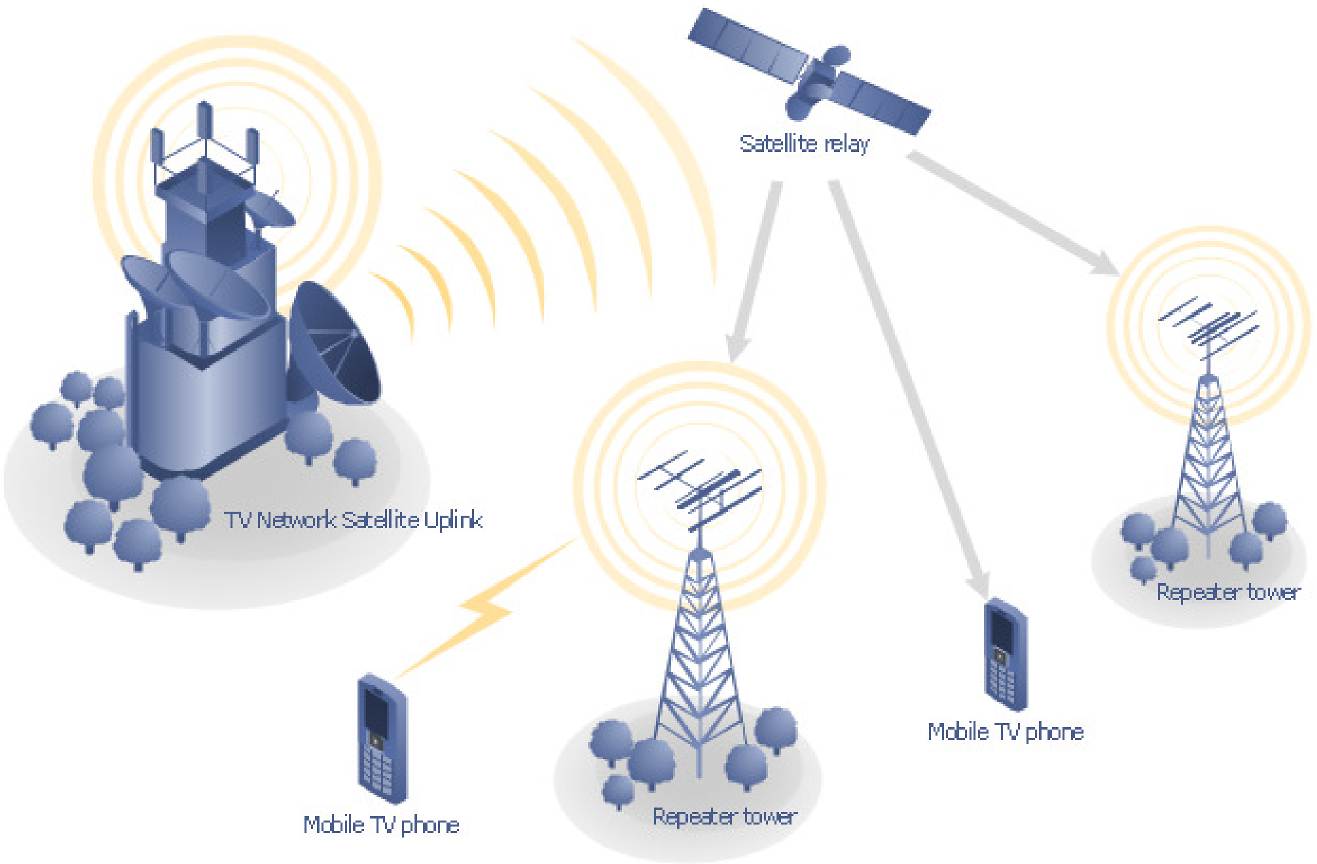


OGS, optical ground station; GPS, Global Positioning System; PBS, polarizing beamsplitter; BS, beamsplitter; HWP, half-wave plate.

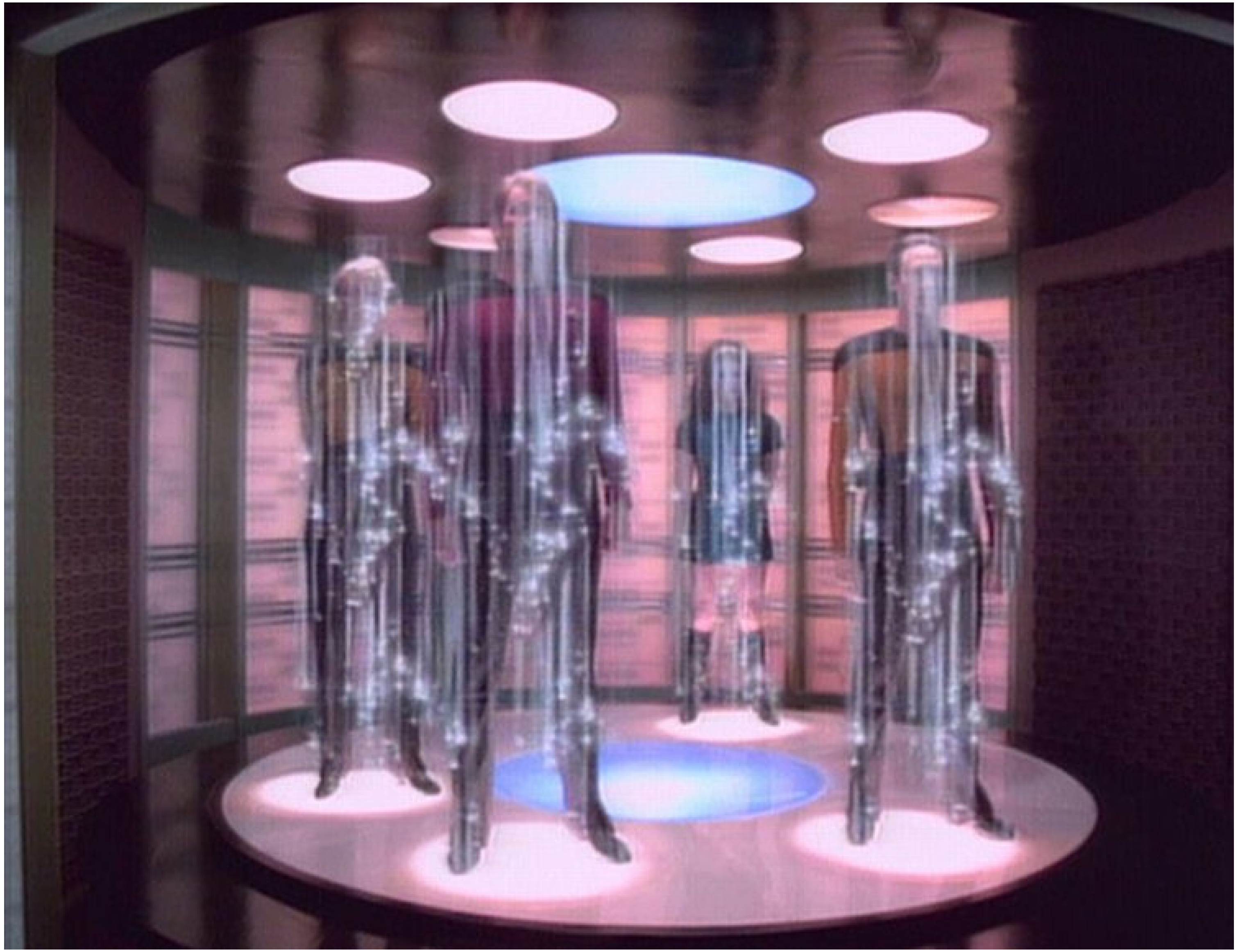
Ursin, R. et al. Nature Phys. 3, 481–486 (2007).

Problems with quantum key distribution

Qubits can not be copied – we can not amplify the signal or retransmit information as in the classical case.



If you can not copy – teleport!



Information is physical

What do we need to build a quantum computer?

Memory: a scalable physical system with well characterized qubit

Initialization: ability to prepare one certain state repeatedly on demand, for example put all to zero at the start.

Ability to perform (universal) logical operations.

