

QSEG650/PHYS650

INTRODUCTION TO QUANTUM COMPUTATION AND QUANTUM INFORMATION

**LECTURES 1 - 2**

**INTRODUCTION:**

**THE WEIRD WORLD OF QUANTUM INFORMATION**

---

**WHAT WOULD YOU DO WITH A 1000 QUBITS?**

Marianna Safronova

**Please ask questions during the lectures!**

## **THE BENEFITS OF ASKING QUESTIONS**

**You will learn more.**

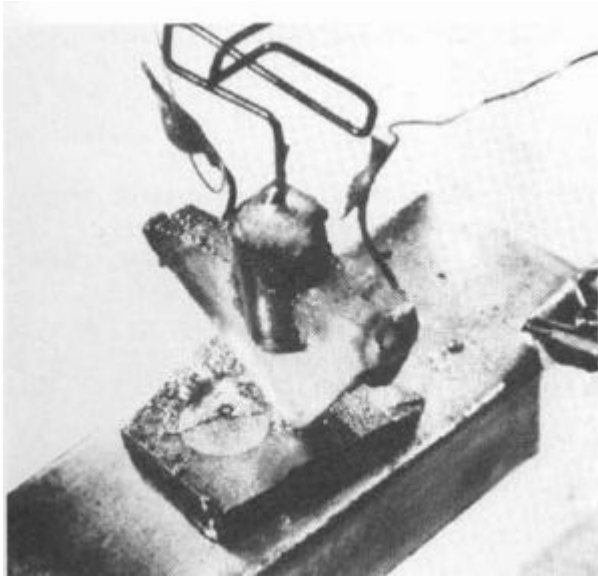
**The lectures will be more fun for you.**

**Great practice for the future.**

**You will stay awake 😊**

# Fantastic story of classical computing

1947



1981



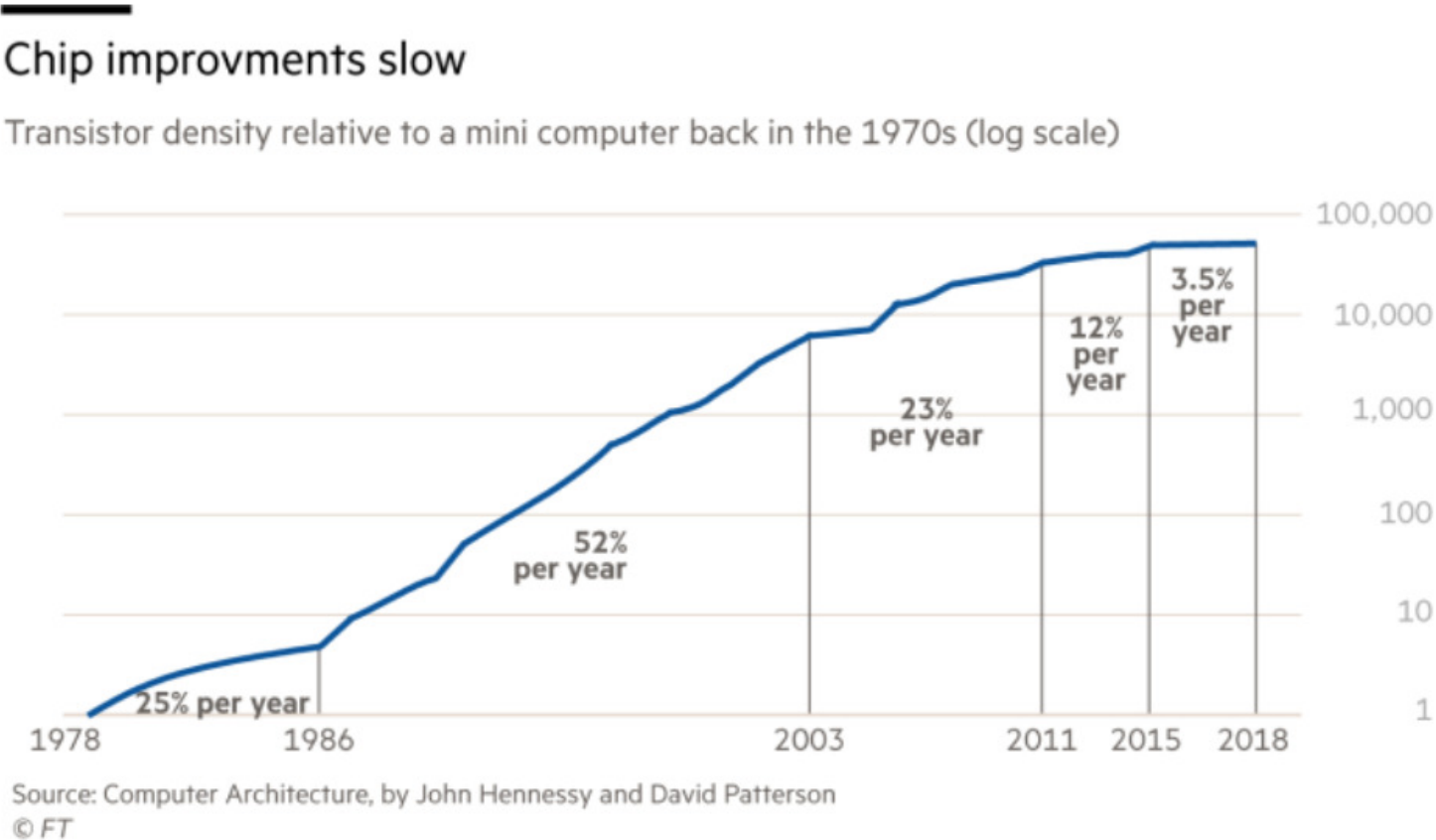
2010s



# The end of Moore's law

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

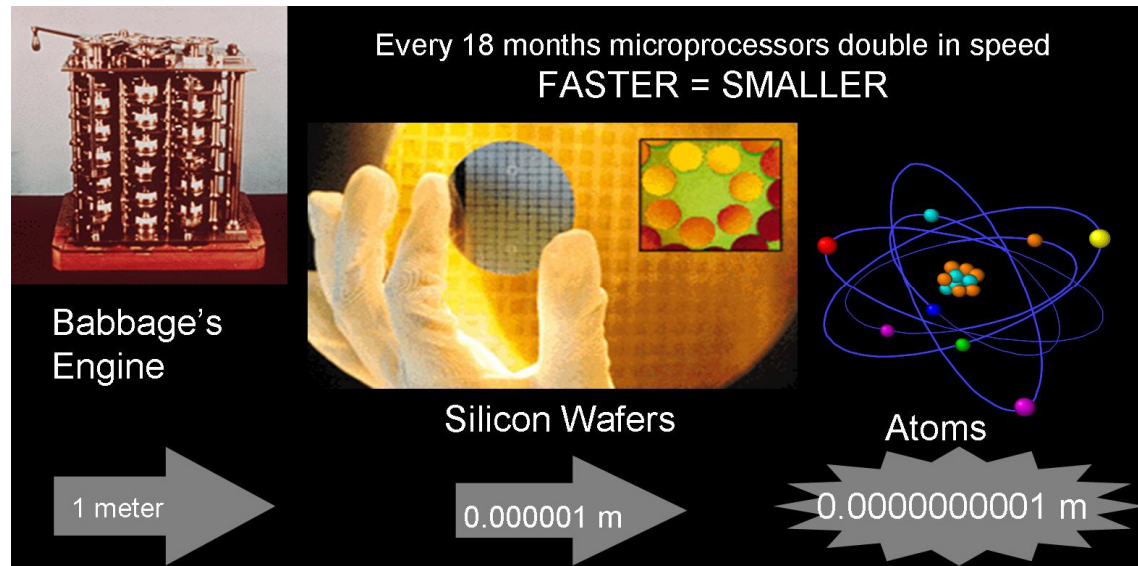
Gordon Moore, 1965



Transistor density: average number of transistors per unit area

# Information is physical

Any processing of information  
is always performed by physical means



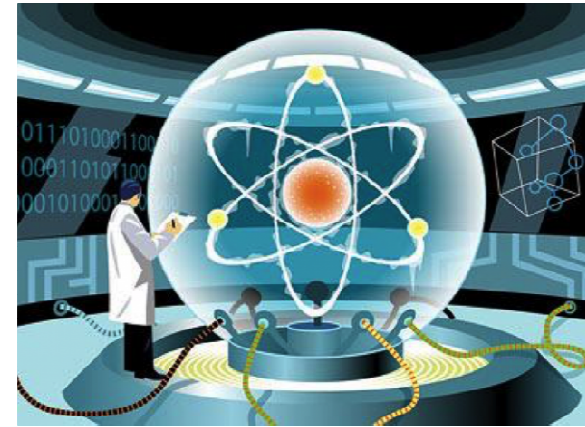
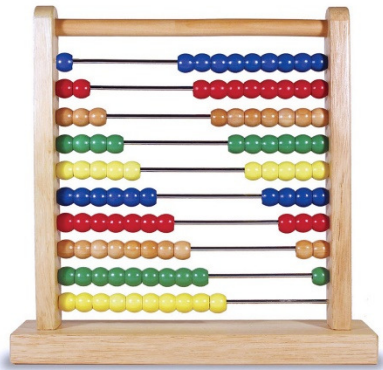
Bits of information obey laws of classical physics.

