



# understanding quantum computing

olivier e兹拉特ty

〈author | QEI founder〉

April 6<sup>th</sup> - 7<sup>th</sup>, 2023

[olivier@oezratty.net](mailto:olivier@oezratty.net) [www.oezratty.net](http://www.oezratty.net) @olivez

# before



1985-1989

software engineer  
software R&D lead



CentraleSupélec

1982-1985

Computer Science Msc



1990-2005

from product manager to  
CMO and Developer  
Division Director

digital TV  
startups

artificial intelligence  
genomics, astronomy  
IoT, semi-conductors

consultant & author

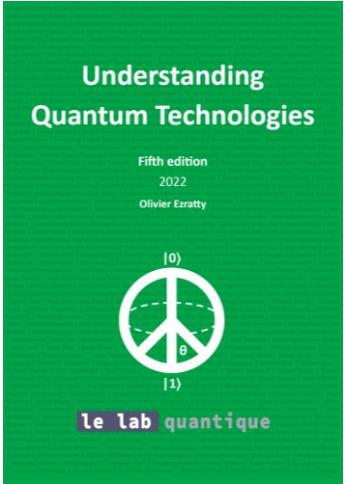
2005-\*



# quantum technologies

since 2018

author



Cornell University  
arXiv physics > arXiv:2202.01925

Physics > Physics and Society  
[Submitted on 23 Jan 2022 (v1); last revised 10 Feb 2022 (this version, v2)]  
**Mitigating the quantum hype**  
Olivier Ezratty

We are in the midst of quantum hype with some excessive claims of quantum computers, quantum sensors, and quantum communication. This hype is exaggerated, and a funding frenzy for very low technology readiness level startups. Governments are contributing to the hype with their large quantum research programs. Some quantum technologies are useful, others are not but per se since they create emulation, drive innovations and also contribute to attracting new talents. It is time as scientists and vendors deliver progress and innovation in quantum technologies. We propose a mitigation strategy with exaggerated overpromises and underdelivers that last long. It could cut short research programs and mitigate the hype. We propose to mitigate the hype looking at the shape and form of technology and science hype and driving some lessons from past hype. We investigate the current quantum hype and its specifics. We look at the quantum computer hype, the quantum sensor hype, the real scalable quantum computers, the scientific and vendor fields are relatively same and related compared to other technology hypes. The vendors hype is more prominent than the scientific hype. The quantum communication hype is also quantum technologies comprise other fields like quantum telecommunications and quantum sensors. We propose to mitigate the quantum hype and the quantum hype. We then make some proposals to mitigate the potential negative effects of the current quantum hype including recommendations on scientific communication to mitigate the quantum hype, vendor behavior improvements, benchmarking methodologies, public education and putting in place a responsible research and innovation approach.

Comments: 20 pages and 1 figure  
Subjects: Physics [q-bio.QM]; Physics [q-bio.QM]; History and Philosophy of Physics [physics.hist-ph]; Cite as: arXiv:2202.01925 [physics.q-bio]; arXiv:2202.01925 [q-bio.QM]; arXiv:2202.01925 [physics.hist-ph] for this version)



DECODE QUANTUM  
Decode Media  
Séries  
★★★★★ 4.9 • 6 notes  
Écouter sur Apple Podcasts ▶

4 JANV. 2023  
[DECODE Quantum] A la rencontre d'Anthony Leverrier, chercheur...  
Nous vous retrouvez dans le 54e épisode des entretiens Decode Quantum où, Olivier Ezratty et Frédéric Boutron accueillent Anthony Leverrier d'Irrla, après avoir reçu Harold Ollivier qui coordonne la recherche dans le quantique chez Irrla. Anthony Leverrier est chercheur Irrla depuis 2012, dans l'équipe COSMIQ...  
LIRE ▶ 1h 6 min



training and education



expertize



research



techno screening



evangelizing



# agenda

## day 1

9h00	<b>quantum physics 101</b>
10h30	<b>break</b>
10h45	<b>state of the art, perspectives and limits of classical computing</b>
12h00	<b>lunch time</b>
13h30	<b>quantum computing architecture and engineering</b>
15h30	<b>break</b>
15h45	<b>qubits types and industry players</b>
17h30	<b>end</b>

## day 2

9h00	<b>qubits types and industry players (contd)</b>
10h30	<b>break</b>
10h45	<b>quantum algorithms</b>
12h00	<b>lunch time</b>
13h30	<b>quantum development tools</b> <b>quantum computing use cases</b>
15h30	<b>break</b>
15h45	<b>quantum ecosystems</b> <b>enterprise readiness</b>
17h30	<b>end</b>

# scope of covered scientific domains



## physics

electromagnetism  
quantum physics  
thermodynamics  
fluids mechanics  
photonics



## engineering

materials design  
electronics engineering  
cryogenics



## human sciences

economics of innovation  
R&D policy making  
startups ecosystem  
philosophy  
sociology  
technology ethics



## computer science

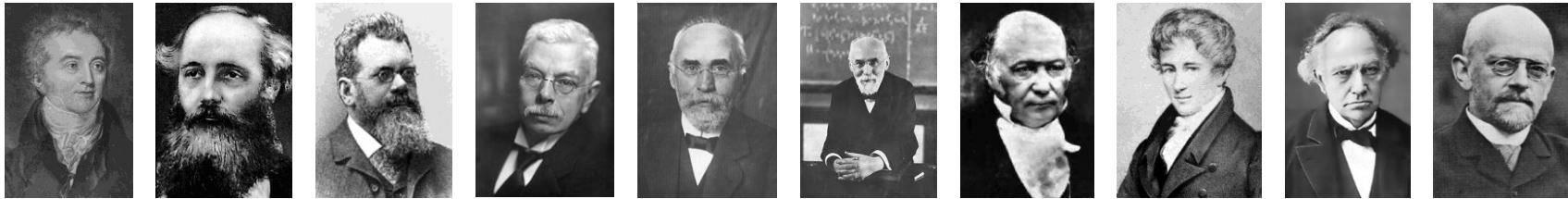
information theory  
algorithms design  
programming  
classical computing  
telecommunications



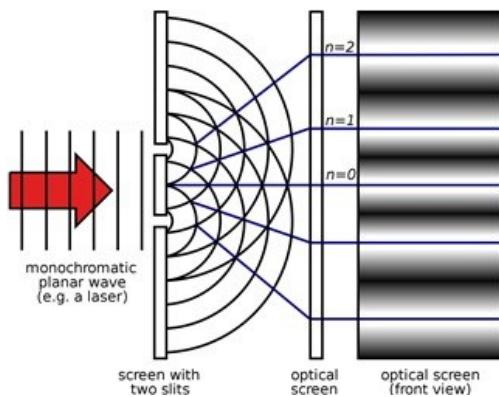
## mathematics

linear algebra  
complexity theories

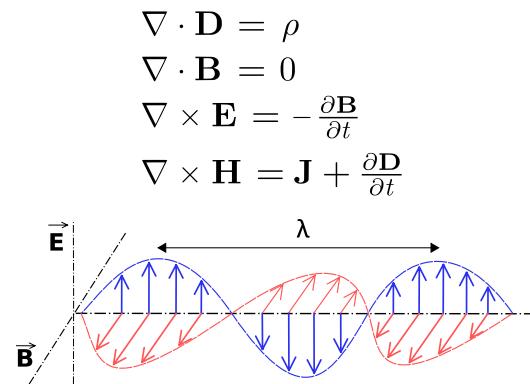
# precursors



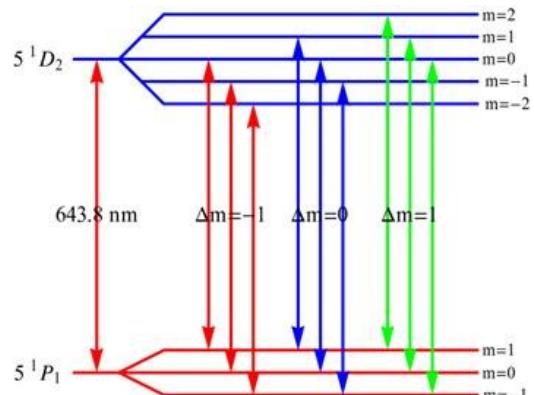
laid the groundwork of quantum physics with their experiments, early theories and mathematical tools



Young's slit experiment - 1806



Maxwell's electro-magnetic waves - 1865



Zeeman effect - 1896



Solvay conference  
Brussels  
october 1927  
6+11/29



## FANTASIES QUANTIQUES

Dans les coulisses des grandes découvertes du xx<sup>e</sup> siècle

Henri Poincaré, Max Planck,  
Marie Curie, Ernest Solvay,  
Albert Einstein...  
Préface Étienne Klein

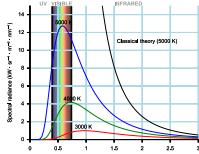
A. PICCARD	E. HENRIOT	ED. HERZEN	TH. DE DONDER	E. SCHOEDINGER	R. H. FOWLER
P. EHRENFEST				E. VERSCHAFFELT	W. HEISENBERG
P. DEBYE	M. KNUDSEN	W. L. BRAGG	H. A. KRAMERS	P. A. M. DIRAC	A. H. COMPTON
I. LANGMEIR	M. PLANCK	MADAME CURIE	H. A. LORENTZ	A. EINSTEIN	L. V. DE BROGLIE
				P. LANGEVIN	CH. E. GUYE
				C. T. R. WILSON	M. BORN
				O. W. RICHARDSON	N. BOHR

# quantum physics basics

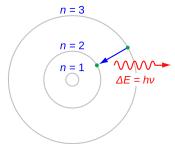


Solvay congress May 2022

# quantum physics beginnings



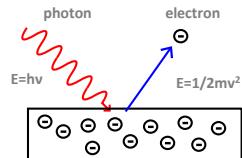
1900 1918  
**Max Planck**  
black body radiation  
energy quanta  
Planck constant



1913 1922  
**Niels Bohr**  
hydrogen atom  
model

1900 1905 1910 1915 1920 1925 1930 1935 1940

1905 1921  
**Albert Einstein**  
photoelectric effect



1922 1944  
**Stern-Gerlach**  
experiment  
atoms angular  
momentum

1924 1945  
**Wolfgang Pauli**  
exclusion principle

1924 1929  
**Louis de Broglie**  
wave-particule duality

1926 1933  
**Erwin Schrödinger**  
wave function  
 $i\hbar \frac{\partial \Psi(x,t)}{\partial t} = H\Psi(x,t)$

1927 1932  
**Werner Heisenberg**  
indetermination

1926 1954  
**Max Born**  
quantum probabilities

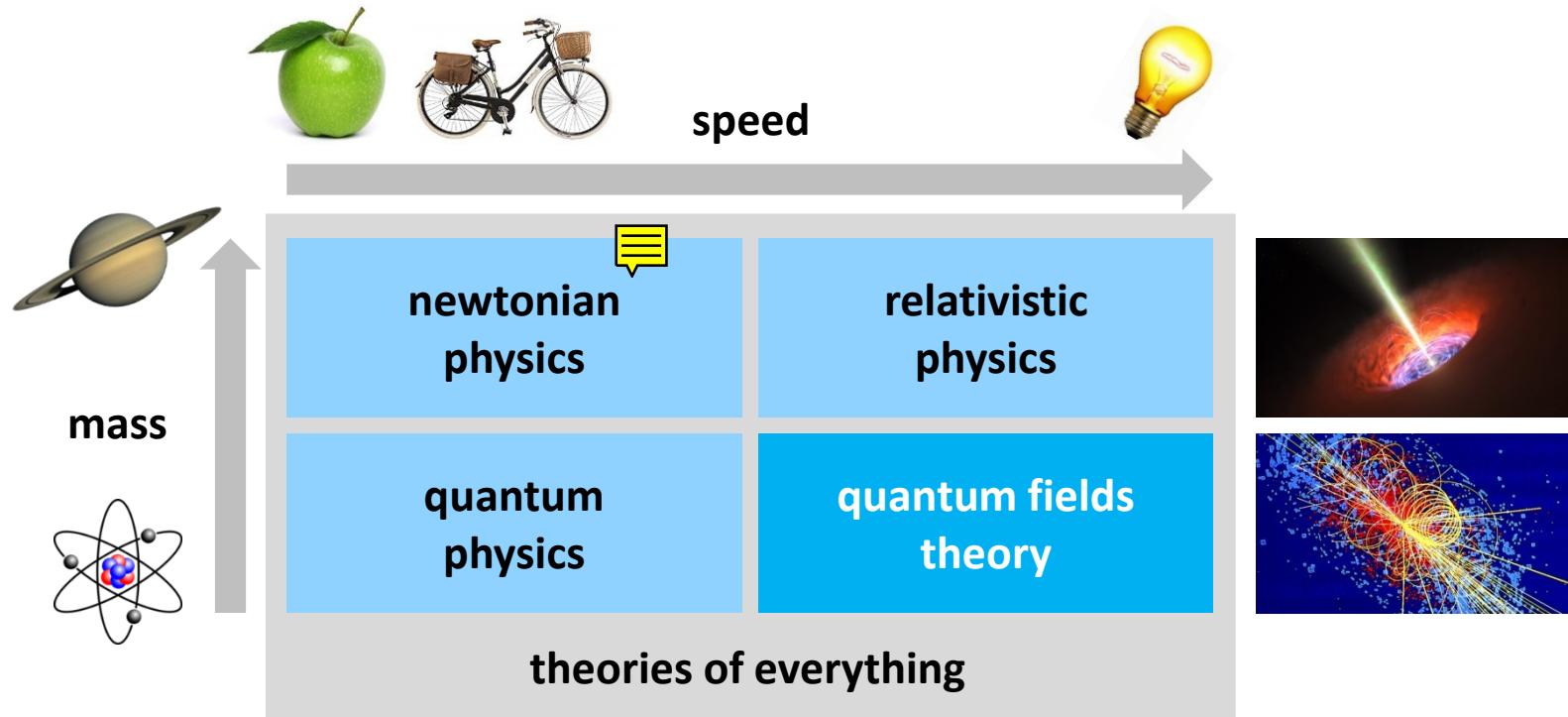
1925  
**Uhlenbeck-Goudsmit**  
electron spin

1935  
**Einstein,**  
**Podolski, Rosen**  
EPR paradox

1935  
**Erwin Schrödinger**  
entanglement, cat

1937  
**Ettore**  
**Majorana**  
fermion

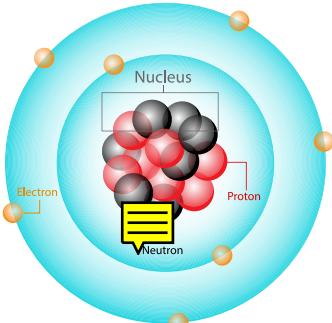
# physics domains classification



# from macro to nano physics

quantum physics deals with  
atomic and sub-atomic  
particles, and photons

at this scale, matter behaves  
differently than macro objects  
in classical physics



atoms and electrons

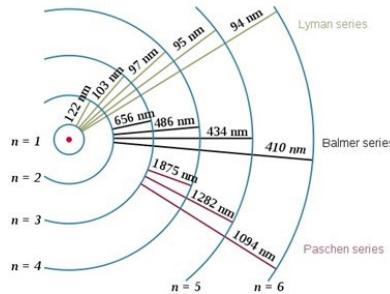
in quantum technologies, we are focused on:

- **photons**: as qubits, entanglement resources and as mediator of atoms/electrons interactions
- **electrons**: define atom energy levels, spin as qubit
- **atoms and their nucleus spin**: energy levels, spin for qubits

## elementary particles standard model

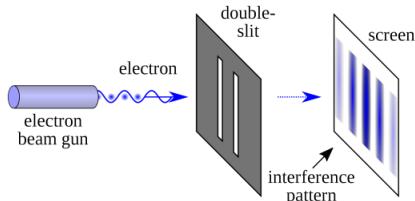
three generations of matter (fermions)			interactions / force carriers (bosons)	
QUARKS				SCALAR BOSONS
I	mass charge spin	$\approx 2.2 \text{ MeV}/c^2$ $\frac{2}{3}$ $\frac{1}{2}$ u up	II	$\approx 1.28 \text{ GeV}/c^2$ $\frac{2}{3}$ $\frac{1}{2}$ c charm
			III	$\approx 173.1 \text{ GeV}/c^2$ $\frac{2}{3}$ $\frac{1}{2}$ t top
				g gluon
				H higgs
d	$\approx 4.7 \text{ MeV}/c^2$ $-\frac{1}{3}$ $\frac{1}{2}$ down	S	$\approx 96 \text{ MeV}/c^2$ $-\frac{1}{3}$ $\frac{1}{2}$ strange	$\gamma$ photon
			b	$Z$ Z boson
e	$\approx 0.511 \text{ MeV}/c^2$ $-1$ $\frac{1}{2}$ electron	$\mu$	$\approx 105.66 \text{ MeV}/c^2$ $-1$ $\frac{1}{2}$ muon	$W$ W boson
			$\tau$	
$\nu_e$	$<1.0 \text{ eV}/c^2$ 0 $\frac{1}{2}$ electron neutrino	$\nu_\mu$	$<0.17 \text{ MeV}/c^2$ 0 $\frac{1}{2}$ muon neutrino	
			$\nu_\tau$	

# what is it to be « quantum »?



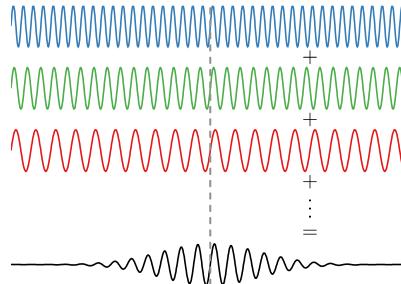
## quantization

discretization of nano-objects properties (energy, frequency, position, angular momentum, spin...)



## wave-particle duality

electrons, photons, atoms



## superposition

linked to wave-particle duality and linearity of Schrödinger's equation

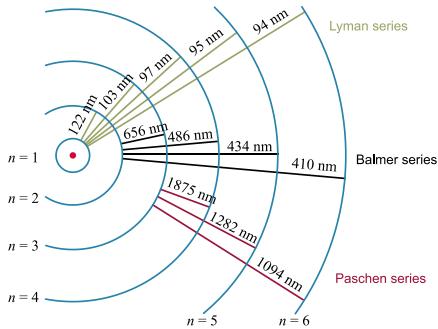


## entanglement

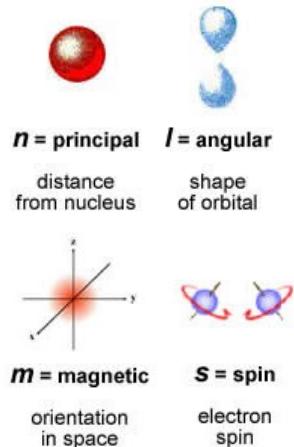
state correlation of distant quantum objects, but random and after measurement



# quantization examples

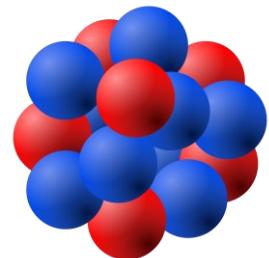


**atoms and ions**  
discrete transitions energy levels between electron shells observed in spectrography

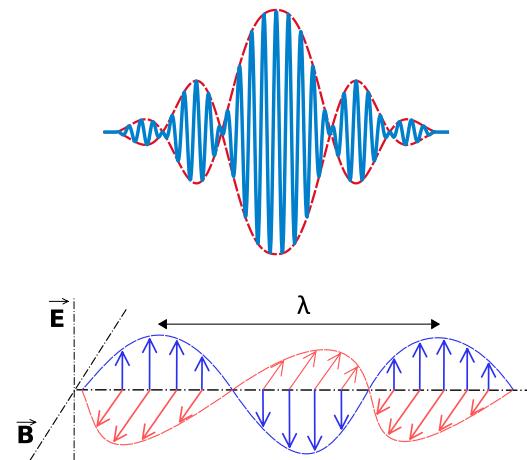


**electrons**  
principal number  
orbital quantum number  
magnetic quantum number  
spin projection (up, down)

**protons**  
**neutrons**



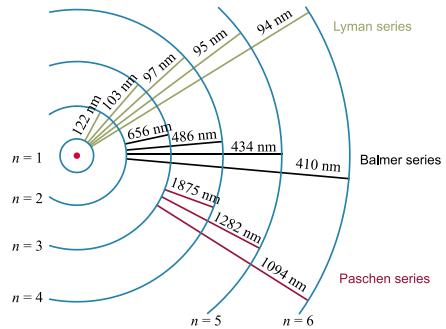
**nucleon**  
shell number  
orbital angular momentum  
magnetic quantum number  
spin



**photons**  
mass and electric charge = 0  
orbital angular momentum  
wavelength  
spin angular momentum

=> used to created qubits with distinct states and at the particle scale (atoms, electrons, photons).

# electron quantum numbers

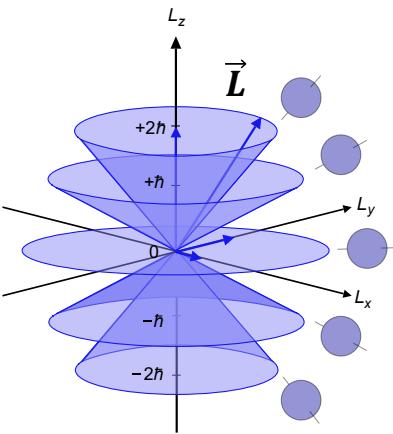


$n$   
 $1 \leq n \leq \infty$   
**principal quantum number**  
shell number  
labelled K, L, M, N

Bohr, 1913

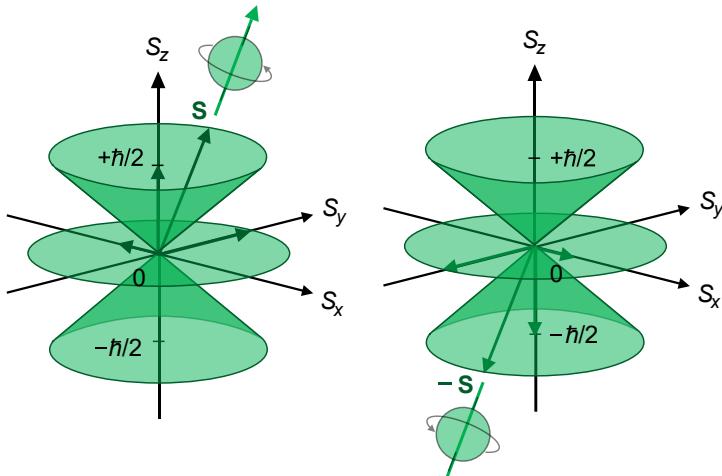
$\ell$   
 $0 \leq \ell < n$ , labelled S, P, D, F  
**orbital quantum number**  
subshell number  
 $\vec{L}$  is the orbital angular momentum vector  
 $|\vec{L}| = \hbar\sqrt{\ell(\ell+1)}$

Zeeman effect 1896,  
Sommerfeld 1916,  
Schrodinger, 1926.



$m_\ell$   
 $-\ell \leq m_\ell \leq \ell$   
**magnetic quantum number**  
subshell orientation in space,  
angle of  $\vec{L}$  measured as projection  
on z in  $\hbar$  integer quantity  
 $L_z = m_\ell \hbar$

Zeeman effect 1896,  
Starck effect 1913,  
Lande formalism 1925



$m_s$   
 $m_s = \pm 1/2$   
**spin projection**  
up or down, with a single amplitude,  
projection on z axis.

Stern & Gerlach experiment 1922,  
Goldshmidt & Ulen Back 1925,  
Dirac 1927

# Grotian diagram

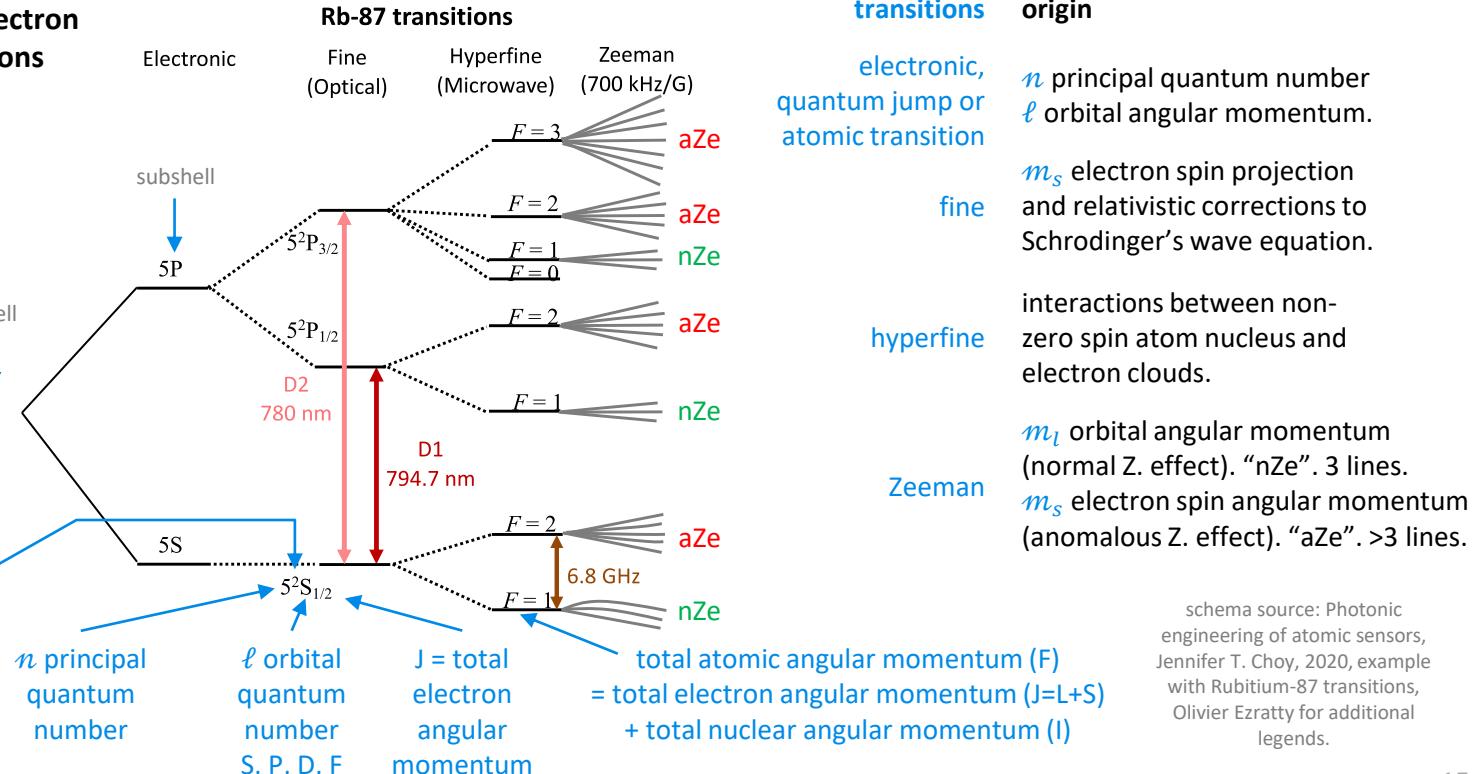
atom energy transitions based on various electron quantum numbers

**Grotian diagram of electron energy level transitions**

$n, \ell, m_s, m_l$  are the 4 quantum numbers of atomic electrons

$n$  = principal quantum number (electron layer or shell)

$2S + 1$ , S being the total subshell electron spin

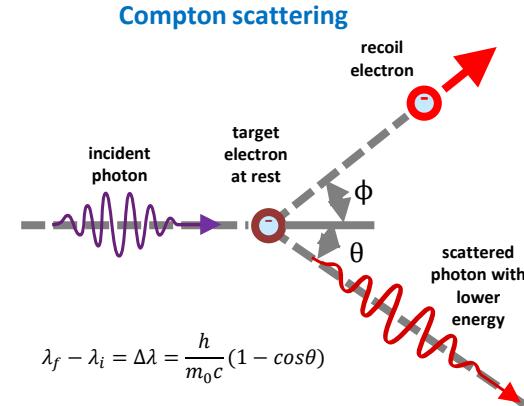
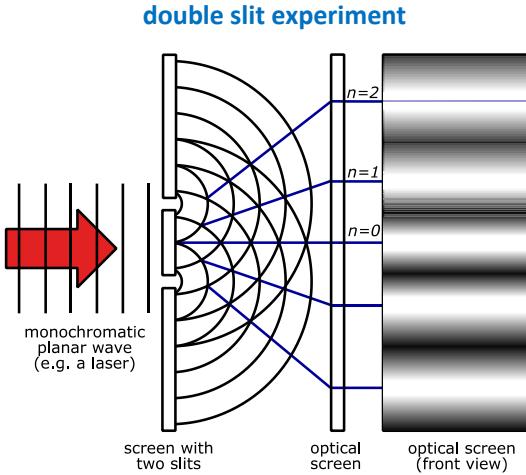
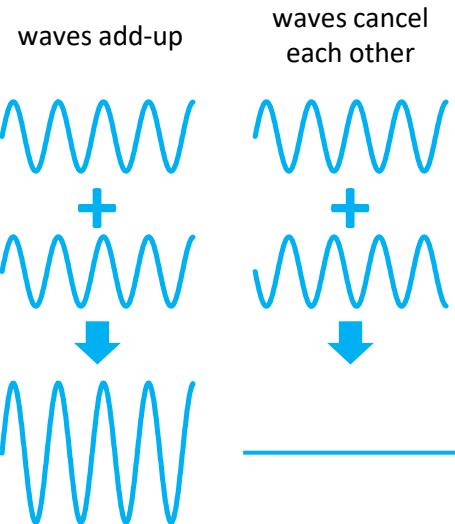


schema source: Photonic engineering of atomic sensors, Jennifer T. Choy, 2020, example with Rubitium-87 transitions, Olivier Ezratty for additional legends.

# photons wave-particle duality



an elementary particle can behave both as particle (with momentum) or as a wave (generating interferences)  
applicable to electrons, photons, neutrons, protons, atoms and even large molecules ( $C_{60}$ )



**additive and subtractive interferences principle**

**interferences observed with photons**  
experiment: Thomas Young, 1801

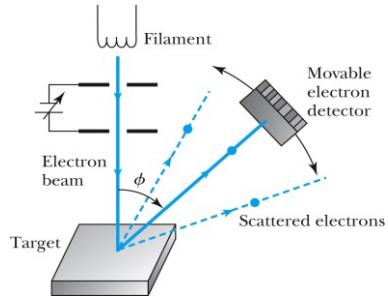
**photons acting as particles**  
experiment: Compton scattering effect, 1923

# electrons wave-particle duality

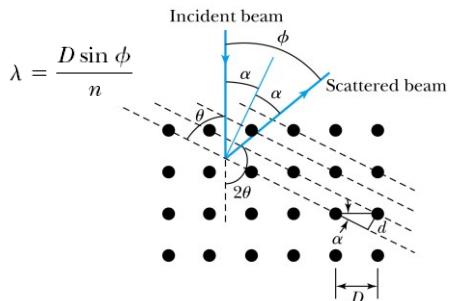
wave-particle duality also applicable to electrons, photons, neutrons, protons, atoms and large molecules ( $C_{60}$ )

## **De Broglie matter wave-particle equation, 1924**

particle energy  $E = h\nu$  wave frequency  
particle momentum  $p = \frac{h}{\lambda}$  Planck constant  
wave length



**George Paget Thomson, Clinton Davisson**  
and **Lester Germer** experiment, 1927 (electrons crystal diffraction)



The diagram illustrates an electron interference experiment. An 'electrons beam gun' on the left emits a beam of electrons represented by blue wavy lines. These electrons pass through a 'double slit' on a grey rectangular plate. The beam then hits a 'screen' on the right, which displays a series of vertical interference fringes. An arrow points from the text 'interference pattern' to one of these fringes.

**Clauss Jönsson**, 1961 (double-slit experiment with electrons)  
and **Pier Giorgio Merli** (same, with a single electron)

=> used in quantum computing to create interferences between qubits through multiple qubits gates and entanglement.

=> used in matter-wave interference in neutral atom based absolute gravimeters.

# Schrödinger's equation

partial derivative equation with solutions =  $\psi(x, t)$   
 function and variables = initial conditions  $\psi(x, 0)$   
 and energy potential constraints  $V(x)$ .

$i$  = imaginary number, its square equals -1

first derivative of the wave function vs time



second derivative of the wave function vs position (laplacian)

potential energy function depends on the particle, its physical constraints and its position

$$-\frac{\hbar^2}{2m} \frac{\partial^2 \Psi(x, t)}{\partial x^2}$$

$$+ V(x) \Psi(x, t)$$

$\hbar$  = Dirac constant

$$\hbar = \frac{h}{2\pi}$$

$h$  = Planck constant  
 $m$  = particle mass

total energy of particle



kinetic energy

(« impulsion » observable)

potential energy

(« position » observable)  
 equals zero for a free particle

massive non relativistic particle wave function defining its evolution in time and space, returning a complex number. this is the equation unknown variable

$$\hat{H} = -\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2} + V(x)$$

« hamiltonian » : function applicable to the particle wave function  $\psi(x, t)$  to evaluate its total energy, is a unitary operator.

# Schrödinger's equation constraints

$$z = a + ib \quad |z| = \sqrt{a^2 + b^2}$$

complex number module

size of its vector in two dimensional space

$$|\psi(x, t)|^2$$

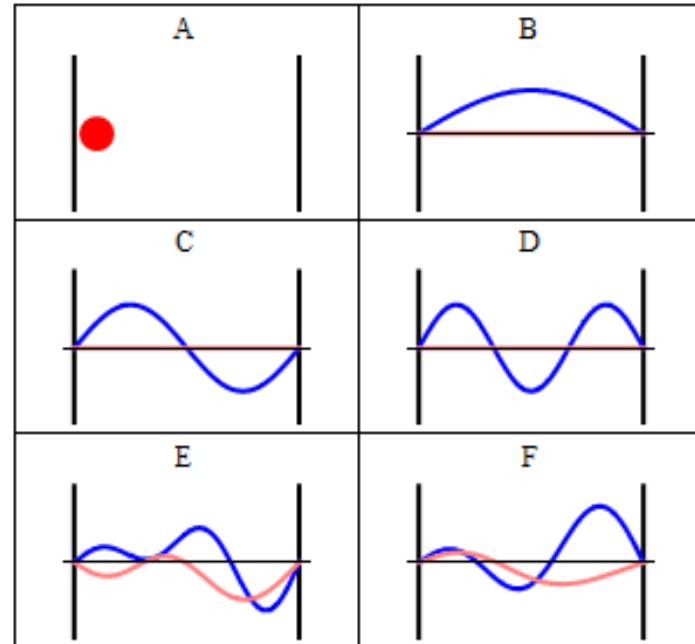
wave function module square

probability to find the particle at position x at time t.

If it's time independant, the system is in a stationary state.

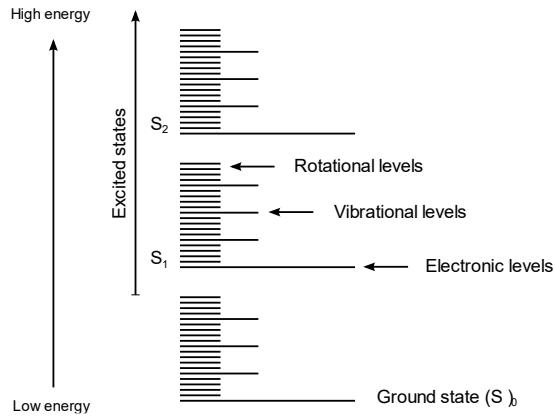
$$\int_{-\infty}^{+\infty} |\psi(x, t)|^2 dx = 1$$

integral of the probability to find the particle  
in any position equals 1

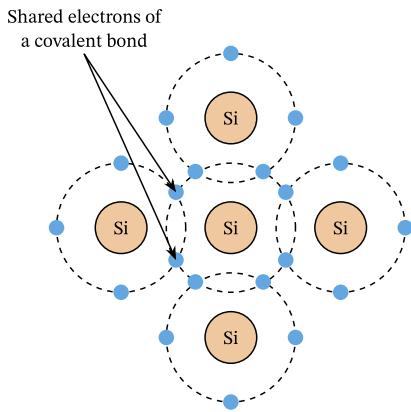


example of  $V(x)$  potential energy constraints  
in cavities

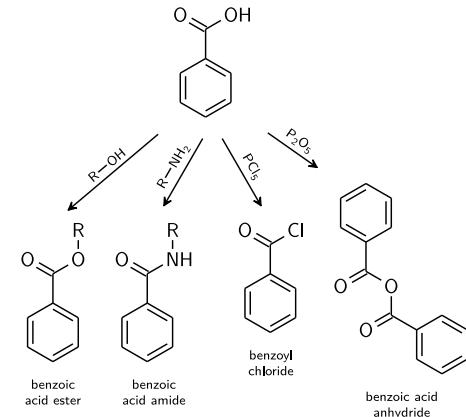
# some Schrödinger's equation use cases



**predict atoms and molecules  
energy levels**



**studying the behavior  
of electrons in solids**

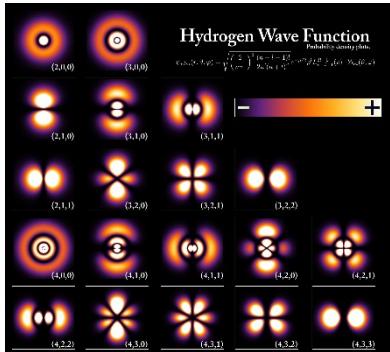


**modeling chemical  
reactions**

**designing new materials**

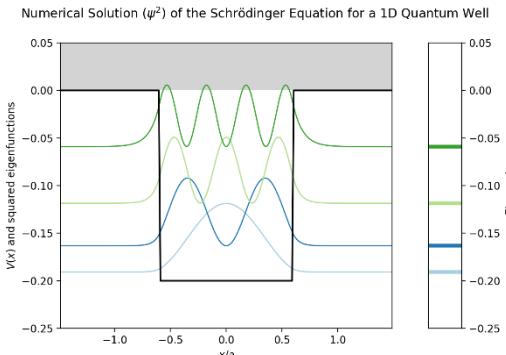
**understanding quantum systems properties  
(entanglement, superposition)**

# solving Schrödinger's equation

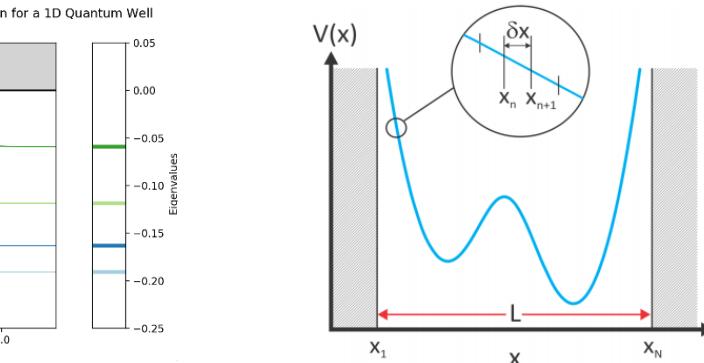


**exact solution**  
exists only for the  
hydrogen atom

$\Psi(x, t) = \psi(x)f(t)$   
**variables separation**  
time and space  
dependent



**Fourier decomposition**  
decompose quantum object in  
elementary waves for which a  
solution already exists

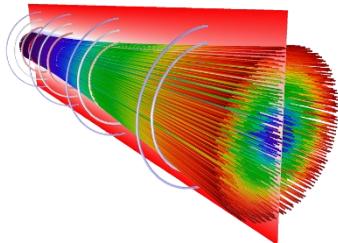


**numerical methods**  
finite element methods,  
DFT, ...

**variational methods**  
deep learning methods  
**quantum computing**

# Schrödinger's equation scope

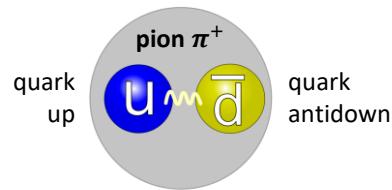
applicable to non-relativistic massive particles : atoms, electrons and molecules



$$i\hbar\gamma^\mu \partial_\mu \psi(x) - mc\psi(x) = 0$$

**Dirac equation**

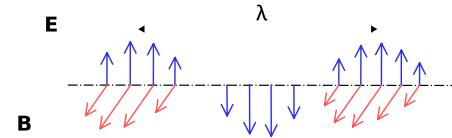
relativistic massive particles  
(fermions), e.g. electrons in inner  
shells of large atoms, relativistic  
electron beam



$$\left( \frac{1}{c^2} \frac{\partial^2}{\partial t^2} - \nabla^2 + \frac{m^2 c^2}{\hbar^2} \right) \psi(t, \mathbf{x}) = 0$$

**Klein-Gordon equations**

relativistic spinless  
particles (bosons), e.g.  
pions and Higgs boson



$$\nabla \cdot \mathbf{D} = \rho$$
$$\nabla \cdot \mathbf{B} = 0$$

$$\nabla \times \mathbf{E} = - \frac{\partial \mathbf{B}}{\partial t}$$

$$\nabla \times \mathbf{H} = \mathbf{J} + \frac{\partial \mathbf{D}}{\partial t}$$

$$E = h\nu$$

**Maxwell + Planck/Einstein  
equations + second quantization**  
(Fock, Glauber, Wigner)  
photons

# entanglement

**consequence of state superposition with multiple quantum object systems**

**some linear combinations of quantum states create entangled or inseparable states**

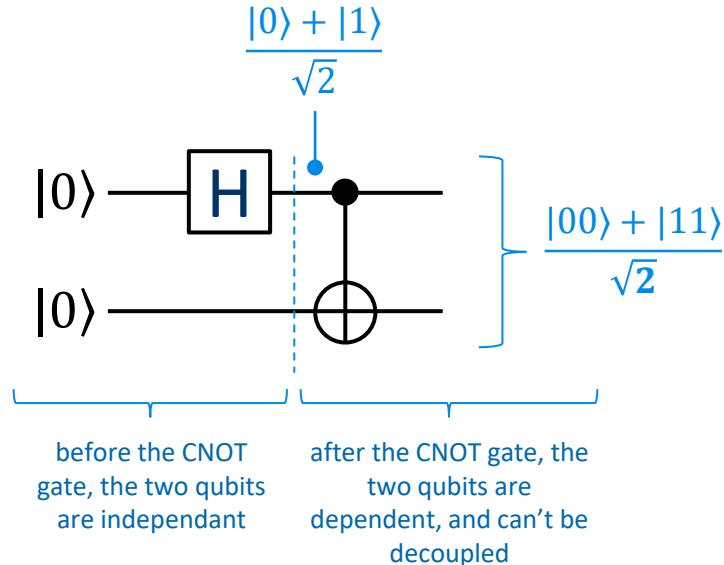
can't be mathematically described by the independent properties of their parties, which is easy to show in mathematical terms using Hilbert space representation of quantum states

formalism: Erwin Schrödinger, 1926 then 1935

argument: EPR paradox, Einstein, Podolsky, Rosen, 1935

theory: John Stewart Bell inequalities, 1964

verification: Alain Aspect et al, 1982



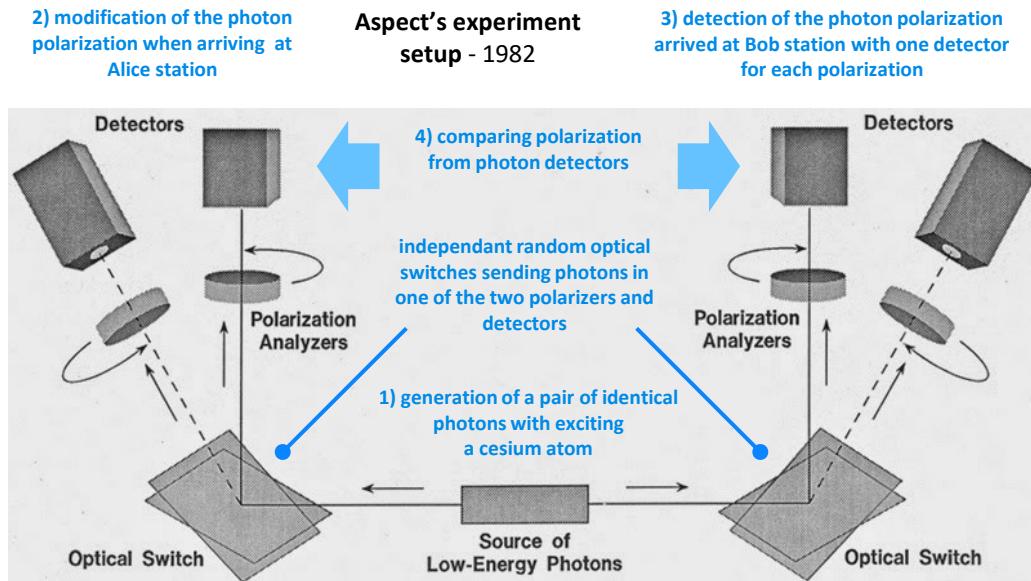
# entanglement and measurement

**entanglement or « spooky action at a distance » happens at measurement time**

when the quantum state of one of the quanta is measured, provoking a state collapse to a basis state, it instantly modifies the quantum state of the other quantum object, with the effect of a similar measurement, with correlated results.

it's like if the quantum objects had an internal "flag" (hidden variable) telling them what to do.

since the measured quantum property is random, entanglement is not usable to transmit some information faster than light, still it is a very powerful resource as we'll see later.



this « non locality » notion was verified with pairs of photons by **Alain Aspect et al** in 1982, showing there were no "hidden variables" compatible with quantum physics postulates, since the measurements violated Bell's inequalities, a statistical model used to detect the existence of hidden variables. The experiment randomly selected the photons measurement polarization with fast optical switches after they were generated.

# entanglement consequences

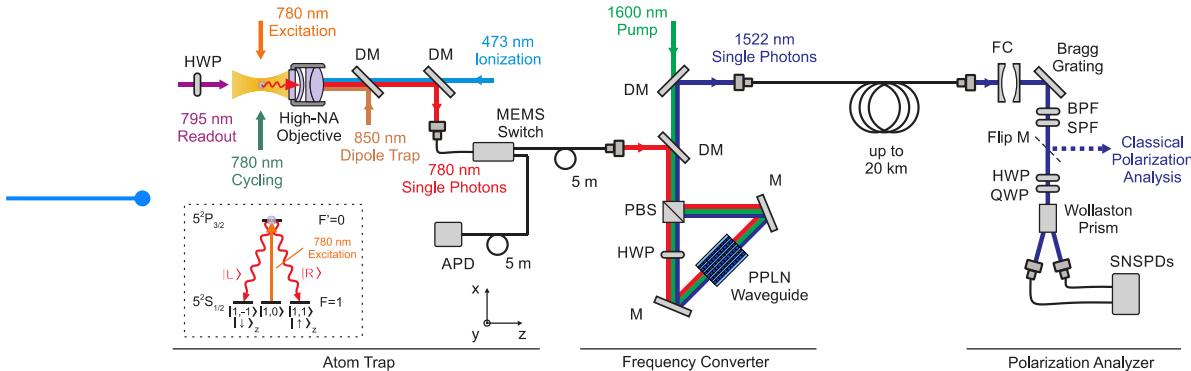
entanglement can be created between several breeds of quantum objects: photons, electrons, atoms, and even in hybrid ways

conditionnally connects qubits in quantum computing.

also used in quantum cryptography and telecommunications.

can be created with more than two quantum objects, that's the basis of quantum computing.

example of the “GHZ state” created by Anton Zeilinger *et al* in 1989, the generalization of which being “cluster states” of entangled photons.



photons entanglement 2020 experiment with converting their wave length

$$|\text{GHZ}\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}.$$

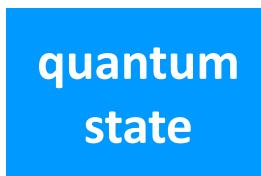
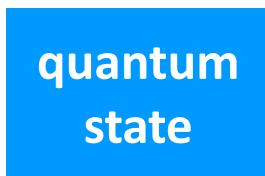
a GHZ state created with 3 entangled qubits

# no cloning

quantum object #1



quantum object #2



a quantum state can't be replicated independently and exactly onto another quantum object

only possible copy is through entangled states creation

discovery : James Park in 1970

then William Wootters and Wojciech Zurek in 1982

**No Cloning** Assume we have a unitary operator  $U_{cl}$  and two quantum states  $|\phi\rangle$  and  $|\psi\rangle$  which  $U_{cl}$  copies, i.e.,

$$\begin{aligned} |\phi\rangle \otimes |0\rangle &\xrightarrow{U_{cl}} |\phi\rangle \otimes |\phi\rangle \\ |\psi\rangle \otimes |0\rangle &\xrightarrow{U_{cl}} |\psi\rangle \otimes |\psi\rangle . \end{aligned}$$

Then  $\langle\phi|\psi\rangle$  is 0 or 1.

**Proof 1:**  $\langle\phi|\psi\rangle = (\langle\phi| \otimes \langle 0|)(|\psi\rangle \otimes |0\rangle) = (\langle\phi| \otimes \langle\phi|)(|\psi\rangle \otimes |\psi\rangle) = \langle\phi|\psi\rangle^2$ . In the second equality we used the fact that  $U$ , being unitary, preserves inner products.  $\square$

**Proof 2:** Suppose there exists a unitary operator  $U_{cl}$  that can indeed clone an unknown quantum state  $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ . Then

$$\begin{aligned} |\phi\rangle|0\rangle &\xrightarrow{U_{cl}} |\phi\rangle|\phi\rangle = (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha^2|00\rangle + \beta\alpha|10\rangle + \alpha\beta|01\rangle + \beta^2|11\rangle \end{aligned}$$

But now if we use  $U_{cl}$  to clone the expansion of  $|\phi\rangle$ , we arrive at a different state:

$$(\alpha|0\rangle + \beta|1\rangle)|0\rangle \xrightarrow{U_{cl}} \alpha|00\rangle + \beta|11\rangle .$$

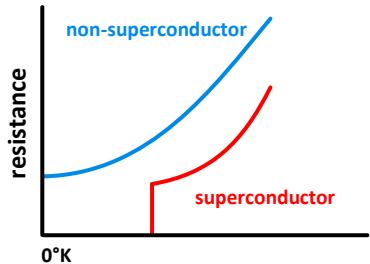
Here there are no cross terms. Thus we have a contradiction and therefore there cannot exist such a unitary operator  $U_{cl}$ .  $\square$

**easy to demonstrate mathematically  
linked to the linearity of quantum physics**

=> secures telecommunications with quantum key distribution.

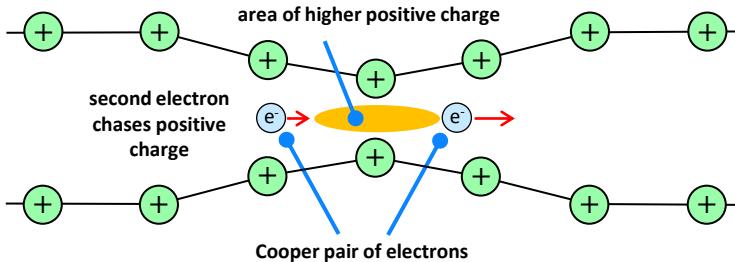
=> creates significant constraints in quantum computing (memory, cache, error correction, ...).

# superconductivity



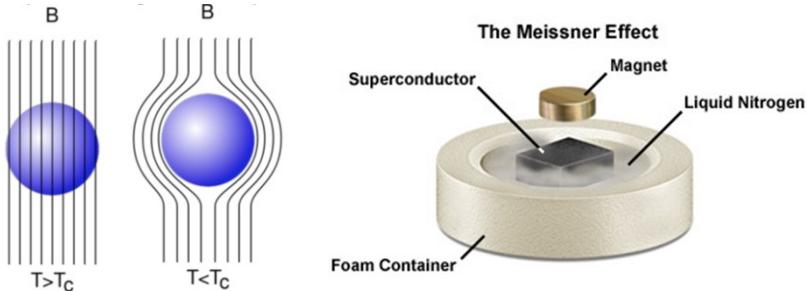
some materials have zero resistivity  
below a threshold temperature ( $T_c$ )

discovery: H. Kamerlingh Onnes et al, 1911



explained by Cooper pairs of electrons with opposed spins  
flowing in crystal lattice, creating bosons

theory: Bardeen, Cooper, Schrieffer (BCS) theory, 1957



expulsion of a magnetic field from a  
superconductor during its transition  
to the superconducting state when it is cooled  
below the critical temperature

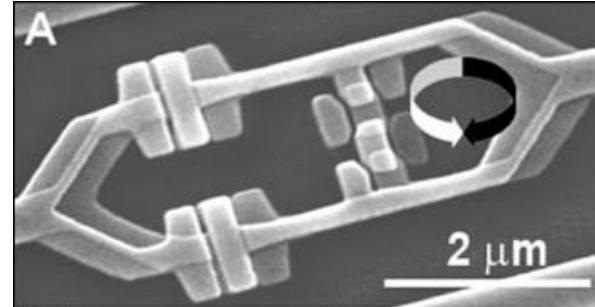
discovery: Walther Meissner  
and Robert Ochsenfeld, 1933

# some superconductivity applications



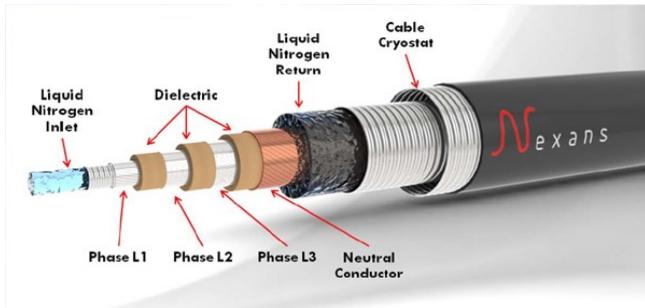
**superconducting magnets**

discovery: Georges Yntema, 1955



**Josephson junction**

discovery: Brian Josephson, 1962

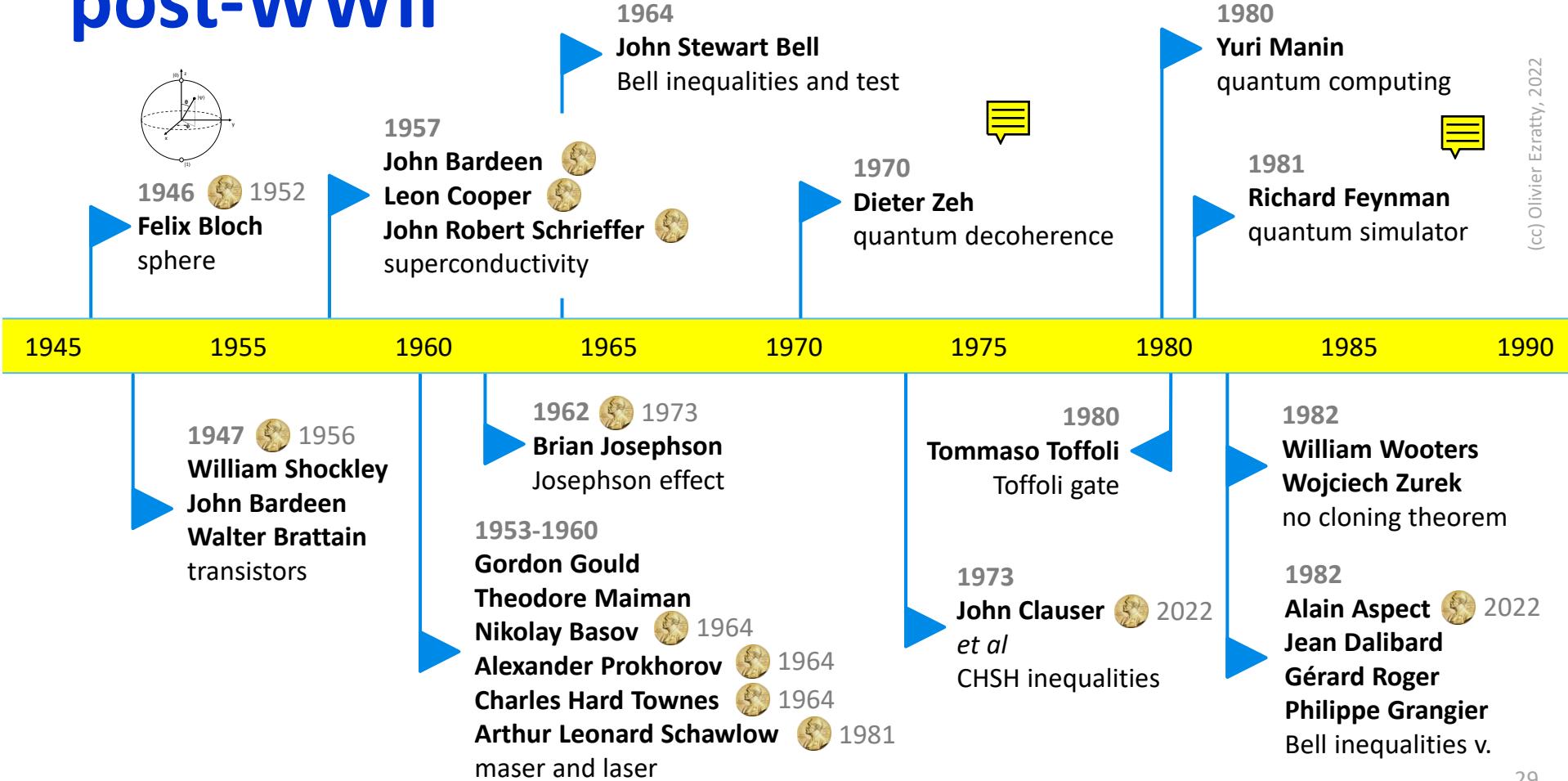


**superconducting power lines**

=> superconducting qubits.

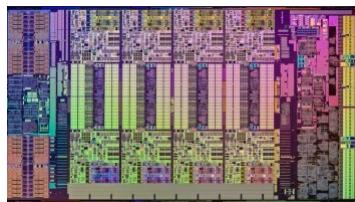
=> quantum sensing SQUIDs (Superconducting Quantum Interference Device) with magnetometer, voltmeter and gradiometer.

# post-WWII

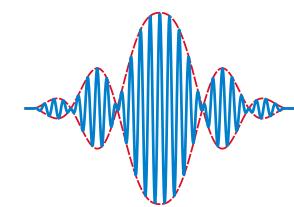
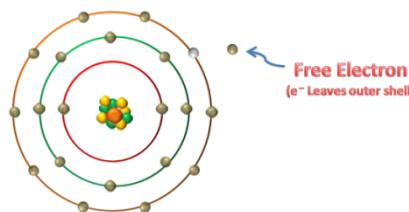


# 1<sup>st</sup> and 2<sup>nd</sup> quantum revolutions

manipulating  
**groups of quantum particles**  
photons, electrons and atoms interactions



manipulating  
**superposition and entanglement**  
and/or individual particles



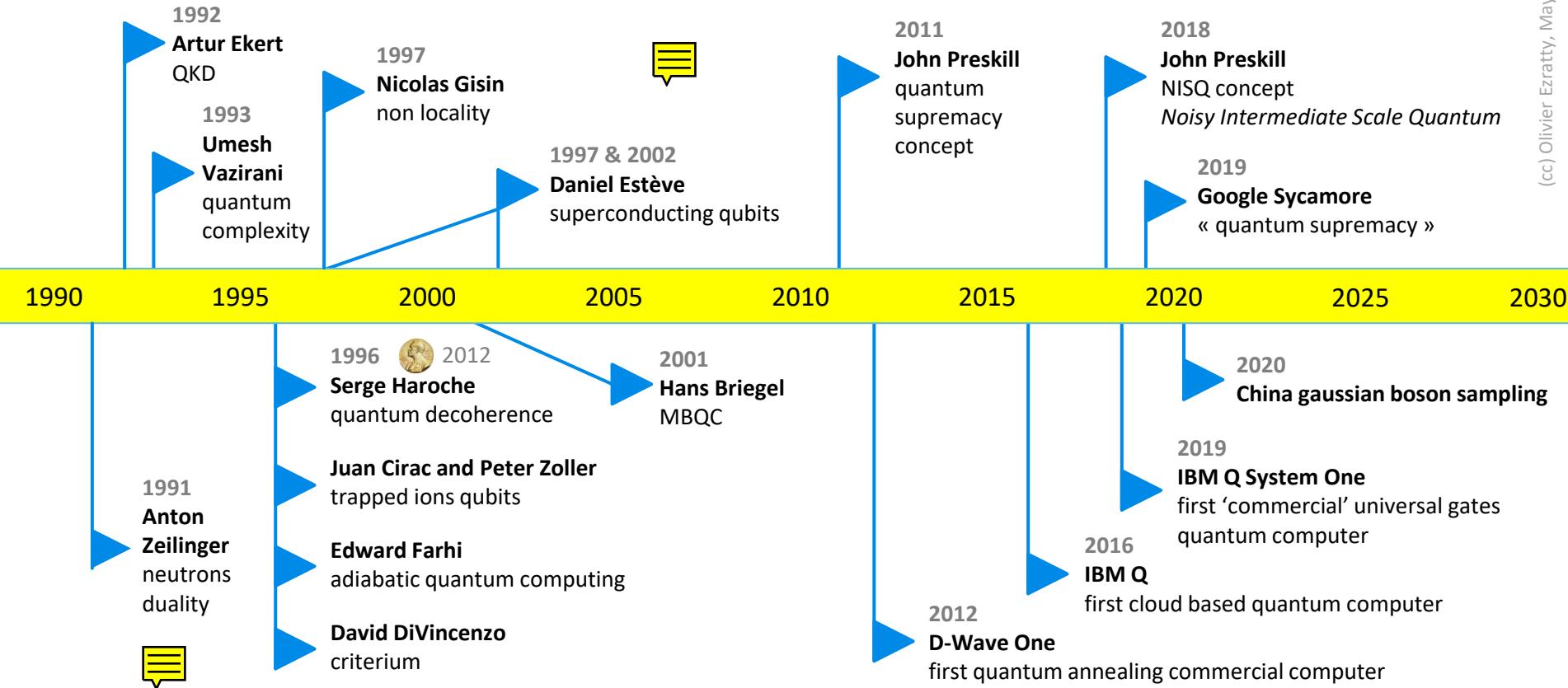
**transistors, lasers, GPS**  
**photovoltaic cells, atom clocks**  
**medical imaging, digital photography and video**  
**LEDs, LCD TV quantum dots**

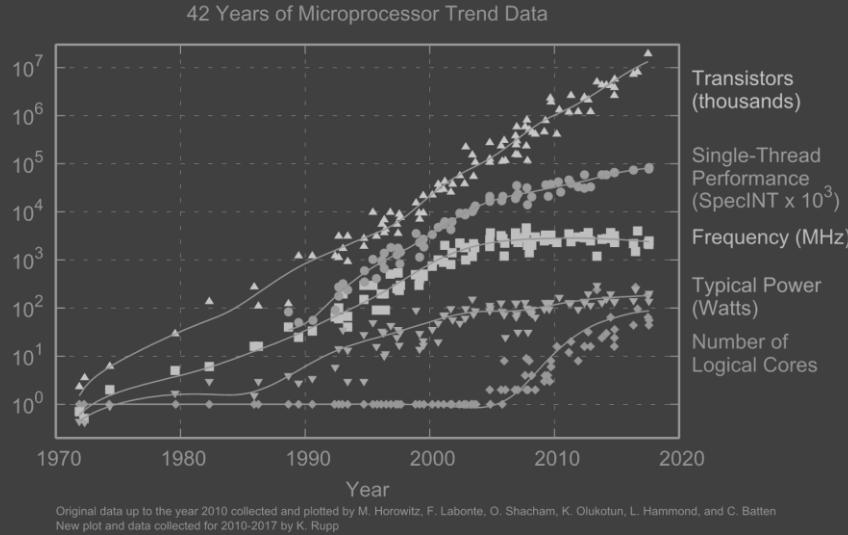
1947-\*

**quantum computing**  
**quantum telecommunications**  
**quantum cryptography**  
**quantum sensing**

1982-\*

# second quantum revolution





classical computing state of the art  
and limitations

# Moore's law: dead or alive?

The experts look ahead

## Cramming more components onto integrated circuits

With unit cost falling as the number of components per circuit rises, by 1975 economics may dictate squeezing as many as 65,000 components on a single silicon chip

By Gordon E. Moore

Director, Research and Development Laboratories, Fairchild Semiconductor division of Fairchild Camera and Instrument Corp.

The future of integrated electronics is the future of electronics itself. The advantages of integration will bring about a proliferation of electronics, pushing this science into many new areas.

Integrated circuits will lead to such wonders as home computers—or at least terminals connected to a central computer—in telephones, control systems for automobiles, and personal portable communications equipment. The electronic wristwatch needs only a display to be feasible today.

But the biggest potential lies in the production of large systems. In telephone communications, integrated circuits in digital filters can separate channels on multiplex equipment. Integrated circuits will also switch telephone circuits and perform data processing.

Computers will be more powerful, and will be organized in completely different ways. For example, memories built of integrated electronics may be distributed throughout the

The author  
Dr. Gordon E. Moore is one of the few true electronic engineers, schooled in the physical sciences rather than in electronics. He received a B.S. degree in chemistry from the University of California and a Ph.D. degree in physical chemistry from the California Institute of Technology. He was one of the founders of Fairchild Semiconductor and has been director of the research and development laboratories since 1959.

Electronics, Volume 38, Number 8, April 19, 1965

empirical observation from 1965

the complexity of integrated circuits doubles every 18 months

“complexity”  
= # of transistors on a chip

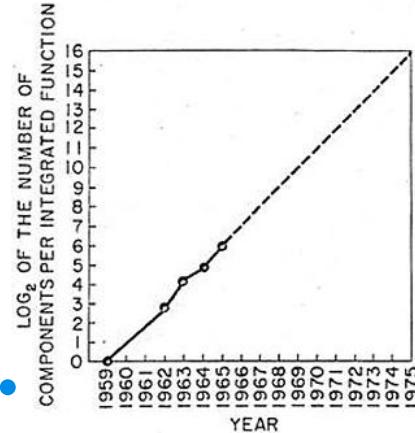
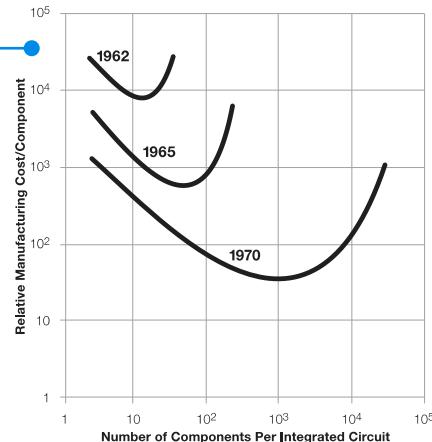


Fig. 2 Number of components per integrated function for minimum cost per component extrapolated vs time.

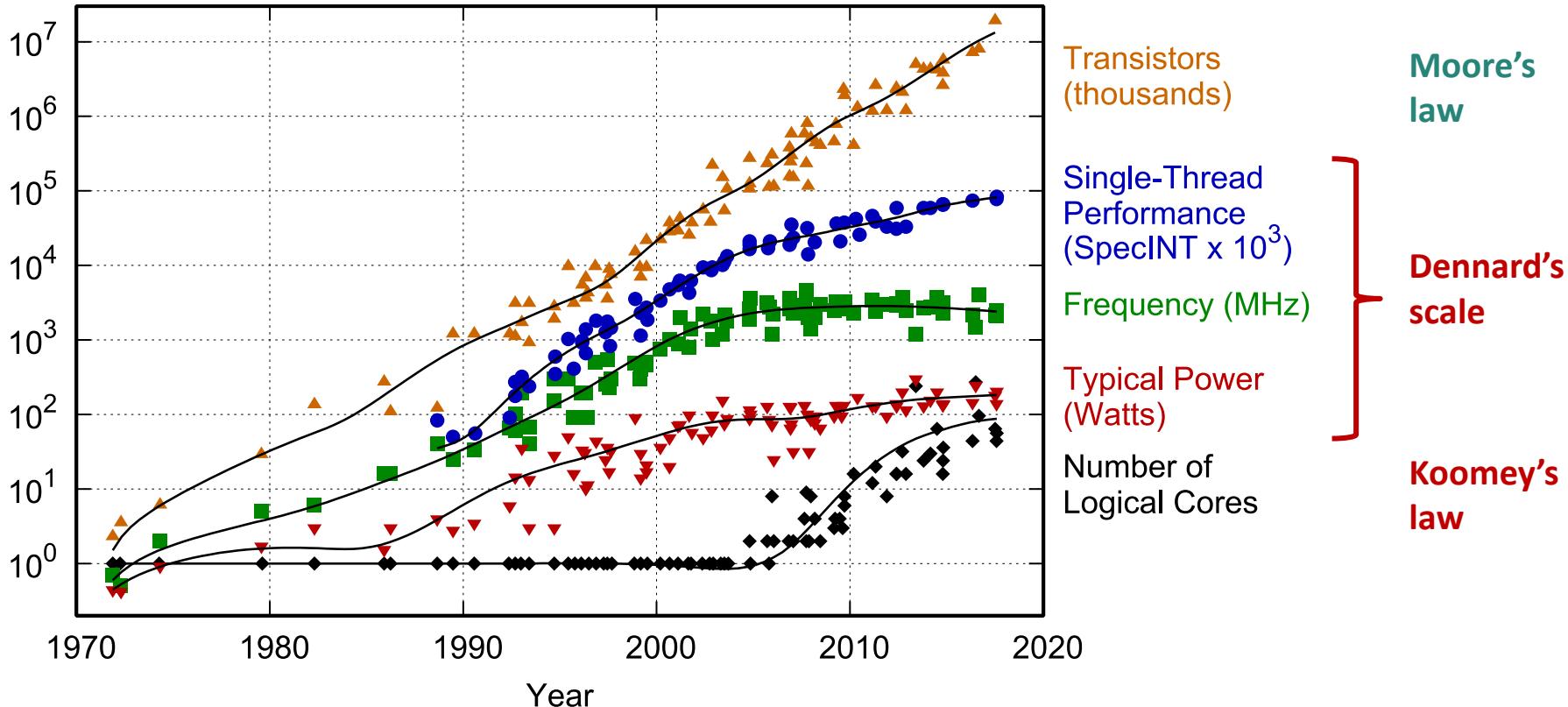
also, an economics driven law

many derivatives with:

- transistors density
- cost / transistor
- supercomputing power
- storage capacity
- cost of storage / GB
- networking speed
- CMOS imaging sensors resolution
- human genome sequencing cost



## 42 Years of Microprocessor Trend Data



Original data up to the year 2010 collected and plotted by M. Horowitz, F. Labonte, O. Shacham, K. Olukotun, L. Hammond, and C. Batten  
New plot and data collected for 2010-2017 by K. Rupp

# end of Dennard scale in 2006

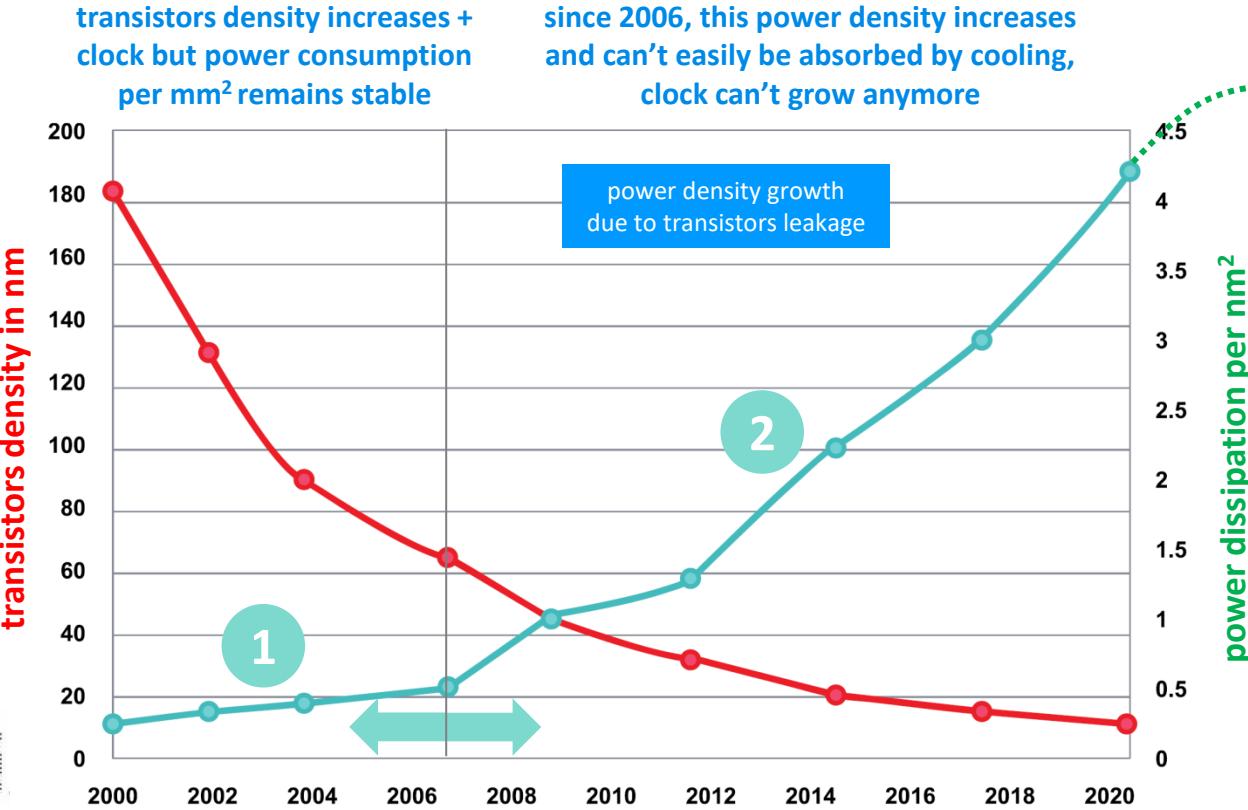
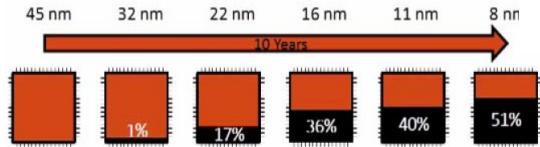
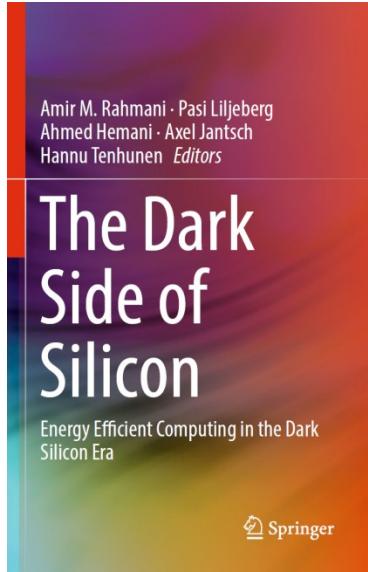
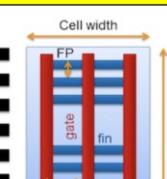


Table MM-7

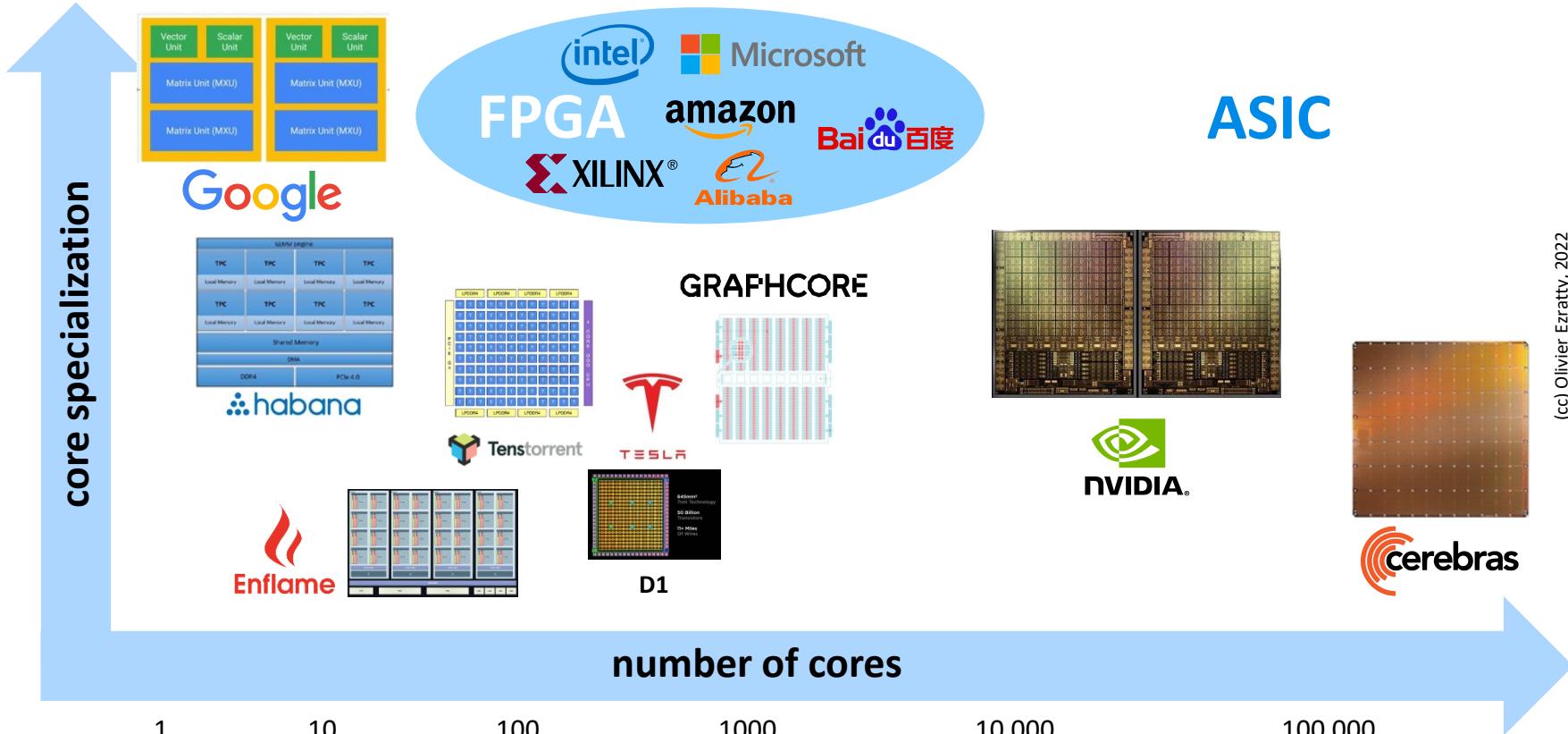
## *Device Architecture and Ground Rules Roadmap for Logic Devices*

Note: GxxMxx/Tx notation refers to Gxx: contacted gate pitch, Mxx: tightest metal pitch in nm, Tx: number of tiers. This notation illustrates the technology pitch scaling capability. On top of pitch scaling there are other elements such as cell height, number of stacked devices, DTCO constructs, 3D integration, etc. that define the target area scaling (gates/mm<sup>2</sup>).

YEAR OF PRODUCTION	2022	2025	2028	2031	2034	2037
<i>Logic industry "Node Range" Labeling</i>	G48M24 "3nm"	G45M20 "2nm"	G42M16 "1.5nm"	G40M16/T2 "1.0nm eq"	G38M16/T4 "0.7nm eq"	G38M16/T6 "0.5nm eq"
<i>Fine-pitch 3D integration scheme</i>	Stacking	Stacking	Stacking	3D VLSI	3D VLSI	3D VLSI
<i>Logic device structure options</i>	finFET LGAA	LGAA	LGAA CFET-SRAM	LGAA-3D CFET-SRAM	LGAA-3D CFET-SRAM	LGAA-3D CFET-SRAM
<i>Platform device for logic</i>	finFET	LGAA	LGAA CFET-SRAM	LGAA-3D CFET-SRAM-3D	LGAA-3D CFET-SRAM-3D	LGAA-3D CFET-SRAM-3D
						
<b>LOGIC DEVICE GROUND RULES</b>						
Mx pitch (nm)	32	24	20	16	16	16
M1 pitch (nm)	32	23	21	20	19	19
<b>M0 pitch (nm)</b>	<b>24</b>	<b>20</b>	<b>16</b>	<b>16</b>	<b>16</b>	<b>16</b>
Gate pitch (nm)	48	45	42	40	38	38
Lg: Gate Length - HP (nm)	16	14	12	12	12	12
Lg: Gate Length - HD (nm)	18	14	12	12	12	12
Channel overlap ratio - two-sided	0.20	0.20	0.20	0.20	0.20	0.20
Spacer width (nm)	6	6	5	5	4	4
Spacer k value	3.5	3.3	3.0	3.0	2.7	2.7
Contact CD (nm) - finFET, LGAA	20	19	20	18	18	18
<i>Device architecture key ground rules</i>						
Device lateral pitch (nm)	24	26	24	24	23	23
Device height (nm)	48	52	48	64	60	56
FinFET Fin width (nm)	5.0					
Footprint drive efficiency - finFET	4.21					
Lateral GAA vertical pitch (nm)	18.0	16.0	16.0	15.0	14.0	
Lateral GAA (nanosheet) thickness (nm)	6.0	6.0	6.0	5.0	4.0	
Number of vertically stacked nanosheets on one device	3	3	4	4	4	
LGAA width (nm) - HP	30	30	20	15	15	
LGAA width (nm) - HD	15	10	10	6	6	
LGAA width (nm) - SRAM	7	6	6	6	6	
Footprint drive efficiency - lateral GAA - HP	4.41	4.50	5.47	5.00	4.75	
Device effective width (nm) - HP	101.0	216.0	216.0	208.0	160.0	152.0
Device effective width (nm) - HD	101.0	126.0	96.0	128.0	88.0	80.0
PN separation width (nm)	45	40	20	15	15	10

*Acronyms used in the table (in order of appearance): LGAA—lateral gate-all-around-device (GAA), CFET (Complementary Field Effect Transistor), 3DVLSI—fine-pitch 3D logic sequential integration.*

# specialization vs core numbers

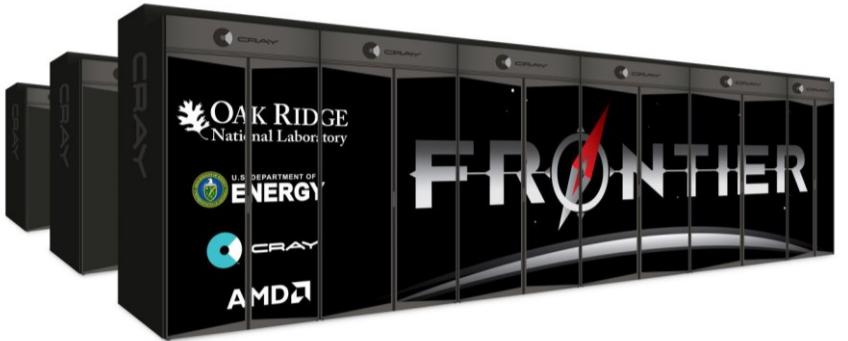


(cc) Olivier Ezratty, 2022

	max bandwidth	capacity
<b>SSD M.2 PCIe storage</b>	3 GB/s	>1 TB
<b>DDR4 CPU external memory</b>	10 GB/s	>16 GB
<b>Infiniband interserver comm</b>	25 GBs/s	<i>data bus</i>
<b>GDDR6X GPU external memory</b>	1 TB/s	2 GB – 12 GB
<b>NVLink 2.0 inter-GPU/CPU comm</b>	1.350 TB/s *	<i>data bus</i>
<b>HBM3 / HMC GPGPU external memory</b>	3 TB/s *	80 GB*
<b>cache &amp; registers CPU/GPU internal memory</b>	> 16 TB/ s	50 MB (L2)*

=> memory and storage speed are key advantages of classical computing vs quantum computing.