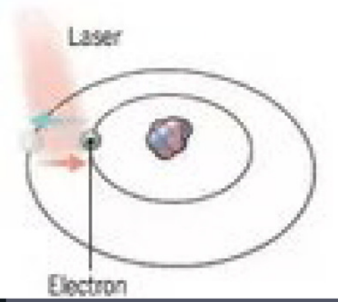
Long relevant decoherence times: small error rate (that can be fixed).

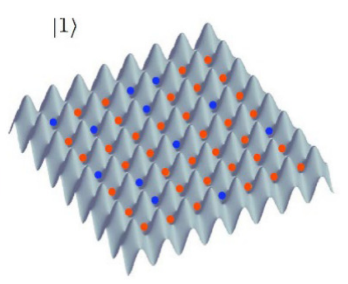
Ability to efficiently **read out the result.**

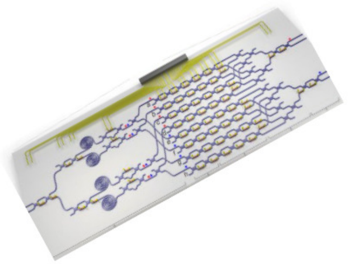
DiVincenzo criteria (2000)

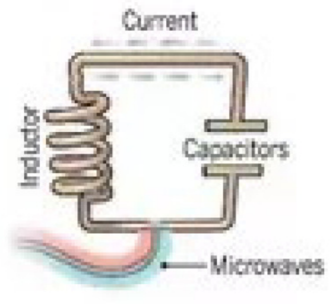
Quantum Computer Technologies

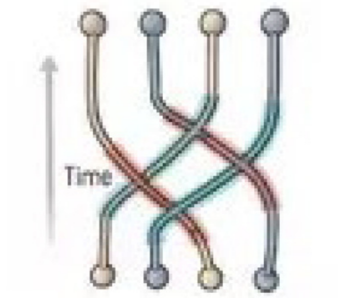
Natural Qubits | **Synthetic Qubits**

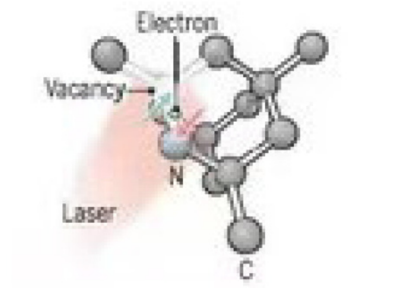












	Trapped Ions	Neutral Atoms	Photonics	Superconducting Loops	Silicon Quantum Dots	Topological Qubits	Diamond Vacancies
	Electrically charged atoms, or ions, are held in place with electric fields. Qubits are stored in electronic states. Ions are pushed with laser beams to allow the qubits to interact.	Neutral atoms, like ions, store qubits within electronic states. Laser activates the electrons to create interaction between qubits.	Photonic qubits (light particles) are sent through a maze of optical channels on a chip to interact. At the end of the maze, the distribution of photons is measured as an output.	A resistance-free current oscillates back and forth around a circuit loop. An injected microwave signal excites the current into super-position states.	These "artificial atoms" are made by adding an electron to a small piece of pure silicon. Microwaves control the electron's quantum state.	Quasiparticles can be seen in the behavior of electrons channeled through semi-conductor structures. Their braided paths can encode quantum information.	A nitrogen atom and a vacancy add an electron to a diamond lattice. Its quantum spin state, along with those of nearby carbon nuclei, can be controlled with light.
Qubit Coherence Time (sec)	>1000	1	--	0.00005	0.03	N/A	10
Fidelity	99.9%	97%	--	99.4%	~99%	N/A	99.2%
Qubits Connected	High	Very high; low individual control	--	High	Very Low	N/A	Low
Company Support	IONQ, AQT, Honeywell, Oxford Ionics	Atom Computing, ColdQuanta, QuEra	Psiquantum, Xanadu	Google, IBM, QCI, Rigetti	HRL, Intel, SQC	Microsoft	Quantum Diamond Technologies
Pros	Very stable. Highest achieved gate fidelities.	Many qubits, 2D and maybe 3D.	Linear optical gates, integrated on-chip.	Can lay out physical circuits on chip.	Borrows from existing semiconductor industry.	Greatly reduce errors.	Can operate at room temperature.
Cons	Slow operation. Many lasers are needed.	Hard to program and control individual qubits; prone to noise.	Each program requires its own chip with unique optical channels. No memory.	Must be cooled to near absolute zero. High variability in fabrication. Lots of noise.	Only a few connected. Must be cooled to near absolute zero. High variability in fabrication.	Existence not yet confirmed.	Difficult to create high numbers of qubits, limiting compute capacity.

Source: Science, Dec. 2016 Slide credit: Chris Monroe, https://boulderschool.yale.edu/sites/default/files/files/BoulderLec1%202021.pdf

Qubits with trapped ions

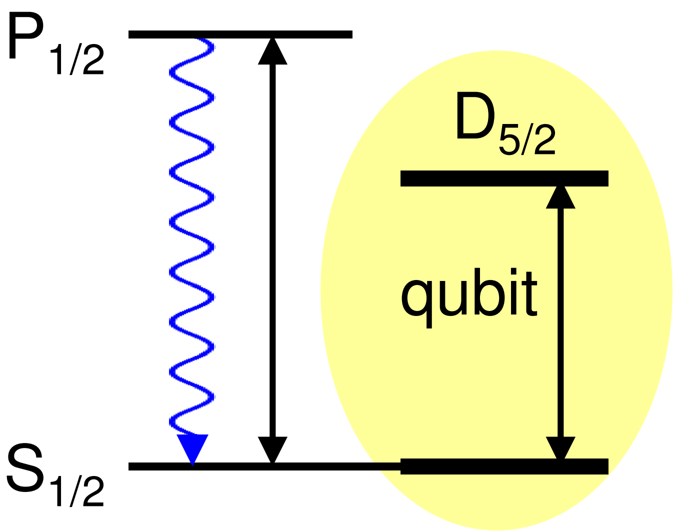
Encoding of quantum information requires long-lived atomic states:

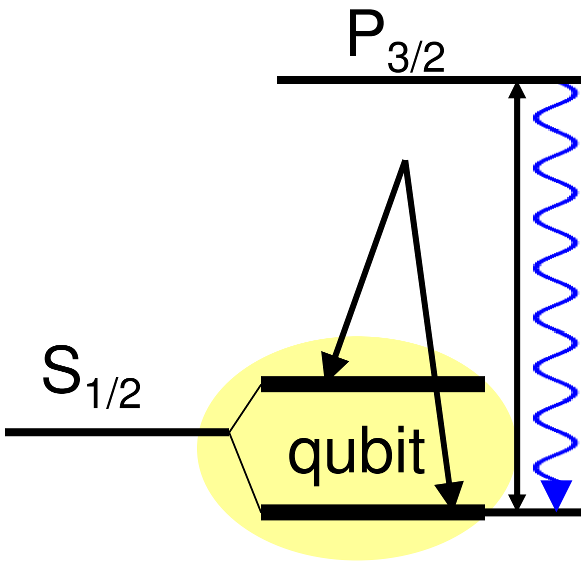
- optical transitions

  Ca^+, Sr^+, Ba^+, Ra^+, Yb^+, Hg^+ etc.

