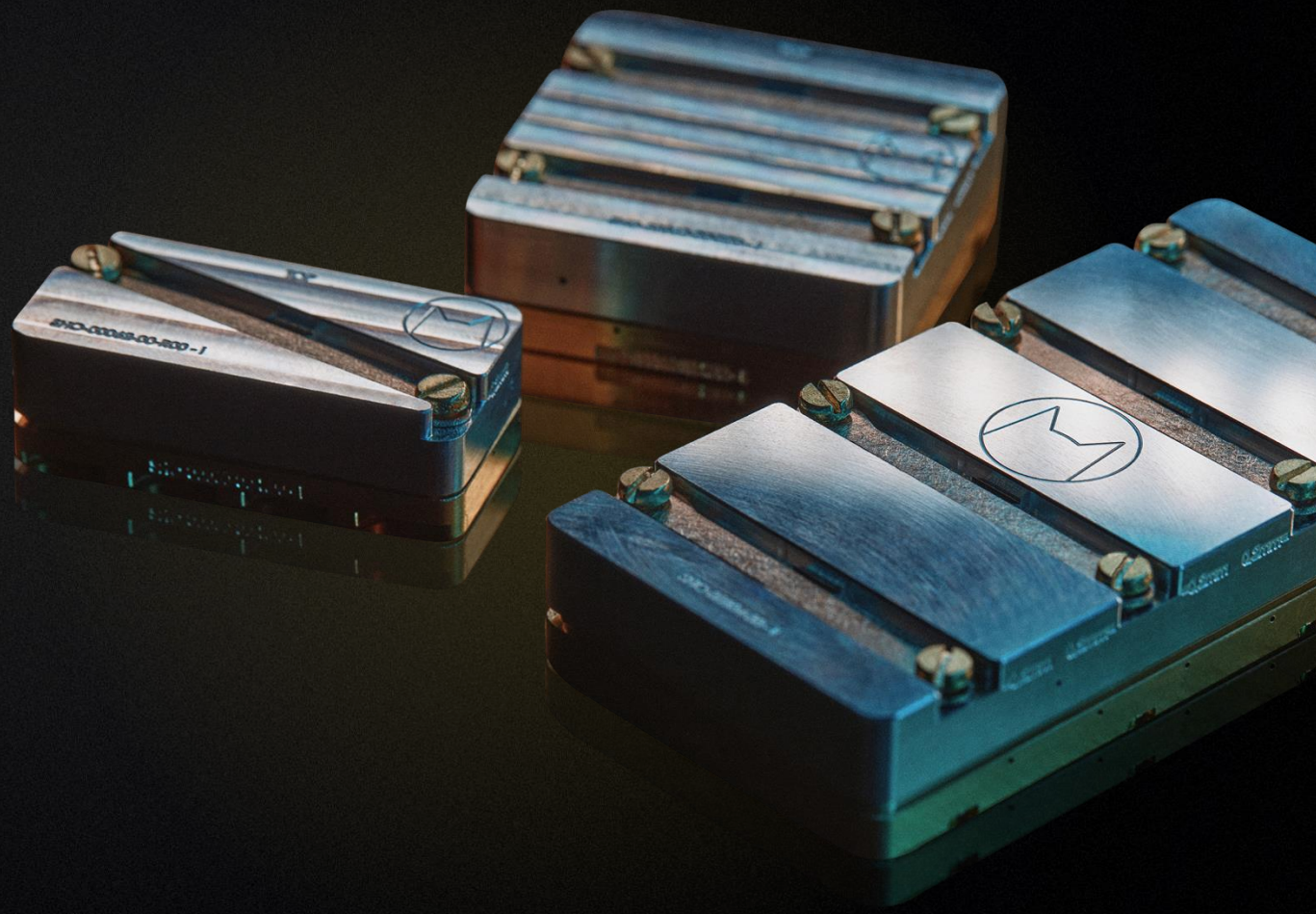
ADVANCEMENT IN QUANTUM COMPUTERS AND SHOR'S ALGORITHM

PQSCA



PQSCA Workshop

Dahmun Goudarzi

MAY 19TH 2026

Alice & Bob
On the highway to FTQC

Théau Peronnin

CO-FOUNDER & CEO

Raphaël Lescanne

CO-FOUNDER & CTO

2020 **Founding date**

2 **Offices** Paris / Boston

190+ **People** 40+ PhDs, 90+ R&D

€130m **Raised to date**

We are a **quantum processor** designer, focused on **FTQC**

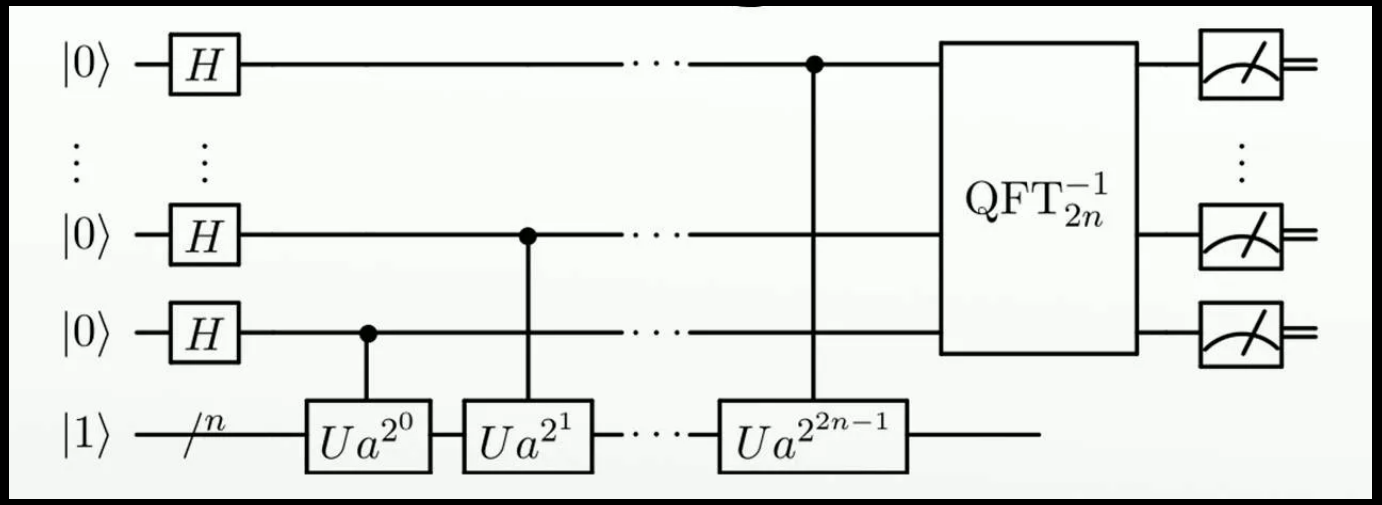
We design the **quantum chip** & the **firmware** that drives it