\*: in Nvidia H100 GPGPU



## HPE Frontier, ORNL (Tennessee)

9,400 AMD Epyc CPUs

37,000 Radeon Instinct MI250X GPUs

**1.1 exaflops**

700 PB storage

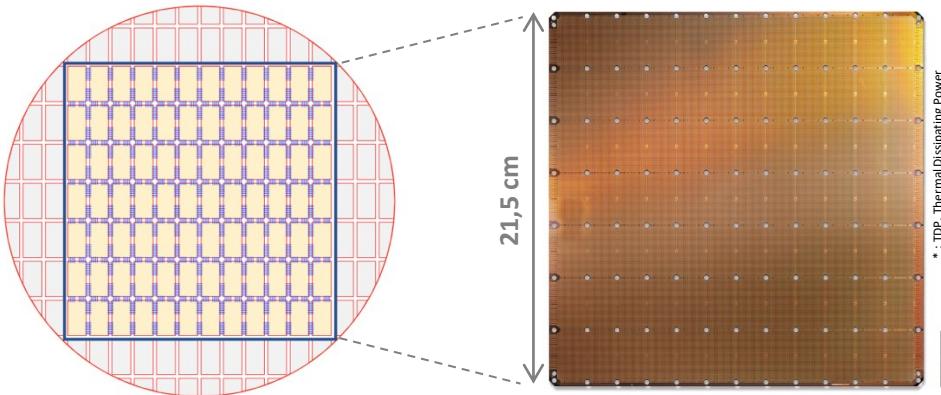
21 MW power consumption

Rank	Name	Computer	Country	Cores	Tflops/s	Gflops/W
1	Frontier	HPE Cray EX235a, AMD Optimized 3rd Generation EPYC 64C 2GHz, AMD Instinct MI250X, Slingshot-11	United States	8 730 112	1 102 000,00	52,23
2	Fugaku	Supercomputer Fugaku, A64FX 48C 2.2GHz, Tofu interconnect D	Japan	7 630 848	442 010,00	14,78
3	LUMI	HPE Cray EX235a, AMD Optimized 3rd Generation EPYC 64C 2GHz, AMD Instinct MI250X, Slingshot-11	Finland	1 110 144	151 900,00	51,63
4	Summit	IBM Power System AC922, IBM POWER9 22C 3.07GHz, NVIDIA Volta GV100, Dual-rail Mellanox EDR Infiniband	United States	2 414 592	148 600,00	14,72
5	Sierra	IBM Power System AC922, IBM POWER9 22C 3.1GHz, NVIDIA Volta GV100, Dual-rail Mellanox EDR Infiniband	United States	1 572 480	94 640,00	12,72
6	Sunway TaihuLight	Sunway MPP, Sunway SW26010 260C 1.45GHz, Sunway	China	10 649 600	93 014,59	6,05
7	Perlmutter	HPE Cray EX235n, AMD EPYC 7763 64C 2.45GHz, NVIDIA A100 SXM4 40 GB, Slingshot-10	United States	761 856	70 870,00	27,37
8	Selene	NVIDIA DGX A100, AMD EPYC 7742 64C 2.25GHz, NVIDIA A100, Mellanox HDR Infiniband	United States	555 520	63 460,00	23,98
9	Tianhe-2A	TH-IVB-FEP Cluster, Intel Xeon E5-2692v2 12C 2.2GHz, TH Express-2, Matrix-2000	China	4 981 760	61 444,50	3,32
10	Adastra	HPE Cray EX235a, AMD Optimized 3rd Generation EPYC 64C 2GHz, AMD Instinct MI250X, Slingshot-11	France	319 072	46 100,00	50,03
11	JUWELS Booster	Bull Sequana XH2000, AMD EPYC 7402 24C 2.8GHz, NVIDIA A100, Mellanox HDR InfiniBand/ParTec ParaStation ClusterSuite	Germany	449 280	44 120,00	25,01
12	HPCS	PowerEdge C4140, Xeon Gold 6252 24C 2.1GHz, NVIDIA Tesla V100, Mellanox HDR Infiniband	Italy	669 760	35 450,00	15,74
13	Voyager-EUS2	ND96amp-_A100_v4, AMD EPYC 7V12 48C 2.45GHz, NVIDIA A100 80GB, Mellanox HDR Infiniband	United States	253 440	30 050,00	
14	Polaris	Apollo 6500, AMD EPYC 7532 32C 2.4GHz, NVIDIA A100 SXM4 40 GB, Slingshot-10	United States	256 592	25 810,00	
15	SSC-21	Apollo 6500 Gen10 plus, AMD EPYC 7543 32C 2.8GHz, NVIDIA A100 80GB, Infiniband HDR200	South Korea	204 160	25 177,00	
16	Frontera	Dell C6420, Xeon Platinum 8280 28C 2.7GHz, Mellanox InfiniBand HDR	United States	448 448	23 516,40	
17	CEA-HF	BullSequana XH2000, AMD EPYC 7763 64C 2.45GHz, Atos BXI V2	France	810 240	23 237,60	4,69
18	Dammam-7	Cray CS-Storm, Xeon Gold 6248 20C 2.5GHz, NVIDIA Tesla V100 SXM2, InfiniBand HDR 100	Saudi Arabia	672 520	22 400,00	
19	ABC1 2.0	PRIMERGY GX2570 M6, Xeon Platinum 8360Y 36C 2.4GHz, NVIDIA A100 SXM4 40 GB, Infiniband HDR	Japan	504 000	22 208,72	13,88
20	Wisteria/BDEC-01 (Odyssey)	PRIMEHPC FX1000, A64FX 48C 2.2GHz, Tofu interconnect D	Japan	368 640	22 121,00	15,07
21	Marconi-100	IBM Power System AC922, IBM POWER9 16C 3GHz, Nvidia Volta V100, Dual-rail Mellanox EDR Infiniband	Italy	347 776	21 640,00	14,66
22	Chervonenkis	YANDEX Y4N-GAI-1Y25-ZB0, AMD EPYC 7702 64C 2.2GHz, NVIDIA A100 80GB, Infiniband	Russia	193 440	21 530,00	
23	Piz Daint	Cray XC50, Xeon E5-2690v3 12C 2.6GHz, Aries interconnect , NVIDIA Tesla P100	Switzerland	387 872	21 230,00	8,90
24	Trinity	Cray XC40, Xeon E5-2698v3 16C 2.3GHz, Intel Xeon Phi 7250 68C 1.4GHz, Aries interconnect	United States	979 072	20 158,70	2,66
25	ARCHER2	Cray EX, AMD EPYC 7742 64C 2.25GHz, Slingshot-10	United Kingdom	716 800	19 539,00	

source: TPC500, June 2022



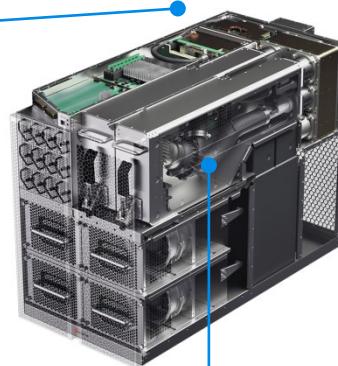
« wafer scale processor »



**WSE-2**  
**2.6 trillion transistors**  
84 units on 215x215 mm, 7 nm  
850 000 SLAC cores  
8 ops/clock per core at 1 GHz  
40 GB SRAM, 15kW TDP\*



water movement assembly (top)  
and air exchanger (bottom)



water movement assembly (top)  
and air exchanger (bottom)



Cerebras CS-2 system  
rack 15U

Nvidia

A100

(cc) Olivier Ezratty, 2022

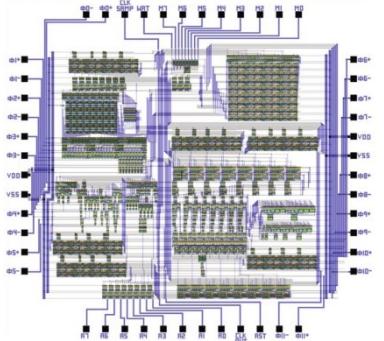


first customer / tester

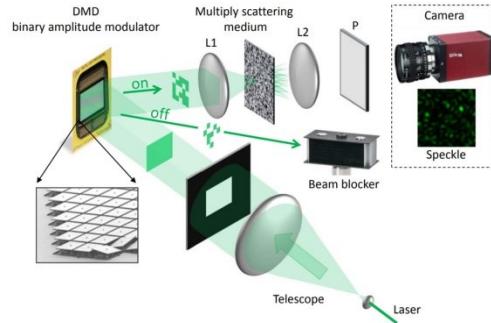
# other unconventional computing



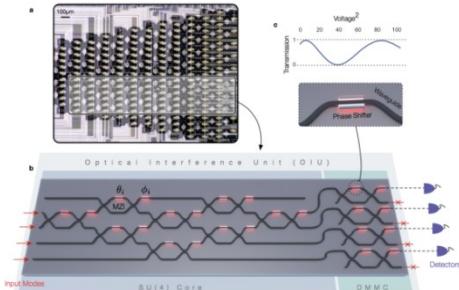
# digital annealing



# reversible computing



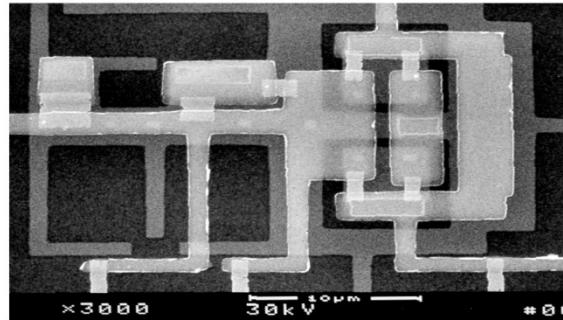
# **light processors**



## III/V optronics

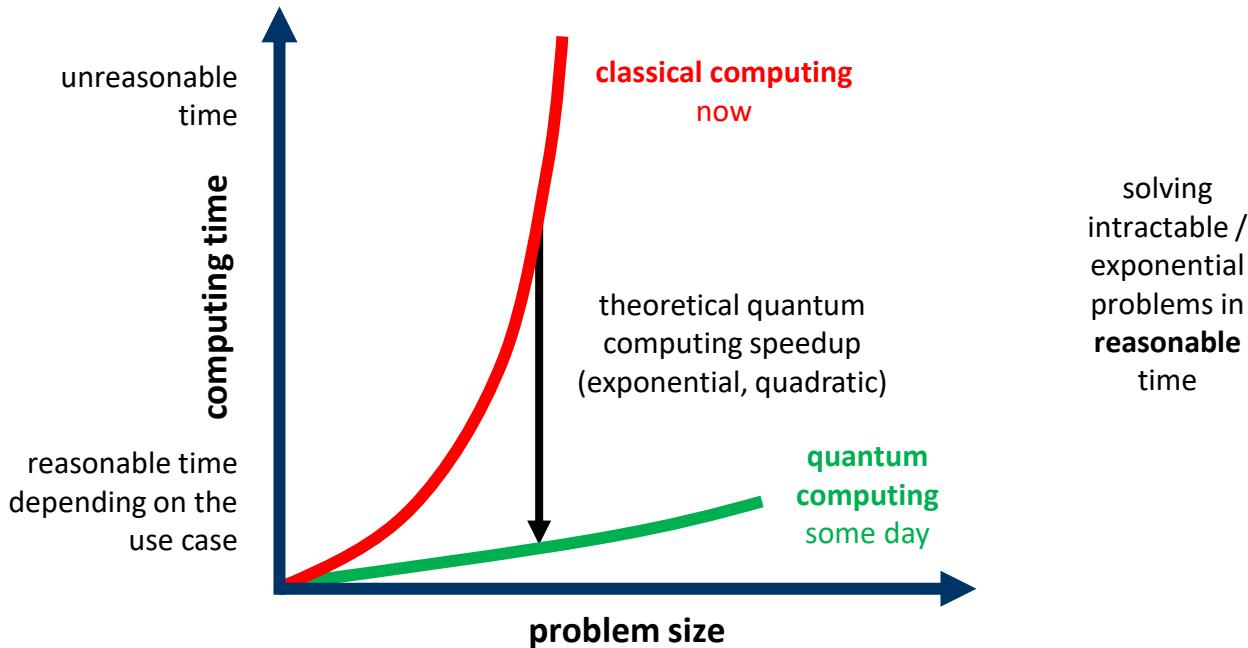


# probabilistic computing

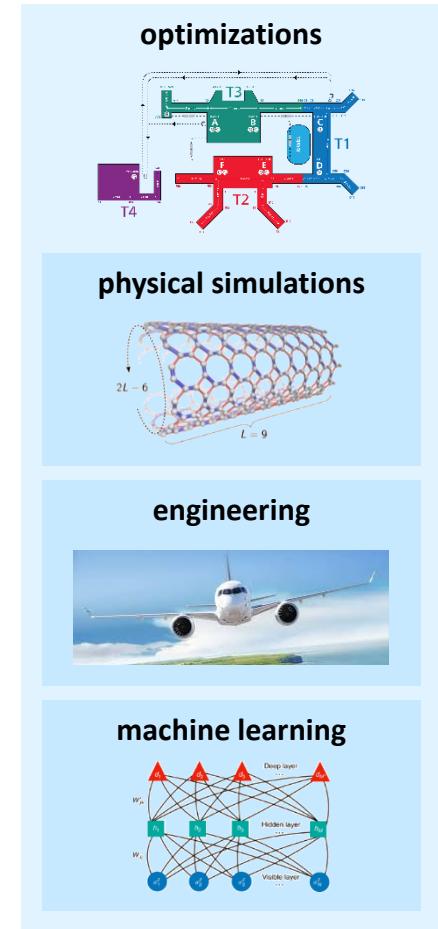


## **superconducting processors**

# quantum computing promise



(cc) Olivier Ezratty, 2023



# quantum computing usage categories

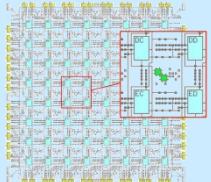
## research



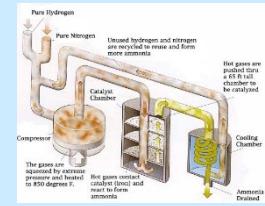
batteries



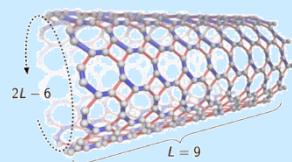
drugs



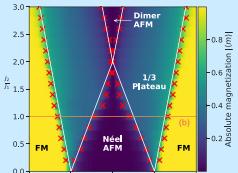
semiconductors



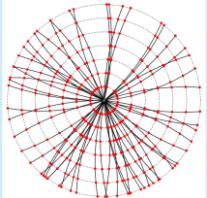
fertilizers production



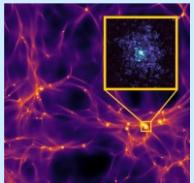
materials design



condensed matter physics



high-energy particle physics

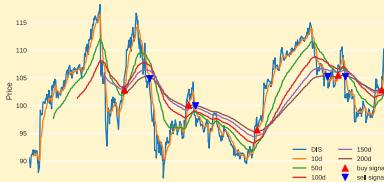


astrophysics

## operations



transportation



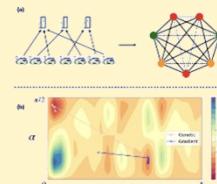
financial services



logistics



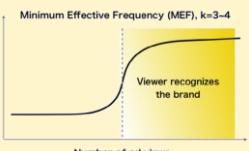
delivery



energy utilities



telecoms

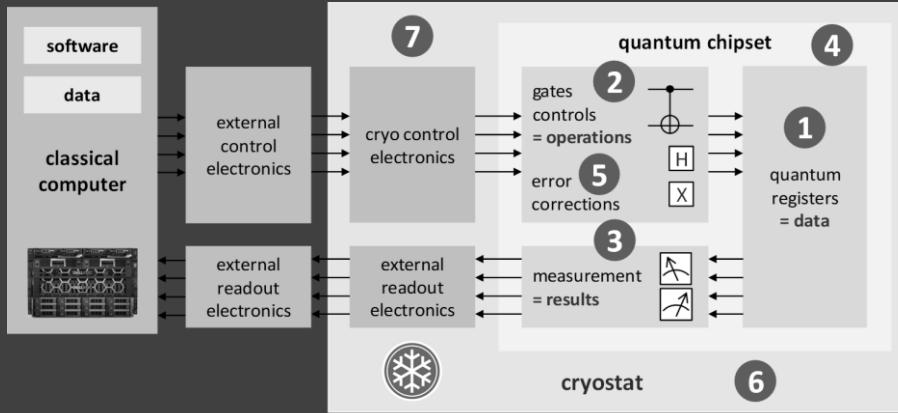


manufacturing

marketing

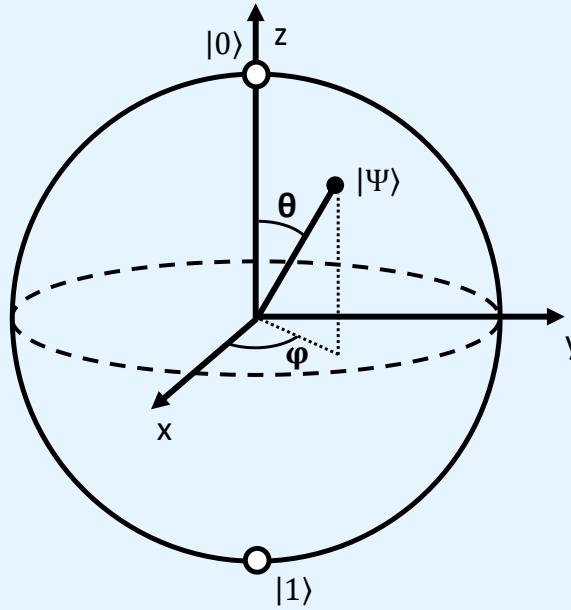
# lunch time





# quantum computing architecture and engineering

# qubits 101



# what is a qubit?

mathematically

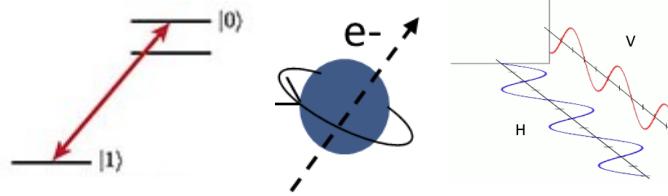
**basic unit of quantum information**  
vector in a 2-dimension Hilbert space



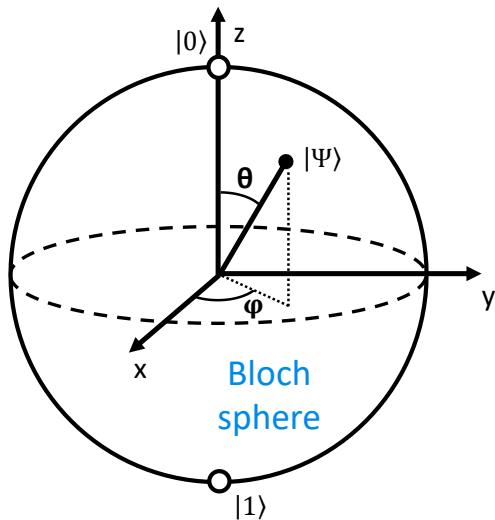
physical  
implementation

**two-state quantum object**

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



# qubits mathematical operations



complex combinations  
amplitudes of 0s and 1s

$$\begin{bmatrix} \alpha_1 \\ \dots \\ \dots \\ \dots \\ \dots \\ \alpha_{2^N} \end{bmatrix} \quad \begin{array}{l} |00\dots00\rangle \\ |10\dots01\rangle \\ |11\dots11\rangle \end{array}$$

CNOT gate

$$\begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{11} \\ \alpha_{10} \end{bmatrix}$$

two-level quantum object,  
handling the equivalent of  
two floating point numbers

N qubits handle the  
equivalent of  $2^{N+1}-1$   
floating point numbers

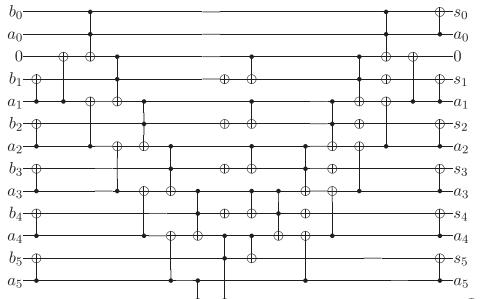
entanglement creates links between  
qubits and brings computing power  
under certain circumstances

# from computing to measurement

« computational basis state vector »

complex amplitudes of all combinations of 0 and 1

$$\begin{bmatrix} \alpha_1 \\ \dots \\ \dots \\ \dots \\ \alpha_{2^N} \end{bmatrix} \begin{array}{l} |00 \dots 00\rangle \\ |10 \dots 01\rangle \\ |11 \dots 11\rangle \end{array}$$

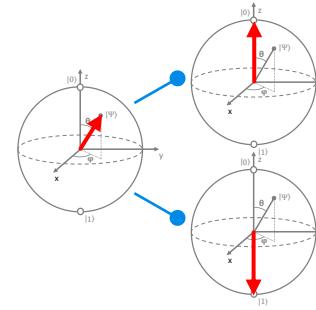


The ripple-carry adder for  $n = 6$ .

**N qubits registers**  
information in  $2^N$  superposed states

**quantum gates**

actions on qubits and their superposed states



**010...1  
11**

**measurement**

ends superposition and entanglement

**outputs**

**N probabilistic classical bits**

**computing**

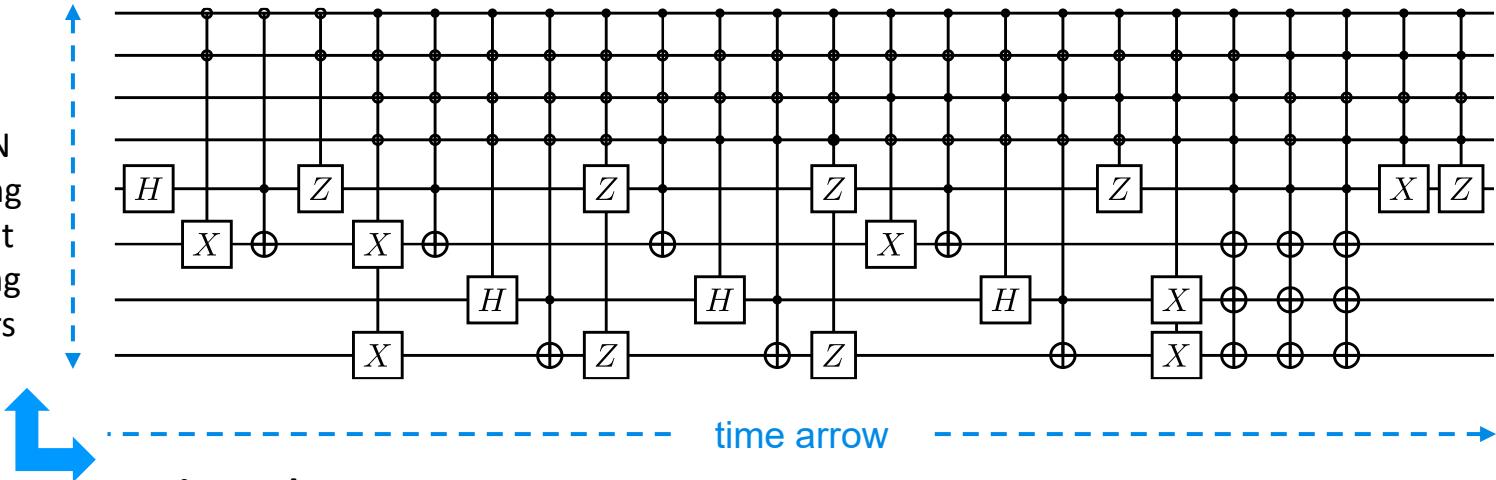
has to be run many times and results averaged  
**>4000 runs and growing with the number of qubits**

- each computing result is non-deterministic
- averaged result is asymptotically deterministic
- errors generated by noise and decoherence

# space vs time advantage

space  
advantage

comes from N  
qubits handling  
the equivalent  
of  $2^{N+1}$  floating  
point numbers



space/time  
trade-offs

one can be improved  
at the expense of the  
other

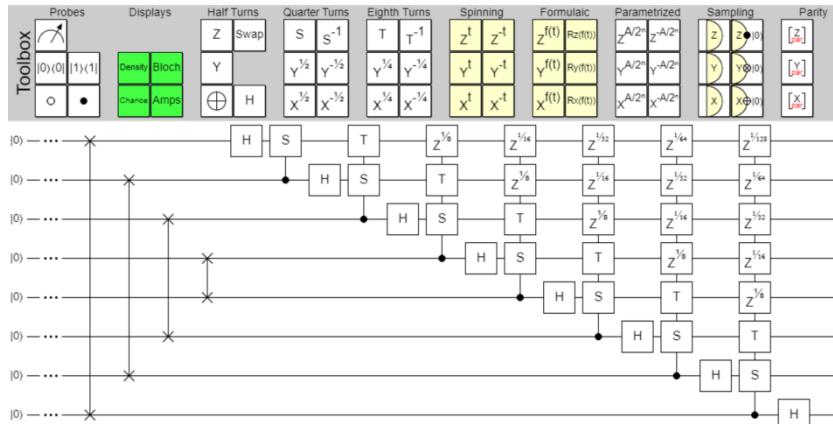
time advantage

when the number of gates  
cycles scales slower than  
with equivalent classical  
algorithms

1. quantum computing is **not instantaneous**.
2. the number of gate cycles can still **scale polynomially** with the number of qubits.
3. non-shallow algorithms require **error correction** which brings its own time overhead.

# a new programming model

## visual quantum circuits design



<https://algassert.com/quirk>

online open source tool to learn, program and emulate up to 16 qubits

## scripted Python code

```
# Initialize counting qubits
# in state |+>
for q in range(n_count):
    qc.h(q)

# And auxiliary register in state |1>
qc.x(3+n_count)

# Do controlled-U operations
for q in range(n_count):
    qc.append(c_amod15(a, 2**q),
              [q] + [i+n_count for i in range(4)])

# Do inverse-QFT
qc.append(qft_dagger(n_count), range(n_count))

# Measure circuit
qc.measure(range(n_count), range(n_count))
qc.draw(fold=-1) # -1 means 'do not fold'
```

IBM Qiskit, Google Cirq, Atos myQLM

# some key differences

$$f(\lambda x) = \lambda f(x) \text{ for all } \lambda, x \in \mathbb{R}$$

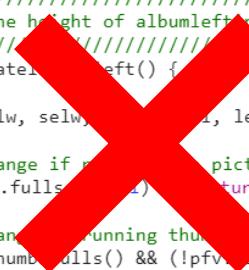
$$f(x + y) = f(x) + f(y) \text{ for all } x, y \in \mathbb{R}$$

$$\langle \Psi_1 | \Psi_2 \rangle = [\overline{\alpha_1}, \overline{\beta_1}] \times \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} = \overline{\alpha_1} \alpha_2 + \overline{\beta_1} \beta_2$$

$$|\Psi_2\rangle\langle\Psi_1| = \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} \times [\overline{\alpha_1}, \overline{\beta_1}] = \begin{bmatrix} \alpha_2 \overline{\alpha_1} & \alpha_2 \overline{\beta_1} \\ \beta_2 \overline{\alpha_1} & \beta_2 \overline{\beta_1} \end{bmatrix}$$

need to understand  
linear algebra

uncopyable data, but transferable

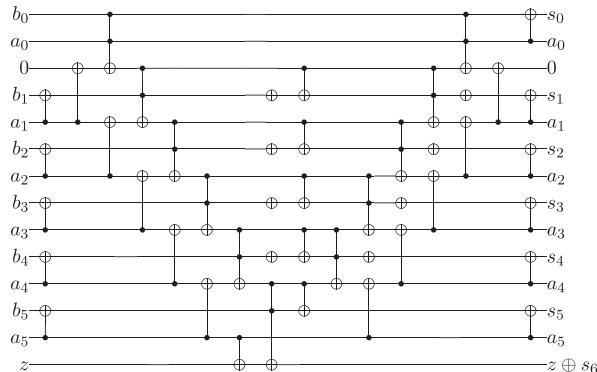


```
711 //////////////////////////////////////////////////////////////////
712 // Updates the height of albumleftinside DIV.
713 //////////////////////////////////////////////////////////////////
714 function updateAlbumLeft() {
715
716     var availw, selw, selh, len, newh;
717
718     // No change if no picture full screen.
719     if (pfv.fullscreen == false) { return; }
720
721     // No change if running thumbfull screen, and not on
722     if (arethumbfulls() && (!pfv.issmart)) { return; }
723 }
```

no breakpoints  
for debugging

# quantum computing paradigms

## gates-based quantum computers



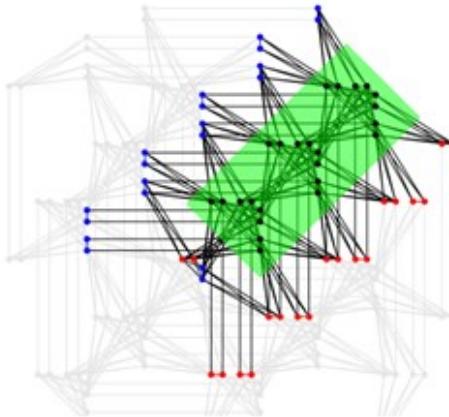
The ripple-carry adder for  $n = 6$ .

sequential programming of quantum gates, can implement any algorithm and Hamiltonian transformation



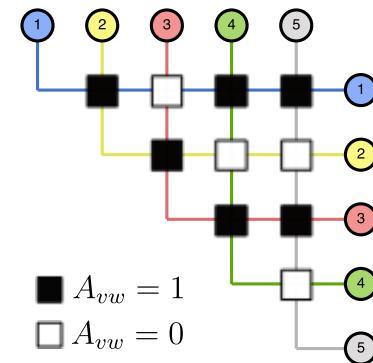
QUANDELA

## quantum annealers



finding a ground state of an Ising model, optimization problems are mapped to Ising models (QUBO)

## quantum simulators

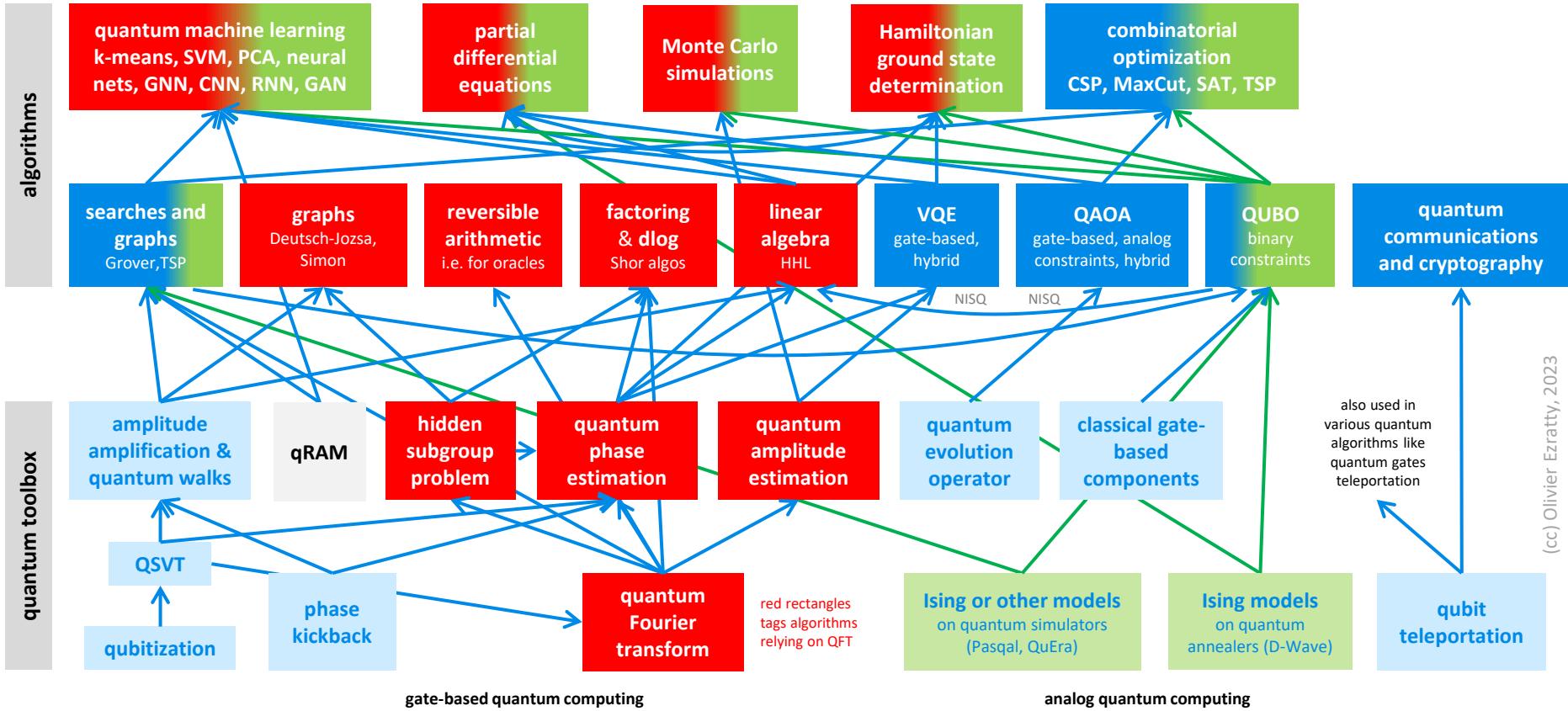


finding a ground state of an Ising model or XY quantum simulation model (with more degrees of liberty)

D-WAVE  
The Quantum Computing Company™

PASQAL  
IQuEra COMPUTING INC.

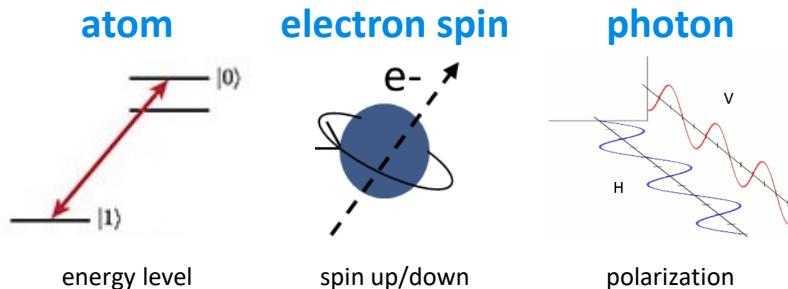
# quantum algorithms zoo



# qubits hardware



# 5 DiVincenzo criteria (IBM, 2000)



## characterized qubits

laser pumping

micro-waves  
DC current

polarizer

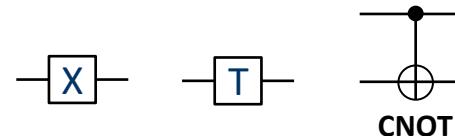
## initializable qubits

laser +  
fluorescence

micro-waves  
phase/amplitude  
analizis

photon  
detectors

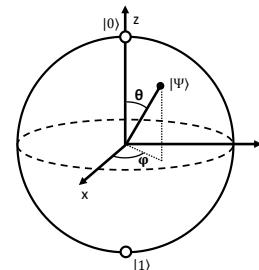
## measureable qubits



hardware level gates depend on the qubit technology

## universal quantum gates set

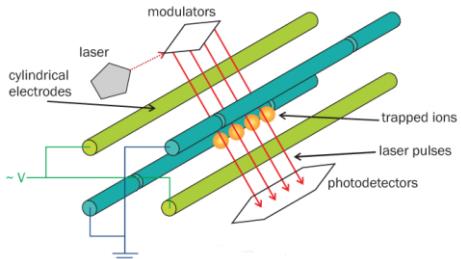
acting on qubits  
for gates and  
measurement



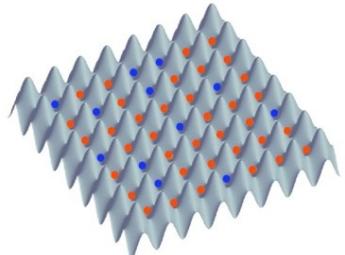
qubit must also  
be as isolated as  
possible to avoid  
decoherence

coherence time  $>>$  gate time

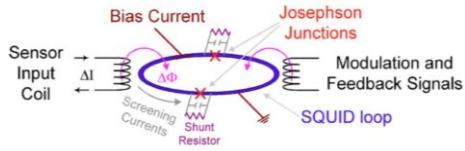
# main qubit types



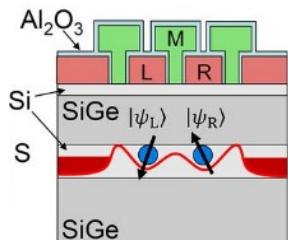
trapped ions



cold atoms

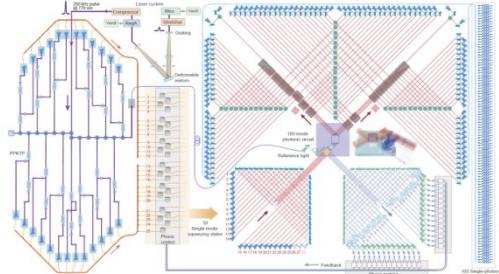


superconducting

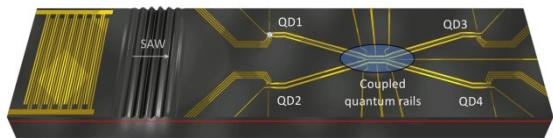


electron spin

stationary qubits



photons



flying and shuttling electrons

flying qubits

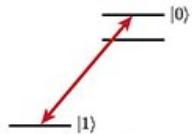
## main qubit types

## quantum states

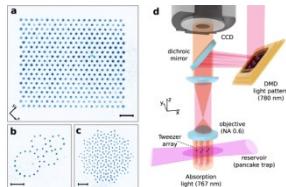
## **physical aspect**

## interactions

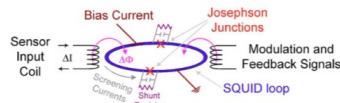
## atoms



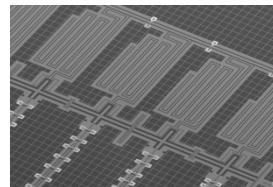
atom energy  
level



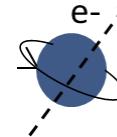
## superconducting



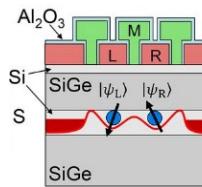
loop phase or  
energy



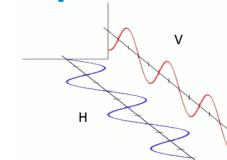
# electron spins



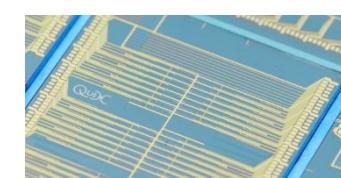
## electron spin orientation



# photons



## photon polarization (or other property)



laser pulses and/or  
microwaves

microwave pulses and/or DC current

**IBM**



**D-Wave**  
The Quantum Computing Company™



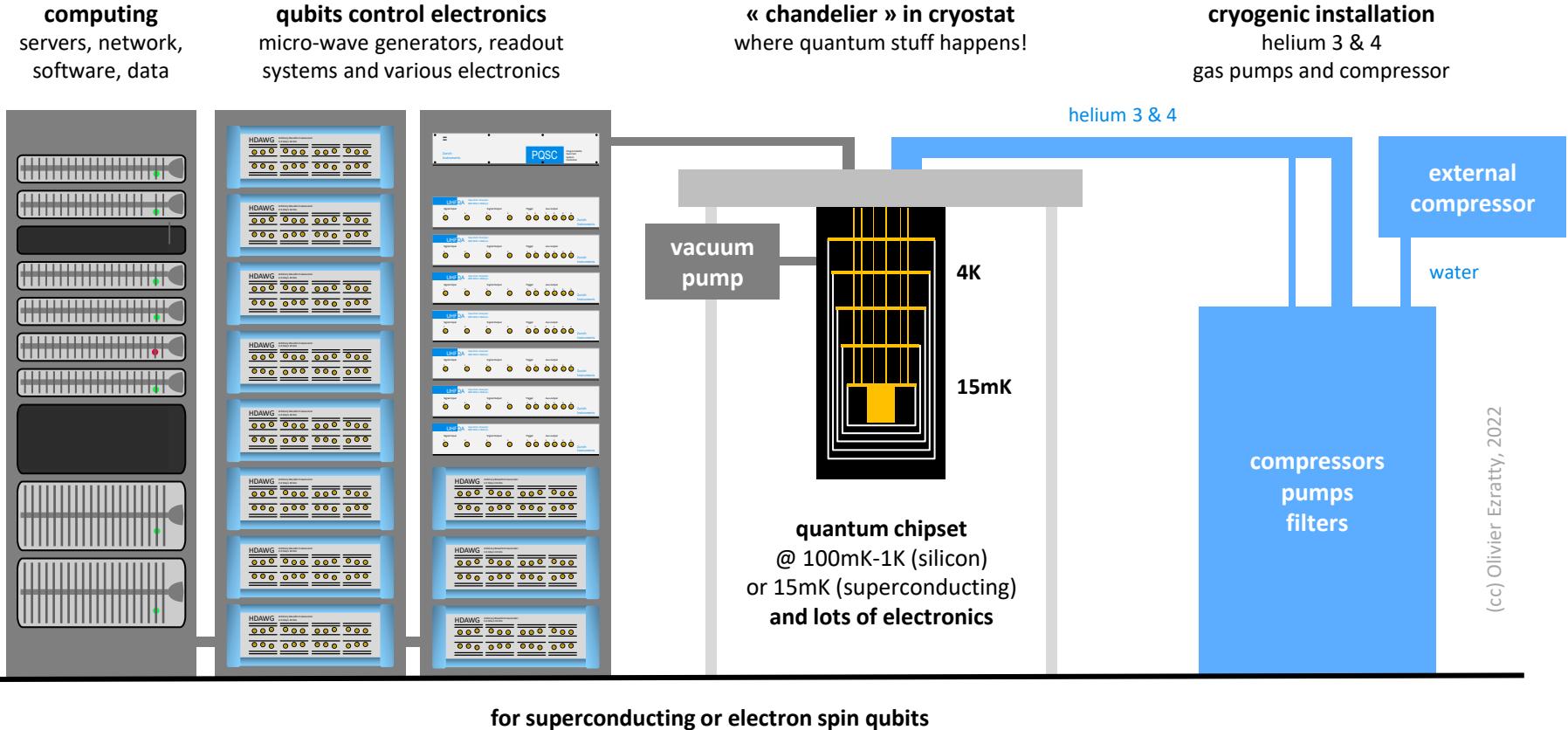
**IONQ**



**PASQAL**

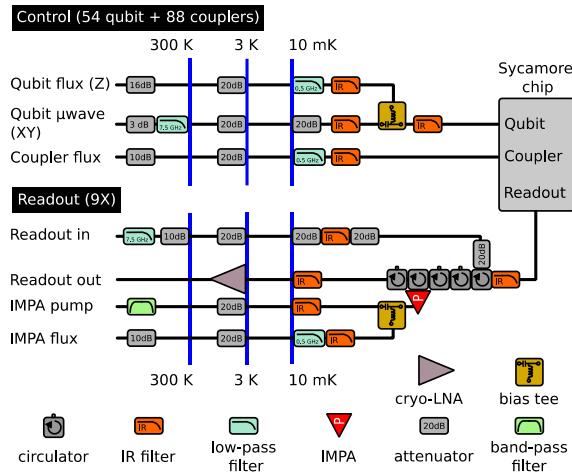


# inside a typical quantum computer

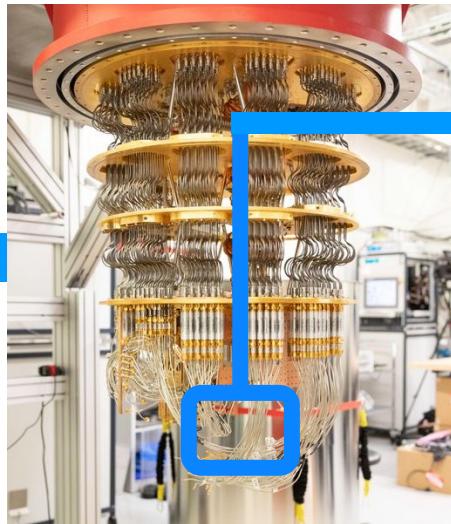


(cc) Olivier Ezratty, 2022

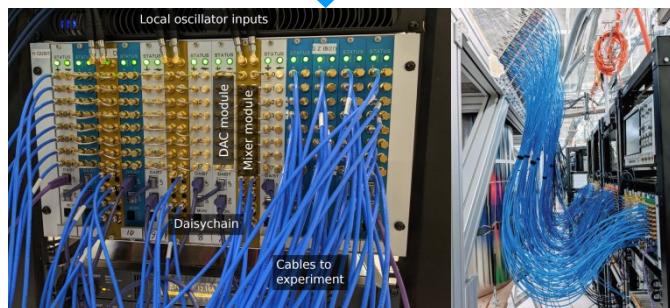
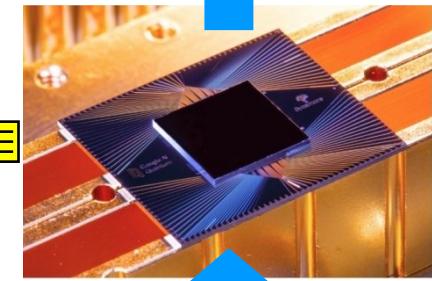
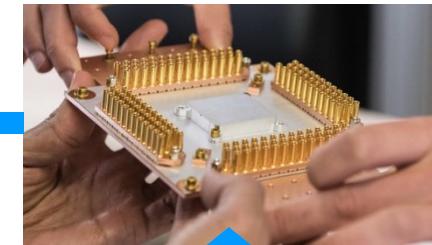
## active and passive control electronics



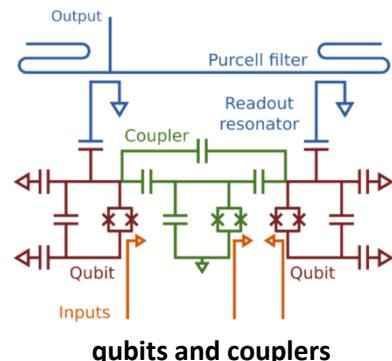
## vacuum chamber



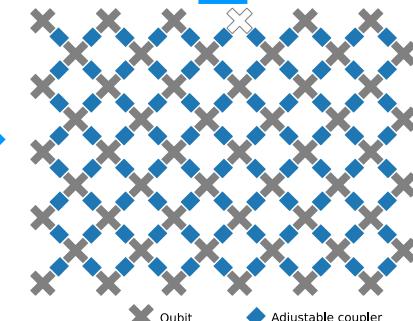
## packaging and chipset



micro-wave sources and readout



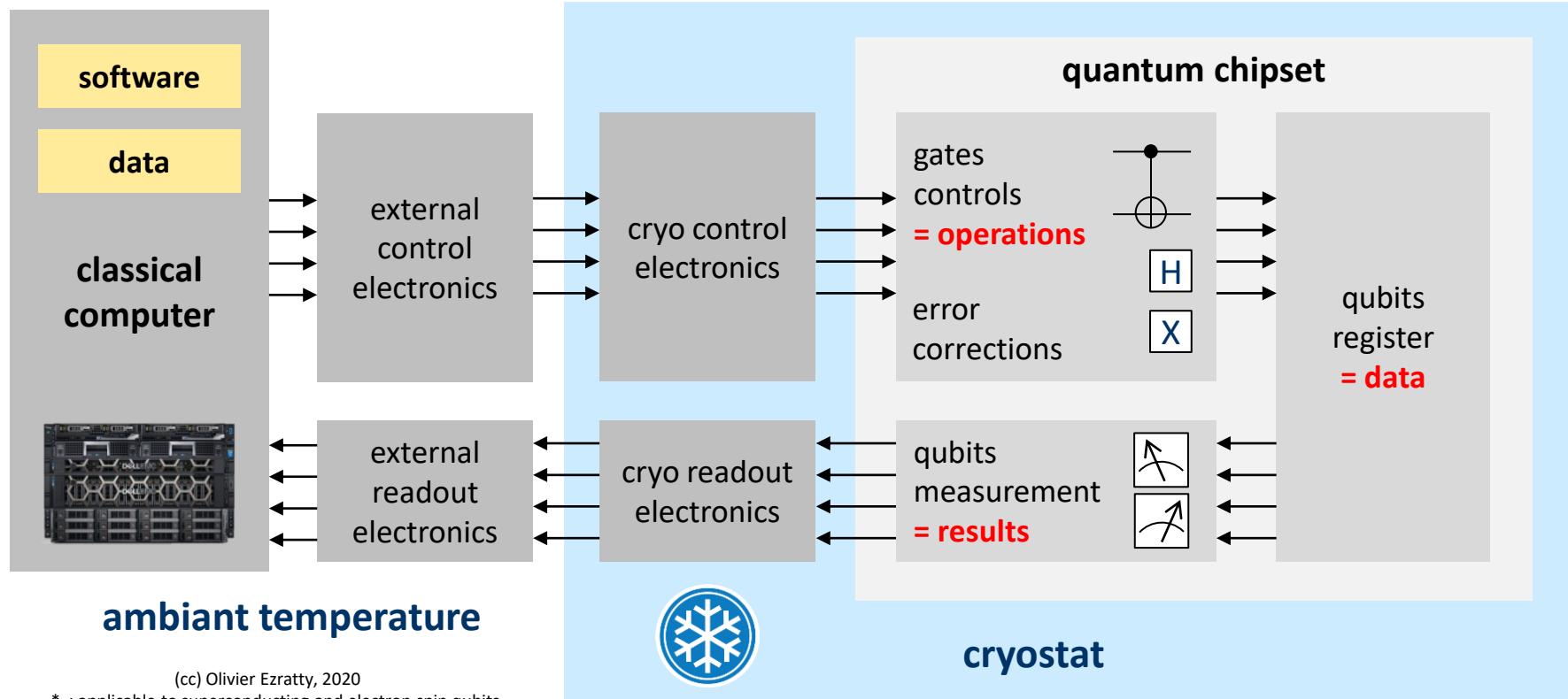
qubits and couplers



Qubit

Adjustable coupler

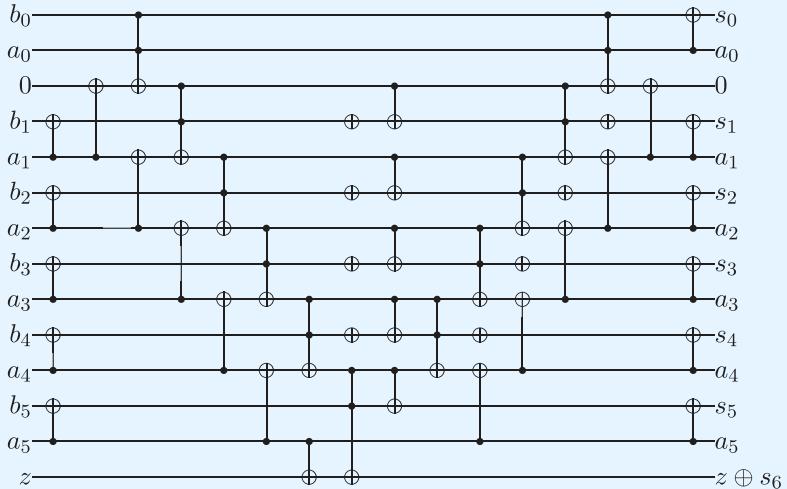
# quantum computer architecture \*



(cc) Olivier Ezratty, 2020

\* : applicable to superconducting and electron spin qubits

# qubits logic



The ripple-carry adder for  $n = 6$ .

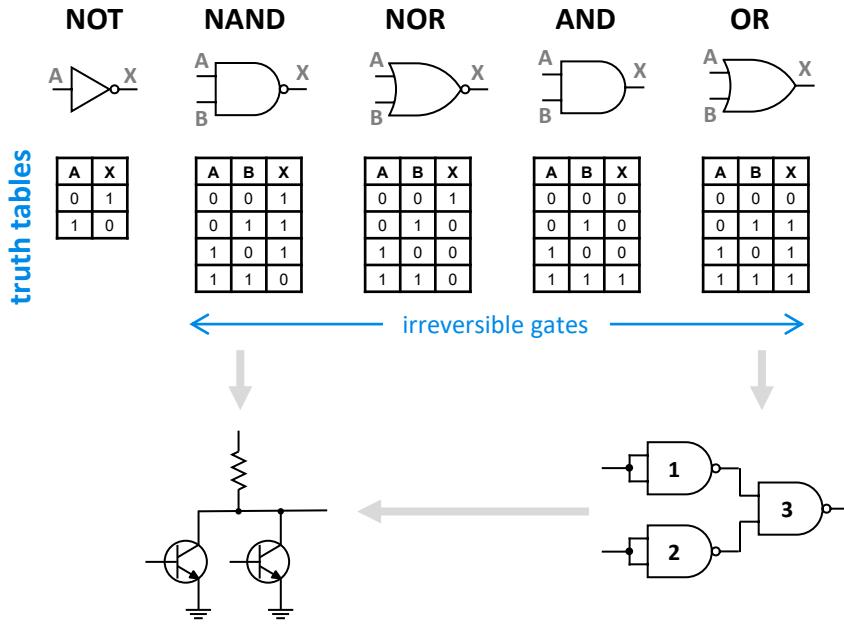
# qubit register

n bits register	n qubits register	
101	$2^n$ possible states once at a time	$000$ $001$ $010$ $011$ $100$ $101$ $110$ $111$
evaluable	$n=3$ example	linearly superposed
independent copies		partially evaluable
individualy erasable		no copy
non destructive readout		non individualy erasable
deterministic		value changed after readout
		probabilistic
		aka register pure states

# qubit gates

## classical logic gates

boolean algebra on 1 or 2 bits



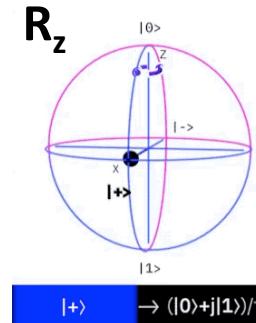
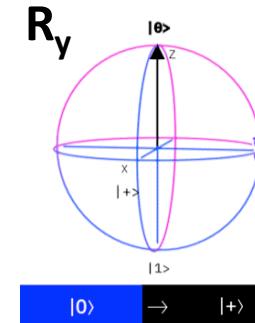
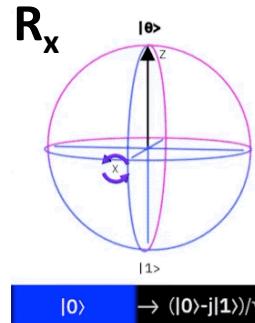
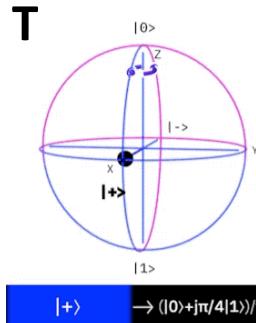
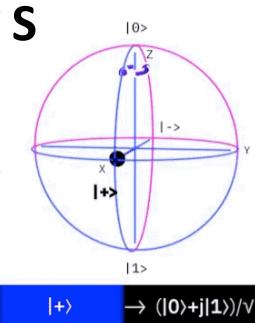
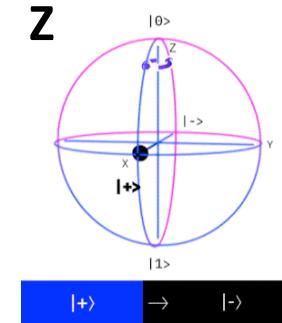
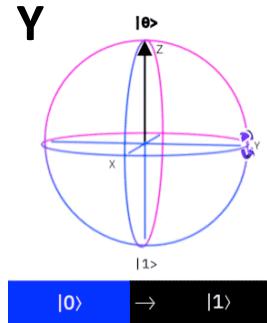
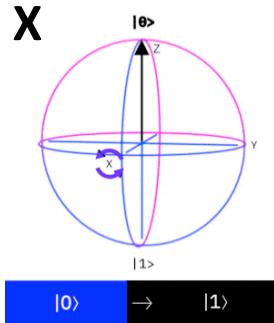
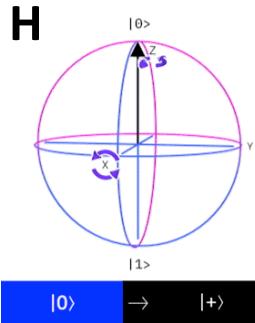
(cc) Olivier Ezratty, february 2021

## quantum gates

matrix based reversible **unitary** transformations

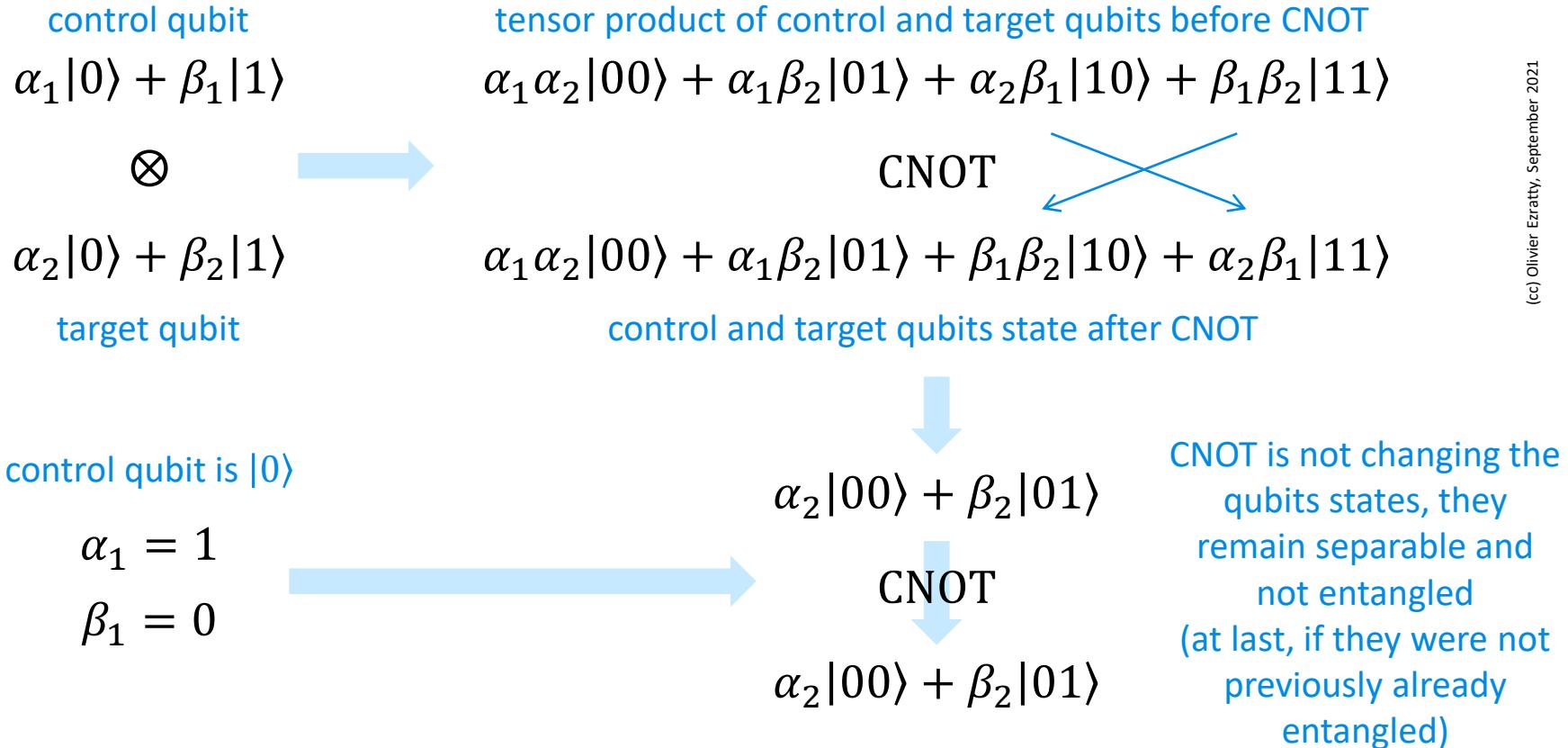
<b>rotation X</b>	<b>rotation Y</b>	<b>rotation Z</b>	<b>superposition</b> Hadamard
<b>NOT</b>			
$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
<b>CNOT</b>	<b>C2NOT</b> Toffoli	<b>SWAP</b>	<b>Fredkin</b> conditional SWAP
$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

# single qubit operations visualization

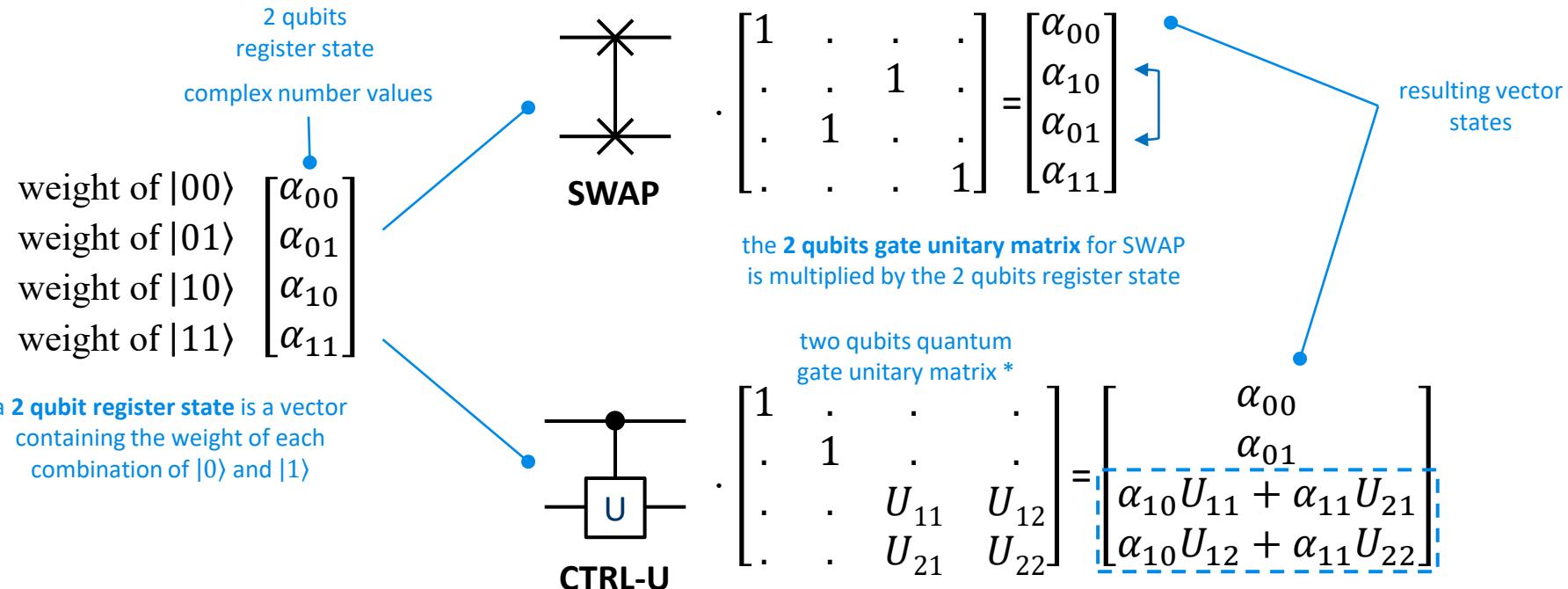


source : IBM Quantum instruction glossary

# CNOT gate effect



# SWAP and control-U gates maths



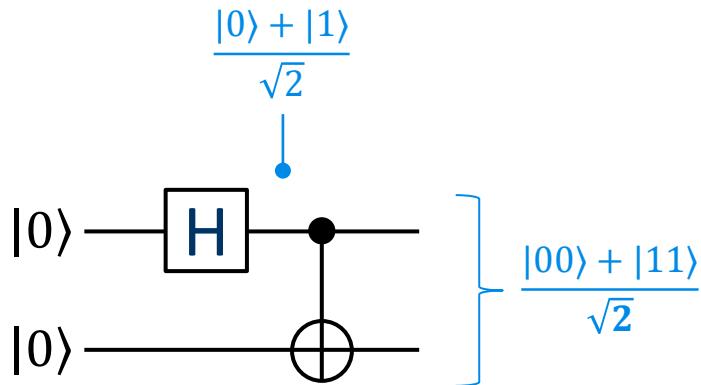
a **2 qubit register state** is a vector containing the weight of each combination of  $|0\rangle$  and  $|1\rangle$

\*  $\therefore = 0$  to improve matrix readability

generic **control-Unitary operation**, Unitary being any qubit gate given  $U^\dagger = U^{-1}$ , meaning  $U$ 's conjugate transpose =  $U$ 's inverse. it changes weights for  $|10\rangle$  and  $|11\rangle$  correlation and **creates some entanglement** between the two qubits

# the EPR pair entanglement building block

put control qubit into superposition state,  
then future gates act on two states  
simultaneously



subsequently, flipping a  
qubit in an entangled state  
modifies all its components

an entangled EPR pair can't be a tensor product  
of two qubits  $|\Psi_1\rangle$  and  $|\Psi_2\rangle$

$$|\Psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle \quad |\Psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$$

$$|\Psi_1\rangle \otimes |\Psi_2\rangle = (\alpha_1|0\rangle + \beta_1|1\rangle)(\alpha_2|0\rangle + \beta_2|1\rangle)$$

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$$

$$\alpha_1\beta_2 = 0 \text{ and } \beta_1\alpha_2 = 0$$

are incompatible with  $\alpha_1\alpha_2 = \frac{1}{\sqrt{2}}$  and  $\beta_1\beta_2 = \frac{1}{\sqrt{2}}$

if  $\alpha_1 = 0$  then  $\alpha_1\alpha_2 = 0$

if  $\beta_2 = 0$  then  $\beta_1\beta_2 = 0$

implications: the density matrix mathematical representation  
of qubits registers

# a simple example with a 4 qubits register

$2^4$  computational states values in register from  $|0000\rangle$  to  $|1111\rangle$ , initialized at  $|0000\rangle$

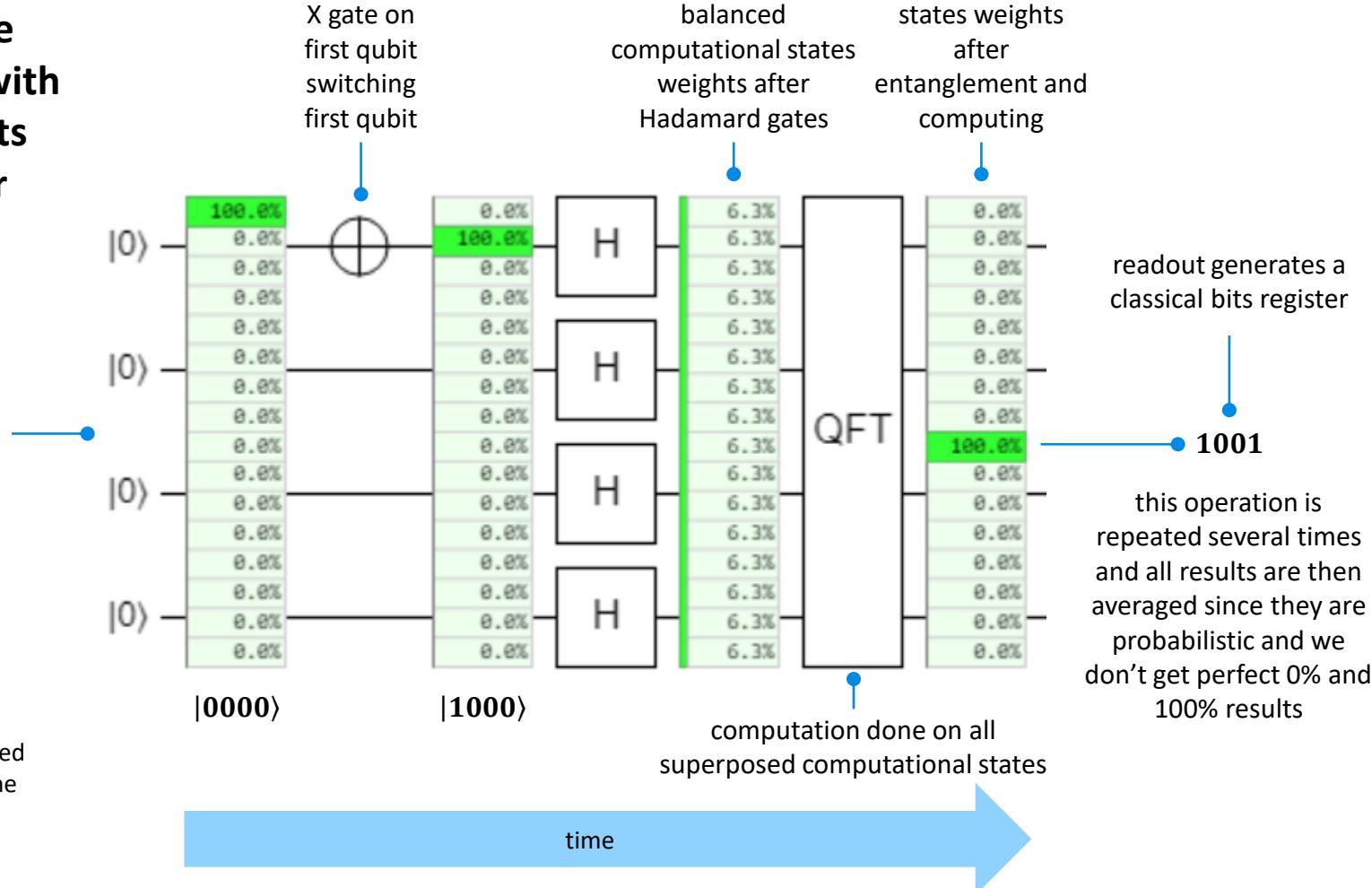


illustration created with Quirk online emulator

# universal gates sets

at the physical qubits level, only a few single and two qubit gates are usually implemented.

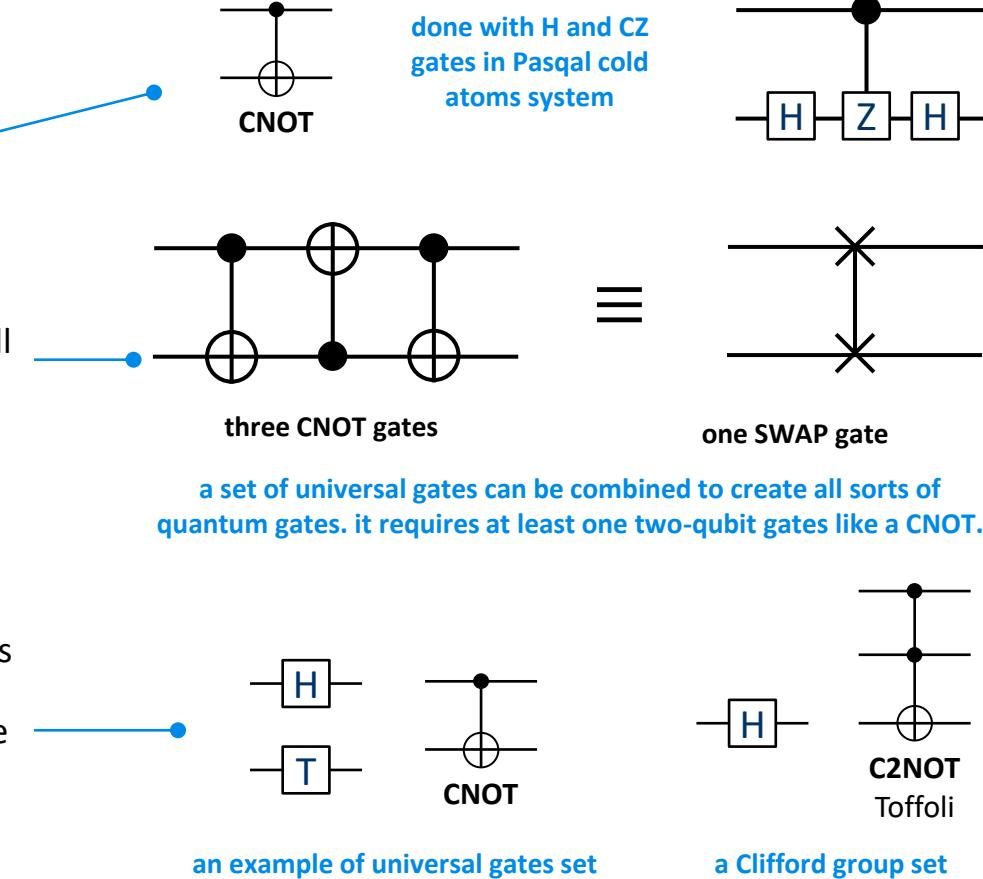
it depends on qubits physics and controls. e.g. :

$\sqrt{SWAP}$  two-qubit gate for electron spin or CZ gates with cold atoms.

**universal gates set** can be combined to create all gates like X, Y, Z, H, R, Control-R, T, S, SWAP, CZ, etc.

**X and Y Pauli single qubit gates and C-NOT** are sufficient to create a wide set of gates and unitary transformations.

**universal quantum computing** requires a T gate ( $\pi/4$  rotation) to create all controlled-phase gates and, by approximation, all possible unitary transformations. these gates are key to generate exponential speed gains.



# $SU(2^n)$ – space of unitaries on $n$ qubits

## $SU(2)$ – space of unitaries on one qubit

### Clifford group

#### Pauli group

##### Pauli gates



X rotation



Y rotation



Z rotation

Pauli gates combinations  
with  $\pm 1$  and  $\pm i$

##### other one-qubit gates



$\pi/2$



Hadamard



$\pi/4$



other rotations  
than  $\pi$   
and  $\pi/2$

### Barenco theorem

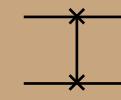
$SU(2^n)$  unitaries can be built out  
of  $SU(2)$  unitaries and a CNOT

Gottesman-Knill theorem  
Clifford gates are classically  
polynomially simulable

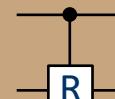
### multi-qubits gates



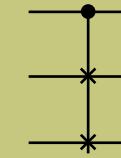
CNOT



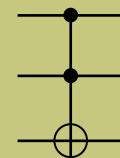
SWAP



control  $\pi$  and  $\pi/2$



Fredkin  
conditional SWAP



C2NOT  
Toffoli



other rotations with  $n > 2$

all linear combinations of Pauli gates

Solovay-Kitaev theorem  
approximation of all  $SU(2)$   
qubit gates requires a T gate

(cc) Olivier Ezratty, 2021

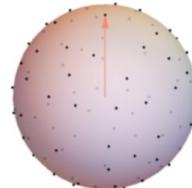
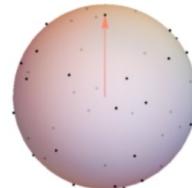
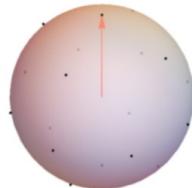
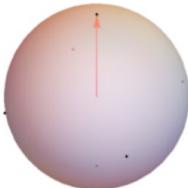
# Solovay-Kitaev theorem 1995-1997

any desired gate can be approximated by a sequence of gates from an universal gates set.

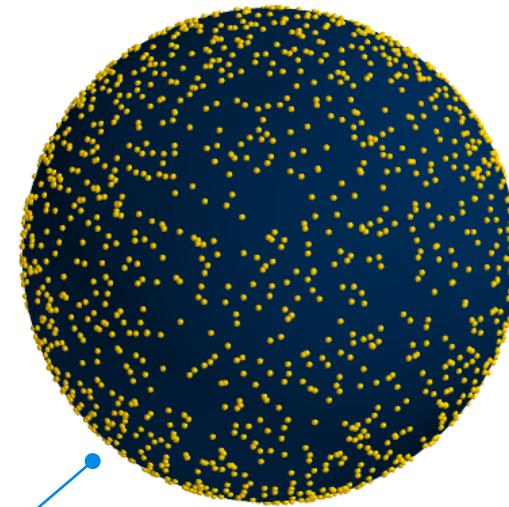
a quantum circuit of  $m$  constant-qubit gates can be approximated to  $\epsilon$  error by a quantum circuit of  $O(m \log^c(m/\epsilon))$  gates from a desired finite universal gate set with  $c=3,97$ .

for example, creating a  $R_{15}$  gate requires 127 H/Z/T gates with an approximation error of  $10^{-5}$  \*.

these approximations are particularly useful for Shor algorithm and to generate a real exponential acceleration.



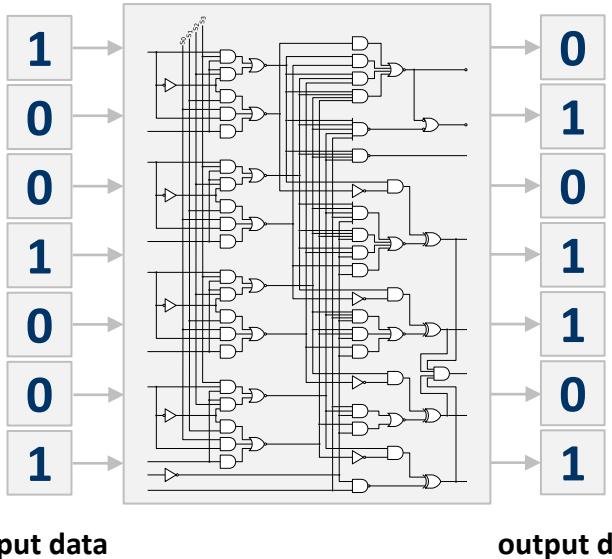
with enough H and T gates, we progressively cover all the surface of the Bloch sphere



\* source: Efficient decomposition methods for controlled- $R_n$  using a single ancillary qubit by Taewan Kim and Byung-Soo Choi, 2017 (7 pages)

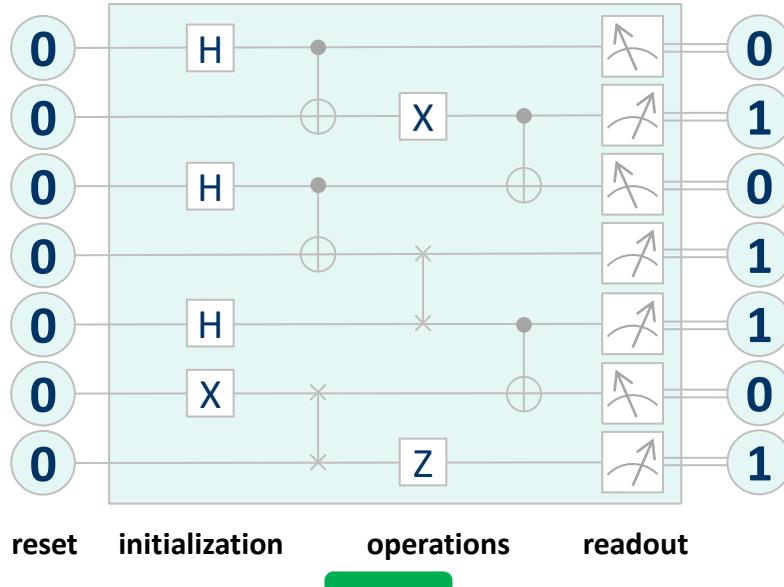
# inputs and outputs

classical gates



space and time  
circulating bits  
static gates

quantum gates



time  
fixed qubits (\*)  
static controlled gates

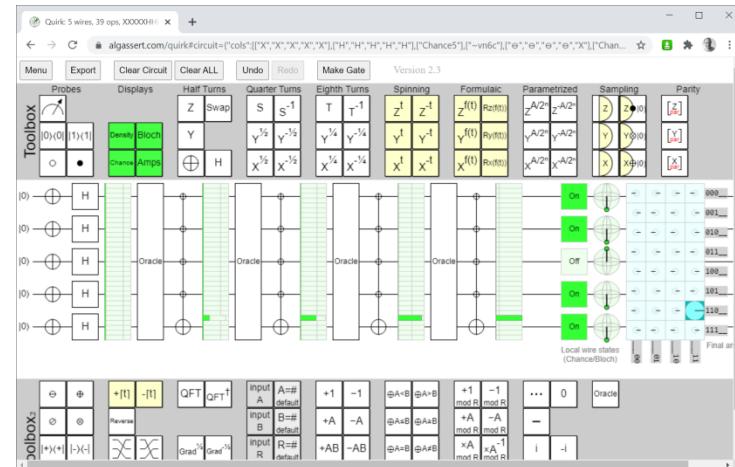
(\*) qubits are fixed in space for cold atoms, trapped ions, and electron-based, but not with photons which are flying qubits.

# testing qubits with Quirk

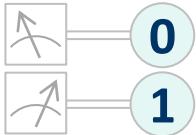
<https://algassert.com/quirk>

by Craig Gidney

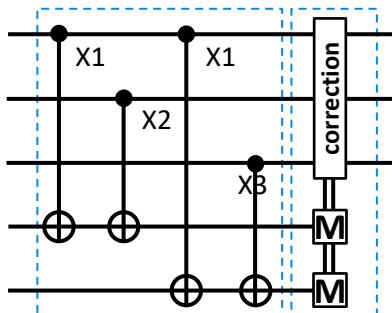
The screenshot shows the Quirk Quantum Circuit Simulator. At the top, there's a toolbar with icons for Probes, Export, Clear Circuit, Undo, Redo, Make Gate, and Version 2.3. Below the toolbar is a sidebar titled "Toolbox" containing various quantum gate icons. The main area is titled "Edit Circuit" and contains three buttons: "How to Use" (with a question mark icon), "Tutorial Video" (with a YouTube icon), and "Source Code" (with a GitHub icon). To the right of the circuit editor is a vertical sidebar titled "Example Circuits" listing various quantum algorithms and phenomena: Grover Search, Shor Period Finding, Bell Inequality Test (CHSH), Quantum Teleportation, Superdense Coding, Delayed Choice Eraser, Symmetry Breaking, Quantum Fourier Transform, Reversible Addition, and Magic State Distillation.



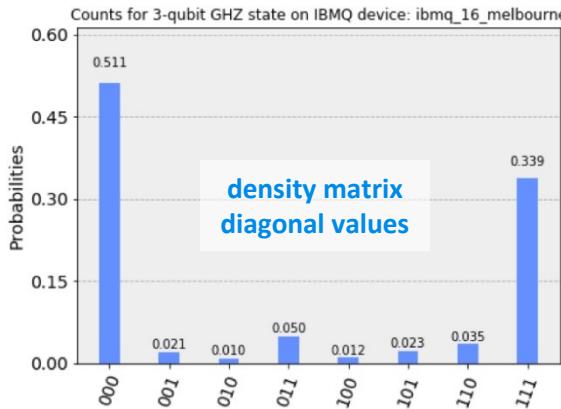
# various qubits measurement methods



qubits are measured at the end of computation on each qubit computational basis, several times and averaged: in the general case when the algorithm must generate a pure state.



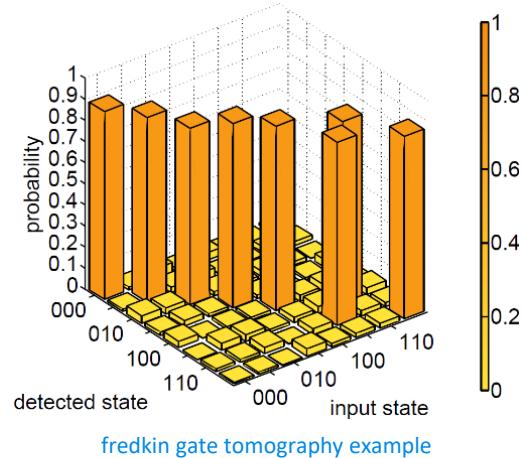
projective measurement on another basis (after  $X$ ,  $Y$ ,  $Z$ ,  $R_x$ ,  $R_y$  or  $R_z$  gates): such as with error correcting codes



an histogram with a  $2^N$  probability split of qubits registers computational basis => useful when the algorithm result combines several states, mostly in the middle of an algorithm for debugging purpose.

at the end of computing, we are supposed to have only one bar with a value close to 1, which is easier the measure with a simple measurement method.

this histogram is possible to compute only for a reasonable number of qubits because of its exponential quantum computing cost.



a quantum state tomography is a richer visualization with the full system density matrix => used to assess the quality of qubit gates, entanglement and measurement. more complicated to generate (more repeat projections/measurement). tomography is usually possible for a number of qubits  $\leq 6$ .

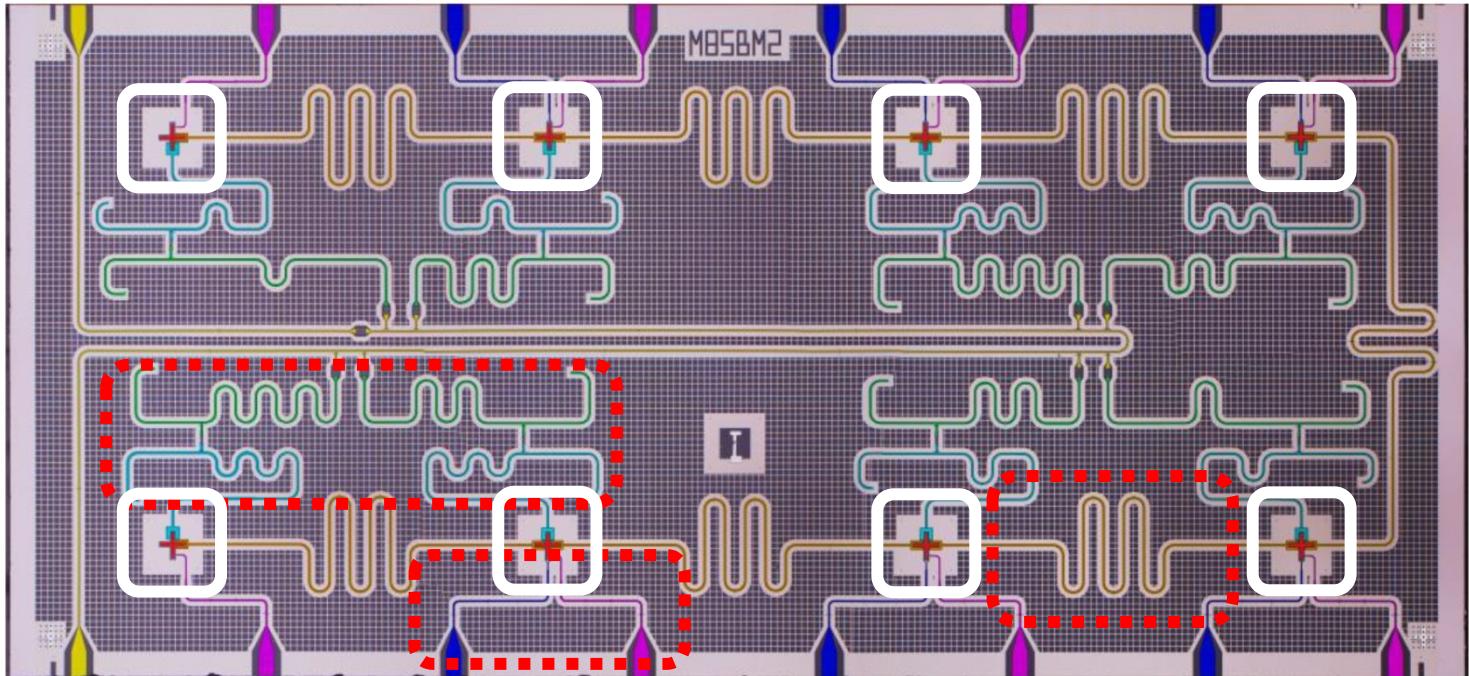
# physical qubit layout example

## qubits

superconducting loops  
with potential barrier  
using Josephson effect

## readout

analysis of the phase of  
a reflected micro-wave  
sent on the qubit by a  
resonator (cyan) and a  
Purcell filter (green)



**ETH** zürich

8 superconducting flux qubits

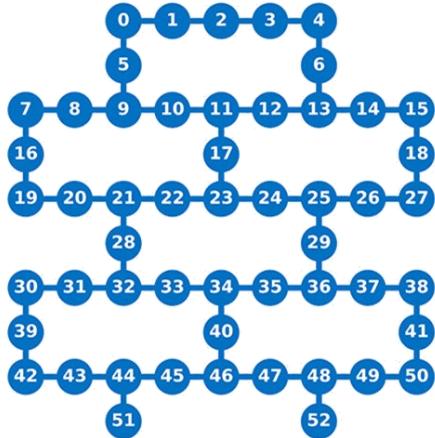
## gates

micro-waves between 5 and 10 GHz  
with different frequencies

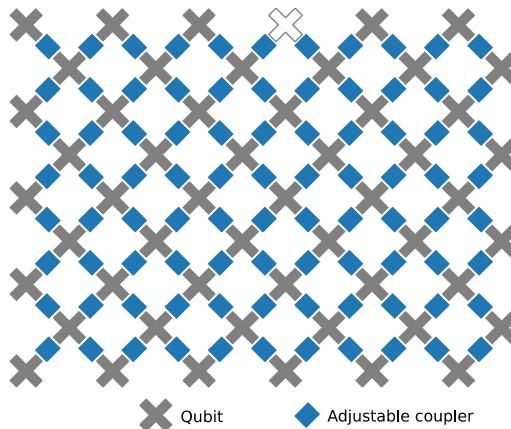
## coupling

with a resonator

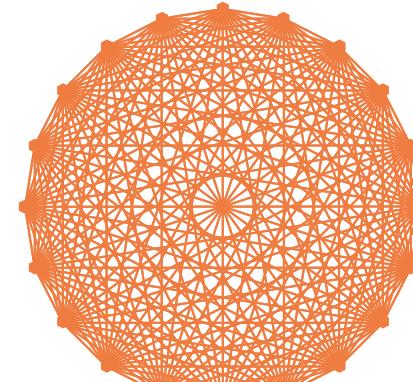
# qubits connectivity



**IBM**  
Rochester 53 qubits, October 2019  
65 qubits, October 2020, etc.



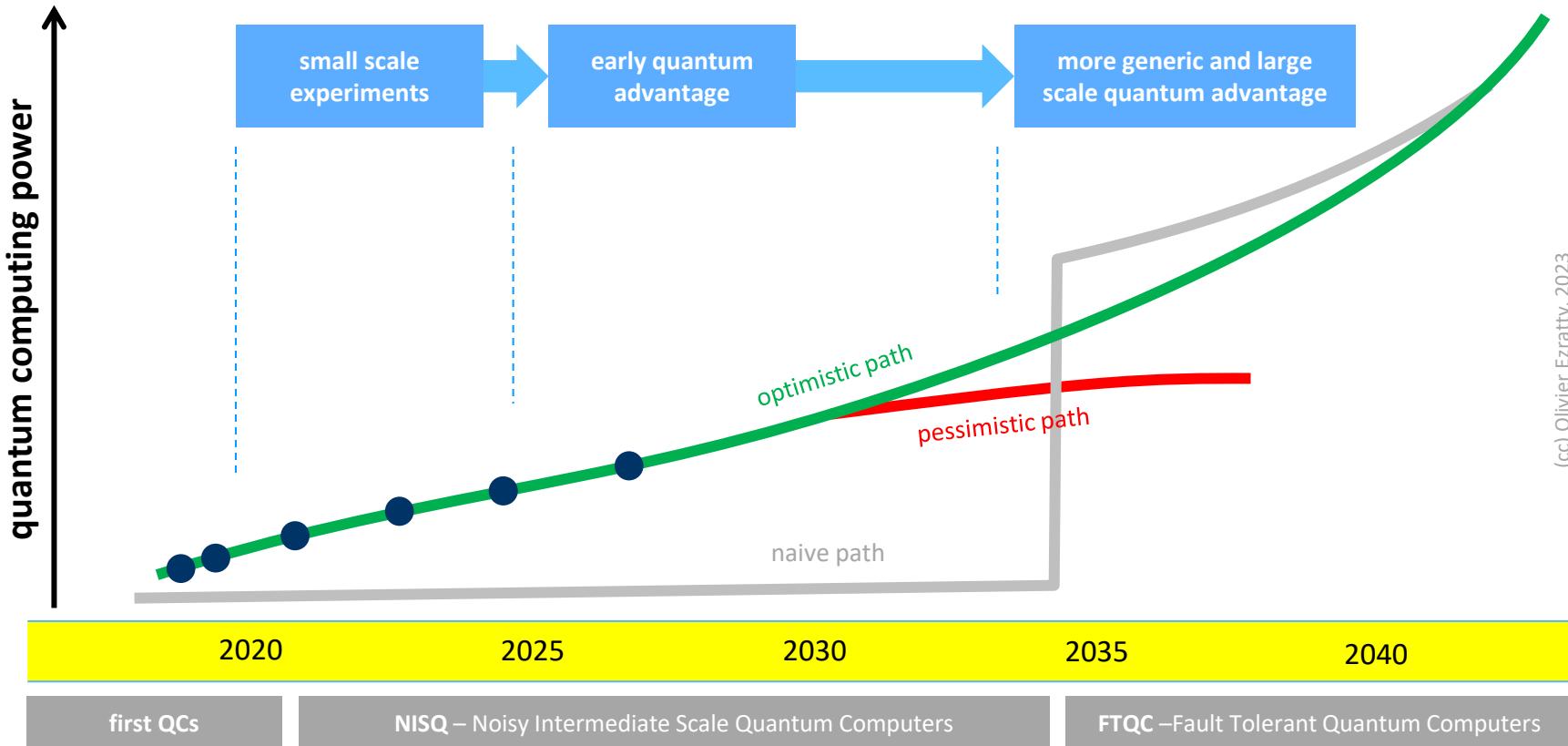
**Google**  
Sycamore 53 qubits, October 2019  
Sycamore 72 qubits, July 2022



**IonQ**  
11 qubits, 2018  
32 qubits, 2020

better

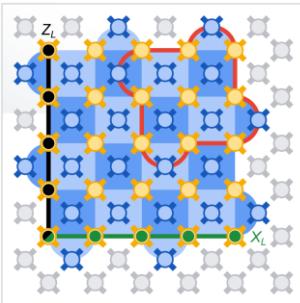
# when will « it » be there?



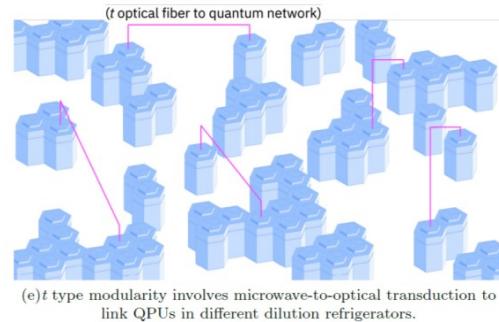
# key scientific and engineering challenges



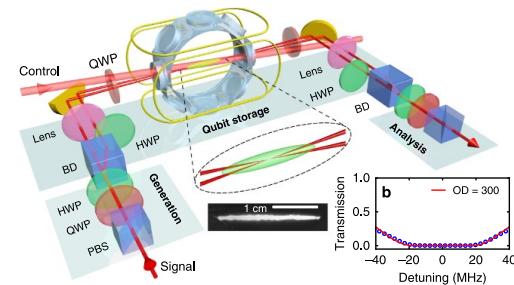
improve qubits fidelities



errors mitigation and correction



quantum interconnect



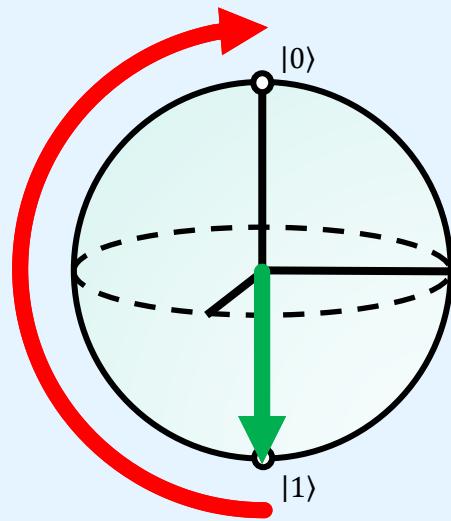
electronics, cabling and/or cryogeny scalability



energy consumption containment or advantage

data loading and quantum memory

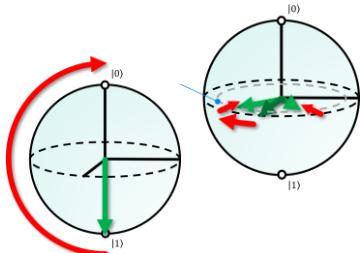
# improve qubit fidelities



# qubit errors

## error types

- initialization
- flip
- phase
- leakage
- readout



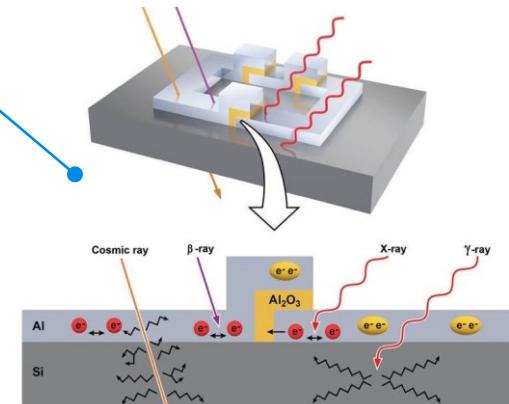
## error sources

- decoherence
- uncontrolled many body interactions
- calibration errors
- control electronics signals jitter
- ambient thermal noise
- ambient electric and magnetic noise
- radioactivity and cosmic rays
- vacuum quantum fluctuations
- gravity
- material defects

it accumulates with the number of quantum gates and qubits.