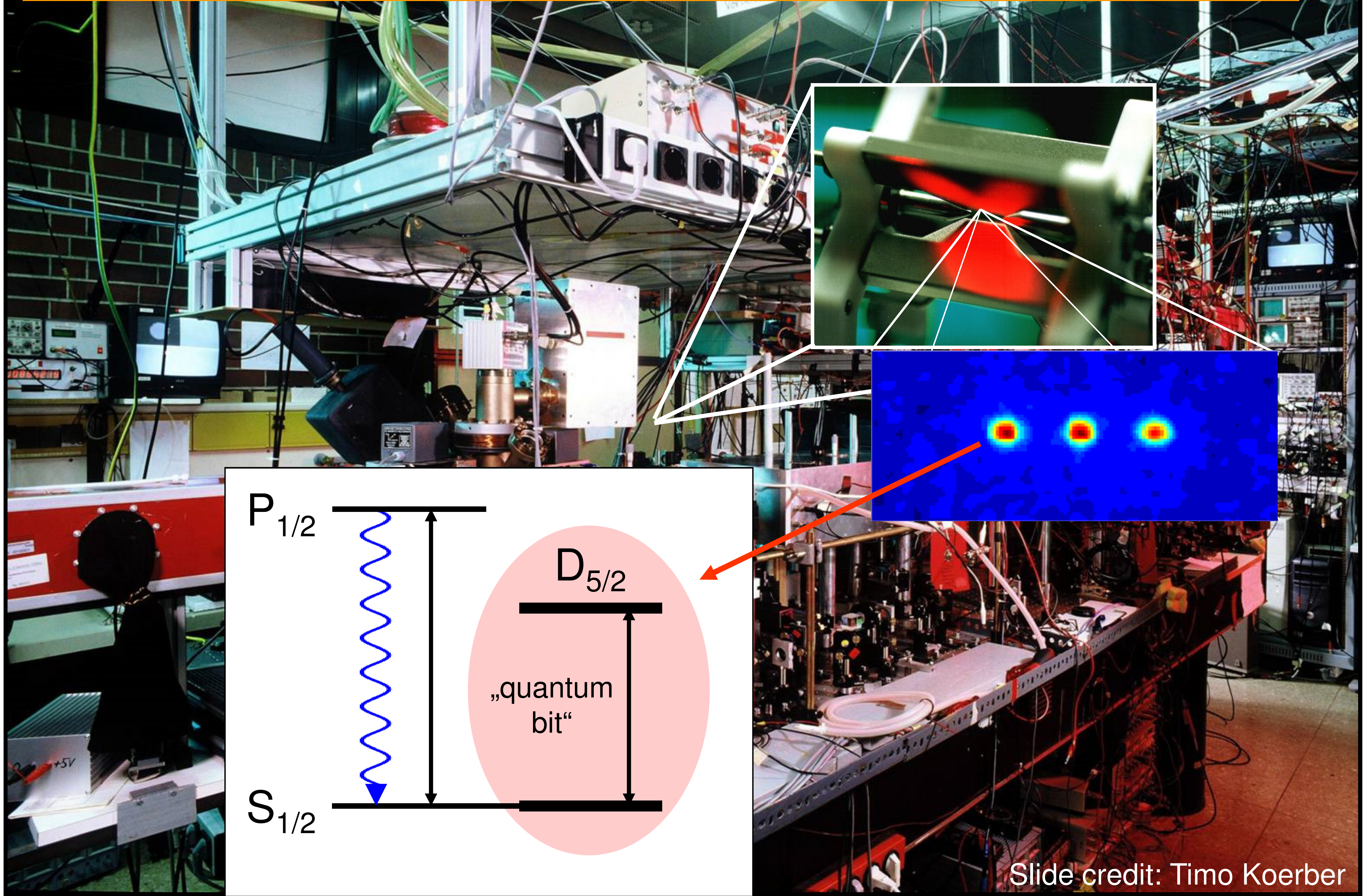
- microwave transitions

  $^{9}Be^+$, $^{25}Mg^+$, $^{43}Ca^+$, $^{87}Sr^+$, $^{137}Ba^+$, $^{111}Cd^+$, $^{171}Yb^+$