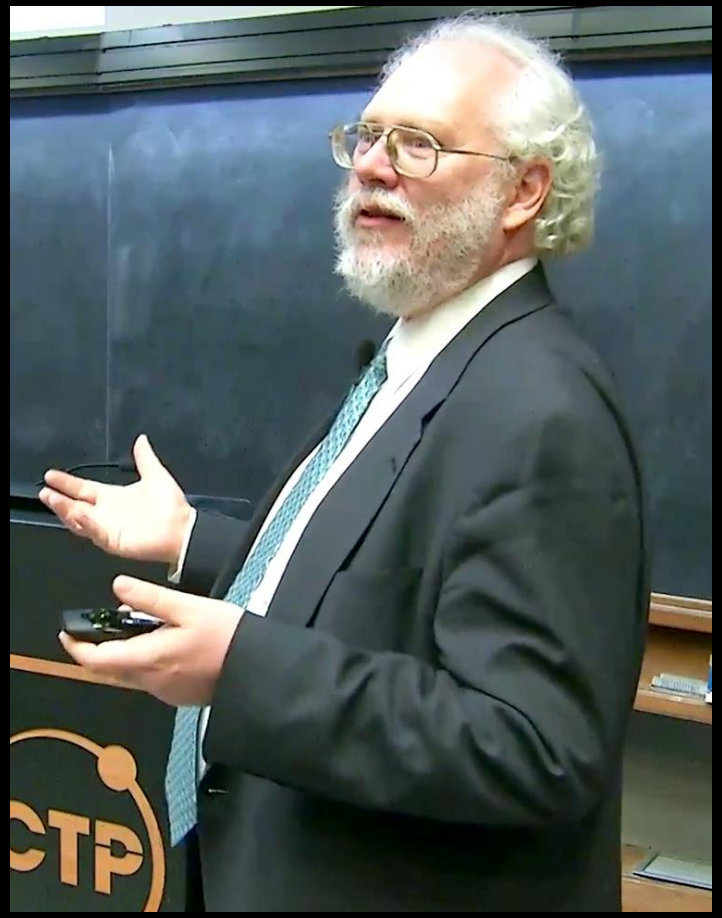
We leverage a unique technology: the **superconducting cat qubit**

“Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy”