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



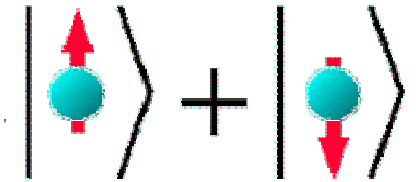
Fundamental building blocks  
of classical computers:

BITS

STATE:  
Definitely  
0 or 1

Fundamental building blocks  
of quantum computers:

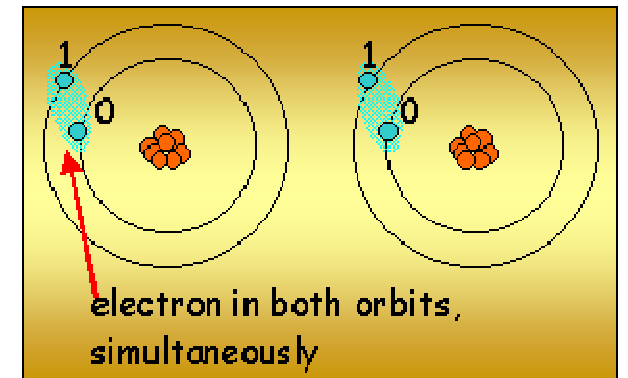
Quantum bits  
or  
QUBITS



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

Superposition:

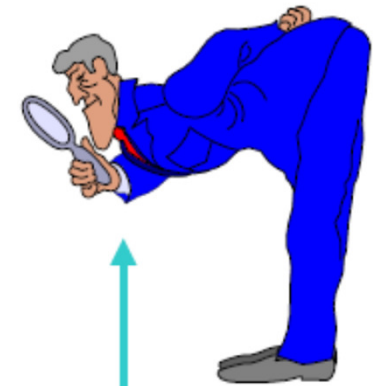
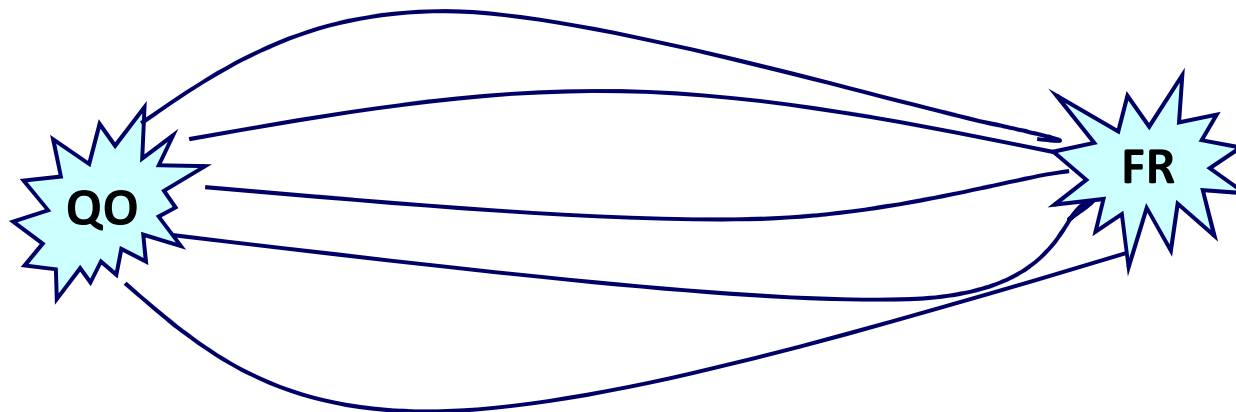
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$



# 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



↑  
Look at final  
answer!



# 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  $\alpha$  and  $\beta$  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!

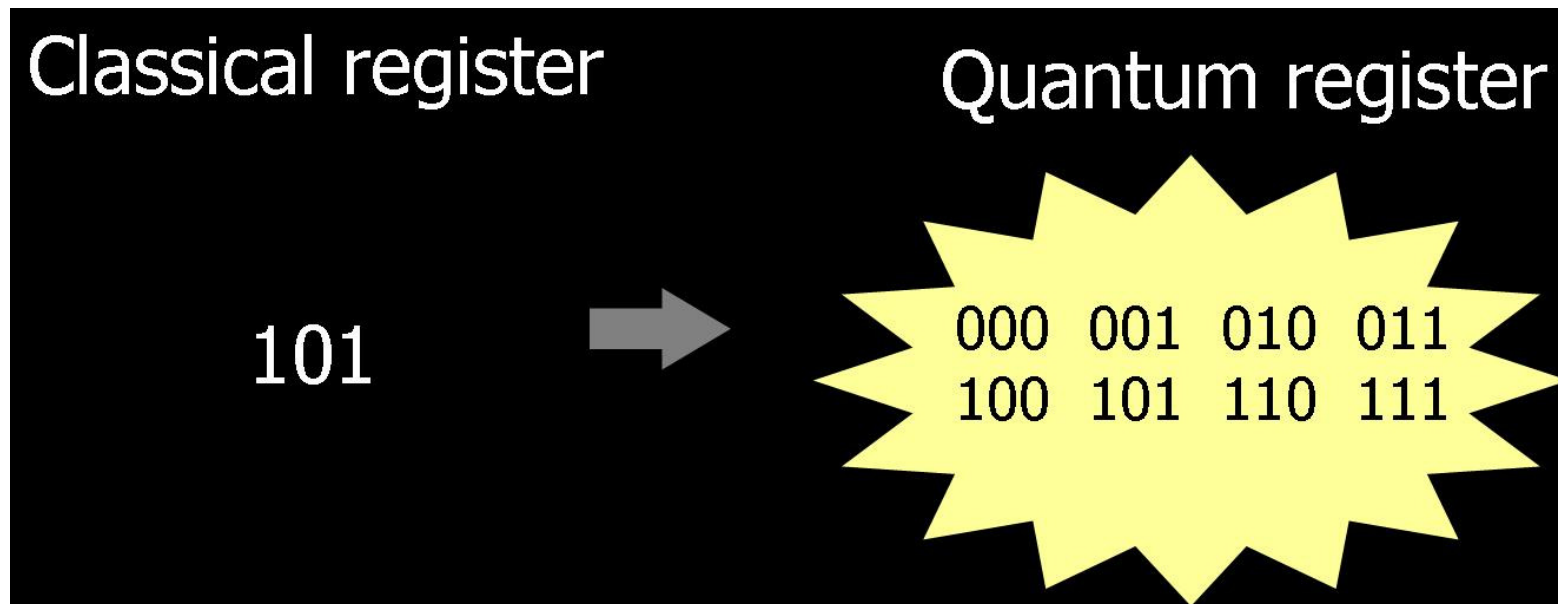
$$|\alpha|^2 + |\beta|^2 = 1$$



# Multiple qubits

*Hilbert space is a big place!*

*- Carlton Caves*



*Hilbert space is a big place!*

*- Carlton Caves*

## Multiple qubits

- 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
<b>500 qubits</b>	<b>More amplitudes than our estimate of number of atoms in the Universe!!!</b>

# Entanglement

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

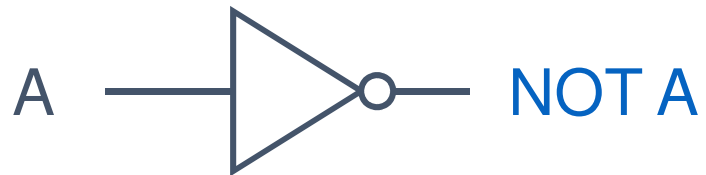
Results of the measurement			
First	qubit	0	1
Second	qubit	0	1

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

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!

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

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \boxed{Z} \longrightarrow \alpha|0\rangle - \beta|1\rangle$$

Hadamard gate:

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

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

# Universality: quantum computation

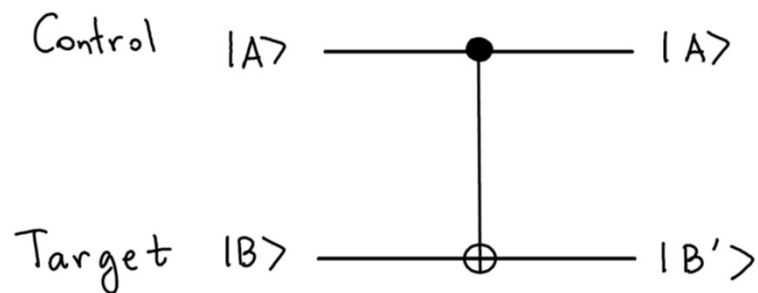
How many quantum gates do we need to build any quantum gate?

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

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

Only one two-qubit gate is needed!

Controlled-NOT (CNOT) gate



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

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

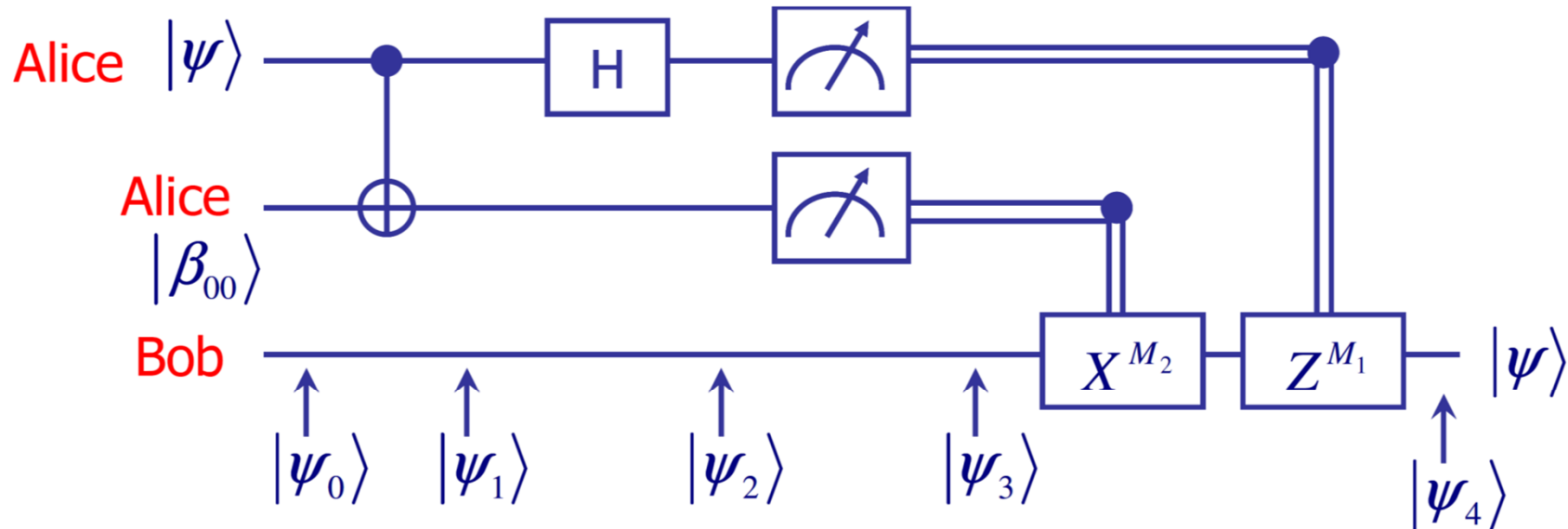
# Quantum circuits: quantum teleportation