## errors reduction techniques

- improving qubits quality and isolation.
- quantum error suppression (at the hardware level).
- quantum error mitigation (NISQ).
- quantum error correction codes (QEC) which lengthens useful computing time (FTQC).



cosmic ray can generate errors in superconducting qubits

# qubit figures of merit

**numbers** qubits #  
connectivity: nearest neighbour 1x4, 1x2, 1x3, 1xN  
simultaneous gates: = or < # of qubits

**fidelities** single qubit fidelity: >99.9%  
two qubit fidelity: >99.9% in « n-nines »  
readout fidelity: >99% for QEC

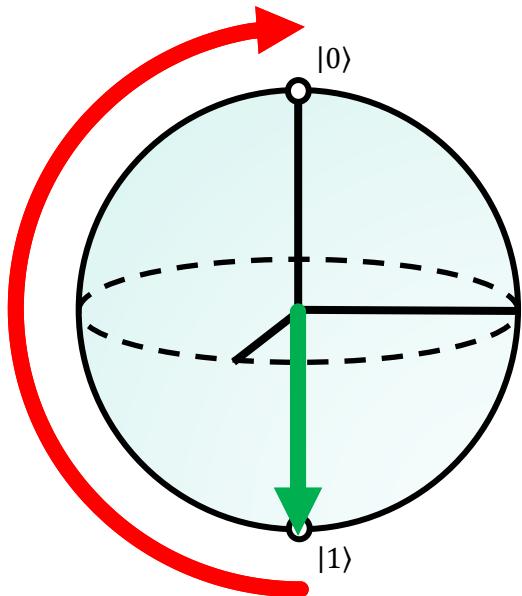
**times**  $T_1$ : relaxation time  
 $T_2$  and  $T_2^*$ : dephasing time  
1Q & 2Q gate time: conditions algo time  
readout time: conditions QEC efficiency



algorithm depth  
$$\frac{\min(T_1, T_2)}{\text{avg(gate time)}}$$

## **T<sub>1</sub> : flip error (relaxation, dampening)**

- qubit energy loss to the environment.
- spontaneous emission, quasiparticle tunneling, flux coupling, dielectric losses and control electronics imprecision.
- more important at qubit readout.
- time to decay from |1⟩ to |0⟩.
- decay of qubit density matrix diagonal.



## **T<sub>2</sub> - T<sub>2</sub><sup>\*</sup> : phase error (dephasing, decoherence time)**

- environment creates loss of phase memory.
- control electronics imprecision.
- important during computation.
- tied to number of consecutive gates.
- decay of qubit density matrix off-diagonal values.

**decay is a continuous process**

$$\frac{1}{T_2} = \frac{1}{2T_1} + \frac{1}{T_\phi}$$

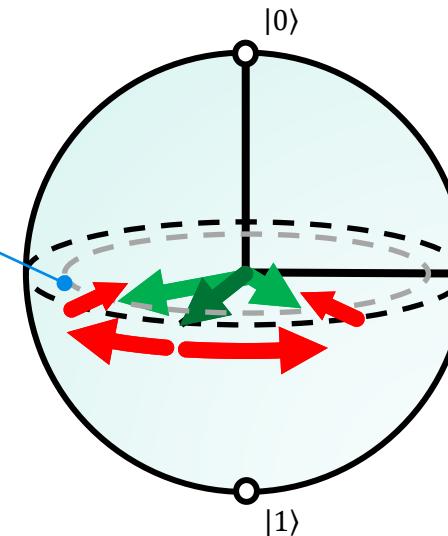
T<sub>φ</sub>: pure dephasing time

$$T_2^* \leq T_2 \leq 2T_1$$

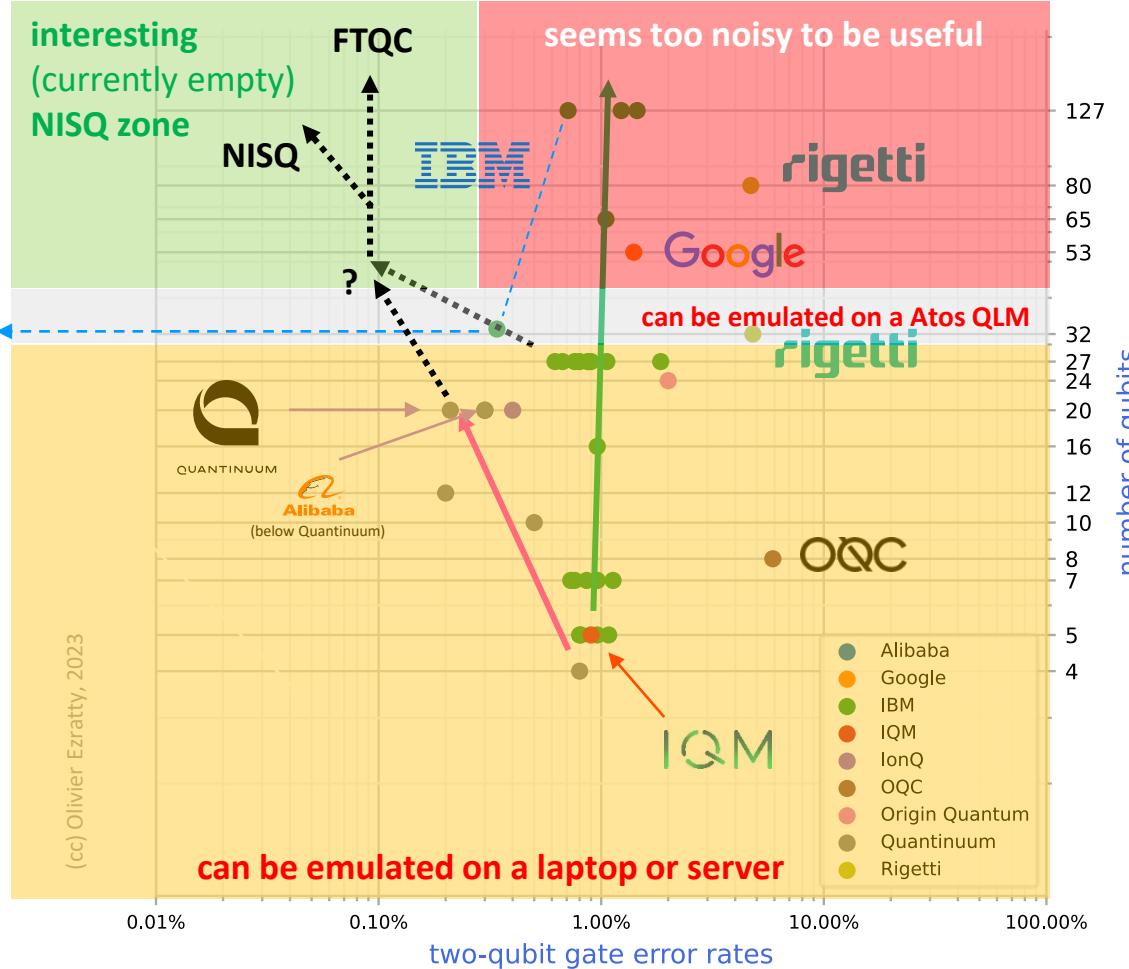
$$Q = \omega_q T_1$$

Q = quality factor

$\omega_q$  = qubit resonant frequency



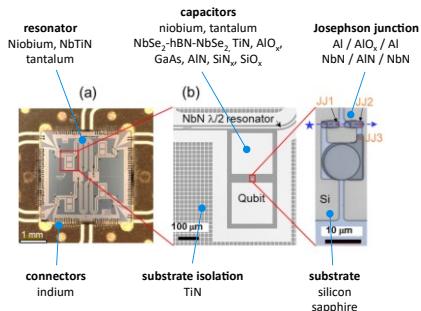
*IBM Sherbrooke (127Q) and Prague (33Q) use ECR gates, not CNOT.*



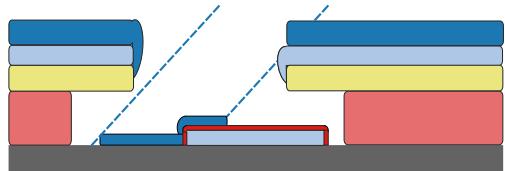
*here, emulation can be slower than QPUs*

*here, a classical emulator is faster, less costly and consumes less energy!*

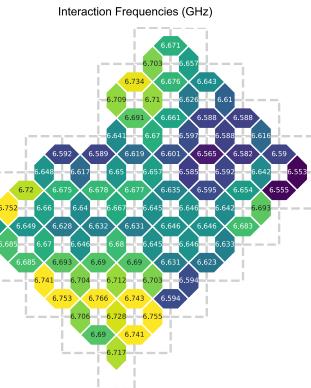
# how to improve qubit fidelities? \*



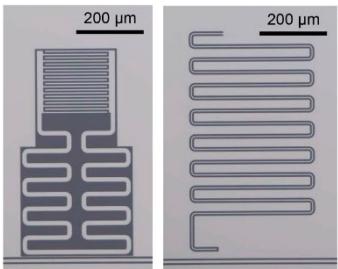
## materials



# manufacturing



## reduce crosstalk



### tune qubit parameters

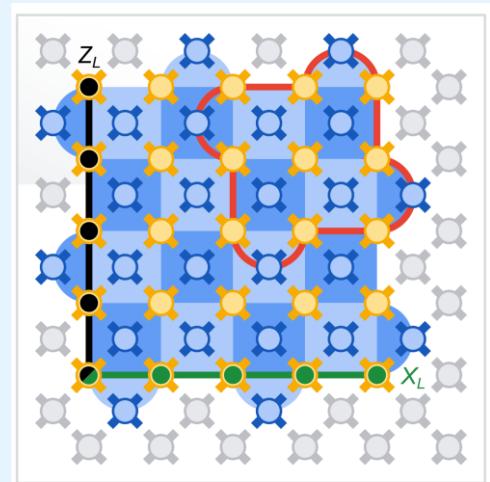
**use different primary gates**

\* using here the example of superconducting qubits



**improve control signals quality**

# quantum error mitigation and correction



# qubit errors impact on computing

$\approx$  algorithm number of quantum gates

	operations depth						
fidelities	10	100	1000	10000	1000000	100000000	1.27E+13
99%	90.44%	36.60%	0.00%	0.00%	0.00%	0.00%	0.00%
99.90%	99.00%	90.48%	36.77%	0.00%	0.00%	0.00%	0.00%
99.99%	99.90%	99.00%	90.48%	36.79%	0.00%	0.00%	0.00%
99.999999999999%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	88.08%

$10^{-14}$  error rates

22M physical qubits  
14238 logical qubits  
1568 physical/logical qubits  
physical qubit fidelities >99.9%

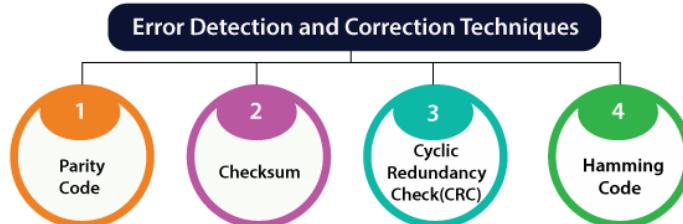
Shor on a RSA  
2048 bits key

# classical errors correction

**memory:**  $2.5 \times 10^{-11}$  bit per hour error rate,  
ECC memory for servers using Hamming code  
(1950)



**telecommunications:** CRC-32 and checksum  
correction, bit parity error detection : requires  
retransmission



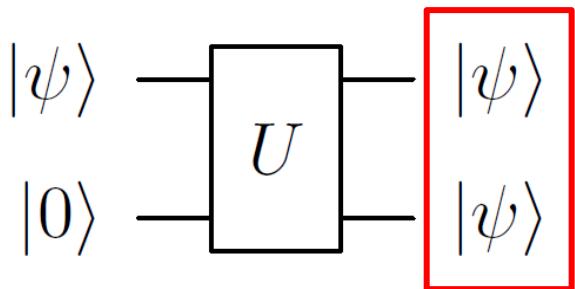
**storage:** RAID redundancy (Redundant Array of  
Inexpensive/Independent Disks)

- RAID 0 : data striped on multiple disks
- RAID 1 : data copied identically in multiple disks
- RAID 3 : data striping with parity bits on an additional disk
- RAID 5 : data and parity split over multiple disks

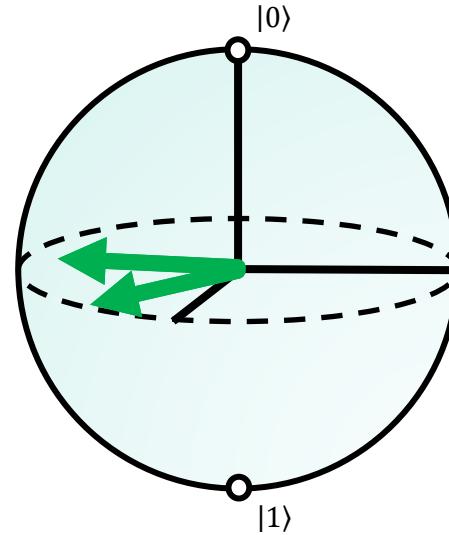
**MCA :** Intel Machine Check Architecture, detects  
and reports errors in microprocessor

fail-over systems with machine redundancies

# quantum error specifics

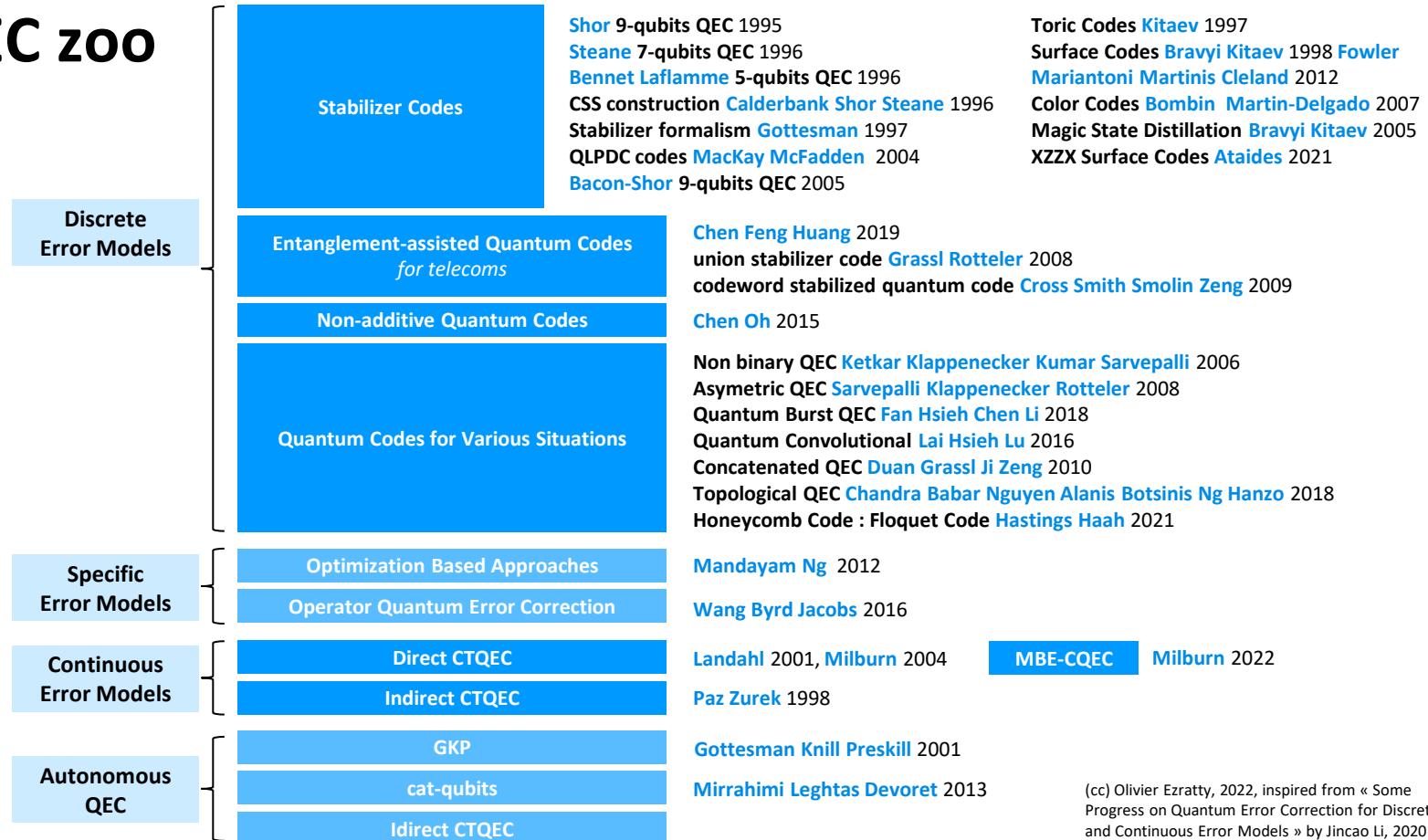


qubits cannot be independently replicated, with some measurement that would be performed on one replicated qubit.



we are correcting analog errors in multiple dimensions, not just a 0/1 error flip.

# QEC zoo



# QEC

VS

# QEM

quantum error correction



FTQC / LSQ

create longer lifetime logical qubits  
with apparent lower error rates  
physical/logical qubit ratios

surface codes, color codes, LDPC codes,  
Floquet codes, etc.

fault-tolerant error correction

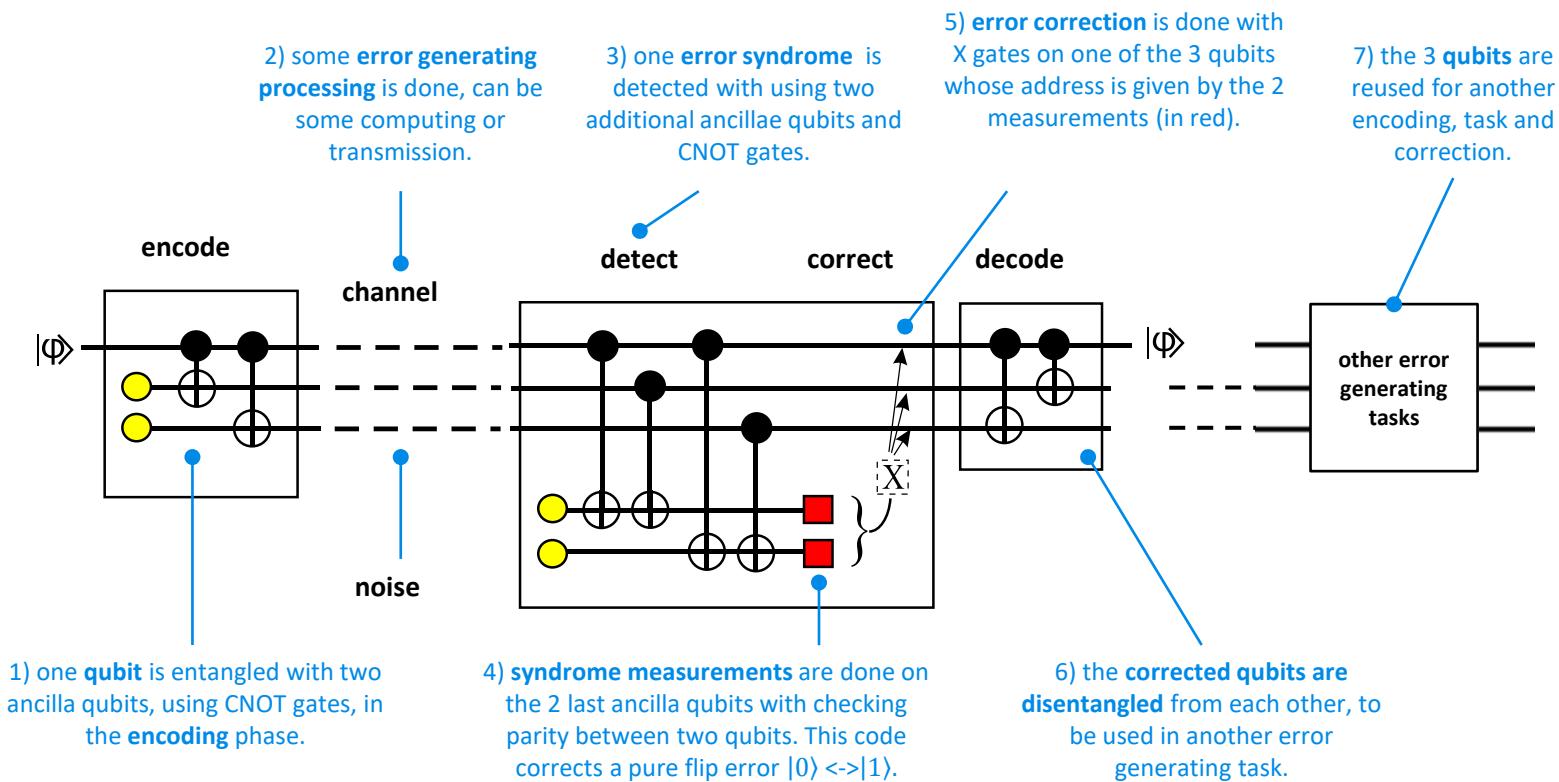
universal FTQC

quantum error mitigation



NISQ

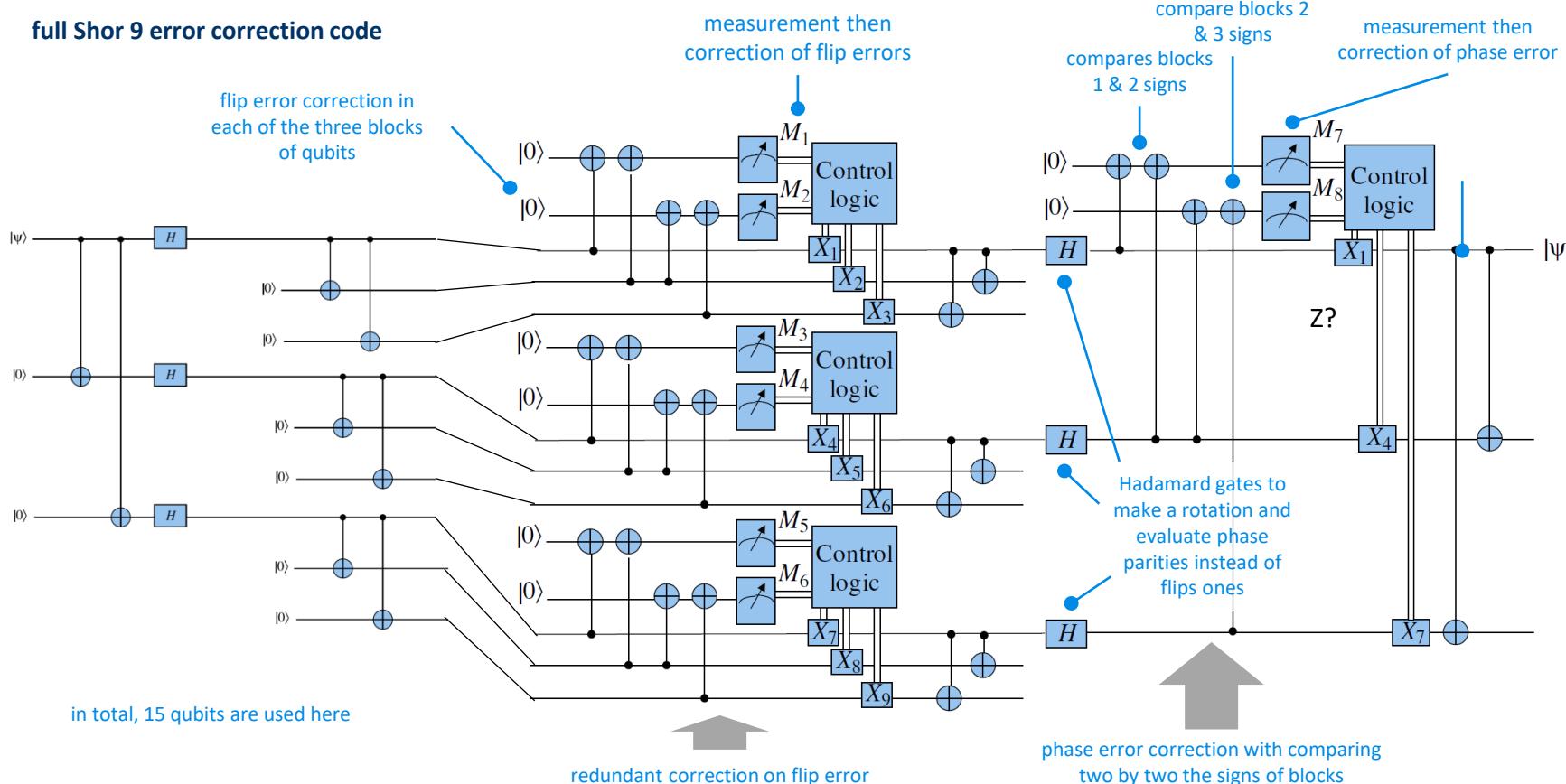
reduce errors with classical post-processing techniques, circuits modifications & several runs and results average, use machine learning techniques



adapted from « A Tutorial on Quantum Error Correction » by Andrew M. Steane, 2006

# Shor 9 error correction code

full Shor 9 error correction code



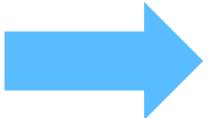
## physical qubit

error rates  $\approx 0.1\%$



## logical qubit

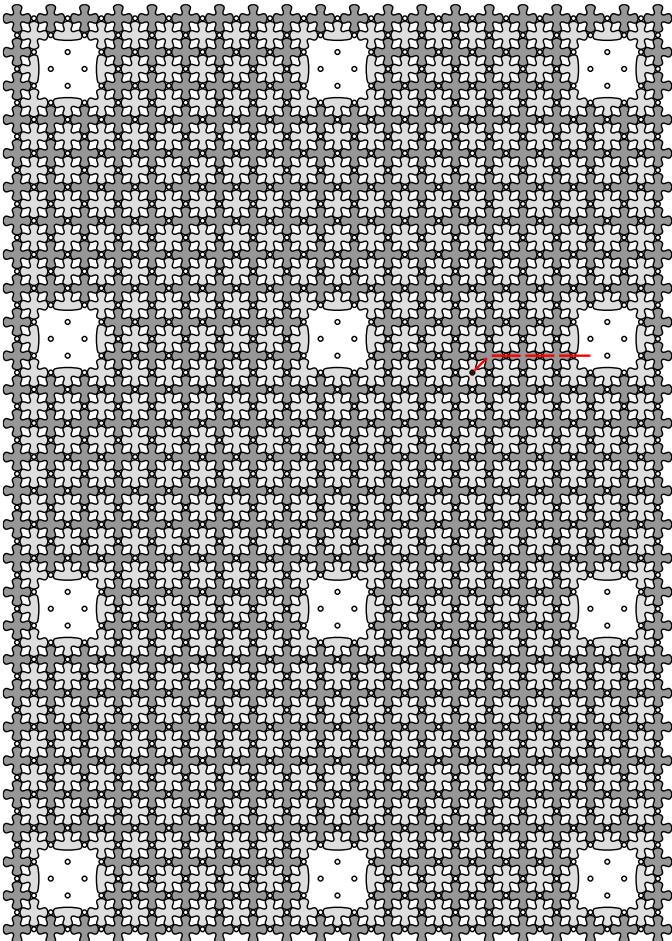
error rate  $< 10^{-8}$  to  $< 10^{-15}$



implementing error correction codes

made of thousands of physical qubits depending on physical qubit fidelities, connectivity, algorithm size, etc.

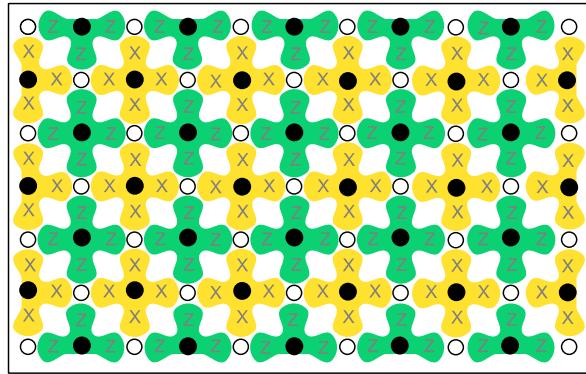
- + fault-tolerant features: transversal error correction to avoid errors spreading but works only with Clifford group gates, (costly) magic state distillation for T gates errors corrections, etc.



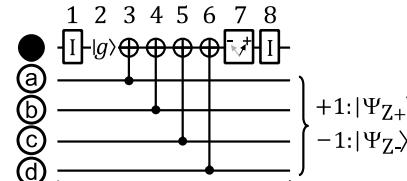
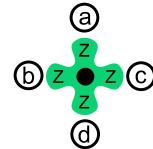
<https://arxiv.org/abs/1202.2639>

# surface code QEC

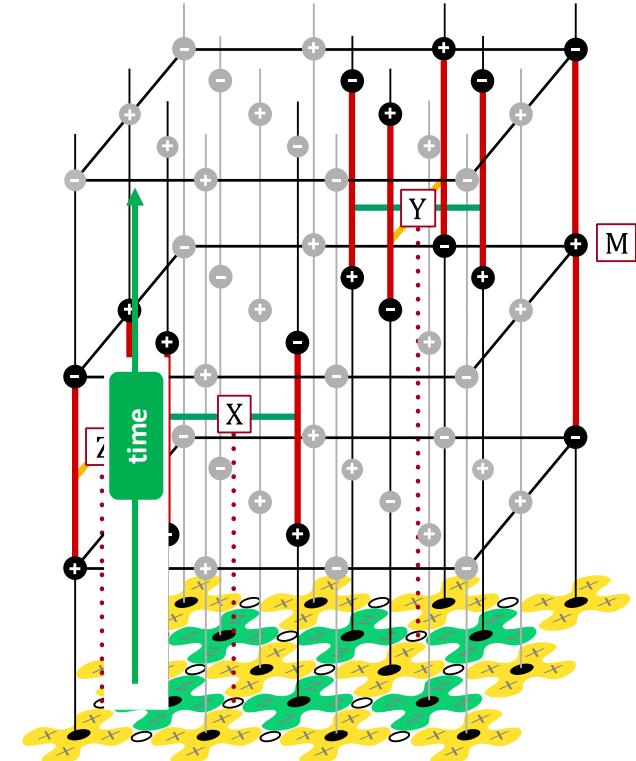
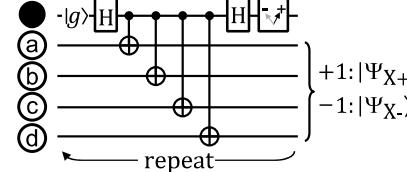
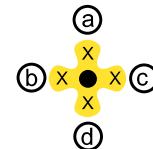
QEC adapted to 2D qubit architectures  
like with  
superconductors from  
Google



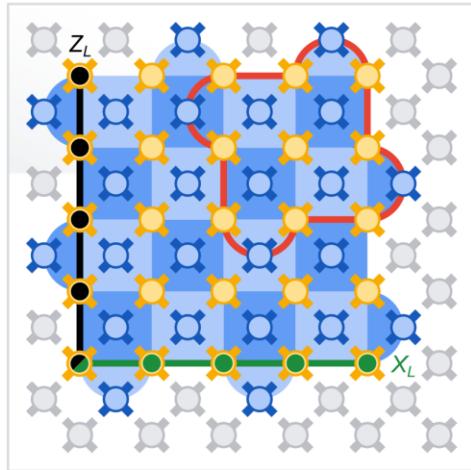
phase error  
correction



flip error  
correction



# Google logical qubit



**Sycamore 72-qubit processor  
distance-5 logical qubit**

Suppressing quantum errors by scaling a surface code logical qubit by Rajeev Acharya et al, Google AI, July 2022.

nature

Explore content ▾ About the journal ▾ Publish with us ▾ Subscribe

[nature](#) > [news](#) > article

NEWS | 22 February 2023

## Google's quantum computer hits key milestone by reducing errors

Researchers demonstrate for the first time that using more qubits can lower error rate of quantum calculations.

[Davide Castelvecchi](#)



logical qubit not yet better than underlying physical qubits  
expected to reach this with >100 qubits in 2023

# what is FTQC?

## QEC limitations

**error correction codes can introduce errors since they use error prone quantum gates and state measurements.**

**error correction codes do not correct all possible errors.**

## FTQC needs

**correct errors faster than new ones are introduced.**

**avoid creating more errors than corrected errors.**

**avoid spreading errors in an uncontrollable way to other qubits.**

**logical qubits and error correction reasonable space (# of physical qubits) and (quantum error codes computing) time overhead.**

## Fault-Tolerant Quantum Computation

Peter W. Shor  
AT&T Research  
Room 2D-149  
600 Mountain Ave.  
Murray Hill, NJ 07974, USA  
shor@research.att.com

<https://arxiv.org/abs/quant-ph/9605011>

May 1996

## FTQC solutions

**error-tolerant state preparation, quantum gates, measurement.**

**transversal error correction to avoid errors spreading but works only with Clifford group gates.**

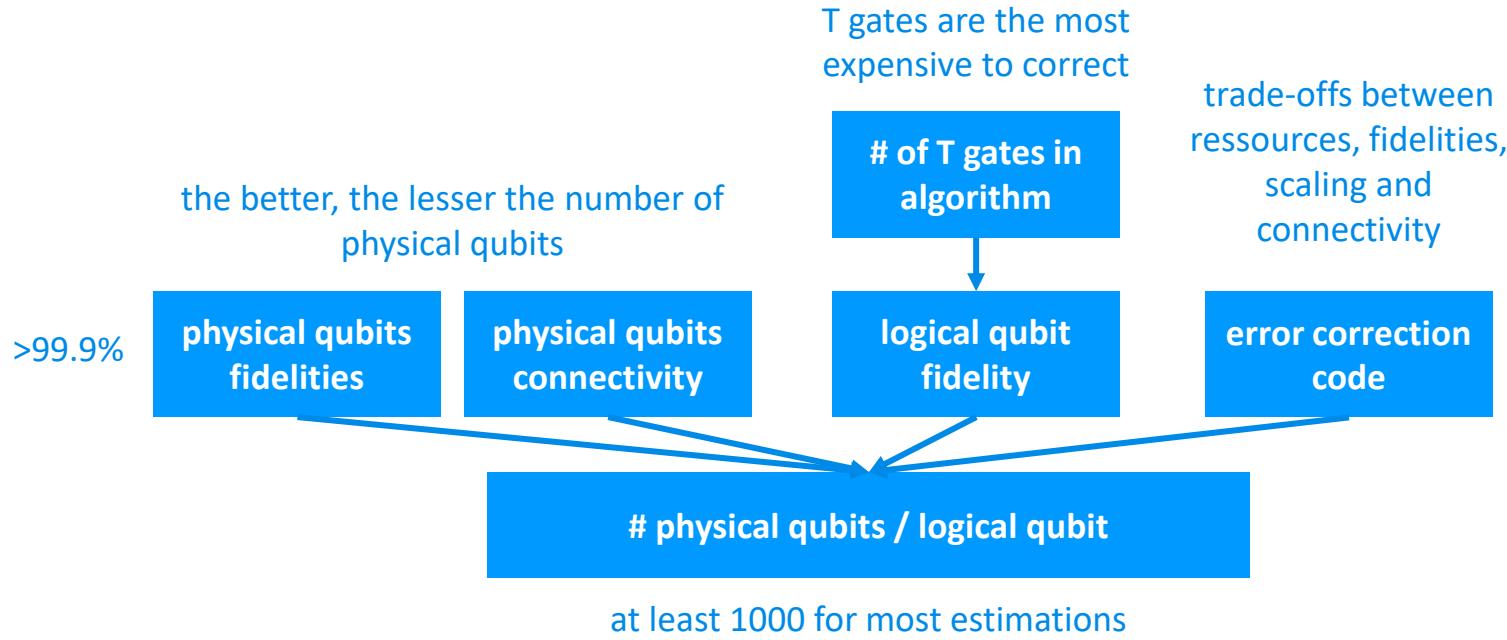
**(costly) magic state distillation for T gates errors corrections.**

**Fujitsu proposal to use analog phase gates.**

**some qubits directly made for FTQC**

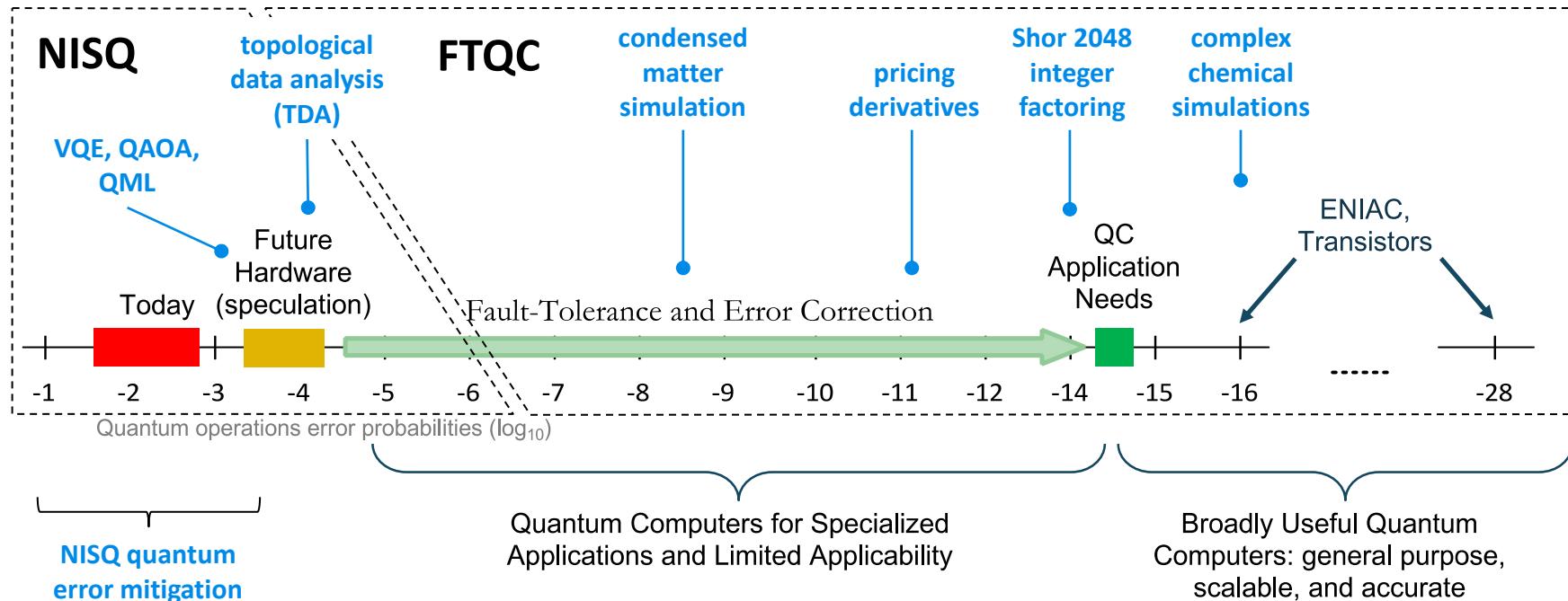
**cat-qubits and topological qubits**

# # physical qubits per logical qubits?



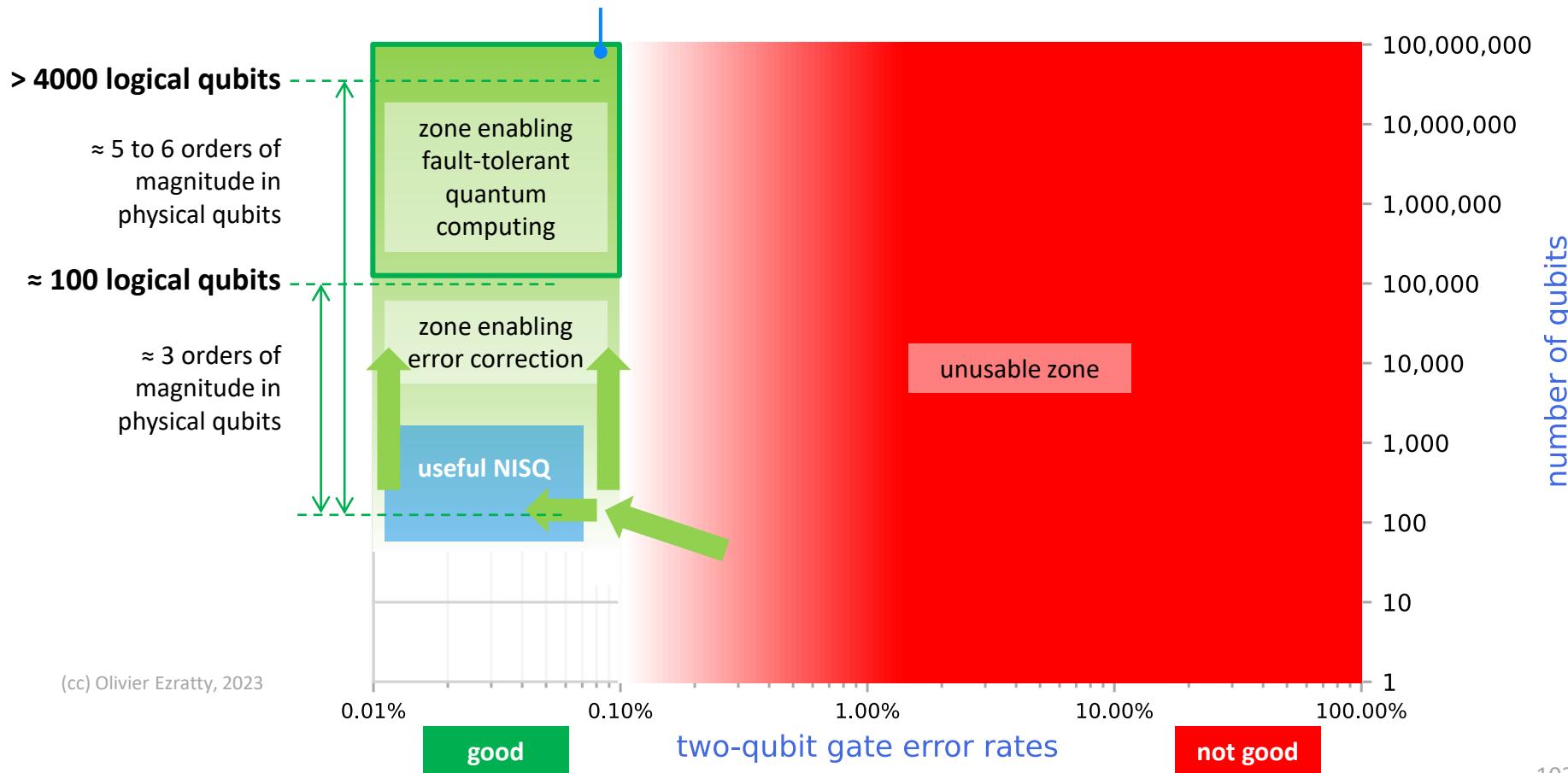
« whatever comes out of these gates, if we stay together we survive »

# from NISQ to FTQC



source: How about quantum computing? by Bert de Jong, DoE Berkeley Labs, June 2019 (47 slides) + Olivier Ezratty additions.

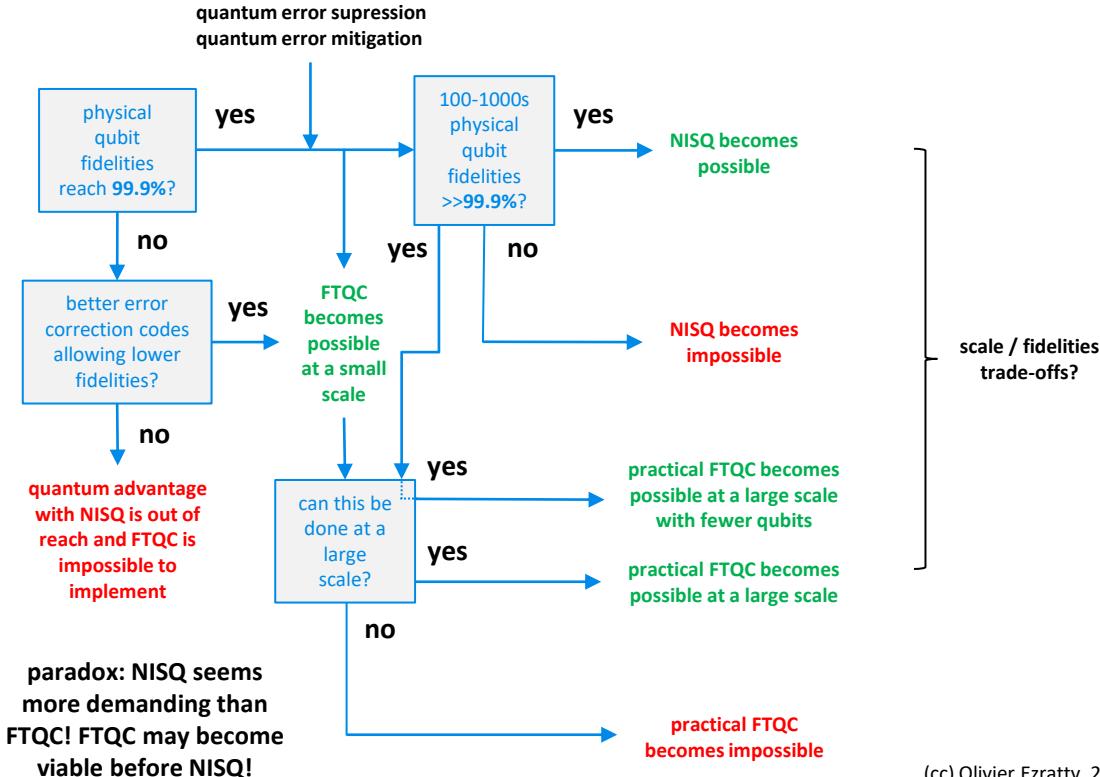
needed for chemical simulations, financial portfolio optimizations, break RSA 2048 keys



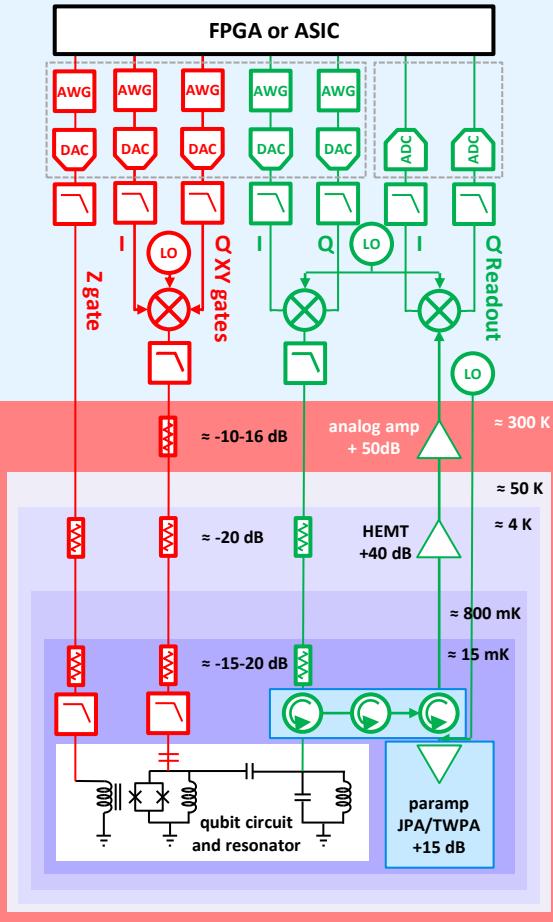
# NISQ vs FTQC

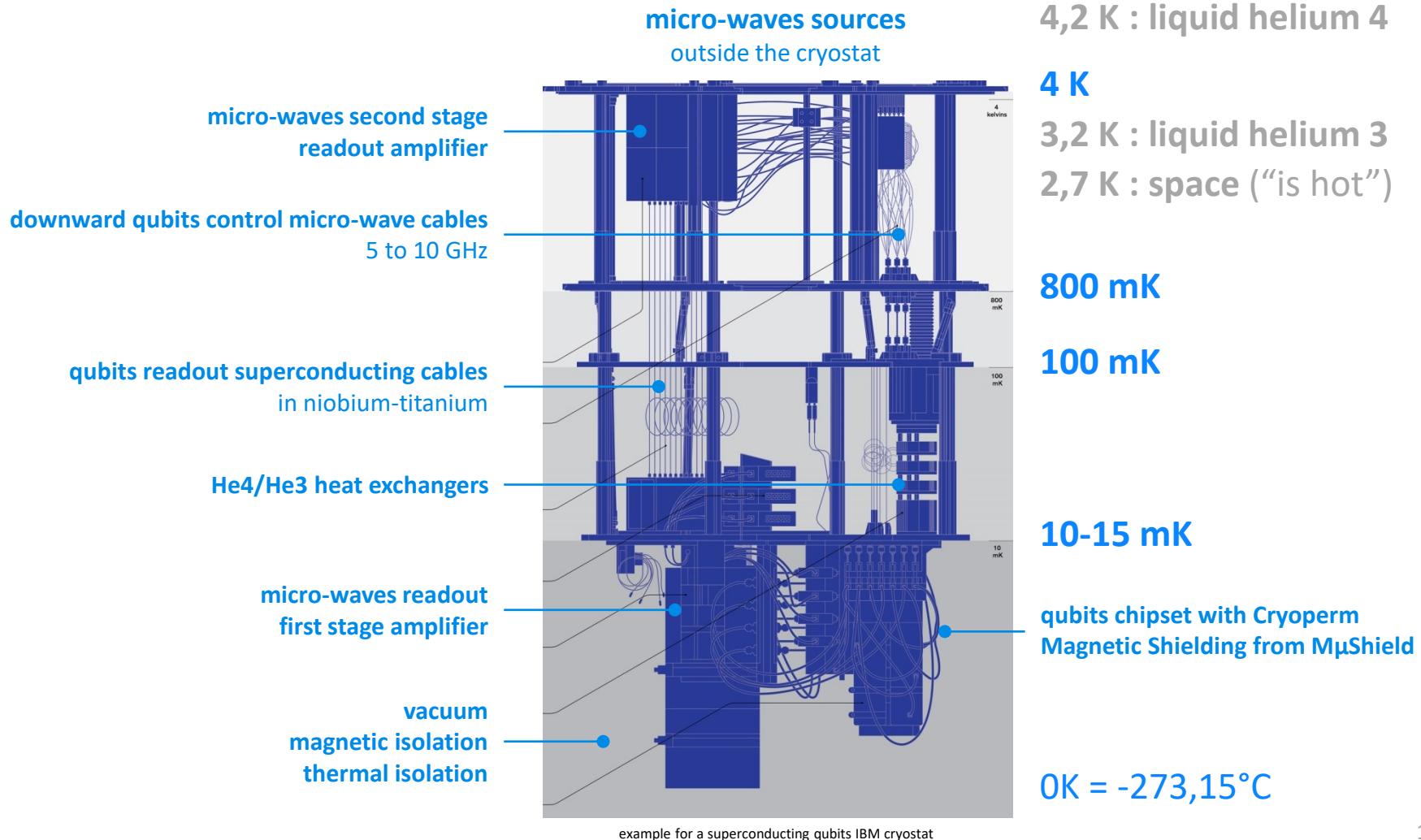
	NISQ	FTQC
physical qubits numbers	50-1000s	9000-millions
algorithmic qubit error rates $\epsilon$	$10^{-3} \leq \epsilon \leq 10^{-7}$	$10^{-5} \leq \epsilon \leq 10^{-15}$
required physical qubit fidelities	99.9% to 99.99999%	$\approx$ 99.9%
errors processing techniques	quantum error suppression	
	quantum error mitigation	quantum error correction
algorithms	VQE, QAOA, QML	Yes
	oracle based search	No
	QFT based	No Yes (HHL, Shor, ...)
qubit challenges	average number of create very high fidelity qubits	very large set of entangled qubits with good fidelities
other challenges	error mitigation scaling	quantum memory / qRAM error correction overhead energetics

# NISQ vs FTQC possible timelines



# enabling technologies cooling, electronics, cabling





# details from a 15 mK cryostat



pulse tube,  
first stage cooling with  
helium 4 gas down to  
2,8K, using an outside  
compressor, usually  
from CryoMech



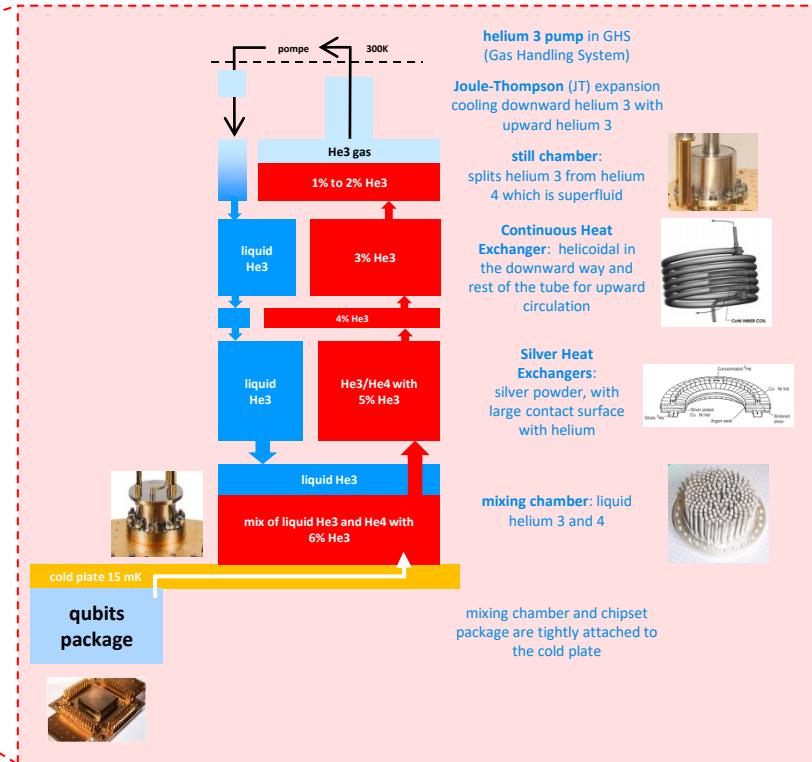
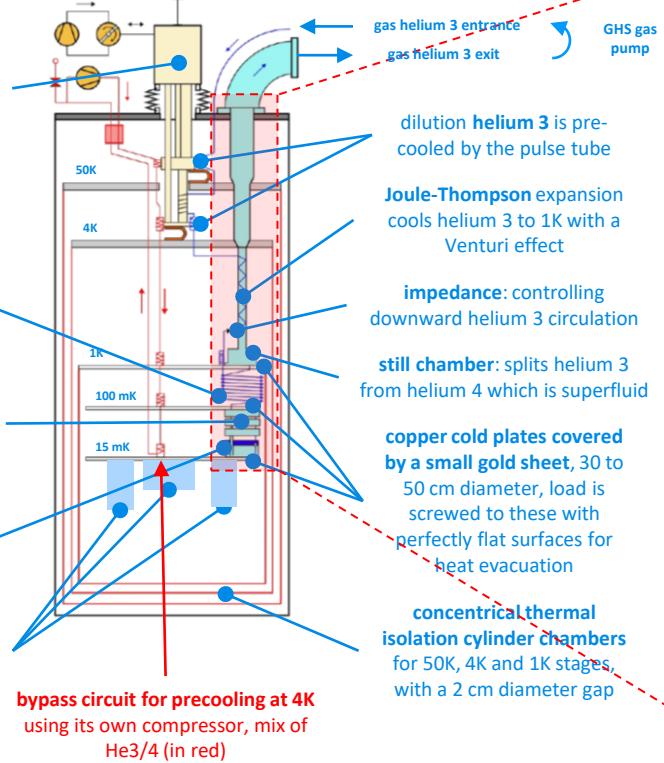
heat  
exchanger



discrete exchangers  
silver powder



dilution chamber  
liquid helium 3 & 4  
  
load  
qubits, attenuators,  
filters, cables and  
amplifiers

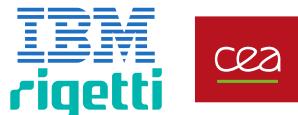


(cc) Olivier Ezratty, 2021

## dilutions and systems



°**BLUEFORS**



**FORMFACTOR™**

**seeqc**



**OXFORD INSTRUMENTS**

**Microsoft**  
**D-Wave**  
The Quantum Computing Company™



**CryoConcept**

**NEEL institut** **LPENS**  
LABORATOIRE DE PHYSIQUE  
DE L'ÉCOLE NORMALE SUPÉRIEURE



**Leiden Cryogenics**  
Leader in Low Temperature Techniques

**IBM**



**Maybell**

**DARPA**



## cabling and connectors



**COAX CO., LTD.**



**Delft Circuits**  
Hardware for quantum engineers



**Radiall**



**ATEM**  
CUSTOMIZED CONNECTIVITY

(cc) Olivier Ezratty, 2022

## pulse tubes and compressors



**CRYOMECH**



**Sumitomo**  
(SHI) Cryogenics of America, Inc.

# available cooling power

**°BLUEFORS**

 FORMFACTOR™

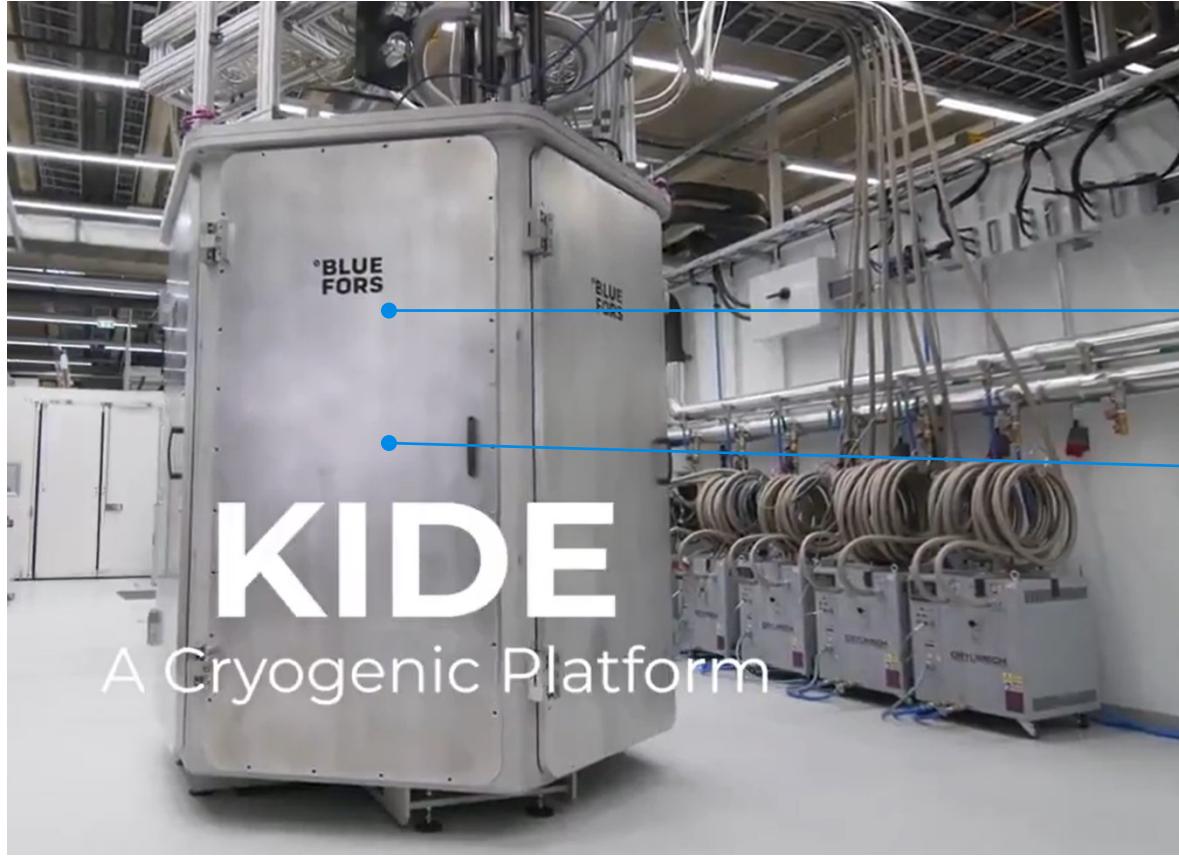
 OXFORD INSTRUMENTS

 CryoConcept  
an Air Liquide affiliate

 Leiden Cryogenics  
Leader in Low Temperature Techniques

	cryostat	pulse tubes	minimum temperature	20mK stage	100mK stage	MC cold plate
<b>°BLUEFORS</b>	LD250	1	10 mK	12 µW	250 µW	30 à 50 cm
	XLD400	2	8 mK	14 µW	450 µW	30 à 50 cm
	XLD1000	2	8 mK	34 µW	1000 µW	30 à 50 cm
 FORMFACTOR™	JDry-500-QPro	1	7 mK	14 µW	500 µW	50 cm
 OXFORD INSTRUMENTS	TritonXL	2	5 mK	25 µW	1000 µW	43 cm
	TritonXL-Q	2 ou 4	7 mK	25 µW	850 µW	50 cm
	Proteox	1	10 mK	>25 µW	500 µW	36 cm
 CryoConcept an Air Liquide affiliate	HD200	1	10 mK	11 µW	350 µW	30 à 50 cm
	HD400	1	10 mK	10 µW	400 µW	30 à 50 cm
Leiden Cryogenics Leader in Low Temperature Techniques	CF2400 Maglev	2	4 mK	? µW	2000 µW	49 cm
	CF1400 Maglev	2	8 mK	? µW	1000 µW	49 cm

# Bluefors KIDE



9 pulse tubes and compressors

3 dilutions

about 110 kWh

# energetic related hardware engineering challenges and trade-offs *the superconducting qubit case*

## optimize RT electronics energetics

# RT or cryogenics electronics?

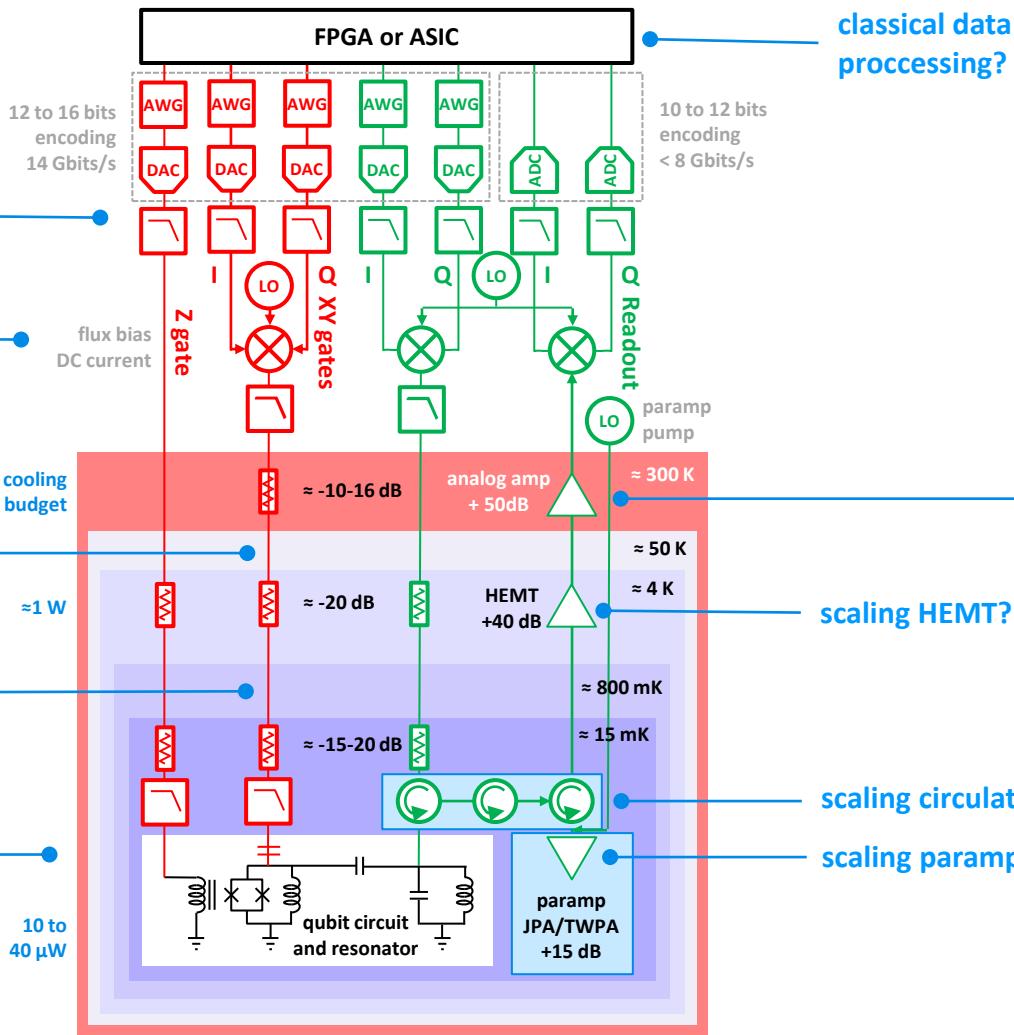
## scaling cabling, att & filters?

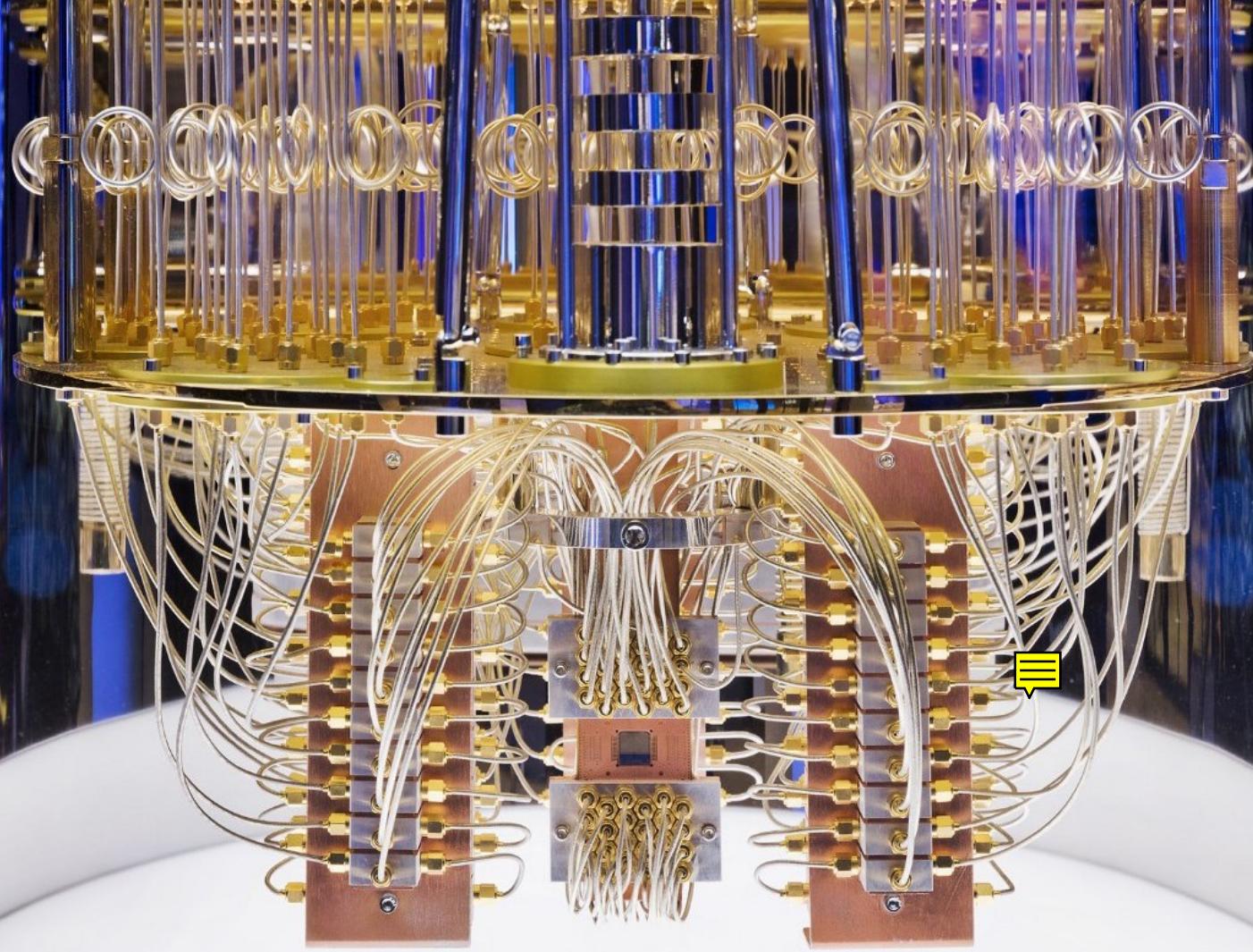
**control signals multiplexing?**

## cryo-CMOS or SFQ electronics

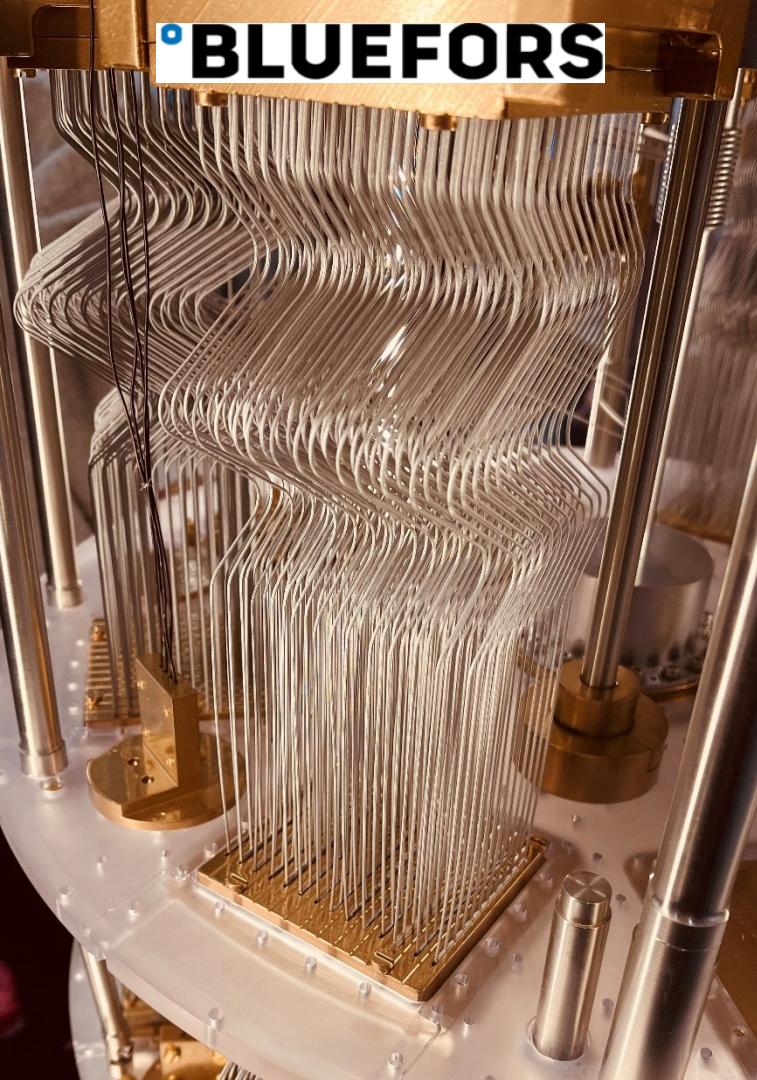
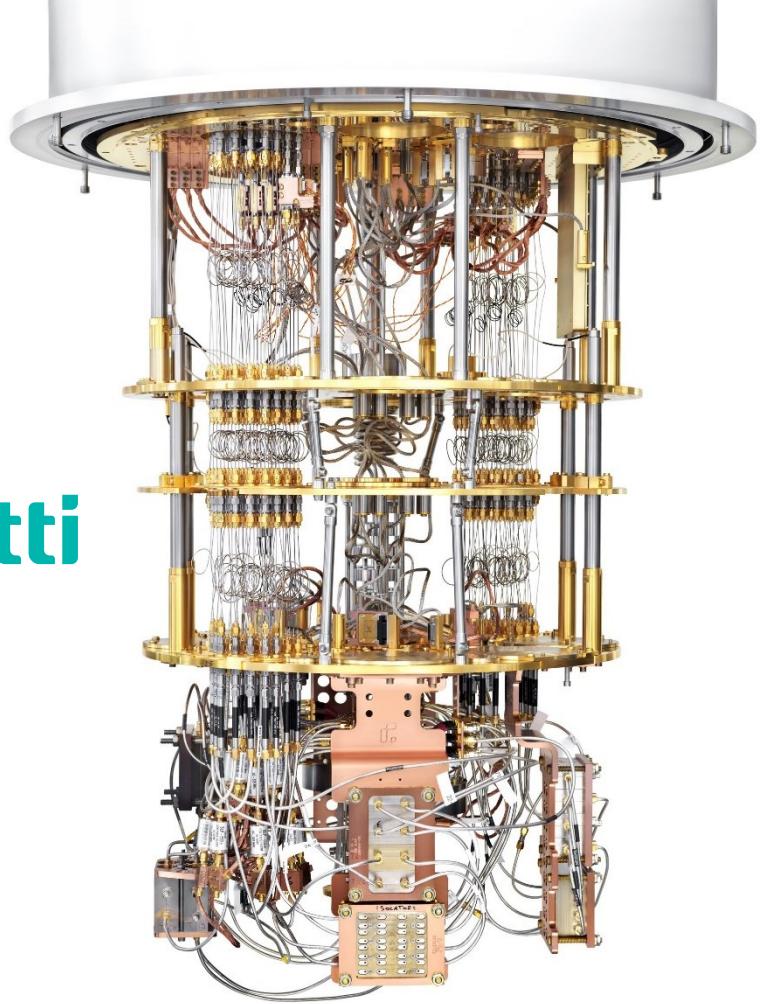
at which temperature?

scaling cryogenics? —



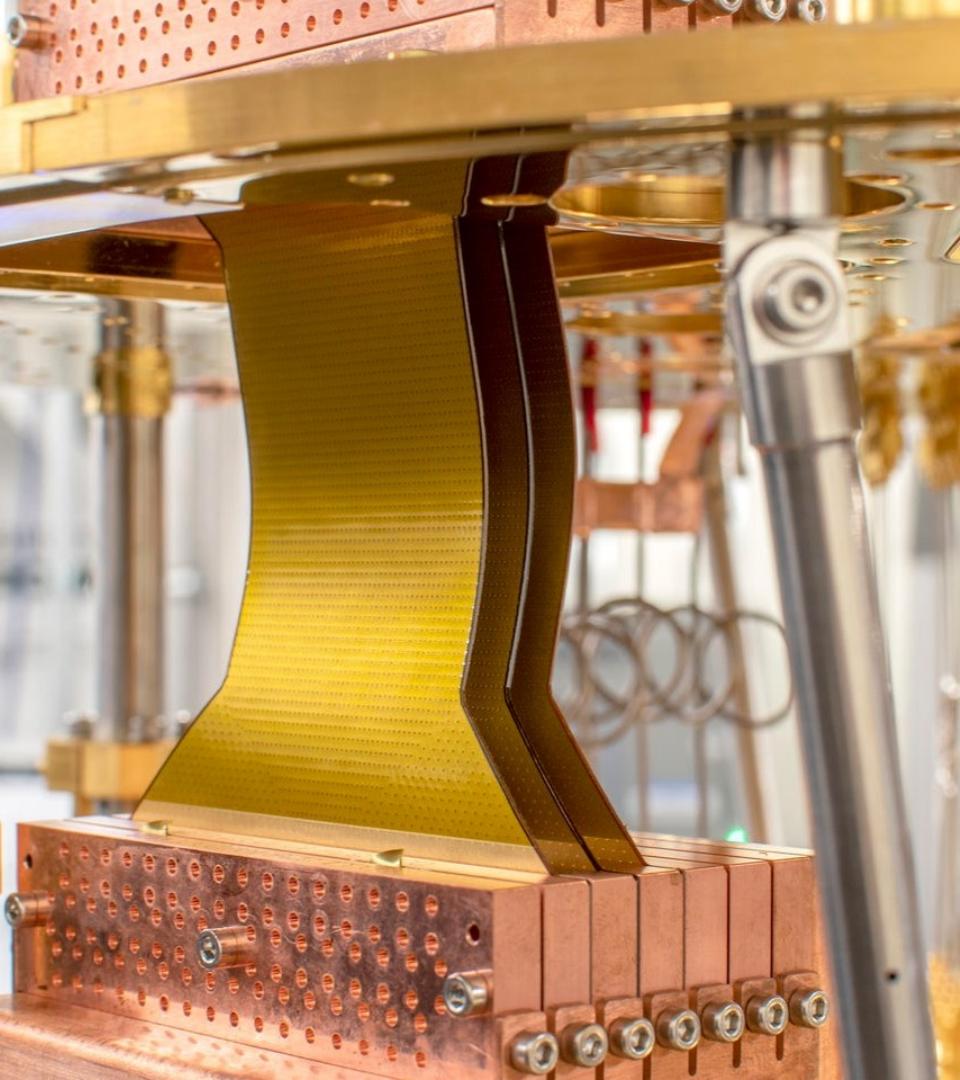


**rigetti**





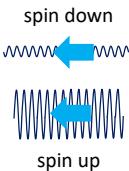
**Osprey**  
novembre 2022  
433 qubits





## HorseRidge II 2021

**drive:** arbitrary waveform microwave pulse generation  
 => creates single qubit gates  $R_x$  and  $R_y$   
 pulse phase => rotation axis X or Y  
 amplitude + duration => rotation angle



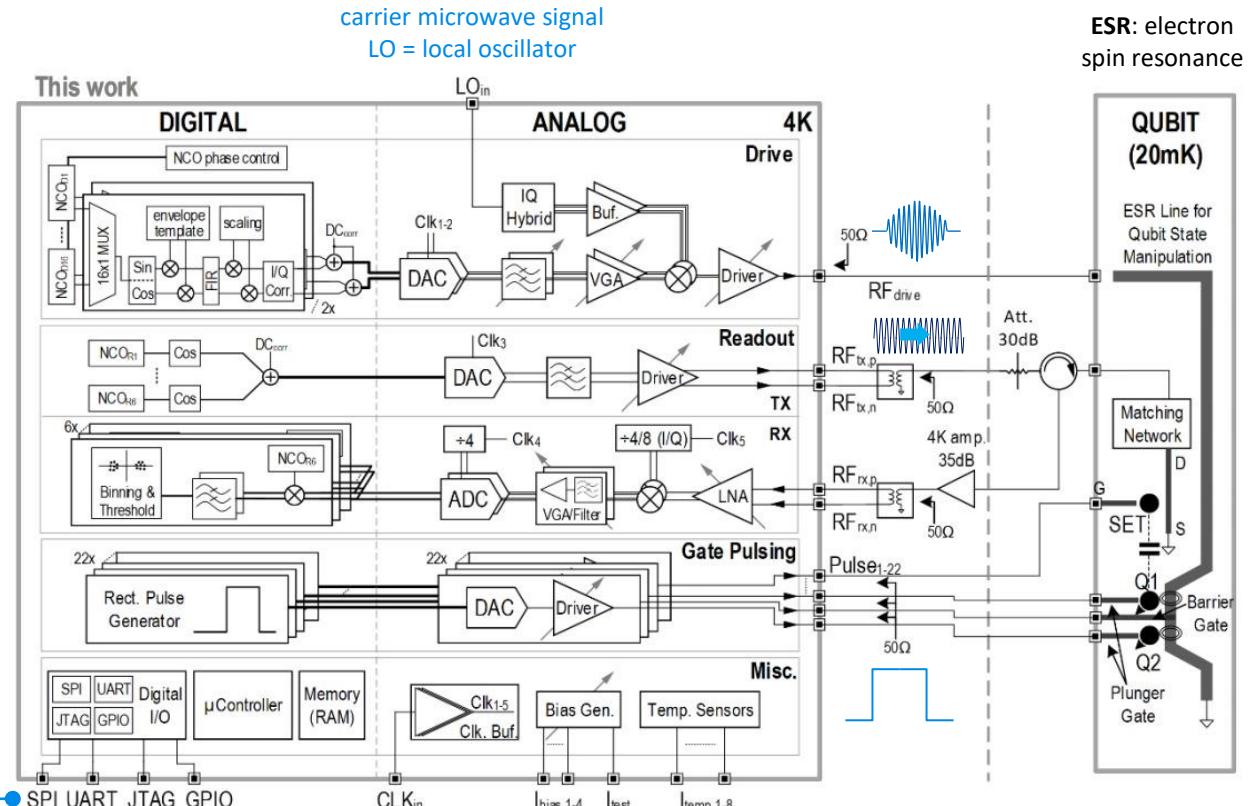
**readout:** multitone microwave pulse

reflected signal phase/amplitude analysis =>  
 spin up or down readout

**gate pulsing:** square pulse generation  
 for qubit barrier and plunger gates  
 => creates two-qubits gates

**microcontroller:** manages  
 firmware instruction set

serial communication  
 with outside the cryostat



SPI: Serial Peripheral Interface  
 UART: Universal asynchronous receiver-transmitter  
 JTAG: Joint Test Action Group (for debugging)

GPIO: General-purpose input/output  
 CLK: clock in

DAC: digital to analog converter  
 ADC: analog to digital converter

ESR: electron spin resonance

energetics

#QEI  
the quantum energy initiative

# QC energetic costs is an open question!

RESEARCH-ARTICLE



## Energy Cost of Quantum Circuit Optimisation: Predicting That Optimising Shor's Algorithm Circuit Uses 1 GWh

Authors: [Alexandru Paler](#), [Robert Basmadjian](#) [Authors Info & Claims](#)

ACM Transactions on Quantum Computing, Volume 3, Issue 1 • March 2022 • Article No.: 3, pp

<https://dl.acm.org/doi/10.1145/3490172>

← energy hog?

or energy saver?



Is quantum computing green? An estimate for an energy-efficiency quantum advantage

Daniel Jaschke<sup>1,2,3</sup> and Simone Montangero<sup>1,2,3</sup>

<sup>1</sup>*Institute for Complex Quantum Systems, Ulm University, Albert-Einstein-Allee 11, 89069 Ulm, Germany*

<sup>2</sup>*Dipartimento di Fisica e Astronomia "G. Galilei" & Padua Quantum Technologies Research Center, Università degli Studi di Padova, Italy I-35131, Padova, Italy*

<sup>3</sup>*INFN, Sezione di Padova, via Marzolo 8, I-35131, Padova, Italy*

(Dated: May 25, 2022)

<https://arxiv.org/abs/2205.12092>



## the quantum energy initiative

[quantum-energy-initiative.org](https://quantum-energy-initiative.org)

295 community participants from 40 countries & 28 partners



Olivier Ezratty

Consultant and Author  
olivier@oezratty.net  
+33 6 67 37 92 41



Alexia Auffèves

CNRS Research Director  
MajuLab, Singapore  
alexia.auffeves@neel.cnrs.fr



Janine Splettstoesser

Professor  
Chalmers University  
janines@chalmers.se



Robert Whitney

Researcher  
CNRS LPMMC Grenoble  
robert.whitney@lpmmc.cnrs.fr

### questions

- is there a **quantum energy advantage** vs classical computing as quantum processors scale up?
- how to avoid **energetic dead-ends** on the road to LSQ?
- create a new **transversal line of research** and collaborative projects.
- create a worldwide **community** working on this matter associating research and industry.
- create **optimization methodologies, frameworks and benchmarks** for quantum technologies, enabling technologies and software engineering,

PRX QUANTUM  
*a Physical Review journal*

Highlights Recent Accepted Authors Referees Search About Scope Staff

Perspective Open Access

Quantum Technologies Need a Quantum Energy Initiative

Alexia Auffèves  
PRX Quantum 3, 020101 – Published 1 June 2022

### mission + goals

# Optimizing resource efficiencies for scalable full-stack quantum computers

Marco Fellous-Asiani,<sup>1, 2, \*</sup> Jing Hao Chai,<sup>2, 3</sup> Yvain Thonnart,<sup>4</sup> Hui Khoon Ng,<sup>5, 3, 6, †</sup> Robert S. Whitney,<sup>7, ‡</sup> and Alexia Auffèves<sup>2, 6, §</sup>

<sup>1</sup>*Centre for Quantum Optical Technologies, Centre of New Technologies, University of Warsaw, Banacha 2c, 02-097 Warsaw, Poland*

<sup>2</sup>*Université Grenoble Alpes, CNRS, Grenoble INP, Institut Néel, 38000 Grenoble, France*

<sup>3</sup>*Centre for Quantum Technologies, National University of Singapore, Singapore*

<sup>4</sup>*Université Grenoble Alpes, CEA-LIST, F-38000 Grenoble, France*

<sup>5</sup>*Yale-NUS College, Singapore*

<sup>6</sup>*MajuLab, International Joint Research Unit UMI 3654, CNRS, Université Côte d'Azur, Sorbonne Université,*

*National University of Singapore, Nanyang Technological University, Singapore*

<sup>7</sup>*Université Grenoble Alpes, CNRS, LPMMC, 38000 Grenoble, France.*

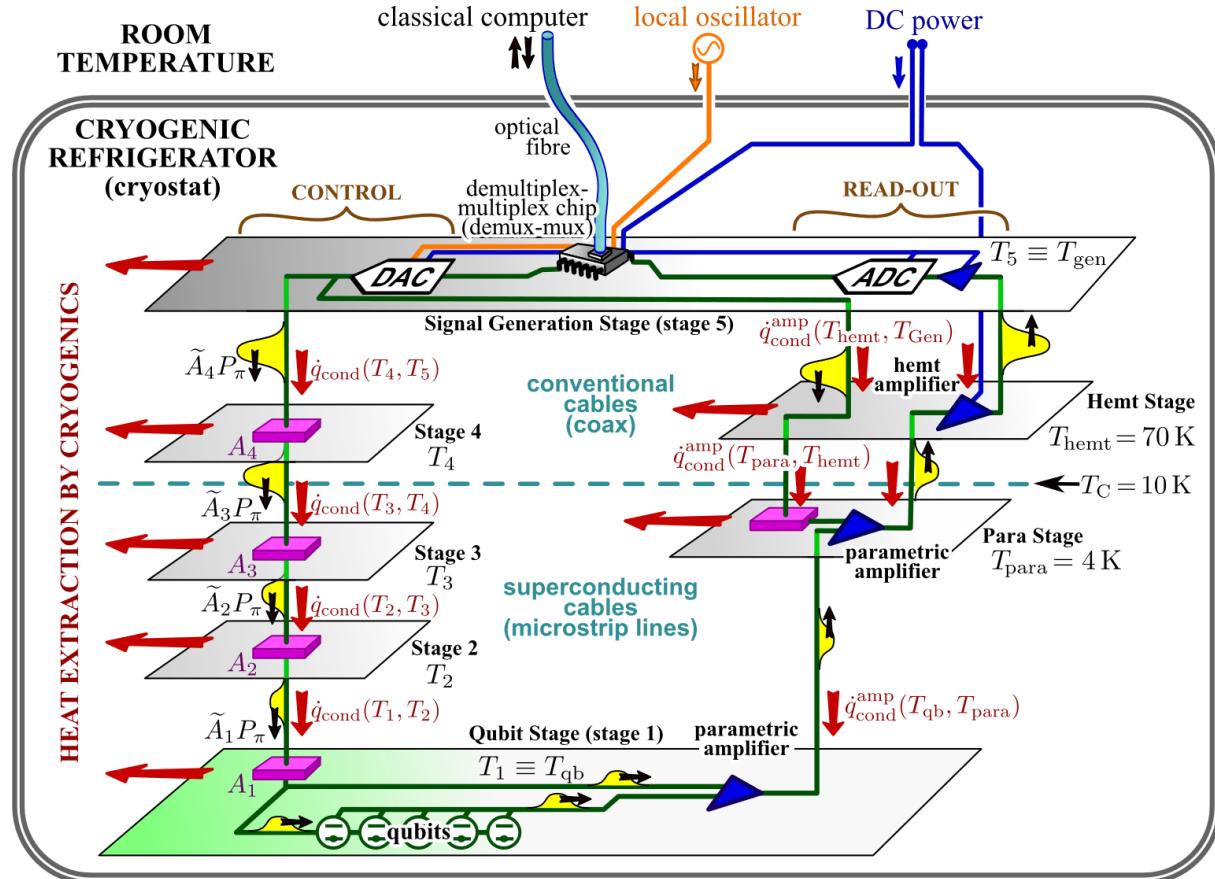


<https://arxiv.org/abs/2209.05469>

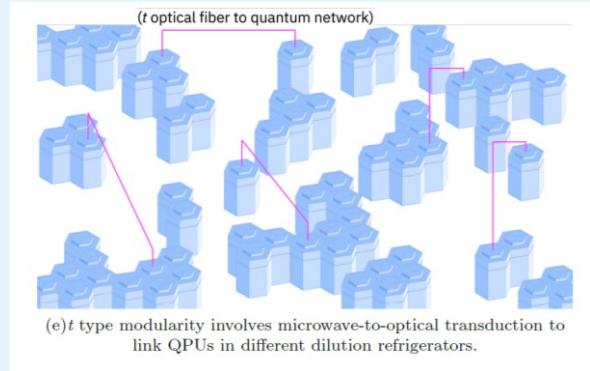
## early findings applying the MNR methodology in a particular example

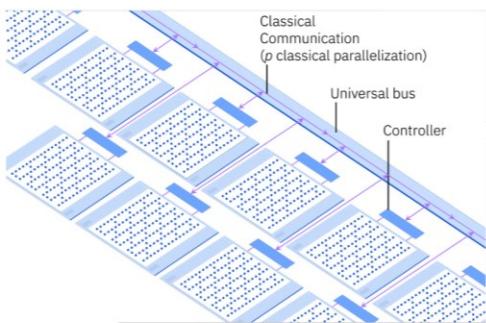
1. **energy advantage** may show up before **computing advantage**.
2. **x10 qubit fidelities => x100 energy savings**.
3. **quantum error correction codes** impact energetic footprint.
4. in FTQC, **control electronics** consumes more energy than cryogeny.
5. significant progress needed in control electronics (room temperature, cryo-electronics, cabling, multiplexing).