Richard Feynman

1981

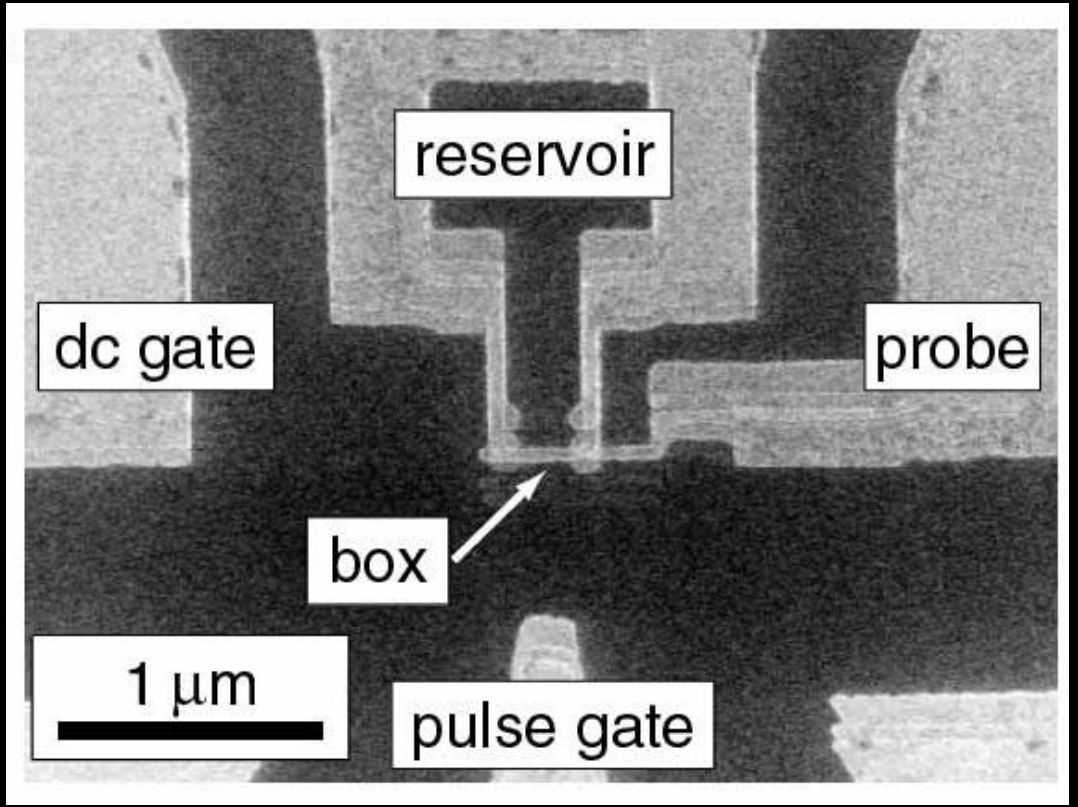




Shor’s algorithm

1981 1994

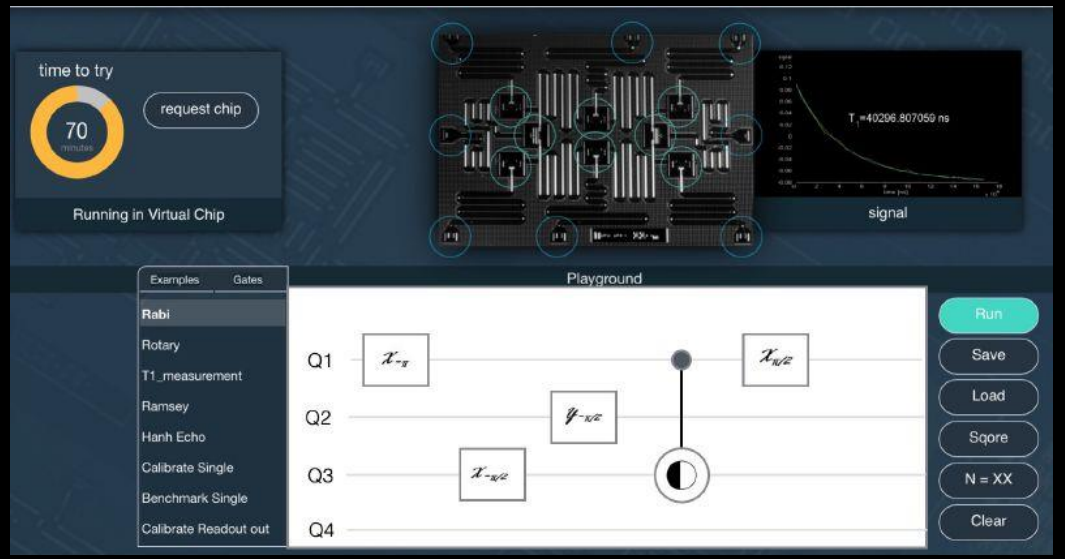
The first qubits



Coherent control of macroscopic quantum states in a single-Cooper-pair box
Y. Nakamura et al., 1999, https://www.nature.com/articles/19718

1981 1994 1999

The first
quantum computers
in the cloud



IBM

1981 1994 1999 2016

The first claim of quantum supremacy

Google