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

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



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



# 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

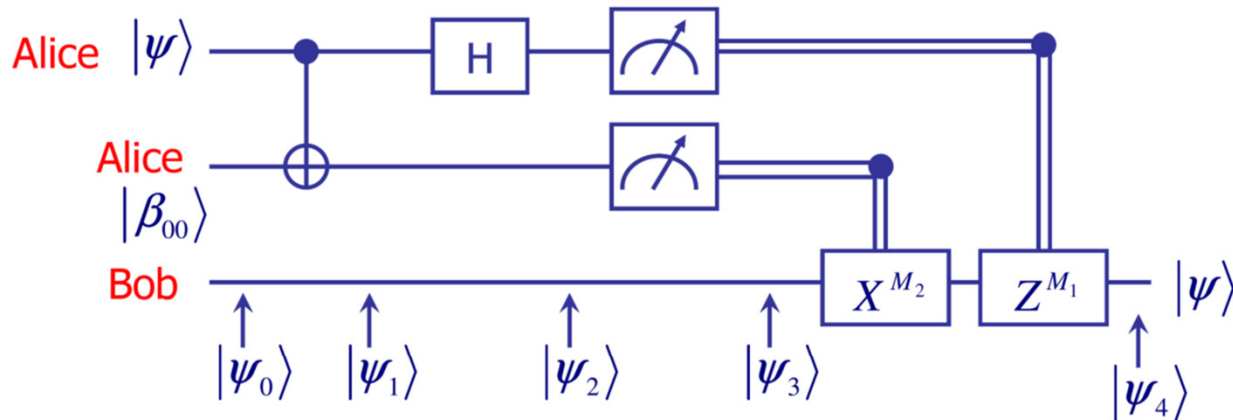
## How does it work?

- 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  $|\psi\rangle$  !

## Teleportation scheme

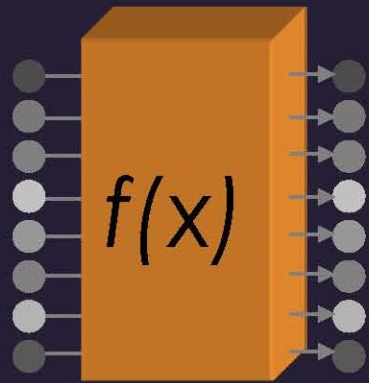


$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

## Good News...

parallel processing  
on  $2^N$  inputs

e.g.,  $N=3$  qubits

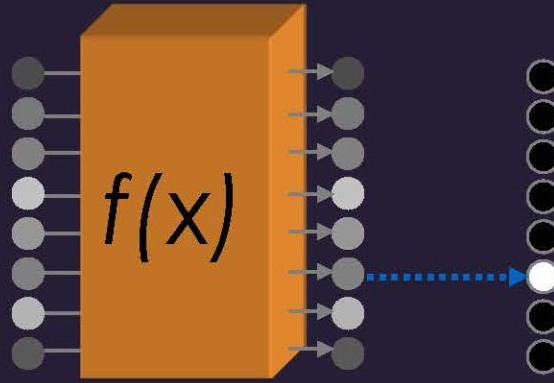


$$a_0|000\rangle + a_1|001\rangle + a_2|010\rangle + a_3|011\rangle \\ a_4|100\rangle + a_5|101\rangle + a_6|110\rangle + a_7|111\rangle$$

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

## ...Bad News...

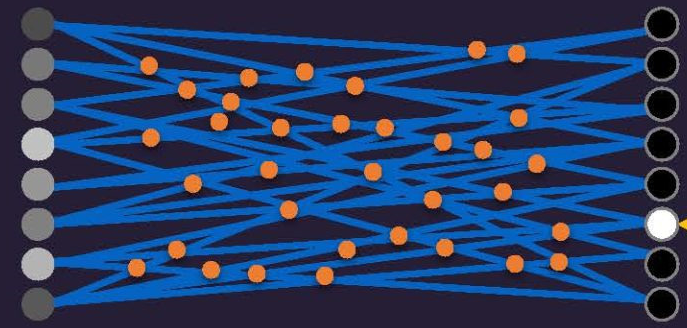
measurement gives  
random result



## ...Good News!

quantum interference

Need smart algorithms!



David Deutsch  
(early 1990s)

**depends  
on all inputs**

# Application: Factoring Numbers

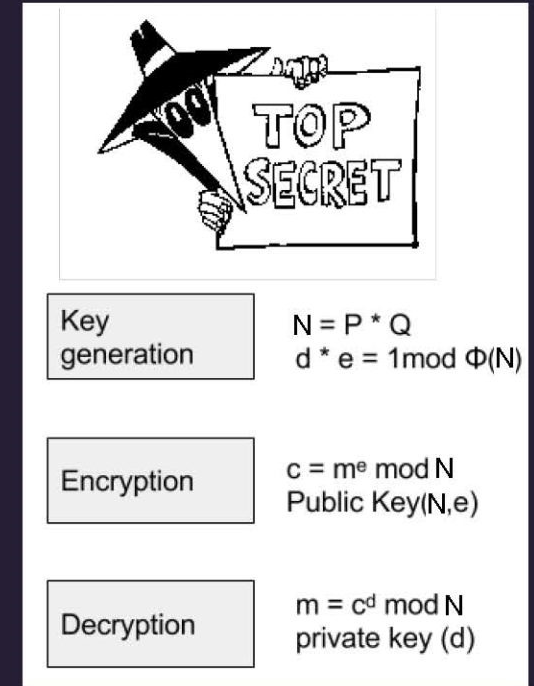
A quantum computer can factor numbers **exponentially faster** than classical computers

P. Shor (1994)

$$39 = 3 \times 13 \text{ (...easy)}$$

$$38647884621009387621432325631 = ? \times ?$$

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:  $time \sim (\log \log n)(\log n)n^2$

# Quantum cryptography

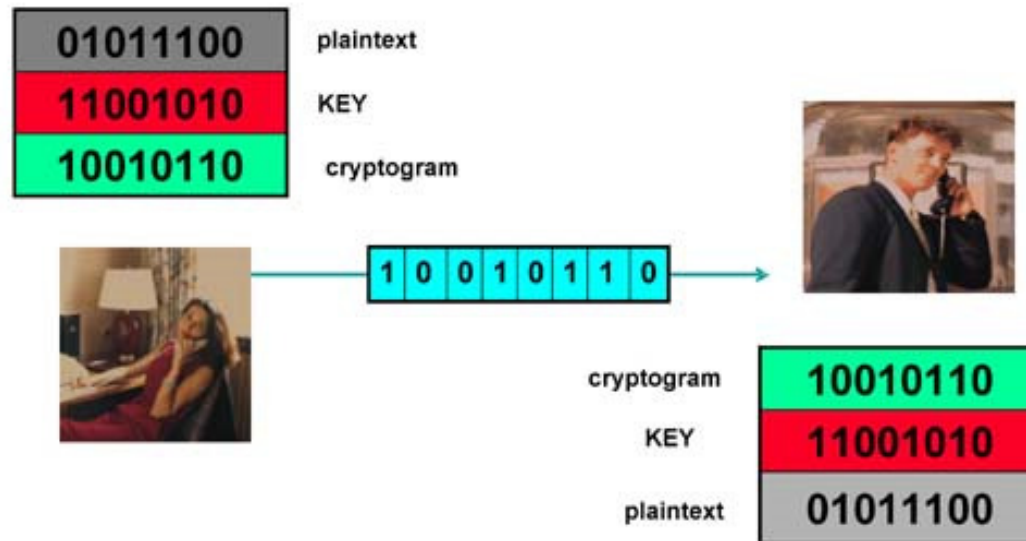
# Classical cryptography

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



# 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.

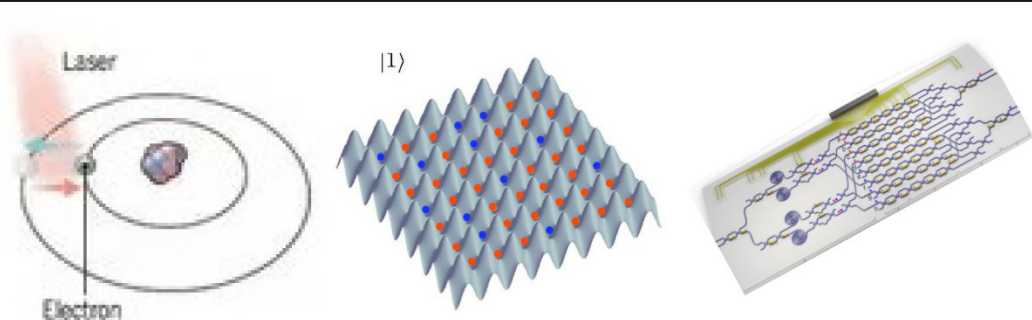
**Ability to perform (universal) logical operations.**