**it's only a beginning, with many outstanding challenges in all quantum technologies**

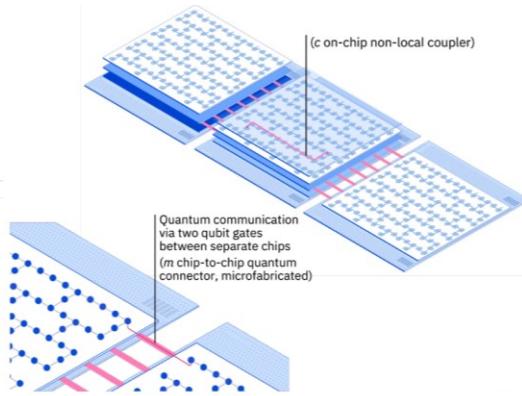


# distributed quantum computing

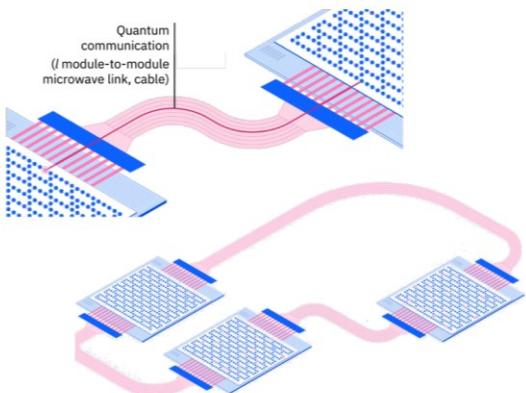




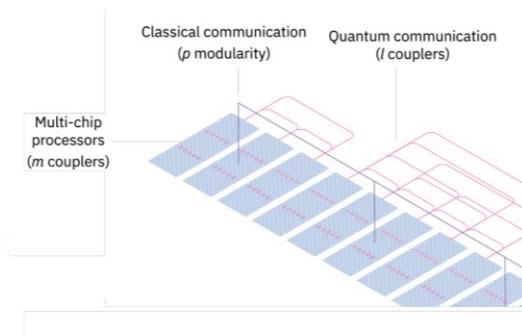
**parallel shots processing**



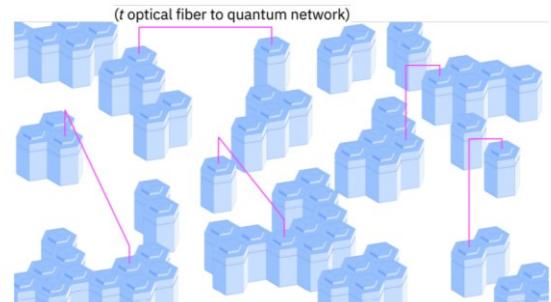
**local chipsets coupling**



**distant chipsets coupling**



**photonic chipset coupling**



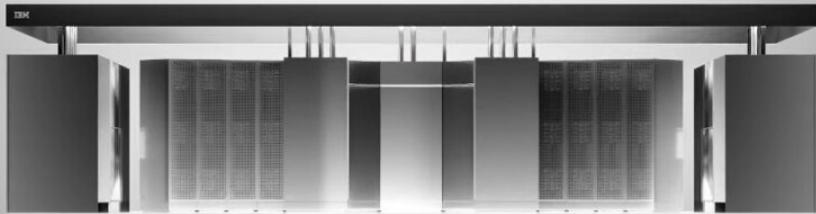
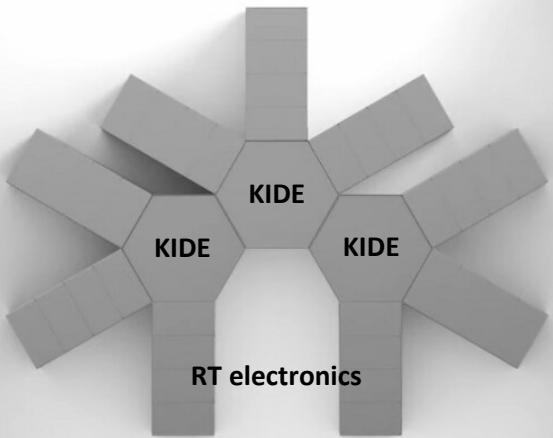
**combining all methods**



**scale-out approaches**

source: The Future of Quantum Computing with Superconducting Qubits by Sergey Bravyi, Oliver Dial, Jay M. Gambetta, Dario Gil and Zaira Nazario, IBM Quantum, September 2022 (20 pages)

compressors



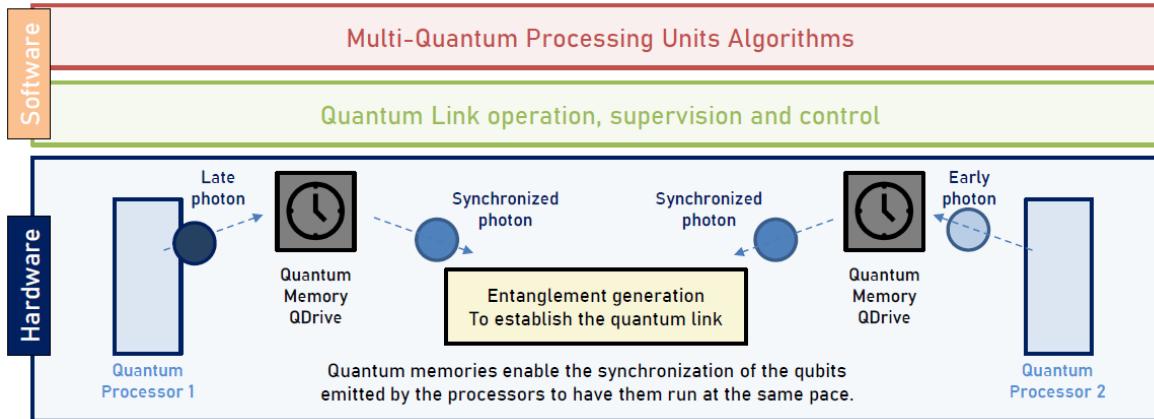
IBM Quantum

IBM  
Research

# WeLinQ

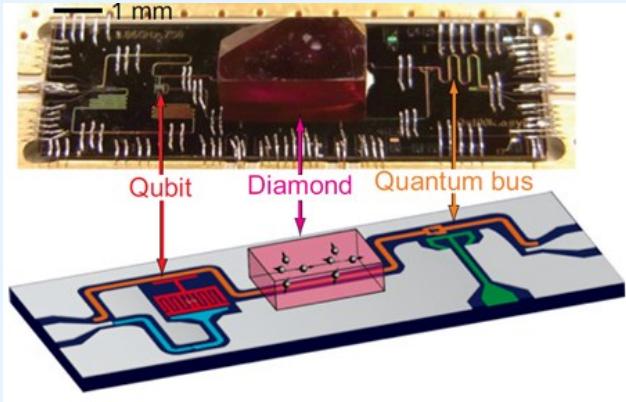
record high storage-and-retrieval efficiency for laser-cooled atom based quantum memory.

enables the synchronization in quantum repeater-based long-distance links and of photonic qubits emitted by quantum processors to efficiently interconnect them by teleportation.

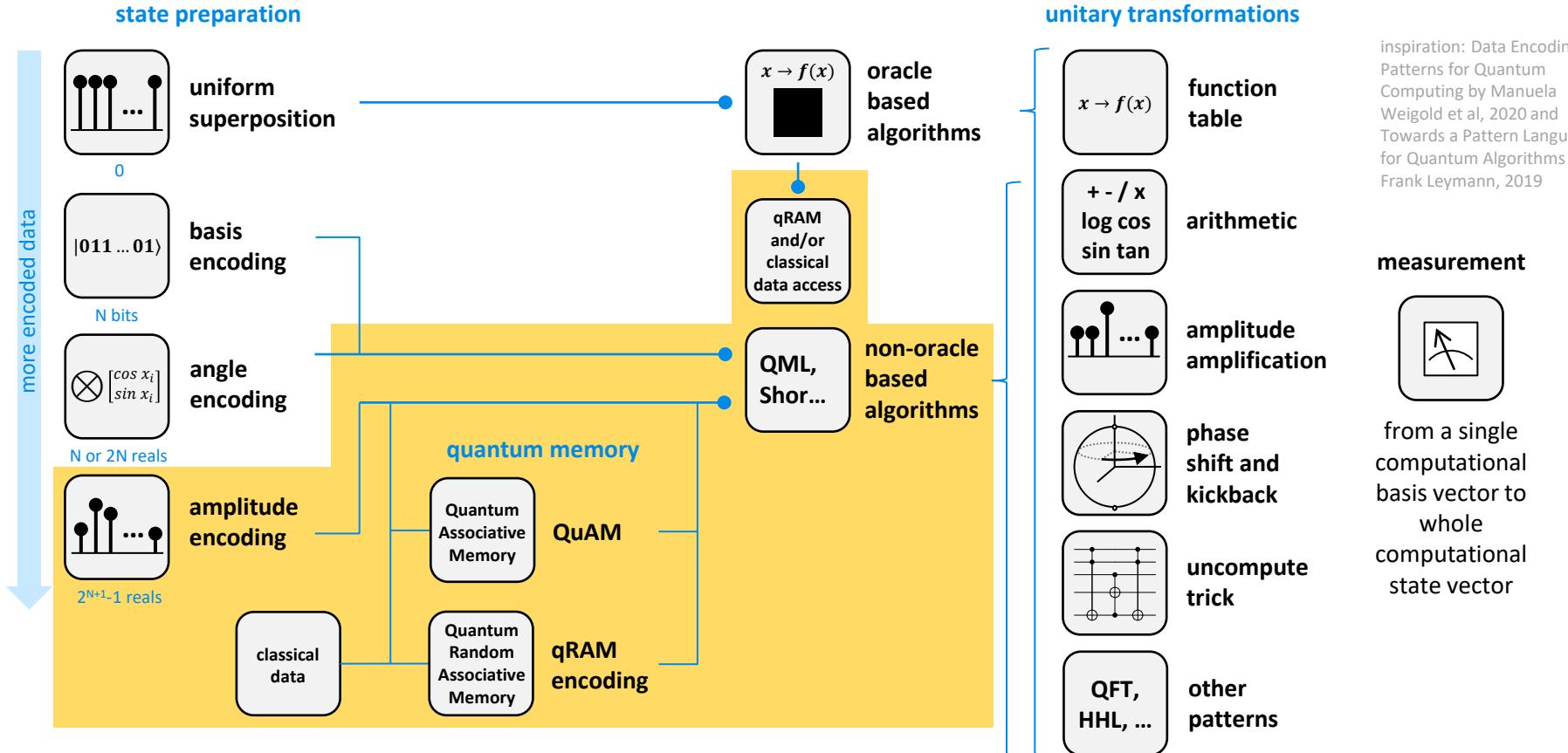


Tom Darras, Julien Laurat, Eleni Diamanti and Jean Lautier-Gaud

# data loading and quantum memory



# the data loading challenge



# quantum memory

due to the non-cloning theorem, you can't copy the state of a qubit to another qubit independently

the only way to do it is to entangle two qubits

still, quantum memories are needed in some situations such as with the Grover algorithm, QML and with quantum repeaters

qRAM adds a notion of qubits addressing these memories are kind of « qubit buffers »

could use photons in cavities or NV centers qubits

not available yet

Quantum technologies with hybrid systems,  
Patrice Bertet et al, 2015 (8 pages)

PHYS.ORG Nanotechnology Physics Earth Astronomy & Space Technology Chemistry

f t r e m

Home > Physics > Quantum Physics > February 22, 2018

## New quantum memory stores information for hours

February 22, 2018, Vienna University of Technology



## Quantum Optical Memory Device One Thousand Times Smaller Than Previous Options

On-chip-scale quantum memory device is not only small, but is capable of on-demand data retrieval

By Dexter Johnson

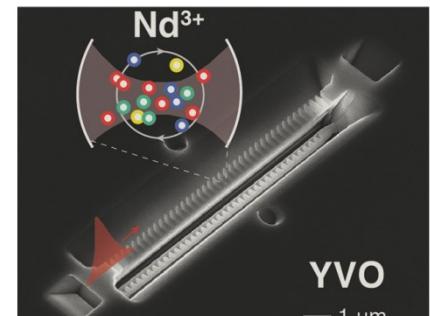
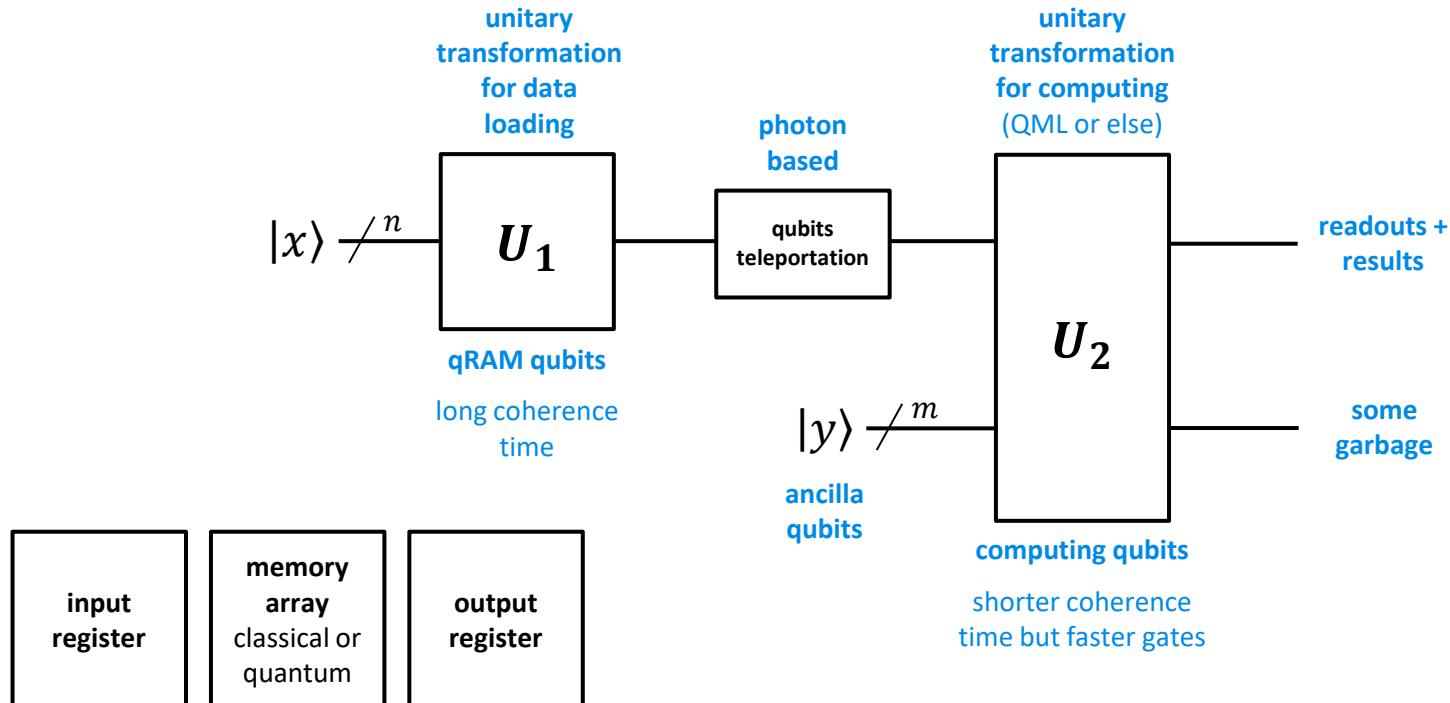
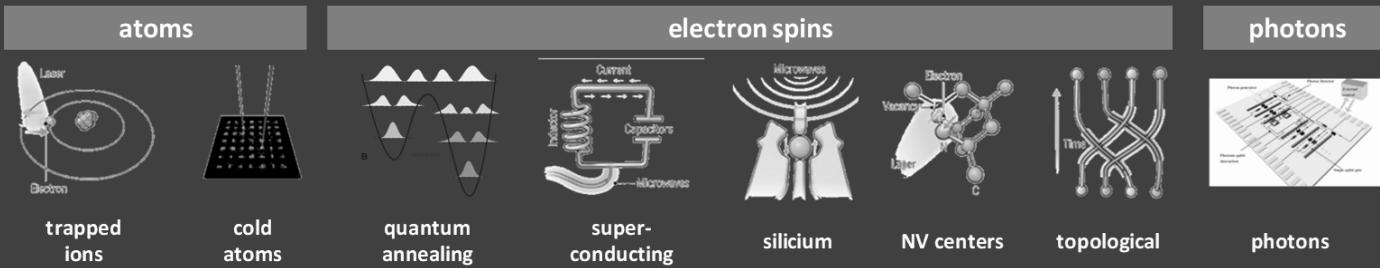


Image: Tam Zhang

Scanning electron microscope image shows the nano-scale optical quantum memory fabricated in yttrium orthovanadate (YVO). The schematic shows that this device is an optical cavity that contains Nd atoms.

# quantum memory principles





# qubits types and computers

# quantum & classical computing paradigms

## classical computers

### quantum inspired

classical algorithms running on classical computer, inspired by quantum algorithms.

classical algorithms improvements

### quantum emulators

running code/models created for quantum computers

quantum algorithms debug and testing



many software vendors like Multiverse



## analog quantum computers

### quantum annealing

### quantum simulators

optimization problems and quantum physics simulation



## digital quantum computers

### gate-based

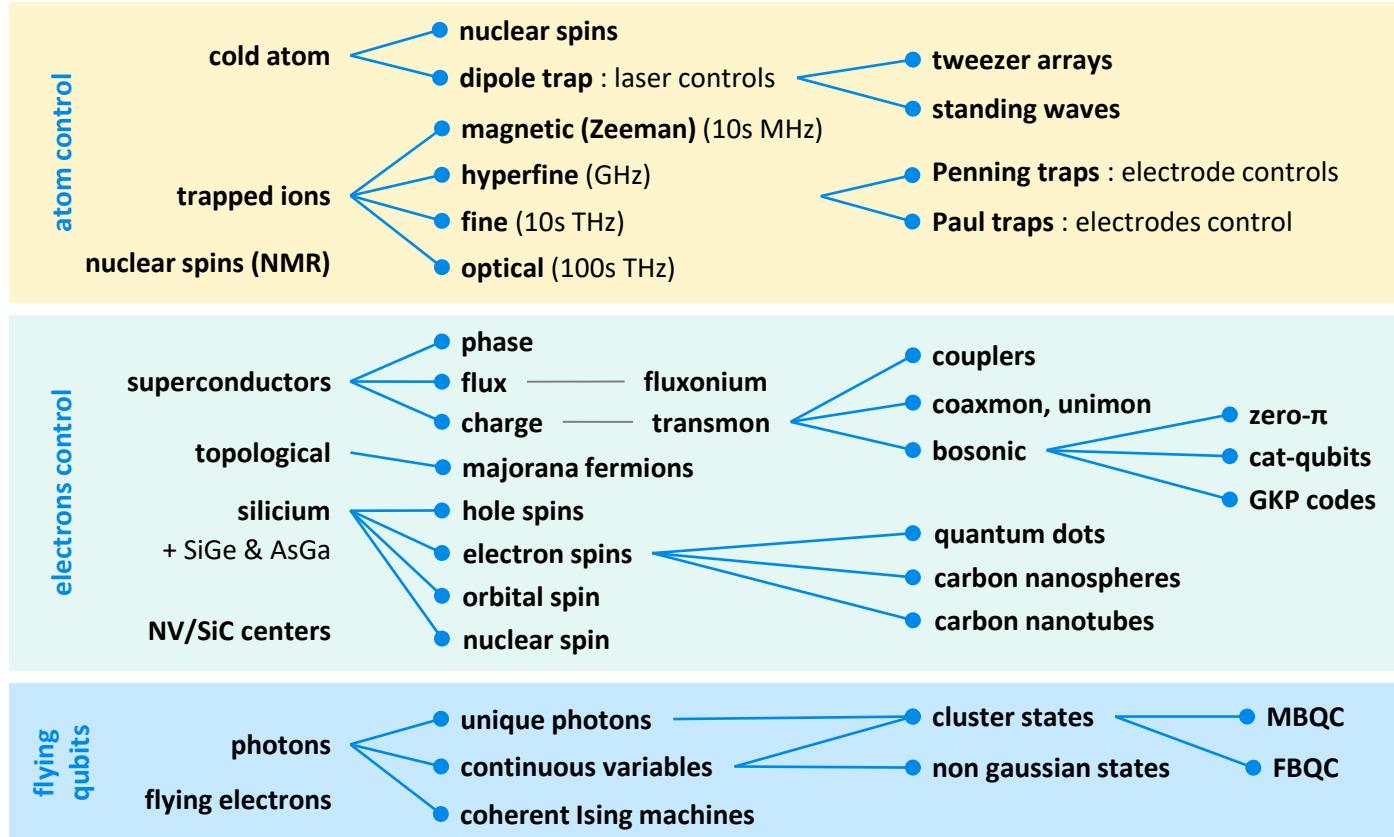
NISQ (Noisy Intermediate Scale Quantum)  
no error correction on a few noisy qubits

general purpose quantum computing,  
adds search and integer factoring

FTQC (Fault-Tolerant Quantum Computers)  
error correction and fault tolerance

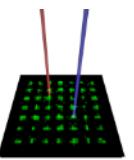
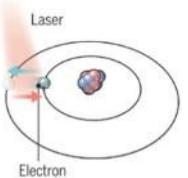


# qubits genealogy



(cc) Olivier Ezratty, 2022

## atoms



trapped ions



OXFORD  
IONICS  
eleQtron  
FOXCONN



cold atoms

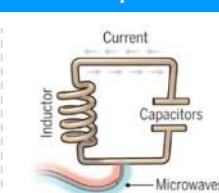


quantum annealing

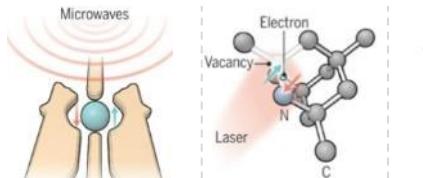


NEC

super-conducting



silicon



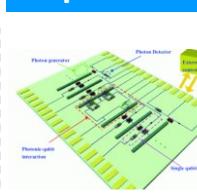
spin vacancies



topological



photons



(cc) Olivier Ezratty, 2023

## electron superconducting loops &amp; controlled spin



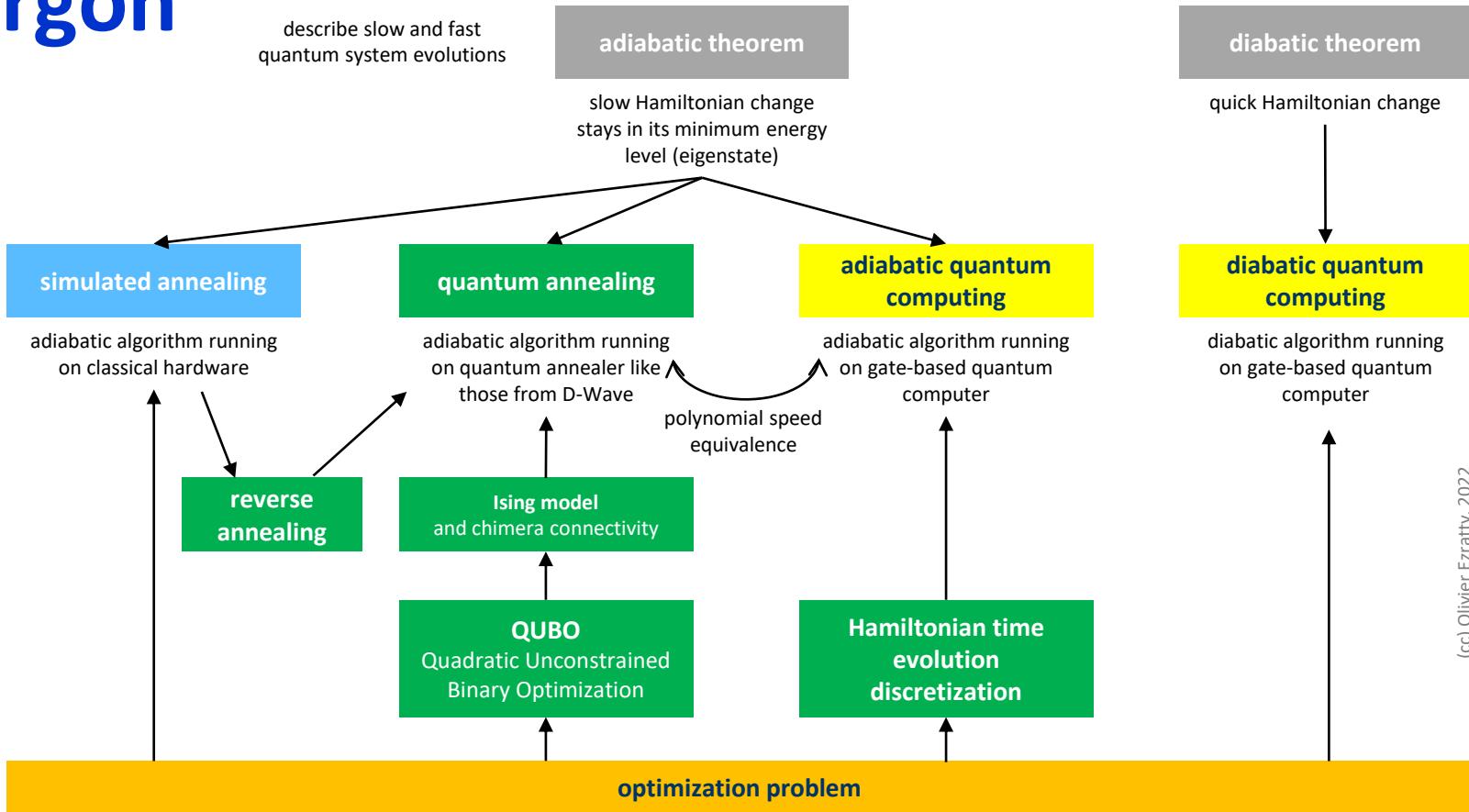
(\*) non exhaustive inventory, missing Chinese labs among others



$$\mathcal{H}_P = \sum_{i=0}^N h_i \sigma_i^z + \sum_{i,j=0}^N J_{ij} \sigma_i^z \sigma_j^z$$

quantum annealing

# jargon





The Quantum Computing Company™

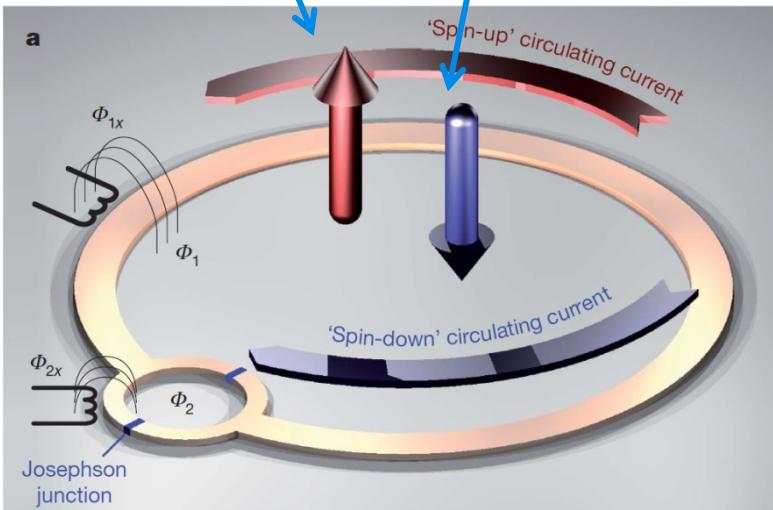
**superconducting quantum annealing  
plans to add gate-based model later**

**1999**

\$194.7M + \$350M SPAC



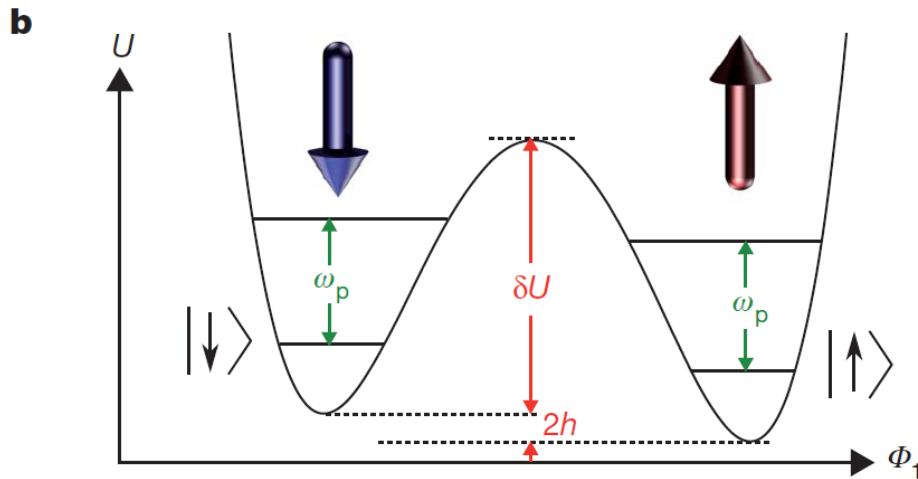
« spin up » qubits  $|\uparrow\rangle$       « spin down » qubits  $|\downarrow\rangle$



$\Phi_{1x}$  : flux bias on the outer superconducting loop which controls the energy difference «  $2h$  » between two states, i.e. superconducting current direction

$\Phi_{2x}$  : flux bias on the inner superconducting loop with two Josephson junctions, controlling energy level  $\delta U$  enabling the switch between two spin directions

# rf-SQUID flux qubits



$\omega_p$  : energy variation for  $|\uparrow\rangle$  et  $|\downarrow\rangle$  states

$\delta U$  : energy potential barrier between states

$2h$  : energy difference between the two base states

# Ising model and quantum annealing

**2-local Ising Hamiltonian initialization**  
defines  $h_i$  and  $J_{ij}$  and set all  $\sigma_i^z$  at +1

$$\mathcal{H}_P = \sum_{i=0}^N h_i \sigma_i^z + \sum_{i < j} J_{ij} \sigma_i^z \sigma_j^z$$

net qubits energy  
*longitudinal interactions*

qubits connections  
*energy longitudinal field*

**quantum annealing process**  
increases  $B(s)$  and decreases  $A(s)$  gradually

$$\mathcal{H}_S(t) = \mathcal{H}_P \frac{B(s)}{2} + \mathcal{H}_n(t) - \frac{A(s)}{2} \sum_{i=0}^N \sigma_i^x$$

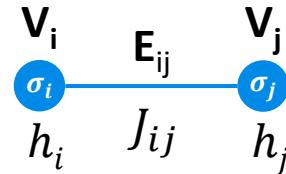
Ising model Hamiltonian

unknown effect of noise

final Hamiltonian

initial Hamiltonian

**qubits connectivity**  
coefficients and couplings



## problem variables

- $h_i$  linear coefficient (bias) on qubit  
usually discretized
- $J_{ij}$  coupling between vertices  $V_i$  and  $V_j$   
discretized and implemented with couplers  
non zero values limited by coupling topology

## problem unknowns

- $\sigma_i^z$  qubits values : +1 or -1 (« spin orientation »)
- $\sigma_i^z$  and  $\sigma_i^x$  are Pauli operators

## annealing time operators

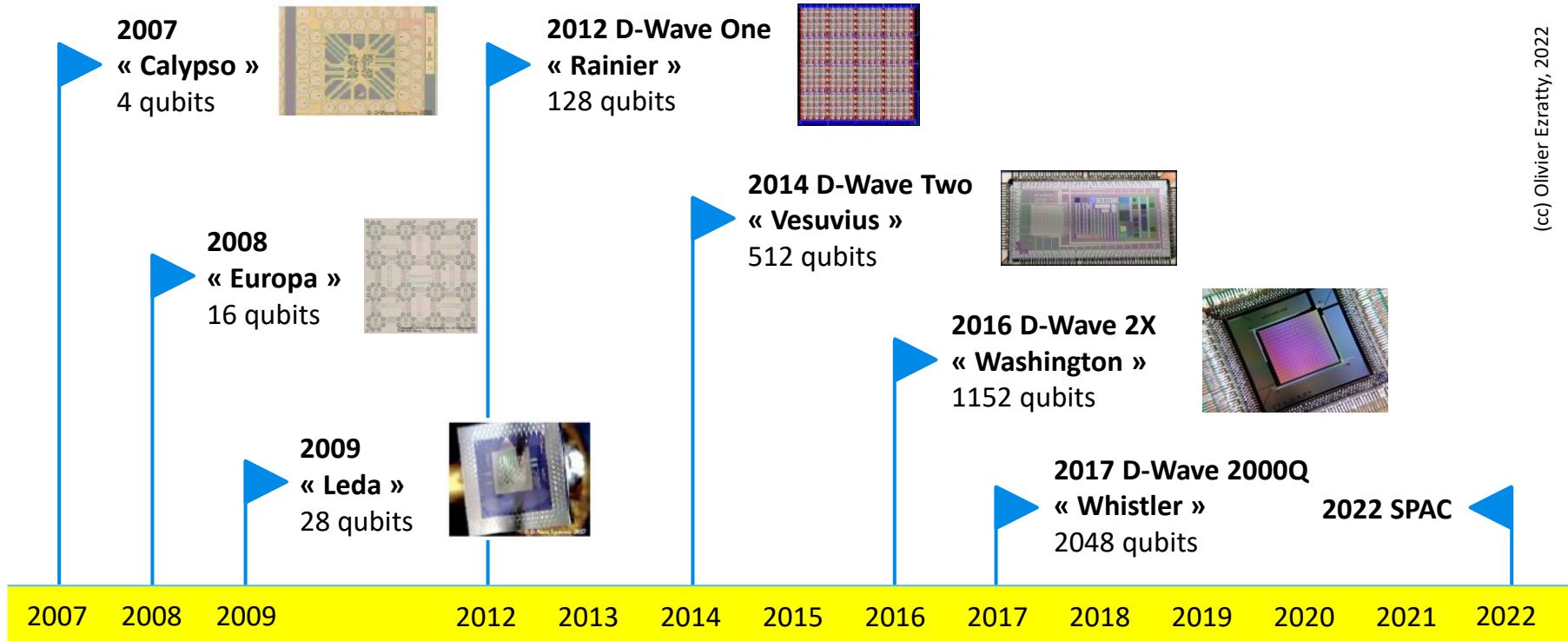
- $t$  time
- $t_f$  total annealing time, about 5μs
- $s$  fraction of annealing time =  $t/t_f$
- $A(s)$  tunneling energy at anneal fraction  $s$   
reduced over time as a  $\Gamma(t)$  transverse magnetic field applied to all qubits is reduced
- $B(s)$  problem Hamiltonian energy at anneal fraction  $s$   
increases over time during annealing

## qubits topology

- $V_i$  vertices containing qubit  $i$
- $E_{ij}$  edge connecting qubits  $i$  and  $j$

## system energy

- $\mathcal{H}_P$  initial system Hamiltonian
- $\mathcal{H}_n(t)$  system noise Hamiltonian
- $\mathcal{H}_S(t)$  total Hamiltonian



**D-WAVE**  
The Quantum Computing Company™

# QUBO and Ising models

**Quadratic Unconstrained Binary Optimization is a NP hard combinatorial optimization problem with applications in finance, logistics and machine learning. It can solve MaxCut, graph coloring and partitioning problems.**

**It can be converted to Ising problems and solved on D-Wave quantum annealing computers.**

## Quadratic Unconstrained Binary Optimization (QUBO)

Quadratic Unconstrained Binary Optimization consists in, given a **real symmetric matrix  $Q$** , minimizing the following cost function  $q$ :

$$q(x_1, \dots, x_n) = \sum_{i,j=1}^n -Q_{ij}x_i x_j$$

where  $x_1, \dots, x_n \in \{0, 1\}$  are **binary variables**.

Written differently, by **solving a QUBO problem**, we mean solving, given  $Q$ :

$$\min_{x_1, \dots, x_n \in \{0, 1\}} \sum_{i,j=1}^n -Q_{ij}x_i x_j$$

QUBO instances are in one-to-one correspondance with **Ising Hamiltonians** and cost functions.

Indeed, starting from the expression above for  $q$ , the **QUBO cost function**, and defining  $s_i = 2x_i - 1$  ( $\in \{-1, 1\}$  as  $x_i \in \{0, 1\}$ ), i.e  $x_i = \frac{s_i+1}{2}$ , one can indeed write:

$$\begin{aligned} q(x_1, \dots, x_n) &= \sum_{i,j=1}^n -Q_{ij}x_i x_j \\ &= - \sum_{i,j=1}^n Q_{ij} \left( \frac{s_i+1}{2} \right) \left( \frac{s_j+1}{2} \right) \\ &= - \sum_{i,j=1}^n \frac{Q_{ij}}{4} (1 + s_i + s_j + s_i s_j) \\ &= - \sum_{i,j=1}^n \frac{Q_{ij}}{4} - \sum_i \left( \sum_j \frac{Q_{ij}}{4} \right) s_i - \sum_j \left( \sum_i \frac{Q_{ij}}{4} \right) s_j - \sum_{i,j=1}^n \frac{Q_{ij}}{4} s_i s_j \\ &= - \sum_{i,j=1}^n \frac{Q_{ij}}{4} - \sum_{i=1}^n \frac{Q_{i,i}}{4} - \sum_i \left( \sum_j \frac{Q_{ij}}{2} \right) s_i - \sum_{i,j|i \neq j}^n \frac{Q_{ij}}{4} s_i s_j \\ &= - \sum_{i=1}^n h_i s_i - \sum_{i,j=1}^n J_{ij} s_i s_j + o \end{aligned}$$

with  $h_i = \sum_j \frac{Q_{ij}}{2}$ ,  $J_{ij} = \frac{Q_{ij}}{4}$  and an offset term  $o = - \sum_{i,j=1}^n \frac{Q_{ij}}{4} - \sum_{i=1}^n \frac{Q_{i,i}}{4}$ .

# D-Wave optimization solvers

## QBSolv solver

Finds a minimum value of a large quadratic unconstrained binary optimization (QUBO) problem by splitting it into pieces. Solves combinatorial problems using an iterative process that alternates between running a quantum annealing algorithm on a D-Wave QPU and a classical search algorithms.

## Hybrid Binary Quadratic Model (BQM) solver

Solve binary quadratic model (BQM) problems.

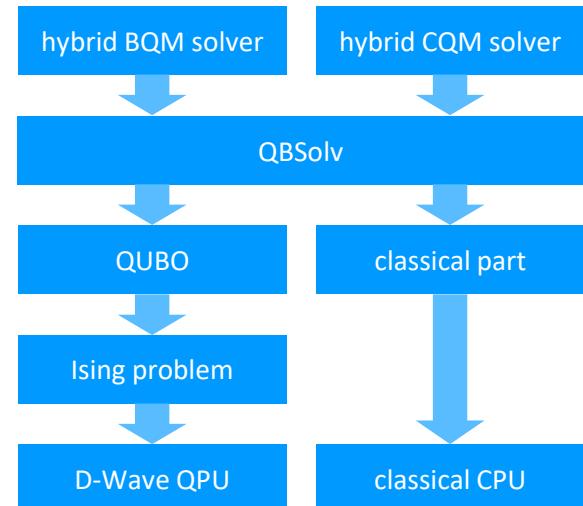
## Hybrid Constraint Quadratic Model (CQM) solver

Solve constraint quadratic model (CQM) problems.

HBQM and HCQM are specialized applications of QBSolv.

Knapsack problem  
MaxCut problem  
MIP problem

TSP problem  
Max clique  
Graph coloring



# quantum annealing algorithms

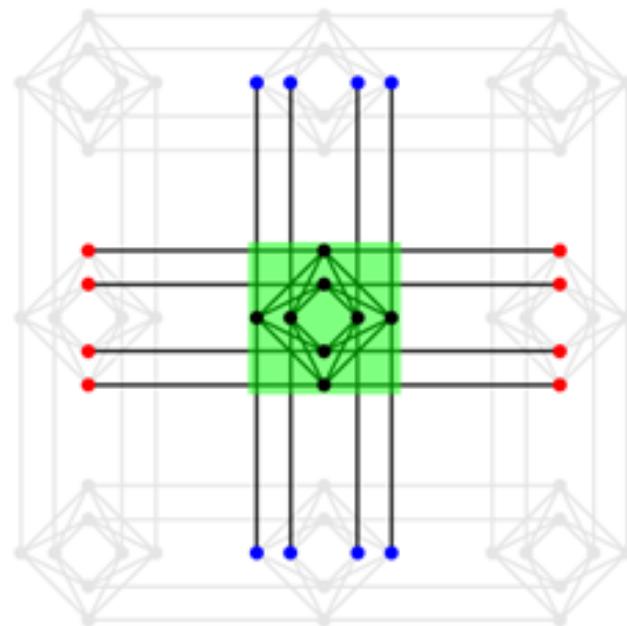
Table 1. Sample Applications for Quantum Annealing Processors

3-satisfiability	Fault tree analysis	Simulating atomic magnetometers
3D image tomography	Job-shop scheduling	Simulating quantum lattice transitions
Bayesian inference in imaging	Linear least squares	Telecommunications network design
Binary matrix factorization	List order optimization	Topological data analysis
Budget pacing in auctions	Modeling molecular dynamics	Traffic flow optimization
Capacitated vehicle routing	Modeling terrorist networks	Tsunami evacuation routing
Chemical structure analysis	Optimizing factory vehicles	ML: accelerating deep learning
Computational hydrology	Phylogenetics	ML: classification
Constrained shortest paths	Portfolio selection	ML: quantum boosting
Election modeling	Satellite scheduling	ML: training neural networks
Factoring	Simulating KT phase transitions	ML: reinforcement learning
Fault diagnosis in networks	Simulating material structures	ML: unsupervised learning

**K<sub>4,4</sub> 8 qubits unit cell**

6 connections per qubits

4 inside the cell and 2 outside

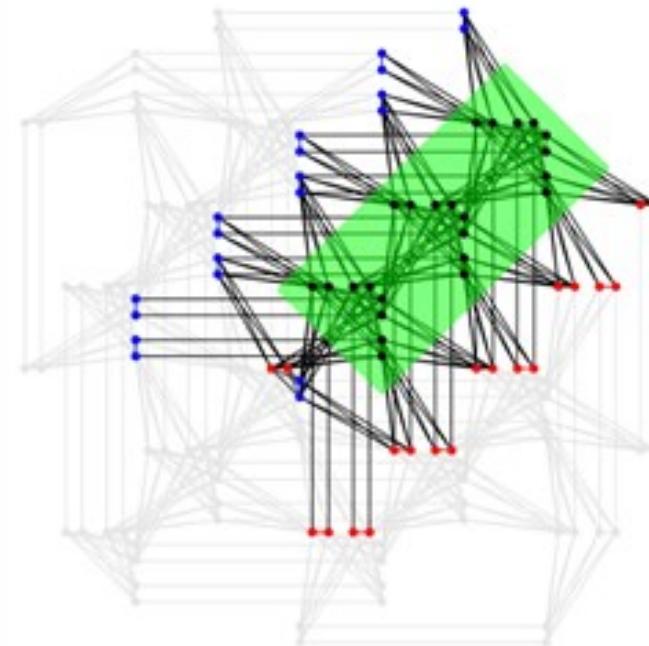


**D-Wave 2000Q chimera**

**8 qubits unit cell**

15 connections per qubits

12 inside the cell and 3 outside

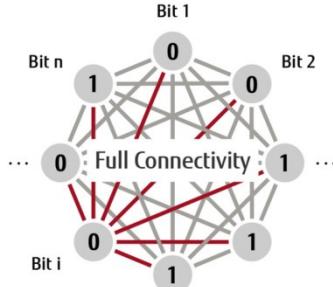


**D-Wave Pegasus graph**

source: [https://docs.dwavesys.com/docs/latest/c\\_gs\\_4.html](https://docs.dwavesys.com/docs/latest/c_gs_4.html)

# digital annealing

« digital annealing »

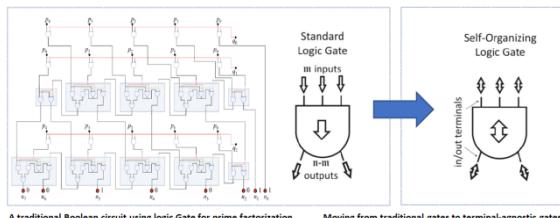


FUJITSU



analog reservoir  
network inspired  
computing

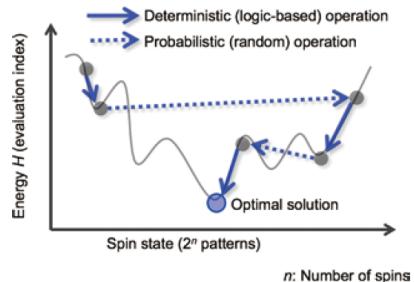
INFINITY|Q>



A traditional Boolean circuit for prime factorization  
It multiplies two integers  $p$  and  $q$  to give  $p \cdot q = 39 \cdot 100011_2$  (in the little-endian notation).

HITACHI

Figure 2: CMOS annealing



CMOS annealing  
combining a  
deterministic and  
probabilistic energy  
minimum search

- => few benchmarks available
- => impact of noise TBD
- => unproven scalability
- => no peer reviews



MemComputing

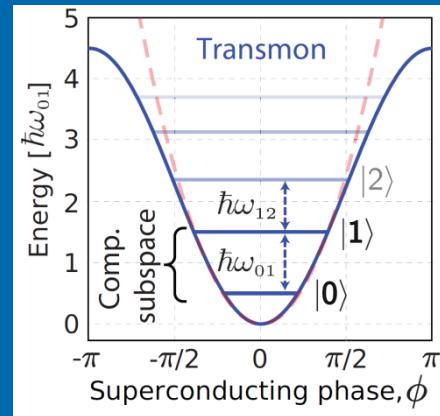
invertible logical  
computing

# quantum annealing summary

## quantum annealers

- mature **development tools** offering.
- large number of **software startups**, particularly in Japan and Canada.
- quantum annealers are available in the **cloud** by D-Wave and Amazon Web Services.
- the greatest number of well documented **case studies** in many industries although still at the proof of concept stage.
- most universal qubits gates algorithms can be have an equivalent on quantum annealing.

- all algorithms are **hybrid**, requiring some preparation on classical computers.
- only **one operational commercial vendor**, D-Wave.
- computing **high error rate**.
- **most commercial applications** are still at the pilot stage and not production-scale grade but they are closer than gate-based use cases.
- no **generic operational proof** of quantum advantage.



# superconducting qubits

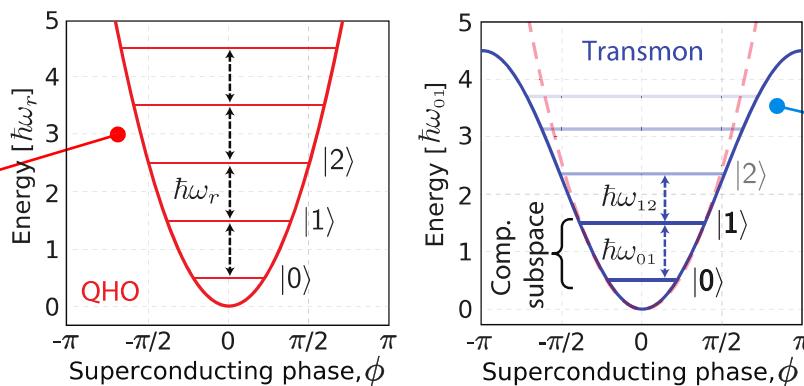
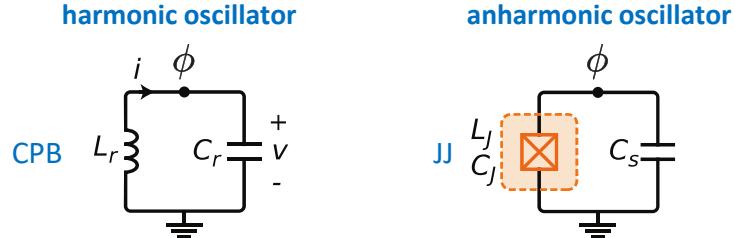
# superconducting qubits

$\phi$  : oscillator phase  
 $L_r$  : linear inductance  
 $C_r$  : capacity  
 $\hbar$  : Dirac constant  
 $\omega_r$  : pulse ( $2\pi \times$ frequency)  
 $H$  : oscillator Hamiltonian

**Cooper Pairs Box (CPB)**  
 inductance+capacitance  
 energy parabolic curve =>  
 equally spaced energy  
 levels.

$$H = 4E_C n^2 + \frac{1}{2} E_L \phi^2$$

$\hbar\omega_r$  : constant energy required to switch levels => hard to control  
 qubits states  $|0\rangle$  and  $|1\rangle$ , since a microwave pulse with energy  $\hbar\omega_r$  could switch qubit from state  $|1\rangle$  to  $|2\rangle$ .



- these oscillators have evenly or unevenly quantized energy levels  $|i\rangle$ .
- $|0\rangle$  and  $|1\rangle$  qubits states are evaluated with the phase of the oscillator.
- the oscillator phase has nothing to do with the qubit relative phase represented in its Bloch sphere representation.

Josephson junction with:  
 $L_J$  : non linear inductance  
 $C_J$  : inductance capacity

**Josephson Junction (JJ)**  
 energy cosinusoidal curve =>  
 unequally spaced energy  
 levels.

$$H = 4E_C n^2 + E_L \cos(\phi)$$

thanks to the loop non-linearity, energy transitions  $\hbar\omega_{nm}$  between adjacent levels are different and are decreasing, so a microwave pulses used to switch from  $|0\rangle$  to  $|1\rangle$  won't push  $|1\rangle$  state to  $|2\rangle$  and beyond.

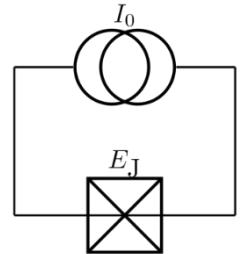
# qubit operating temperatures rationale

	micro-wave frequency to control superconducting qubits			micro-wave frequency to control electron spin qubits	
electromagnetic frequency	1 GHz	4 GHz	8 GHz	20 GHz	26 Ghz
corresponding temperature	48 mK	192 mK	384 mK	960 mK	1,24K
15 mK			100 mK		
qubit temperatures generating an acceptable noise level					

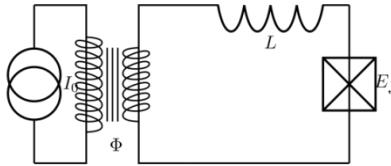
how is temperature associated with electromagnetic waves frequencies?

$$k_B T \ll \hbar\omega$$

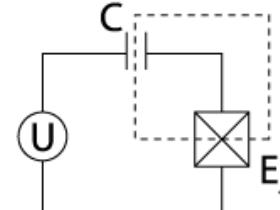
Boltzmann constant      temperature (K)  
Dirac constant      periodicity (frequency \*  $2\pi$ )

**phase qubit**

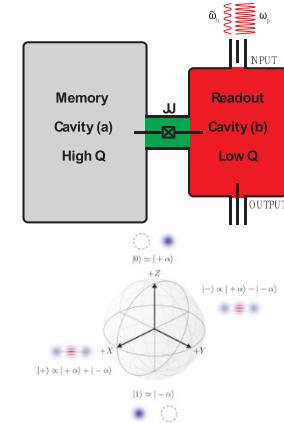
$I_0$  : current  
 $|1\rangle$   
 $|0\rangle$

**flux qubit**

$L$  : inductance

**charge qubit - transmon**

$U$  : tension

**cat-qubits**

Josephson junctions prepare,  
couple and correct the cat-qubits

 **$|0\rangle$  and  $|1\rangle$  qubits**

two energy levels  
in a potential well

two superconducting  
current directions

two levels of charge  
of Cooper pairs

pairs of entangled microwave  
photons in a cavity

**quantum gates**

micro-waves

magnetic field

micro-waves

micro-waves

**qubits readout**

resonator and  
micro-waves

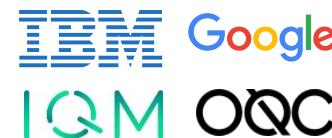
magnetometer (SQUID)

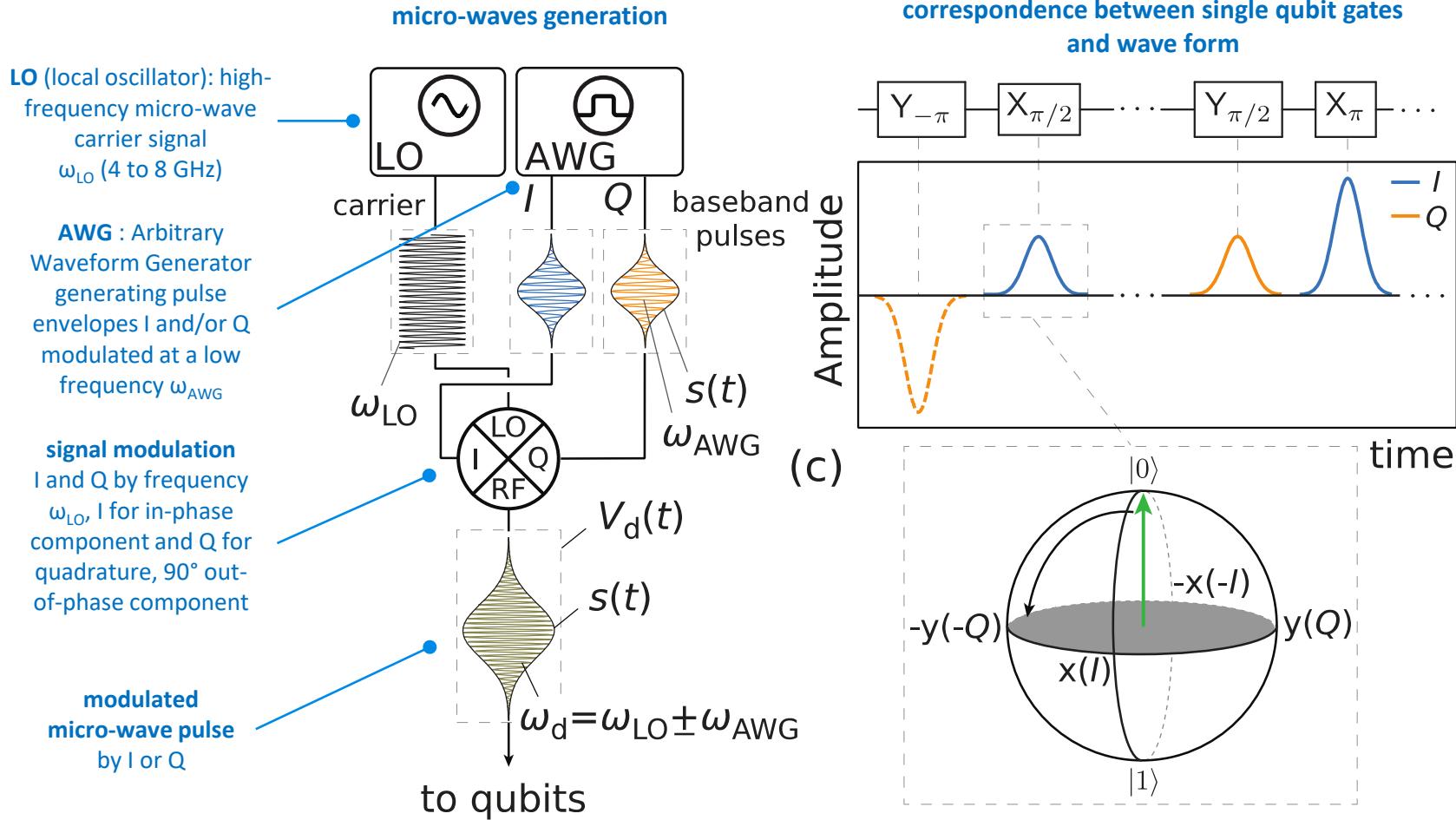
resonator and  
micro-waves

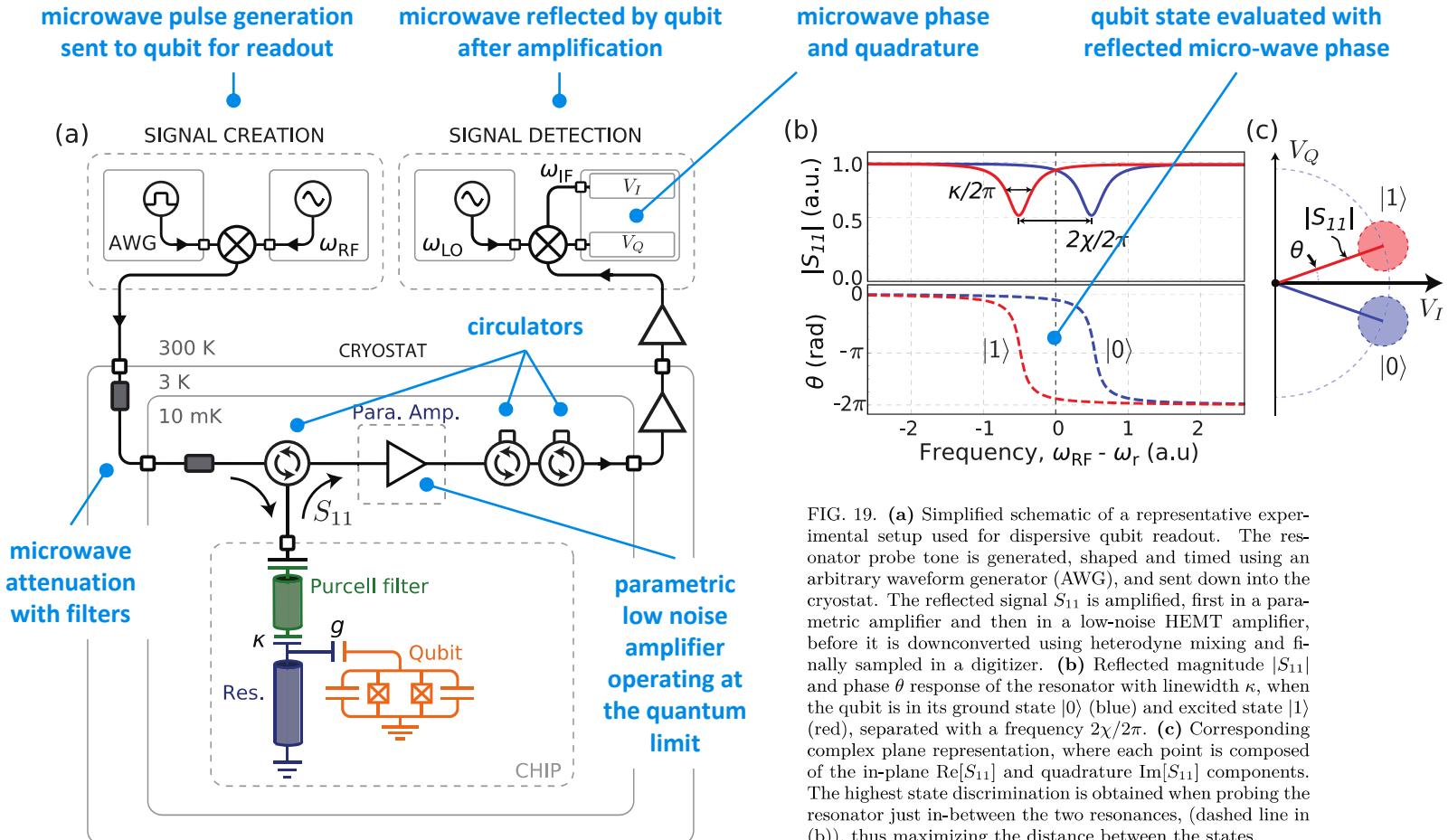
resonator and  
micro-waves

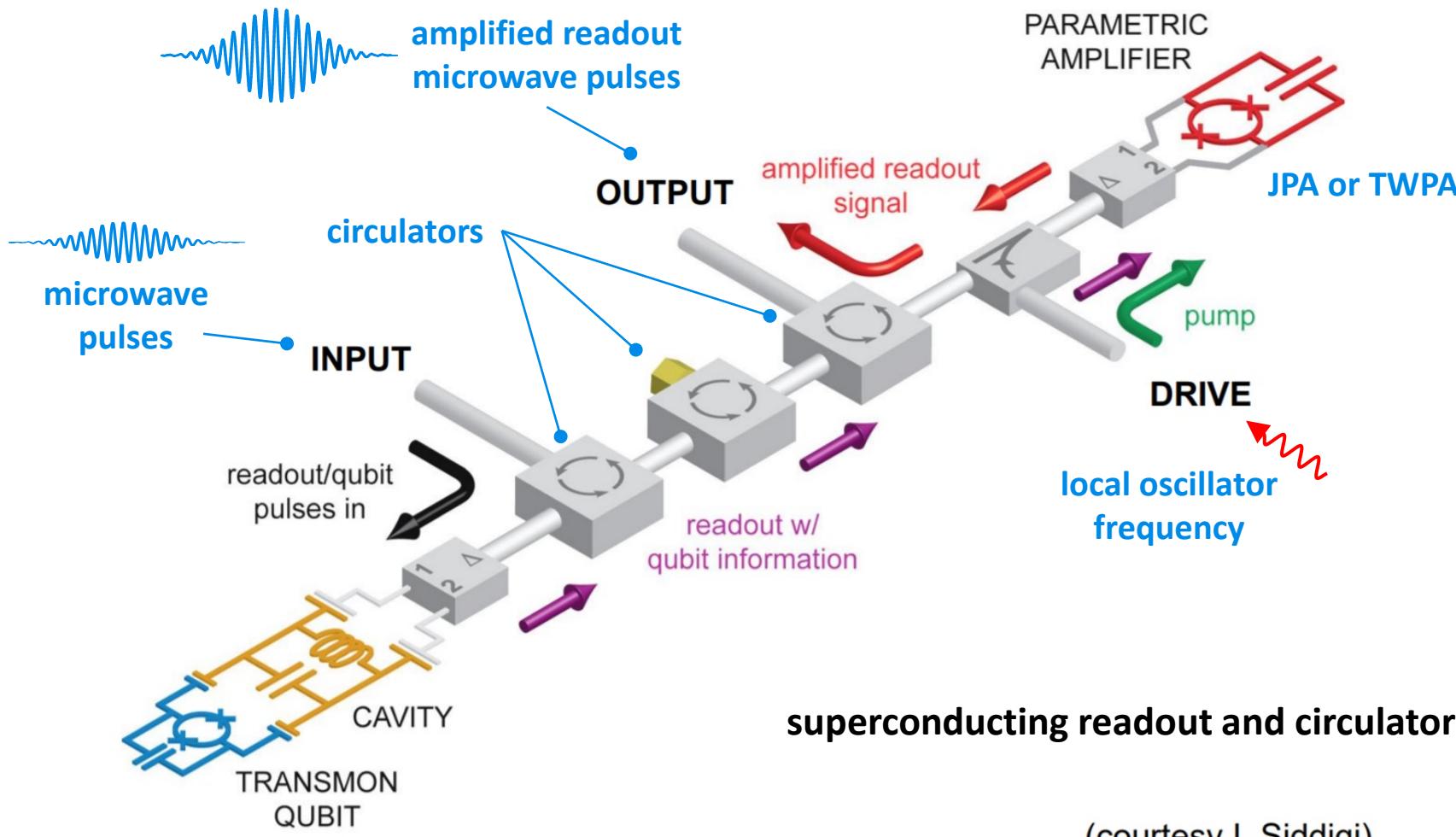
**commercial vendors**

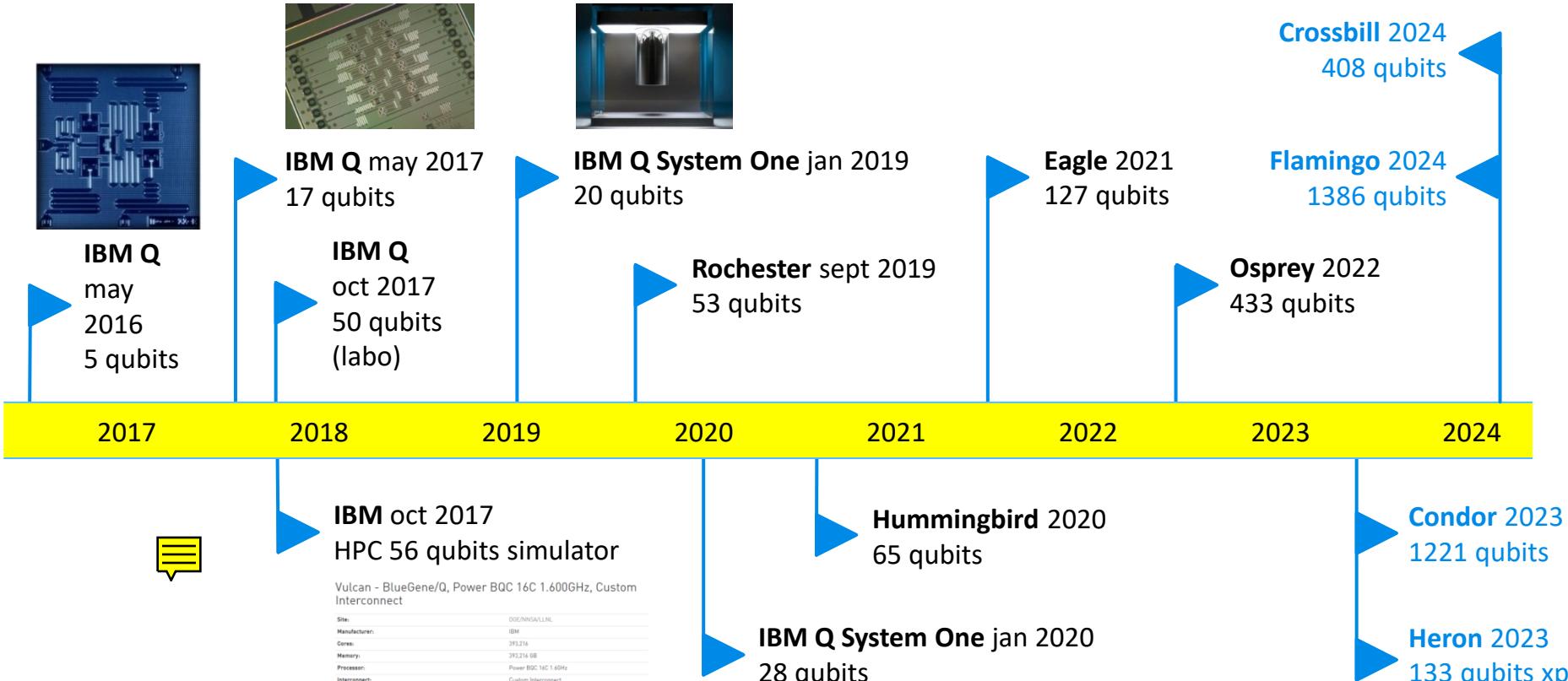
abandonned









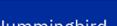
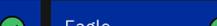
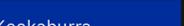


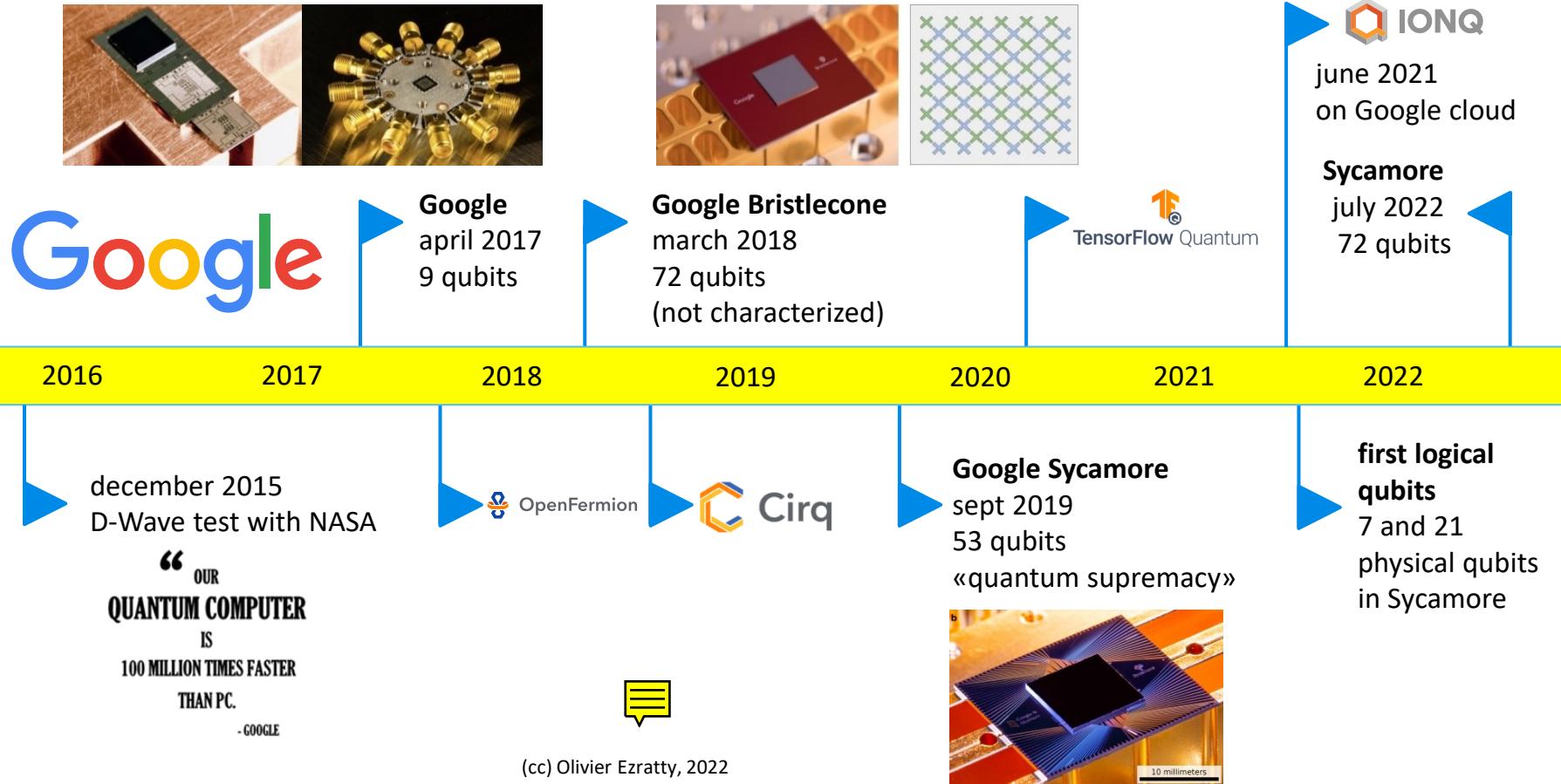
(cc) Olivier Ezratty, 2022

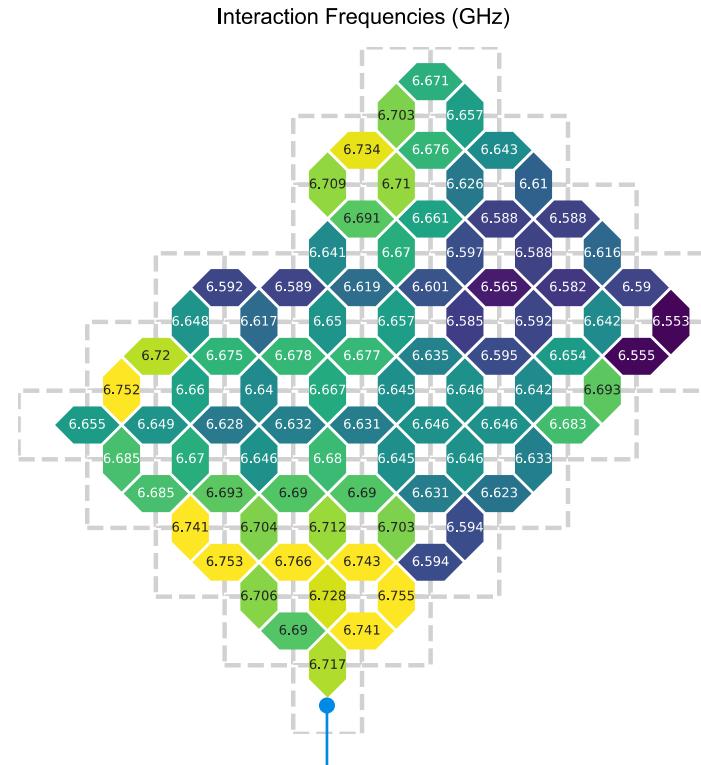
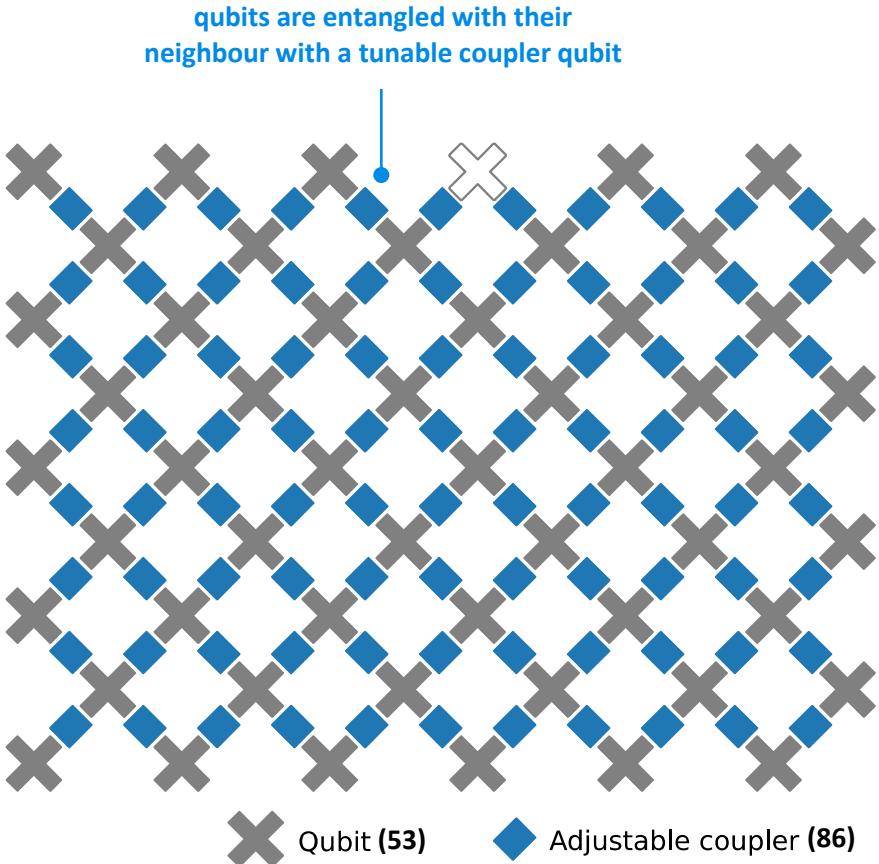
# Development Roadmap

Executed by IBM ✓  
On target ⚡

IBM Quantum

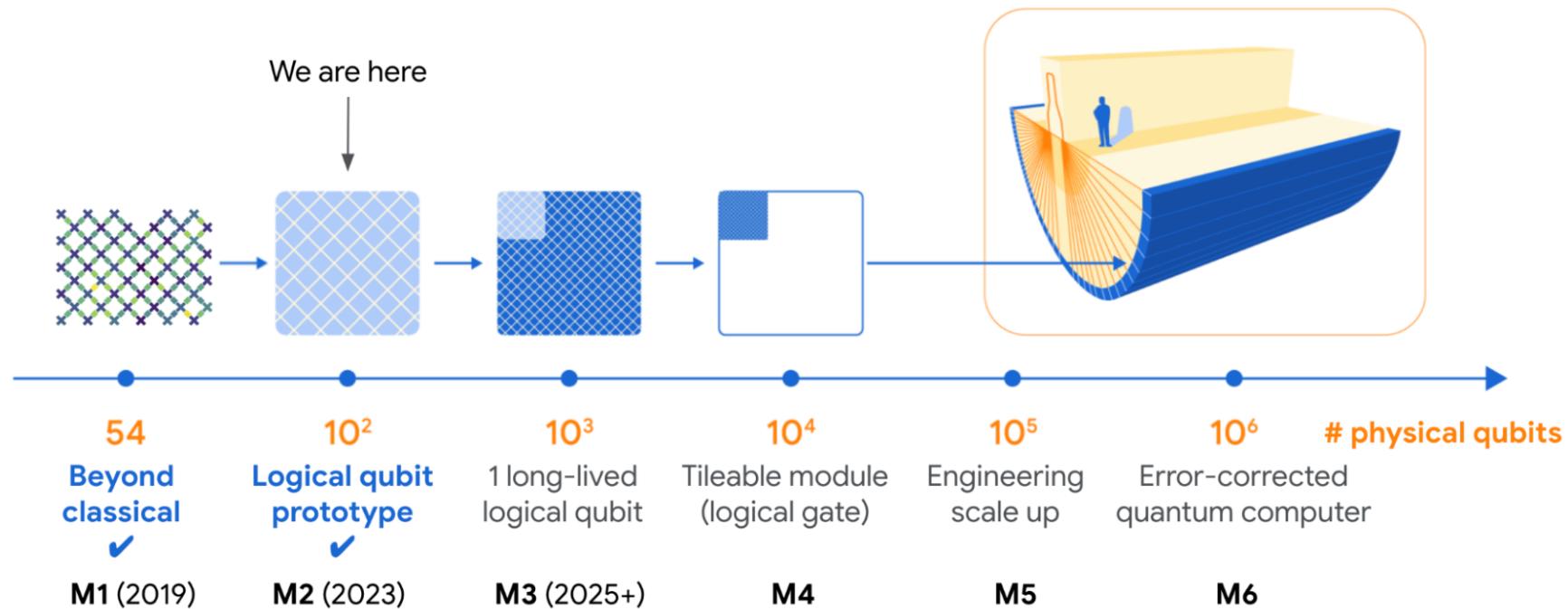
2019 ✓	2020 ✓	2021 ✓	2022	2023	2024	2025	Beyond 2026
Run quantum circuits on the IBM cloud	Demonstrate and prototype quantum algorithms and applications	Run quantum programs 100x faster with Qiskit Runtime	Bring dynamic circuits to Qiskit Runtime to unlock more computations	Enhancing applications with elastic computing and parallelization of Qiskit Runtime	Improve accuracy of Qiskit Runtime with scalable error mitigation	Scale quantum applications with circuit knitting toolbox controlling Qiskit Runtime	Increase accuracy and speed of quantum workflows with integration of error correction into Qiskit Runtime
Quantum algorithm and application modules	Machine learning   Natural science   Optimization	Quantum Serverless	Intelligent orchestration	Circuit Knitting Toolbox	Circuit libraries	Machine learning   Natural science   Optimization	Prototype quantum software applications → Quantum software applications
Circuits	Qiskit Runtime	Dynamic circuits	Threaded primitives	Error suppression and mitigation	Error correction		
Falcon 27 qubits	Hummingbird 65 qubits	Eagle 127 qubits	Osprey 433 qubits	Condor 1,121 qubits	Flamingo 1,386+ qubits	Kookaburra 4,158+ qubits	Scaling to 10K-100K qubits with classical and quantum communication
							
							





qubits couplers micro-waves frequencies were optimized with machine learning to limit crosstalk between qubits

Quantum error correction	–	Enabled	At scale
# Physical qubits	10 – 100	100 – 1000	$10^4 – 10^6$
# Logical qubits	–	1	10 – 1000+
Logical error	$10^{-3}$	$10^{-2} – 10^{-6}$	$10^{-6} – 10^{-12}$



# rigetti

2013  
\$198,5M



Aspen-9		Median Time Duration (μs)	Median Fidelity (per op.)
Deployed	07.02.21	T1 Lifetime	27
Qubits	31	T2 Lifetime	19
		Single-qubit gates	99.8%
		Two-qubit gates (CZ)	95.8%
		Two-qubit gates (XY)	95.4%

128 qubits announced in 2018 but never delivered

Forest is a developer environment for **quantum programming**.

Forest provides free developer access for up to 26-qubits of our simulator the Quantum Virtual Machine™ and private access to our quantum hardware systems for select partners.

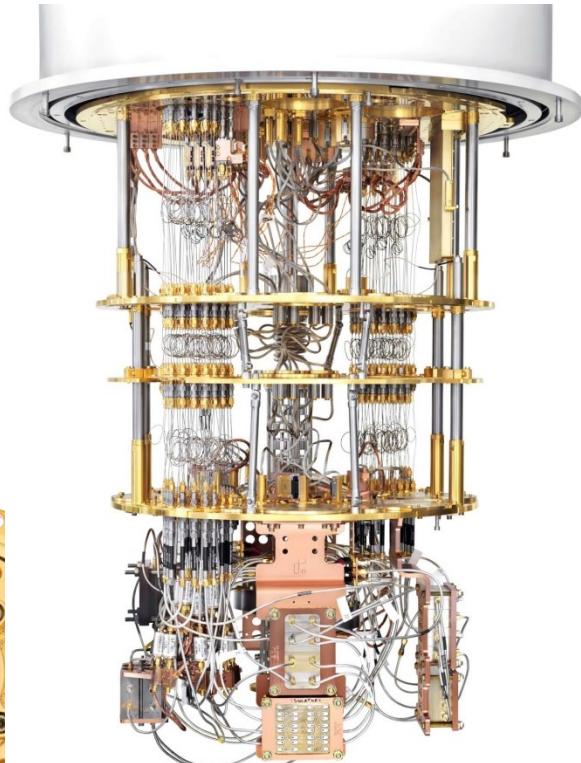
Watch Video 55:38

Open Source Software

Superconducting Quantum Processors

Example Algorithms

Python Development Tools



# rigetti

## Superconducting caps

Developed 2015 - 2018

Facilitates scaling and enhances performance<sup>2</sup>



## Superconducting TSVs

Developed 2016 - 2019

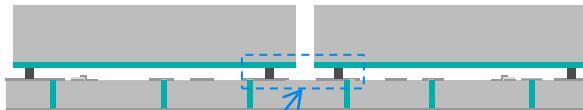
Isolates on-chip components and maximizes performance<sup>3</sup>



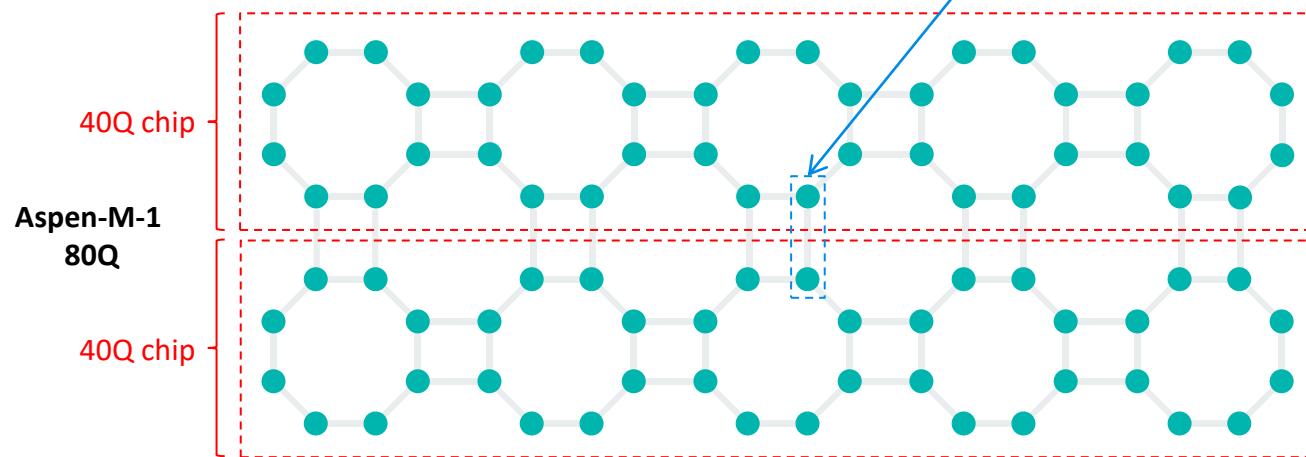
## Interchip Coupling

Developed 2018 - 2021

Interchip coupling enables fast gates and scaling qubit fabric across multiple chips<sup>4</sup>

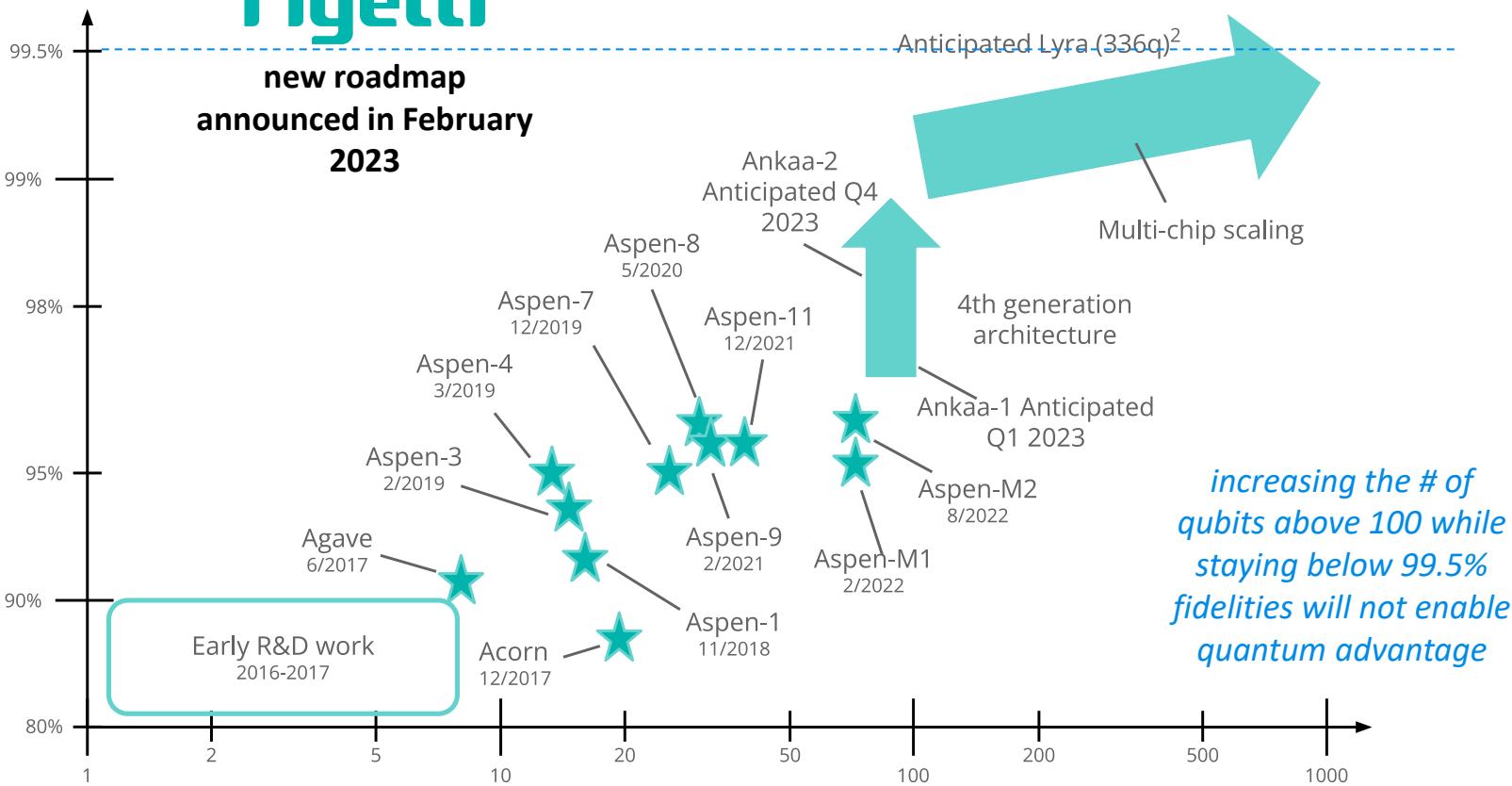


<sup>1</sup> Covering aspects of the modular, multi-chip quantum processor and the modular system architecture described herein. <sup>2</sup> O'Brien, William, et al. "Superconducting Caps for Quantum Integrated Circuits." ArXiv:1708.02219 [Physics, Physics:Quant-Ph]. Aug, 2017. arXiv.org. <sup>3</sup> Vahidpour, Mehmoosh, et al. "Superconducting Through-Silicon Vias for Quantum Integrated Circuits." ArXiv:1708.02226 [Physics, Physics:Quant-Ph]. Aug, 2017. arXiv.org. <sup>4</sup> Gold, Alysson, et al. "Entanglement Across Separate Silicon Dies in a Modular Superconducting Qubit Device." ArXiv:2102.03293 [Quant-Ph]. Mar, 2021. arXiv.org.