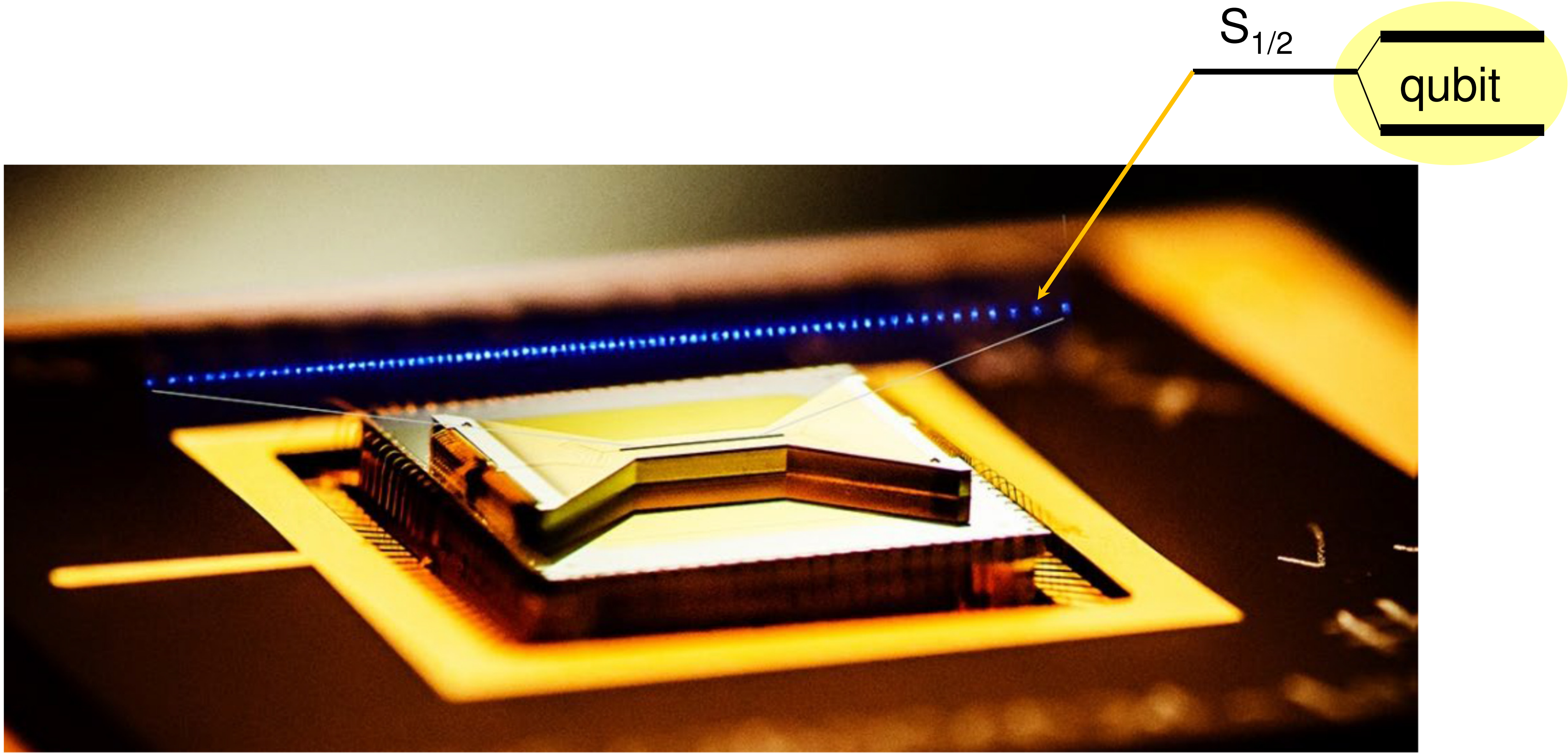


Trapped ion quantum computer in 2005



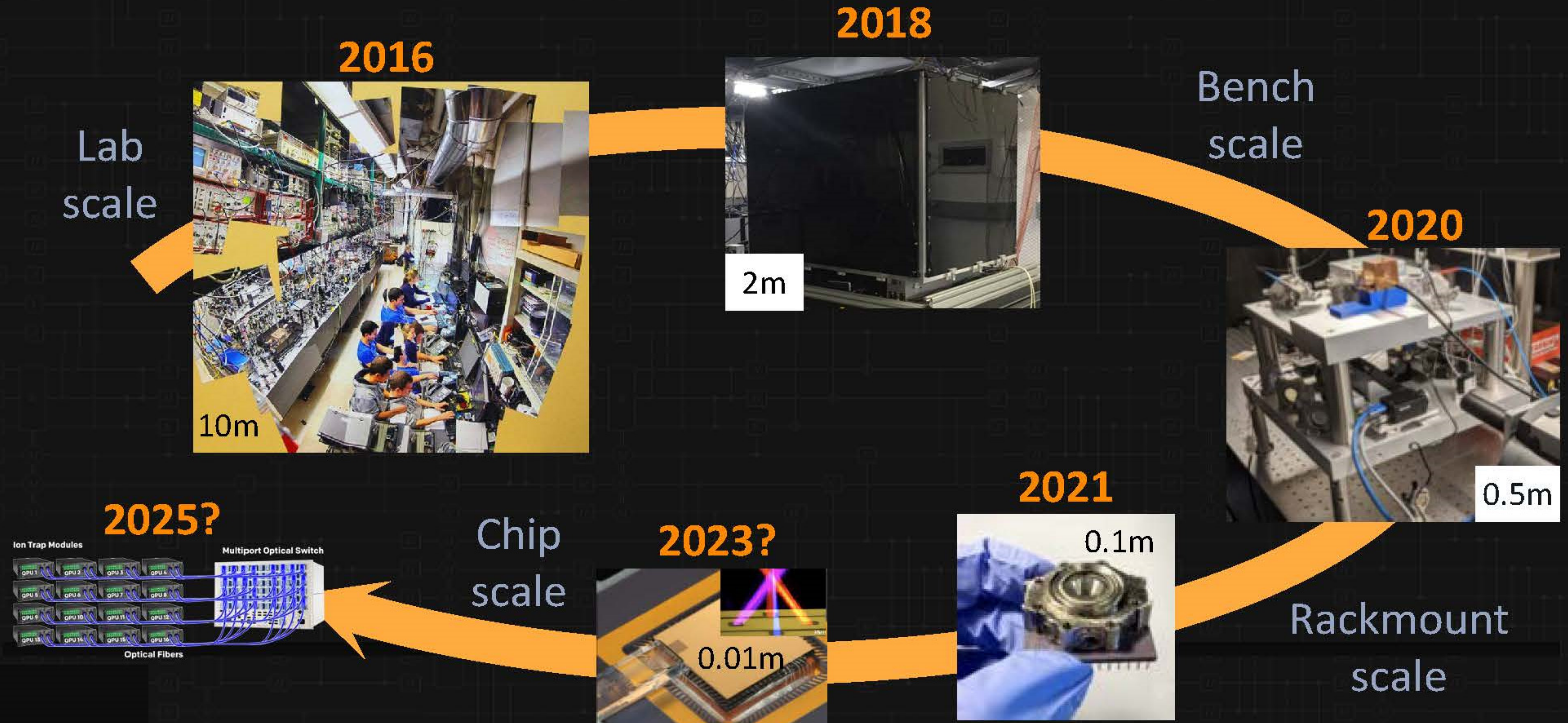
Slide credit: Timo Koerber

Ion trap with 80 Yb+ ions



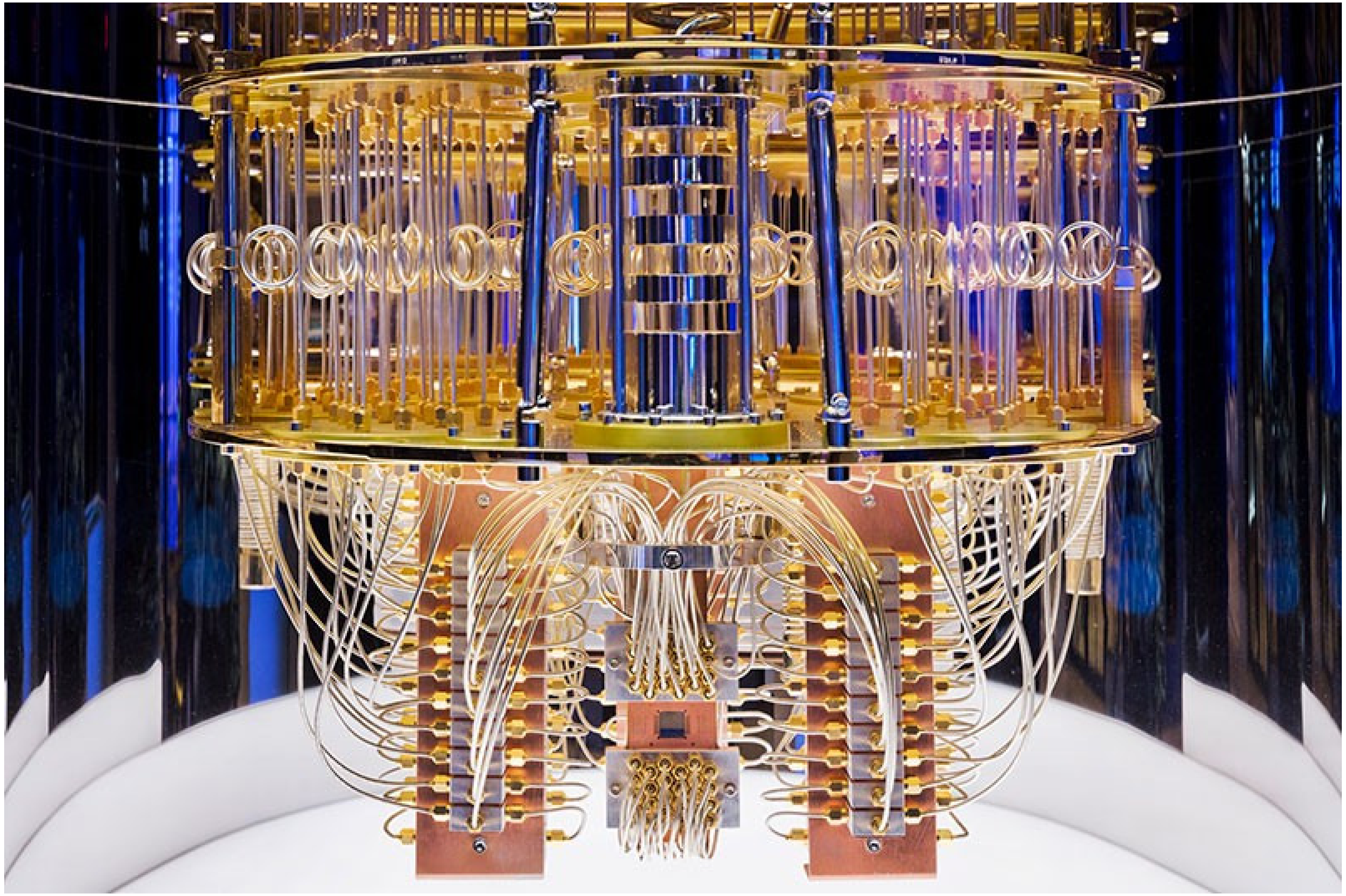
Picture credit: Chris Monroe, https://boulderschool.yale.edu/sites/default/files/files/BoulderLec1%202021.pdf

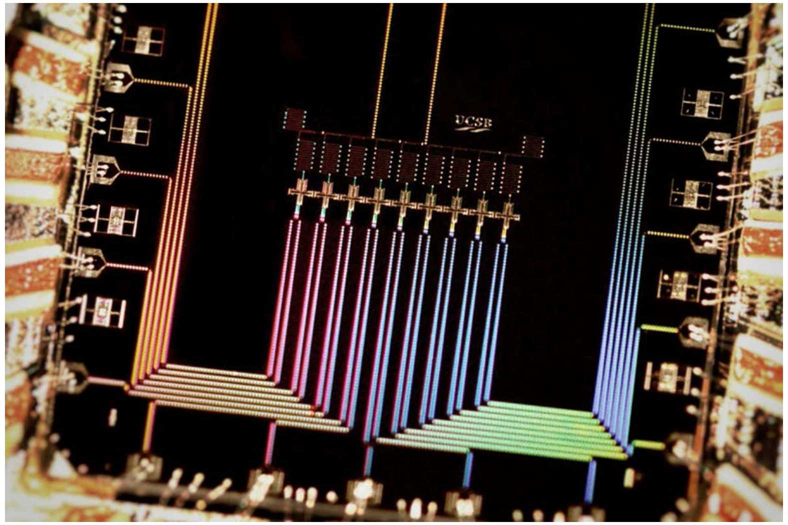
Ion Trap QC path to scale



Slide credit: Chris Monroe, from Patrick Kennedy, https://www.servethehome.com/ionq-quantum-computing-at-hot-chips-33/