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

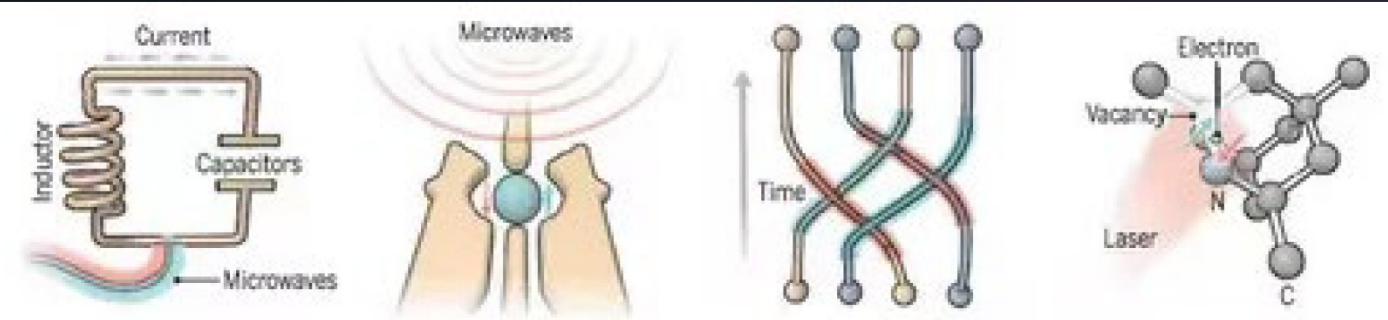
Ability to efficiently **read out the result.**

# Quantum Computer Technologies

## Natural Qubits



## Synthetic Qubits



	Trapped Ions	Neutral Atoms	Photonics	Superconducting Loops	Silicon Quantum Dots	Topological Qubits	Diamond Vacancies
<b>Trapped Ions</b> 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.	<b>Neutral Atoms</b> Neutral atoms, like ions, store qubits within electronic states. Laser activates the electrons to create interaction between qubits.	<b>Photonics</b> 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.	<b>Superconducting Loops</b> A resistance-free current oscillates back and forth around a circuit loop. An injected microwave signal excites the current into superposition states.	<b>Silicon Quantum Dots</b> These "artificial atoms" are made by adding an electron to a small piece of pure silicon. Microwaves control the electron's quantum state.	<b>Topological Qubits</b> Quasiparticles can be seen in the behavior of electrons channeled through semiconductor structures. Their braided paths can encode quantum information.	<b>Diamond Vacancies</b> 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.	
<b>Qubit Coherence Time (sec)</b>	>1000	1	--	0.00005	0.03	N/A	10
<b>Fidelity</b>	99.9%	97%	--	99.4%	~99%	N/A	99.2%
<b>Qubits Connected</b>	High	Very high; low individual control	--	High	Very Low	N/A	Low
<b>Company Support</b>	IONQ, AQT, Honeywell, Oxford Ionics	Atom Computing, ColdQuanta, QuEra	Psiquantum, Xanadu	Google, IBM, QCI, Rigetti	HRL, Intel, SQC	Microsoft	Quantum Diamond Technologies
<b>Pros</b>	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.
<b>Cons</b>	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.

# Qubits with trapped ions

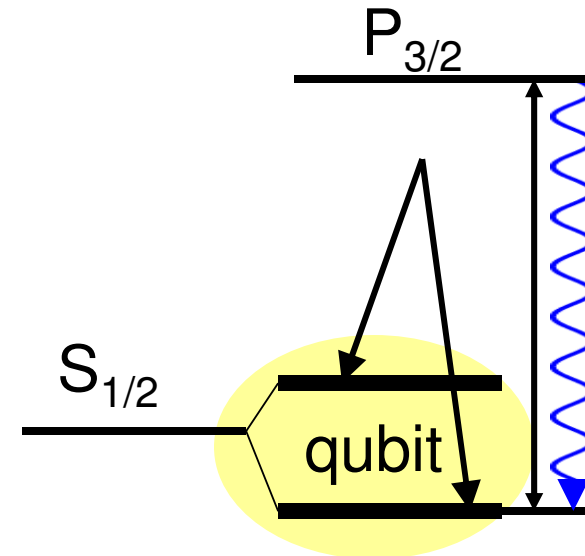
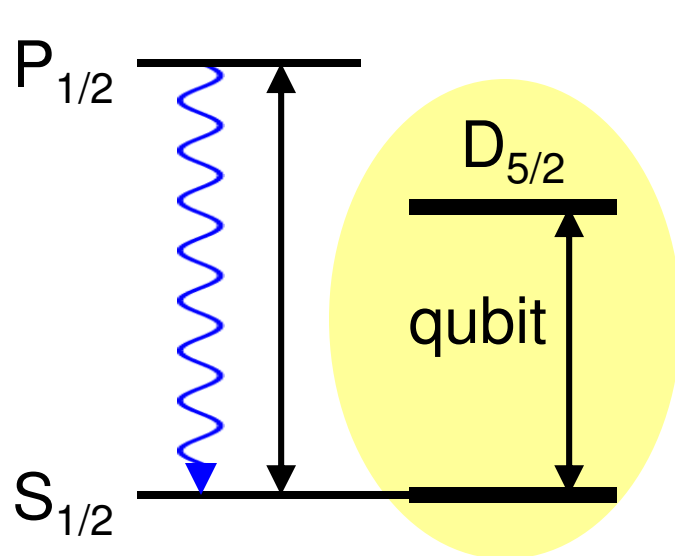
Encoding of quantum information requires **long-lived atomic states**:

- optical transitions

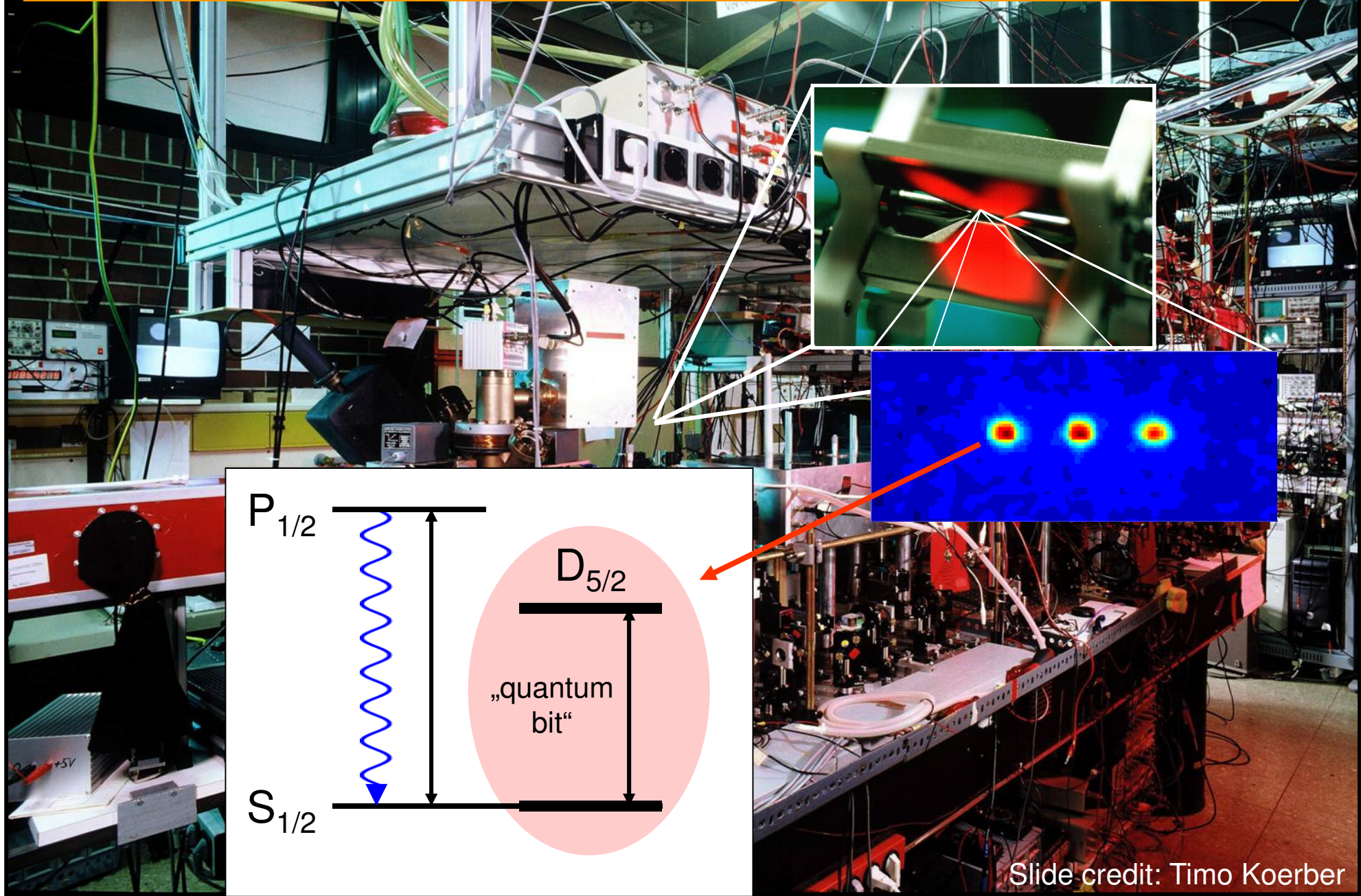
Ca<sup>+</sup>, Sr<sup>+</sup>, Ba<sup>+</sup>, Ra<sup>+</sup>, Yb<sup>+</sup>, Hg<sup>+</sup> etc.