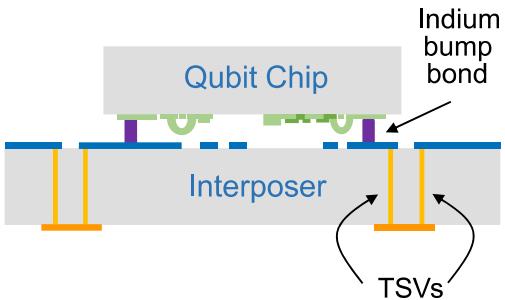


**new roadmap  
announced in February  
2023**

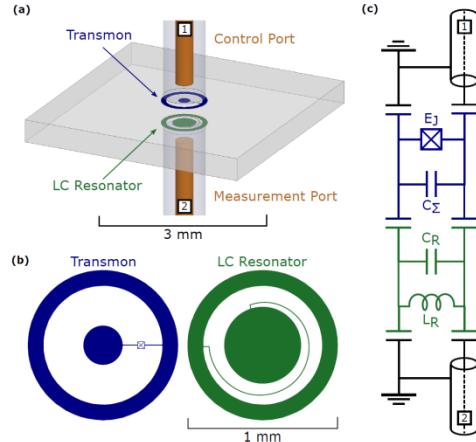
**Median 2Q fidelity**



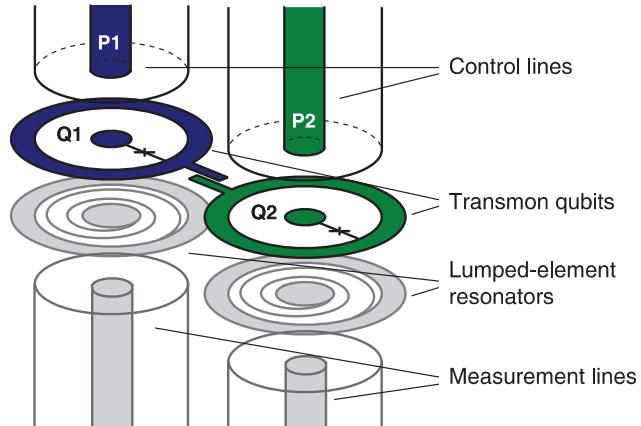
# OQC



Solid-state qubits integrated with superconducting through-silicon vias by D. R. W. Yost et al, MIT, September 2020



Double-sided coaxial circuit QED with out-of-plane wiring  
by J. Rahamim et al, 2017



Calibration of a Cross-Resonance Two-Qubit Gate Between Directly Coupled Transmons by A.D. Patterson et al, 2019

 + seeQC®

RIVERLANE

## What is Deltaflow.OS®?

Deltaflow.OS® is a radically new operating system for quantum computers. Quantum computers contain classical and quantum computing elements which must be orchestrated to tease out optimal performance. This is crucial for near-term applications such as quantum chemistry. In the long term, quantum error correction requires close integration of quantum and classical compute.



ALICE & BOB

**buffer serving as thermal bath**  
**Asymmetrically Threaded SQUID (ATS) implementing single and multiple qubit gates**

french startup created by Théau Peronnin and Raphaël Lescanfne, from ENS

with the help from Benjamin Huard (ENS Lyon), Zaki Leghtas (ENS Paris), Mazyar Mirrahimi (Inria), Philippe Campagne-Ibarcq (Inria) and Emmanuel Flurin (CEA)

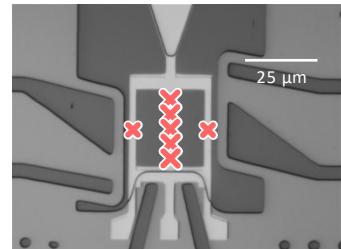
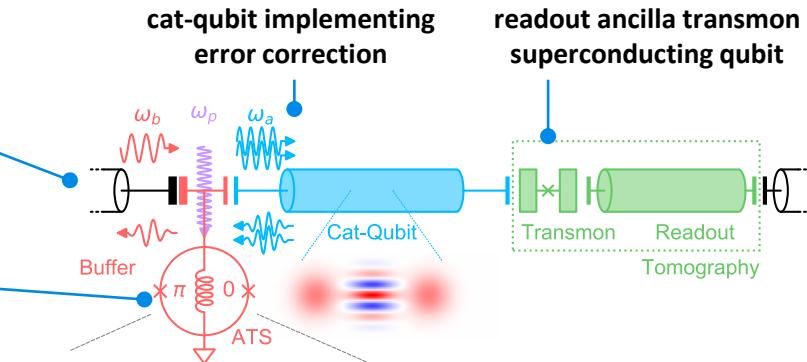
use cat-qubits based on two photons coupling in a cavity to increase reliability of superconducting qubits

qubit information comes from measuring cavity photon number parity without measuring photon number

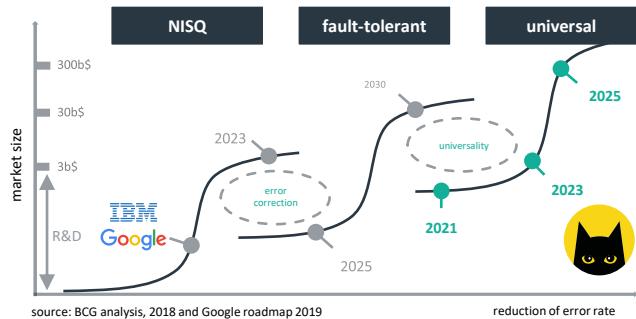
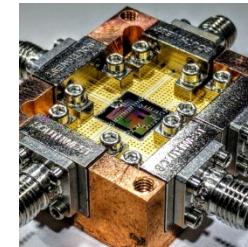
expect to build a logical superconducting qubit with only 30 cat-qubits instead of 10 000 classical superconducting qubits

significantly reduce the burden to create a LSQ FTQC (large scale quantum / fault tolerant quantum computer)

plan to produce a first processor with logical qubits by 2023



existing prototype correcting flip errors and improving error rate by a factor of 300



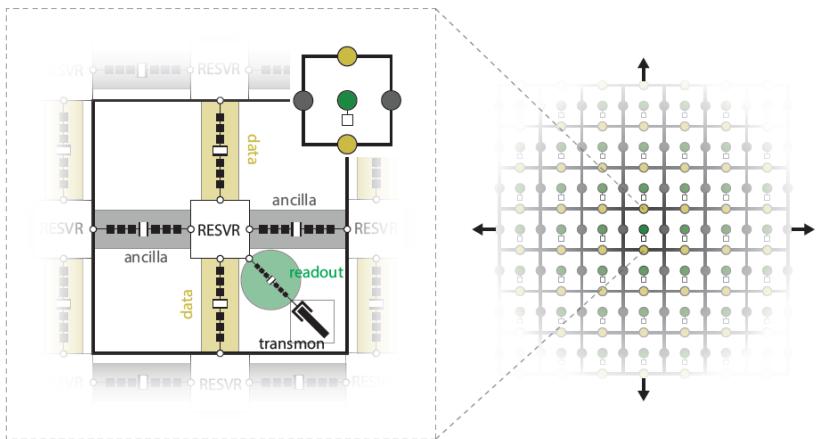
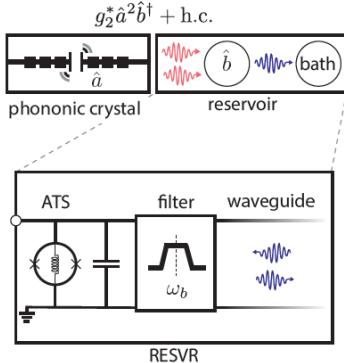
Alice & Bob directly shoots for full quantum advantage



**Amazon announced in december 2020 it will build its own quantum computers using cat-qubits superconducting, in a 118 pages theoretical paper**

**it plans to use surface codes QEC**

it's partnering with Caltech (incl John Preskill), Yale (Devoret/Schoelkopf teams) and other universities



## Building a fault-tolerant quantum computer using concatenated cat codes

Christopher Chamberland,<sup>1,2</sup> Kyungjoo Noh,<sup>1</sup> Patricio Arrangoiz-Arriola,<sup>1,\*</sup> Earl T. Campbell,<sup>1,\*</sup> Connor T. Hahn,<sup>1,3,\*</sup> Joseph Iverson,<sup>1,\*</sup> Harold Puttermann,<sup>1</sup> Thomas C. Bohdanowicz,<sup>1,2</sup> Steven T. Flammia,<sup>1</sup> Andrew Keller,<sup>1</sup> Gil Refael,<sup>1,2</sup> John Preskill,<sup>1,2</sup> Liang Jiang,<sup>1,4</sup> Amir H. Safavi-Naeini,<sup>1,5</sup> Oskar Painter,<sup>1,2</sup> and Fernanda G.S.L. Brandao,<sup>1,2</sup>

<sup>1</sup>AWS Center for Quantum Computing, Pasadena, CA 91125, USA

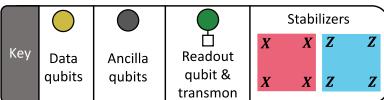
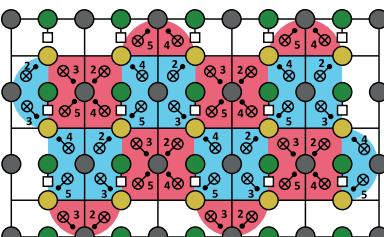
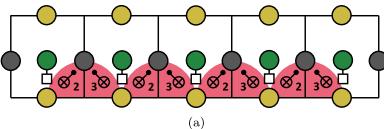
<sup>2</sup>IQIM, California Institute of Technology, Pasadena, CA 91125, USA

<sup>3</sup>Department of Physics, Yale University, New Haven, CT 06511, USA

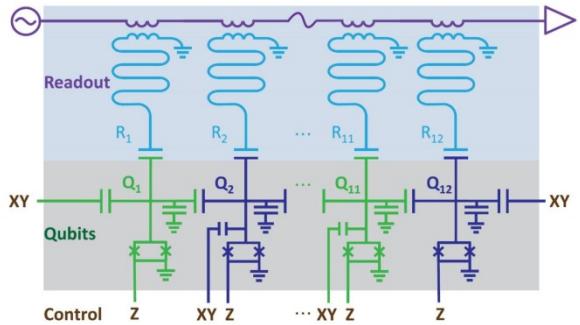
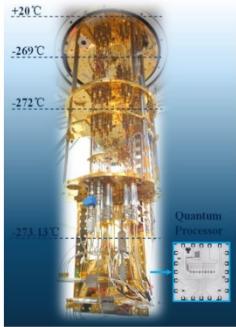
<sup>4</sup>Pritzker School of Molecular Engineering, The University of Chicago, Illinois 60637, USA

<sup>5</sup>Department of Applied Physics and Ginzton Laboratory, Stanford University, Stanford, CA 94305, USA

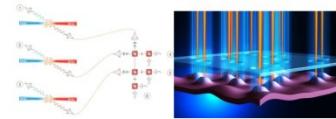
We present a comprehensive architectural analysis for a fault-tolerant quantum computer based on cat codes concatenated with outer quantum error-correcting codes. For the physical hardware, we propose a system of acoustic resonators coupled to superconducting circuits with a two-dimensional layout. Using estimated near-term physical parameters for electro-acoustic systems, we perform a detailed error analysis of measurements and gates, including CNOT and Toffoli gates. Having built a realistic noise model, we numerically simulate quantum error correction when the outer code is either a repetition code or a thin rectangular surface code. Our next step toward universal fault-tolerant quantum computation is a protocol for fault-tolerant Toffoli gates. Stabilizer correction that significantly improves upon the fidelity of physical Toffoli gates at very low qubit cost. To achieve even lower overheads, we derive a more modest distillation protocol for Toffoli states. Combining these results together, we obtain realistic full-resource estimates of the physical error rates and overheads needed to run useful fault-tolerant quantum algorithms. We find that with around 1,000 superconducting circuit components, one could construct a fault-tolerant quantum computer that can run circuits which are intractable for classical supercomputers. Hardware with 32,000 superconducting circuit components, in turn, could simulate the Hubbard model in a regime beyond the reach of classical computing.



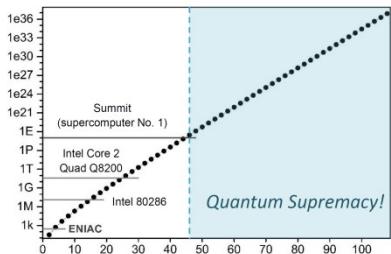
# superconducting qubits in China



Towards Scalable Quantum Computation and Simulation



- More entangled particles with the help of quantum memory
- Efficient quantum dot single photon emitters



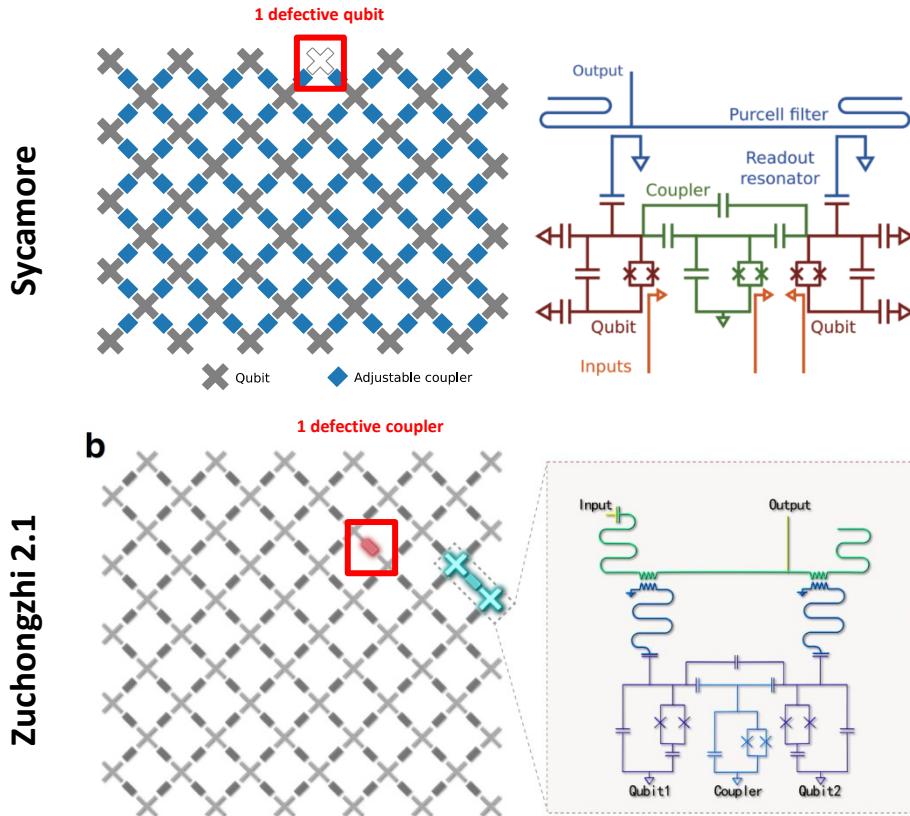
- ▶ Entanglement of 12 superconducting qubits
- ▶ Scalable engineering of high-fidelity 24 qubits

Fabrication and measurement of 30-50 qubit entanglement in progress

- ▶ In next 3-5 years: quantum computer with 50-60 qubits ➔ beating classical super computer in specific tasks (e.g. Boson sampling and portfolio optimization)
- ▶ In next 5-10 years: quantum computer with hundreds of qubits ➔ mimicking condensed matter physics (e.g., high temperature superconductor, quantum Hall effect, etc.)

- + 62 qubits in 2021 implementing a quantum walk
- + 121 qubits in 2022 with only 68 being used to create topological qubits
- + Origin Quantum with 24 qubits

# comparing Sycamore and Zuchongzhi 2.1



single qubit gate: **99,84%**  
two qubits gate: **99,07%**  
readout: **94,20%**  
qubit lifetime: **16 µs**  
*october 2019*

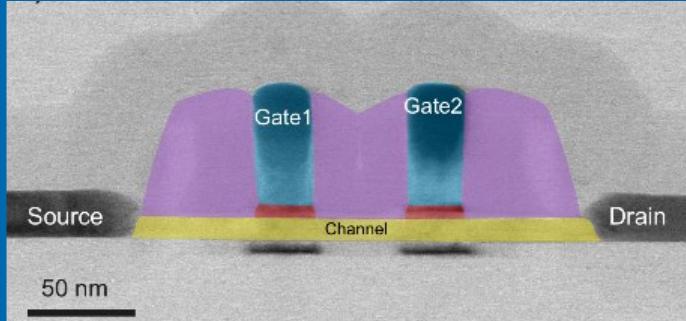
single qubit gate: **99,86%**  
two qubits gate: **99,24%**  
readout: **95,23%**  
qubit lifetime: **30.6 µs**  
*june 2021*

# superconducting qubits summary

## superconducting qubits

- **key technology** in public research and with commercial vendors (IBM, Google, Rigetti, Intel, Amazon, OQC, IQM, etc).
- **record of 127 programmable qubits** with IBM.
- constant progress in **noise reduction**, particularly with the cat-qubits variation which could enable a record low ratio of physical/logical qubits.
- many existing **enabling technologies**: cryostats, cabling, amplifiers, logic, sensors.
- **potentially scalable technology** and deployable in 2D geometries.

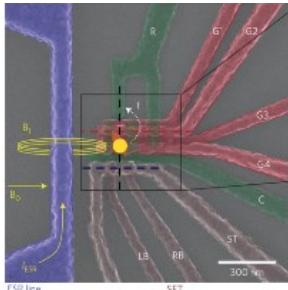
- **qubit coherence time usually < 300 µs.**
- **cryogeny constrained technology at <15 mK.**
- **heterogeneous qubits requiring calibration and complex micro-wave frequency maps.**
- **qubit coupling limited to neighbor qubits in 2D structures (as compared with trapped ions).**
- **cabling complexity and many passive and active electronic components to control qubits with micro-waves.**
- **qubits size and uneasy miniaturization.**
- **qubit fidelities are average with most vendors.**



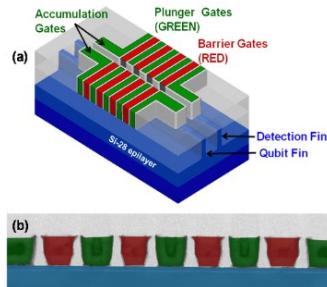
electron spins qubits

# different electron spin qubits platforms

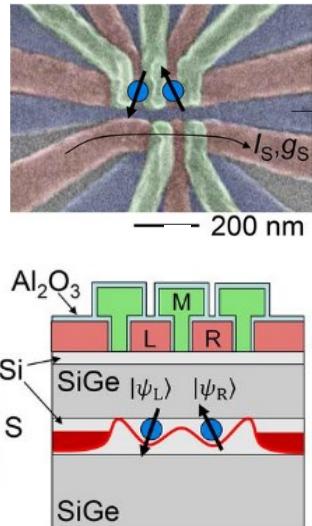
Si-MOS, CMOS



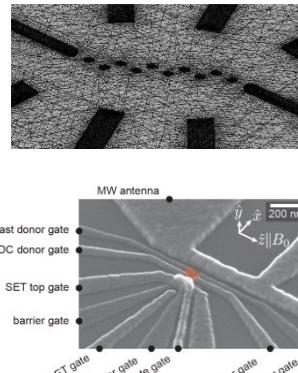
Fin-FET



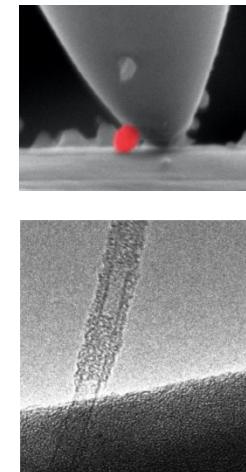
Si/SiGe



donors



carbon  
nanotubes/spheres



UNSW, Sandia  
Labs, CEA-Leti,  
Siquance

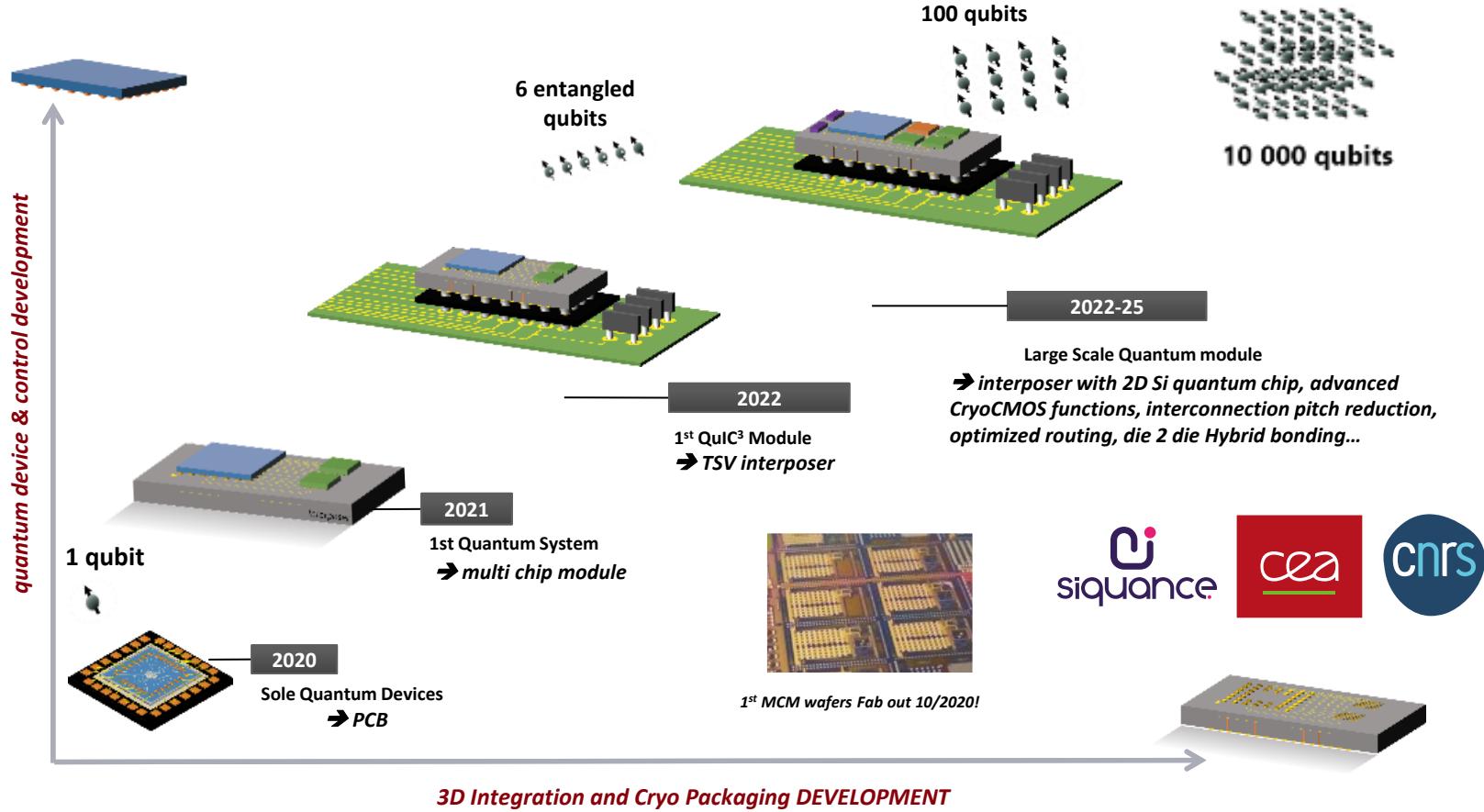
Intel, TU Delft,  
IBM, U. Basel

Princeton, RIKEN,  
HRL, TU Delft,  
CEA IRIG

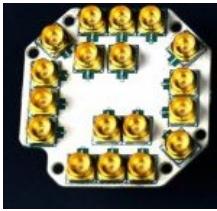
UNSW,  
SQC

C12 Quantum  
Electronics,  
Archer Materials

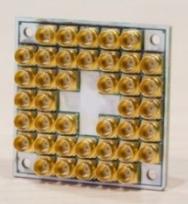
# toward a scalable platform



source: Maud Vinet IEDM tutorial, 2020

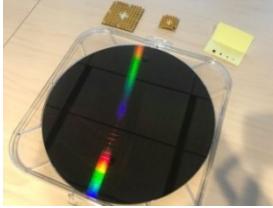


invests \$50M  
in QuTech



7 supraco  
qubits

17 super-co  
qubits



silicon qubits wafer  
(not characterized)

Horse Ridge II

Si/SiGe single spin  
qubits

2 qubits logic gates

QSDK

2016

2017

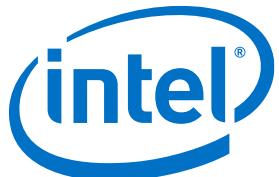
2018

2019

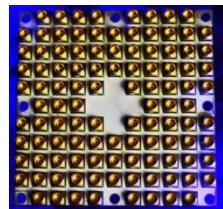
2020

2021

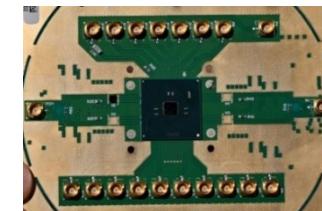
2022



**double bet:**  
superconducting and silicon



49 supraco qubits  
Tangle Lake





# C12 Quantum Electronics

french startup created by Matthieu and Pierre Desjardins

with the help from Taki Kontos (LPENS)

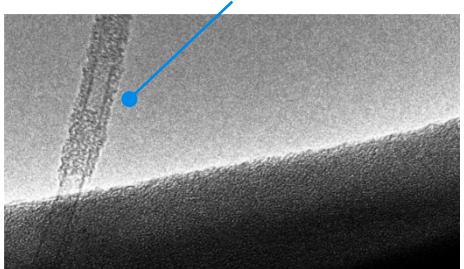
electron spins qubits trapped in carbon nanotubes

5 qubits demonstrator planned for 2021/2022

multiple spins can be coupled for **2-qubit gate** to the same resonator enabling all-to-all connectivity between qubit

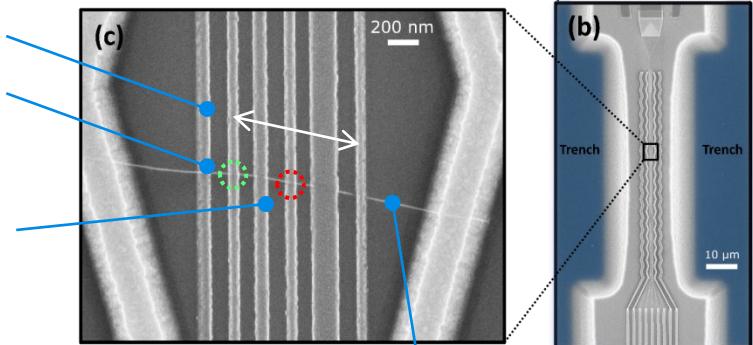
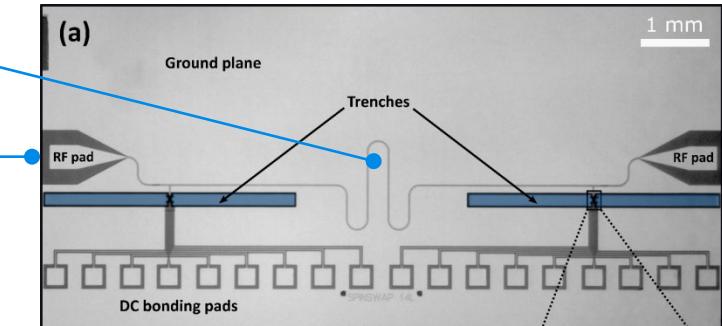
spin qubit manipulated and read-out with a **7 GHz microwave superconducting resonator**

qubits are based on a **single electron spin** isolated in a 2 nm diameter carbon nanotube



electrons move in **one direction** it can be trapped in a **quantum dot** by defining an electrostatic potential with underneath control electrodes.

**coupling to the resonator** can be switched on and off by freezing the motion of electron in one of the two quantum dots.



decoherence is limited with using **zero spin isotope C<sub>12</sub>** in nanotubes, suspending the tube above the substrate and removing the oxide

# electron spin qubits summary

## quantum dots spins qubits

- **good scalability potential** to reach millions of qubits, thanks to their size of 100x100 nm.
- **works at around 100 mK - 1K** => larger cooling budget for control electronics vs superconducting qubits.
- **average qubits fidelity** reaching 99% for two qubits gates in labs.
- adapted to **2D architectures** usable with surface codes or color codes QEC.
- can leverage existing semiconductor **fabs**.
- good quantum **gates speed**.

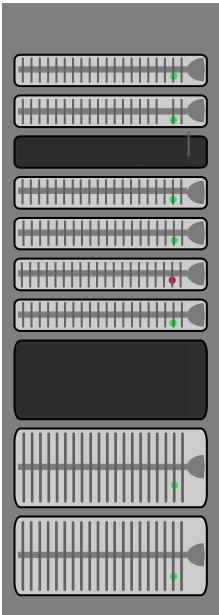
- **active research in the field started later than with other qubit technologies and spread over several technologies** (full Si, SiGe, atom spin donors).
- **less funded startup scene**.
- **qubits variability to confirm**.
- **high fabs costs and long test cycles** (18 months average).
- **so far, only 4 to 15 entangled qubits** (QuTech, UNSW, Princeton, University of Tokyo).
- **scalability remains to be demonstrated**.



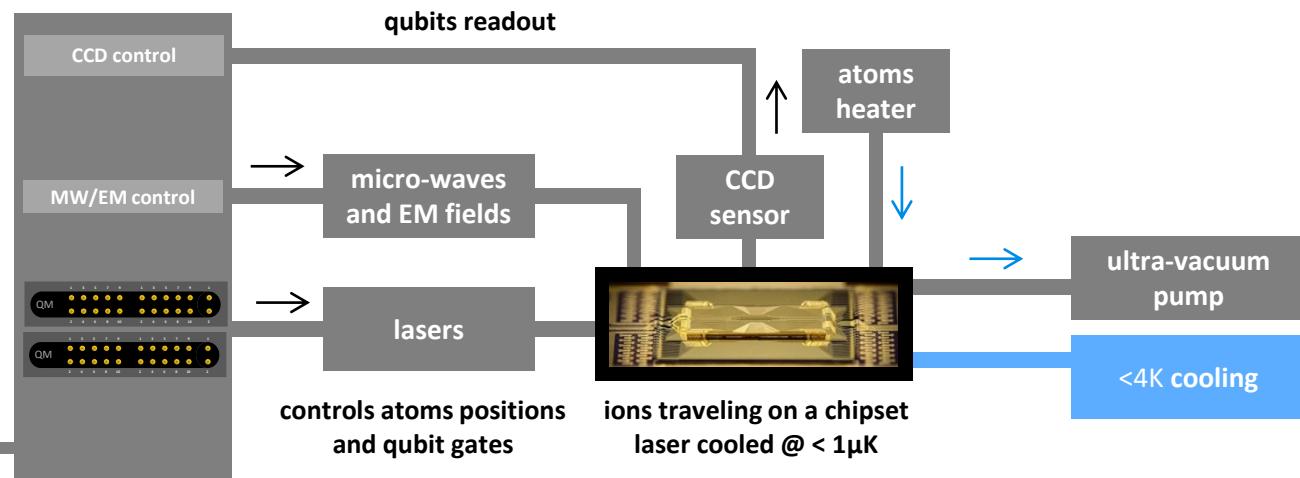
trapped ions qubits

# inside a trapped ions QC

**computing**  
servers, network,  
software, data



**qubits control electronics**  
laser controls, SLM drive,  
CCD readout



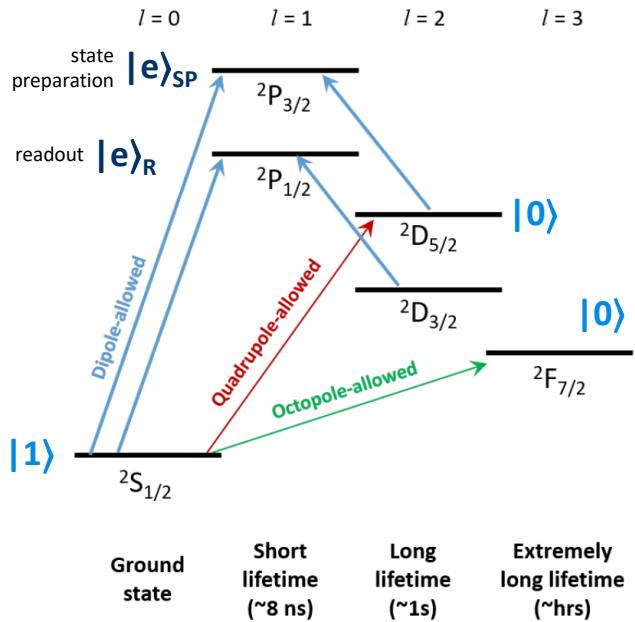
IonQ trapped ions case



# trapped ions types

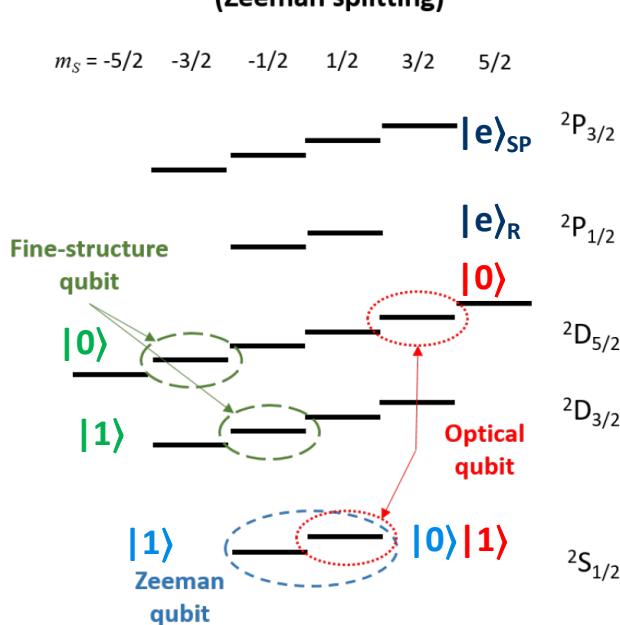
(a)

**Basic Ion Structure  
( $I=0, B=0$ )**



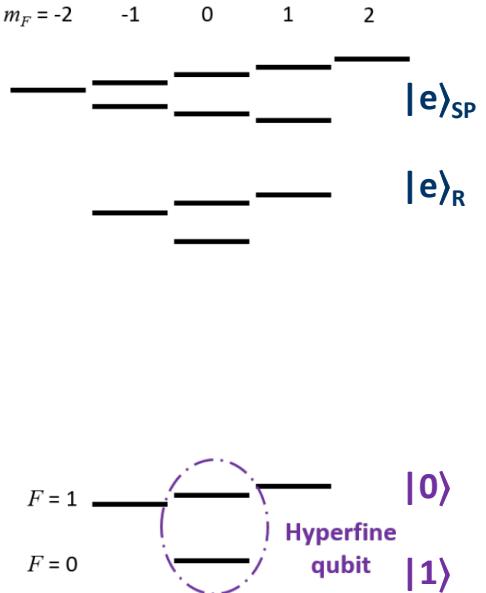
(b)

**$I=0$  Ion Structure  
(Zeeman splitting)**



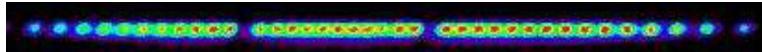
(c)

**$I\neq 0$  Ion Structure ( $I=1/2$ ,  
Hyperfine and Zeeman splitting)**



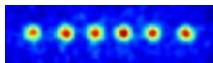
**40  $^{199}\text{Hg}^+$ , University of Colorado Boulder or NIST, ions control, no qubits**

1997



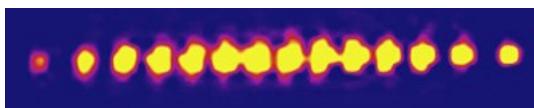
**6 qubits  $^{40}\text{Ca}^+$ , Innsbruck**

<2005



2011

**14 qubits  $^{40}\text{Ca}^+$ , Innsbruck**



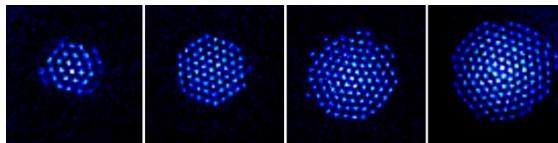
2013

**15  $^{40}\text{Ca}^+$ , Innsbruck + MIT**



2016

**219 beryllium ions, NIST Boulder, Penning traps**



**53 qubits  $^{171}\text{Yb}^+$  (quantum simulation), Maryland University**

2017



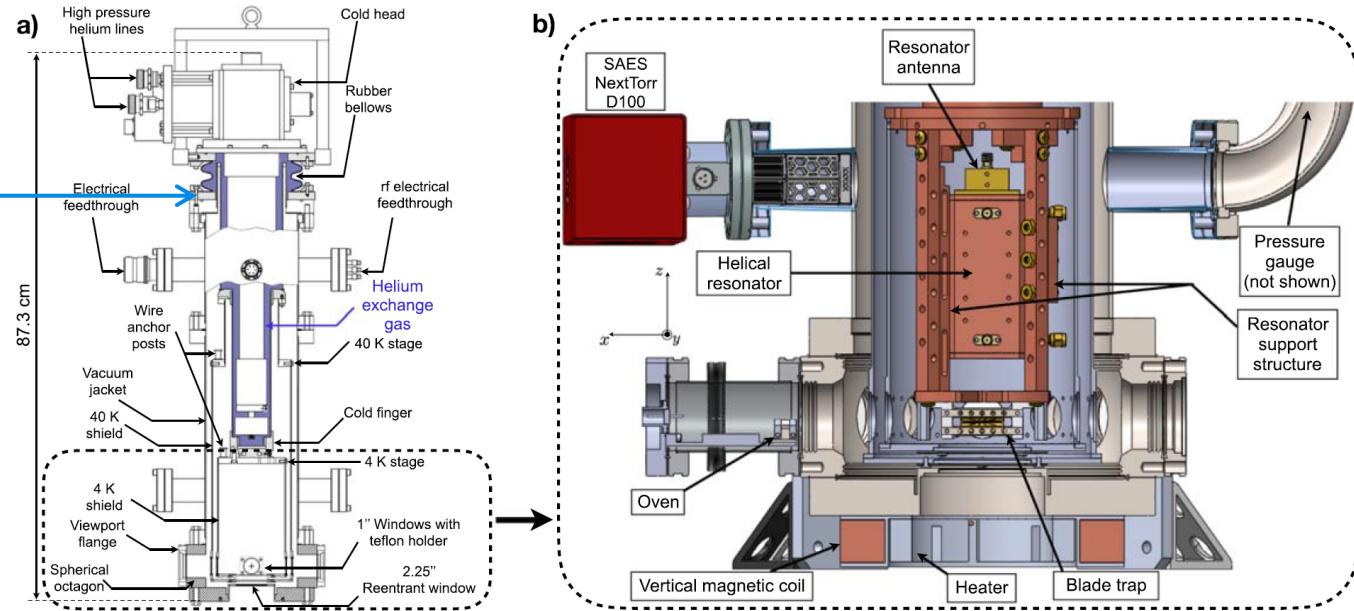
**121 qubits  $^{171}\text{Yb}^+$  (quantum simulation), Maryland University**

2019





**SHS SRDK-415D2 pulse tube  
with Sumitomo F-70L  
compressor**



**Figure 1.** Cryogenic vacuum apparatus. (a) Side view section of the cryostat (courtesy of Janis Inc). (b) Cross section view of the lower section, 90° rotated with respect to (a). The vertical magnetic coil is mounted on the bottom of the reentrant window flange. An aluminium fixture with heaters held on it is designed to rest in the coil's inner diameter in order to avoid water condensation on the outside face of the recessed window, when the apparatus is at 4 K.

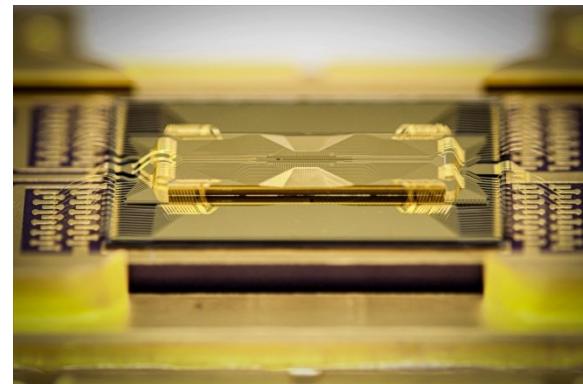
source : Cryogenic trapped-ion system for large scale quantum simulation, Christopher Monroe et al, 2018 (17 pages).



# IONQ

2015

\$432M+ \$650M SPAC



Maryland and Duke Universities spin-off launched by Christopher Monroe  
laser controlled gates

11 qubits online in AWS, Microsoft and Google clouds

32 qubits with a large quantum volume of  $2^{22}$  reached in 2020 (not peer reviewed)

long coherence time and good qubits fidelity

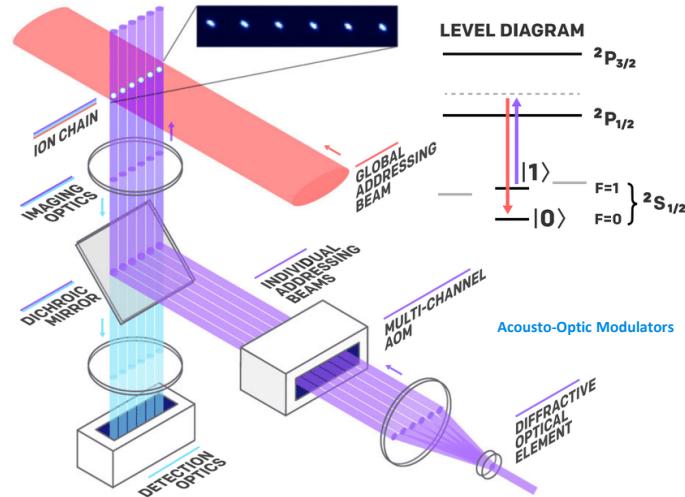
excellent qubit connectivity thanks to phonons

available on Microsoft and Amazon cloud services

switch from ytterbium to baryum in 2022

slow gates

hard to scale, planning to network several tiny units with photons interconnect





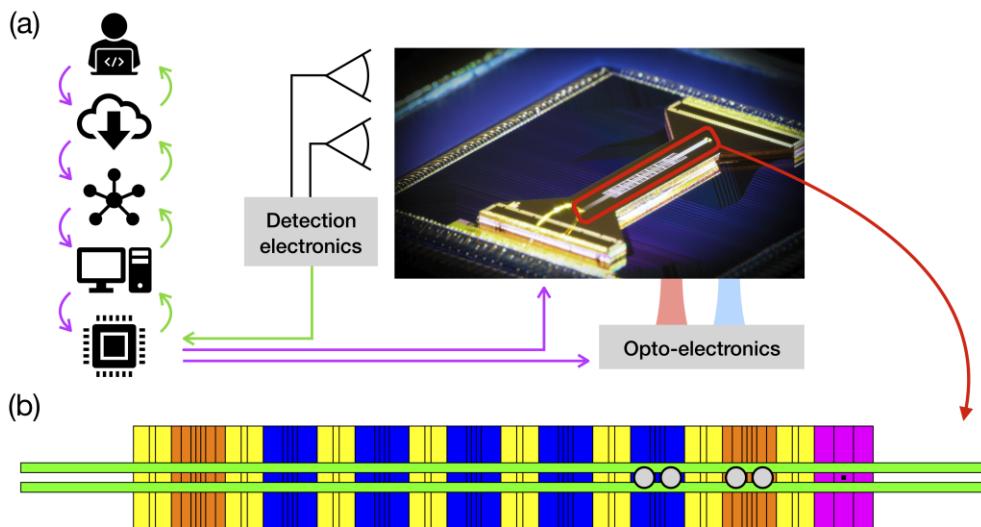
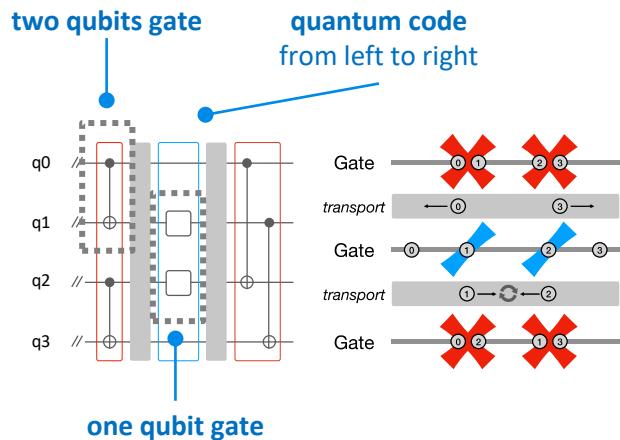
## QUANTINUUM

2D trapped ions announced in march 2020

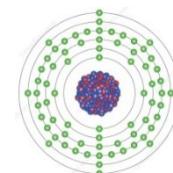
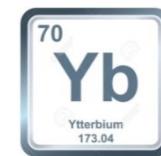
4 qubits (3/2020) to 12 qubits (4/2022)

better scalability prospects

HQS spin-off and merger with CQC (UK) announced in June 2021, becoming Quantinuum



- ions are positioned by pairs on the outer band for two qubits operations
- ions are moving in this zone, as ytterbium-baryum atoms pairs
- ions are positioned in the center lane for single qubit gates
- physical SWAP operation between ions 2 and 3
- ions are cooled before each two qubit gate



# HONEYWELL QUANTUM SOLUTIONS

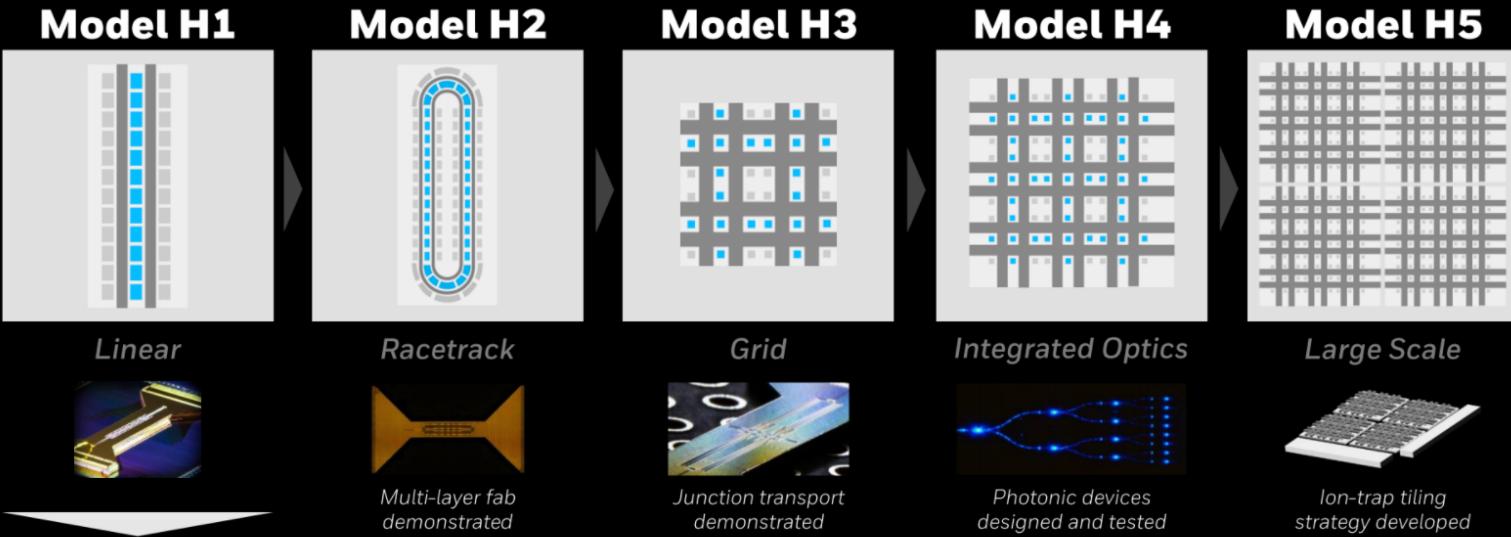
## GENERATIONAL ROADMAP

Noisy Intermediate-Scale Quantum (NISQ) Era

2020

2030

Fault-Tolerant Quantum Computing

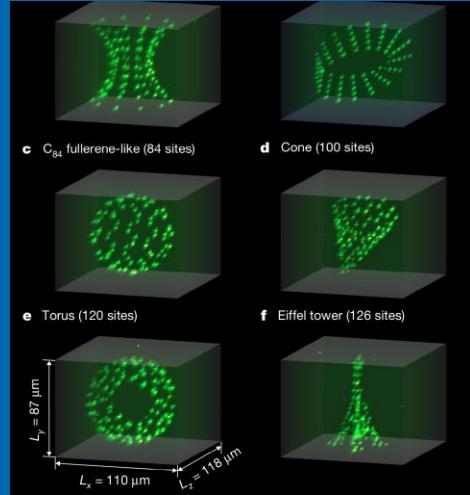


- 10 → 40 Qubits
- 2Q Fidelity: ≥99.5%
- All-to-all connectivity
- Conditional quantum logic
- Mid-circuit measurement
- Qubit reuse
- Massive scaling of physical qubits and computing power
- Ion trap fabrication in Honeywell's foundry
- Key enabling technologies already demonstrated for generational upgrades

# trapped ions qubits summary

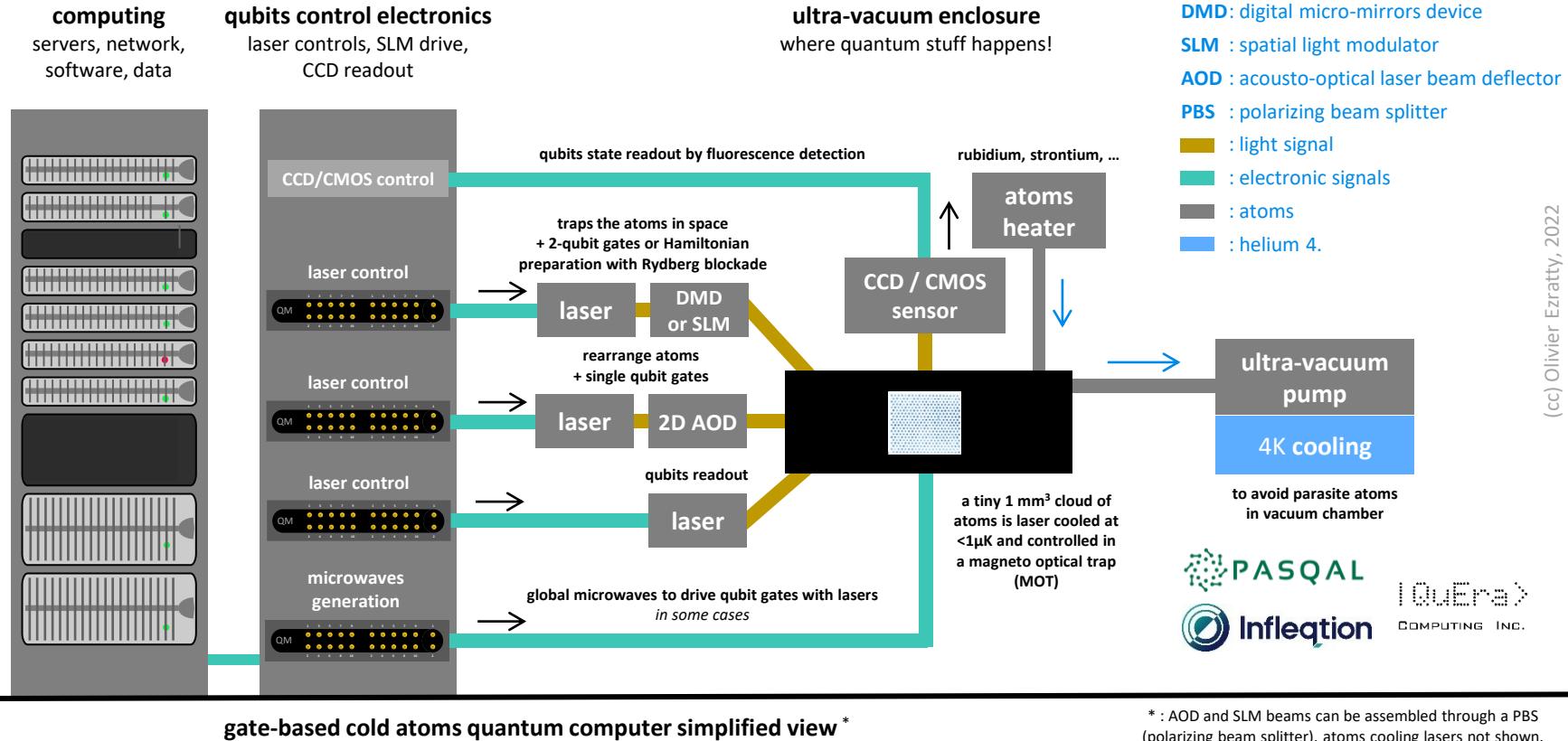
## trapped ions qubits

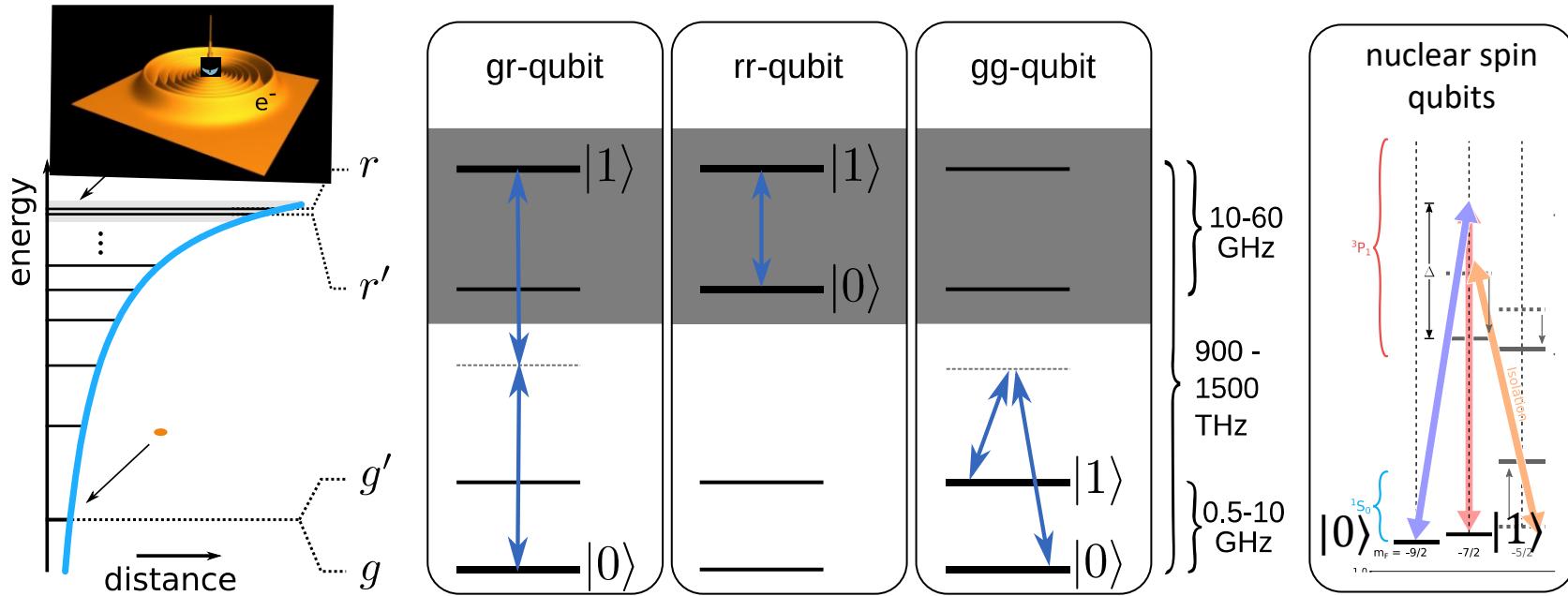
- **identical ions** => no calibration required like with superconducting/electron spin qubits.
- **good qubits stability** with best in class low error rate.
- **long coherence time** and high ratio between coherence time and gate time => supports deep algorithms in number of gates.
- **entanglement** possible between all qubits on 1D architecture. It speeds up computing.
- works at **4K to 10K** => simpler cryogeny than for superconducting/electron spins.
- **easy to entangle ions with photons** for long distance communications.
- **relatively slow computing** due to slow quantum gates which may be problematic for deep algorithms.
- **unproven scalability options beyond 50 qubits** (ions shuttling, 2D architectures, photon interconnect).
- **entanglement doesn't seem to scale well with a large number of ions.**



# neutral atoms qubits

# with a neutral atoms quantum computer





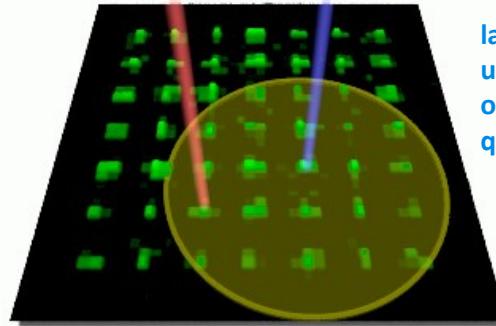
qubit type	ground-Rydberg	Rydberg-Rydberg	ground-ground	nuclear spin
transitions	UV laser or visible/IR lasers	microwaves	microwaves and optical lasers	2 optical photons Raman transition
$T_2^*$	2 to 100 $\mu$ s	22 $\mu$ s	3.5 ms	42 s
vendors	<b>Caltech</b>  <b>PASQAL</b> <sup>(1)</sup> <b>IQuEra</b> <sup>(1)</sup> <small>COMPUTING INC.</small>	 <b>PASQAL</b> <sup>(1)</sup> <b>IQuEra</b> <sup>(1)</sup> <small>COMPUTING INC.</small>	 <b>Inflection</b>  <b>PASQAL</b> <sup>(2)</sup> <b>IQuEra</b> <sup>(2)</sup> <small>COMPUTING INC.</small>	 <b>ATOM</b> <small>COMPUTING</small>

(1): in quantum simulation mode  
(2): in gate-base mode

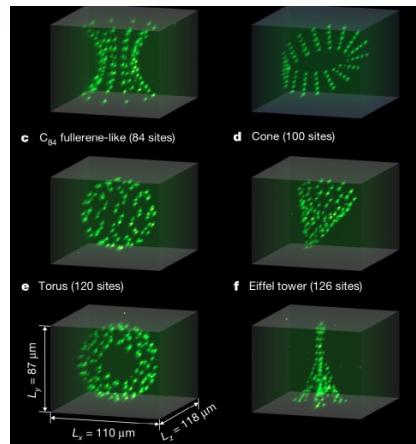
schema source: Quantum simulation and computing with Rydberg-interacting qubits by Manuel Agustin Morgado and Shannon Whitlock, December 2020 and additions by Olivier Ezratty, 2022.

laser  
pulse P2

laser pulses  
P1 and P3

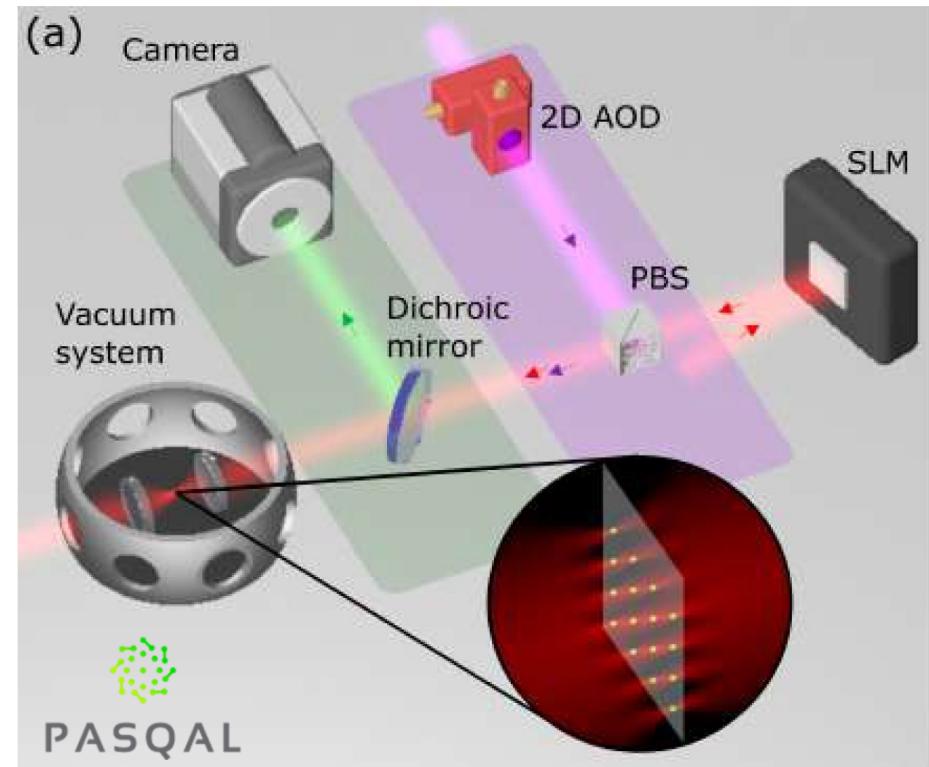


laser pulses are  
used to create  
one and two  
qubit gates

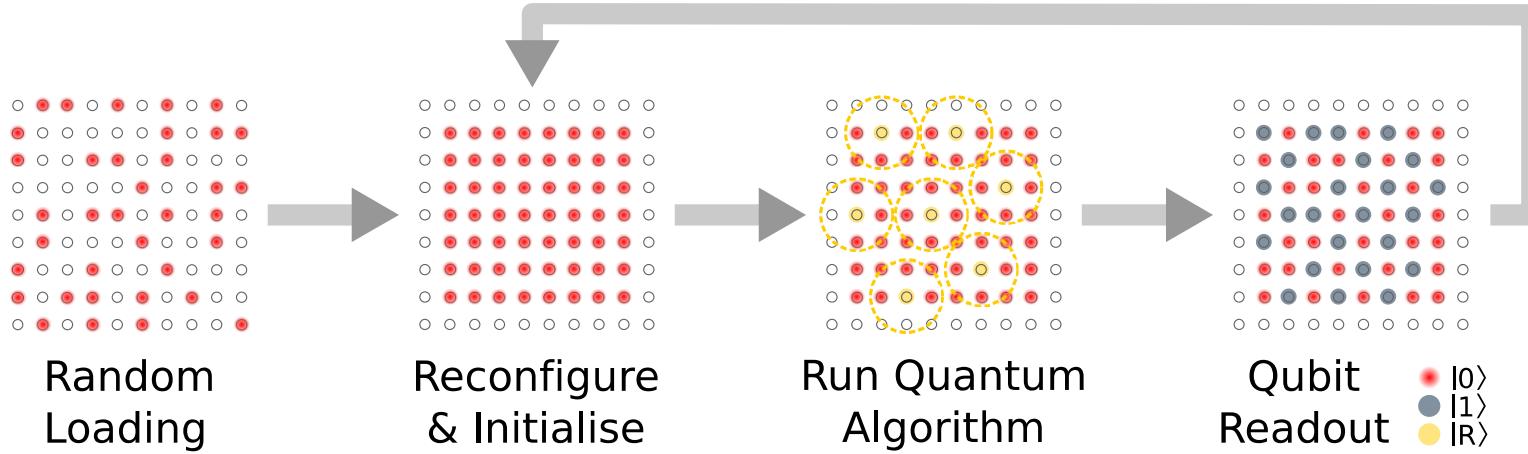


qubits can be  
arranged in 3D  
networks

using SLM (high-resolution phaser) illuminated by a laser to control atoms  
and readout done with fluorescence and a CMOS or CCD image sensor

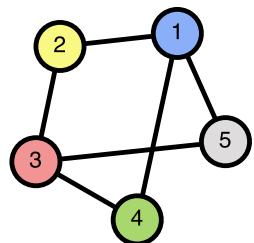


PASQAL

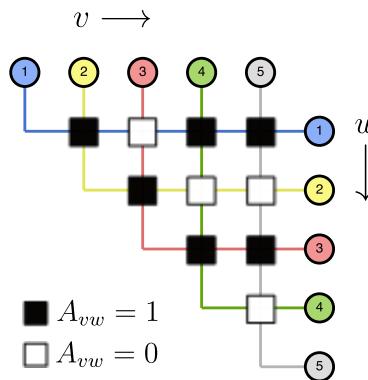


**Figure 2.** Schematic of a Rydberg array quantum computer. Atoms are initially loaded stochastically, followed by rearrangement to achieve a defect free qubit register. Coherent excitation to Rydberg states allows implementation of quantum algorithms exploiting long-range interactions to couple neighbouring qubits, followed by state-selective readout which is repeated many times to tomographically reconstruct the output state.

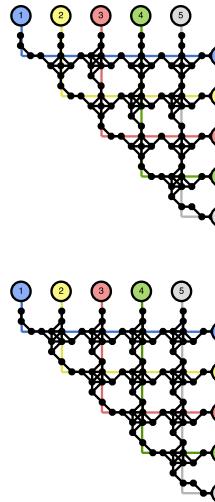
(a) Problem Graph



(b) Arbitrary Connectivity

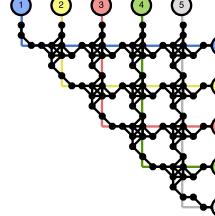


(c)



Maximum  
Independent Set

(d)

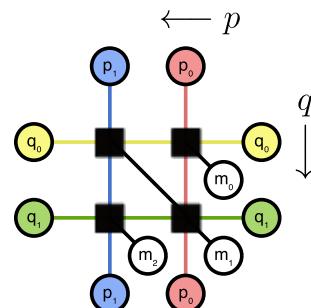


QUBO / Ising

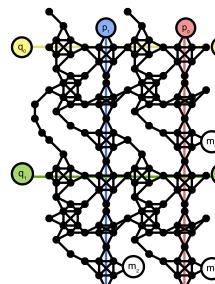
(e) Factoring Problem

$$m = p \cdot q$$
$$\sum_{i=0}^{n-1} 2^i m_i = \sum_{i,j} 2^{i+j} p_i q_j$$

(f) Arbitrary Connectivity



(g)



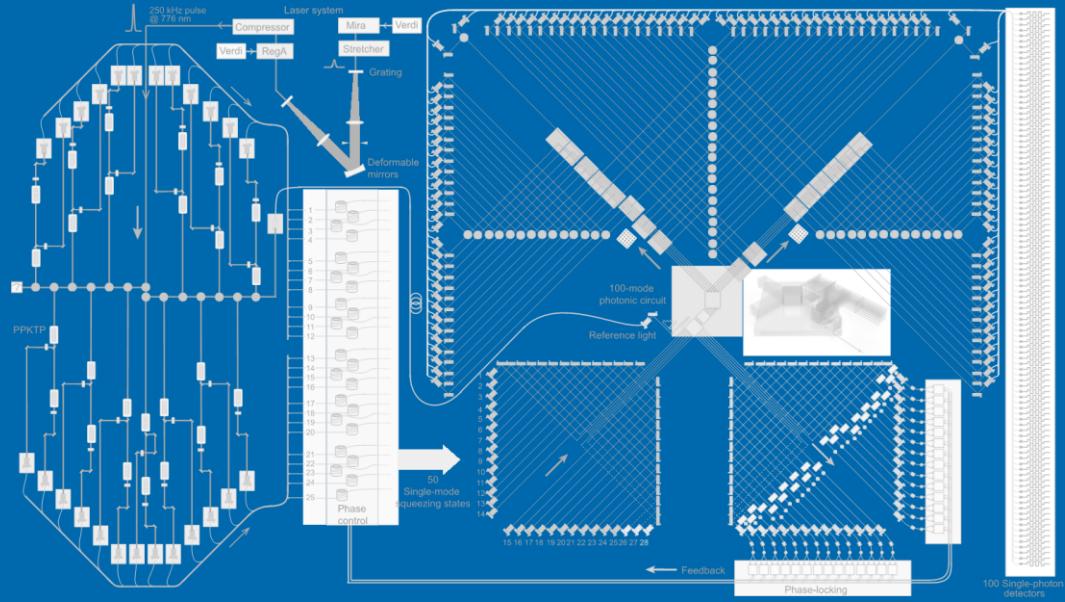
Integer  
Factorization

# neutral atoms qubits summary

## cold atoms qubits

- long qubit **coherence time and fast gates**.
- **operational systems** with 100-300 atoms.
- **identical atoms**, that are controlled with the same laser and micro-wave frequencies (but dual-elements architectures are investigated).
- works in both **simulation** and **gate-based** paradigms.
- no need for specific **integrated circuits**.
- uses **standard apparatus**.
- low **energy consumption**.

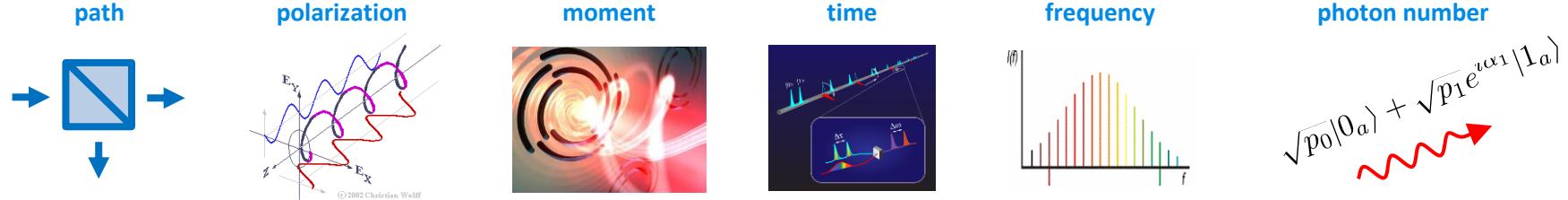
- adapted to **quantum simulations** more than to **universal gates computing**.
- crosstalk between qubits that can be mitigated with two-elements atom architectures.
- not yet operational QND (quantum non demolition) measurement that is required for QEC and FTQC.
- hard to implement with gate-based model.



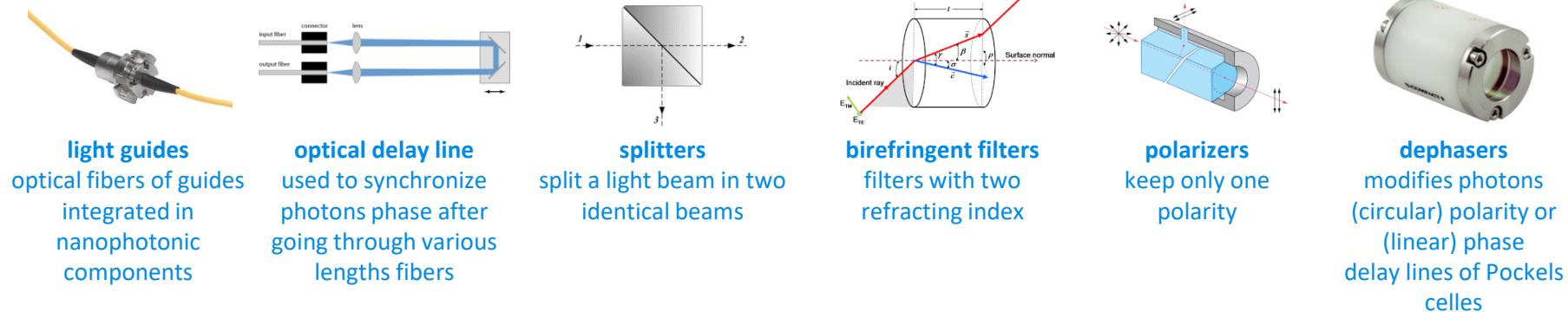
# photon qubits

# photons qubits types and tools

## qubits



## instrumentation

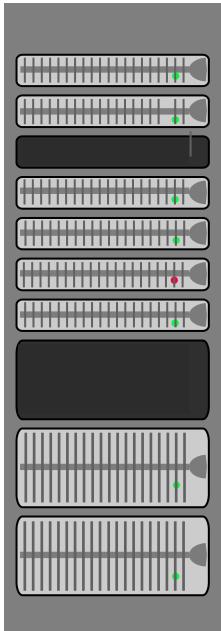


# DV and CV photon qubits

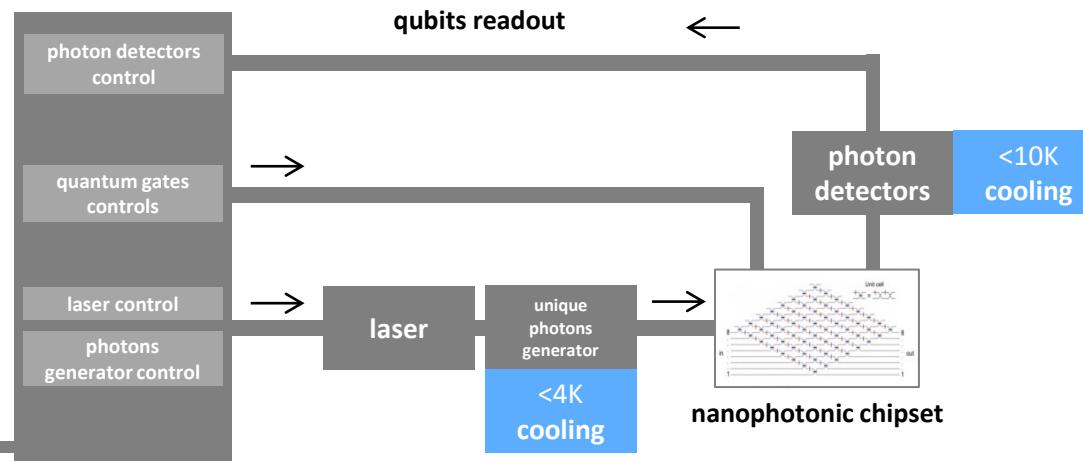
	discrete variables	continuous variables	boson sampling
quantum information	discrete degree of freedom of a photon Fock states: $ 0\rangle,  1\rangle,  2\rangle \dots$ single or many photon properties	quadrature of a light field coherent states, qumodes, spectral and time modes	multimode photons
photon sources	single indistinguishable photon sources	entangled photons sources squeezed states, ...	unique photons source
representation	density matrix	Wigner function	permanent
gates	KLM model, MZI (Mach-Zehnder Interferometer) gates	determinist gates modes measurement gaussian and non gaussian gates	MZI and interferometer
photon detectors	photon counters /detectors APD, SNSPD, VLPC, TES	homodyne and heterodyne detectors	single photons detectors
players	$\Psi$ PsiQuantum  QUANDELA  ORCA Computing  DUALITY QUANTUM PHOTONICS 		 

# with a photon qubits quantum computer

**computing**  
servers, network,  
software, data



**qubits control electronics**  
laser, unique photon  
generator, quantum gates,  
photons readout



Quandela case

**nanophotonic chipset**  
where quantum computation is done

$\Psi$  PsiQuantum



QUANDELA



(cc) Olivier Ezratty, 2023

[Subscribe](#)[Latest Issues](#)

Cart 0

[Sign In](#) | [Stay Informed](#)[CORONAVIRUS](#)[THE SCIENCES](#)[MIND](#)[HEALTH](#)[TECH](#)[SUSTAINABILITY](#)[VIDEO](#)[PODCASTS](#)[OPINION](#)[PUBLICATIONS](#) Q

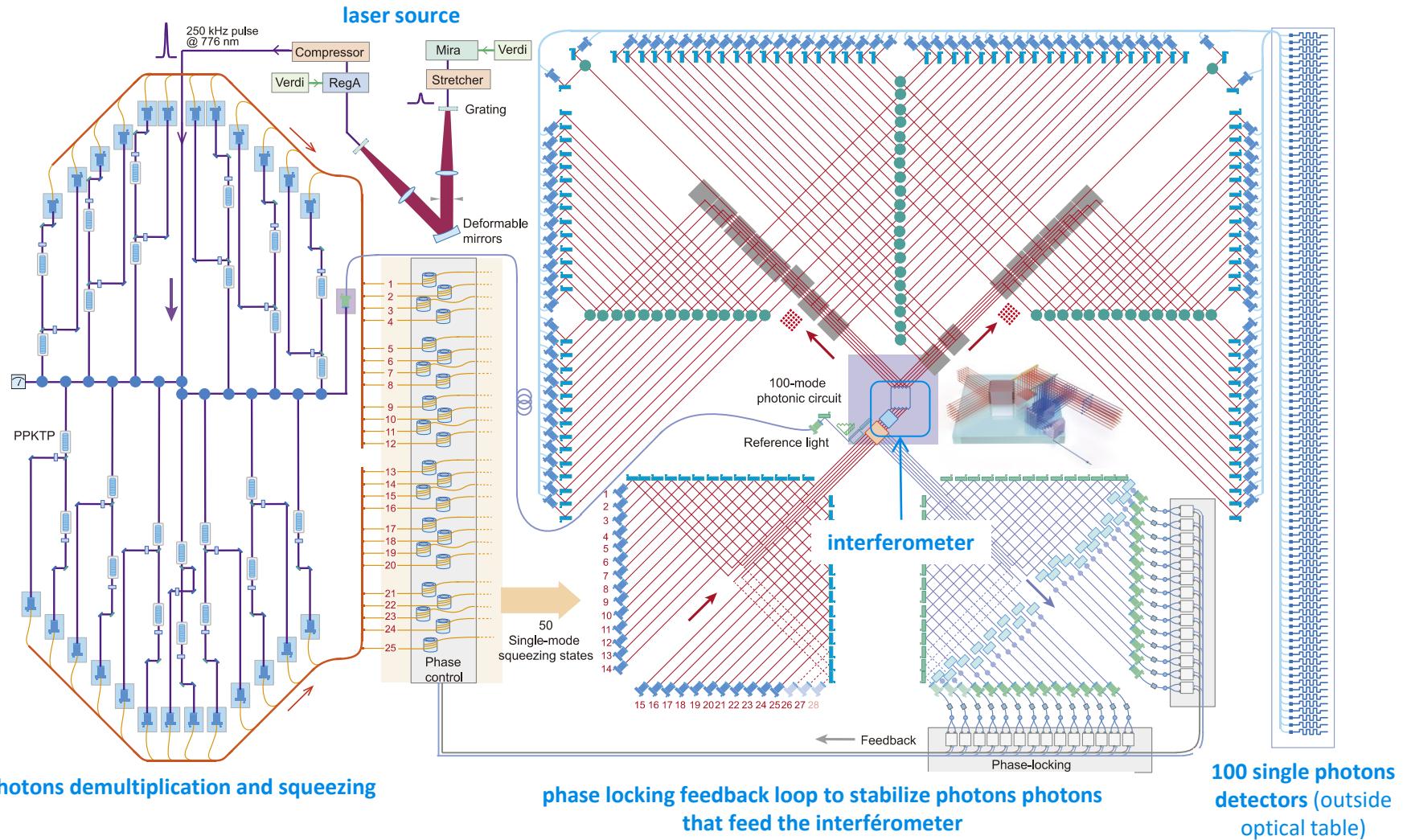
PHYSICS

# Light-based Quantum Computer Exceeds Fastest Classical Supercomputers

The setup of lasers and mirrors effectively “solved” a problem far too complicated for even the largest traditional computer system

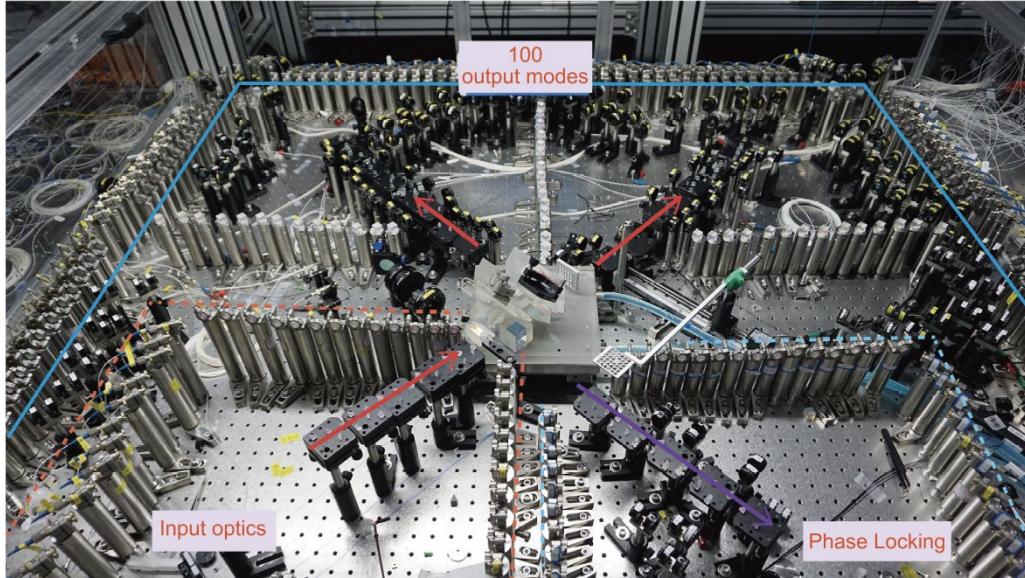
---

By Daniel Garisto on December 3, 2020



**warning: at this point in time, the device is not (yet) programmable**

**to be programmable, photon qubits should be prepared in differentiated states before entering the interferometer**



**Supplementary Figure S14 |** Schematic diagram (A) and photograph (B) of our photonic network. The experimental setup is built on an optical table with an area about 3 square meters. In the input optics region, 25 TMSSs are injected into the photonic network. Correspondingly, at lower right, 25 phase-locking light is collected. The output modes of our photonic network are separated to 100 spatial modes by using mini-mirrors and PBSs.

## Using Gaussian Boson Sampling to Find Dense Subgraphs

Juan Miguel Arrazola\* and Thomas R. Bromley†  
*Xanadu, 372 Richmond Street W, Toronto, Ontario M5V 1X6, Canada*

Boson sampling devices are a prime candidate for exhibiting quantum supremacy, yet their application for solving problems of practical interest is less well understood. Here we show that Gaussian boson sampling is NP-hard for finding the densest  $k$ -subgraph of a graph  $G$ , which is the NP-hard problem of determining the maximum density of a subgraph of size  $k$ . We propose enhanced versions of the random search and simulated annealing algorithms and apply them through numerical simulations of GBS to identify the densest subgraph of a 30 vertex graph.

Quantum algorithms are often designed with the assumption that they can access the full power of universal quantum computation. However, presently developing quantum devices have limited resource capabilities and are not fault-tolerant. Their emergence has motivated a reexamination of methods for designing quantum algorithms, with the focus now on harnessing the computational power of small-scale, noisy quantum computers. Candidate algorithms for near-term devices include quantum simulators for many-body physics [1, 2], variational algorithms [3–6], quantum approximate optimization algorithms [7, 8], and machine learning on hybrid devices [9–13].

Boson sampling is a limited model of quantum computation given by passing photons through a linear interferometer and observing their output configurations [14]. Significant efforts have been performed to implement boson sampling [15–18], leading to the proposal of related models such as scatterhost boson sampling [19–21] and Gaussian boson sampling [22, 23] that are more suitable for experimental realizations. Moreover, boson sampling devices are in principle capable of performing tasks that cannot be efficiently simulated on classical computers, a feature that has made them a leading candidate for challenging the extended Church-Turing thesis. In fact, the primary objective of implementing boson sampling has so far been to demonstrate quantum supremacy, leaving the real-world application of such devices underdeveloped. A notable exception is the use of Gaussian boson sampling for efficiently calculating the vibronic spectra of molecules, [24–26], which provided the first clue of the usefulness of this platform.

In this work, we show that Gaussian boson sampling (GBS) can be used to enhance classical stochastic algorithms for the densest  $k$ -subgraph (DkS) problem. The DkS problem is NP-Hard [27] and defined through the following optimization task: given a graph  $G$  with  $n$  vertices, find the subgraph of  $k < n$  vertices with the largest density. Among subgraphs with a fixed number of vertices, the density and the number of edges are equivalent quantities, and we hence refer to both interchangeably throughout this manuscript. Beyond its fundamental in-

terest in mathematics and theoretical computer science, the DkS problem has a natural connection to clustering problems with the goal of finding highly correlated subsets of data. Clustering has applications in a wide range of fields such as data mining [28–31], bioinformatics [32, 33], and finance [34].

Our approach uses a technique from Ref. [35] to encode a graph into the GBS paradigm. Here, the probability of observing a given photon configuration is proportional to the number of perfect matchings of the corresponding subgraph. We highlight a correspondence between the number of perfect matchings in a subgraph and its density, meaning that a suitably programmed GBS device will prefer to output dense subgraphs. Our results are in line with those in a companion paper [36] showing that the stochastic element of our heuristics for the DkS problem, i.e., time approximation schemes, are better suited for the DkS problem [37], certain worst-case superpolynomial runtimes may be avoided.

*Applying GBS to the DkS problem.*—The important concepts of GBS are first briefly reviewed. In GBS, photon-number detection is performed on a multi-mode Gaussian state [22, 23, 38]. For an  $n$ -mode system, we denote the possible outputs of GBS by vectors  $S = (s_1, s_2, \dots, s_n)$ , where  $s_i$  is the number of photons detected in output mode  $i$ . It was shown in Ref. [22] that the probability of observing an output pattern  $S$  is

$$P(S) = |\sigma_Q|^{-\frac{1}{2}} \frac{\text{Haf}(\mathcal{A}_S)}{s_1! s_2! \dots s_n!}, \quad (1)$$

where  $\sigma_Q = \sigma + 1_{2n}/2$ ,  $\sigma$  is the  $(2n \times 2n)$ -dimensional covariance matrix of the  $n$ -mode Gaussian state, and  $\mathcal{A}_S$  is a submatrix of  $\mathcal{A} = \begin{pmatrix} 0 & 1_n \\ 1_n & 0 \end{pmatrix} [\mathbb{1}_{2n} - \sigma_Q^{-1}]$  fixed by

## dense subgraphs search

## useful algorithms based on parameterized gaussian boson sampling

arXiv:1412.1412

## Boson Sampling for Molecular Vibronic Spectra

Joonsuk Huh\*, Gian Giacomo Guerreschi, Borja Peropadre, Jarrod R. McClean, and Alán Aspuru-Guzik†  
*Department of Chemistry and Chemical Biology,  
Harvard University, Cambridge, Massachusetts 02138, United States*  
(Dated: December 30, 2014)

Quantum computers are expected to be more efficient in performing certain computations than any classical machine. Unfortunately, the technological challenges associated with building a full-scale quantum computer have not yet allowed the experimental verification of such an expectation. Recently, however, it has become feasible to build a quantum computer that is able to perform calculations on any input. Therefore, the Church-Turing thesis implies that at least some problems can be solved by a quantum computer. In relation to molecular vibronic spectra, the question is whether a boson sampling apparatus would not only answer such inquiries, but also yield a practical tool for difficult molecular computations. Specifically, we show that a boson sampling device with a modified input state can be used to generate molecular vibronic spectra, including complicated effects such as Duschinsky rotations.

### I. INTRODUCTION

Quantum mechanics allows the storage and manipulation of information in ways that are not possible according to classical physics. At a glance, it appears evident that the set of operations characterizing a quantum computer is strictly larger than the operations possible in a classical hardware. This speculation is at the basis of quantum speedups that have been achieved for oracle problems [1, 2]. Particularly significant speedups have been achieved for the prime factorization problem [3], a problem for which no algorithm is currently known. Another application of quantum computers is quantum simulation [4], it has recently been shown that chemical reactions [10] as well as molecular [11] are attractive applications for or all these instances, the realization of a quantum computer would challenge the Extended Church-Turing thesis (ECT), which claims that a Turing machine can efficiently simulate any physically realizable system, and even disprove it if prime factorization was finally demonstrated to be not efficiently solvable on classical machines.

At the same time, the realization of a full-scale quantum computer is a very demanding technological challenge, even if it is not forbidden by fundamental physics. This fact motivated the search for intermediate quantum hardware that could efficiently solve specific computational problems, believed to be intractable with classical machines, without being capable of universal quantum computation. Recently, Aaronson and Arkhipov found that sampling the distribution of photons at the output of a linear photonic network is expected (modulo a few conjectures) to be computationally inefficient for any

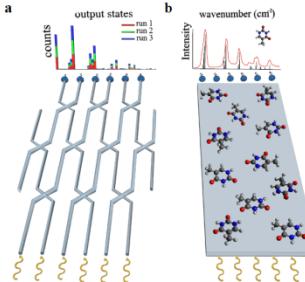


FIG. 1. Pictorial description of boson sampling and molecular vibronic spectroscopy. a, Boson sampling consists of sampling the output distribution of photons obtained from quantum interference inside a linear quantum optical network. b, Vibronic spectroscopy uses coherent light to electronically excite an ensemble of identical molecules and measures the re-emitted (or scattered) radiation to infer the vibrational spectrum of the molecule. We show in this work how the fundamental physical process underlying b is formally equivalent to situation a together with a non-linear state preparation step.

classical computer since it would require the estimation of lots of matrix permanents [12]. On the contrary, this task is naturally simulated by indistinguishable photons injected as input of a photonic network (see the pictorial description of boson sampling in Fig. 1a). While several groups have already realized small-scale versions of boson sampling [13–16], to challenge the ECT one also

\* Email: huh@fas.harvard.edu

† Email: aspuru@chemistry.harvard.edu

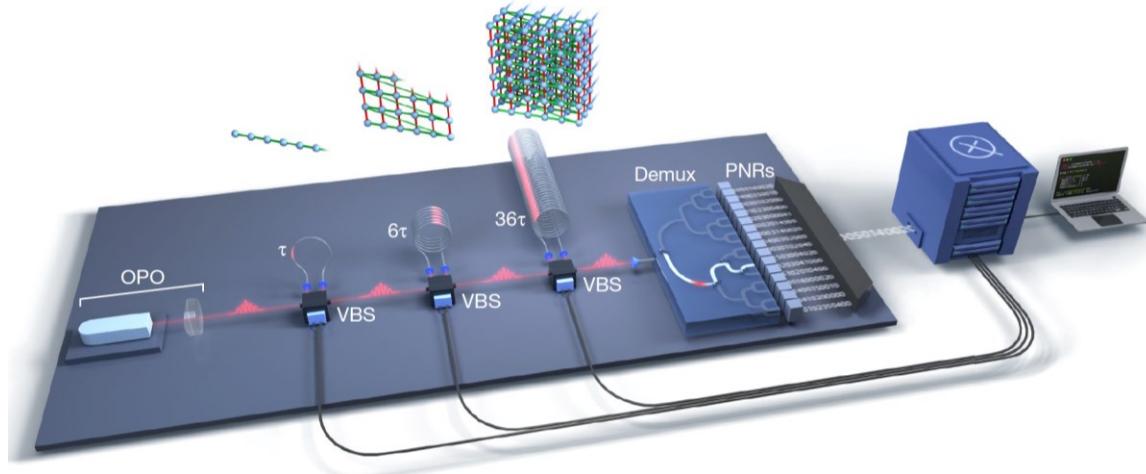


XANADU

first programmable GBS (Gaussian Boson Sampling).

available on AWS.

but not the core product strategy from Xanadu.