1981 1994 1999 2016 2019

Where are we today?

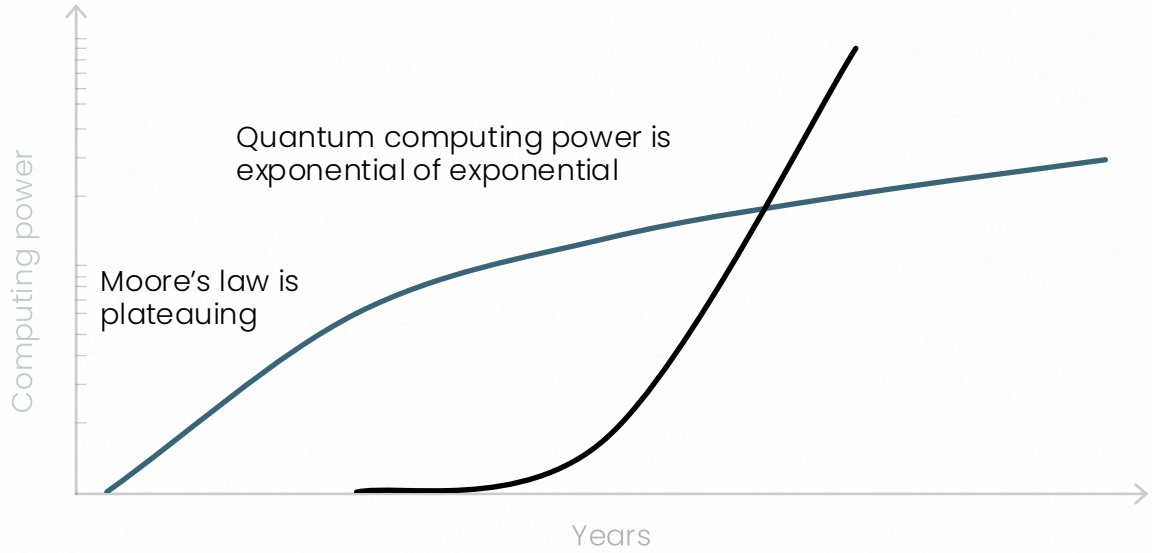
Forget about quantum: the goal is exponential increase in computing power to create value

Quantum is the engine of the next economic breakthrough

→ Source

1. McKinsey

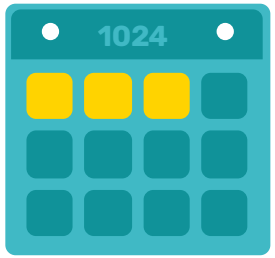
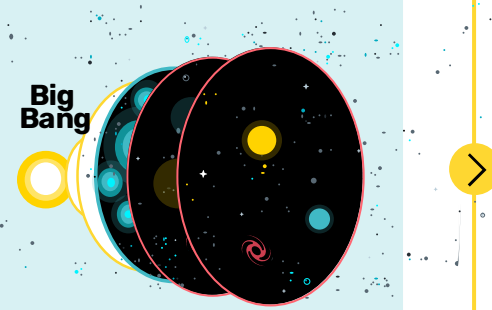
Quantum computing is the only way to generate exponential increase in computing power