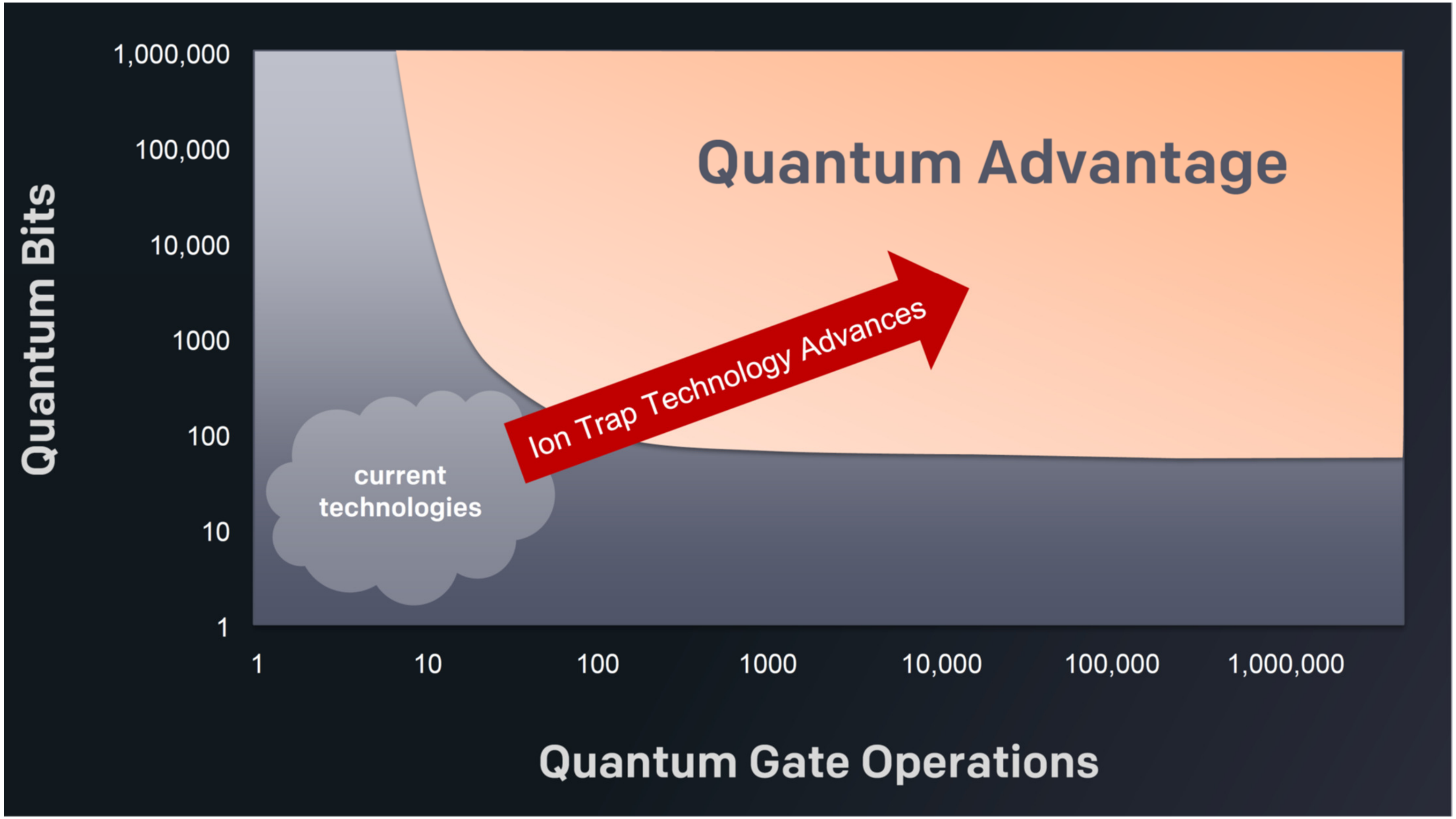
Quantum computer with superconducting qubits





The innards of an IBM quantum computer show the tangle of cables used to control and read out its 127 qubits.
Credits: IBM Nature, 599, 542 (2021); Google, New Scientist (chip)

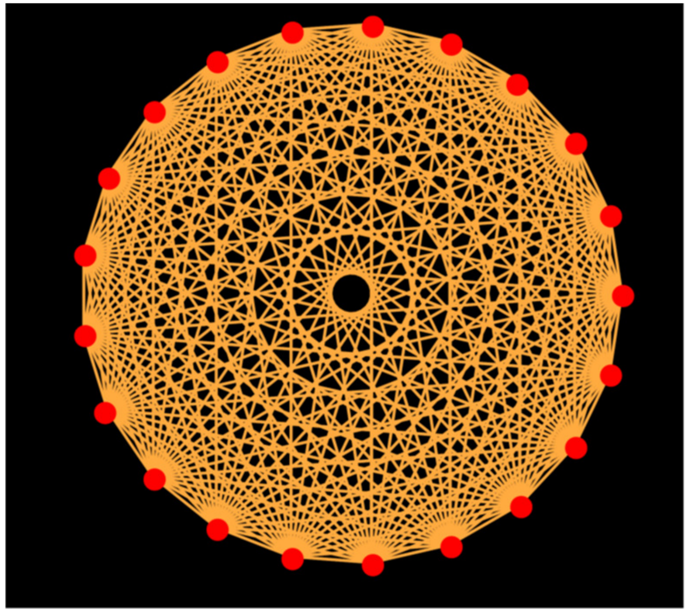
How good is a quantum computer?



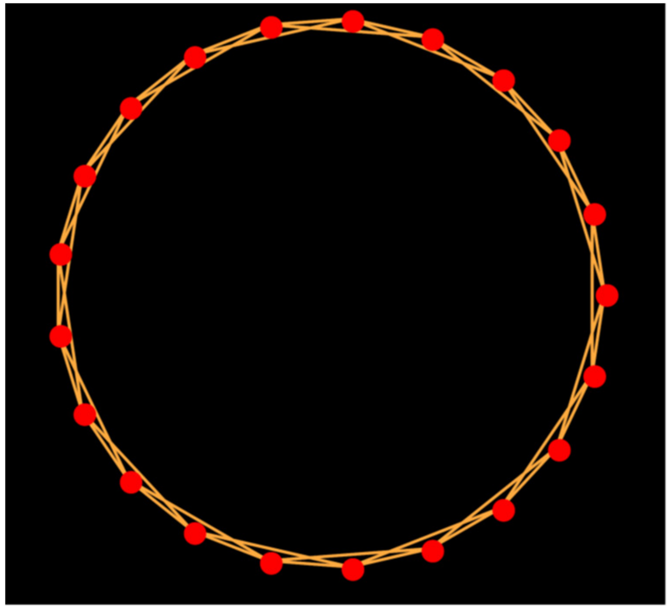
Slide credit: Chris Monroe, https://boulderschool.yale.edu/sites/default/files/files/BoulderLec1%202021.pdf