## Article

# Quantum computational advantage with a programmable photonic processor

[Quantum computational advantage with a programmable photonic processor](#) by Lars S. Madsen et al, Xanadu, June 2022 (11 pages) and the earlier and more detailed [Quantum Computational Advantage via High-Dimensional Gaussian Boson Sampling](#) by Abhinav Deshpande et al, February 2021 and January 2022 (24 pages).

<https://doi.org/10.1038/s41586-022-04725-x>

Received: 12 November 2021

Accepted: 5 April 2022

Published online: 1 June 2022

Lars S. Madsen<sup>1,3</sup>, Fabian Laudenbach<sup>1,3</sup>, Mohsen Falamarzi, Askarani<sup>1,3</sup>, Fabien Rortais<sup>1</sup>, Trevor Vincent<sup>1</sup>, Jacob F. F. Bulmer<sup>1</sup>, Filippo M. Miato<sup>1</sup>, Leonhard Neuhaus<sup>1</sup>, Lukas G. Helt<sup>1</sup>, Matthew J. Collins<sup>1</sup>, Adriana E. Lita<sup>2</sup>, Thomas Gerrits<sup>2</sup>, Sae Woo Nam<sup>2</sup>, Varun D. Vaidya<sup>1</sup>, Matteo Menotti<sup>1</sup>, Ish Dhand<sup>1</sup>, Zachary Vernon<sup>1</sup>, Nicolás Quesada<sup>1</sup> & Jonathan Lavoie<sup>1</sup>

# Solving Graph Problems Using Gaussian Boson Sampling

Yu-Hao Deng,<sup>1,2,\*</sup> Si-Qiu Gong,<sup>1,2,\*</sup> Yi-Chao Gu,<sup>1,2,\*</sup> Zhi-Jiong Zhang,<sup>1,2</sup> Hua-Liang Liu,<sup>1,2</sup> Hao Su,<sup>1,2</sup> Hao-Yang Tang,<sup>1,2</sup> Jia-Min Xu,<sup>1,2</sup> Meng-Hao Jia,<sup>1,2</sup> Ming-Cheng Chen,<sup>1,2</sup> Han-Sen Zhong,<sup>1,2</sup> Hui Wang,<sup>1,2</sup> Jiarong Yan,<sup>1,2</sup> Yi Hu,<sup>1,2</sup> Jia Huang,<sup>3</sup> Wei-Jun Zhang,<sup>3</sup> Hao Li,<sup>3</sup> Xiao Jiang,<sup>1,2</sup> Lixing You,<sup>3</sup> Zhen Wang,<sup>3</sup> Li Li,<sup>1,2</sup> Nai-Le Liu,<sup>1,2</sup> Chao-Yang Lu,<sup>1,2</sup> and Jian-Wei Pan<sup>1,2</sup>

<sup>1</sup>Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics,  
University of Science and Technology of China, Hefei, Anhui, 230026, China

<sup>2</sup>CAS Centre for Excellence and Synergetic Innovation Centre in Quantum Information and Quantum Physics,  
University of Science and Technology of China, Shanghai, 201315, China

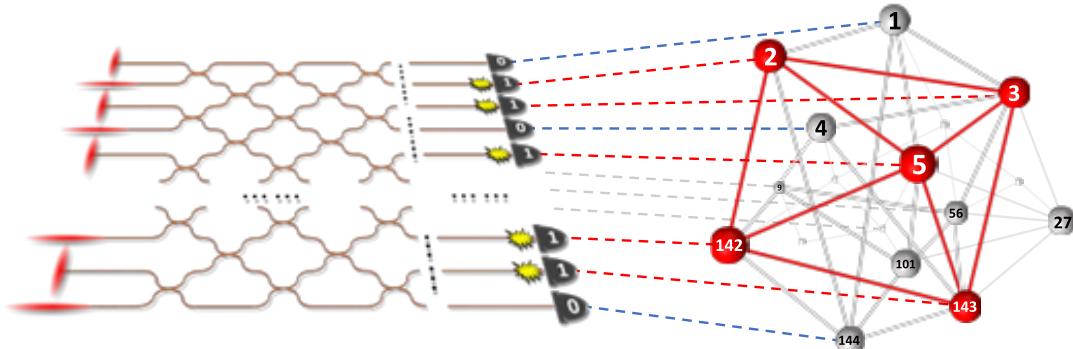
<sup>3</sup>State Key Laboratory of Functional Materials for Informatics,  
Shanghai Institute of Micro system and Information Technology (SIMIT),  
Chinese Academy of Sciences, 865 Changning Road, Shanghai, 200050, China  
(Dated: February 3, 2023)

<https://arxiv.org/abs/2302.00936> February 2023

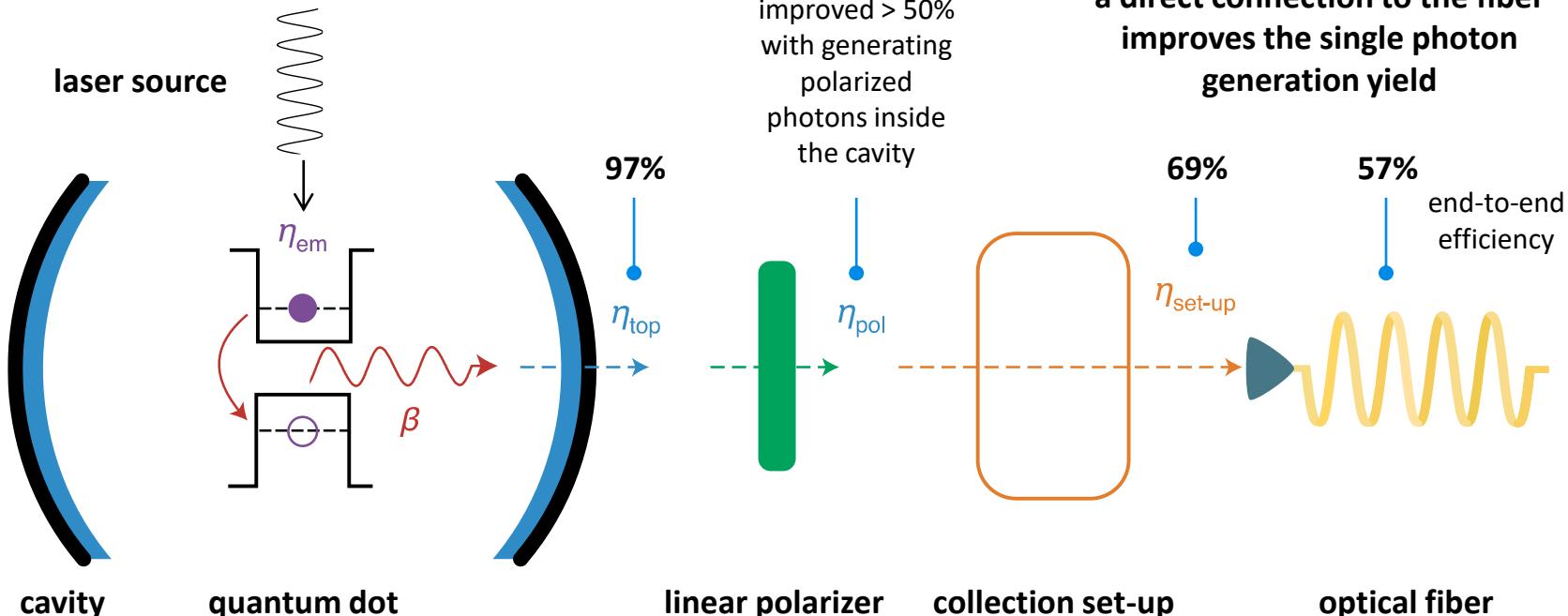
another programmable GBS  
(Gaussian Boson Sampling) in China.

solves graph problems.

comparison made with US DoE  
Frontier supercomputer.



# quantum dot photon source

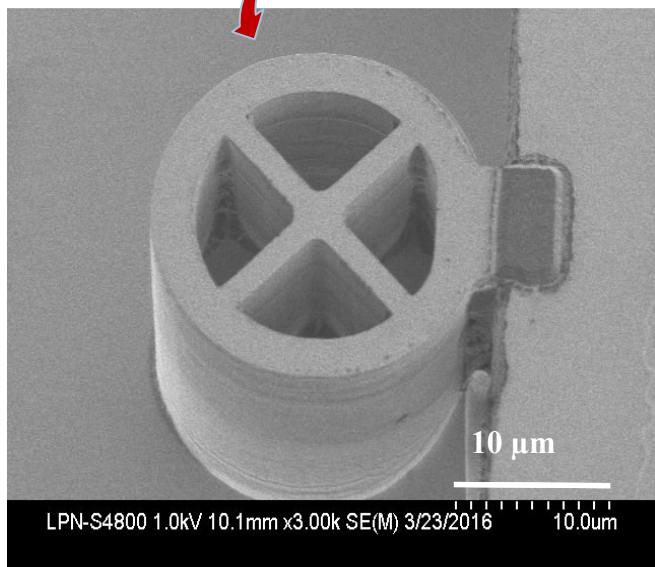


source: The race for the ideal single-photon source is on by Sarah Thomas and Pascale Senellart, Nature Nanotechnology, January 2021

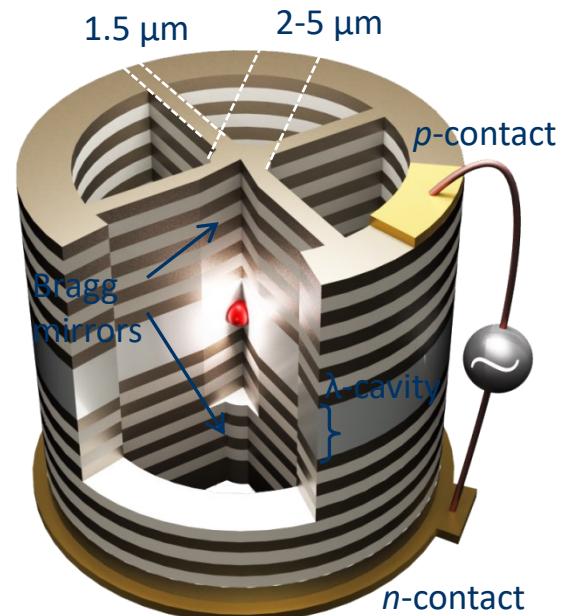
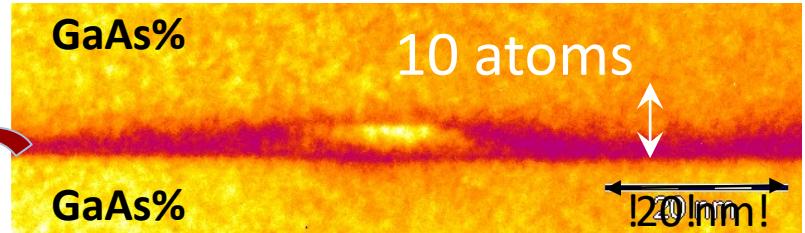
# indistinguishable photon source



Pascale Senellart



Nowak et al, Nat. Com 2014

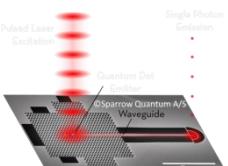


## indistinguishable photons generation

10K

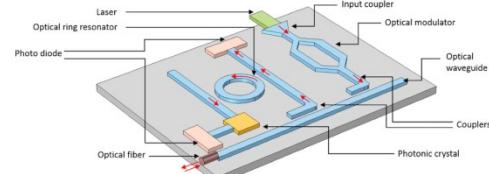
QUANDELA

SPARROW  
QUANTUM



## integrated photonic circuits

300K



## unique photons detectors

2K

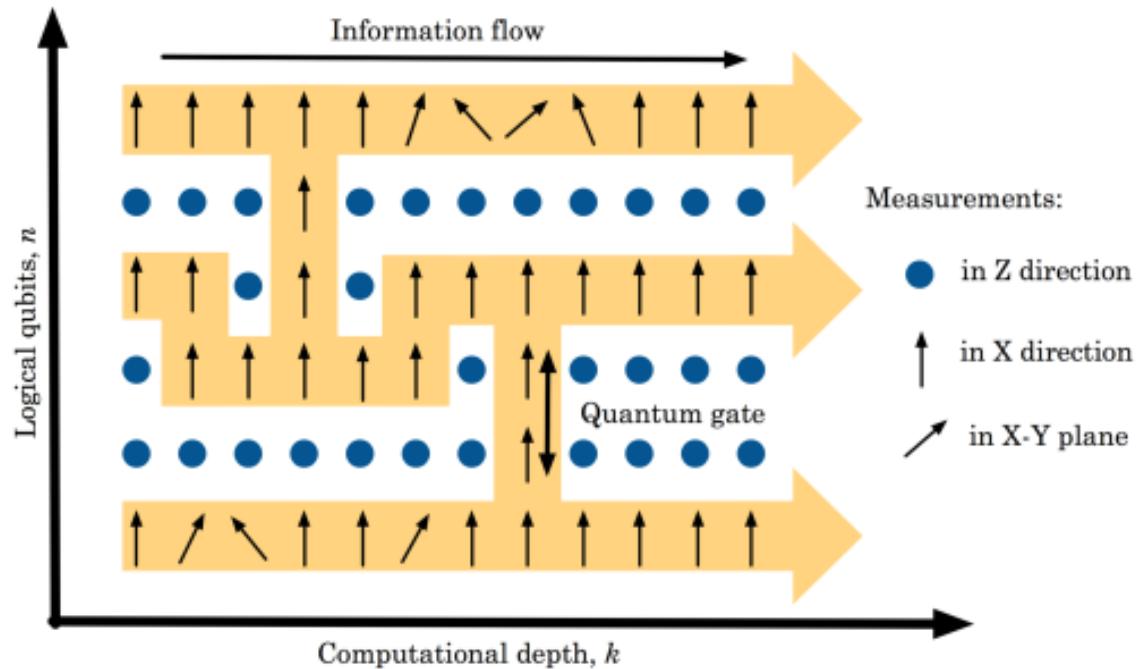


# MBQC

**Measurement Based Quantum Computing (MBQC)** starts with entangling every qubits in a network, often 2D, then to isolate different parts of the network with qubits readouts and X/Z gates

computing can be heavily parallelized

this is useful for implementing quantum gates on photonic qubits where two-qubits gates are difficult to implement and where the number of quantum gates are physically limited



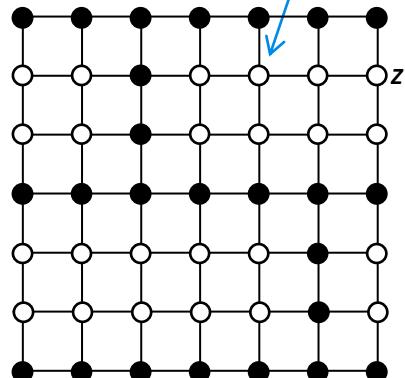
### projective measurement



MBQC is using projective measurements. It combines X, Y or Z gates modifying the qubit state on an orthonormal basis followed by a measurement.

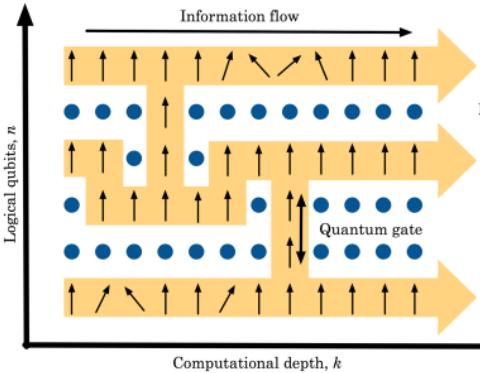
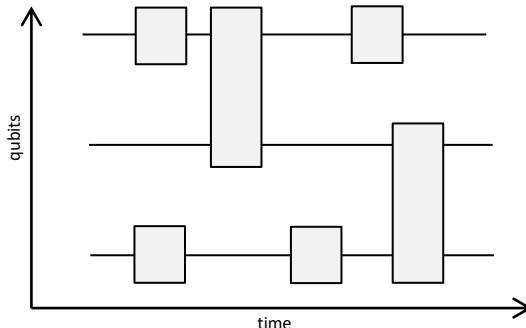
all qubits are prepared as  $(|0\rangle + |1\rangle)/\sqrt{2}$  with a H gate and entangled with Control-Phase (R) gates

measured qubits (no information used)



pre-entangled qubits cluster state preparation

### series of classical quantum gates



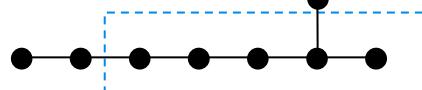
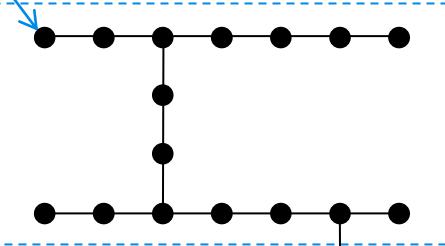
Z projective measurement isolates filaments of qubits which are used to create quantum gates

qubits prepared and measured (ancilae qubits)

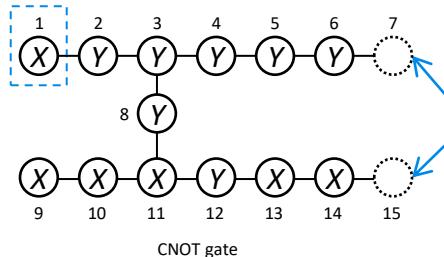
0

transposition in MBQC

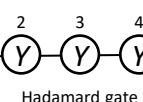
1



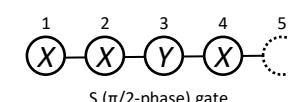
remainder of calculus



classical quantum gates are realized with series of projective measurements



Hadamard gate



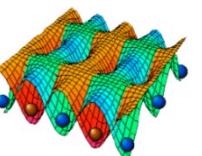
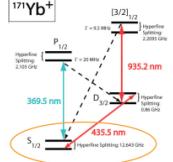
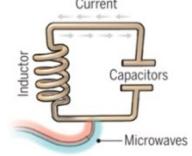
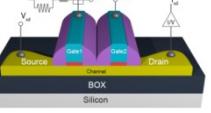
S ( $\pi/2$ -phase) gate

# photons qubits summary

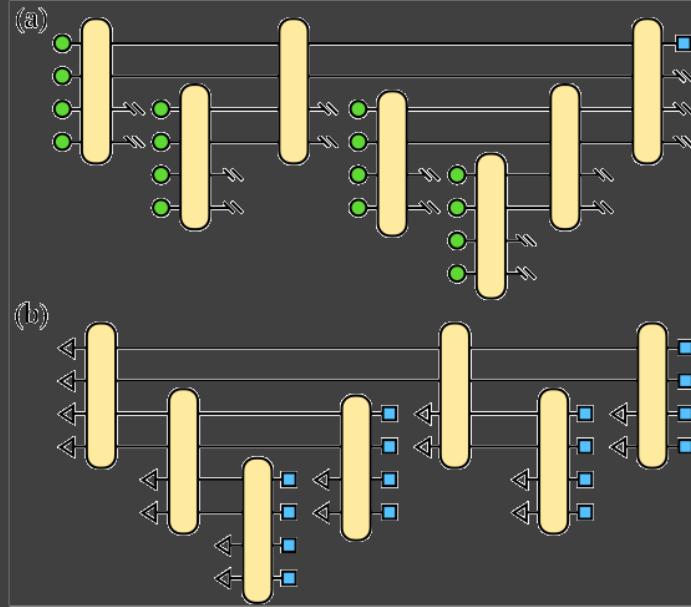
## photons qubits

- **stable qubits** with absence of decoherence.
- qubits processing at **ambiant temperature**.
- **emerging nano-photonic** manufacturing techniques enabling scalability.
- **easier to scale-out** with inter-qubits communications and quantum telecommunications.
- **MBQC/FBQC** circumventing the fixed gates depth computing capacity.

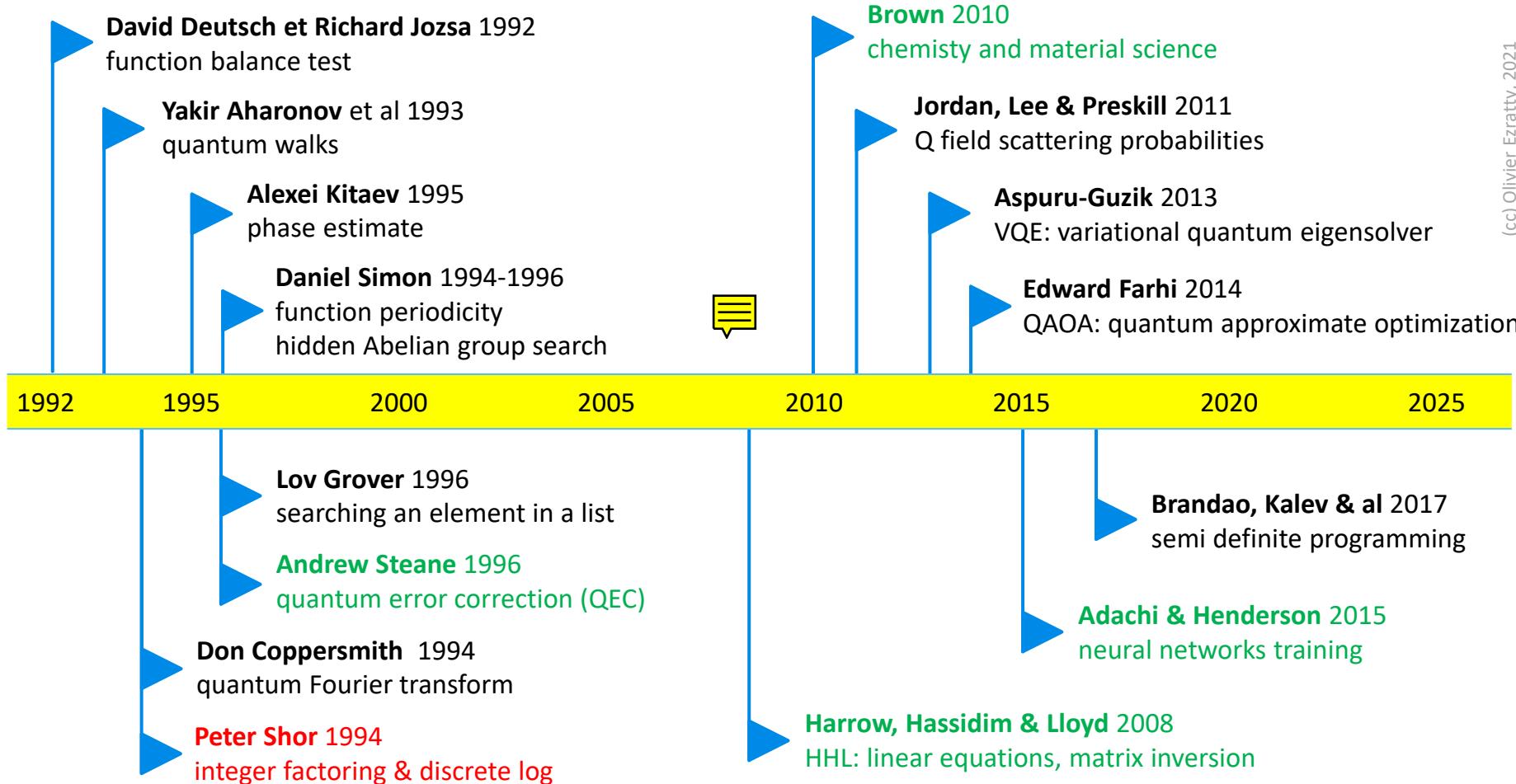
- need to cool photon sources and detectors, but at relatively reasonable temperatures between 2K and 10K, requiring lighweight cryogenic systems.
- **boson sampling based quantum advantage** starts to being programmable but a practival quantum advantage remains to be proven.
- not yet scalable in number of operations due to probabilistic character of quantum gates and the efficiency of photon sources in most paradigms.

	atoms	electrons superconducting & spins	photons			
	 cold atoms	 trapped ions	 superconducting	 silicon		
qubit size	about 1 $\mu\text{m}$ space between atoms	about 1 $\mu\text{m}$ space between atoms	$(100\mu)^2$	$(100\text{nm})^2$	$<(100\text{nm})^2$	nanophotonics waveguides lengths, MZI, PBS, etc
best two qubits gates fidelities	99.4%	99.9%	99.68% (IBM Egret 33 qubits)	>99% (SiGe)	99.2%	98%
best readout fidelity	99.1%	99.9%	99.4%	99% (SiGe)	98%	50%
best gate time	1 ns	100 $\mu\text{s}$	20 ns - 300 ns	$\approx 5 \mu\text{s}$	10-700 ns	<1 ns
best $T_1$	> 1 s	0,2s-10mn	100-400 $\mu\text{s}$	20-120 $\mu\text{s}$	2.4 ms	$\infty$ & time of flight
qubits temperature	< 1mK 4K for vacuum pump	<1mK 4K cryostat	15mK dilution cryostat	100mK-1K dilution cryostat	4K to RT	RT 4K-10K cryostats for photons gen. & det.
operational qubits	324 (Pasqal)	32 (IonQ) 20 (AQT)	127 (IBM) 56-66 (China)	15 (Delft) in SiGe	5 (Quantum Brilliance)-10	216 modes GBS (Xanadu)
scalability	up to 10,000	<50	1000s	millions	100s	100s-1M

these are the best figures of merit, but it doesn't mean a single system in a column has them all!



# quantum algorithms



# Quantum Algorithm Zoo

This is a comprehensive catalog of quantum algorithms. If you notice any errors or omissions, please email me at [stephen.jordan@microsoft.com](mailto:stephen.jordan@microsoft.com). (Alternatively, you may submit a pull request to the [repository](#) on github.) Your help is appreciated and will be [acknowledged](#).

## Algebraic and Number Theoretic Algorithms

**Algorithm:** Factoring

**Speedup:** Superpolynomial

**Description:** Given an  $n$ -bit integer, find the prime factorization. The quantum algorithm of Peter Shor solves this in  $\tilde{O}(n^3)$  time [82, 125]. The fastest known classical algorithm for integer factorization is the general number field sieve, which is believed to run in time  $2^{\tilde{O}(n^{1/3})}$ . The best rigorously proven upper bound on the classical complexity of factoring is  $O(2^{n/4+o(1)})$  via the Pollard-Strassen algorithm [252, 362]. Shor's factoring algorithm breaks RSA public-key encryption and the closely related quantum algorithms for discrete logarithms break the DSA and ECDSA digital signature schemes and the Diffie-Hellman key-exchange protocol. A quantum algorithm even faster than Shor's for the special case of factoring "semiprimes", which are widely used in cryptography, is given in [271]. If small factors exist, Shor's algorithm can be beaten by a quantum algorithm using Grover search to speed up the elliptic curve factorization method [366]. Additional optimized versions of Shor's algorithm are given in [384, 386]. There are proposed classical public-key cryptosystems not believed to be broken by quantum algorithms, cf. [248]. At the core of Shor's factoring algorithm is order finding, which can be reduced to the [Abelian hidden subgroup problem](#), which is solved using the quantum Fourier transform. A number of other problems are known to reduce to integer factorization including the membership problem for matrix groups over fields of odd order [253], and certain diophantine problems relevant to the synthesis of quantum circuits [254].

**Algorithm:** Discrete-log

**Speedup:** Superpolynomial

**Description:** We are given three  $n$ -bit numbers  $a$ ,  $b$ , and  $N$ , with the promise that  $b = a^s \pmod N$  for some  $s$ . The task is to find  $s$ . As shown by Shor [82], this can be achieved on a quantum computer in  $\text{poly}(n)$  time. The fastest known classical algorithm requires time superpolynomial in  $n$ . By similar techniques to those in [82], quantum computers can solve the discrete logarithm problem on elliptic curves, thereby breaking elliptic curve cryptography [109, 14]. A further optimization to Shor's algorithm is given in [385]. The superpolynomial quantum speedup has also been extended to the discrete logarithm problem on semigroups [203, 204]. See also [Abelian hidden subgroup](#).

## Navigation

[Algebraic & Number Theoretic](#)

[Oracular](#)

[Approximation and Simulation](#)

[Optimization, Numerics, & Machine Learning](#)

[Acknowledgments](#)

[References](#)

## Translations

This page has been translated into:

[Japanese](#)

[Chinese](#)

## Other Surveys

For overviews of quantum algorithms I recommend:

[Nielsen and Chuang](#)

[Childs](#)

[Preskill](#)

[Mosca](#)

[Childs and van Dam](#)

[van Dam and Sasaki](#)

[Bacon and van Dam](#)

[Loeff](#)

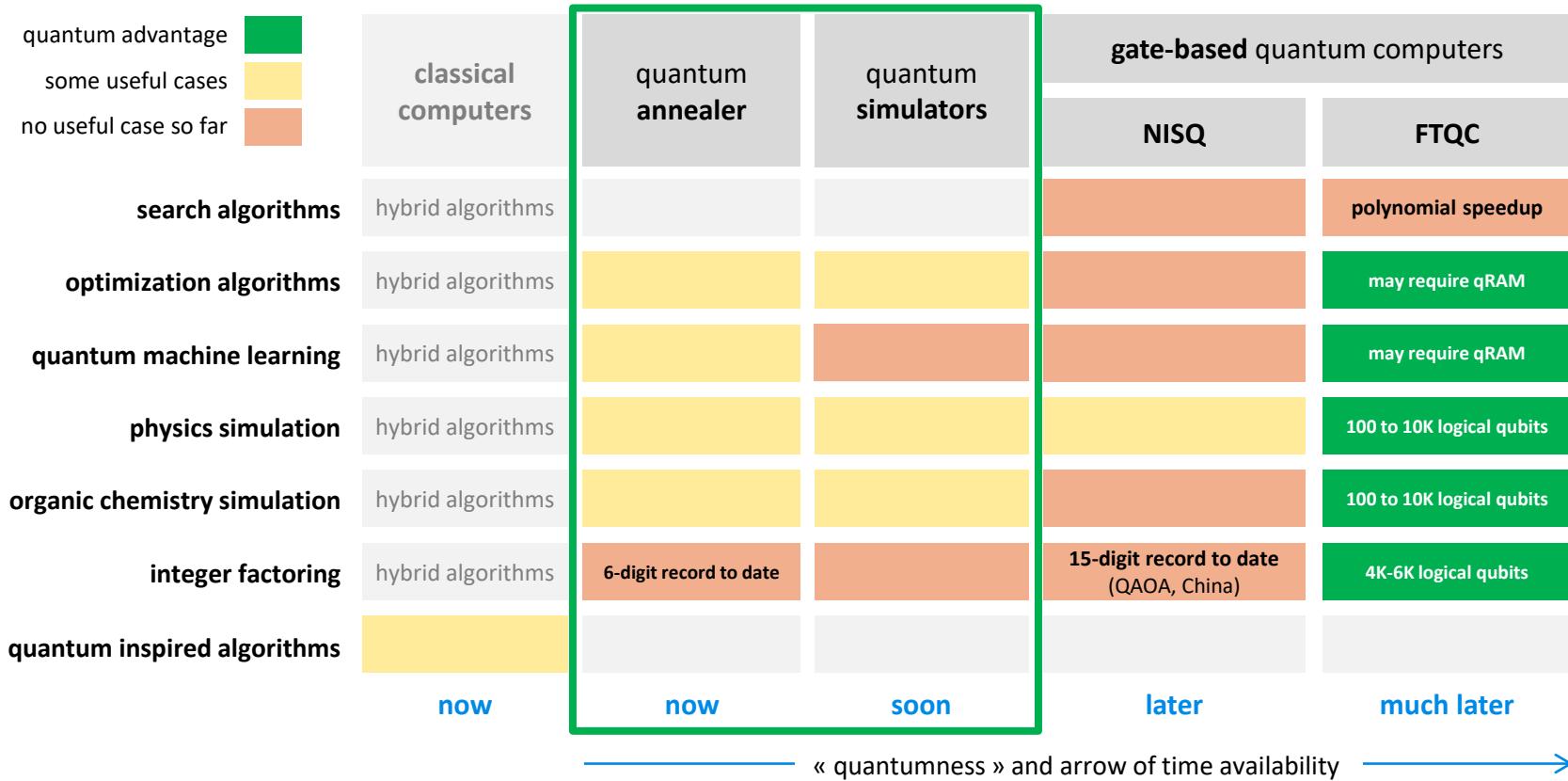
[Montanaro](#)

[Hidary](#)

**430 algorithms  
known in 2021**

## Terminology

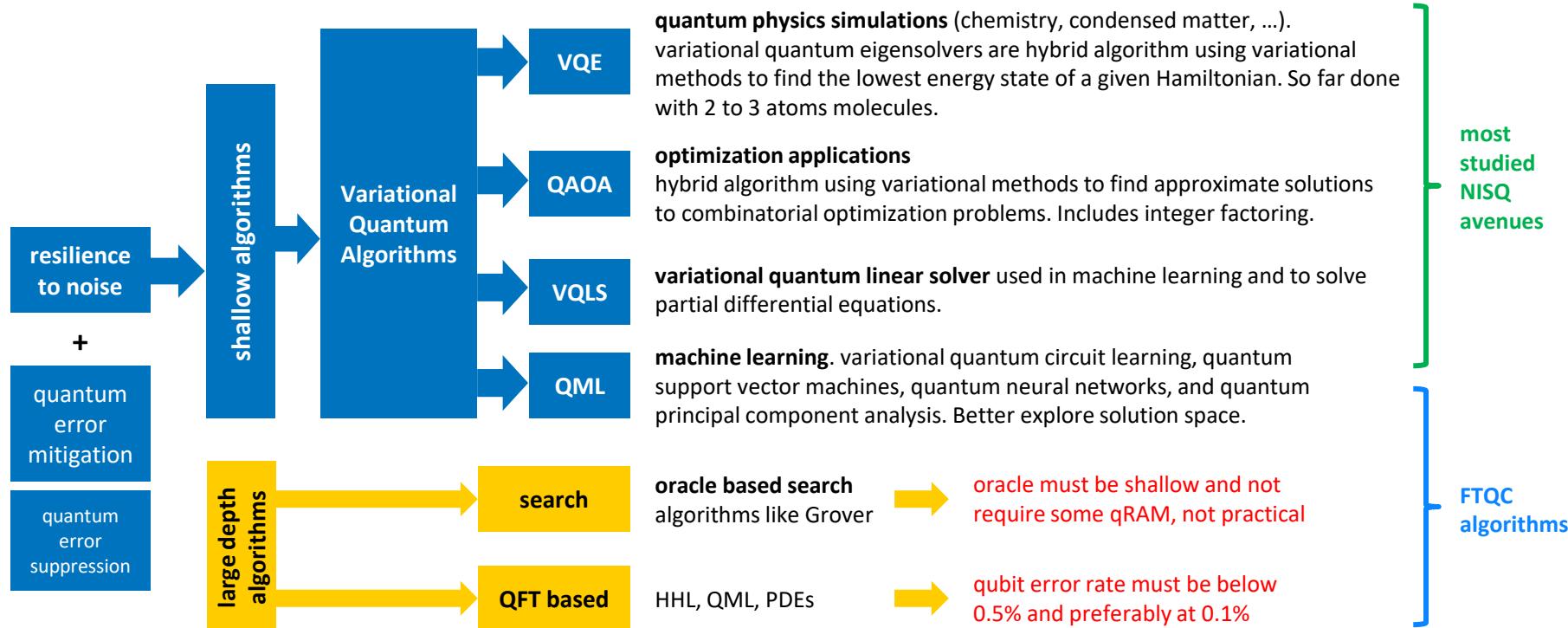
# computing paradigms and algorithms



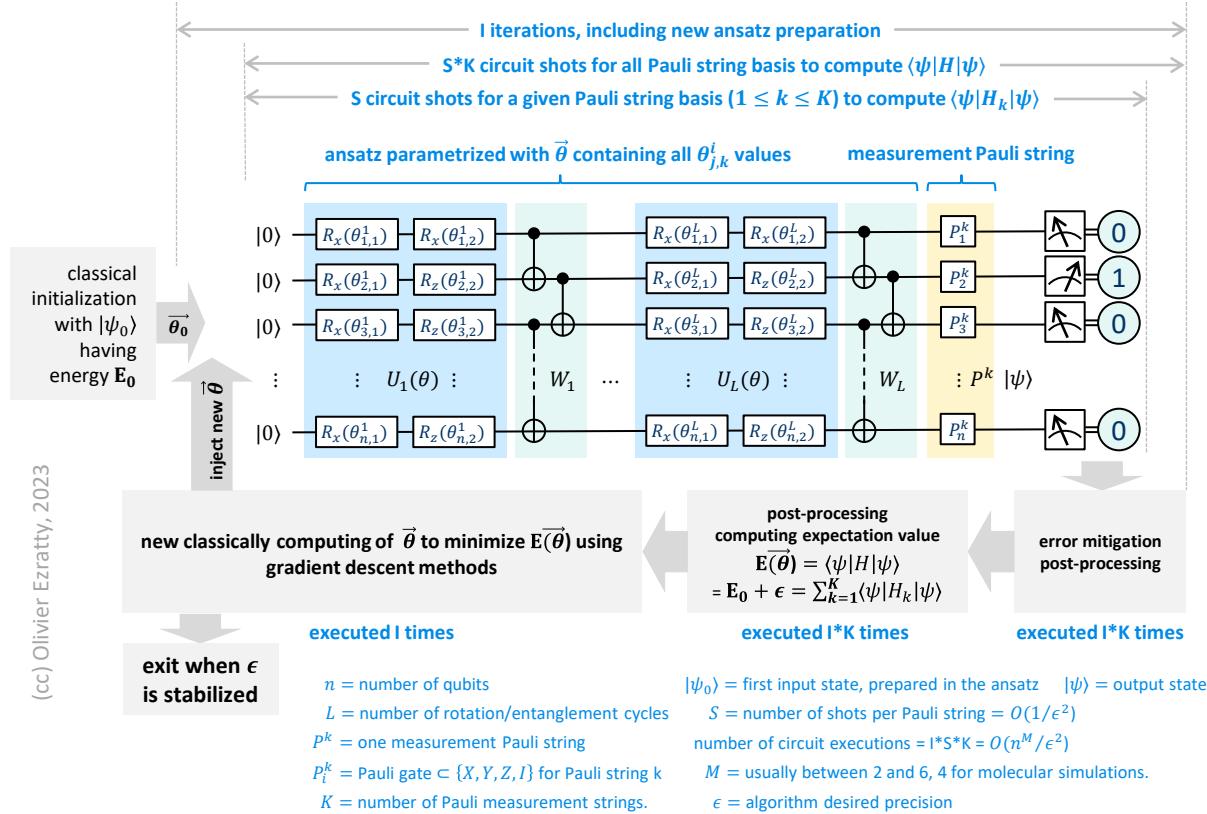
NISQ: noisy intermediate scale quantum computer, FTQC: fault tolerant quantum computer

(cc) Olivier Ezratty, 2022

# NISQ and FTQC algorithms scopes



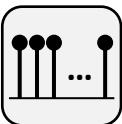
# typical VQA process



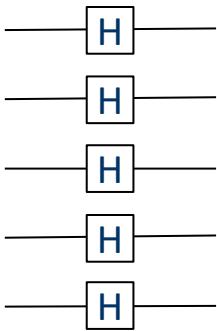
(cc) Olivier Ezratty, 2023

- used in VQE, QAOA, QML, etc.
- parametrized circuit (aka ansatz) with shallow depth circuit.
- minimum depth of 8, but frequently much higher as  $L$  grows.
- use R gates of arbitrary angle and some CNOTs.
- number of shots depends on algorithm, precision, and can scale exponentially with the number of qubits.
- classical cost of ansatz preparation has to be assessed.

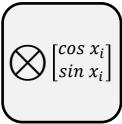
# data loading



**uniform superposition**  
for oracle based algorithms



$$\sum_{i=1,2^N} \frac{1}{2^{N/2}} |i\rangle = \begin{bmatrix} \frac{1}{2^{N/2}} \\ \frac{1}{2^{N/2}} \\ \vdots \\ \frac{1}{2^{N/2}} \end{bmatrix}$$



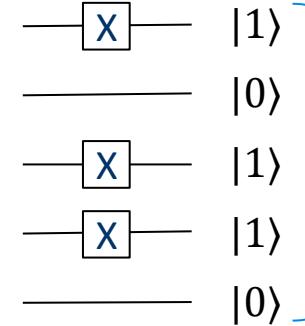
**angle encoding**  
tensor product  
of single qubits  
encoding

tensor product of N qubits  $\bigotimes_{i=1}^N \begin{bmatrix} \cos x_i \\ \sin x_i \end{bmatrix} \quad \bigotimes_{i=1}^N \begin{bmatrix} \cos x_{2i-1} \\ e^{ix_{2i}} \sin x_{2i-1} \end{bmatrix}$

N qubits encoding a vector of N  $x_i$  real values in individual qubits with a series of  $R_x$  gates, no entanglement, we can also encode 2 real values in a qubit in the dense angle encoding variation (right)

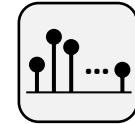


**basis encoding**  
one value in  
encoded in  
binary, used in  
Shor algorithm



$$|10110\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

$$x = (x_0, \dots, x_{2^N-1})^T$$



**amplitude encoding**  
encodes the greatest wealth  
of data in qubits, with the  
whole computational state  
vector, but lengthy

$$\sum_{i=1,2^N} x_i |i\rangle = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{2^N-1} \end{bmatrix}$$

# algorithms inputs and outputs

algorithm	input	output
Deutsche-Josza	oracle function	function is balanced if all output qubits are at ground state $ 0\rangle$
Bernstein-Vazirani	oracle function	(integer) secret string in basis encoding
Grover	oracle function	searched item index as integer in basis encoding
Simon	oracle function	parameters for a linear equation used to find a period, with average of basis encoding
Shor factoring	integer in basis encoding	integer in basis encoding
Shor dlog	integers in basis encoding	integer in basis encoding
QFT	series of complex amplitudes with amplitude encoding (any quantum input state)	Fourier coefficients in amplitude encoding, enabling the recovery of the main frequency
HHL	one vector and one matrix amplitude encoding	characteristics of inverted matrix x entry vector (= one vector) in amplitude encoding
VQE	cost function parameters encoded as an Hamiltonian with unitaries (quantum gates)	researched ground state in amplitude encoding
QML classification	object vector to classify encoded in amplitude	prediction result as an integer index in basis encoding

# what is an oracle function?

an oracle function aka black box algorithm is a classical operation encoded with qubit gates that is applied to multiple register states simultaneously used in **Deutsch-Jozsa**, **Simon** and **Grover** algorithms among others.

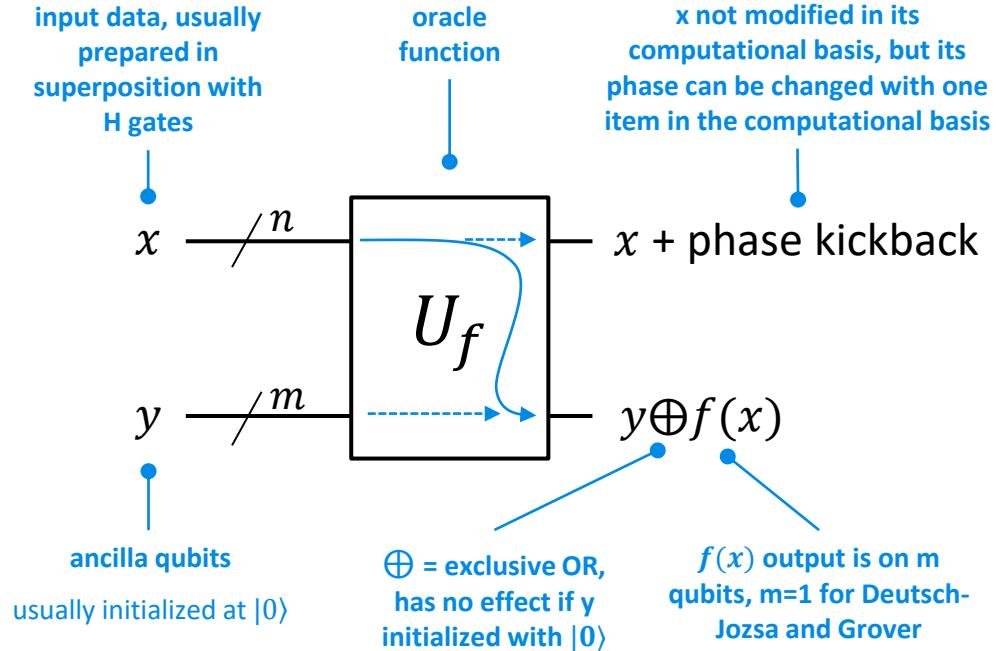
uses one and two qubits gates and **entanglement**.

contains **reversible quantum equivalents** of boolean and arithmetic functions using ancilla qubits.

leverages **quantum parallelism** with input initialized with Hadamard qubit gates.

outputs initial computational states with a **changed phase** depending on the oracle function result ( $x$ ) and the **function result** on ancilla qubits ( $y$ ).

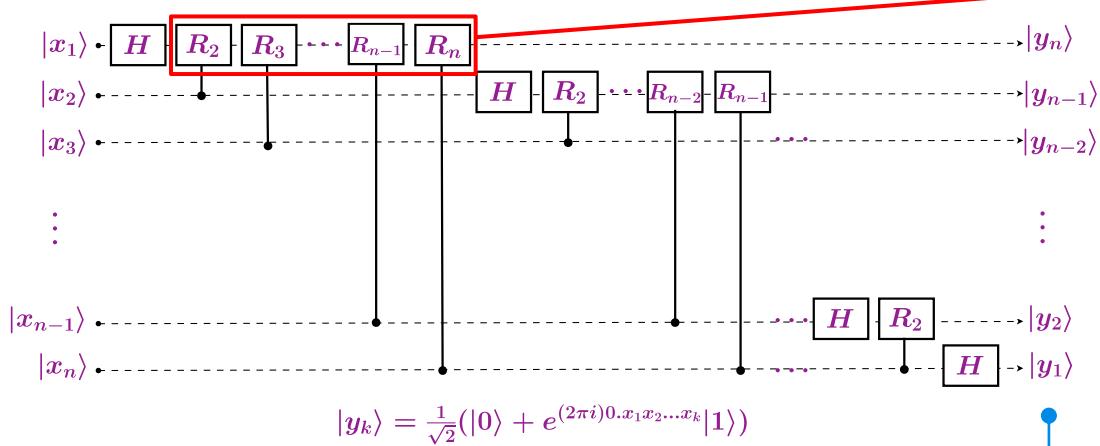
may often need to rely on some (not yet available) **qRAM** with qubits memory accessed through an addressing mechanism.



$$|x\rangle|y\rangle \Rightarrow |x\rangle|y\rangle \oplus f(x)$$

# quantum Fourier transform

QFT decomposes a series of qubits computational base states amplitudes in frequencies  
 can also easily do an inverse Fourier transform, used in quantum phase estimate  
 used in Shor algorithm, discrete log algorithm,  
 and various quantum arithmetic algorithms (adders, multipliers)

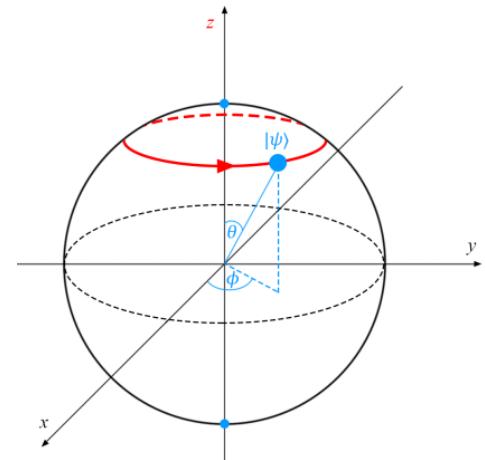


$N * \log(N) \Rightarrow (\log(N))^2$   
 exponential speed gain

$$R_m = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^m}} \end{pmatrix}$$

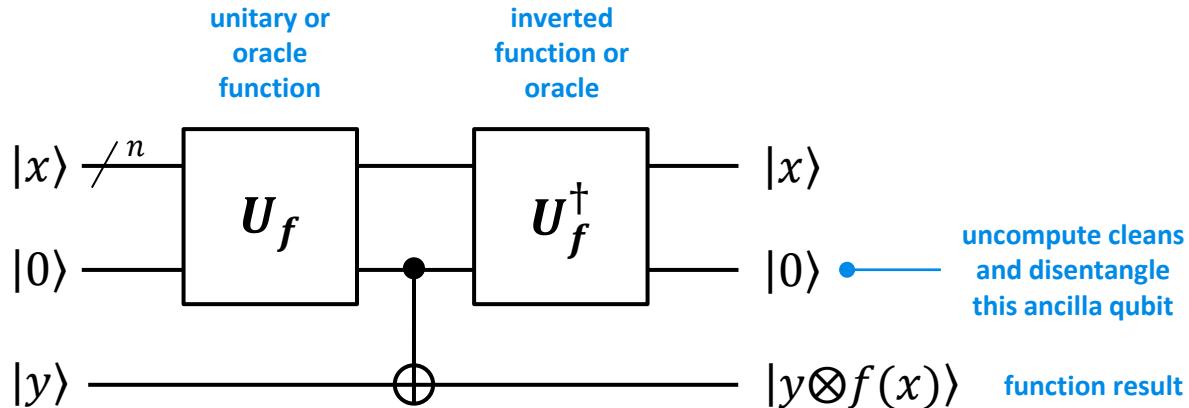
needs many controlled R phase gates

$y_n$  are inverted vs  $x_n$ ,  
 and require a SWAP



# uncompute trick

uncomputing  $U_f$  will:  
disentangle ancilla qubits  
make it available for  
subsequent computation  
leave  $x$  and  $f(x)$  intact



# Deutsch-Jozsa algorithm

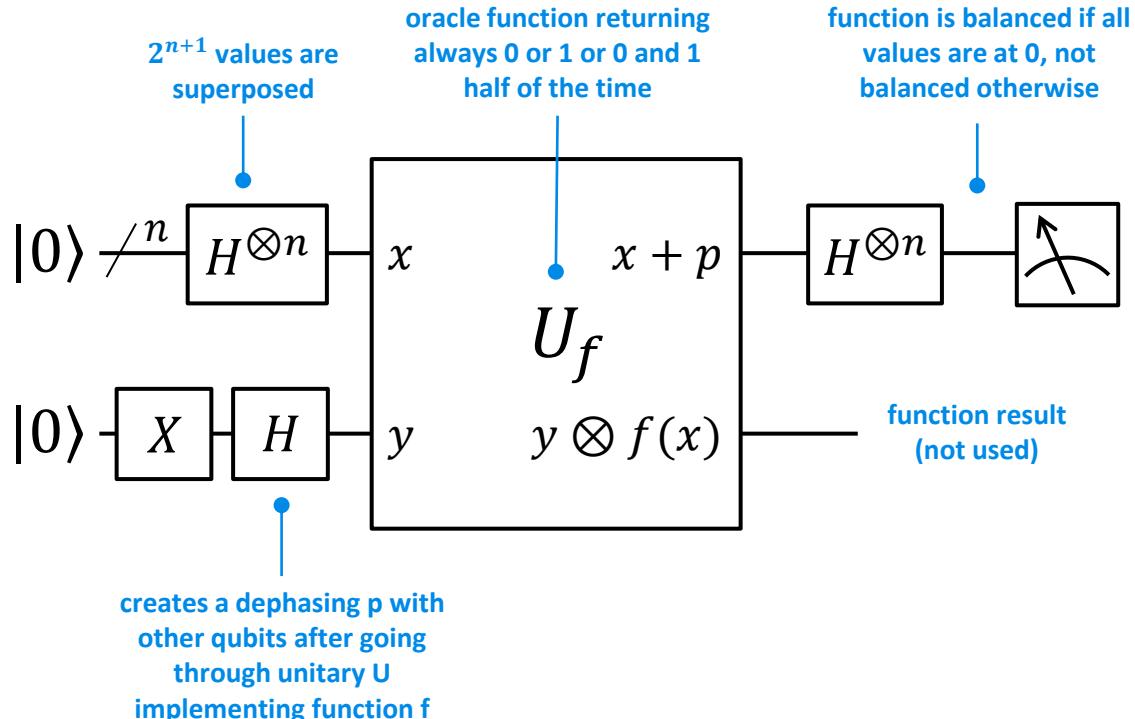


David Deutsch

Richard Jozsa

checks if oracle function f  
is balanced or not  
has no known use case

$O(2^{N-1}) \Rightarrow O(1)$   
exponential speed gain



# Bernstein-Vazirani algorithm

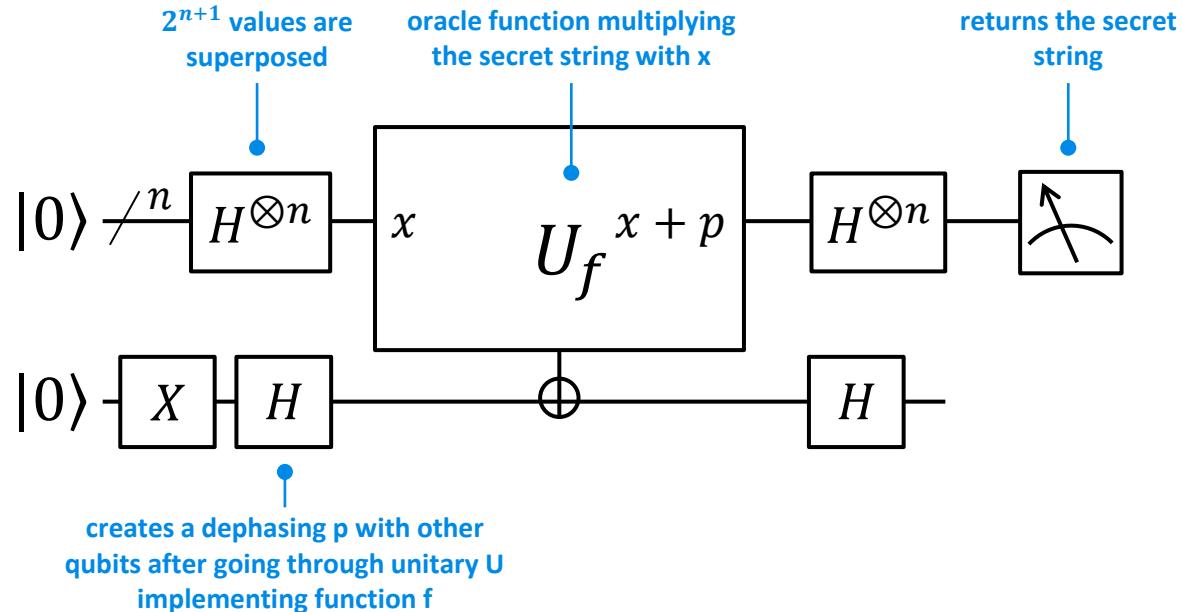


Ethan Bernstein and Umesh Vazirani - 1992

learns a secret string encoded in an oracle function

$$O(n) \Rightarrow O(1)$$

exponential speed gain



# Simon algorithm

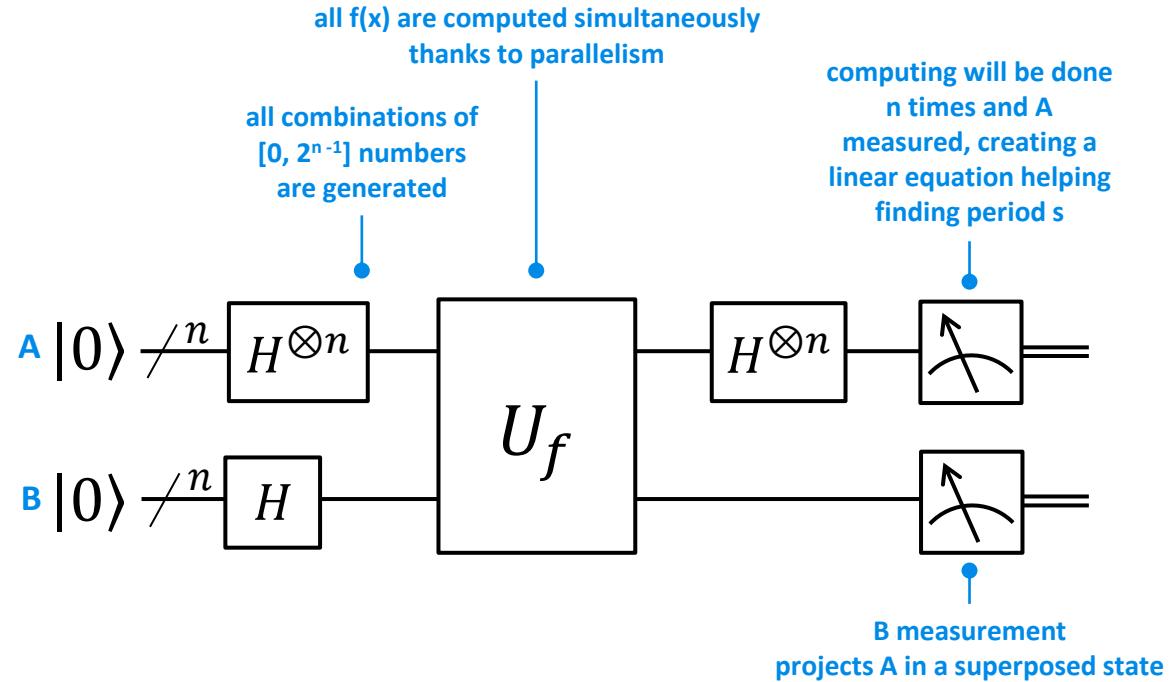


Daniel Simon 1994-1996

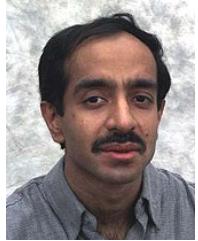
search a subset of numbers matching a condition imposed by unknown oracle function  $f$ , so that  $f(x')=f(x)$  if  $x'=x \oplus s$   
indirectly used in QFT and Shor

$$O(2^N) \Rightarrow O(N)$$

exponential speed gain



# Grover algorithm



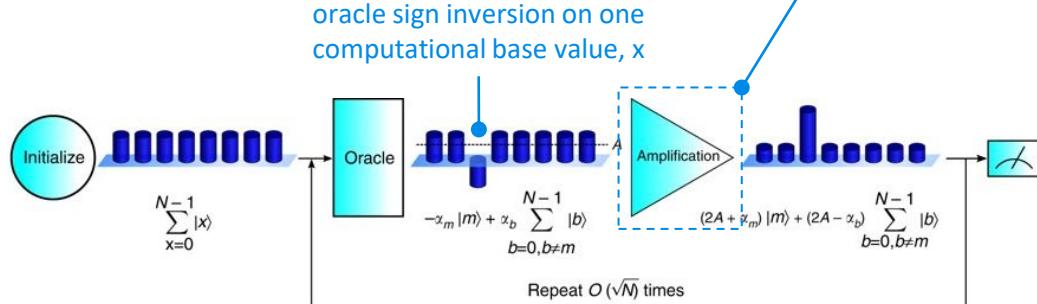
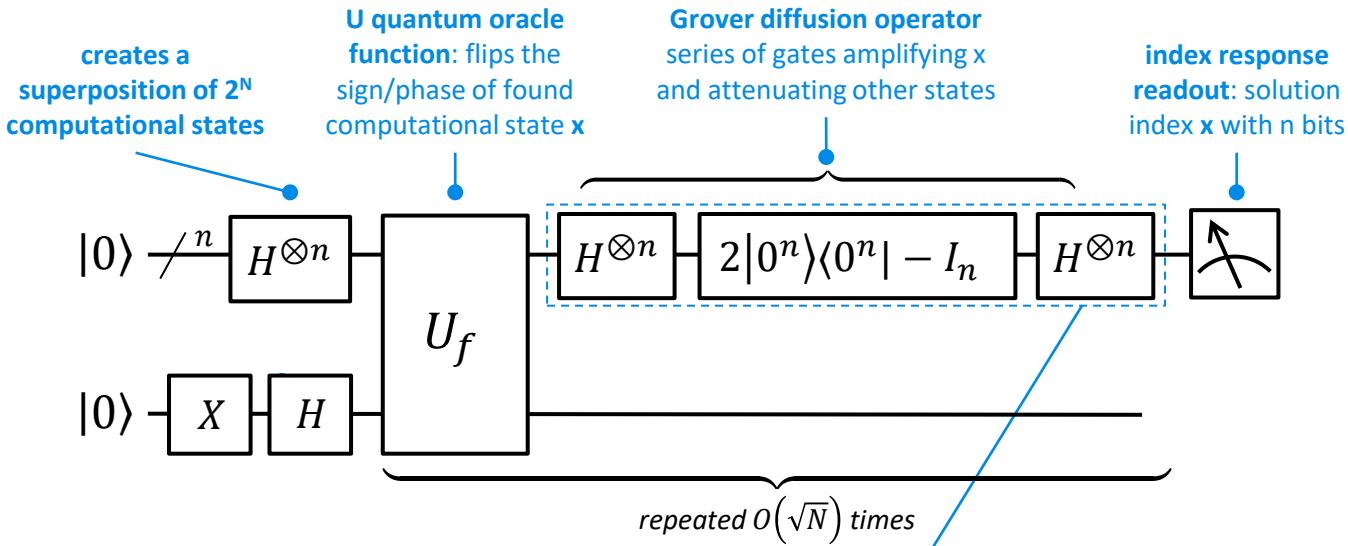
Lov Grover 1996

find one item verifying a condition with an oracle function

can be used to find an index in a database or in cryptography to use brute force to find a symmetric key

$$O(N) \rightarrow O(\sqrt{N})$$

polynomial speed gain



## Grover's Algorithm Offers No Quantum Advantage

E.M. Stoudenmire<sup>1</sup> and Xavier Waintal<sup>2</sup>

<sup>1</sup>Center for Computational Quantum Physics, Flatiron Institute, 162 5th Avenue, New York, NY 10010, USA

<sup>2</sup>PHELIQS, Université Grenoble Alpes, CEA, Grenoble INP, IRIG, Grenoble 38000, France

(Dated: March 21, 2023)

Grover's algorithm is one of the primary algorithms offered as evidence that quantum computers can provide an advantage over classical computers. It involves an "oracle" (external quantum subroutine) which must be specified for a given application and whose internal structure is not part of the formal scaling of the quantum speedup guaranteed by the algorithm. Grover's algorithm also requires exponentially many steps to succeed, raising the question of its implementation on near-term, non-error-corrected hardware and indeed even on error-corrected quantum computers. In this work, we construct a quantum inspired algorithm, executable on a classical computer, that performs Grover's task in a *linear* number of calls to the oracle — an exponentially smaller number than Grover's algorithm — and demonstrate this algorithm explicitly for boolean satisfiability problems (3-SAT). Our finding implies that there is no *a priori* theoretical quantum speed-up associated with Grover's algorithm. We critically examine the possibility of a practical speed-up, a possibility that depends on the nature of the quantum circuit associated with the oracle. We argue that the unfavorable scaling of the success probability of Grover's algorithm, which in the presence of noise decays as the exponential of the exponential of the number of qubits, makes a practical speedup unrealistic even under extremely optimistic assumptions on both hardware quality and availability.

<https://arxiv.org/abs/2303.11317>

### a typical debate between theoreticians and practitioners

Grover's algorithm speedup relies on its oracle function, not its amplitude amplification routine that benefit poorly from entanglement and thus, any quantum acceleration.

E. M. Stoudenmire is a preeminent US scientist working on tensor networks and Xavier Waintal is a CEA IRIG polymath researcher with experience in condensed matter physics, tensor networks and even software development.



« On overexcitable children

Xavier Waintal responds (tl;dr Grover is still quadratically faster) »

Of course Grover's algorithm offers a quantum advantage!

I was really, *really* hoping that I'd be able to avoid blogging about [this new arXiv preprint](#), by E. M. Stoudenmire and Xavier Waintal:

So, on to the preprint, as reviewed by the human Scott Aaronson. Yeah, it's basically a tissue of confusions, a mishmash of the well-known and the mistaken. As they say, both novel and correct, but not in the same places.

It turns out that, for their "quantum-inspired classical algorithm," the authors assume you're given, not merely an oracle for  $f$ , but the *actual circuit* to compute  $f$ . They then use that circuit in a non-oracular way to extract the marked item. In which case, I'd prefer to say that they've actually solved the Grover problem with **zero** queries—simply because they've entirely left the black-box setting where Grover's algorithm is normally formulated!

What could possibly justify such a move? Well, the authors argue that *sometimes* one can use the actual circuit to do better classically than Grover's algorithm would do quantumly, and therefore, they've shown that the Grover speedup is not "generic," as the quantum algorithms people always say it is.

But this is pure wordplay around the meaning of "generic." When we say that Grover's algorithm achieves a "generic" square-root speedup, what we mean is that it solves the generic black-box search problem in  $O(2^{n/2})$  queries, whereas any classical algorithm for that generic problem requires  $\Omega(2^n)$  queries. We don't mean that for every  $f$ , Grover achieves a quadratic speedup for searching *that f*, compared to the best classical algorithm that could be tailored to *that f*. Of course we don't; that would be trivially false!

<https://scottaaronson.blog/?p=7143>

# Shor integer factoring



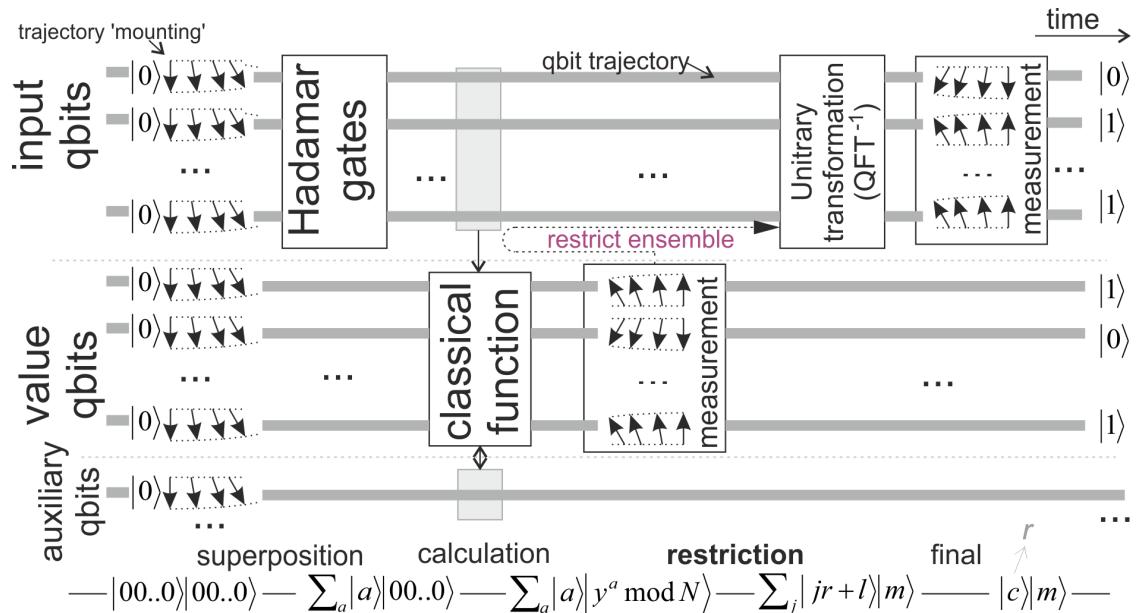
factors an integer in prime numbers

algorithm relies on a period finding algorithm and an inverse quantum Fourier transform

**breaking RSA 2048 bits key requires  
22 millions qubits with an error rate  
of 0,1% and 8 compute hours.**

$$O\left(\frac{\sqrt{N}}{2}\right) \Rightarrow O(\log(N)^3)$$

exponential speed gain



# Schnorr schneller than Shor?

The screenshot shows a news article from the Financial Times. At the top, there's a navigation bar with links to US COMPANIES, TECH, MARKETS, CLIMATE, OPINION, WORK & CAREERS, LIFE & ARTS, and HTSI. Below the navigation bar, a red banner says "Quantum technologies" and has a button "+ Add to myFT". The main headline is "Chinese researchers claim to find way to break encryption using quantum computers". A sub-headline below it reads "Experts assess whether method outlined in scientific paper could be a sooner-than-expected turning point in the technology".

- hybrid QAOA based algorithm using classical “Schnorr” algorithm.
- would require 372 NISQ physical qubits and 1139-1490 gate depth.
- QAOA doesn't scale well.
- classical and quantum part speedup/time are not provided.
- NISQ qubit noise would require some QEC and a much larger number of qubits.



« Happy 40th Birthday Dana!

## Cargo Cult Quantum Factoring

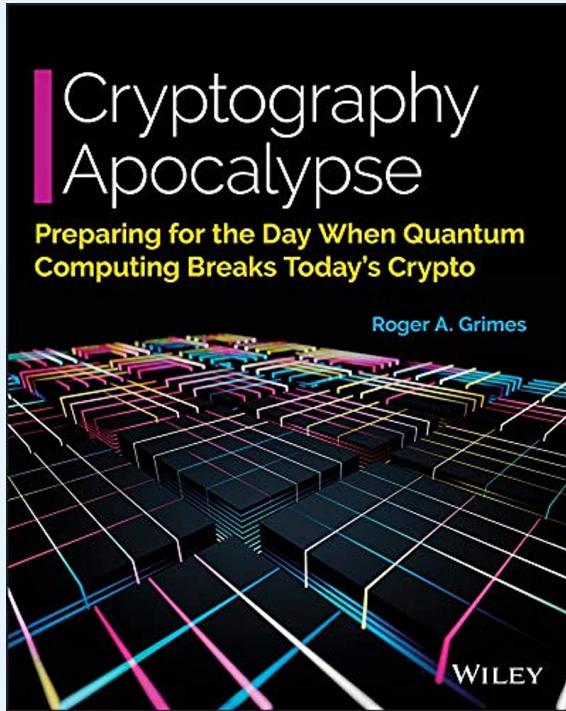
For those who don't care to read further, here is my 3-word review:

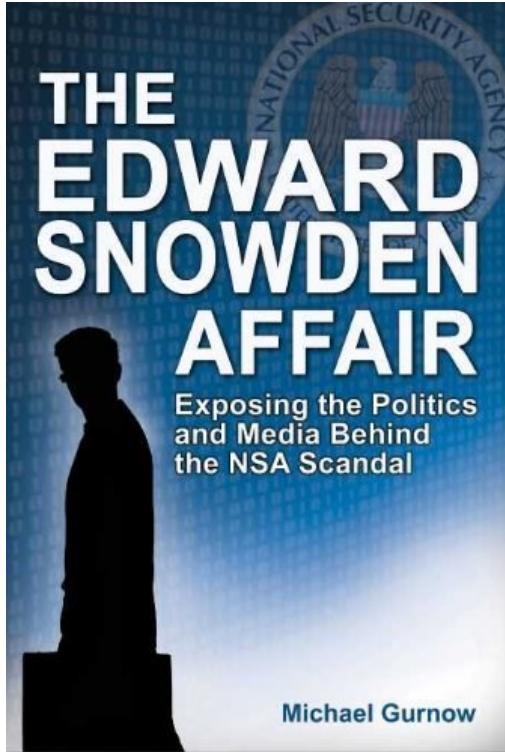
No. Just No.

And here's my slightly longer review:

<https://arxiv.org/abs/2212.12372>, December 23<sup>rd</sup>, 2022

# *break on* **post-quantum cryptography**





---

## Connectivity

---

# Quantum Computing Paranoia Creates a New Industry

Even though quantum computers don't exist yet, security companies are preparing to protect against them.

by Tom Simonite January 30, 2017

**MIT  
Technology  
Review**

**F**ear sells in the computer security business. And in late 2015 Massachusetts-based **Security Innovation** got an unexpected boost from one of the scariest organizations around—the National Security Agency.

For six years the company had been trying to create a new revenue stream by licensing an unusual encryption technology called NTRU, which it **acquired** from four Brown University mathematicians. It was invented as a solution to the powerful code-breaking power of computers that exploit quantum physics, but interest was slack because quantum computers didn't yet exist or look likely to exist anytime soon.



# The quantum computing apocalypse is imminent

Shlomi Dolev January 2018

---

Connectivity

---

## Quantum Computing Paranoia Creates a New Industry

Even though quantum computers don't exist yet, security companies are preparing to protect against them.

by Tom Simonite January 30, 2017



**F**ear sells in the computer security business. And in late 2015 Massachusetts-based [Security Innovation](#) got an unexpected boost from one of the scariest organizations around—the National Security Agency.

For six years the company had been trying to create a new revenue stream by licensing an unusual encryption technology called NTRU, which it [acquired](#) from four Brown University mathematicians. It was invented as a solution to the powerful code-breaking power of computers that exploit quantum physics, but interest was slack because quantum computers didn't yet exist or look likely to exist anytime soon.

# dual quantum computing beyond Shor

**Peter Shor factoring algorithm** - 1994

integer factoring  
exponential acceleration

$$O\left(\frac{\sqrt{N}}{2}\right) \Rightarrow O(\log(N)^3)$$

**threatens public key based cybersecurity**

RSA, ECDH, ECDSA, SSL/TLS, VPNs (IPSEC), SSH, PGP,  
S/MIME), Signal (Whatsapp), Bitcoin & Blockchain signatures

**Peter Shor dlog algorithm** - 1994

exponential acceleration

$$O\left(\frac{\sqrt{N}}{2}\right) \Rightarrow O(\log(N)^3)$$

**threatens Digital Signature Algorithm, Diffie-Hellman  
key exchanges and El-Gamal encryption**

**Lov Grover search algorithm** - 1996

brute force to break symmetric codes  
polynomial acceleration

$$O(N) \Rightarrow O(\sqrt{N})$$

**threatens symmetric keys cybersecurity**

improves brute force attack of hash  
functions (SHA) and block ciphers (AES)  
used in symmetric encryption

**David Simon algorithm** - 1996

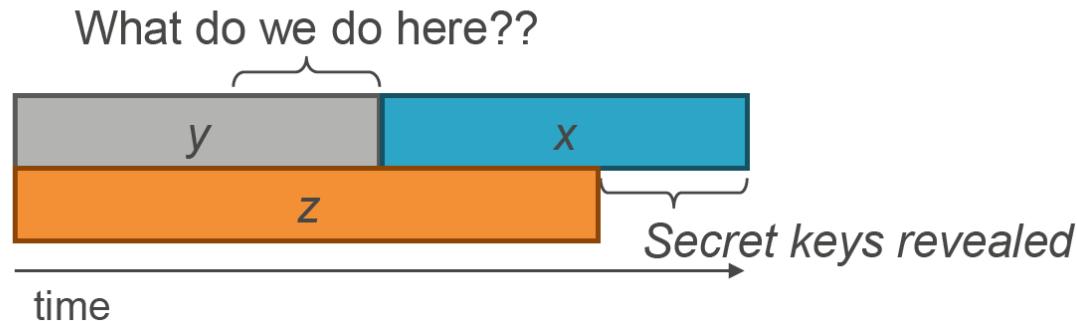
exponential acceleration

$$O(2^N) \Rightarrow O(N)$$

**threatens Even-Mansour ciphers  
used in some disk encryptions**

# Mosca « XYZ risk model » or theorem

Theorem 1: If  $x + y > z$ , then worry.

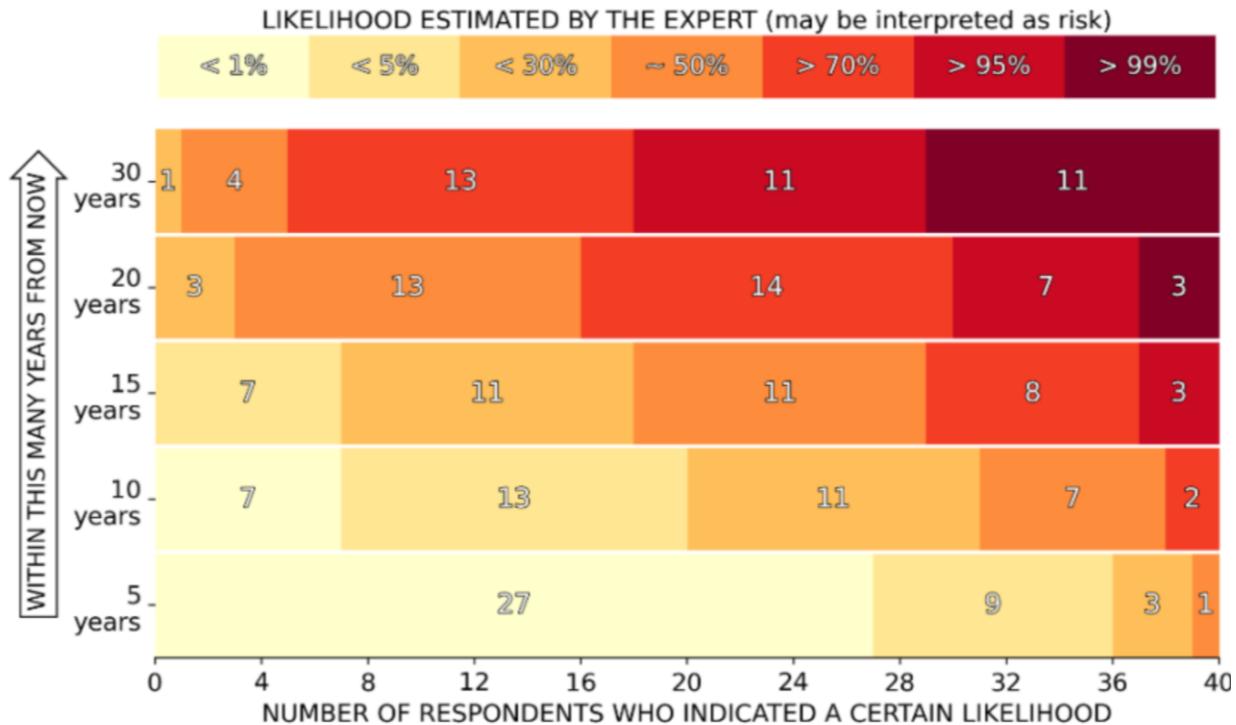


	definition	estimation	uncertainty
x	time that you need encryption to be secure	≈ 10-20 years	none: regulatory
y	time to re-tool the existing infrastructure with PQC	≈ 5-10 years	average: operational
z	time to build a FTQC computer breaking RSA-2048	≈ 15-30 years	total



## 2022 EXPERTS' ESTIMATES OF LIKELIHOOD OF A QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS

The experts indicated their estimate for the likelihood of a quantum computer that is cryptographically relevant—in the specific sense of being able to break RSA-2048 quickly—for various time frames, from a short term of 5 years all the way to 30 years.



<https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/>

### QUANTUM THREAT TIMELINE REPORT 2022



Authors  
Dr. Michele Mosca  
Co-Founder & CEO, evolutionQ Inc.

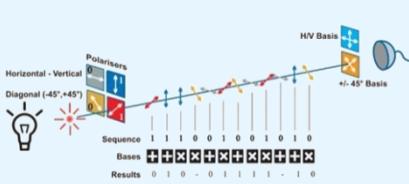
Dr. Marco Piani  
Senior Research Analyst, evolutionQ Inc.

GRI | GLOBAL RISK INSTITUTE evolutionQ

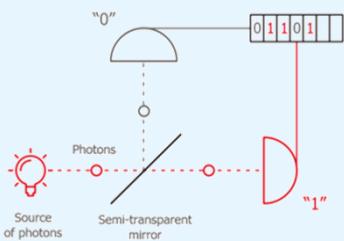
DECEMBER 2022

# quantum telecommunications

## quantum technologies

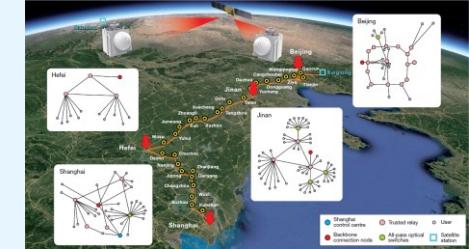


**quantum key distribution**  
protects public keys sent  
through optical links

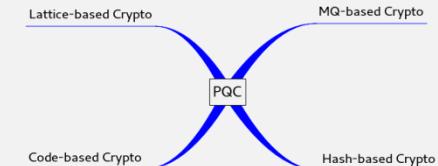


**random key generators**  
ensure the quality of public  
keys in classical and  
quantum cryptography

**quantum telecommunications**  
distributed quantum computing,  
connection between quantum  
computing and sensing, blind  
computing, ...

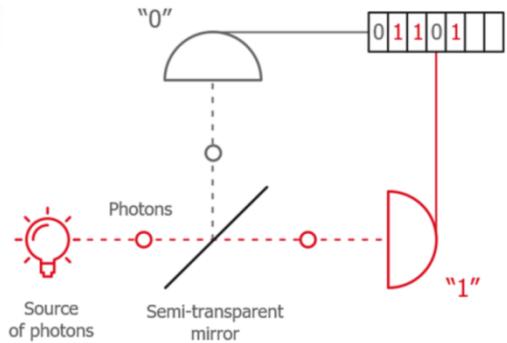


**post-quantum cryptography**  
resists to quantum algorithms

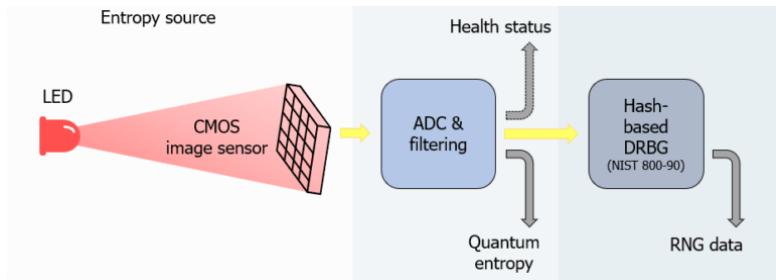


**classical technologies**

# quantum random number generator



first generation QRNG



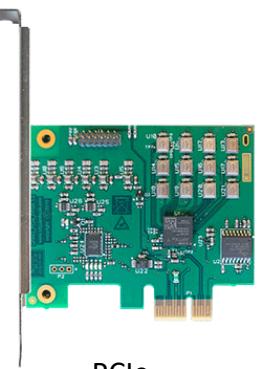
existing generation QRNG



USB (legacy)



250 kbits/s to 19.64 Mbits/s  
of real random numbers



PCIe



network appliance

# quantum random number generators

photons  
counting



Q → N U



photons  
arrival time



PicoQUANT



vacuum  
fluctuations



CRYPTOMATHIC

$\langle$  InfiniQuant  $\rangle$

other



phase noise



| KETS >

self-certified SDI  
QRNG



QUANTUM  
DICE

radioactive  
decay



qubits  
measurement



# post-quantum cryptography

Name of Cryptographic Algorithm	Type	Purpose	Resilience against Quantum Computer
AES-256	Symmetric Key	Encryption	Ok but larger key sizes needed
SHA-256, SHA-3		Hash function	Ok but larger output needed
Lattice-based (NTRU)	Public Key	Encryption; signature	Believed
Code-based (Mc Eliece)	Public Key	Encryption	Believed
Multivariate polynomials	Public Key	Encryption; signature	Believed
Supersingular elliptic curve isogenies (SIDH)		Encryption; possibly signature	Believed
ECDSA, ECDH (Elliptic Curve Crypto)	Public Key	Signatures, Key exchange	No longer secure
RSA	Public Key	Signatures, Key establishment	No Longer secure
DSA (Finite Field Crypto)	Public Key	Signatures	No Longer secure

High level of confidence

Under investigation

threatened by quantum algorithms



# NIST finalists

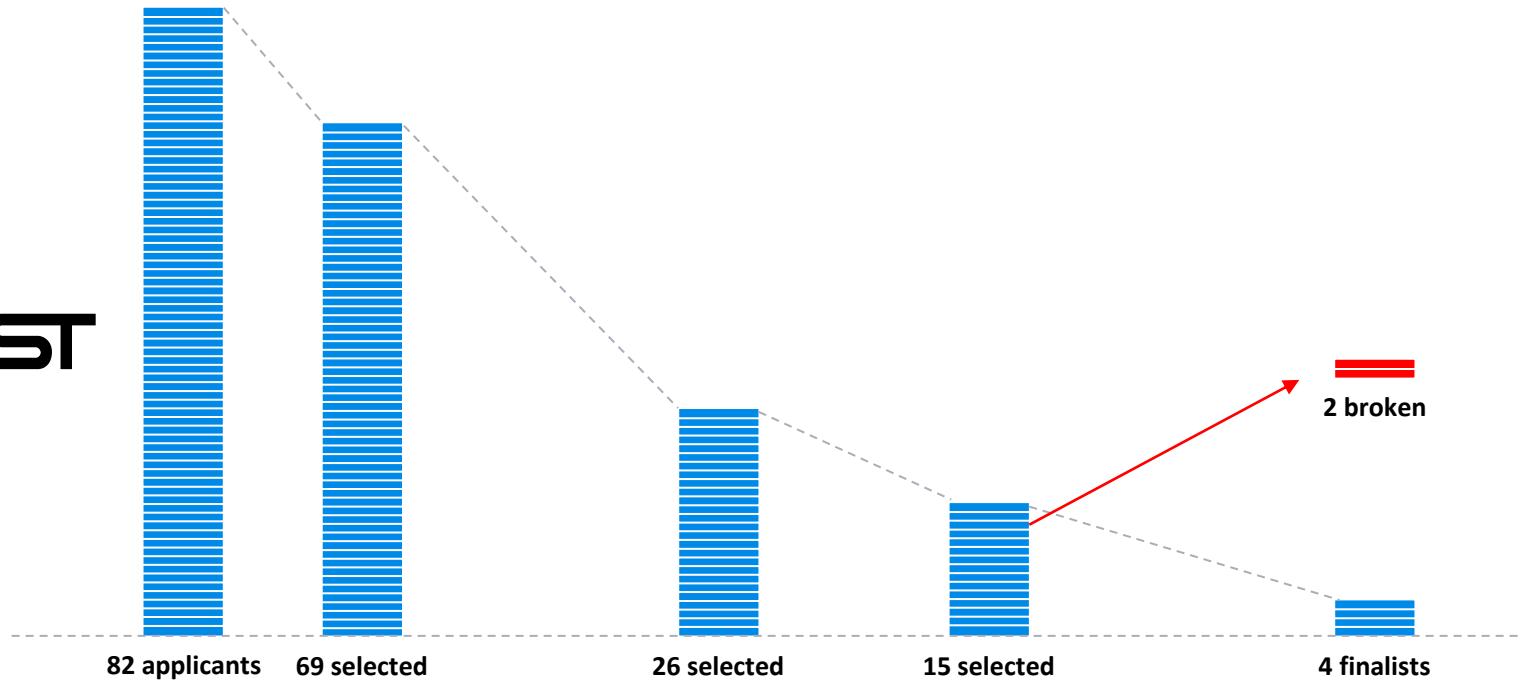
finalists	research teams	vendors teams
Public-Key Encryption/KEMs	Classic McEliece  <b>UK:</b> U. London, U. Plymouth. <b>Switzerland:</b> ETH Zurich. <b>USA:</b> U. Illinois & Chicago, U. Florida, Yale. <b>Europe:</b> U.Ruhr Bochum, U. Eindhoven, U. Southern, Denmark, MPI, Inria (France). <b>Taiwan:</b> Academia Sinica.	Google PQ Solutions PQShield
	CRYSTALS-KYBER  <b>USA:</b> SRI. <b>Canada:</b> U. Waterloo. <b>Europe:</b> Radboud U. Netherlands, Ruhr U. Bochum, ENS Lyon.	IBM Research Europe Arm, PQShield NXP Semiconductors
	NTRU  <b>Europe:</b> Radboud U Netherlands, Eindhoven U. <b>USA:</b> Brown U. <b>Canada:</b> U. Waterloo.	Qualcomm NTT Algorand, PQShield
Digital Signatures	SABER  <b>Europe:</b> KU Leuven (Belgium). <b>UK:</b> Birmingham U.	
	CRYSTALS-DILITHIUM  <b>USA:</b> Florida Atlantic U. <b>Switzerland:</b> ETH Zurich. <b>Europe:</b> CWI Netherlands, Ruhr U. Bochum, MPI, ENS Lyon.	IBM Research Europe Google, PQShield
	FALCON  <b>Europe:</b> ENS Paris, U. Rennes (France). <b>USA:</b> Brown U.	IBM Research PQShield, Qualcomm Ethereum Foundation Thales
Rainbow	<b>Europe:</b> FAU Erlangen Nuremberg, U. Versailles. <b>USA:</b> Cincinnati U. <b>Taiwan:</b> Academia Sinica, National Taiwan U.	Grey: 2020 selection Green: 2022 selection Red: broken in 2022

# NIST alternate candidates

finalists	research teams	vendors teams
Public-Key Encryption/KEMs	<p><b>BIKE</b></p> <p><b>USA:</b> U.Washington, Florida U.</p> <p><b>Europe:</b> U. Limoges, ENAC &amp; U. Toulouse, Inria, U. Bordeaux (France), U. Ruhr Bochum (Germany).</p> <p><b>Israel:</b> U. Haifa.</p>	Intel Google IBM Worldline France
	<p><b>FrodoKEM</b></p> <p><b>USA:</b> U. Michigan, Stanford U.</p> <p><b>Netherlands:</b> CWI.</p> <p><b>Canada:</b> U. Waterloo.</p> <p><b>Middle-East:</b> Ege University (Turkey).</p>	NXP Microsoft Research PQShield
	<p><b>HQC</b></p> <p><b>France:</b> ISAE-Supaero, Limoges U., ENAC, U. Toulouse, Toulon U., Bordeaux U.</p> <p><b>USA:</b> Florida U.</p>	Worldline France and Netherlands
	<p><b>NTRU Prime</b></p> <p><b>Taiwan:</b> Academia Sinica, National Taiwan U.</p> <p><b>Australia:</b> U. Adelaide.</p> <p><b>Europe:</b> Eindhoven U (Netherlands), Hamburg U. (Germany), Tampere U. (Finland).</p> <p><b>USA:</b> Illinois U.</p>	NXP
	<p><b>SIKE</b></p> <p><b>USA:</b> Florida U.</p> <p><b>Canada:</b> Waterloo U., Toronto U.</p> <p><b>Europe:</b> Radboud U. Netherlands, U. Versailles (France).</p>	evolutionQ Amazon Microsoft Research Infosec Global Texas Instruments
Digital Signatures	<p><b>GeMSS</b></p> <p><b>France:</b> Inria, University of Versailles and Sorbonne Université.</p>	Grey: 2020 selection Green: 2022 selection Red: broken in 2022
	<p><b>Picnic</b></p> <p><b>USA:</b> Northwestern U., GeorgiaTech, U. Maryland., Princeton U.</p> <p><b>Europe:</b> Austrian Institute of Technology, TU Graz (Austria), Aarhus U. (Denmark), DTU (Denmark).</p>	Microsoft Research Dfinity
	<p><b>SPINCS+</b></p> <p><b>Europe:</b> U.Ruhr Bochum, KU Leuven, TU Graz, Eindhoven U, Radboud U.</p>	Cisco, Infineon Infosec Global Genua, Taurus

# NIST PQC standardization

NIST



2016

2017

2018

2019

2020

2021

2022

2023

## cryptography QKD/PQC

quantum keys QKD / BB84

protects symmetric keys with optical link (fiber or sat)



post-quantum cryptography

public key cryptography  
resisting to quantum algorithms



**end of post-quantum cryptography**  
*break*

# linear equations

Harrow, Hassidim and Lloyd developed the HHL algorithm in 2009 which quantum mechanically inverts a system of linear equations. solves the system of equations  $A\vec{x} = \vec{b}$  where:

- $A$  : sparse square hermitian matrix  $n \times n$
- $\vec{b}$  : vector with  $n$  values
- $\vec{x}$  : solution vector to be characterized

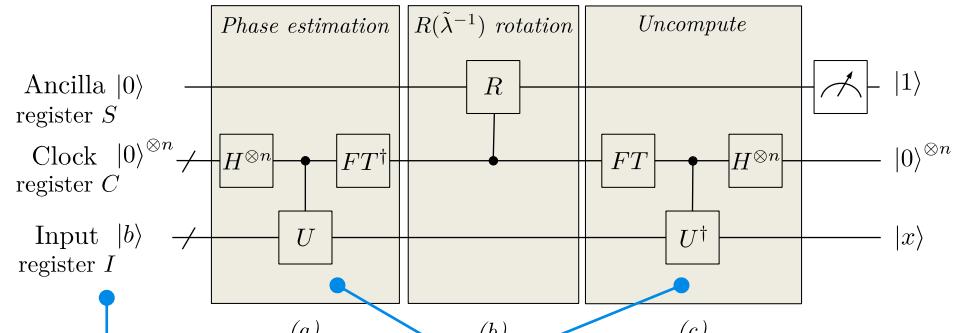
requires inverting a matrix and uses a quantum phase estimate.

part of the QBLAS algorithms family  
(Quantum Basic Linear Algebra Subroutines)  
used in many QML algorithms.

$$N * \log(N) \Rightarrow (\log(N))^2$$

exponential speed gain, but finding the full  $\vec{x}$  vector requires  $O(N)$  repetitions!

if matrix  $A$  is not hermitian, we construct another matrix with  $A$  that is hermitian



requires costly state preparation and qRAM

$U$  implements matrix  $A$  as a unitary operator

# quantum machine learning

**SVM:** uses HHL and requires qRAM.

**PCA:** matrix diagonalization using quantum phase estimate.

**K-means and K-nearest neighbours clustering:** uses Grover's algorithm.

**Deep Neural Networks training:** can use quantum annealing and universal gates computing.

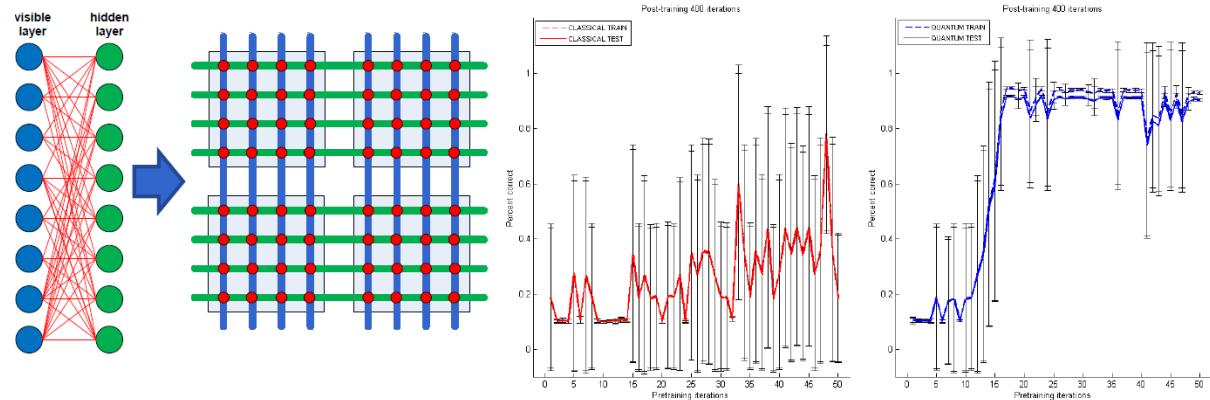
**ConvNets:** also possible with quantum qubits/gates and quantum annealing.  
Problem: training data encoding optimization.

needs to be addressed:

- training data preparation and loading.
- results readout.
- need for non linear activation functions.
- getting a real computing time gain.