+1 qubit

= x2
computing power

Quantum Computers Expand the Set of Problems we can Solve, Unlocking a Technological Revolution

Key to decrypt (bits)	512	1024	Today's RSA encryption 2048
CLASSICAL COMPUTERS HP Frontier Supercomputer	 **0.5 Milliseconds (20x faster than a hummingbird flaps its wings)**	 **3 Months**	 **6 Trillion year (400x the age of the universe)**
Quantum Computer Alice & Bob Architecture	**10 Hours**	**1 Day**	**1 Week**

- Life Sciences
- Chemicals
- Energy
- Telecom
- Manufacturing
- Logistics
- Finance

$850 billion[2]

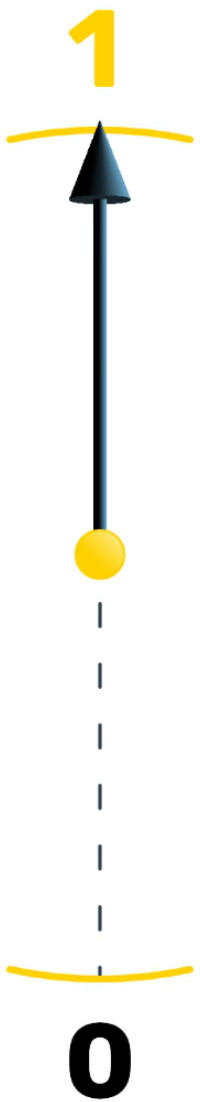
1. *Élie G. et al."Performance Analysis of a Repetition Cat Code Architecture" Physical Review Letters 131, no. 4 (2023).*
2. *Boston Consulting Group, 2024*

Quantum computing is NOT always faster

We compare the peak performance of a single classical chip that can be manufactured today (like an NVIDIA A100 GPU, or an ASIC with a similar number of transistors) with a future quantum computer with 10,000 error-corrected logical qubits, 10μs gate time for logical operations and all-to-all connectivity. We consider an estimate of the I/O bandwidth (namely the number of operations per second) and three types of operations: logical binary operations, 16-bit floating point, 32-bit integer or fixed-point arithmetic multiply add operations.

	GPU	ASIC	Future Quantum
I/O Bandwidth	10,000 Gbit/s	10,000 G/s	1 Gbit/s
Operation throughput			
16-bit floating point	195 Top/s	550 Top/s	10.5 kop/s
32-bit integer	9.75 Top/s	215 Top/s	0.83 kop/s
binary (Boolean logical)	4,992 Top/s	77,000 Top/s	235 kop/s

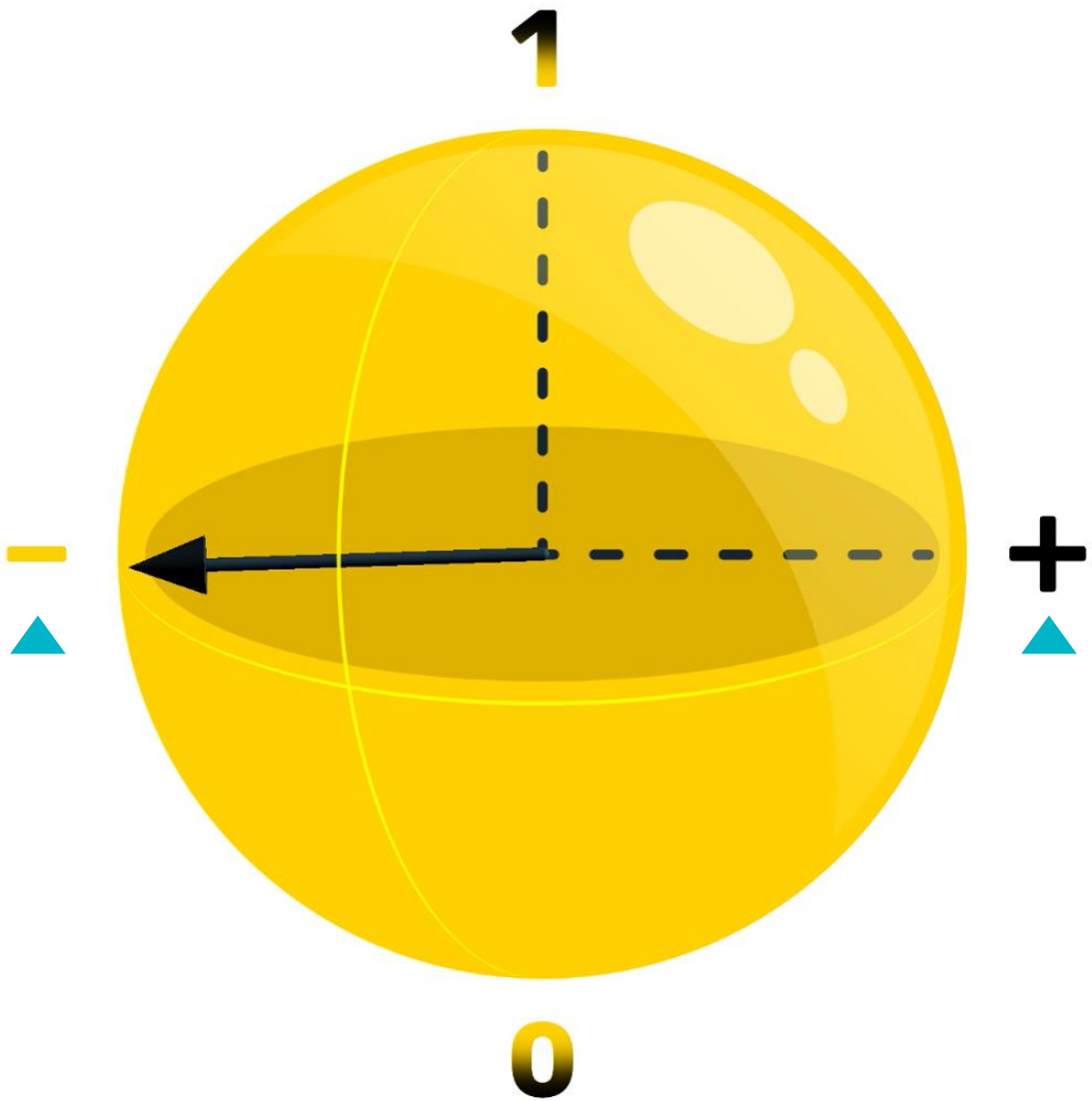
Source : https://cacm.acm.org/research/disentangling-hype-from-practicality-on-realistically-achieving-quantum-advantage/