Connectivity between qubits

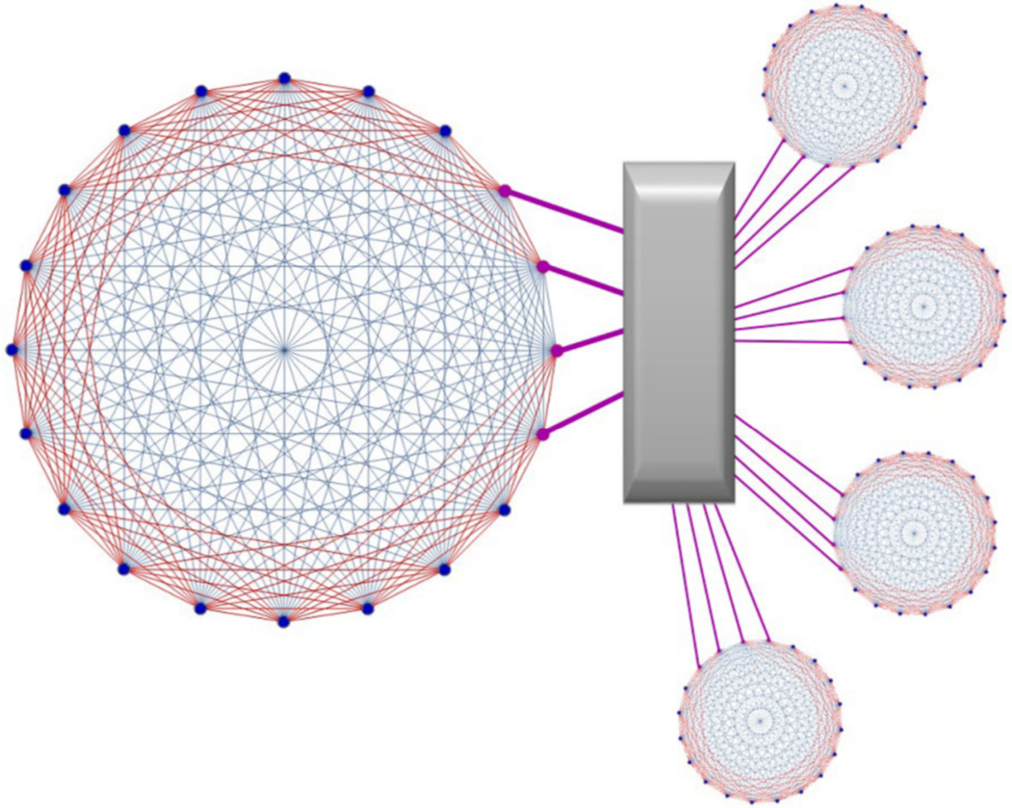
21 qubits fully connected



21 qubits nearest-neighbor connected



Fully connected scaling to
1000 qubits with trapped ions

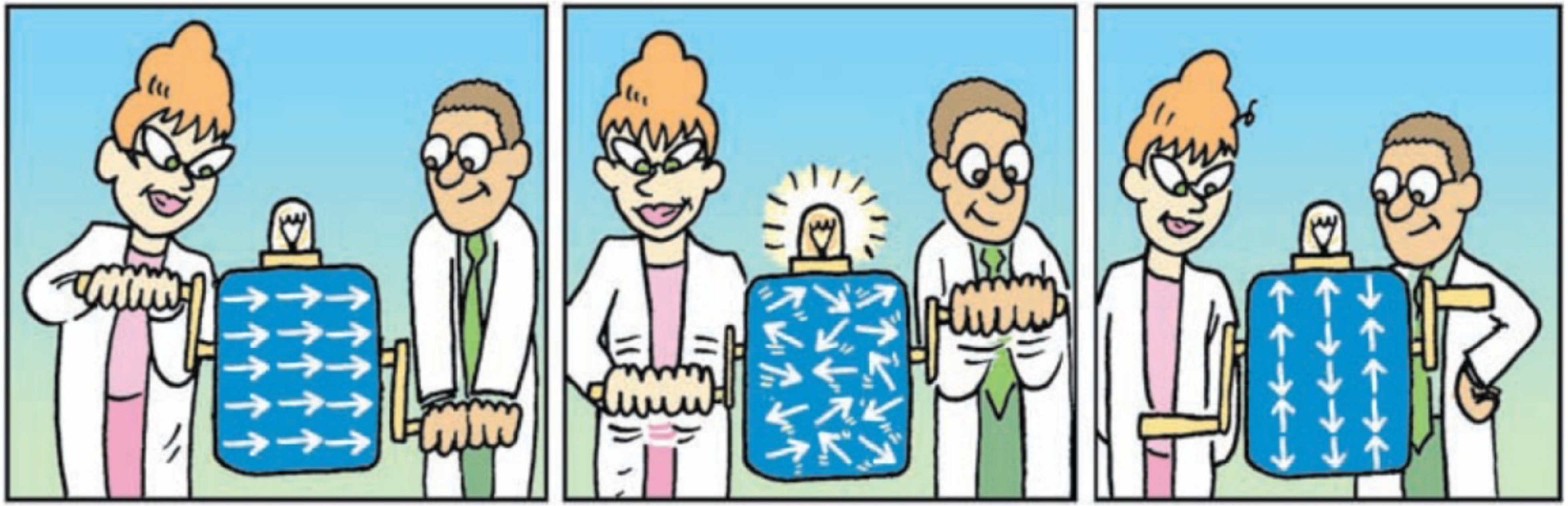


Nature Quant. Inf. 2, 16034 (2016)

Picture credits: Chris Monroe, https://boulderschool.yale.edu/sites/default/files/files/BoulderLec2%202021.pdf
https://boulderschool.yale.edu/sites/default/files/files/BoulderLec3%202021.pdf

What would you do with less then 100 qubits?