Method	Speedup	AA	HHL	Adiabatic	QRAM
Bayesian Inference [107, 108]	$O(\sqrt{N})$	Y	Y	N	N
Online Perceptron [109]	$O(\sqrt{N})$	Y	N	N	optional
Least squares fitting [9]	$O(\log N^{(*)})$	Y	Y	N	Y
Classical BM [20]	$O(\sqrt{N})$	Y/N	optional/N	N/Y	optional
Quantum BM [22, 62]	$O(\log N^{(*)})$	optional/N	N	N/Y	N
Quantum PCA [11]	$O(\log N^{(*)})$	N	Y	N	optional
Quantum SVM [13]	$O(\log N^{(*)})$	N	Y	N	Y
Quantum reinforcement learning [30]	$O(\sqrt{N})$	Y	N	N	N

Quantum Machine Learning by Jacob Biamonte et al, 2018 (24 pages)



Application of Quantum Annealing to Training of Deep Neural Networks  
by Steven H. Adachi and Maxwell P. Henderson, 2015 (18 pages)

**TABLE 1** Overview of the main quantum machine learning algorithms that have been reported in the literature, and complexities

Algorithm	Classical	Quantum	QRAM
Linear regression	$\mathcal{O}(N)$	$\mathcal{O}(\log N)^*$	Yes
Gaussian process regression	$\mathcal{O}(N^3)$	$\mathcal{O}(\log N)^\dagger$	Yes
Decision trees	$\mathcal{O}(N \log N)$	Unclear	No
Ensemble methods	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$	No
Support vector machines	$\approx\mathcal{O}(N^2)\text{-}\mathcal{O}(N^3)$	$\mathcal{O}(\log N)$	Yes
Hidden Markov models	$\mathcal{O}(N)$	Unclear	No
Bayesian networks	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$	No
Graphical models	$\mathcal{O}(N)$	Unclear	No
$k$ -Means clustering	$\mathcal{O}(kN)$	$\mathcal{O}(\log kN)$	Yes
Principal component analysis	$\mathcal{O}(N)$	$\mathcal{O}(\log N)$	No
Persistent homology	$\mathcal{O}(\exp N)$	$\mathcal{O}(N^5)$	No
Gaussian mixture models	$\mathcal{O}(\log N)$	$\mathcal{O}(\text{polylog } N)$	Yes
Variational autoencoder	$\mathcal{O}(\exp N)$	Unclear	No
Multilayer perceptrons	$\mathcal{O}(N)$	Unclear	No
Convolutional neural networks	$\mathcal{O}(N)$	$\mathcal{O}(\log N)$	No
Bayesian deep learning	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$	No
Generative adversarial networks	$\mathcal{O}(N)$	$\mathcal{O}(\text{polylog } N)$	No
Boltzmann machines	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$	No
Reinforcement learning	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$	No



QUANTINUUM



- hybrid algorithm with a lot of classical data preparation.
- classical part analyzed a dataset of 300,000 news articles from CNN and the Daily Mail and precomputed it with a BERT NLP classical deep learning model that handles sentences extraction and converts them into vectors.
- quantum part summarized text from respectively **20 to 8 and 14 to 8 sentences**, with Quantinuum QPUs H1-1 and H1-2 QPUs (20 and 14 qubits).
- **we are not yet in the quantum advantage regime with this number of qubits which can be emulated on a simple laptop!**

## Long Story Short: Researchers Say Quantum Computers May be Better at Summarizing Long Documents

BY MATT SWAYNE • JUNE 27, 2022 • RESEARCH

## Constrained Quantum Optimization for Extractive Summarization on a Trapped-ion Quantum Computer

Pradeep Niroula<sup>1,2,3,+</sup>, Ruslan Shaydulin<sup>1,+,\*</sup>, Romina Yalovetzky<sup>1,+</sup>, Pierre Minszen<sup>1</sup>, Dylan Herman<sup>1</sup>, Shaohan Hu<sup>1</sup>, and Marco Pistoia<sup>1</sup>

<sup>1</sup>JPMorgan Chase, New York, NY, USA

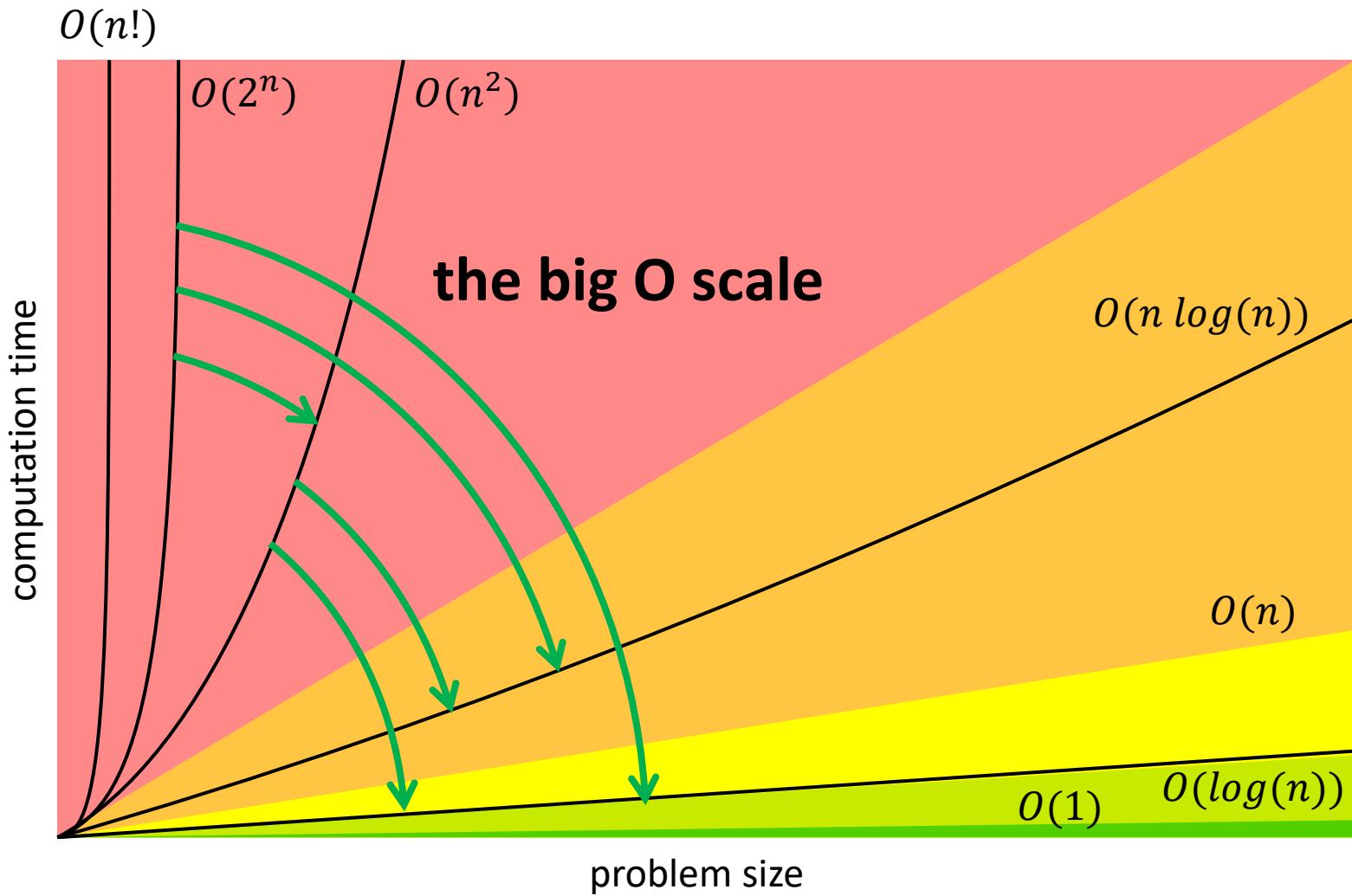
<sup>2</sup>Joint Center for Quantum Information and Computer Science, NIST/University of Maryland, College Park, MD, USA

<sup>3</sup>Joint Quantum Institute, University of Maryland, College Park, MD, USA

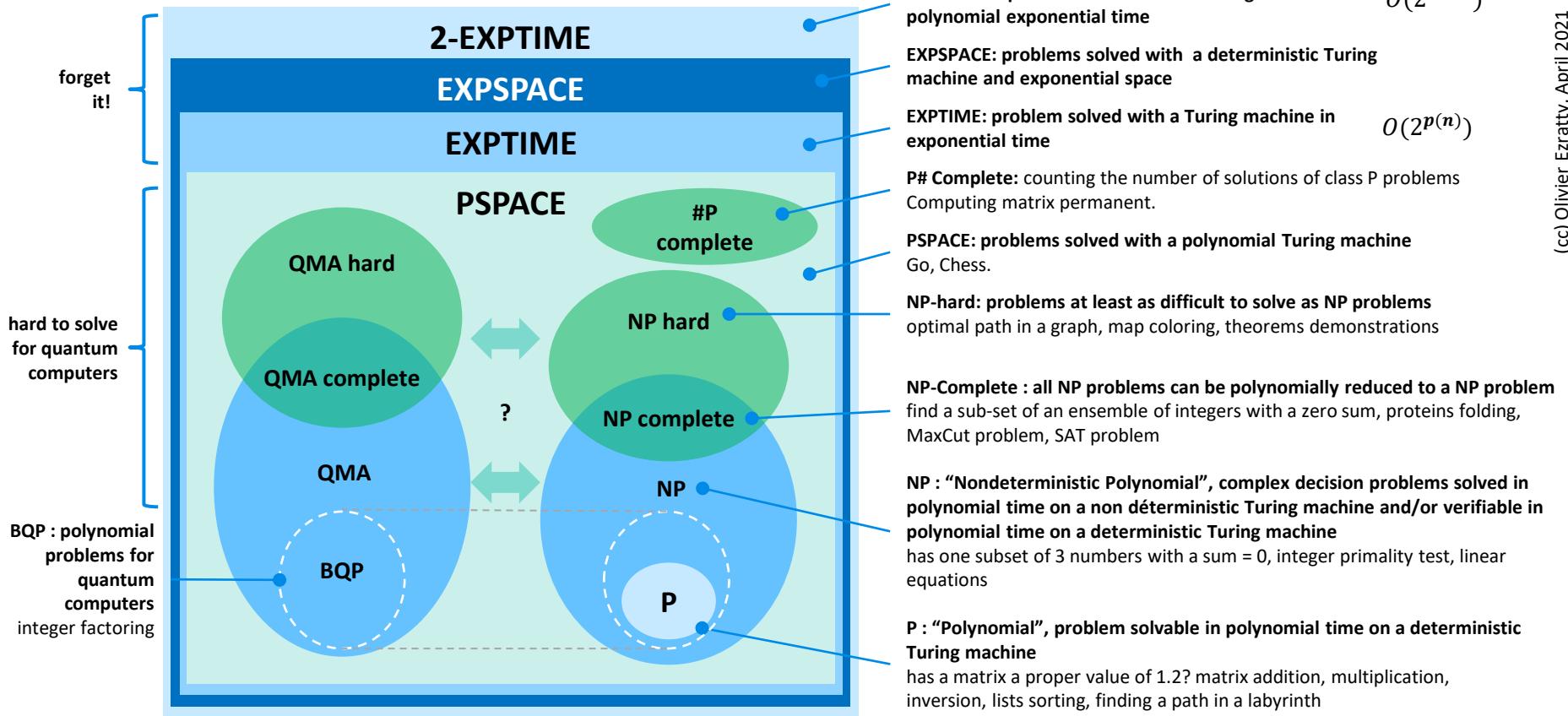
+These authors contributed equally.

\*ruslan.shaydulin@jpmchase.com

<https://arxiv.org/abs/2206.06290>

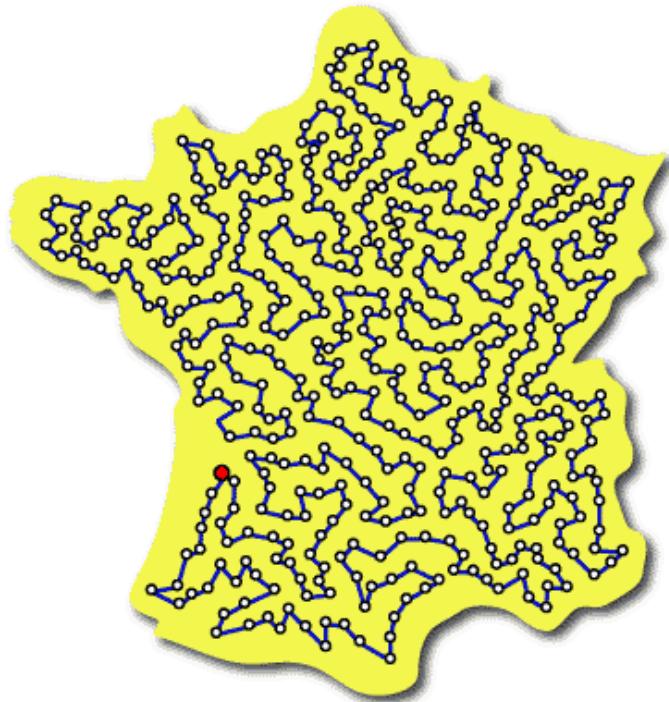
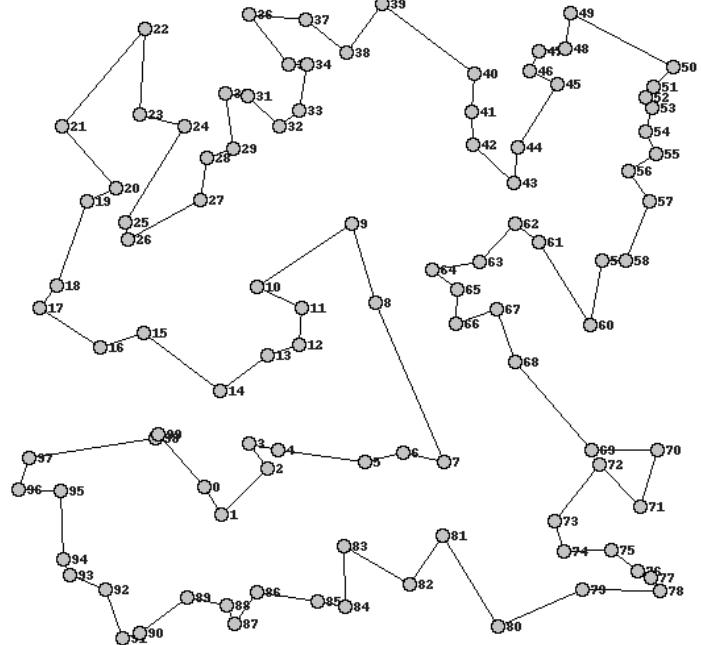


# problems complexity classes



# traveling salesperson problem

city100.txt: -4039.860428



what is the shortest possible route that visits each place exactly once and returns to the origin place : **NP-hard**

# MaxCut problem

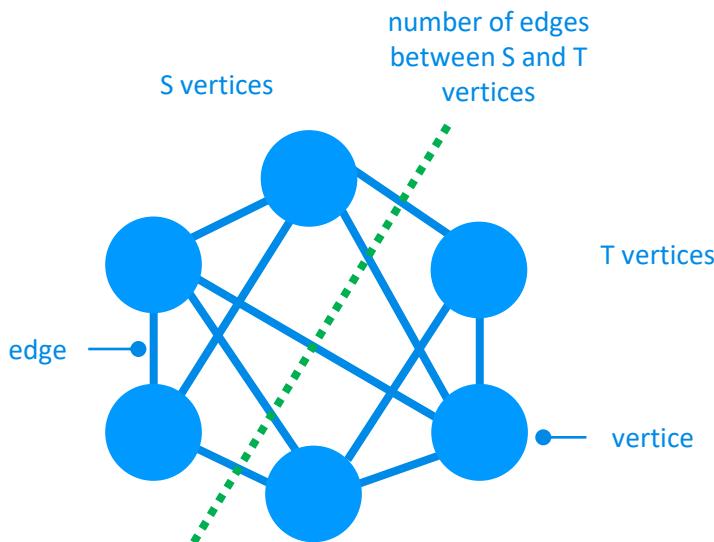
for a graph, a maximum cut is a cut whose size is at least the size of any other cut.

it is a partition of the graph's **vertices** into two complementary sets S and T, such that the number of **edges** between the set S and the set T is as large as possible. The problem of finding a maximum cut in a graph is known as the Max-Cut Problem. It's a NP-complete problem.

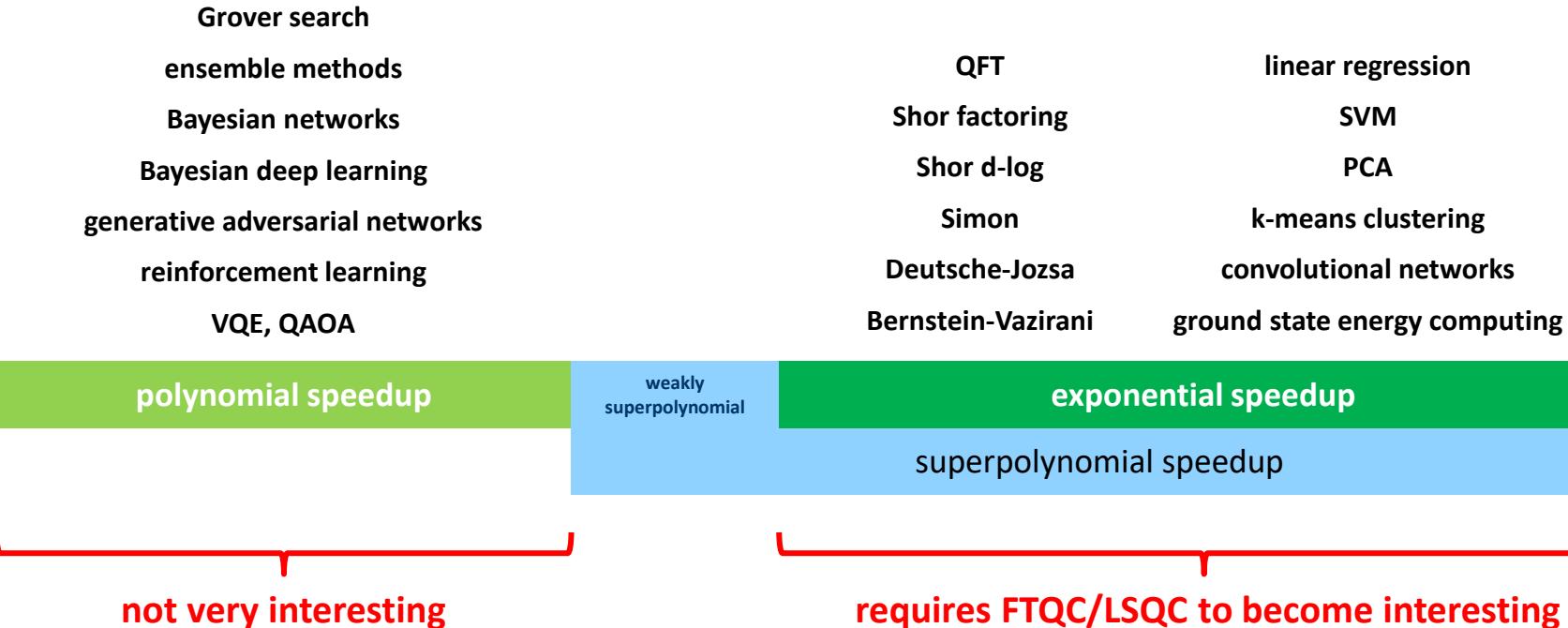
one wants a subset S of the vertex set such that the number of edges between S and the complementary subset is as large as possible. Equivalently, one wants a bipartite subgraph of the graph with as many edges as possible.

can be solved with an **Ising model** on quantum annealing or with a **QAOA hybrid** algorithm and requires hundreds of qubits to provide some acceleration

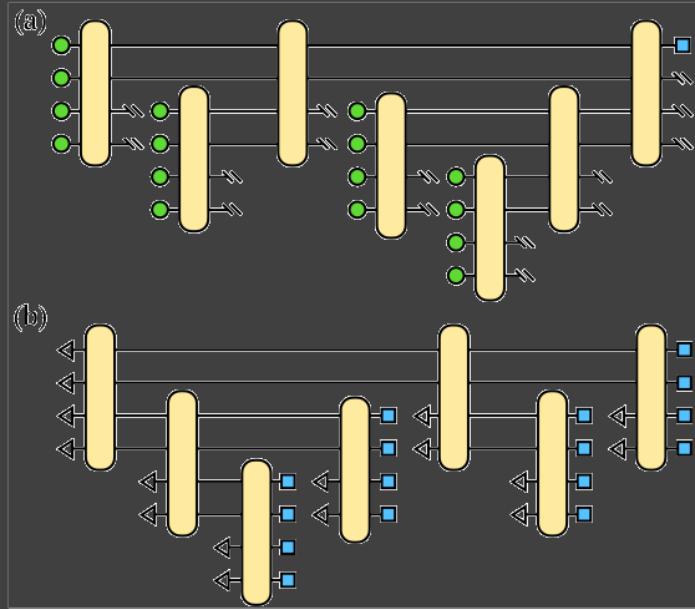
applications in VLSI design and machine scheduling



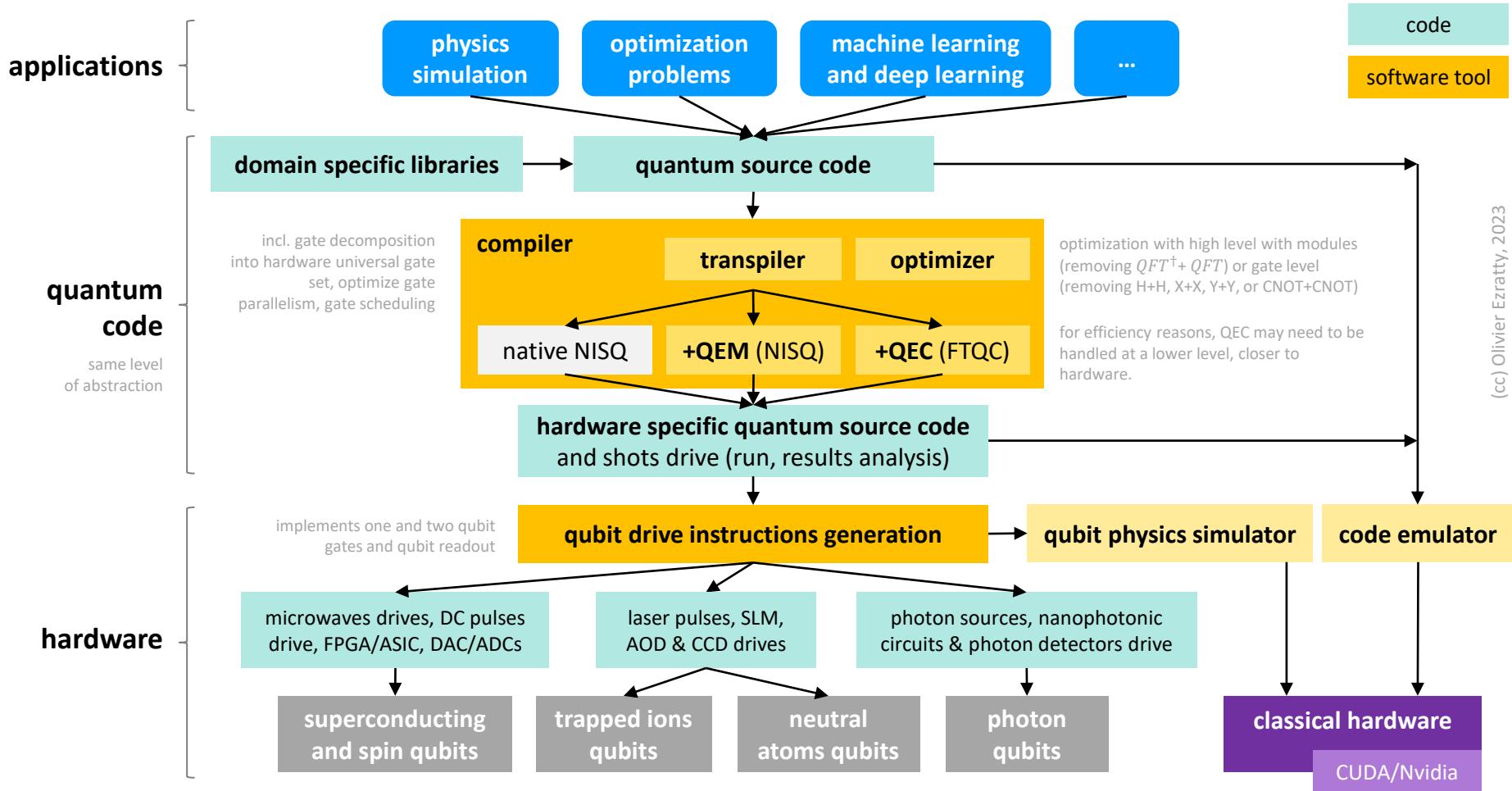
# quantum speedups categories



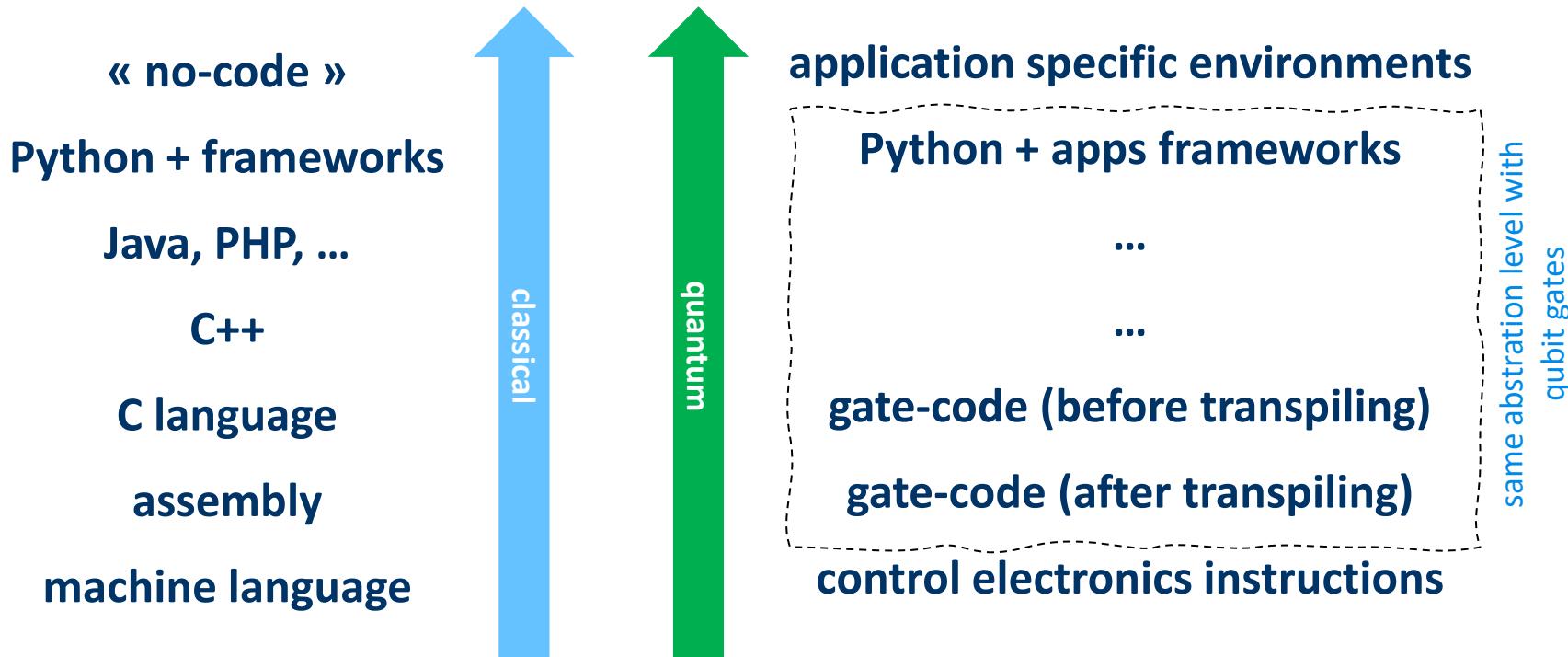
(cc) Olivier Ezratty, 2022

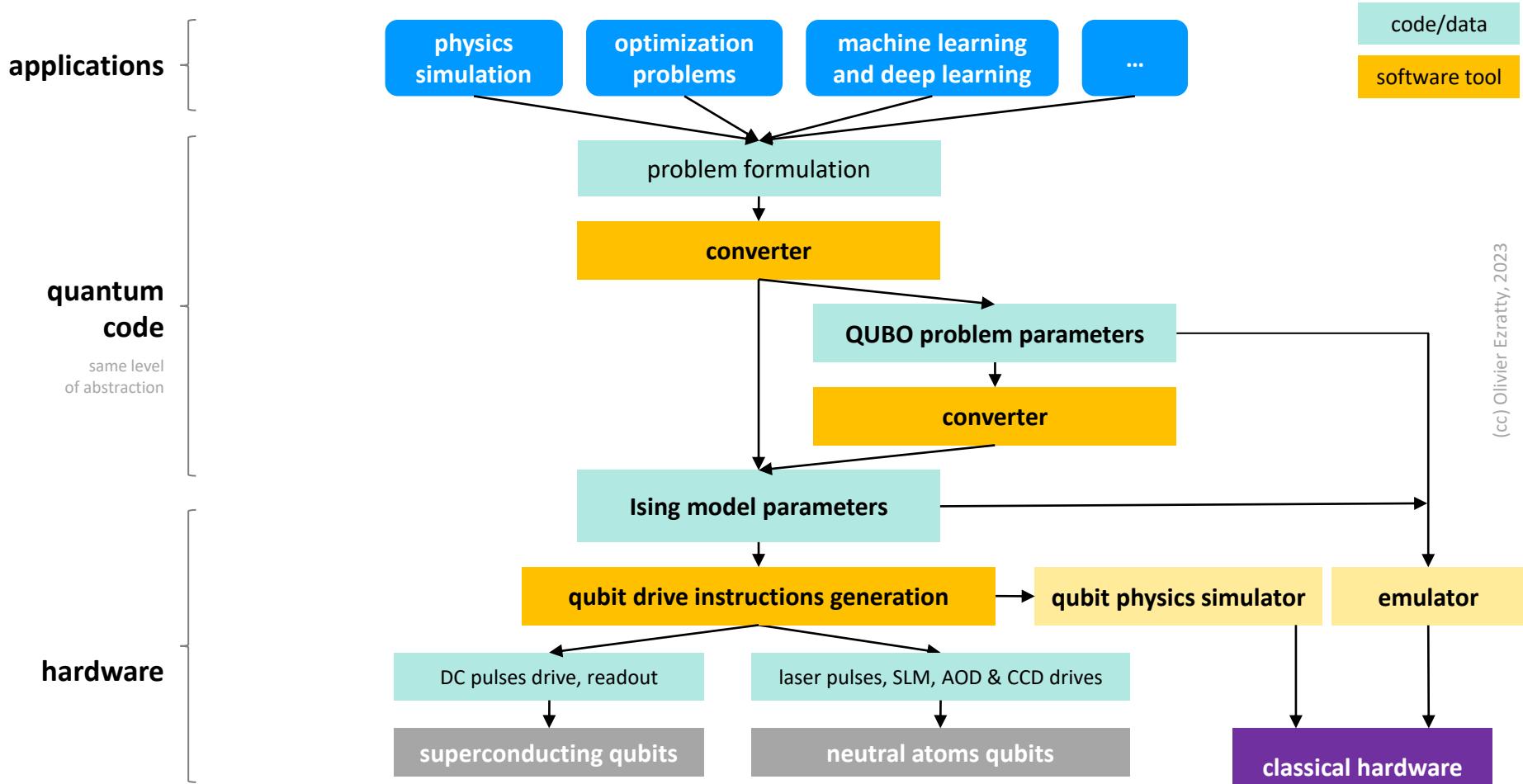


# development tools



# coding abstraction levels?





Year	Language	Reference(s)	Semantics	Host Language	Paradigm
1996	Quantum Lambda Calculi	[181]	Denotational	lambda Calculus	Functional
1998	QCL	[206–209]		C	Imperative
2000	qGCL	[241, 312–314]	Operational	Pascal	Imperative
2003	$\lambda_q$	[282, 283]	Operational	Lambda Calculus	Functional
2003	Q language	[32, 33]		C++	Imperative
2004	QFC (QPL)	[245–247]	Denotational	Flowchart syntax (Textual syntax)	Functional
2005	QPAAlg	[141, 160]		Process calculus	Other
2005	QML	[10, 11, 113]	Denotational	Syntax similar to Haskell	Functional
2004	CQP	[102–104]	Operational	Process calculus	Other
2005	cQPL	[180]	Denotational		Functional
2006	LanQ	[188–191]	Operational	C	Imperative
2008	NDQJava	[298]		Java	Imperative
2009	Cove	[227]		C#	Imperative
2011	QuECT	[48]		Java	Circuit
2012	Scaffold	[1, 138]		C (C++)	Imperative
2013	QuaFL	[162]		Haskell	Functional
2013	Quipper	[114, 115]	Operational	Haskell	Functional
2013	Chisel-Q	[175]		Scala	Imperative, functional
2014	LIQUI $\rangle$	[292]	Denotational	F#	Functional
2015	Proto-Quipper	[234, 237]		Haskell	Functional
2016	QASM	[212]		Assembly language	Imperative
2016	FJQuantum	[82]		Feather-weight Java	Imperative
2016	ProjectQ	[122, 266, 272]		Python	Imperative, functional
2016	pyQuil (Quil)	[259]		Python	Imperative
2017	Forest	[61, 259]		Python	Declarative
2017	OpenQASM	[66]		Assembly language	Imperative
2017	qPCF	[213, 215]		Lambda calculus	Functional
2017	QWIRE	[217]		Coq proof assistant	Circuit
2017	cQASM	[146]		Assembly language	Imperative
2017	Qiskit	[4, 232]		Python	Imperative, functional
2018	IQu	[214]		Idealized Algol	Imperative
2018	Strawberry Fields	[147, 148]		Python	Imperative, functional
2018	Blackbird	[147, 148]		Python	Imperative, functional
2018	QuantumOptics.jl	[157]		Julia	Imperative
2018	Cirq	[271]		Python	Imperative, functional
2018	Q $\#$	[269]		C#	Imperative
2018	Q SI $\rangle$	[174]		.Net language	Imperative
2020	Silq	[35]		Python	Imperative, functional

- **imperative languages:** describe step by step algorithms. Contains C, C++, PHP, Java, Scaffold, Quipper, QASM, Q#.
- **functional languages:** define various functions that called on an ad-hoc fashion by the program. Loops (for, while) are replaced by functions recursivity and there are no/few modifiable variables. Enable the use of high level abstract data types handled by functions. Are more concise languages.

# using IBM qiskit

IBM Quantum Experience

File Edit Inspect View Share Help

Run settings Run on ibmq\_santiago

Job run settings System: ibmq\_santiago Provider: ibm-q/open/main Shots (max 8192): 1024 Job limit: 4 remaining

Circuits / Vector state readout Saved Simple Hadamard and vector state readout

Simulator seed 5430 </> Code Docs Jobs

+ Add

Quantum circuit diagram:

```
graph LR; q0((q0)) -- H --> q1((q1)); q1 --+--> q2((q2)); q2 --+--> q3((q3)); q3 -- Rz --> q0; q3 -- Rz --> q1; q3 -- Rz --> q2; q3 -- Rz --> q3
```

Code editor

OpenQASM 2.0

```
OPENQASM 2.0;
include "qelib1.inc";
qreg q[3];
creg c[3];
h q[0];
cx q[0],q[1];
cx q[1],q[2];
measure q[0] -> c[0];
measure q[1] -> c[1];
measure q[2] -> c[2];
```

Statevector

Amplitude

Computational basis states

Measurement Probabilities

Measurement probability (%)

Computational basis states

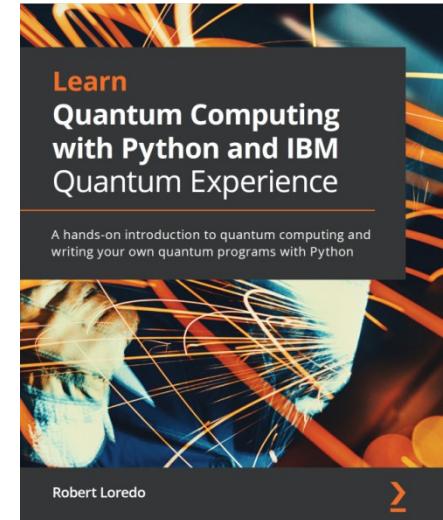
Output state

Show more

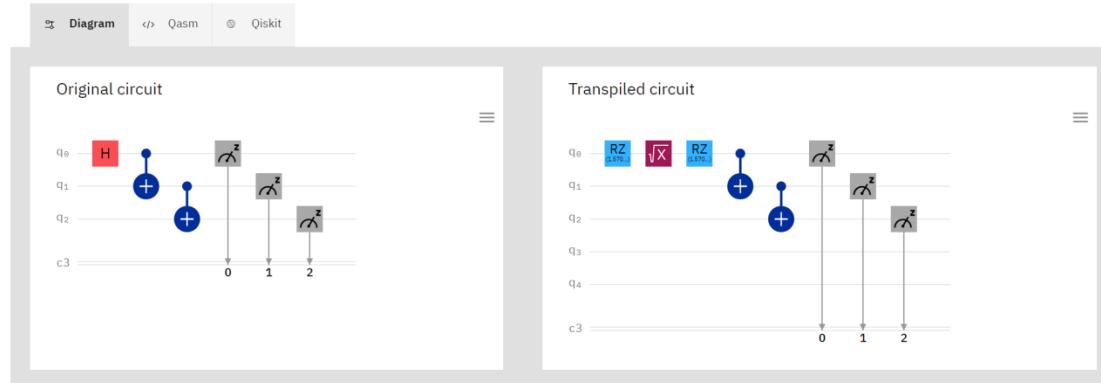
Phase 0

$\pi/2$

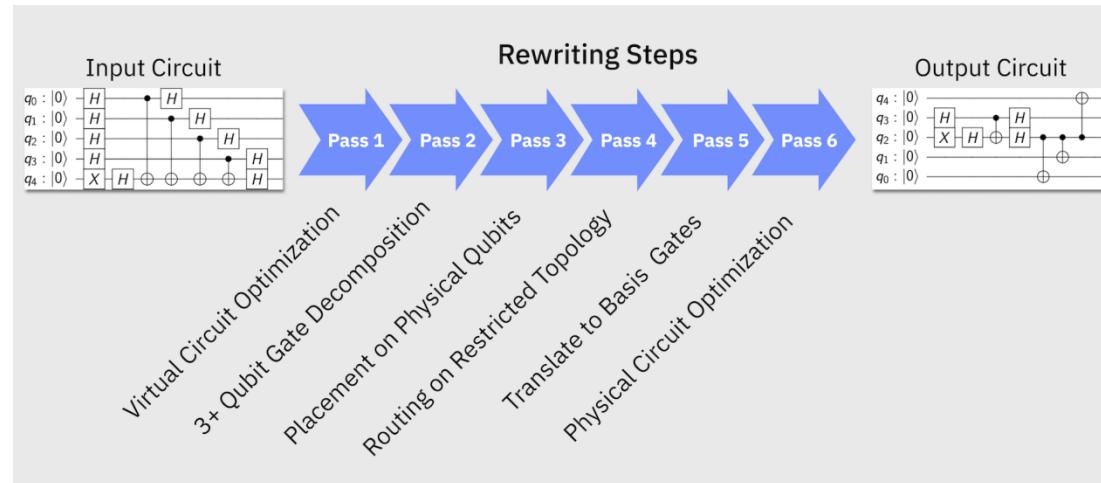
$3\pi/2$



### Circuit



**before execution, qiskit circuits  
are transpiled to be adapted to  
the physical gates implemented  
in the superconducting chipset  
and to the geometry linking  
qubits with each other**



## Compute resources

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

[Learn more](#)

Your resources

All Systems

All Simulators

New pay-as-you-go access to 27 qubit systems on IBM Cloud [Learn more](#)

Card | Table

Search by system name

<b>ibm_washington</b> System status: <span style="color: green;">● Online</span> Processor type: Eagle r1  Qubits: 127 QV: 64 CLOPS: 850	<b>ibm_sherbrooke</b> System status: <span style="color: green;">● Online</span> Processor type: Eagle r3  Qubits: 127 QV: 32 CLOPS: 904	<b>ibm_kyiv</b> <span style="background-color: yellow; border-radius: 50%; padding: 2px 5px;">●</span> Online - Queue paused maintenance Processor type: Eagle r3  Qubits: 127	<b>ibm_ithaca</b> <span style="background-color: yellow; border-radius: 50%; padding: 2px 5px;">●</span> Online - Queue paused maintenance Processor type: Hummingbird r3  Qubits: 65	<b>ibm_prague</b> System status: <span style="color: green;">● Online</span> Processor type: Egret r1  Qubits: 33	<b>ibmq_kolkata</b> System status: <span style="color: green;">● Online</span> Processor type: Falcon r5.11  Qubits: 27 QV: 128 CLOPS: 2K
<b>ibmq_montreal</b> System status: <span style="color: green;">● Online</span> Processor type: Falcon r4  Qubits: 27 QV: 128 CLOPS: 2K	<b>ibmq_mumbai</b> System status: <span style="color: green;">● Online</span> Processor type: Falcon r5.10  Qubits: 27 QV: 128 CLOPS: 1.8K	<b>ibm_cairo</b> System status: <span style="color: green;">● Online</span> Processor type: Falcon r5.11  Qubits: 27 QV: 64 CLOPS: 2.4K	<b>ibm_aukland</b> <span style="background-color: yellow; border-radius: 50%; padding: 2px 5px;">●</span> Online Processor type: Falcon r5.11  Qubits: 27 QV: 64 CLOPS: 2.4K	<b>ibm_hanoi</b> System status: <span style="color: green;">● Online</span> Processor type: Falcon r5.11  Qubits: 27 QV: 64 CLOPS: 2.3K	<b>ibmq_geneva</b> <span style="background-color: yellow; border-radius: 50%; padding: 2px 5px;">●</span> Online Processor type: Falcon r8  Qubits: 27 QV: 32 CLOPS: 1.9K
<b>ibmq_toronto</b> System status: <span style="color: green;">● Online</span> Processor type: Falcon r4  Qubits: 27 QV: 32 CLOPS: 1.8K	<b>ibmq_peekskill</b> <span style="background-color: yellow; border-radius: 50%; padding: 2px 5px;">●</span> Online Processor type: Falcon r8  Qubits: 27	<b>ibmq_guadalupe</b> System status: <span style="color: green;">● Online</span> Processor type: Falcon r4P  Qubits: 16 QV: 32 CLOPS: 2.4K	<b>ibm_perth</b> <span style="background-color: yellow; border-radius: 50%; padding: 2px 5px;">●</span> Online - Queue paused maintenance Processor type: Falcon r5.11H  Qubits: 7 QV: 32 CLOPS: 2.9K	<b>ibm_lagos</b> System status: <span style="color: green;">● Online</span> Processor type: Falcon r5.11H  Qubits: 7 QV: 32 CLOPS: 2.7K	<b>ibmq_nairobi</b> <span style="background-color: yellow; border-radius: 50%; padding: 2px 5px;">●</span> Online Processor type: Falcon r5.11H  Qubits: 7 QV: 32 CLOPS: 2.6K
<b>ibm_oslo</b> System status: <span style="color: green;">● Online</span> Processor type: Falcon r5.11H  Qubits: 7 QV: 32 CLOPS: 2.6K	<b>ibmq_jakarta</b> <span style="background-color: yellow; border-radius: 50%; padding: 2px 5px;">●</span> Online - Queue paused maintenance Processor type: Falcon r5.11H  Qubits: 7 QV: 16 CLOPS: 2.4K	<b>ibmq_manila</b> System status: <span style="color: green;">● Online</span> Processor type: Falcon r5.11L  Qubits: 5 QV: 32 CLOPS: 2.8K	<b>ibmq_quito</b> System status: <span style="color: green;">● Online</span> Processor type: Falcon r4T  Qubits: 5 QV: 16 CLOPS: 2.5K	<b>ibmq_belem</b> <span style="background-color: yellow; border-radius: 50%; padding: 2px 5px;">●</span> Online - Queue paused internal Processor type: Falcon r4T  Qubits: 5 QV: 16 CLOPS: 2.5K	<b>ibmq_lima</b> <span style="background-color: yellow; border-radius: 50%; padding: 2px 5px;">●</span> Online - Queue paused internal Processor type: Falcon r4T  Qubits: 5 QV: 8 CLOPS: 2.7K

all the IBM Q

Experience quantum units available online,  
up to 127 qubits, as of  
March 25<sup>th</sup>, 2023

# IBM 127 qubits performance

ibm\_washington

[OpenQASM 3](#)

## Details

**127**

Qubits

Status: ● Online - Queue paused

Median CNOT Error: 1.249e-2

Total pending jobs: 535 jobs

Median Readout Error: 1.390e-2

**64**

QV

Processor type ①: Eagle r1

Median T1: 102.58 us

**850**

CLOPS

Version: 1.6.15

Median T2: 96.32 us

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

ibm\_sherbrooke

[OpenQASM 3](#)

## Details

**127**

Qubits

Status: ● Online

Median ECR Error: 6.608e-3

Total pending jobs: 877 jobs

Median Readout Error: 9.900e-3

**32**

QV

Processor type ①: Eagle r3

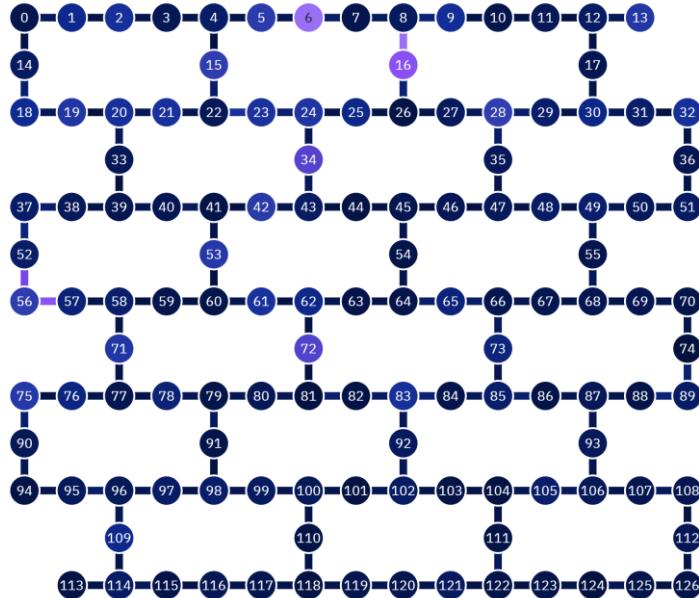
Median T1: 288.47 us

**904**

CLOPS

Version: 1.2.7

Median T2: 166.14 us



as of March 25<sup>th</sup>, 2023

Created

Transpiling

776ms

Validating

913ms

In queue

4m 42s

Running

4.9s

Completed

## Run details

Backend

ibmq\_quito

Run mode

fairshare

Shots

1024

Status:

COMPLETED

Time taken

4m 51.9s

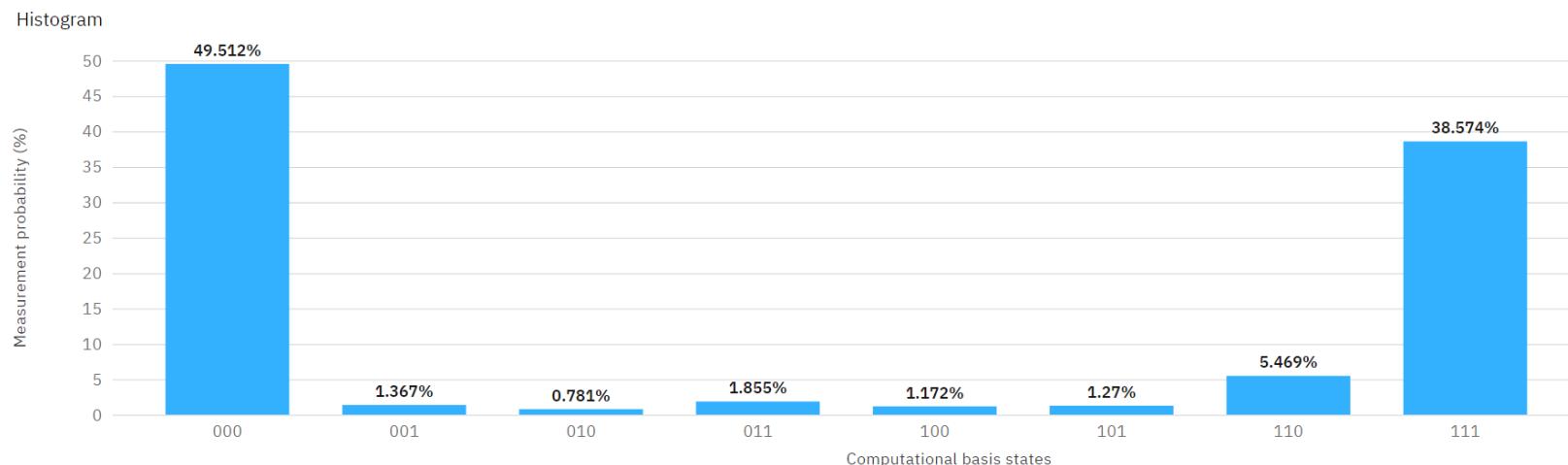
Last Update

Feb 13, 2021 9:13 AM

## Result

**the two entangled states  $|000\rangle$  and  $|111\rangle$  were well detected  
but with a significant error for  $|111\rangle$ .**

### Histogram



# main vendors development tools



visual programming and integrated development environments

thematic quantum libraries  
(chemistry, finance, machine learning, ...)

generic quantum libraries / full-stack

high level machine language  
(quantum circuits)

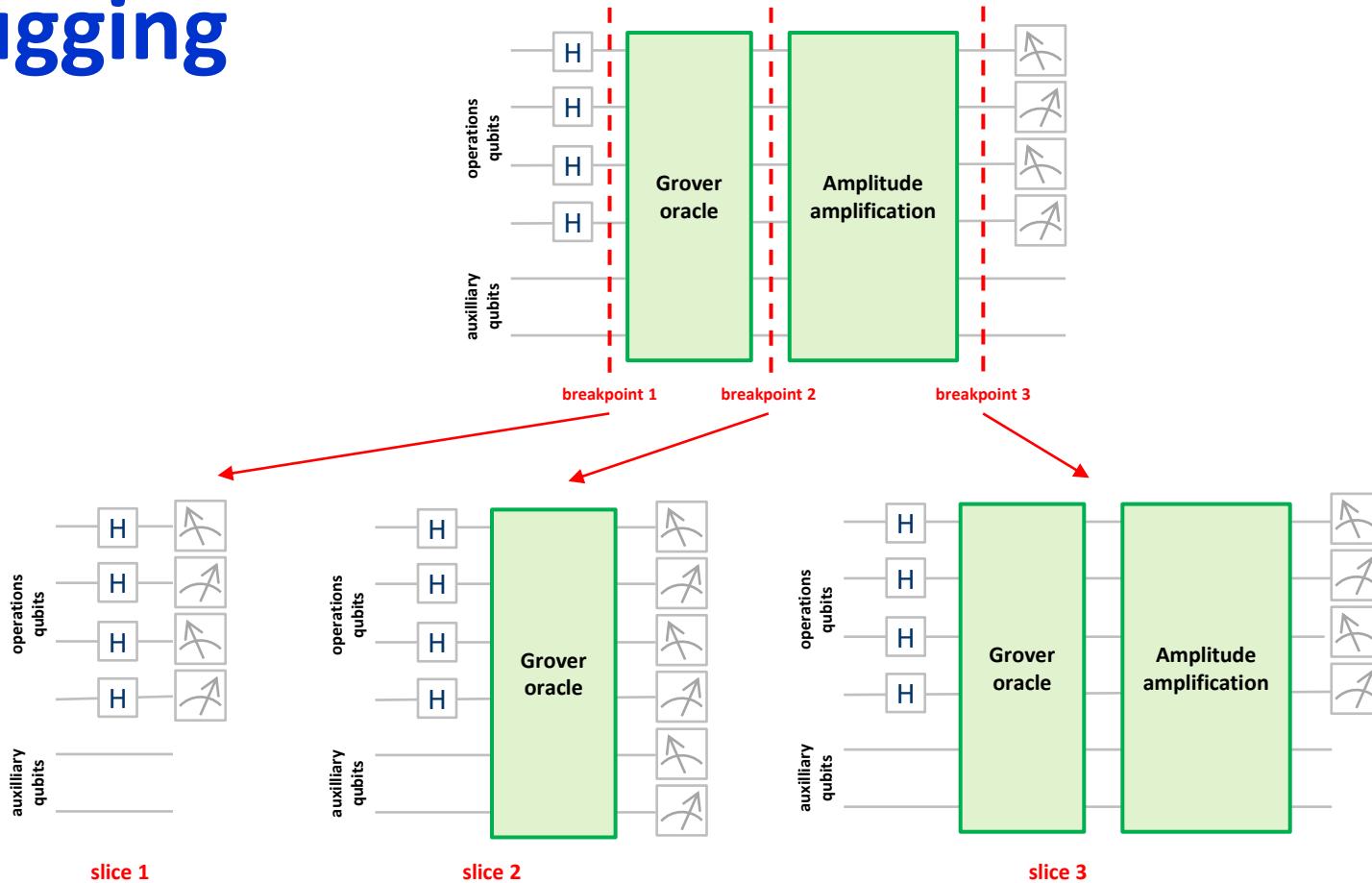
low level machine language

qubits and quantum gates

Quantum Experience	Forest	OCEAN		Quantum Playground	Visual Studio	PENNY LANE	QLIB
QisKit Aqua	OpenFermion	BQM CQM	PENNY LANE	OpenFermion	Quantum Chemistry PNNL	PENNY LANE	QLIB
QisKit	Grove QAOA	qbsolv QUBO		Cirq	Quantum Developer Kit		Braket SDK
QisKit Terra	PyQuil	QMASM			Q#		
Open QASM	QUIL Quil-T	QMI	Blackbird	many machine languages		rigetti	Cirq QPU
super-conducting	super-conducting	quantum annealing	qumodes photons, GBS	super-conducting	topologic, IonQ, Quantinuum	IONQ OQC	any

schema inspired from Alba Cervera-Lierta for the QWA 2018, updated in April 2023  
[https://medium.com/@quantum\\_wa/quantum-computing-languages-landscape-1bc6dedb2a35](https://medium.com/@quantum_wa/quantum-computing-languages-landscape-1bc6dedb2a35)

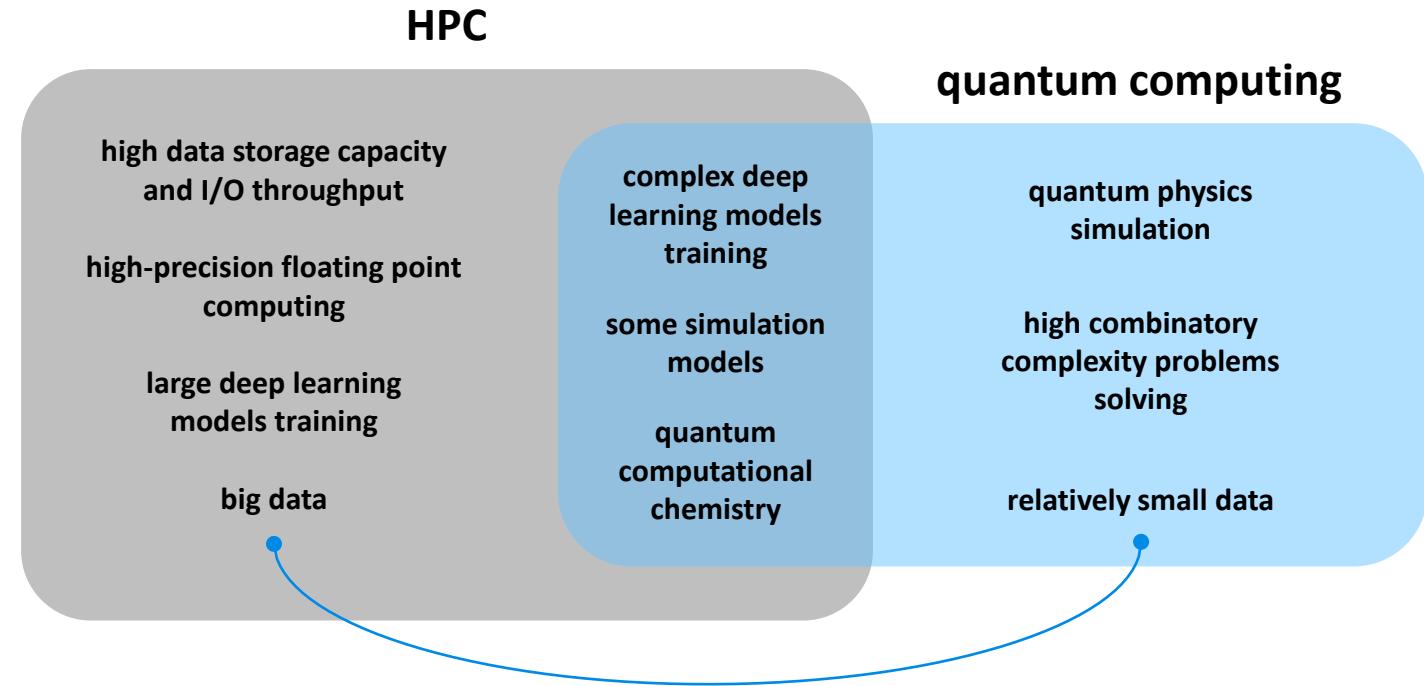
# debugging



Inspired by « A Tool For Debugging Quantum Circuits » by Sara Ayman Metwali and Rodney Van Meter, Keio University, May 2022 (111 pages)

# will quantum computers replace HPCs?

no, quantum computers will expand HPC capabilities as coprocessors  
in « hybrid classical/quantum systems »



Très Grand Centre de calcul du CEA

in 2023, with Pasqal



in 2023, with IQM

# quantum computing cloud offerings

quantum computing emulation

hybrid computing centers



40 qubits  
**Atos**

**Atos**  
QUANDELA

36 qubits

34-50 qubits

30 qubits

40 qubits

hybrid quantum



in 2023

PASQAL  
100 qubits (simulation)

QUANDELA

...

IBM  
5 to 127 qubits

D-Wave  
5000 qubits (annealing)  
 PASQAL  
100 qubits (simulation)

IONQ

32 qubits

IONQ

32 qubits

IONQ

11 qubits

rigetti

80 qubits

rigetti

80 qubits

OQC

8 qubits

QUANTINUUM

12 qubits

D-Wave

QCWARE

XANADU

Quantum Inspire - By QuTech

QuEra COMPUTING INC. XANADU

(cc) Olivier Ezratty, 2022

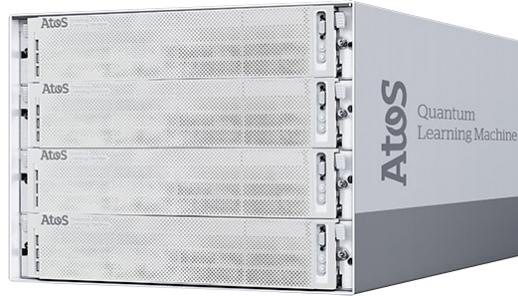
# quantum emulators

emulators characteristics:

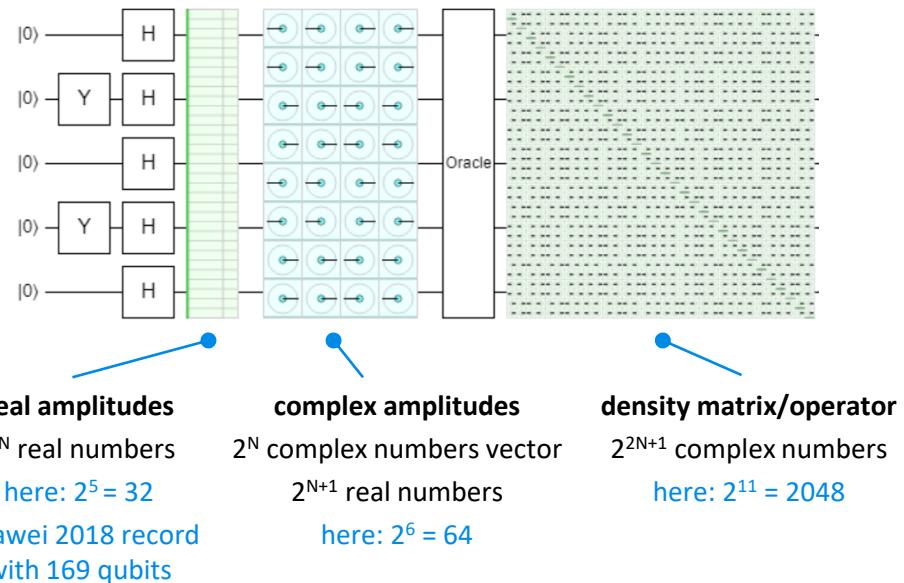
- hardware executing classical software emulating quantum gates and algorithms
- laptop until 30 qubits
- a large server until 48 qubits
- a data-center or HPC from 50 to 200 qubits, depending on the type of emulation
- constraints: available memory and storage + latency

use cases:

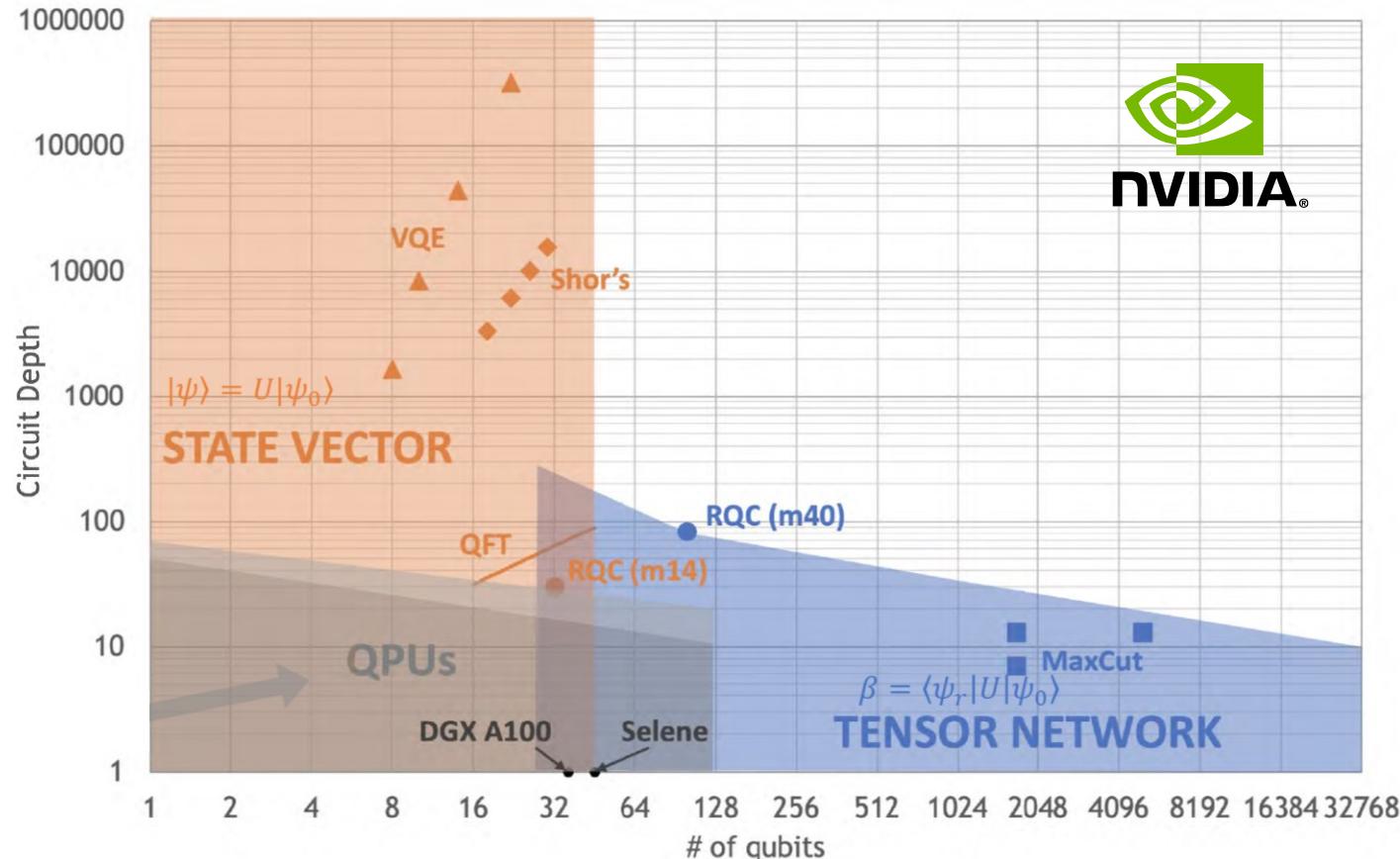
- learning quantum development
- quantum code debug and verification
- simulating qubits characteristics
- simulating quantum error correction
- **not benchmarking quantum vs classical algorithms since the classical equivalent is usually a classical non quantum algorithm**



Atos aQLM emulates up to 41 qubits with full density matrix



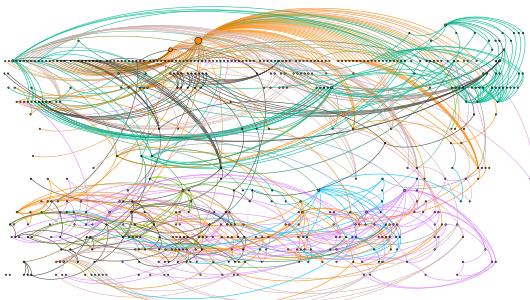
## Researching & Developing the Computers of Tomorrow Requires Powerful Simulations Today



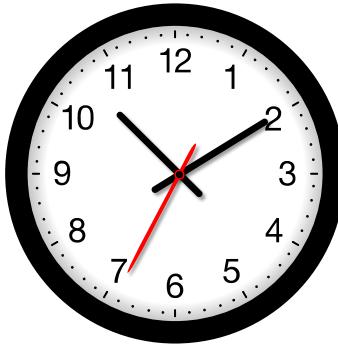
# benchmarking

## quantum supremacy and quantum advantages

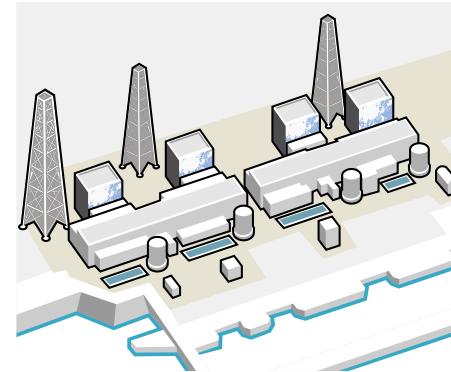
# quantum supremacy or advantage?



and  
/  
or



and  
/  
or



**complex problem**  
unreachable in human time  
for classical computing

**much faster resolution**  
than classical computing and  
useful task with input data

**energy, cost, weight**  
better with quantum  
computing

aka « quantum supremacy »  
or « quantum primacy »

aka « quantum advantage »

aka « quantum energy  
advantage » or « quantum  
energy supremacy/primacy »

**sometimes used as synonyms...**

# supremacy relativity...

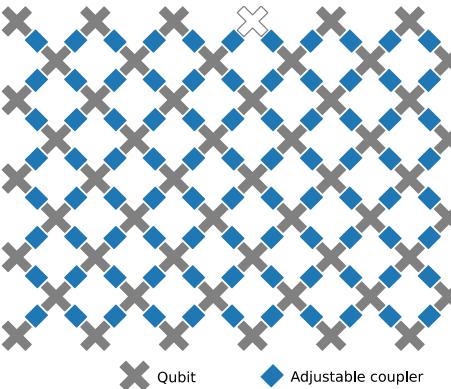
nature

Explore content ▾ About the journal ▾ Publish with us ▾

nature > articles > article

Article | Published: 23 October 2019

## Quantum supremacy using a programmable superconducting processor



### A density-matrix renormalization group algorithm for simulating quantum circuits with a finite fidelity

Thomas Ayral,<sup>1</sup> Thibaud Louvet,<sup>2</sup> Yiqing Zhou,<sup>3</sup> Cyprien Lambert,<sup>1</sup> E. Miles Stoudenmire,<sup>4</sup> and Xavier Waintal<sup>2</sup>

<sup>1</sup>Atos Quantum Laboratory, Les Clayes-sous-Bois, France

<sup>2</sup>PHELIQS, Université Grenoble Alpes, CEA, Grenoble INP, IRIG, Grenoble 38000, France

<sup>3</sup>Department of Physics, Cornell University, Ithaca, NY 14853, USA

<sup>4</sup>Center for Computational Quantum Physics, Flatiron Institute, New York, NY 10010, USA

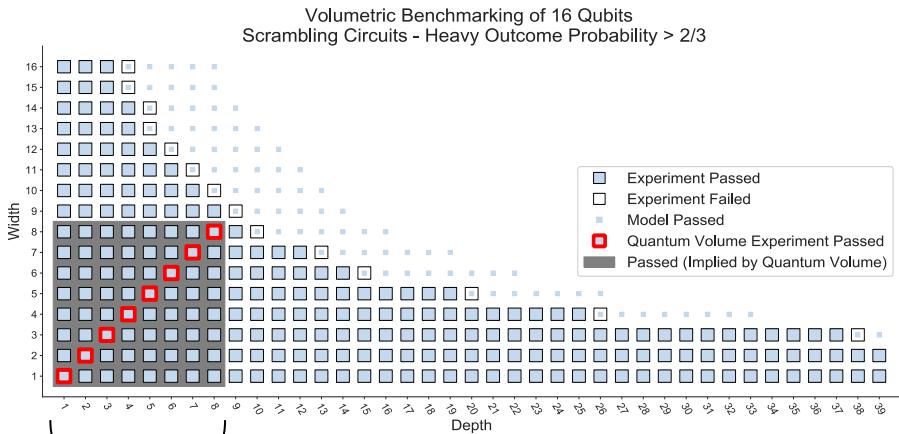
(Dated: August 30, 2022)

- 2.5 mn computing time.
- compared with IBM Summit 10K years (Google) / 2.5 days (IBM rebuttal). 25 kW vs 20 MW.
- 53 qubits.
- yields good results 0.15% of the time.
- cross-entropy benchmarking (XEB) with no input data.

- 8 hours on a single core of an Atos QLM appliance.
- tensor networks based.
- scales linearly with the number of noisy qubits.

# quantum volumes

Year	Brand	Version	Hw Qubits	Log2(QV)	%
2017	IBM	Tenerife	5	2	40%
2018	IBM	Tokyo	20	3	15%
2019	IBM	Johannesburg	20	4	20%
2020	Honeywell		4	4	100%
2020	IBM	Raleigh	28	5	18%
2020	IBM	Montreal	27	6	22%
2020	Honeywell	H0	6	6	100%
2021	IBM	Montreal	27	7	26%
2020	Honeywell	H1-1	10	7	70%
2021	Honeywell	H1-1	10	9	90%
2021	Honeywell	H1-1	10	10	100%
2022	IBM	Manhattan	127	6	5%
2020	IonQ	Aria	32	22	69%
2022	Quantinuum	H1-2	12	12	100%
2022	Quantinuum	H1-1	22	13	59%
2023	Quantinuum	H1-1	22	15	68%



**required error rates**

$$\epsilon \ll \frac{1}{(\log_2(QV))^2}$$

for 40 qubits  $1 - \epsilon \gg 99, 93\%$

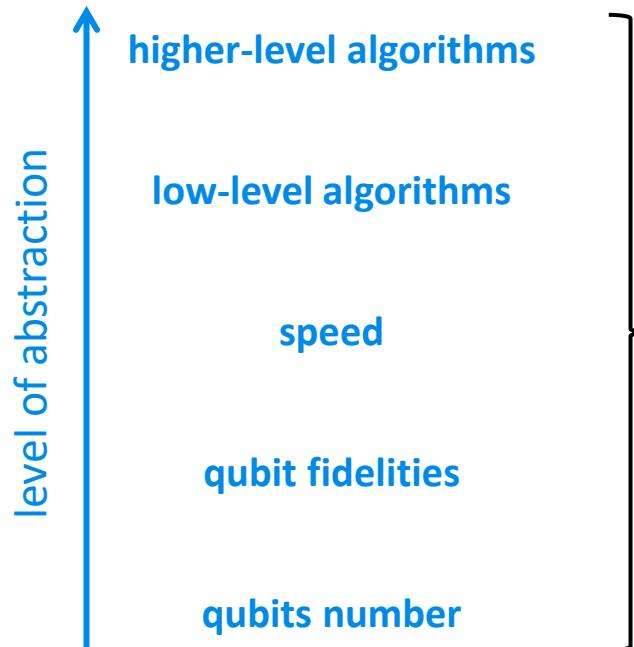
for 50 qubits  $1 - \epsilon \gg 99, 96\%$

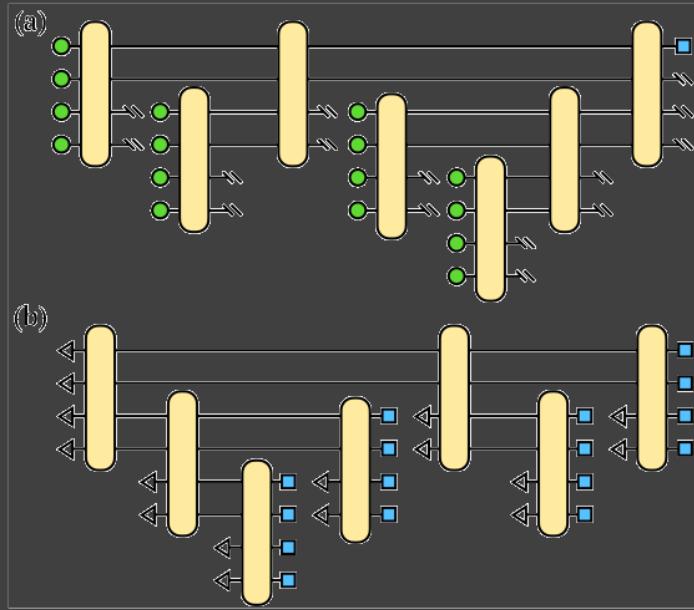
# what can be benchmarked in QC?

THALES BACQ  
myQLM/qscore  
SupermarQ QED-C  
TU Delft: QPack

IBM CLOPS  
randomized  
benchmarking

IBM QV





# use cases in financial services

problem category	use cases	classical solutions	quantum solutions
<b>simulation</b>	<ul style="list-style-type: none"> <li>• derivative pricing</li> <li>• risk analysis (Basel, Solvency)</li> <li>• financial econometrics</li> <li>• maximum likelihood estimation</li> <li>• dynamic stochastic general equilibrium modelling (DSGE)</li> <li>• dynamic economic models.</li> </ul>	<ul style="list-style-type: none"> <li>• Monte Carlo integration</li> <li>• machine learning</li> <li>• Black-Scholes model</li> </ul>	<ul style="list-style-type: none"> <li>• quantum amplitude estimation in quantum Monte Carlo</li> <li>• quantum machine learning</li> </ul>
<b>optimization</b>	<ul style="list-style-type: none"> <li>• portfolio optimization</li> <li>• trading optimization</li> <li>• hedging</li> <li>• optimal arbitrage</li> <li>• credit scoring</li> <li>• financial crash prediction</li> </ul>	<ul style="list-style-type: none"> <li>• discrete/continuous variables</li> <li>• branch-and-bound for non-convex cases</li> <li>• interior-point methods for certain convex cases</li> </ul>	<ul style="list-style-type: none"> <li>• quantum optimization</li> <li>• quantum annealing with QUBO or NISQ QAOA</li> <li>• reverse quantum annealing</li> <li>• VQE</li> </ul>
<b>machine learning</b>	<ul style="list-style-type: none"> <li>• anomaly and fraud detection</li> <li>• natural language modeling</li> <li>• risk clustering</li> <li>• modeling credit spread</li> <li>• product recommendation</li> </ul>	<ul style="list-style-type: none"> <li>• regression, classification, clustering, PCA</li> <li>• deep learning</li> <li>• unsupervised cluster analysis</li> </ul>	<ul style="list-style-type: none"> <li>• quantum SVM, PCA, ...</li> <li>• quantum machine learning (QCNN, QGAN, QGNN, ...)</li> <li>• quantum cluster analysis</li> </ul>

source: adapted from “A Survey of Quantum Computing for Finance” by Dylan Herman et al, JP Morgan, Universities of Chicago, Delaware, DoE Argonne National Lab and Menter AI, January 2022 (56 pages).

# Illustration : 14 use cases in financial institutions

	Use cases	Unlock capability / value	Typical industry	FI publicly experimenting
Optimization	1 Portfolio selection, alloc. & optimization	Increase both the scope of assets that can be taken into account and dynamic multi-period scenarios that can be considered	Asset Management, Global Markets	Natwest, BBVA, Commerzbank, Standard Chartered, CBA, Nomura
	2 Optimal execution	Design the best execution strategy for entry, exit and rebalancing	Asset Management, Global Markets	-
	3 Capital allocation	Allow dynamic capital allocation without making oversimplifications (credit risk and insurance risk in particular)	All Financial Institutions	-
	4 Asset Liability Management	Increase the number or detail of assets and run much more detailed scenarios	Universal Banks, Asset Managers	-
	5 Transaction settlement	Ensure that large volume of trades is settled in the most optimized sequence and prioritization.	Global Markets, Transaction Banking, Clearing House	Barclays, Mastercard
	6 Yield curve fitting	Can solve much complex models to improve yield curve fitting accuracy	Global Markets, HFT	-
Machine Learning	7 Credit scoring / clustering	Build more realistic models thanks to the ability to take into account more variables and speed-up the training process	Retail banking	CaixaBank, Crédit Agricole
	8 Default early warnings	Improve detection of changing customer behaviours indicative of financial stress leveraging much more complex datasets	Retail banking	-
	9 Fraud detection / AML	Identify outliers based on a growing number of variables, which will lead to better adjusted models	Retail & Transaction banking, Global Markets	-
	10 Next Best Action / Product	Rely on more consistent clusters defined with a wider range of variables to improve outputs of predictive analytics	Retail and Private Banking, Insurance	-
Simulation	11 Derivative pricing	Improve dramatically the accuracy and efficiency of complex option pricing such as path-dependent and barrier options	Global Markets	JP Morgan, Goldman Sachs, BMO, Scotiabank
	12 Valuation and regulatory ratios	Perform computation on much wider and complex scenarios (VaR, XVA, valuation of credit derivatives, Solvency 2)	Banking, Insurance	HSBC
	13 Risk assessment & tail risk simulations	Compute a wide range of intraday complex stress tests, potentially even on a real time basis	Banking, Insurance	CaixaBank
	14 Multi-factor Interest rate models	Allow to take into account more realistic assumptions	Global Markets	-

# bank trials 1/4

customer	hw vendor	sw vendor	when	application
Deutsche Bank	D-Wave	1QBit	2016	Working with LBNL and the CME group for the creation of the Quantumforquants web site. (abandoned).
Mastercard	D-Wave		2022	multiyear collaboration on quantum-hybrid applications for optimizing consumer loyalty and rewards programs, cross-border settlement, and fraud management. <a href="https://www.mastercard.com/news/press/2022/july/d-wave-and-mastercard-take-quantum-leap-into-future-of-financial-services/">https://www.mastercard.com/news/press/2022/july/d-wave-and-mastercard-take-quantum-leap-into-future-of-financial-services/</a>
NatWest	Fujitsu digital annealer	1QBit	2018	quantum inspired portfolio optimization (HQLA). <a href="https://1qbit.com/news/natwest-works-1qbit-fujitsu-develop-new-method-deciding-portfolio-composition/">https://1qbit.com/news/natwest-works-1qbit-fujitsu-develop-new-method-deciding-portfolio-composition/</a>
Goldman Sachs	IBM		2020	pricing derivatives cost estimation of 7.5K logical qubits. <a href="https://arxiv.org/abs/2012.03819">https://arxiv.org/abs/2012.03819</a>
Goldman Sachs		Microsoft	2022	pricing derivatives cost estimation in Q#, with 19.2K logical qubits. <a href="https://cloudblogs.microsoft.com/quantum/2022/09/15/using-q-to-estimate-resources-needed-for-quantum-advantage-in-derivative-pricing/">https://cloudblogs.microsoft.com/quantum/2022/09/15/using-q-to-estimate-resources-needed-for-quantum-advantage-in-derivative-pricing/</a>

# bank trials 2/4

customer	hw vendor	sw vendor	when	application
J.P.Morgan Chase	Quantinuum		2022	small-scale portfolio-optimization created with NISQ-HHL hybrid version of the HHL algorithm. <a href="https://arxiv.org/abs/2110.15958">https://arxiv.org/abs/2110.15958</a>
J.P.Morgan Chase	IBM		2019	risk analysis, portfolio optimization, Monte Carlo method, HHL improvements, with 20 qubits. <a href="https://arxiv.org/abs/1905.02666">https://arxiv.org/abs/1905.02666</a>
GE Research	IonQ		2022	risk management hybrid algorithm (Copula-based risk aggregation). small scale trial with 8 qubits. <a href="https://arxiv.org/abs/2206.11937">https://arxiv.org/abs/2206.11937</a>
Bank of Canada	D-Wave	Multiverse	2022	cryptocurrency market simulation. <a href="https://multiversec computing.com/resources/bank-of-canada-and-multiverse-computing-complete-preliminary-quantum-simulation-of-cryptocurrency-market">https://multiversec computing.com/resources/bank-of-canada-and-multiverse-computing-complete-preliminary-quantum-simulation-of-cryptocurrency-market</a>
Itaú Unibanco		QC Ware	2022	quantum inspired based customer retention domain, improved predictions by 2% and the model precision by 6,4% (from 71%). <a href="https://thequantumin insider.com/2022/05/11 qc-ware-applies-quantum-computing-principles-to-increase-customer-retention-at-itau-unibanco/">https://thequantumin insider.com/2022/05/11 qc-ware-applies-quantum-computing-principles-to-increase-customer-retention-at-itau-unibanco/</a>

# bank trials 3/4

customer	hw vendor	sw vendor	when	application
Caixabank	D-Wave		2019	<p>investment portfolio optimization and investment hedging calculation in insurance. Up to 90% decrease in compute time over the traditional solution.</p> <p><a href="https://www.dwavesys.com/company/newsroom/press-release/caixabank-group-d-wave-collaborate-on-innovative-new-quantum-applications-for-finance-industry/">https://www.dwavesys.com/company/newsroom/press-release/caixabank-group-d-wave-collaborate-on-innovative-new-quantum-applications-for-finance-industry/</a></p>
	D-Wave	1Qbit	2017	detect market instability, seek signature of impending market instability by detecting onset of anomalously correlated moves
HSBC	D-Wave		2019	<p>XVA quantitative multi-period reverse stress testing using quantum and simulated annealing, 12 risk factors, QUBO. Some speed gain vs simulated annealing.</p> <p><a href="https://www.dwavesys.com/media/xyvpzswc/28_qxva-v2.pdf">https://www.dwavesys.com/media/xyvpzswc/28_qxva-v2.pdf</a></p>
HSBC	IBM		2022	<p>Monte-Carlo risk analysis, unsupervised quantum machine learning for fraud detection.</p> <p><a href="https://newsroom.ibm.com/2022-03-29-HSBC-Working-with-IBM-to-Accelerate-Quantum-Computing-Readiness">https://newsroom.ibm.com/2022-03-29-HSBC-Working-with-IBM-to-Accelerate-Quantum-Computing-Readiness</a></p>

# bank trials 4/4

customer	hw vendor	sw vendor	when	application
<b>BBVA and Bankia (Spain)</b>	D-Wave	Multiverse	2021	dynamic portfolio optimization with a significant quantum computational time advantage computing $10^{382}$ portfolios. <a href="https://www.bbva.com/en/bbva-and-multiverse-showcase-how-quantum-computing-could-help-optimize-investment-portfolio-management/">https://www.bbva.com/en/bbva-and-multiverse-showcase-how-quantum-computing-could-help-optimize-investment-portfolio-management/</a>
<b>CACIB</b>		Multiverse	2022	trial for solving partial derivative equations using quantum inspired tensor neural networks. <a href="https://arxiv.org/abs/2208.02235">https://arxiv.org/abs/2208.02235</a>
	D-Wave	Multiverse	2022	financial index tracking for portfolio optimization. <a href="https://arxiv.org/abs/2208.11380">https://arxiv.org/abs/2208.11380</a>
<b>Raiffeisen Bank</b>	D-Wave	Data Reply	2023	portfolio optimization using QUBO formulation. <a href="https://arxiv.org/abs/2303.12601">https://arxiv.org/abs/2303.12601</a>
<b>Intesa Sanpaolo</b>	D-Wave	Data Reply	2023	portfolio optimization, Sharpe ratio <a href="https://arxiv.org/abs/2302.12291">https://arxiv.org/abs/2302.12291</a>

# assessing case studies

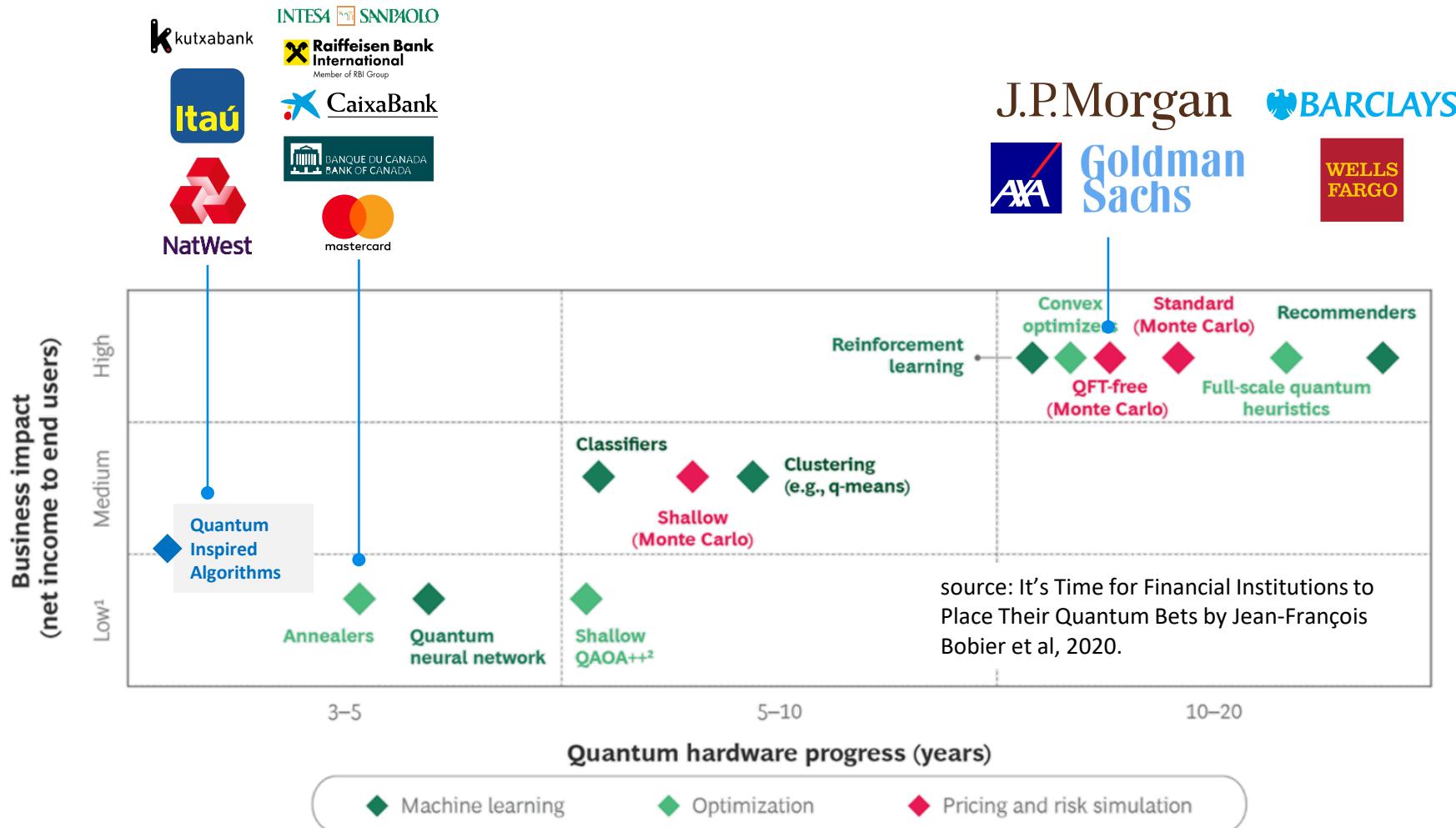
**problem sizing:** is it a small case study or is it matching usual business needs?