1
0

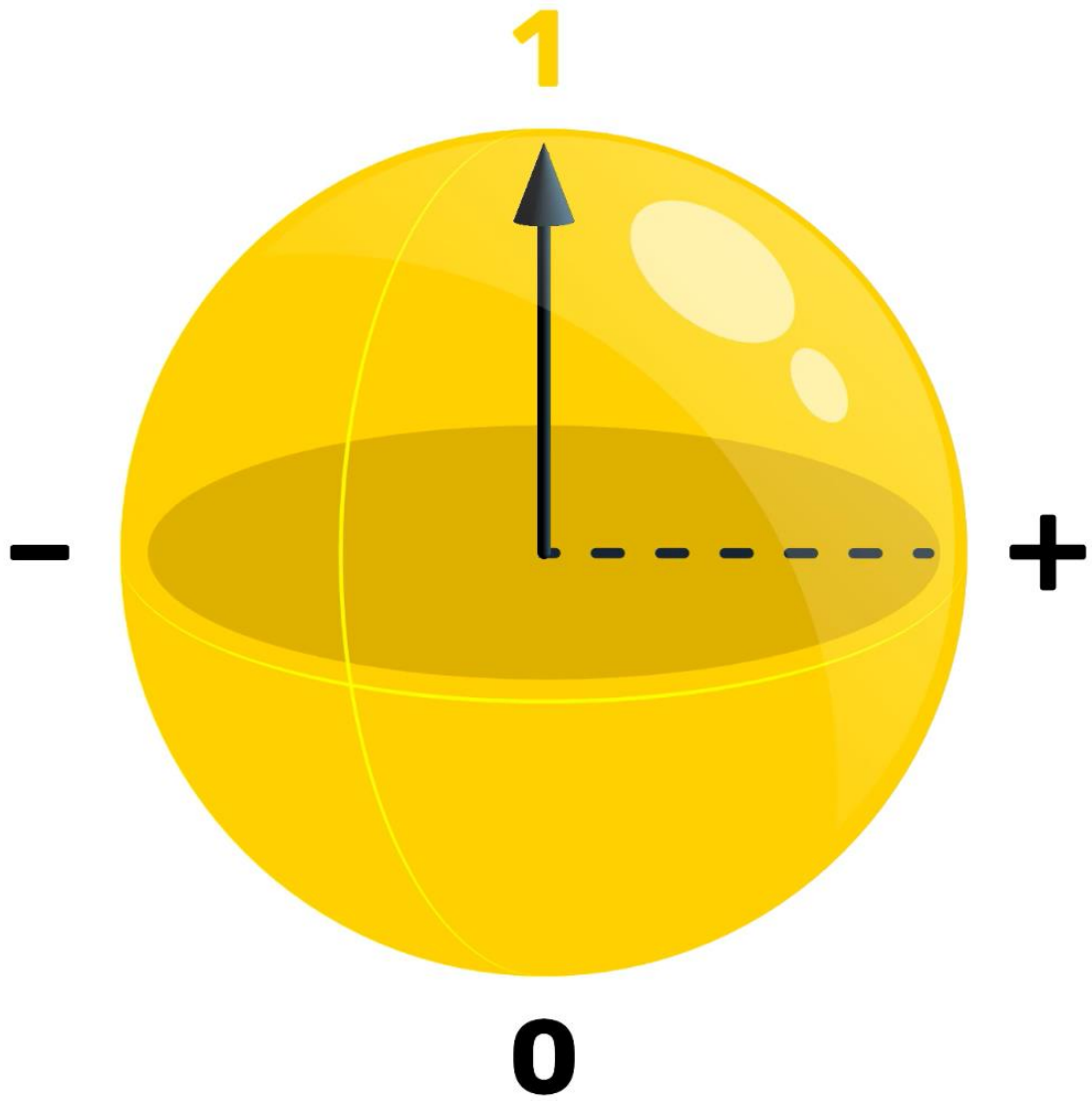
Bit

Bit

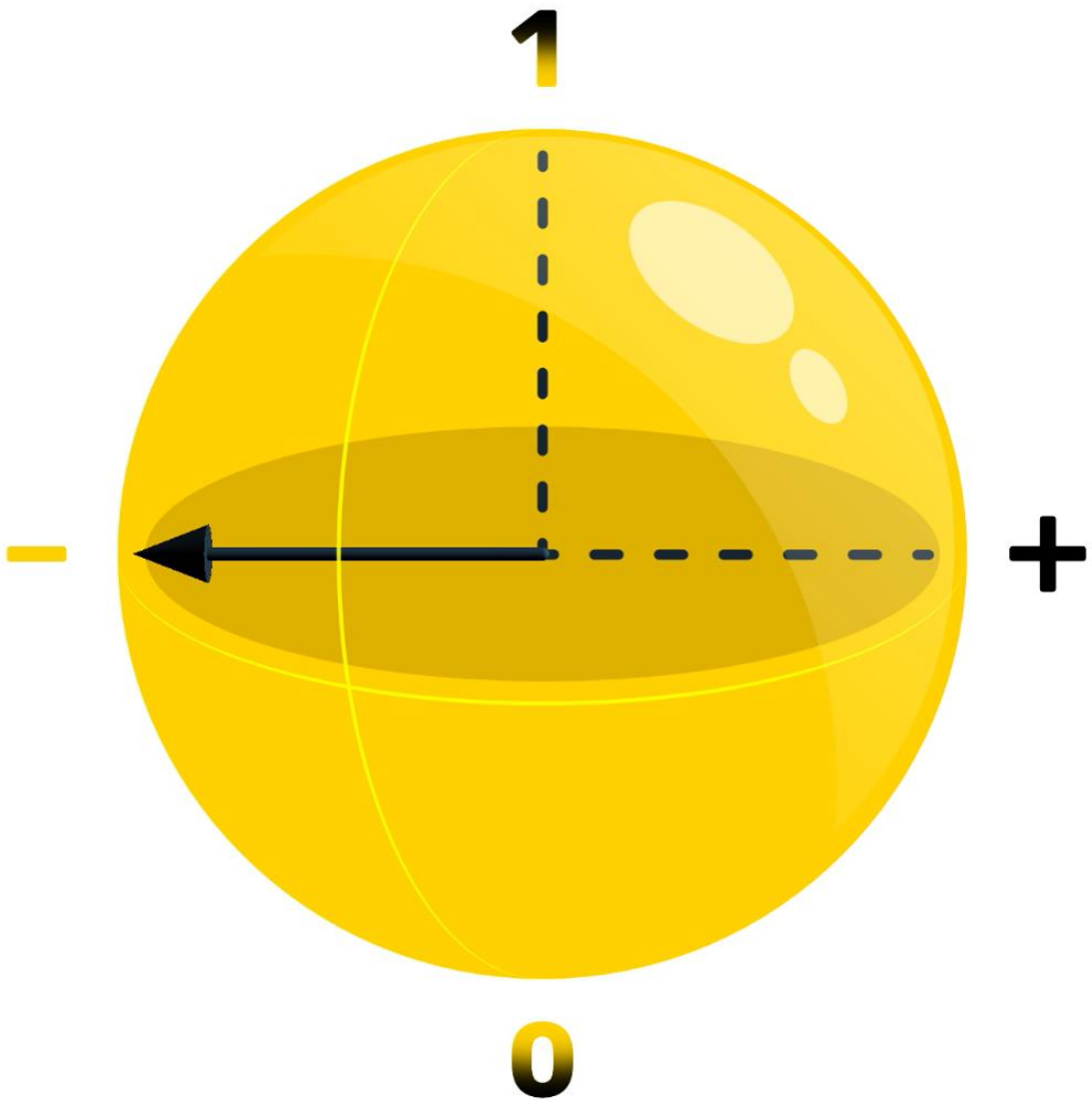
Phase

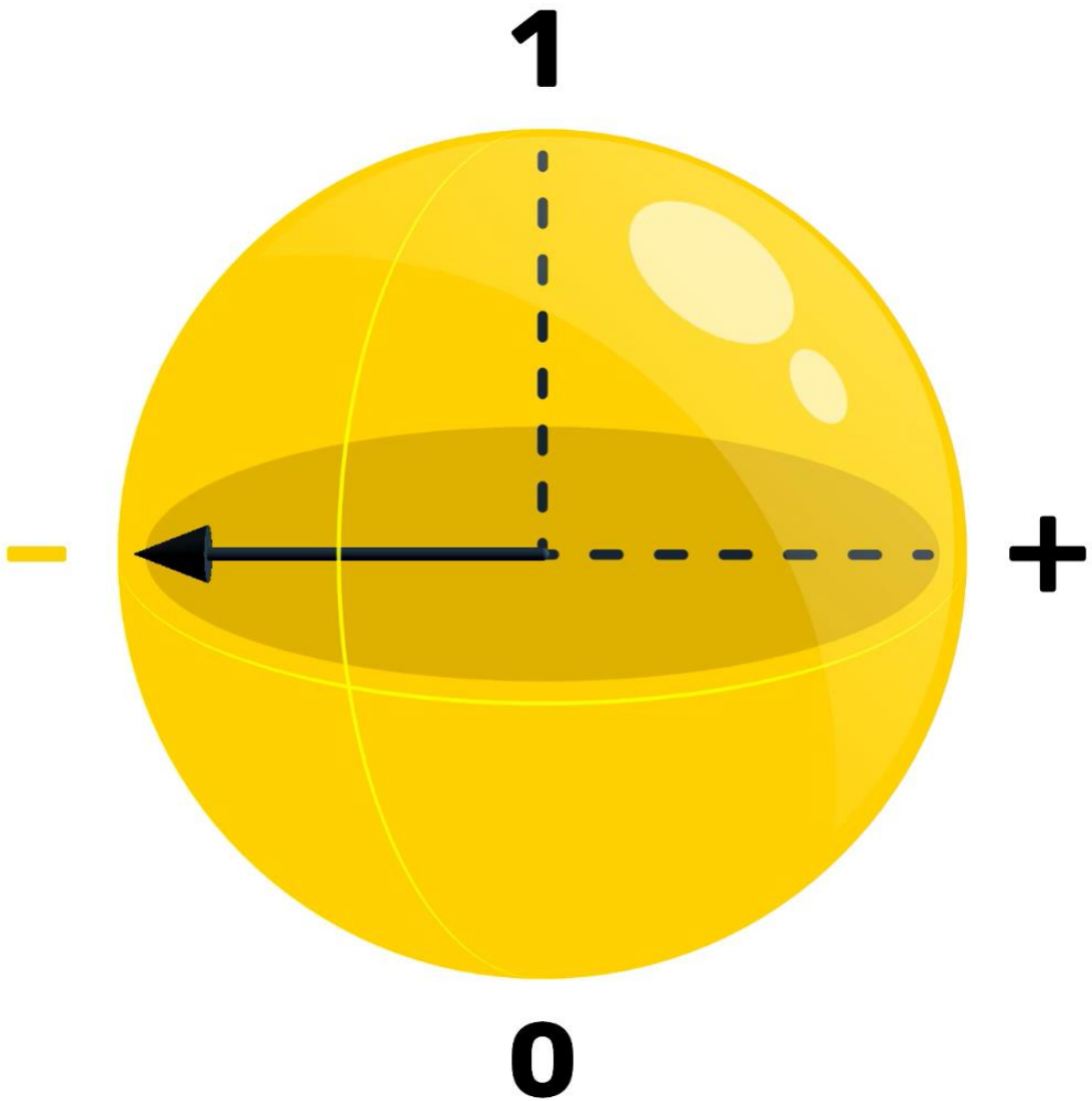


Bit-Flip



Phase-Flip

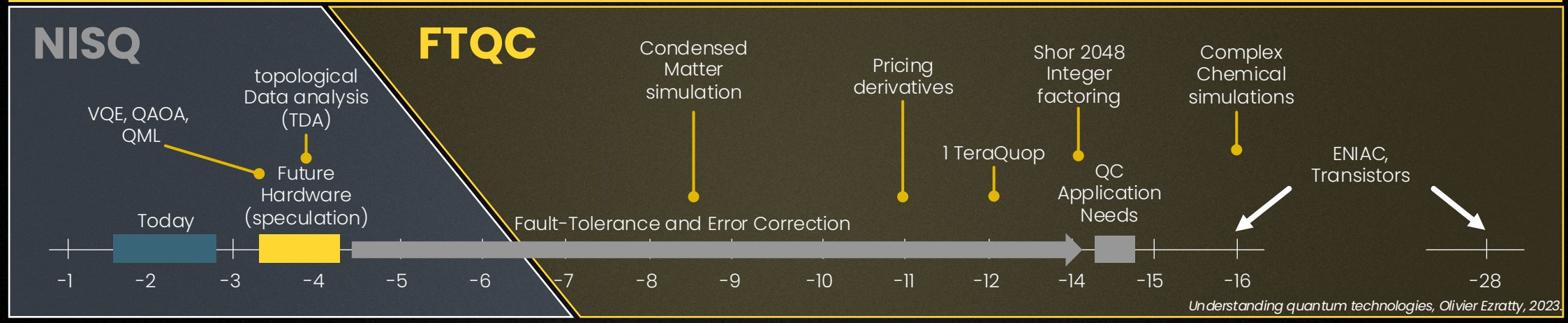



1
−
+
0

Quantum computers are still not reliable enough for their first use case

Very low error rates is required to unlock exponential speed-up

QC are not reliable enough at the moment



Quantum operations error probabilities ($\log_{10}$)