- microwave transitions

<sup>9</sup>Be<sup>+</sup>, <sup>25</sup>Mg<sup>+</sup>, <sup>43</sup>Ca<sup>+</sup>, <sup>87</sup>Sr<sup>+</sup>,  
<sup>137</sup>Ba<sup>+</sup>, <sup>111</sup>Cd<sup>+</sup>, <sup>171</sup>Yb<sup>+</sup>



# Trapped ion quantum computer in 2005



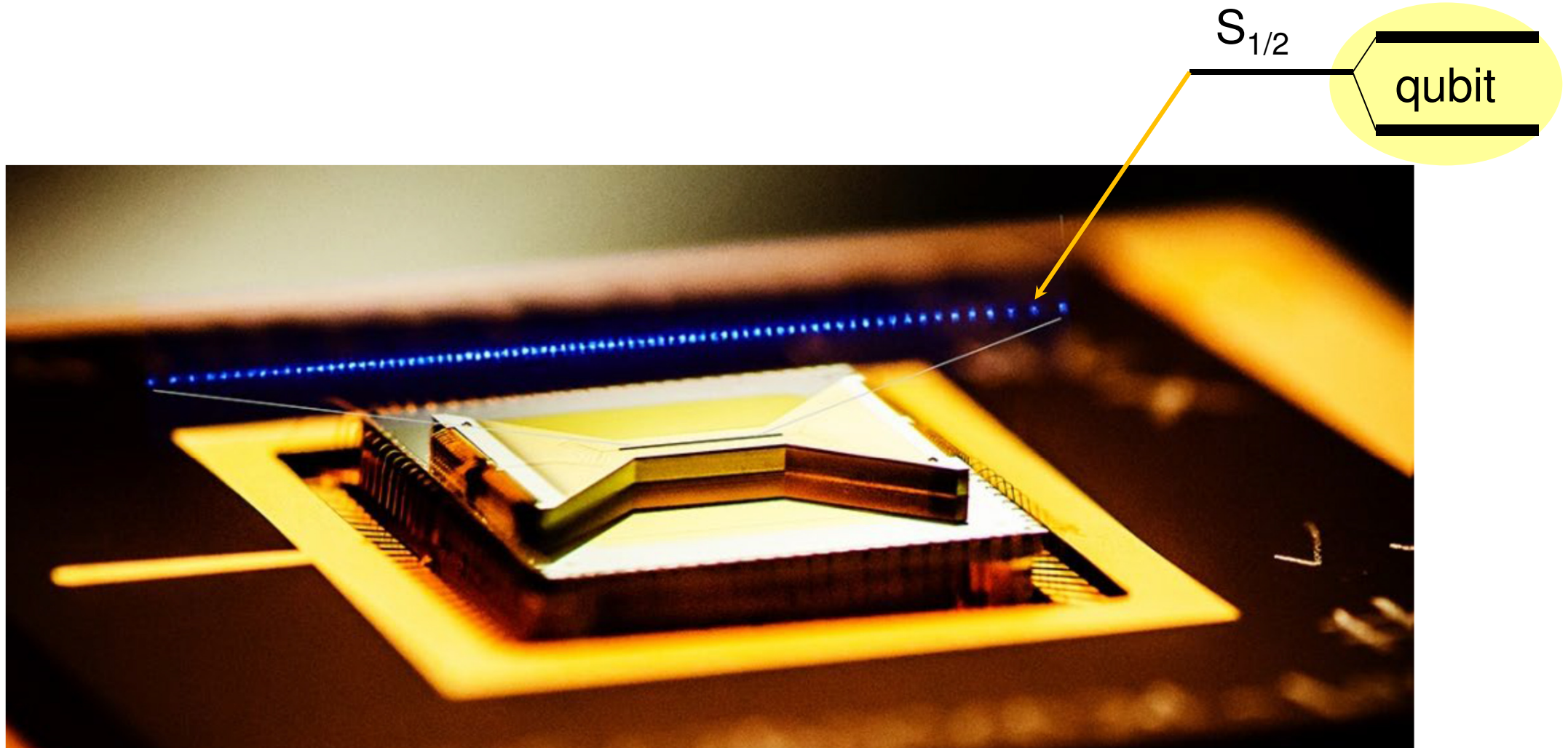
$P_{1/2}$

$S_{1/2}$

$D_{5/2}$

„quantum bit“

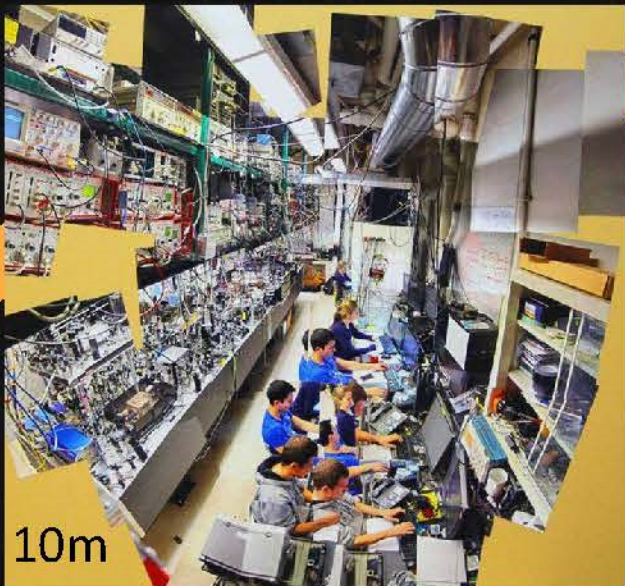
# Ion trap with 80 Yb+ ions



# Ion Trap QC path to scale

Lab scale

2016

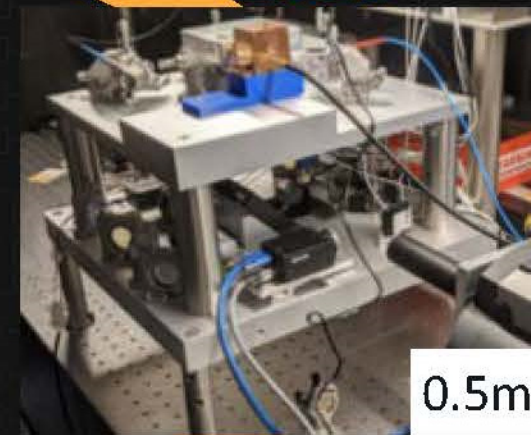


2018



Bench scale

2020

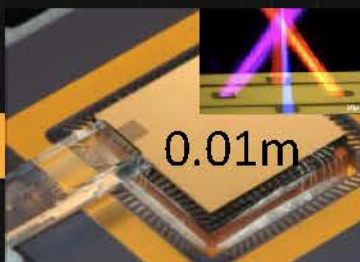


2021



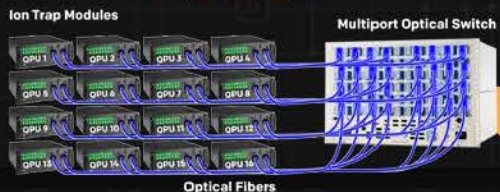
Rackmount scale

2023?

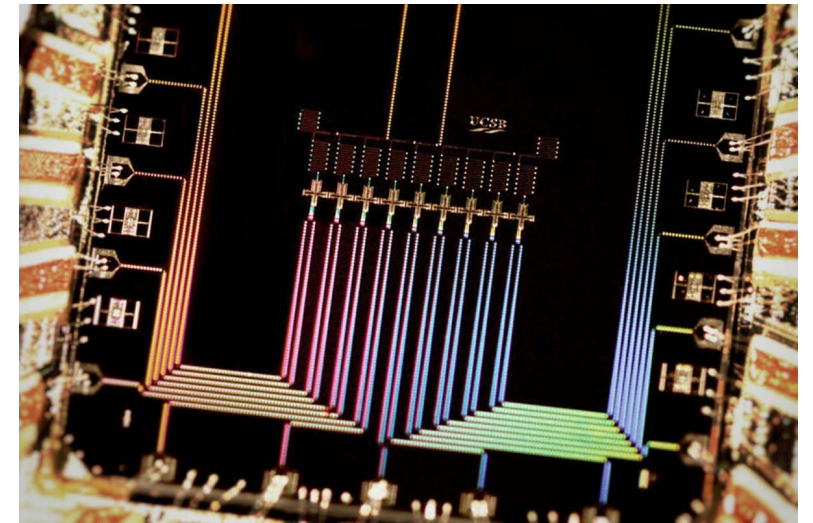
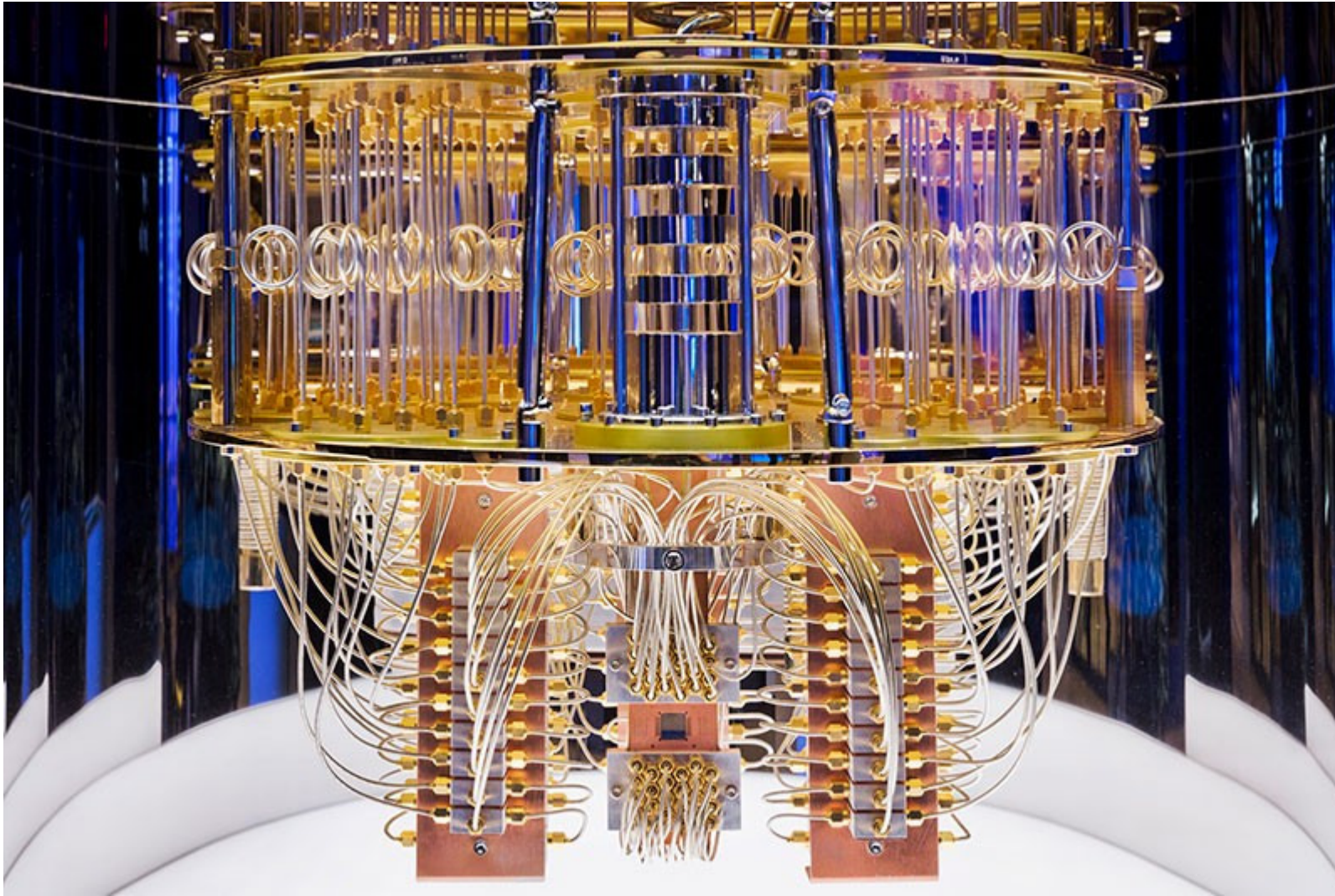