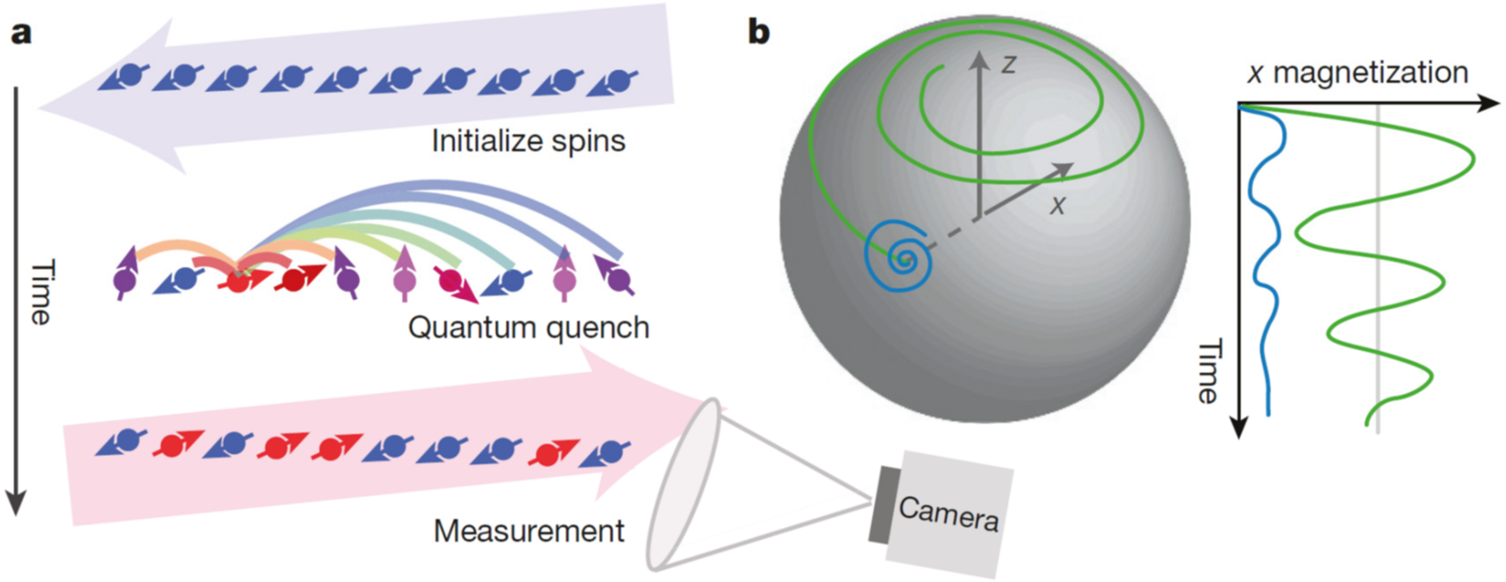
Quantum simulations

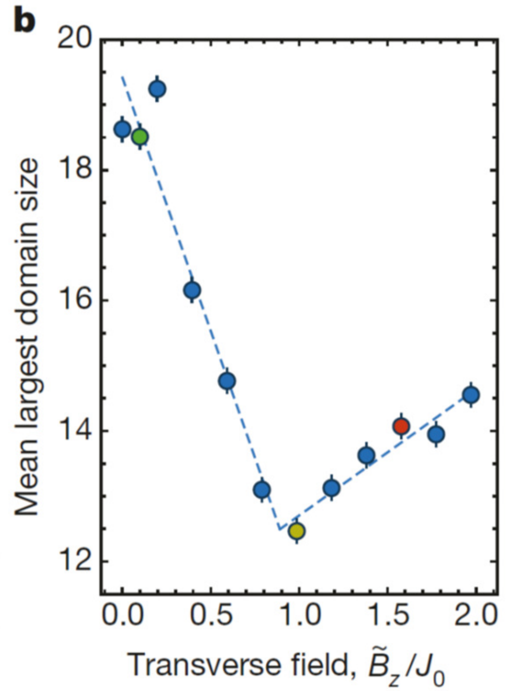


S. Lloyd, Science **319**, 1209 (2008)

Quantum simulation: Exotic Magnetism Dynamical Phase Transition with 50+ Qubits

$$H = \sum_{i<j} J_{ij}\sigma_i^x\sigma_j^x + B_z \sum_i \sigma_i^z$$



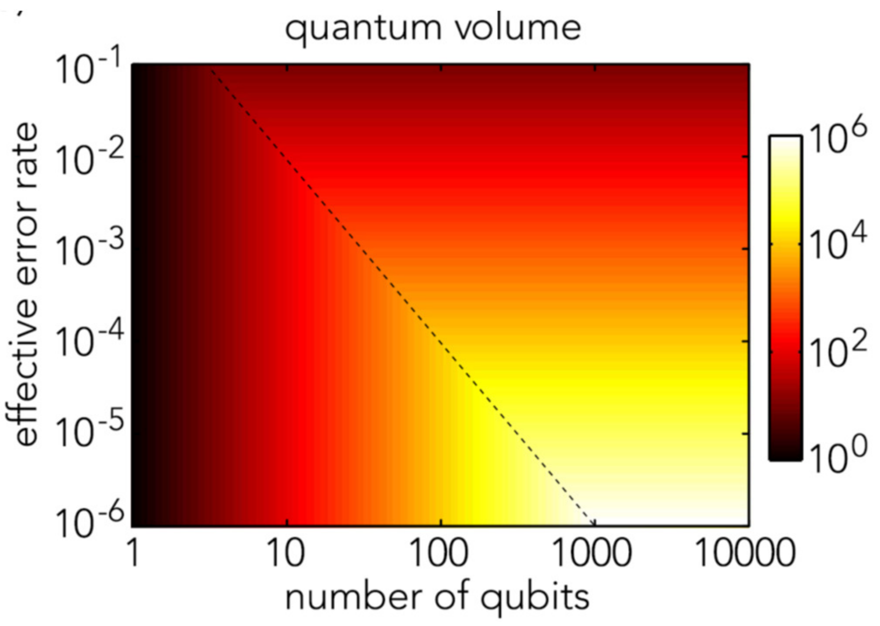


How to compare quantum computers based on different hardware?

Measuring the capabilities of a quantum computer requires a measurement that can summarize the complex operation.

Quantum Volume is a metric that can be used to express the effectiveness of a given quantum computer.

- Number of physical qubits N.
- Connectivity between qubits.
- Number of gates that can be applied before errors or decoherence mask the result.
- Available hardware gate set.
- Number of operations that can be run in parallel.

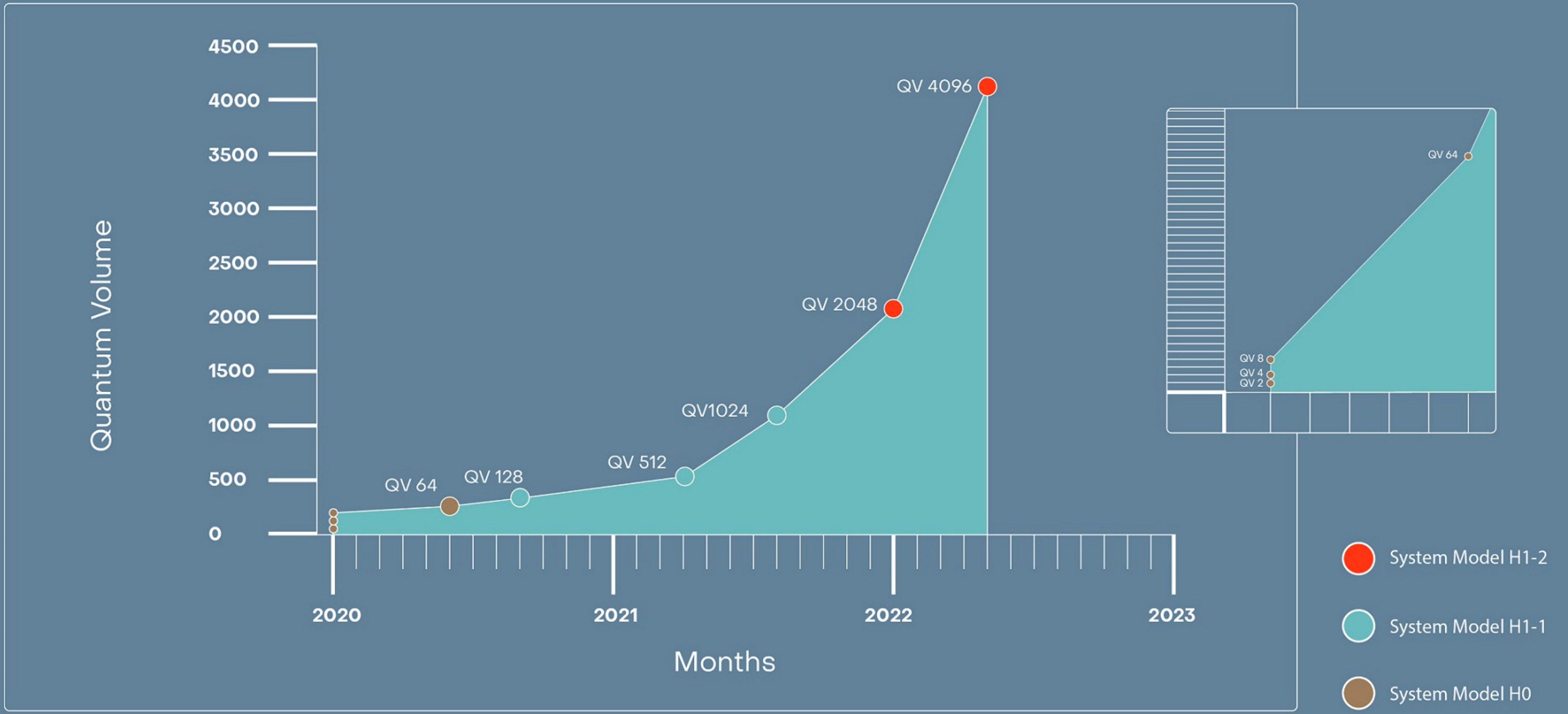


The dashed line denotes the tipping point where circuit depth $d = N$.

Quantum Sci. Technol. 3 (2018) 030503

Achievements in Quantum Volume

Quantinuum's H-Series quantum computers, Powered by Honeywell, again set a new industry bar, doubling quantum volume to 4096 in less than four months.



https://www.hpcwire.com/off-the-wire/quantinuum-announces-quantum-volume-4096-achievement/

What will you do with a 1000 qubits?

- A broad range of quantum simulations in physics and quantum chemistry
- Quantum-assisted machine learning, particularly in the realm of problems that are intractable for classical machine learning.
- Quantum optimization algorithms (possible classical-quantum hybrids)
- Learn how to program and optimize a large-scale quantum computer
- Learn how best to characterize and optimize fault-tolerant protocols

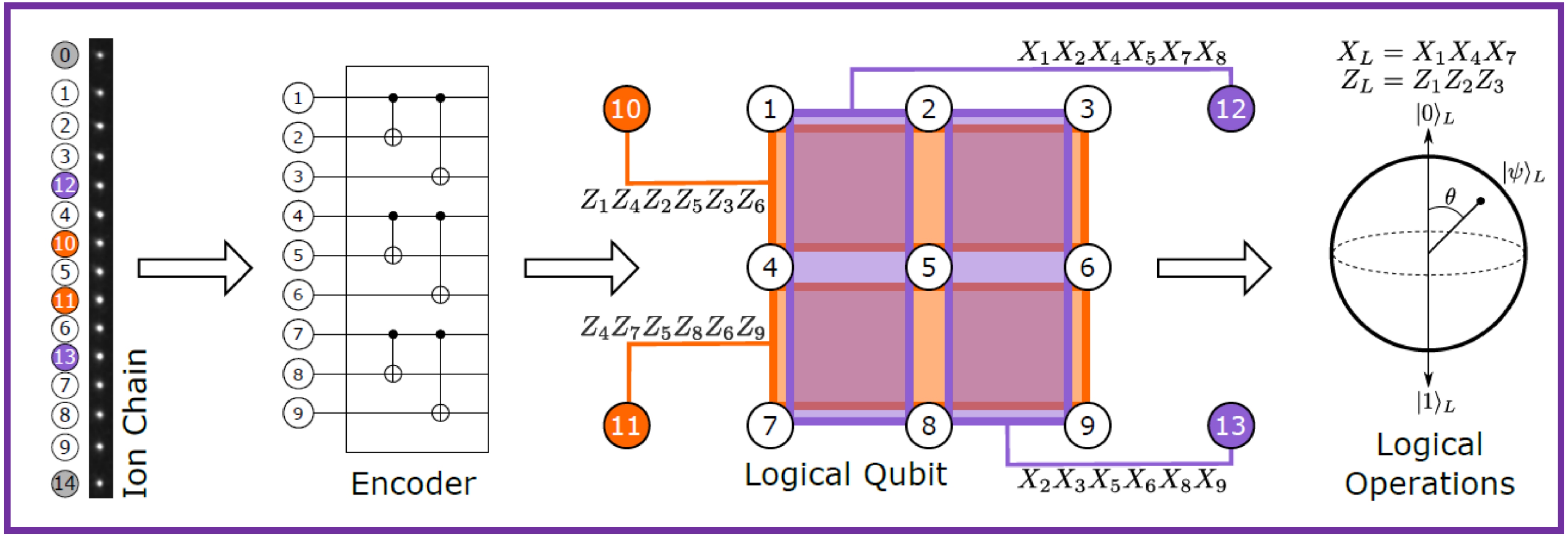
Review: Noisy intermediate-scale quantum (NISQ) algorithms, arXiv:2101.08448v2
Quantum Science and Technology focus issues: https://iopscience.iop.org/journal/2058-9565/page/What-would-you-do-with-1000-qubits