**resource estimates:** are qubit # and fidelities numbers mentioned in case study and for its extension to a real business need sizing? Are the number of shots (for measuring observables) and iterations (in the case of NISQ variational circuits) provided with their scaling vs problem size?

**nature of quantum advantage:** is it a speedup? a result quality? a TCO? an energetic one?

**classical comparison:** is there an honest comparison made with best-in-class classical algorithms and hardware?

**advance:** what was new in the case study vs state of the art?



# **NISQ and analog QC financial services use cases**



**MULTIVERSE**

**D-Wave**  
The Quantum Computing Company™

**portfolio optimization**

Method	XS	S	M	L	XL	XXL
VQE	2.4 %	-	-	-	-	-
Exhaustive	5.1 %	13.9 %	-	-	-	-
VQE Constrained	5.1 %	9.1 %	7.1 %	-	-	-
Gekko	5.8 %	13.9 %	13.6 %	54.1 %	71.6 %	-
D-Wave Hybrid	5.8 %	13.9 %	13.6 %	18.9 %	29.3 %	67.6 %
Tensor Networks	5.8 %	13.9 %	15.4 %	38.2 %	39.6 %	39.7 %

TABLE III. Profits (percentual) computed by the different methods for the different datasets and time periods from Table I.

Method	XS	S	M	L	XL	XXL
VQE	278	-	-	-	-	-
Exhaustive	0.005	34	-	-	-	-
VQE Constrained	123	412	490	-	-	-
Gekko	24	27	21	221	261	-
D-Wave Hybrid	8	39	19	52	74	171
Tensor Networks	0.838	51	120	26649	82698	116833

TABLE IV. Run-times (in seconds) estimated for the different methods for the different datasets from Table I.

- **55 assets over 8 year.**
- **comparison with gate-based QPU (VQE) and classical (Gekko, Tensor Networks).**

<https://arxiv.org/pdf/2007.00017.pdf>



## Hybrid Quantum Investment Optimization with Minimal Holding Period

Samuel Mugel,<sup>1</sup> Mario Abad,<sup>2</sup> Miguel Bermejo,<sup>3</sup> Javier Sánchez,<sup>3</sup> Enrique Lizaso,<sup>4</sup> and Román Orús<sup>4, 5, 6, 7</sup>

<sup>1</sup> Multiverse Computing, Centre for Social Innovation,  
192 Spadina Ave, Suite 412, Toronto M5T 2C2, Canada

<sup>2</sup> Bankia Asset Management, Paseo de la Castellana, 189 28046 Madrid, Spain  
<sup>3</sup> Bankia Innovation & Cybersecurity, Paseo de la Castellana, 189 28046 Madrid, Spain

<sup>4</sup> Multiverse Computing, Paseo de Miramón 170, E-20014 San Sebastián, Spain  
<sup>5</sup> Donostia International Physics Center, Paseo Manuel de Lardizabal 4, E-20018 San Sebastián, Spain

<sup>6</sup> Ikerbasque Foundation for Science, Maria Diaz de Haro 3, E-48013 Bilbao, Spain

<sup>7</sup> Corresponding author: roman.orus@dipc.org

### Abstract

In this paper we propose a hybrid quantum-classical algorithm for dynamic portfolio optimization with minimal holding period. Our algorithm is based on sampling the near-optimal portfolios at each trading step using a quantum processor, and efficiently post-selecting to meet the minimal holding constraint. We found the optimal investment trajectory in a dataset of 50 assets spanning a one year trading period using the D-Wave 2000Q processor. Our method is remarkably efficient, and produces results much closer to the efficient frontier than typical portfolios. Moreover, we also show how our approach can easily produce trajectories adapted to different risk profiles, as typically offered in financial products. Our results are a clear example of how the combination of quantum and classical techniques can offer novel valuable tools to deal with real-life problems, beyond simple toy models, in current NISQ quantum processors.

- **50 assets over 1 year.**
- **hybrid classical/annealing.**
- **D-Wave 2000Q.**
- **encoded as a QUBO problem.**
- **a few mn computing/day.**

<https://arxiv.org/pdf/2012.01091.pdf>

# portfolio optimization

# Deloitte.



The Quantum Computing Company™

- SP500 portfolio optimization.
- CPLEX: classical optimization.
- BQM: QUBO Binary Quadratic Model.
- CQM: QUBO Constrained Quadratic Model

## Comparing Classical-Quantum Portfolio Optimization with Enhanced Constraints

Salvatore Certo,<sup>1,\*</sup> Anh Dung Pham,<sup>1</sup> and Daniel Beaulieu<sup>1</sup>

<sup>1</sup>*Deloitte Consulting, LLP*

(Dated: March 10, 2022)

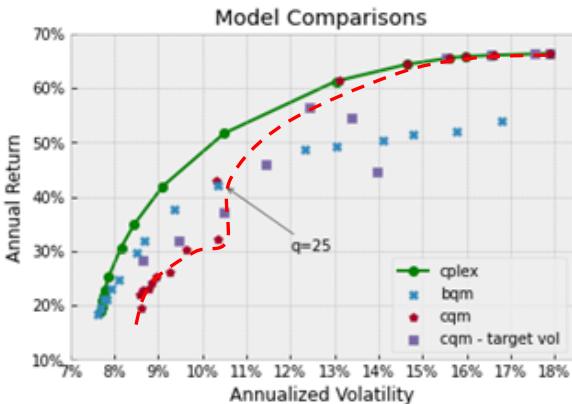


FIG. 3: Comparison of results from the BQM and CQM models for different values of  $q$ . We used a range of  $q$  values from .1 to 500. The crossover point found was  $q = 25$ , after which the BQM dealt better with the higher values in the quadratic terms and found higher returns for the same volatility as CQM. Explicitly stating the target volatility as a constraint, showed in purple, did not outperform the standard CQM model.

# financial index tracking and portfolio optimization

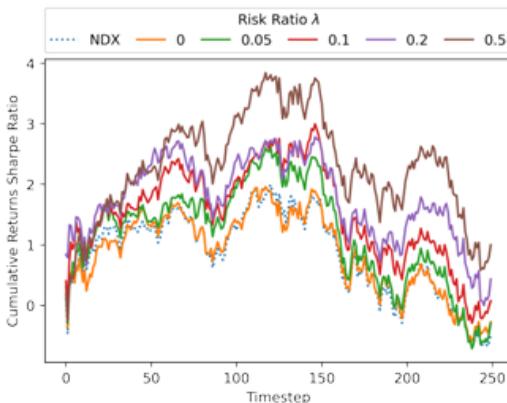


FIG. 7: [Color online] Enhanced Nasdaq-100 (NDX) tracking portfolios with  $C = 25$  and varying covariance minimization ratios 0.2, 0.5 and 0.95: cumulative returns (upper panel) and cumulative returns Sharpe ratio (lower panel).

## Financial Index Tracking via Quantum Computing with Cardinality Constraints

Samuel Palmer,<sup>1</sup> Konstantinos Karagiannis,<sup>2</sup> Adam Florence,<sup>3</sup> Asier Rodriguez,<sup>4</sup> Román Orús,<sup>4,5,6</sup> Harish Naik,<sup>3</sup> and Samuel Mugel<sup>1</sup>

<sup>1</sup> Multiverse Computing, Centre for Social Innovation,

192 Spadina Avenue Suite 509, Toronto, ON M5T 2C2, Canada

<sup>2</sup> Quantum Computing Services, Protiviti, 2884 Sand Hill Rd # 200, Menlo Park, CA 94025, USA

<sup>3</sup> Advanced Analytics, Ally Financial, Ally Charlotte Center, 601 S Tryon St, Charlotte, NC 28202, USA

<sup>4</sup> Multiverse Computing, Parque Científico y Tecnológico de Gipuzkoa,  
Paseo de Miramón, 170 3º Planta, E-20014 San Sebastián, Spain

<sup>5</sup> Donostia International Physics Center, Paseo Manuel de Lardizabal 4, E-20018 San Sebastián, Spain

<sup>6</sup> Ikerbasque Foundation for Science, María Diaz de Haro 3, E-48013 Bilbao, Spain

In this work, we demonstrate how to apply non-linear cardinality constraints, important for real-world asset management, to quantum portfolio optimization. This enables us to tackle non-convex portfolio optimization problems using quantum annealing that would otherwise be challenging for classical algorithms. Being able to use cardinality constraints for portfolio optimization opens the doors to new applications for creating innovative portfolios and exchange-traded-funds (ETFs). We apply the methodology to the practical problem of enhanced index tracking and are able to construct smaller portfolios that significantly outperform the risk profile of the target index whilst retaining high degrees of tracking.

- **financial index tracking.**
- **reference to past work with 500 assets.**
- **NASDAQ 100 items portfolio tracking with 25 assets.**

- **portfolio optimization using QUBO formulation.**
- **dataset with portfolio structured into three main asset classes: equity (EQ), fixed-income (FI) and money market (MM ). A client portfolio typically ranges from 9 to 11 assets.**
- **using various methods: two D-Wave hybrid solvers, that combine the employment of a quantum annealer together with classical methods, and a purely classical algorithm.**
- **uses binary encoding of problem's weight.**
- **“tested QBSolv, the Hybrid BQM and the Hybrid CQM solvers, this last one and its automating handling of multiple optimization terms and constraints QUBO can lead to higher quality solutions. Our satisfactory results show that the Quantum Computing approach is able to find solutions that are close to the exact optimum in terms of return and volatility”.**
- comparison with Fujitsu classical digital annealer not done.

# A real world test of Portfolio Optimization with Quantum Annealing

<https://arxiv.org/abs/2303.12601> March 2023

Wolfgang Sakuler<sup>1\*</sup>, Johannes M. Oberreuter<sup>2</sup>, Riccardo Aiolfi<sup>3</sup>, Luca Asproni<sup>3</sup>, Branislav Roman<sup>1</sup> and Jürgen Schiefer<sup>1</sup>

<sup>1</sup>Raiffeisen Bank International AG, Am Stadtpark 9, Vienna, 1030, Austria.

<sup>2</sup>Machine Learning Reply GmbH, Reply SE, Luisa-Ullrich-Str. 14, Munich, 80636, Germany.

<sup>3</sup>Data Reply S.r.l., Corso Francia 110, Turin, 10143, Italy.

## 2 Problem Formulation

We consider the Markowitz portfolio optimization as a quadratic programming problem [1] that determines the fraction  $\omega_i$  of available budget  $B$  to be allocated on the purchase of the  $i^{\text{th}}$  asset out of potentially  $N$  assets with the goal of maximizing returns, while keeping the risk below a target volatility  $\sigma_{\text{target}}^2$ . For simplicity we set  $B = 1$  and we consider weights  $\omega_i$  as normalized weights.

The optimization problem is formulated as

$$\max_{\omega} \{r^T \cdot \omega\} \quad (1)$$

subject to

$$\omega^T \Sigma \omega \leq \sigma_{\text{target}}^2 \quad (\text{Volatility constraint}) \quad (2)$$

$$1^T \cdot \omega = 1, \omega_i \geq 0, \quad \forall i = 1, \dots, N \quad (\text{Weights constraint}) \quad (3)$$

$$A \cdot \omega \leq b, \quad \langle \text{op} \rangle \in \{=, \leq, \geq\} \quad (\text{Linear constraints}) \quad (4)$$

where

- $r$  is the vector of (mean historical) asset returns
- $\omega$  is the vector of asset weights
- $\Sigma$  is the covariance matrix of the returns
- $\sigma_{\text{target}}^2$  is the target volatility, i.e. the maximum allowed risk
- $A$  is a matrix of coefficients specifying further linear constraints
- $b$  is a vector of constants

## Financial Portfolio Optimization: a QUBO Formulation for Sharpe Ratio Maximization

Mirko Mattesi<sup>1,3</sup>, Luca Asproni<sup>\*1</sup>, Christian Mattia<sup>2</sup>, Simone Tufano<sup>1</sup>, Giacomo Ranieri<sup>2</sup>, Davide Caputo<sup>1</sup> and Davide Corbelletto<sup>2</sup>

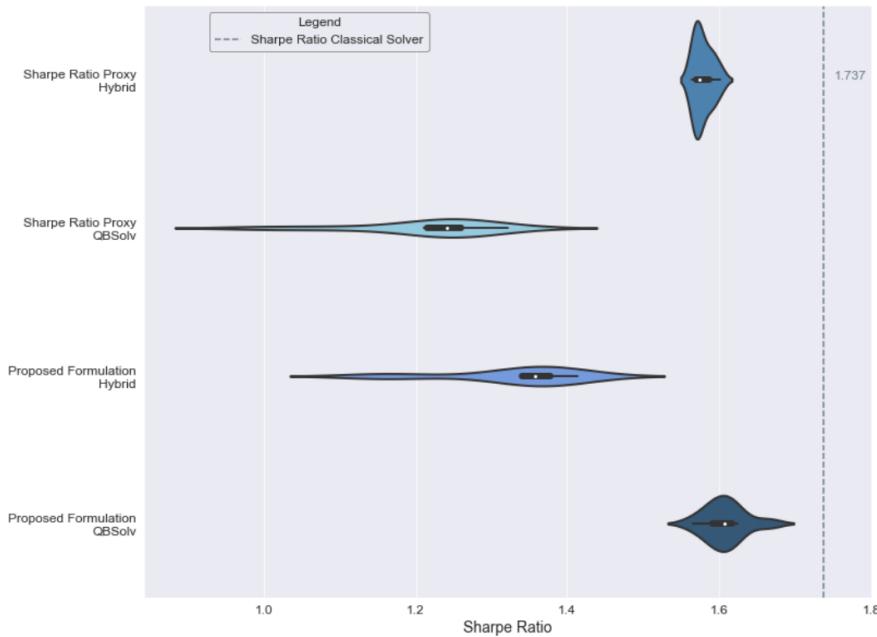
<sup>1</sup> Data Reply S.r.l., corso Francia, 110, Torino, 10143, Italy.

<sup>2</sup> Intesa Sanpaolo S.p.A., piazza San Carlo, 156, Torino, 10121, Italy.

<sup>3</sup> Department of Mathematical Sciences, Politecnico di Torino, Corso Duca degli Abruzzi, 24, Torino, 10129, Italy.

<https://arxiv.org/abs/2302.12291> February 2023

- another portfolio optimization using QUBO formulation.
- maximization of Sharpe ratio with 432 assets.
- the QBsolv solution performs the best.



**Fig. 2:** Violinplot of the results provided by each combination of QUBO formulation and solver. The statistics are drawn from 10 feasible solutions with fixed values for the  $\lambda$  coefficients. All solutions are feasible: for the Sharpe Ratio Proxy formulation, feasibility is given by the sum of asset weights equal to 1, while for the Proposed Formulation we consider the constraint satisfied if  $\mu^T y$  (ref. to Section 3.2) is in a neighbourhood of 1, up to a factor equal to  $2.5 \times 10^{-4}$ , which is given by multiplying the minimum discretization coefficient by the minimum expected return.

# Financial Risk Management on a Neutral Atom Quantum Processor

Lucas Leclerc<sup>1,2,\*</sup>, Luis Ortiz-Gutiérrez<sup>1</sup>, Sebastián Grijalva<sup>1</sup>, Boris Albrecht<sup>1</sup>,  
Julia R. K. Cline<sup>1</sup>, Vincent E. Elfving<sup>1</sup>, Adrien Signoles<sup>1</sup>, and Loïc Henriet<sup>1†</sup>

<sup>1</sup>PASQAL, 7 rue Léonard de Vinci, 91300 Massy, France and

<sup>2</sup>Université Paris-Saclay, Institut d'Optique Graduate School,  
CNRS, Laboratoire Charles Fabry, 91127 Palaiseau, France

Gianni Del Bimbo<sup>3,\*</sup>, Usman Ayub Sheikh<sup>3,\*</sup>, Maitree Shah<sup>4</sup>, Luc Andrea<sup>5</sup>, Faysal Ishtiaq<sup>3</sup>,  
Andoni Duarte<sup>3</sup>, Sam Mugel<sup>4</sup>, Irene Cáceres<sup>3</sup>, Michel Kurek<sup>5</sup>, and Roman Orús<sup>3,6,7</sup>

<sup>3</sup>Multiverse Computing, Parque Científico y Tecnológico de Gipuzkoa,  
Paseo de Miramón 170, 20014 San Sebastián, Spain

<sup>4</sup>Centre for Social Innovation, 192 Spadina Ave, Suite 509, M5T 2C2 Toronto, Canada

<sup>5</sup>WIPSE Paris-Saclay Enterprises 7, rue de la Croix Martre 91120 Palaiseau, France

<sup>6</sup>Donostia International Physics Center, Paseo Manuel de Lardizabal 4, E-20018 San Sebastián, Spain and

<sup>7</sup>Ikerbasque Foundation for Science, Maria Diaz de Haro 3, E-48013 Bilbao, Spain

Achraf Seddik<sup>8</sup>, Oumaima Hammami<sup>8</sup>, Hacene Isselnane<sup>8</sup>, and Didier M'tamon<sup>8</sup>

<sup>8</sup>Crédit Agricole Corporate and Investment Bank,  
12 Place des États-Unis, 92545 Montrouge, France  
(Dated: December 7, 2022)

Machine Learning models capable of handling the large datasets collected in the financial world can often become black boxes expensive to run. The quantum computing paradigm suggests new optimization techniques, that combined with classical algorithms, may deliver competitive, faster and more interpretable models. In this work we propose a quantum-enhanced machine learning solution for the prediction of credit rating downgrades, also known as fallen-angels forecasting in the financial risk management field. We implement this solution on a neutral atom Quantum Processing Unit with up to 60 qubits on a real-life dataset. We report competitive performances against the state-of-the-art Random Forest benchmark whilst our model achieves better interpretability and comparable training times. We examine how to improve performance in the near-term validating our ideas with Tensor Networks-based numerical simulations.

<https://arxiv.org/abs/2212.03223>



**QBoost hybrid algorithm** used to predict « fallen angels », businesses who could fail in loans reimbursements. Quantum algorith is reduced to a QUBO problem.

**data set:** 20 years + 90 000 items with 150 features on 2000 companies in 10 verticals and 100 sub-verticals from 70 countries. 65 000 items in training data and 26 000 items for tests.

**quantum advantage:** could show up with 150 - 342 neutral atoms when compared to a best-in-class classical tensor network, 2800 atoms for the more precise subsampling method.

# **FTQC financial services use cases**

Method	(d, T)		Error		T-count		T-depth		# Logical Qubits	
	Auto	TARF	Auto	TARF	Auto	TARF	Auto	TARF	Auto	TARF
Riemann Sum					$\geq 10^{43}$	$\geq 10^{18}$	$\geq 10^{43}$	$\geq 10^{18}$	-	-
Riemann Sum (no-norm)	(3, 20)	(1, 26)	$2 \times 10^{-3}$		$1.6 \times 10^{11}$	$5.5 \times 10^{10}$	$1.5 \times 10^8$	$1.6 \times 10^8$	23k	17k
Re-parameterization					$1.2 \times 10^{10}$	$9.8 \times 10^9$	$5.4 \times 10^7$	$8.2 \times 10^7$	8k	11.5k

Table 1: Resources estimated in this work for pricing derivatives using different methods for a target error of  $2 \times 10^{-3}$ . As representative use cases of business interest with non-trivial complexity, we consider a basket autocallable (Auto) with 3 underlyings, 5 payment dates and a knock-in put option with 20 barrier dates, and a TARF with one underlying and 26 payment dates. Detailed definitions of these contracts and their parameters can be found in Appendix A.4. We find that Grover-Rudolph methods [10] are not applicable in practice (details in Appendix B) and that Riemann summation methods require normalization assumptions to avoid errors that grow exponentially in  $T$ . Even if those normalization issues were avoided, as detailed in the Riemann Sum (no-norm) row, the re-parameterization method still performs best. See Section 4.1 for a discussion of the Riemann summation normalization. The detailed resource estimation is discussed in Sections 4.1.2 and 4.2.3.

- **gate-based QPU resource assessment for pricing derivatives.**
- **8K logical qubits minimum.**
- **54M T gates =>  $\approx 10^{-8}$  logical qubit error rate.**

source: A threshold for quantum advantage in derivative pricing by Shouvanik Chakrabarti et al, May 2021 (41 pages).

<https://arxiv.org/abs/2012.03819>



- **gate-based QPU resource assessment for portfolio optimization with 100 items.**
- **quantum interior point methods (QIPMs) for second-order cone programming (SOCP).**
- **8 million logical qubits!**
- **$8 \times 10^{29}$  T-count => prohibitive computing time.**
- **would also need some qRAM.**

## End-to-end resource analysis for quantum interior point methods and portfolio optimization

Alexander M. Dalzell,<sup>1,2</sup> B. David Clader,<sup>3</sup> Grant Salton,<sup>4,1,2</sup> Mario Berta,<sup>1,2,5,6</sup> Cedric Yen-Yu Lin,<sup>7</sup> David A. Bader,<sup>3,8</sup> Nikitas Stamatopoulos,<sup>3</sup> Martin J. A. Schuetz,<sup>4,1</sup> Fernando G.S.L. Brandão,<sup>1,2</sup> Helmut G. Katzgraber,<sup>4,1,9</sup> and William J. Zeng<sup>3</sup>

<sup>1</sup>*AWS Center for Quantum Computing, Pasadena, CA, USA*

<sup>2</sup>*California Institute of Technology, Pasadena, CA, USA*

<sup>3</sup>*Goldman Sachs, New York, NY, USA*

<sup>4</sup>*Amazon Quantum Solutions Lab, Seattle, WA, USA*

<sup>5</sup>*Department of Computing, Imperial College London, London, UK*

<sup>6</sup>*Institute for Quantum Information, RWTH Aachen University, Aachen, Germany*

<sup>7</sup>*AWS Quantum Technologies, Seattle, WA, USA*

<sup>8</sup>*New Jersey Institute of Technology, Newark, NJ, USA*

<sup>9</sup>*University of Washington, Seattle, WA, USA*

<https://arxiv.org/abs/2211.12489>

November 2022

Resource	QIPM complexity	Estimated at $n = 100$
Number of logical qubits	$800n^2$	$8 \times 10^6$
T-depth	$(2 \times 10^{10})\kappa_F n^{1.5} \xi^{-2} \log_2(n) \log_2(\epsilon^{-1}) \log_2(\kappa_F n^{14/27} \xi^{-1})$	$2 \times 10^{24}$
T-count	$(7 \times 10^{11})\kappa_F n^{3.5} \xi^{-2} \log_2(n) \log_2(\epsilon^{-1}) \log_2(\kappa_F \xi^{-1})$	$8 \times 10^{29}$

# options pricing

J.P.Morgan



- **tested on 20-qubit IBM QPU.**
- **amplitude estimation algorithm.**
- **random data feeding optimized with a qGAN.**
- **quadratic speed-up compared vs Monte Carlo simulations,**
- **significant computing depth vs number of qubits.**
- **requires a universal fault tolerant quantum computer.**

## Option Pricing using Quantum Computers

Nikitas Stamatopoulos<sup>1</sup>, Daniel J. Egger<sup>2</sup>, Yue Sun<sup>1</sup>, Christa Zoufal<sup>2,3</sup>, Raban Iten<sup>2,3</sup>, Ning Shen<sup>1</sup>, and Stefan Woerner<sup>2</sup>

<sup>1</sup>Quantitative Research, JPMorgan Chase & Co., New York, NY, 10017

<sup>2</sup>IBM Quantum, IBM Research – Zurich

<sup>3</sup>ETH Zurich

#	Single-qubit	CX	CCX	Depth
$m = 3$	2,091	2,056	90	3,927
$m = 5$	12,768	9,078	378	17,332
$m = 7$	52,275	37,132	1,530	70,916
$m = 9$	210,144	149,290	6,138	285,204

Table 2: Single-qubit, CNOT, Toffoli gate counts and overall circuit depth required for the full amplitude estimation circuits for each instance in Fig. 8, as a function of the number of sampling qubits  $m$ . These figures assume all-to-all connectivity across qubits.

source: Option Pricing using Quantum Computers by Nikitas Stamatopoulos, Daniel J. Egger, Yue Sun, Christa Zoufal, Raban Iten, Ning Shen and Stefan Woerner, JPMorgan Chase, ETH Zurich and IBM, May 2019-July 2020 (20 pages), <https://arxiv.org/abs/1905.02666>

## Quantum Monte Carlo simulations for financial risk analytics: scenario generation for equity, rate, and credit risk factors

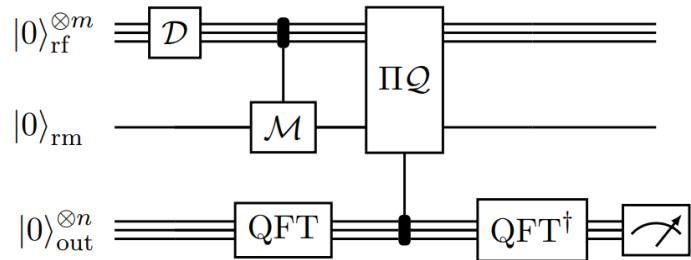
Titos Matsakos and Stuart Nield

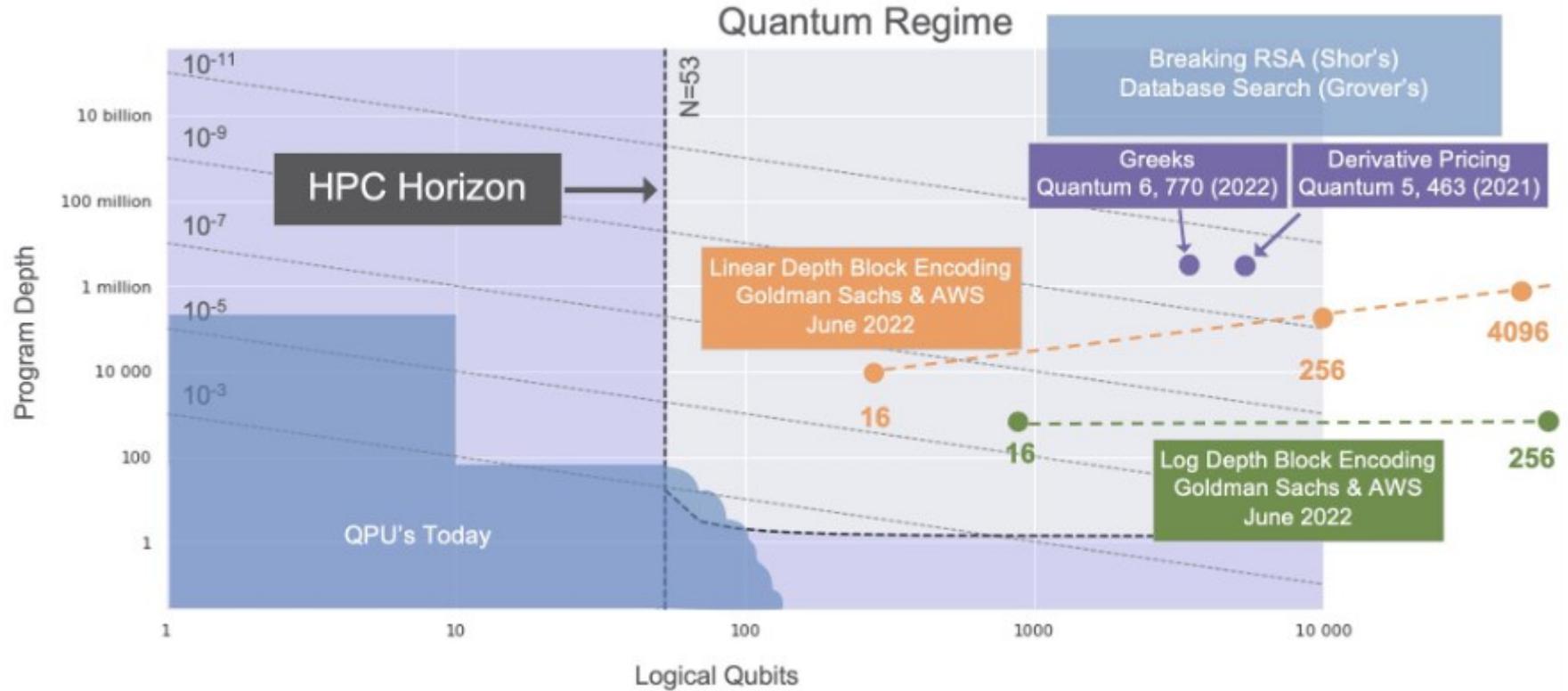
Financial Risk Analytics, Credit & Risk Solutions, Market Intelligence, S&P Global, 25 Ropemaker St, London, EC2Y 9LY, UK

<https://arxiv.org/abs/2303.09682>

March 2023

- Monte Carlo (MC) simulations used in financial risk management, from estimating value-at-risk (VaR) to pricing over-the-counter derivatives.
- In this paper, we focus on incorporating scenario generation into the quantum computation by simulating the evolution of risk factors over time. Specifically, we assemble quantum circuits that implement stochastic models for equity (geometric Brownian motion), interest rate (mean-reversion models), and credit (structural and reduced-form credit models) risk factors. We then feed these scenarios to QMC simulations to provide end-to-end examples for both market and credit risk use cases.
- algorithm is using quantum phase estimates and QFT, thus belonging to the long-term FTQC realm.
- expecting quadratic speedups.
- tests done only on a zero-noise classical emulator running Qiskit.
- lacks scaling resource estimates.





source: [Goldman Sachs and AWS examine efficient ways to load data into quantum computers](#) by Grant Salton et al, 2022.

# other papers

## annealing

[Quantum Boltzmann Machines: Applications in Quantitative Finance](#) by Cameron Perot, January 2023 (62 pages). “It does not appear that the Advantage 4.1-trained BQRBM can produce results good enough to replace the classical RBM”.

[Quantum computing reduces systemic risk in financial networks](#) by Amine Mohamed Aboussalah, Cheng Chi and Chi-Guhn Lee, Nature Scientific Reports, March 2023 (24 pages).

## quantum inspired

[Fujitsu's Quantum-inspired Algorithm Improves Investment Portfolios' Asset Allocation](#) by Matt Swayne, The Quantum Insider, December 2022.

## requires future FTQC hardware:

[Quantum Deep Hedging](#) by El Amine Cherrat, Iordanis Kerenidis et al, March 2023 (32 pages).

[Towards practical Quantum Credit Risk Analysis](#) by Emanuele Dri et al, December 2022 (12 pages).

[Quantum Monte Carlo algorithm for solving Black-Scholes PDEs for high-dimensional option pricing in finance and its proof of overcoming the curse of dimensionality](#) by Yongming Li and Ariel Neufeld, January 2023 (46 pages).

[Real Option Pricing using Quantum Computers](#) by Alberto Manzano et al, March 2023 (20 pages).

[Finding the Optimal Currency Composition of Foreign Exchange Reserves with a Quantum Computer](#) by Martin Vesely, Czech National Bank, March 2023 (30 pages).

[Preparing random state for quantum financing with quantum walks](#) by Yen-Jui Chang et al, February 2023 (11 pages).

# insurance use cases

# quantum computing in insurance

NOVARICA | Executive Brief

## QUANTUM COMPUTING AND INSURANCE: OVERVIEW AND POTENTIAL PLAYERS

DECEMBER 2019

### Summary

Quantum computing has the potential to break the barriers of classical computing, forcing a redesign of the fundamental technology underlying data protection, risk modeling, and select insurance third-party services.

This report provides an overview of quantum theory, current challenges, potential areas of impact for insurers, and recommendations for insurers preparing to become quantum-ready. It also features profiles of players actively developing solutions in this space, including Accenture, Cisco, D-Wave, Google, Guardtime Federal, IBM, ID Quantique, ISARA, MagiQ, Microsoft, Post-Quantum, QC Ware, QuantCor Security, QuNu Labs, QxBranch, Rigetti, SpeQtral, Willis Towers Watson, Xanadu, and Xoffia.

### Contents

Introduction	2
Quantum Computing and Impact	3
How is Quantum Different?	3
Technical Challenges	3
Areas of Insurer Impact	4
Quantum Computing Providers	5
Cave Technology	6
Artificial Intelligence and Machine Learning	7
Risk Modelling	8
Security	8
Getting Ready for Quantum	10
Concluding Thoughts	10

### Primary Report Contacts



Mitch Wein  
Senior Vice President  
mwein@novarica.com



Tiffany Wang  
Senior Associate  
twang@novarica.com

Page Count  
11  
Figures & Tables  
1

**best analysts report to date:** december 2019,  
11 pages, 1.5 pages on « solutions »

### showcased QC applications domains:

- quantum machine learning to better detect and mitigate fraud.
- risks assessment with actuarial models for enhanced pricing and risk pooling precision.
- portfolio optimization.
- model life expectancy for large populations.
- faster (**no**) and more secure data transfer (**yes**).

### one Evergreen Actuarial case study running on D-Wave, on optimizing Solvency matching adjustment

#### Insurance- Optimisation of the Solvency II Matching Adjustment

Evergreen Actuarial  
Insurance, Optimization

An exploration of whether quantum computing can be used to select an optimal subset of assets such that an insurer's Solvency II matching adjustment is maximised: If an insurer has 1,000 assets, such as corporate and government bonds, then there are  $2^{1000}$  permutations of assets that could be selected. Being of order of  $10^{301}$  means that it would not be possible for a classical computer to consider each permutation. This work considers a simplified matching adjustment problem and tests whether a quantum computing approach finds the optimal solution.



### Quantum computing a potential cyber risk for re/insurers: Fitch

12th November 2019 - Author: Charlie Wood

The day when quantum computing power can be applied to real world scenarios is fast approaching, posing a number of important questions around the parameters of cyber risk and security of data encryption.

**wrong risk  
assessment:** we're  
far far away from a  
quantum computer  
breaking RSA codes

Fitch Ratings analysts note how quantum computers – estimated to run 100 million times faster than current technology – stand to revolutionise research efforts, new product development and operating efficiency.

Concurrently, Fitch warns of the potential implications should a 'bad actor' be the first to fully develop and make operational a quantum computer.



## Potential Applications of Quantum Computing for the Insurance Industry

Michael Adam\*  
AXA Konzern AG†

October 10, 2022

### Abstract

This paper is the documentation of a pre-study performed by AXA Konzern AG in collaboration with Fraunhofer ITWM to assess the relevance of quantum computing for the insurance industry. Beside a general overview of the status quo of quantum computing technologies, we investigate its applicability for the valuation of insurance contracts as a concrete use case. This valuation is a computationally intensive problem because the lack of closed pricing formulas requires the use of Monte Carlo methods. Therefore current technical capabilities force insurers to apply approximation methods for many subsequent tasks like economic capital calculation or optimization of strategic asset allocations. The business-criticality of these tasks combined with the existence of a quantum algorithm called Amplitude Estimation which promises a quadratic speed-up of Monte Carlo simulation makes this use case obvious. We provide a detailed explanation of Amplitude Estimation and present two quantum circuits which describe insurance-related payoff features in a quantum circuit model. An exemplary circuit that encodes dynamic lapse is evaluated both on a simulator and on real quantum hardware.

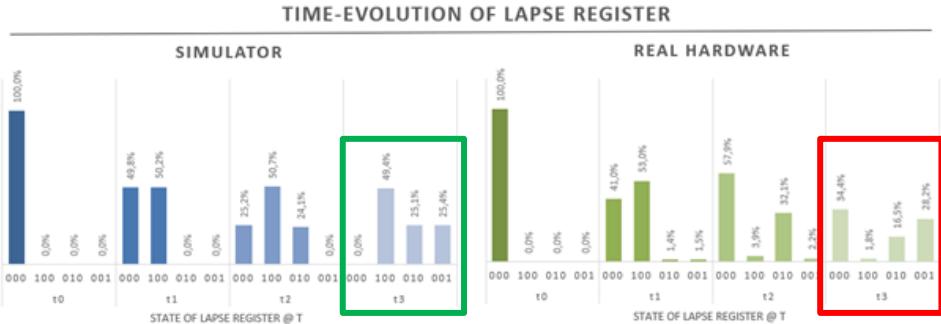


Figure 13: Comparison of simulator and real hardware results for the lapse register. We can see that the first lapse event delivers results which are close to the theoretical expectation. After a tenfold increase of the costs by the controlled linear amplitude function at step 2.2, the QPU returns more or less meaningless results.

<https://arxiv.org/pdf/2210.06172.pdf>

- **investigation on a « quantum amplitude estimate » based algorithm to implement insurance contracts valuation.**
- **compared with Monte-Carlo classical algorithms.**
- **tested with existing IBM QPUs with 27 qubits, showing the detrimental effect of qubit noise (in red).**
- **no assessment on the FTQC required resources.**

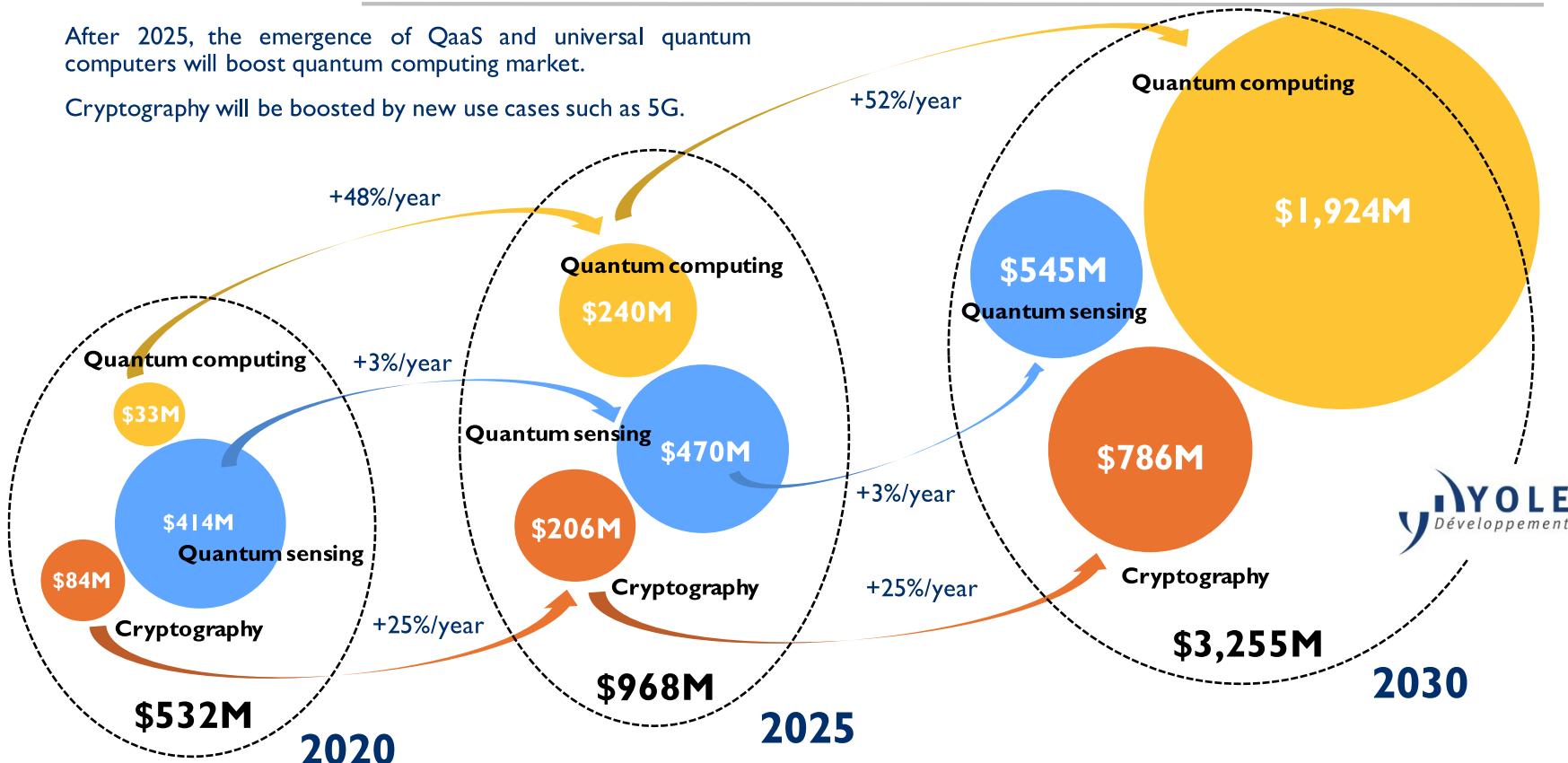


**quantum economics and politics**

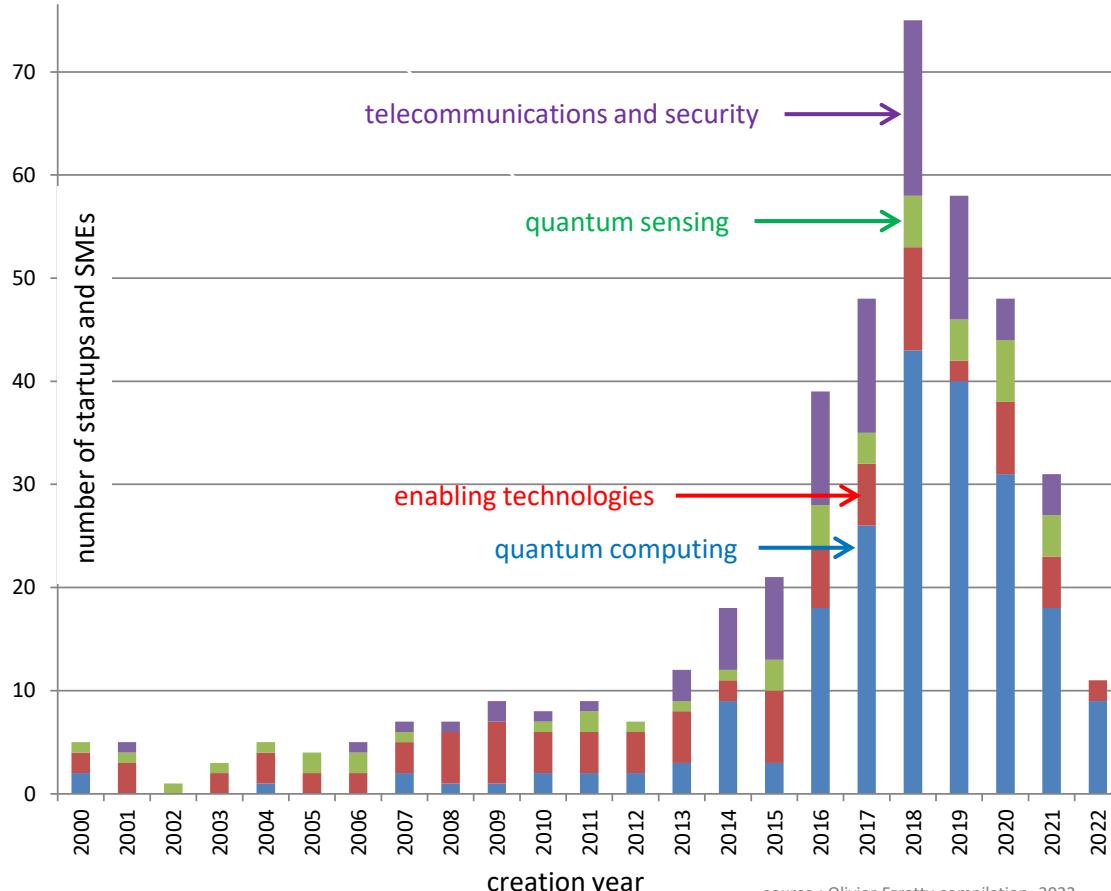
# 2020 – 2025 – 2030 QUANTUM TECHNOLOGIES FORECAST

After 2025, the emergence of QaaS and universal quantum computers will boost quantum computing market.

Cryptography will be boosted by new use cases such as 5G.



# startups and SME per country + creation year



Country	Computing	Enabling	Sensing	Services	Comm - Sec	Total
USA	58	40	19	4	25	146
UK	20	11	8	5	18	62
France	10	27	10	4	5	56
Canada	31	6	4	1	11	52
Germany	16	19	4	1	6	46
India	11	0	0	3	4	18
Switzerland	3	8	1	0	4	16
Netherlands	7	4	1	1	2	15
China	6	0	1	0	6	13
Japan	10	2	0	0	1	13
Spain	7	3	0	0	1	11
Finland	4	3	0	0	2	11
Israel	4	2	2	0	3	11
Australia	6	0	3	1	1	11
Denmark	3	6	0	0	1	10
Singapore	5	1	1	1	1	9
Italy	2	3	1	1	1	7
Sweden	2	4	0	0	0	6
Russia	0	0	2	0	4	6
Poland	3	0	0	0	2	5
Austria	3	0	0	0	1	4
Turkey	0	0	1	1	0	2
Bulgaria	1	0	0	0	1	2
Czechia	0	0	0	1	1	2
Estonia	2	0	0	0	0	2
UAE	2	0	0	0	0	2
Greece	2	0	0	0	0	2
Belgium	0	0	0	1	0	1
Bielorussia	1	0	0	0	0	1
South-Korea	1	0	0	0	0	1
Hong-Kong	1	0	0	0	0	1
Uruguay	1	0	0	0	0	1
Taiwan	0	0	0	0	1	1
Ukraine	1	0	0	0	0	1
Chile	0	0	0	0	1	1
Lybia	1	0	0	0	0	1
Luxembourg	0	0	0	1	0	1
Norway	1	0	0	0	0	1
Columbia	1	0	0	0	0	1
<b>Total</b>	<b>226</b>	<b>144</b>	<b>56</b>	<b>25</b>	<b>101</b>	<b>552</b>

computers



simulators



software



telecoms

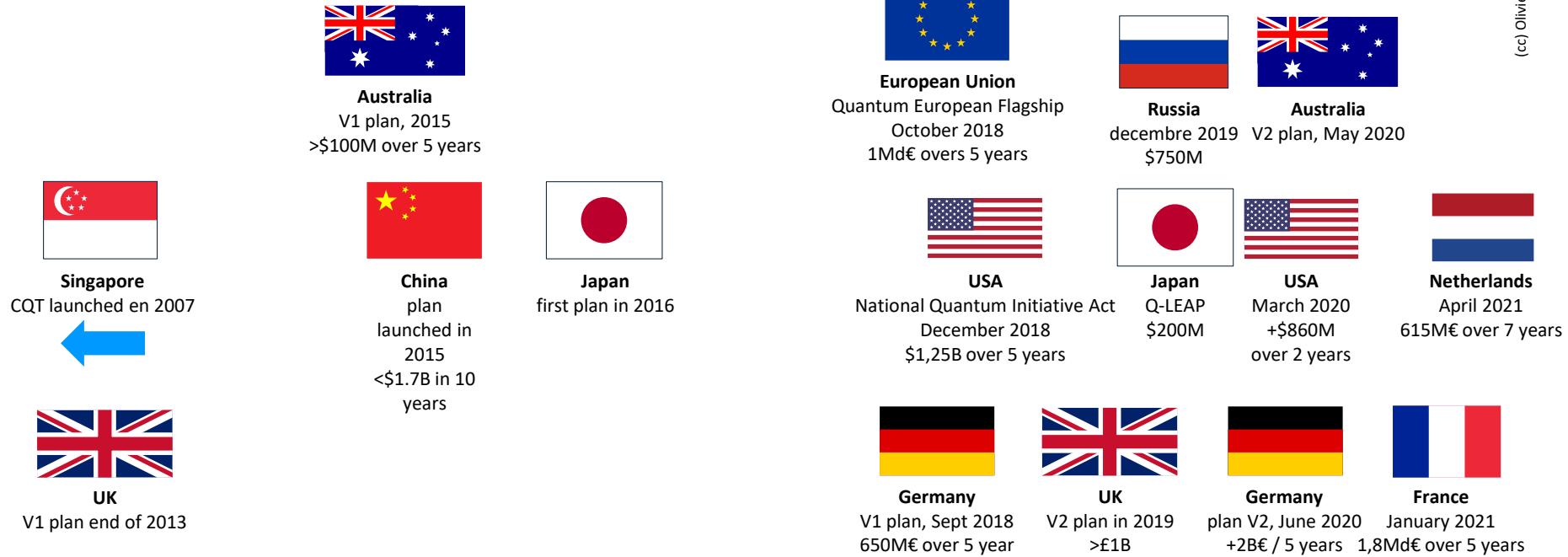


sensing

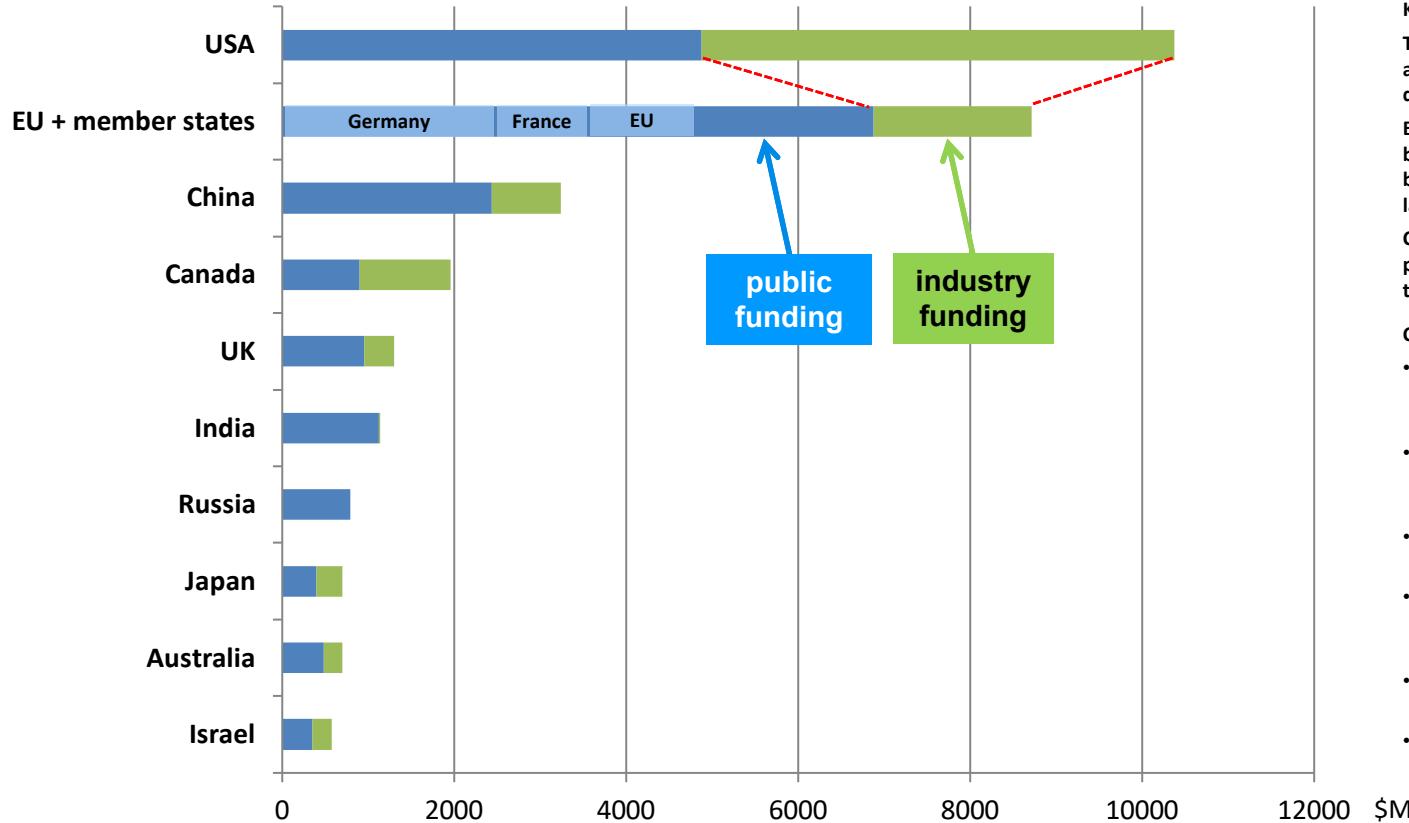


# national quantum plans

(cc) Olivier Ezratty, April 2022



# the « true » global investments



## Key findings:

The European Union and its member states are #1 worldwide public investors in quantum technologies.

EU lags the USA only in private investments, both due to the large IT investments (can't be fixed) and larger funding rounds for their large startups (could be fixed).

China is behind the USA and the EU for both private and public investments in quantum technologies.

## Chart hypothesis:

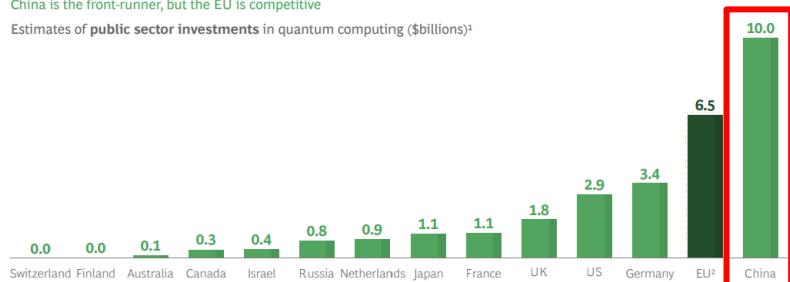
- Classified military/intelligence expenses, in the USA and China: estimated at 30% of civil expenses.
- Most countries do not include legacy public investments in their numbers: unlike France.
- Investment duration: data normalized over 5 years period, particularly for the UK.
- Large IT vendors quantum investments are guestimates: IBM, Google, Microsoft, Intel, Alibaba, Baidu, etc.
- Undisclosed early stage investment in startups: is usually negligible.
- Unspent amounts not accounted for: like probably in India.

# the China quantum investment hoax

## Exhibit 6 - Ranking Countries by Government Investments in Quantum Computing

China is the front-runner, but the EU is competitive

Estimates of **public sector investments** in quantum computing (\$billions)<sup>1</sup>



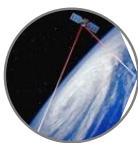
Sources: Literature search; BCG analysis.

<sup>1</sup>The data in this exhibit represents public announcements made after 2013; investments may be made for different time horizons.

<sup>2</sup>Investments made centrally by the EU (~\$1.1 billion) as well as those made by Germany, France, the Netherlands, and Finland.

## Overview of the major Chinese government QC programs

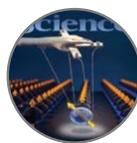
- 2006-2010 (Eleven Five-Year Plan) ~1 billion CNY
  - 2011-2016 (Twelve Five-Year Plan) ~5 billion CNY
  - 2016-present (Thirteen Five-Year Plan) ~2 billion CNY
- ~4 billion CNY from Anhui , Shanghai, Shandong, etc. Province



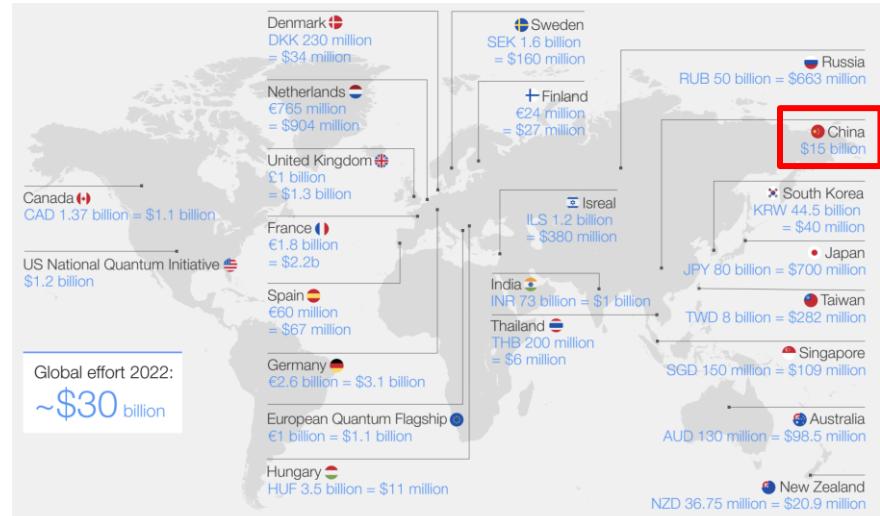
Quantum communication



Quantum computation and simulation



Quantum Metrology



"An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology" by Edward Parker, Rand Corporation, February 2022 (140 pages) : « *In summary, official reports of the PRC's government investment in quantum R&D in recent years have varied widely, from a low of \$84 million per year (Pan's estimate) to a high of at least \$3 billion per year (the Anhui Business Daily's reported funding for Pan's laboratory). We are unable to assess from public information which figure is more accurate. By comparison, the U.S. government has spent \$450-\$710 million per year in recent years; we cannot determine whether the PRC total is higher or lower than this amount.* »

China's quantum investments from 2006 to 2021 did not exceed \$1.8B. This number is very different from the \$10B to \$15B investment showcased in various analyst publications. These >\$10B numbers are false and based on fuzzy propaganda coming from China and amplified by various US interests.

Source: Chinese QC Funding by Xiaobo Zhu, 2017 (35 slides). And... 1 CNY ≈ 0.14 US \$.

Get 12 weeks for \$29.99 \$6



NEW YORKER FAVORITES When I Met Dr. King The Perils of Pearl and Olga The Age of Instagram Face The Itch

**A**t the campuses of the University of Science and Technology of China, four competing quantum-computing technologies are being developed in parallel. In a paper published in *Science*, in 2020, a team led by the scientists Lu Chao-Yang and Pan Jian-Wei announced that their processor had solved a computational task millions of times faster than the best supercomputer. But is this all the news about quantum computing? Lu and I spoke by video earlier this year. He joined the call late and was covered in sweat, having sprinted home from a mandatory COVID test. Lu immediately began debunking claims made by his competitors, and even claims made about his own effort. One widely reported figure stated that China has invested fifteen billion dollars in developing a quantum computer. "I have no idea how that was started," Lu said. "The actual money is maybe twenty-five per cent of that."

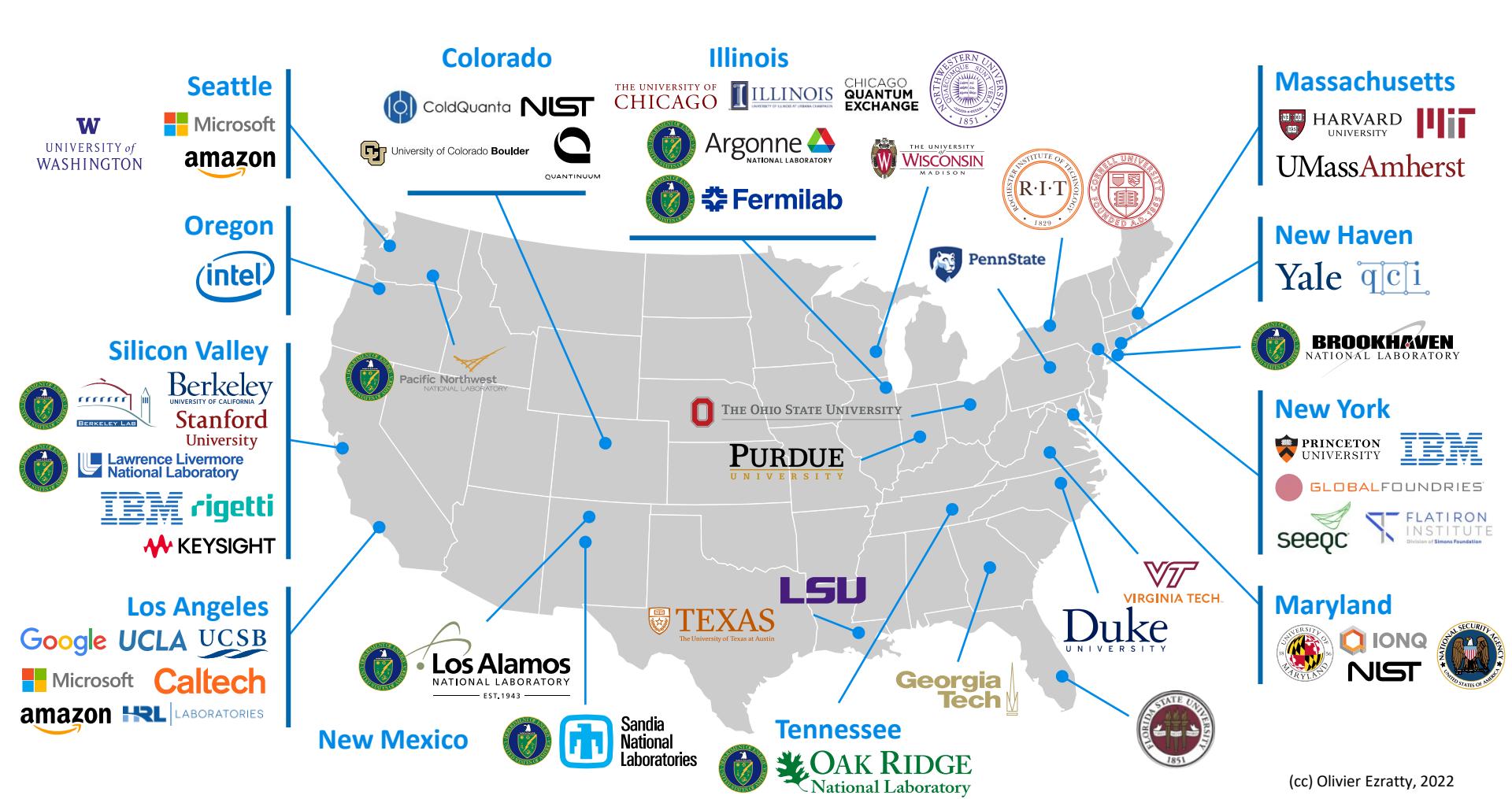
ANNALS OF TECHNOLOGY DECEMBER 19, 2022 ISSUE

# THE WORLD-CHANGING RACE TO DEVELOP THE QUANTUM COMPUTER

*Such a device could help address climate change and food scarcity, or break the Internet. Will the U.S. or China get there first?*

By Stephen Witt

December 12, 2022



(cc) Olivier Ezratty, 2022

## British Columbia



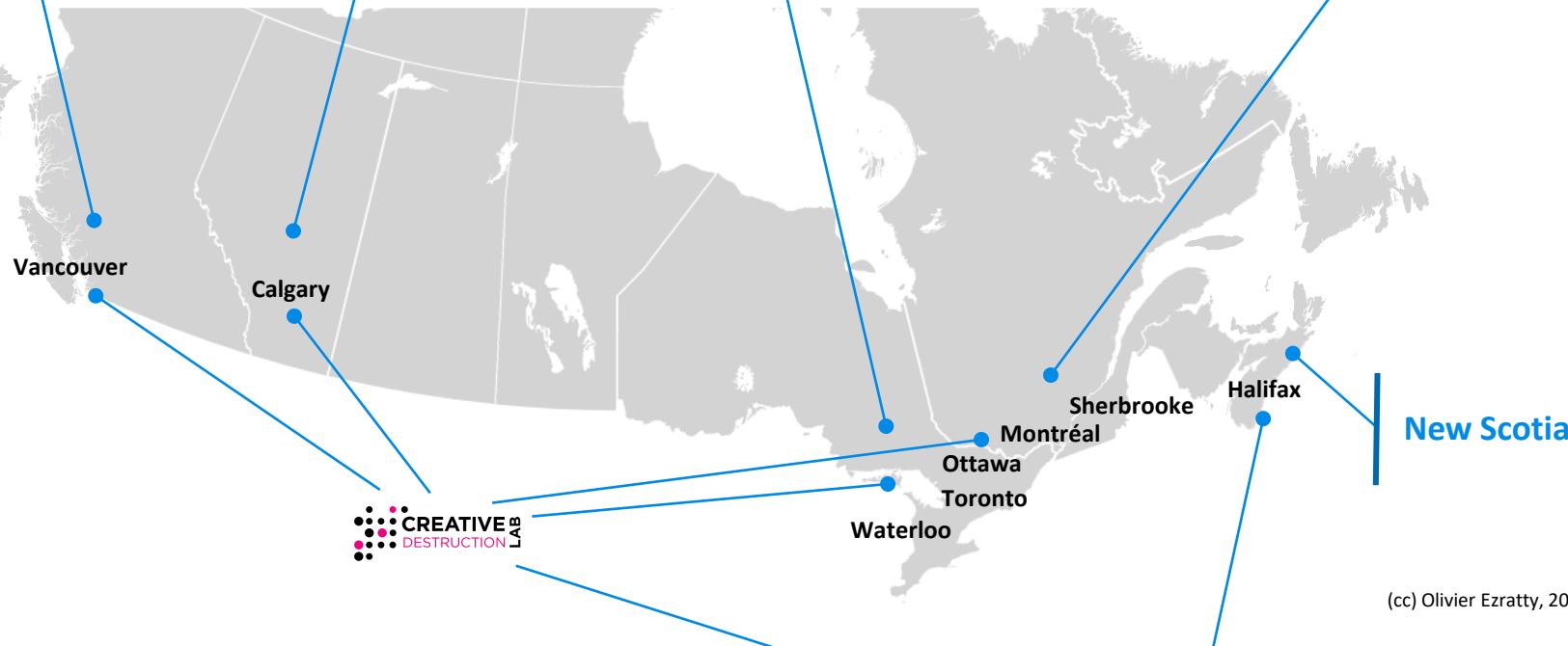
## Alberta



## Ontario



## Quebec



(cc) Olivier Ezratty, 2022

# France quantum strategy



as usual, all segments of quantum technologies are funded

Répartition par axe technologique

Axes technologiques de la stratégie nationale						Total 2021 – 2025 [M€]
NISQ	LSQ	Capteurs quantique	Communications quantiques	Cryptographie post quantique	Technologies capacitanentes	
352	432	258	325	156	292	1815

a strong effort in research

Répartition par modalité de soutien

Total 2021 – 2025 [M€]	
Recherche (Organismes CNRS, CEA, INRIA, ONERA, CNES; programmes UE, infrastructures)	725
Formation (PhD, Ingénieurs, masters, techniciens)	61
Maturité Technologique	171
Innovation de rupture (ordinateur quantique)	114
Soutien au déploiement industriel (lignes pilotes et cryogénération)	224
Politique d'Achat Public (calcul, défense)	72
Entrepreneuriat (fonds d'investissement, incubateurs)	439
Intelligence Economique (standardisation, PI)	9

1045M€ public funding with 2/3 being incremental

Répartition par origine du financement

Total 2021 – 2025 [M€]	
PIA 4	594
Subvention aux organismes de recherche	274
Autres contributions nationales	164
Financements européens	238
Secteur Privé	545

expecting 545M€ of industry funding (R&D and startups investments)

## Stratégie nationale sur les technologies quantiques



SACLAY  
21 janvier 2021



# France various quantum plans

## PEPR

programmes et équipements prioritaires de recherche.  
Recherche fondamentale  
CNRS, CEA, Inria et Universités.

## QuanTEdu

formation publique couvrant la physique et les technologies quantiques. 21 universités. Piloté par UGA (Grenoble).

## HQI

plateforme nationale de calcul hybride. Pilotée par GENCI, CEA et Inria.

## grand défi LSQ

piloté par l'IRT Nanoelec à Grenoble.

## pack quantique IDF

associe entreprises et fournisseurs / startups.

## technologies habilitantes

cryogénie et électronique (QRYOLink), isotopes rares (Orano, CEA), lasers (IOGS).

## maturation

création de startups par les chercheurs, piloté par CNRS Innovation.

## standardisation

LNE et AFNOR, avec les entreprises.

Paris



Plateau  
de Saclay

quantum | université PARIS-SACLAY

Villetaneuse

Cergy

## quantum research labs in France

(cc) Olivier Ezratty, 2022





# industry vendors ecosystem

computing



cryogeny



software



cybersecurity



photronics



sensing



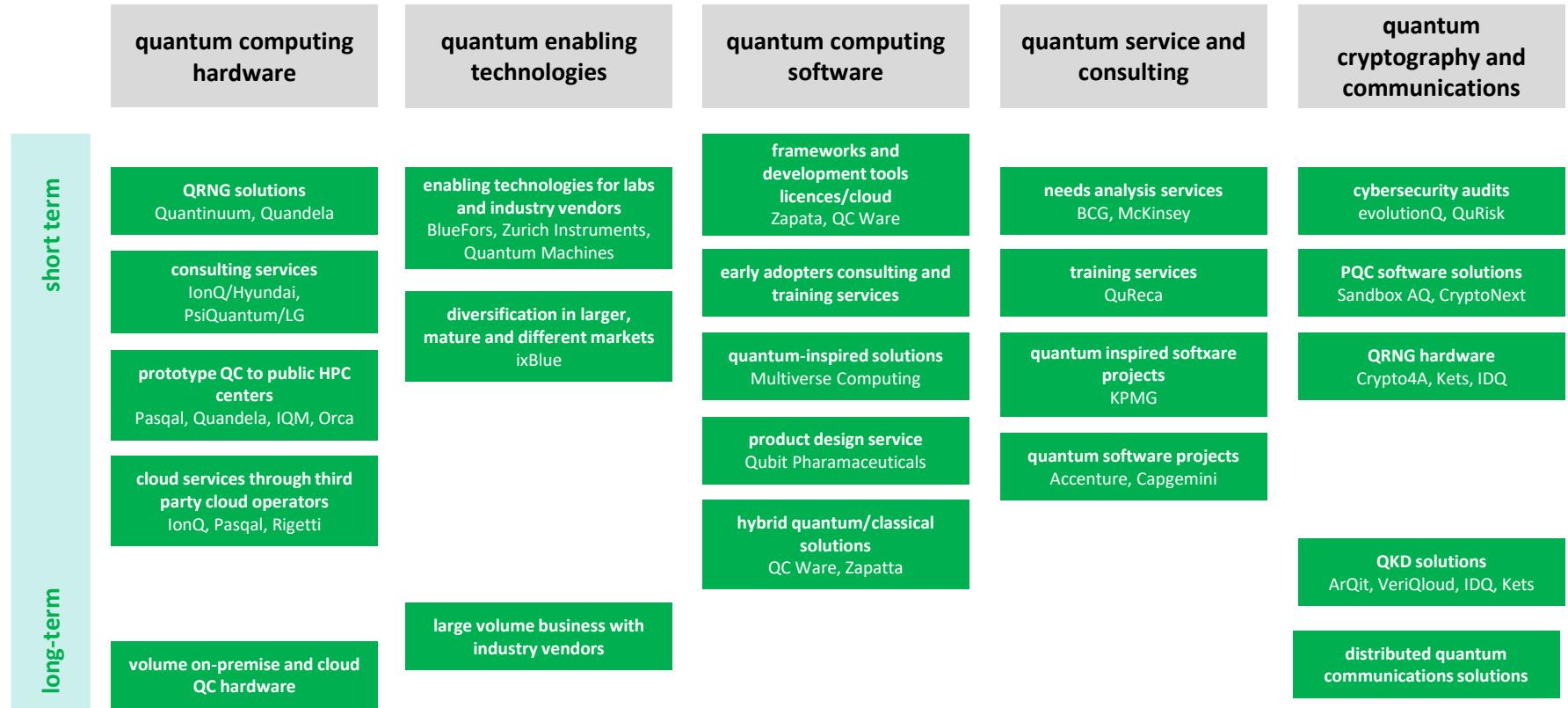
manufacturing



materials

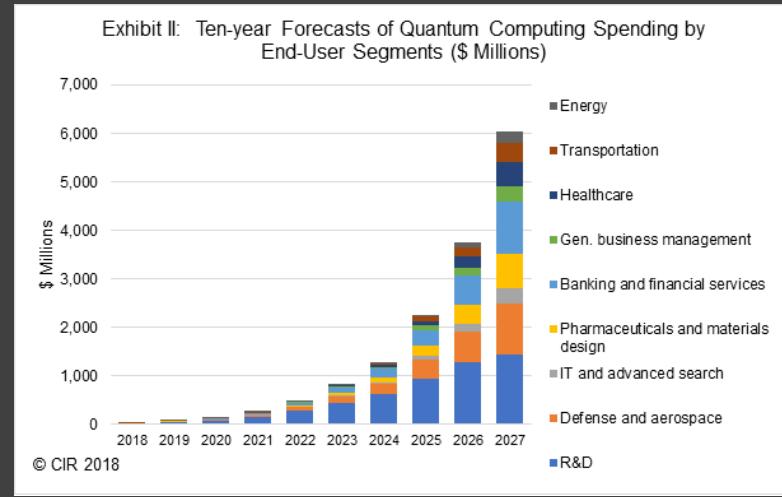


# quantum vendors business models



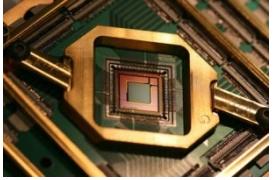
# why and how are they investing in QC?

	why	R&D effort	offering	evangelism
	need a leading position in a growth IT market	strong integrated R&D, publicized and respected roadmap	QisKit, 24 QC system online, free <10 qubits	invest early on in building an ecosystem (customers, developers, academic)
	extension of their AI and online services	slow product cycles, not in their cloud (Sycamore)	Cirq, TensorFlow Quantum, third party QC in their cloud (IonQ)	low engagement with ecosystem (a few US universities)
	create a new enterprise cloud activity	betting the farm on a high-risk/high-reward technology (topological qubits)	Q#, Azure Quantum, third party QC in their cloud (IonQ, Quantinuum, Pasqal, ...)	relatively low-key customer and developer engagement
	create a new enterprise cloud activity	betting the farm on a high-risk/high-reward technology (cat-qubits), Caltech	Braket, many third party QC in their cloud (IonQ, D-Wave, Rigetti)	relatively low-key customer and developer engagement
	sell leading-edge hardware components or systems	silicon qubits, reuse CMOS design and manufacturing skills	IQS emulation software	



quantum computing  
enterprise readiness

# exploratory methodology



## technology screening

- understand quantum technologies
- concepts and wording
- decipher vendor's messages and hype
- understand the news
- what can quantum algorithms do?
- case studies applicability and range



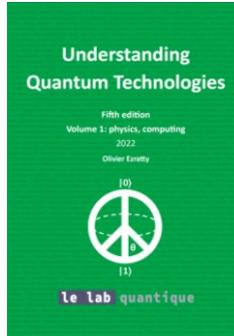
## needs analysis

- existing unsolved problems or problems that are too lengthy or costly to solve?
- create an internal community
- involved security specialists
- security protocols mapping



## evaluation

- test some quantum algorithms at small scale
- on universal gates qubits as well as on quantum annealing or quantum simulators



## education and training

- some developers, IT architects and line of businesses R&D scientists.
- study the link between quantum computing and R&D unsolved problems.
- online training
- initial training

## resources

- «Understanding Quantum Technologies» ebook (free, >1120 pages).
- ecosystem events (Q2B, QCB, Lab Quantique, ...)
- vendors quantum offerings (IBM, Amazon, Microsoft, D-Wave, Pasqal, Quantinuum, IonQ, ...)
- independant software vendors offerings (QC-Ware, Multiverse, ...).

# France early adoption examples



AIRBUS

THALES

MBDA  
MISSILE SYSTEMS

NAVAL  
GROUP



ONERA  
THE FRENCH AEROSPACE LAB



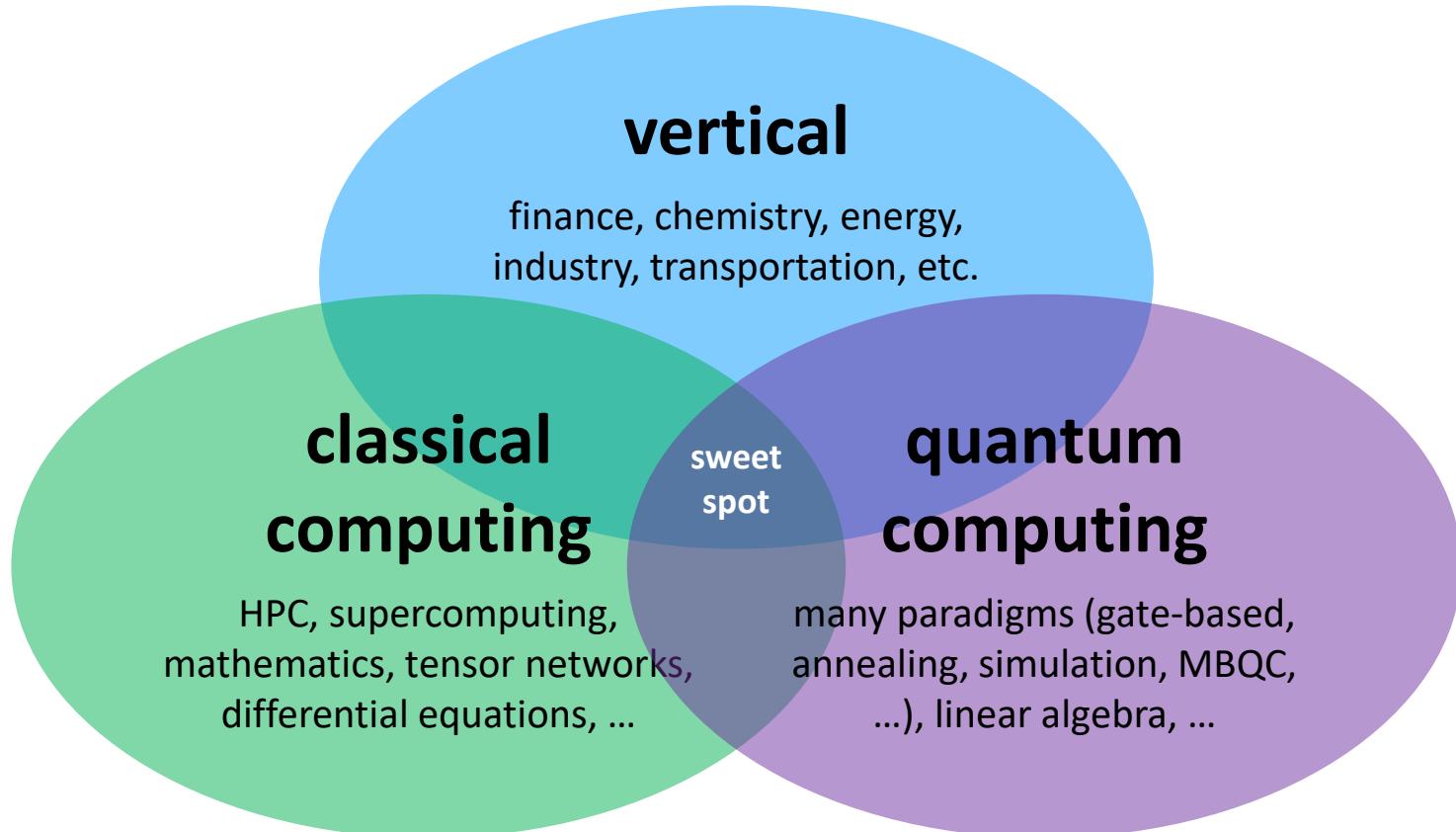
sopra steria

Capgemini

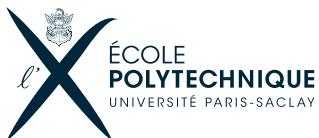


OVHcloud®

# skills needs



# some education in France



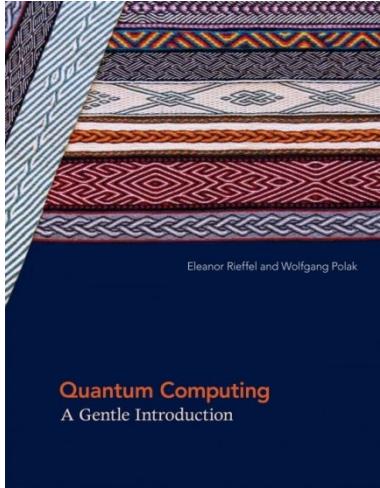
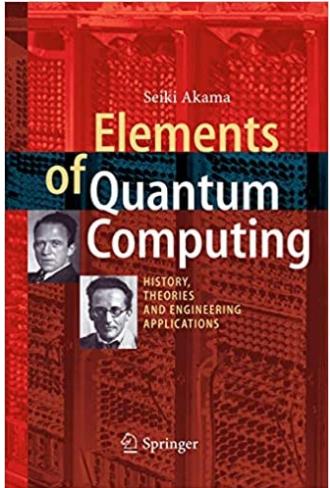
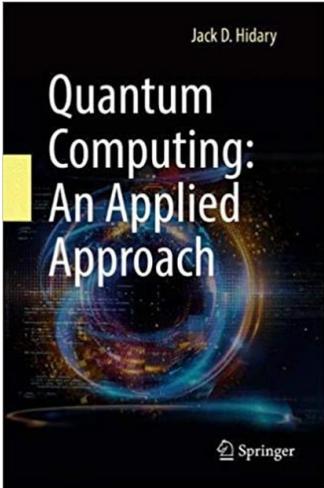
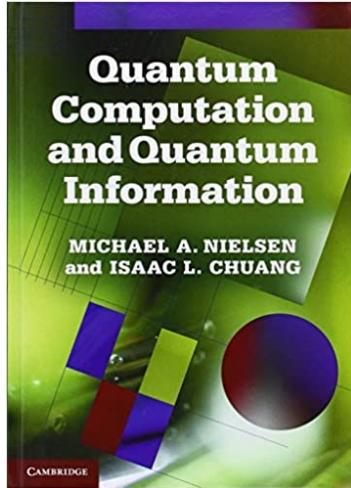
ÉCOLE NORMALE  
SUPÉRIEURE  
Paris, Saclay, Lyon



COLLÈGE  
DE FRANCE  
1530



# some reference books



**John Preskill's 2021 Caltech course**

[https://www.youtube.com/playlist?list=PL0ojirEqlyPy-1RRD8cTD\\_IF1hflo89lu](https://www.youtube.com/playlist?list=PL0ojirEqlyPy-1RRD8cTD_IF1hflo89lu)

**Elias Combaro CERN course**

A Practical Introduction to Quantum Computing From Qubits to Quantum Machine Learning and Beyond, 2020 (251 slides)

<https://indico.cern.ch/event/970909/>

# discussion

# test de connaissances

en quelle année l'équation de Schrödinger a-t-elle été formulée ?

quel fameux sujet lié à Erwin Schrödinger avons-nous évité de citer dans cette formation ?

quel outil open source en ligne permet-il de tester graphiquement des qubits ?

à quelle température sont refroidis les qubits supraconducteurs ?

quelle porte quantique est indispensable pour créer un jeu de portes véritablement universel ?

quel type de qubit génère la meilleure fidélité de portes quantiques ?

combien de qubits physique faudrait-il assembler pour créer un qubit logique ?

combien de qubits physiques sont nécessaires pour factoriser une clé RSA de 2048 bits ?

quelle est l'accélération de l'algorithme de Shor et de l'algorithme de Grover ?

quelle scientifique française est à l'origine de la meilleure source de photons uniques au monde ?

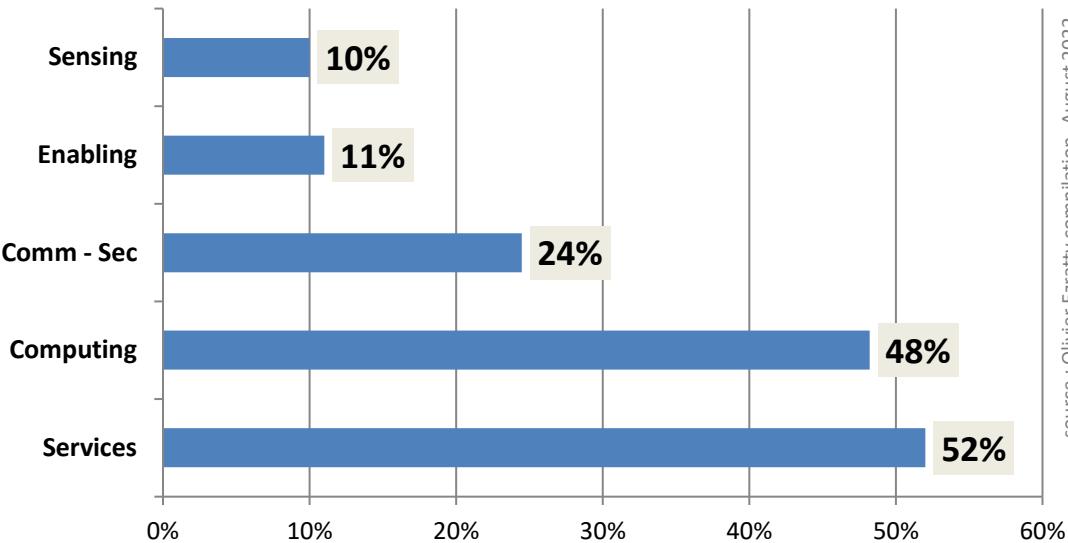
quel est le montant du plan quantique français annoncé le 21 janvier 2021 ?

quelle chercheuse du CEA a lancé la startup Siquance ?

quelle chercheuse du CNRS étudie la dimension énergétique du calcul quantique ?

# branding and creativity

share of worldwide quantum startups and SMEs  
with a name starting with Q



source : Olivier Ezratty compilation, August 2022