Chip scale

2025?

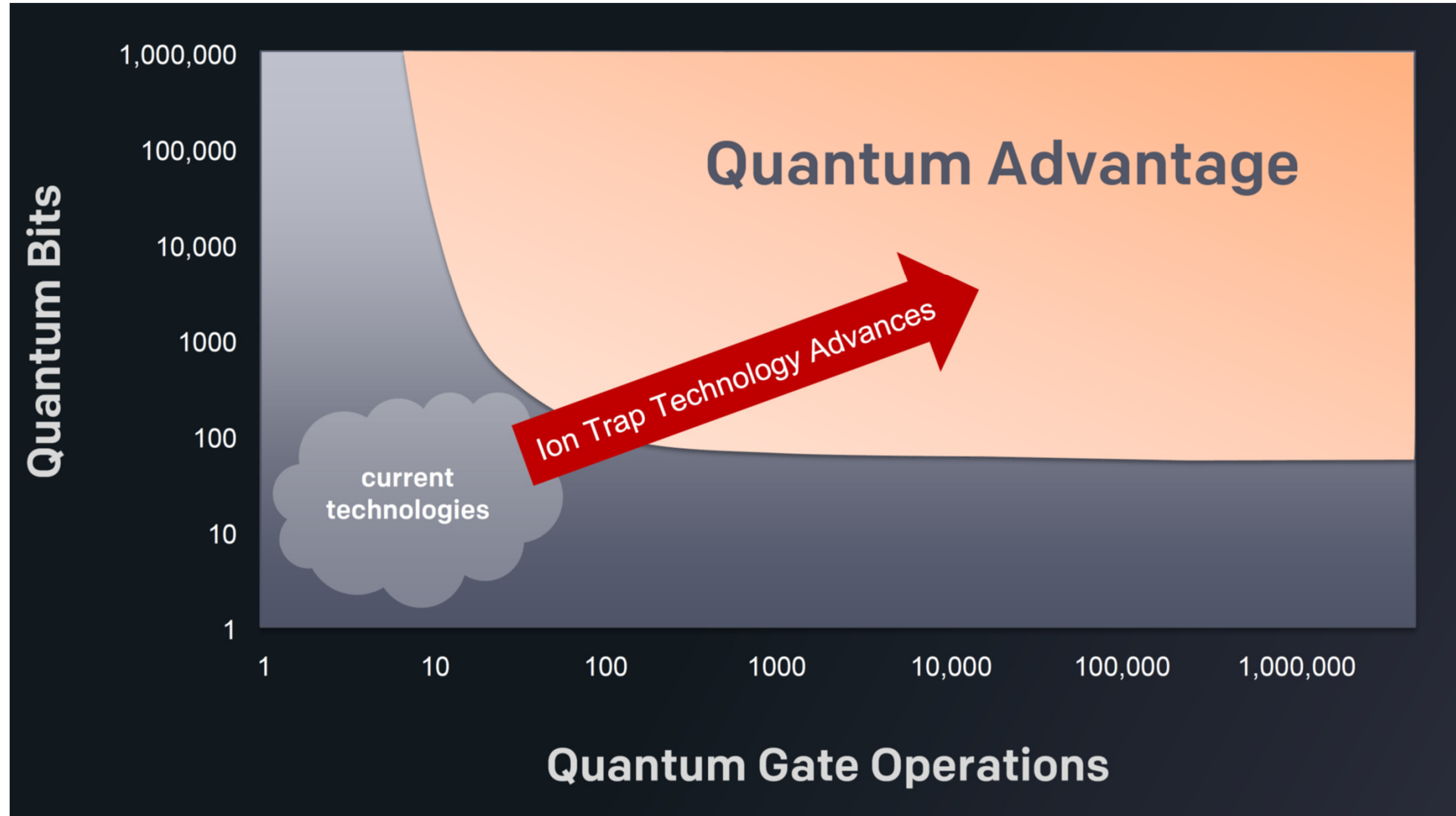


# Quantum computer with superconducting qubits



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)

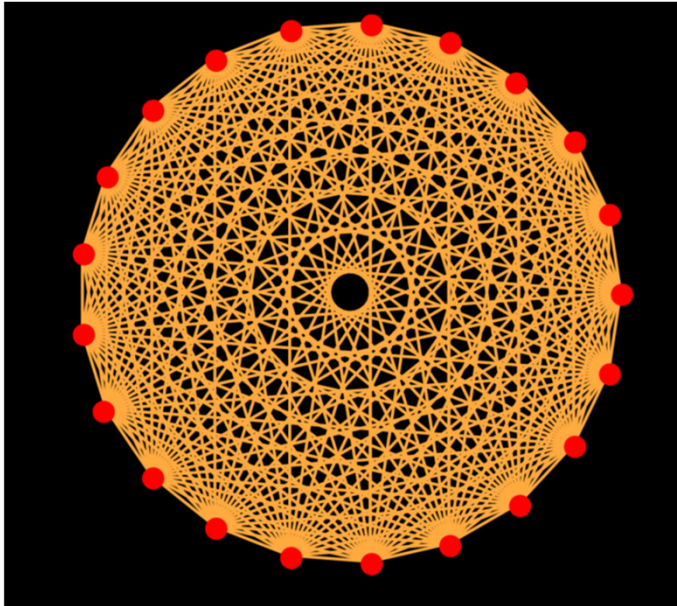
# How good is a quantum computer?