Quantum error correction

Bacon-Shor [[9,1,3]] Subsystem Code
- Can correct any single qubit error (Distance-3)
- Fault tolerant encoding, gates, stabilizer readout, and measurement

4 Weight-6 Stabilizers
- $Z_1Z_4Z_2Z_5Z_3Z_6$
- $Z_4Z_7Z_5Z_8Z_6Z_9$
- $X_1X_2X_4X_5X_7X_8$
- $X_2X_3X_5X_6X_8X_9$

On a 15 ion chain
- 9 Data qubits
- 4 Ancilla qubits
- 2 idle qubits



L. Egan, et al., arXiv 2009.11482 (2020)

EXHIBIT 1 | Quantum-Advantaged Computational Problems

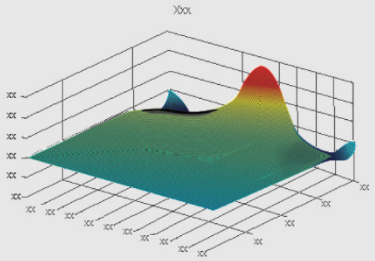
Type of problem | **Useful for…** | **Industry applications include…**

Combinatorial optimization

Useful for… Minimizing or maximizing an objective function, such as finding the most efficient allocation of resources or the shortest total distance among a set of points (e.g., the traveling salesman problem)

Industry applications include…

- Network optimization (e.g., for airlines, taxis)
- Supply chain and logistics optimization
- Portfolio optimization in financial services

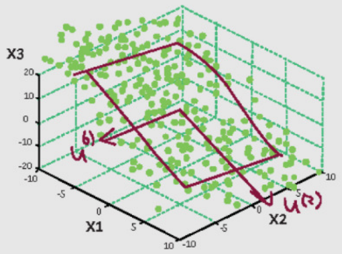


Differential equations

Useful for… Modeling the behavior of complex systems involving fundamental laws of physics (e.g., Navier Stokes for fluid dynamics and chemistry)

Industry applications include…

- Fluid dynamics simulations for automotive and aeronautical design and medical devices (e.g., blood flow analysis)
- Molecular simulation for specialty materials design and drug discovery

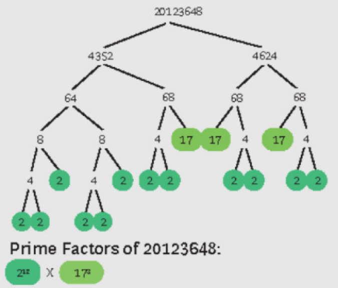


Linear algebra

Useful for… Machine learning tasks involving matrix diagonalization, such as clustering, pattern matching, and principal components analysis, as well as support vector machines, which are ubiquitous in applications across industries

Industry applications include…

- Risk management in quantitative finance
- DNA sequence classification
- Marketing and customer segmentation



Factorization

Useful for… Cryptography and computer security, where the most common protocols today (e.g., RSA) rely on the infeasibility (for classical computers) of factoring the product of two large prime numbers

Industry applications include…

- Decryption and code breaking (e.g., for governments)

Source: BCG analysis.

https://www.bcg.com/en-us/publications/2019/quantum-computers-create-value-when

Where Will Quantum Computers Create Value - and When?

Report of the Boston Consulting Group

EXHIBIT 2 | The Expected Phases of Quantum Computing Maturity

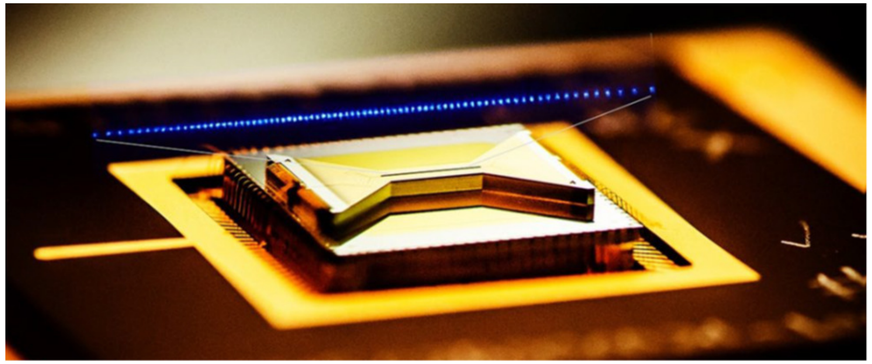
	NISQ era 3–5 years	Broad quantum advantage 10+ years	Full-scale fault tolerance 20+ years
Technical achievement	Error mitigation	Error correction	Modular architecture
Example of business impact	Material simulations that reduce expensive and time-consuming trial-and-error lab testing	Near-real-time risk assessment for financial services firms (e.g., quant hedge funds)	De novo drug design with large biologics that have minimal off-target effects
Estimated impact (operating income)	**$2 billion–$5 billion**	**$25 billion–$50 billion**	**$450 billion–$850 billion**

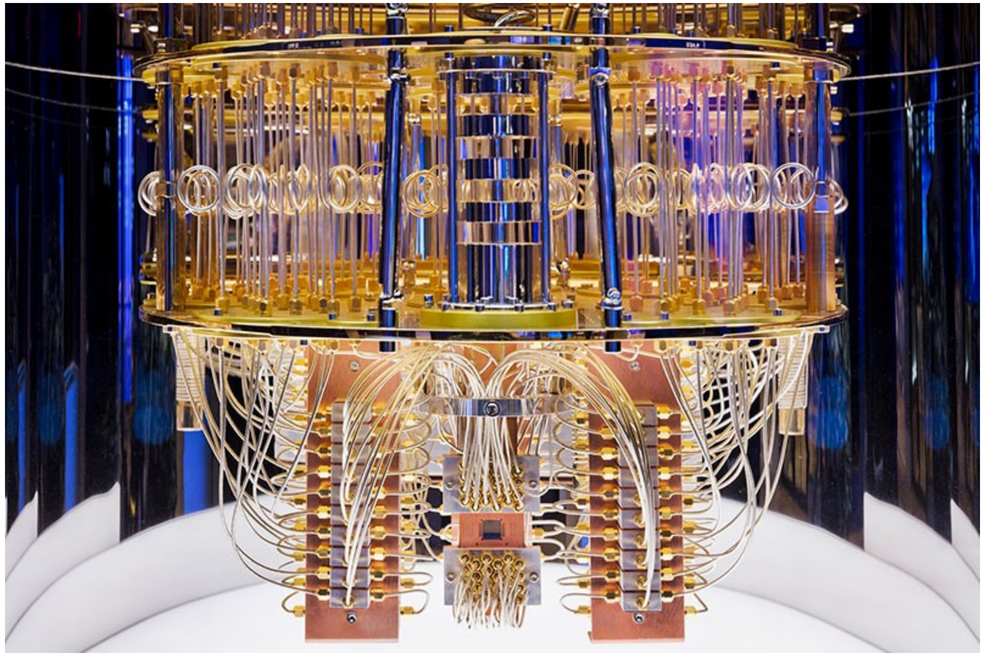
Source: BCG analysis.

https://www.bcg.com/en-us/publications/2019/quantum-computers-create-value-when

Quantum computing: predicting the future!

2022





?