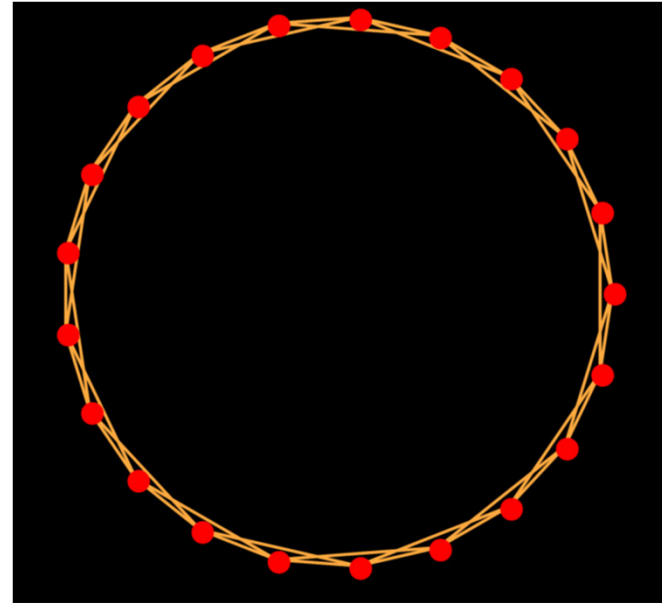


# Connectivity between qubits

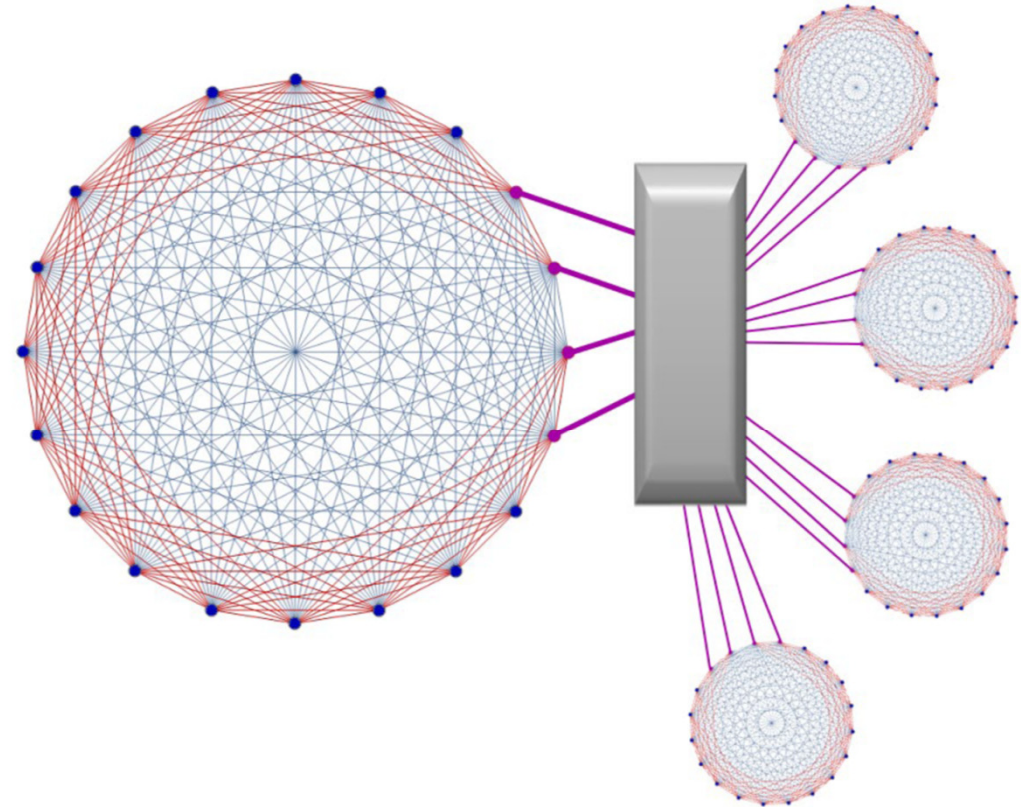
21 qubits fully connected



21 qubits nearest-neighbor connected



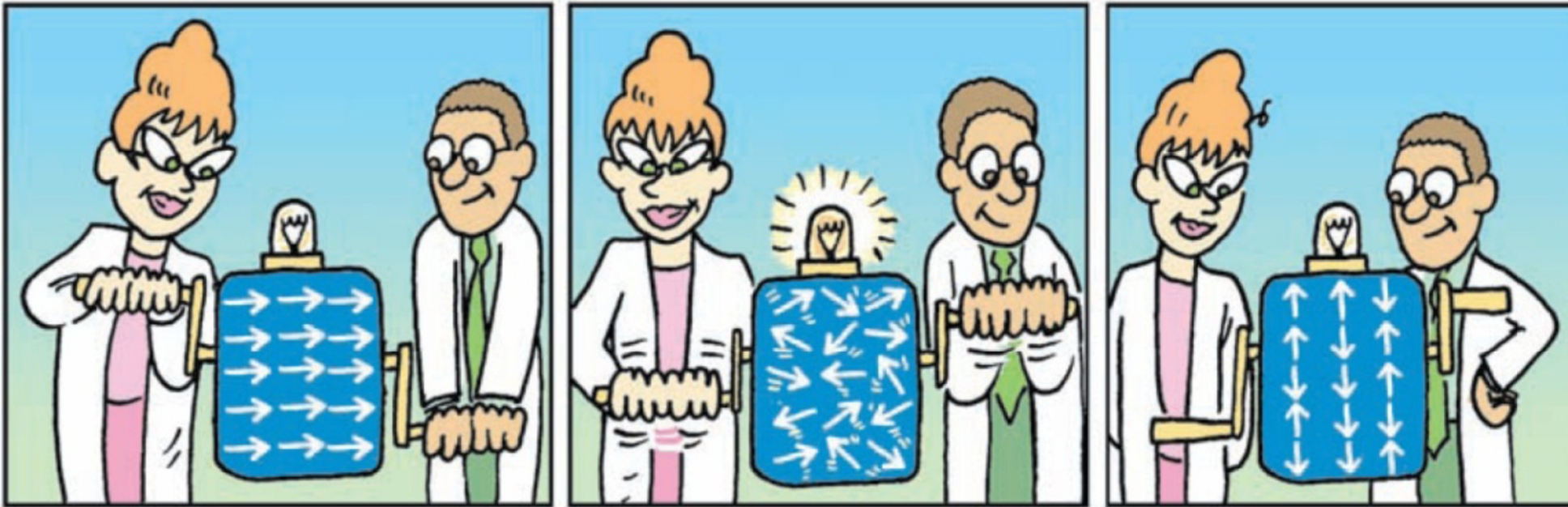
Fully connected scaling to 1000 qubits with trapped ions



Nature Quant. Inf. 2, 16034 (2016)

# What would you do with less than 100 qubits?

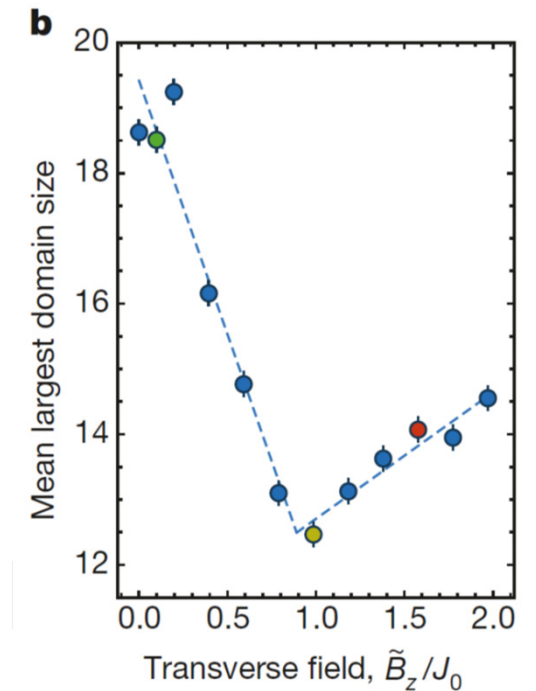
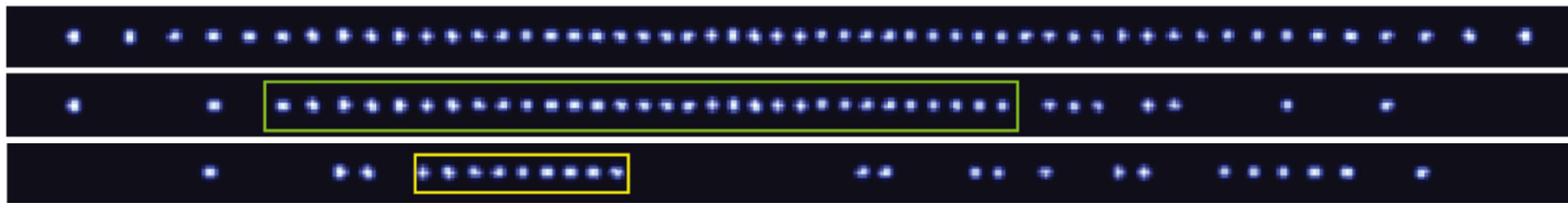
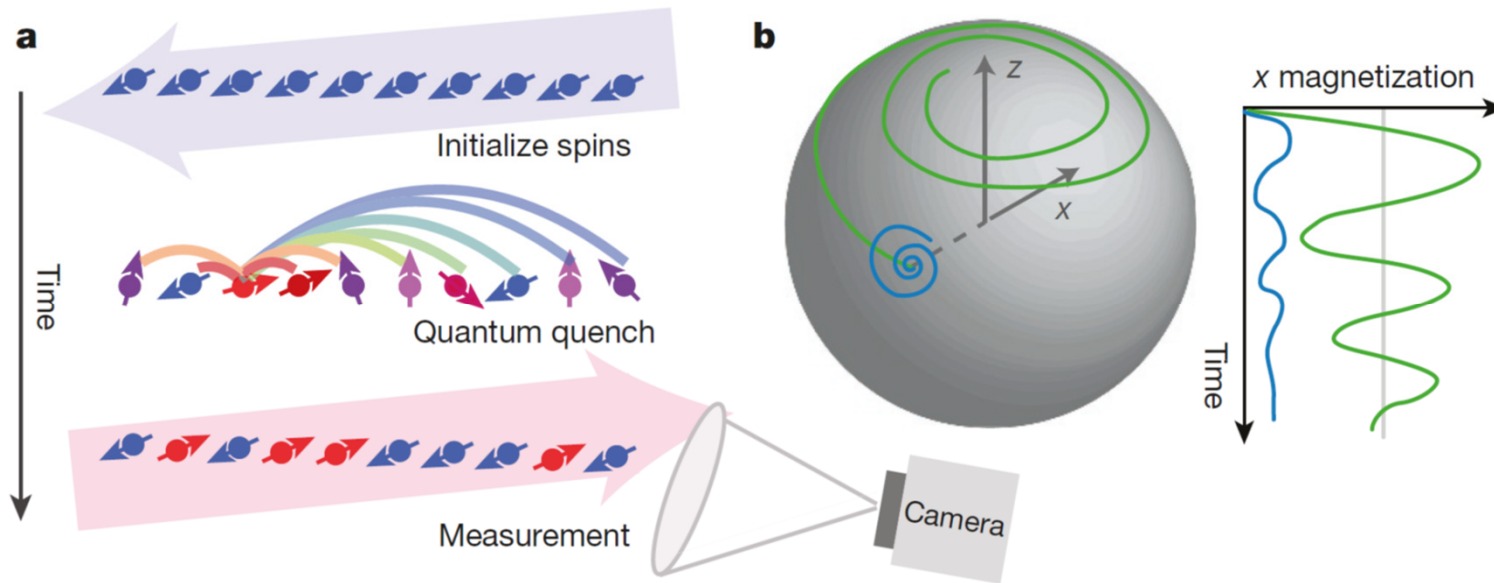
## Quantum simulations



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

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

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

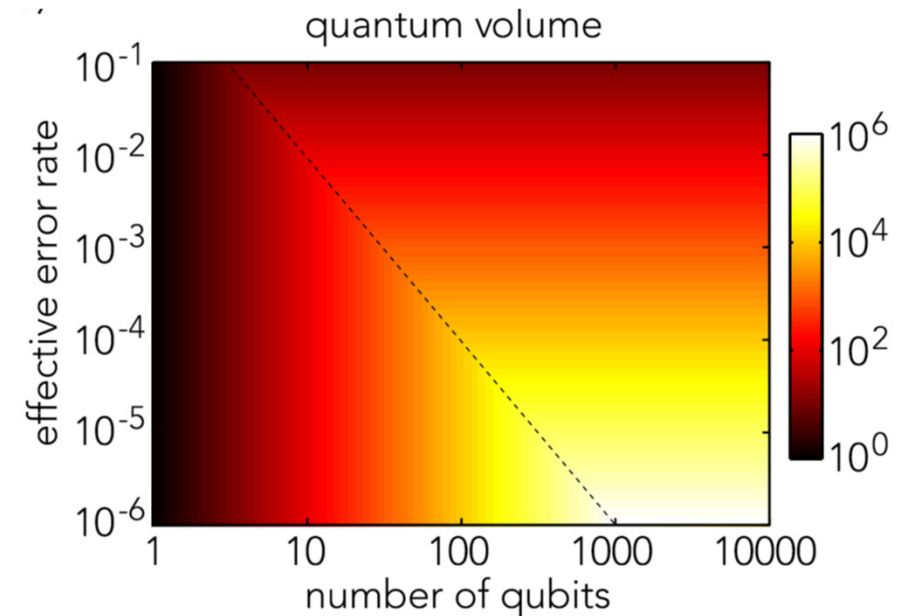


# How to compare quantum computers based on different hardware?

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.

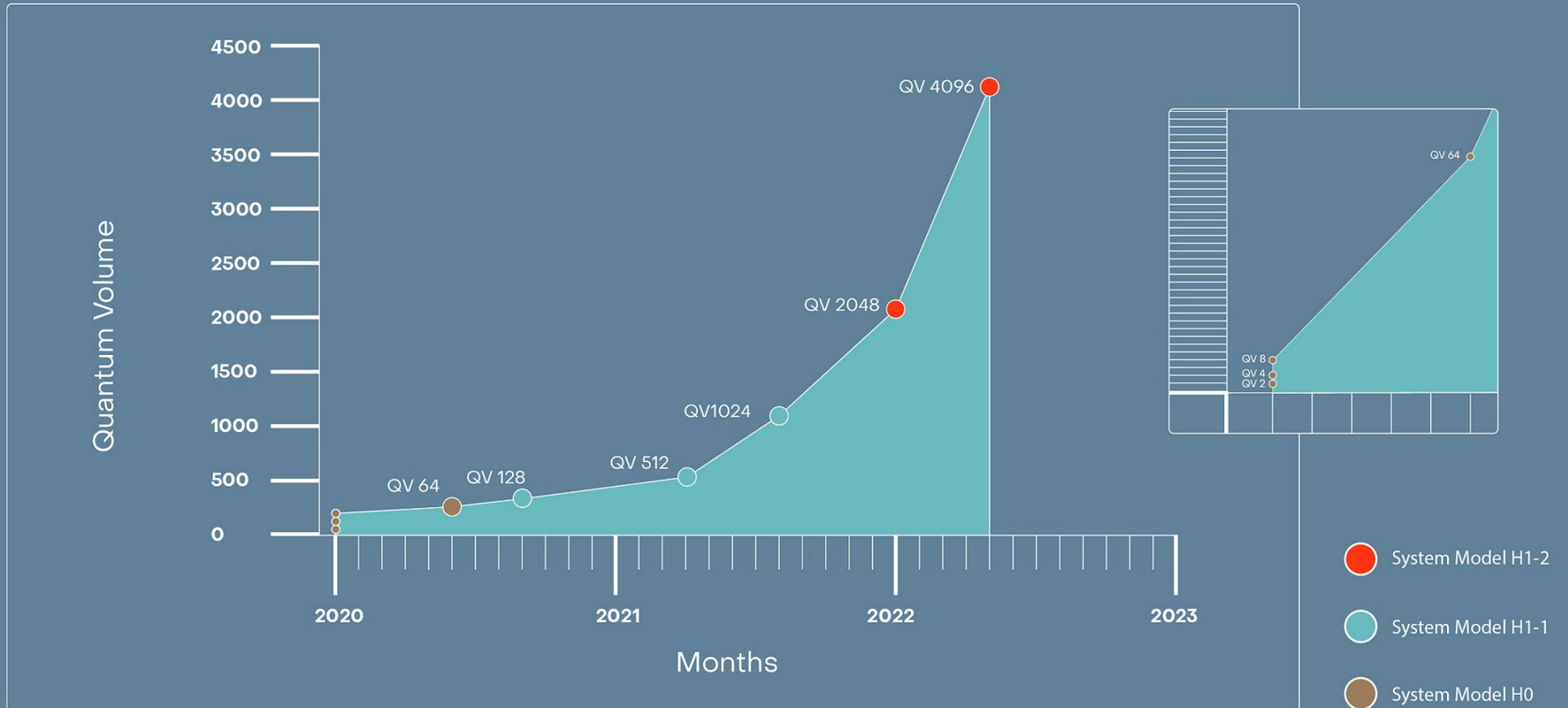
- Number of physical qubits  $N$ .
- Connectivity between qubits.
- Number of gates that can be applied before errors or decoherence mask the result.
- Available hardware gate set.
- Number of operations that can be run in parallel.



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

# 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.



# 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

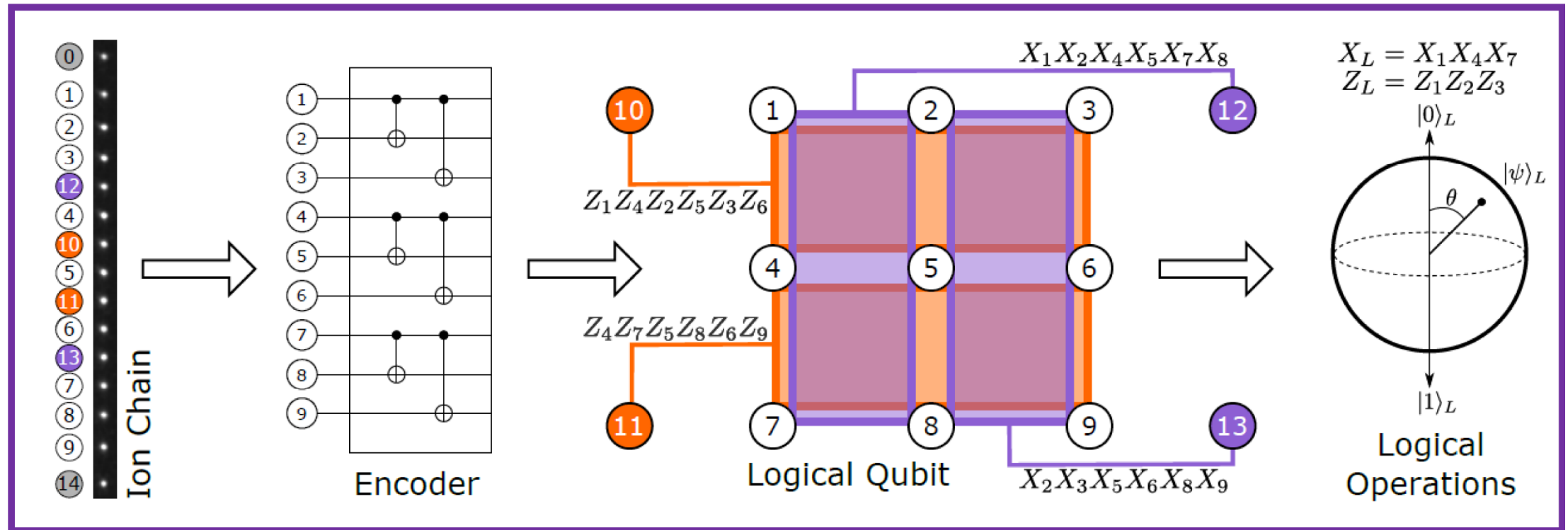
- Can correct any single qubit error (Distance-3)
- Fault tolerant encoding, gates, stabilizer readout, and measurement

## 4 Weight-6 Stabilizers

- $Z_1 Z_4 Z_2 Z_5 Z_3 Z_6$
- $Z_4 Z_7 Z_5 Z_8 Z_6 Z_9$
- $X_1 X_2 X_4 X_5 X_7 X_8$
- $X_2 X_3 X_5 X_6 X_8 X_9$

## On a 15 ion chain

- 9 Data qubits
- 4 Ancilla qubits
- 2 idle qubits



# EXHIBIT 1 | Quantum-Advantaged Computational Problems

## Type of problem



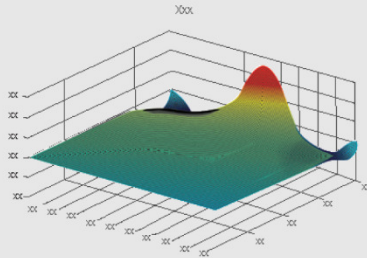
### Combinatorial optimization

## 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...

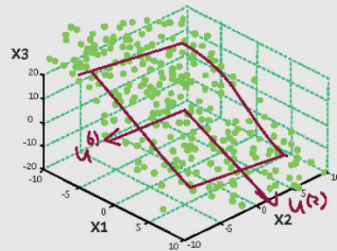
- Network optimization (e.g., for airlines, taxis)
- Supply chain and logistics optimization
- Portfolio optimization in financial services



### Differential equations

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

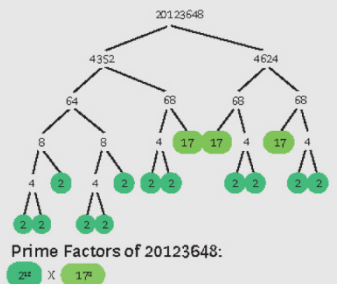
- Fluid dynamics simulations for automotive and aeronautical design and medical devices (e.g., blood flow analysis)
- Molecular simulation for specialty materials design and drug discovery



### Linear algebra

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

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



### Factorization

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






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



# 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)	<b>\$2 billion–\$5 billion</b>	<b>\$25 billion–\$50 billion</b>	<b>\$450 billion–\$850 billion</b>

Source: BCG analysis.

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

# Quantum computing: predicting the future!

2022