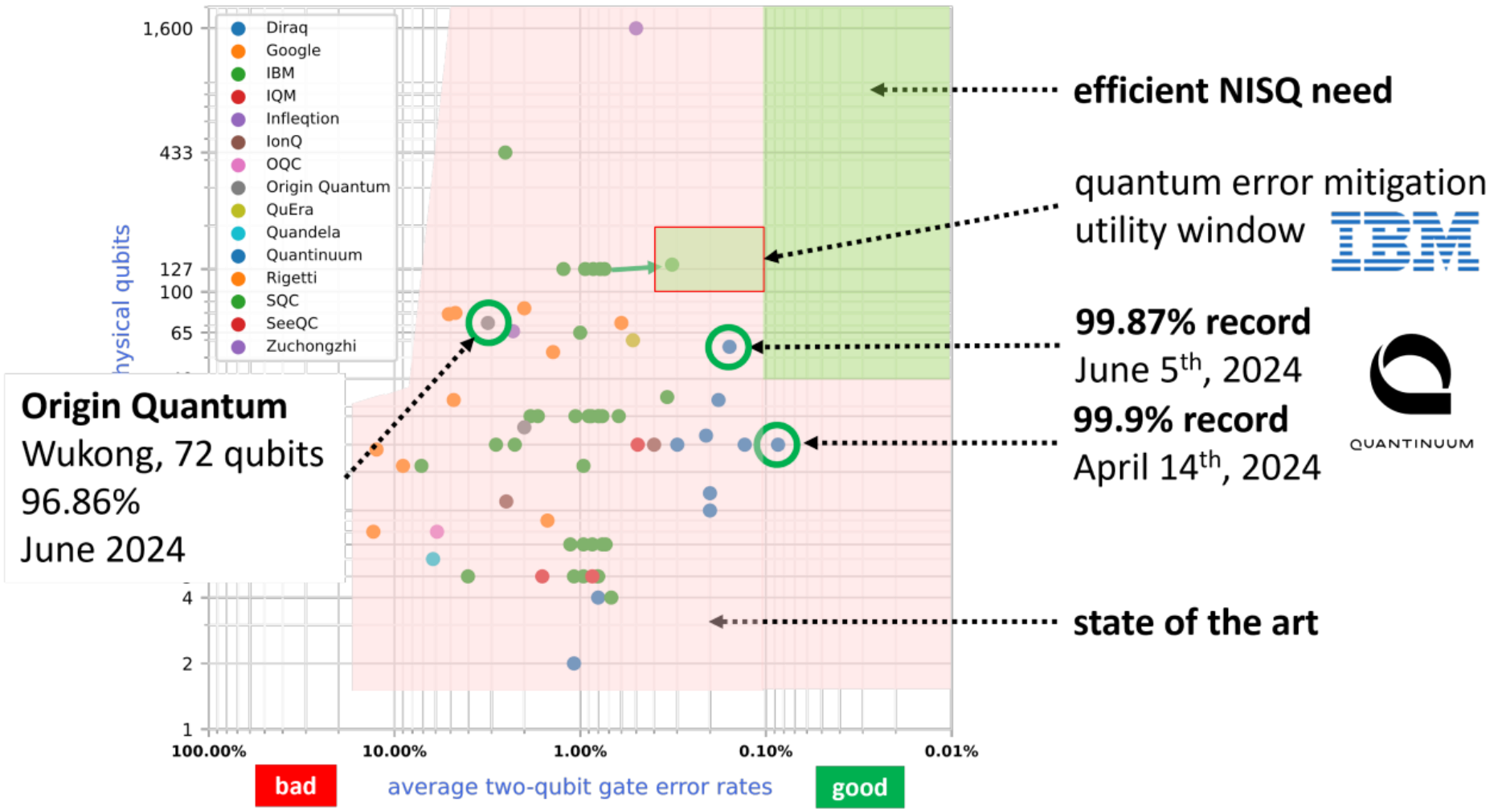
NISQ quantum Error mitigation

Quantum Computers for Specialized Applications and Limited Applicability

Broadly Useful Quantum Computers: general purpose, Scalable, and accurate

	Chemistry	Finance	Cryptography
# of perfect qb	100 - 1,000	10,000	1,000 – 10,000
# of gates	10^{14} - 10^{16}	10^{10} - 10^{11}	10^{11}
Error per gate	10^{-17}	10^{-13}	10^{-14}

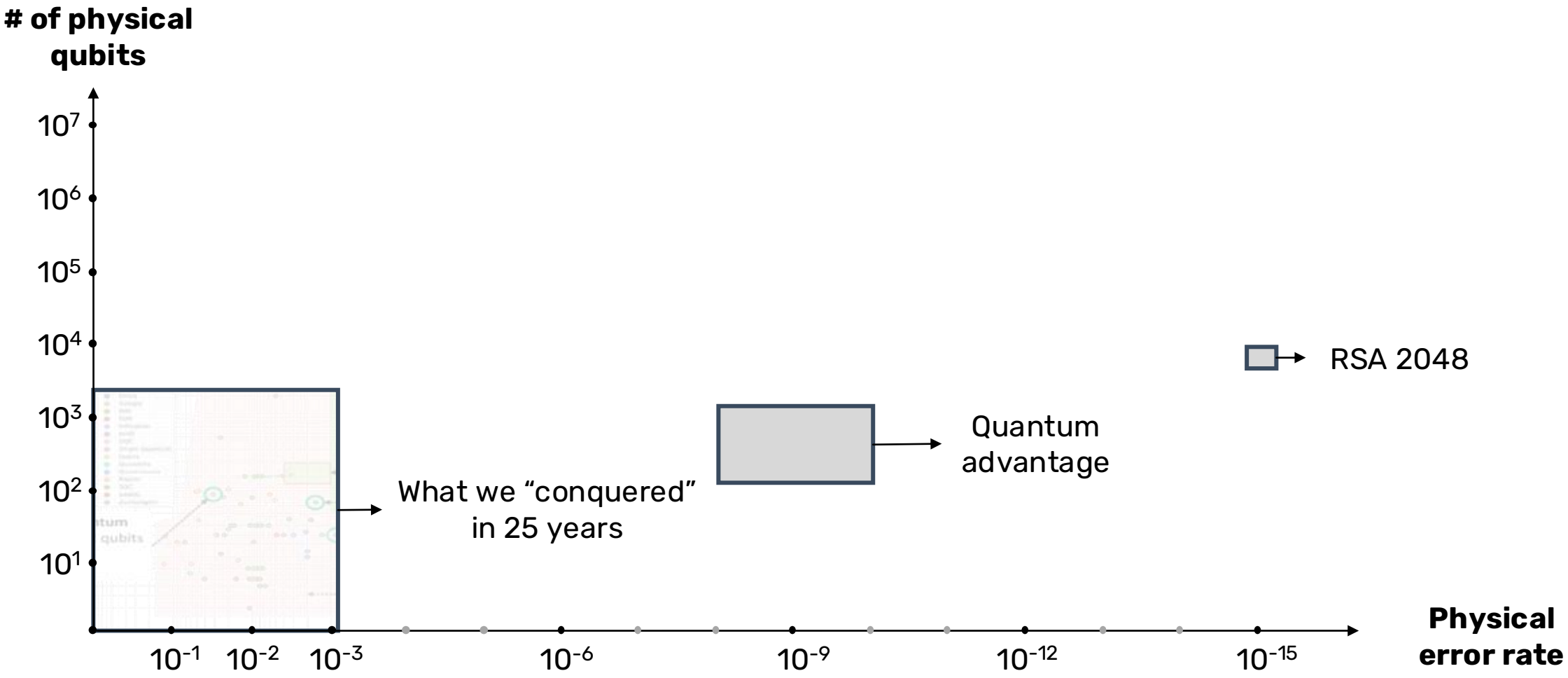
The specs of the current hardware…



SOURCE

1. Olivier Ezratty

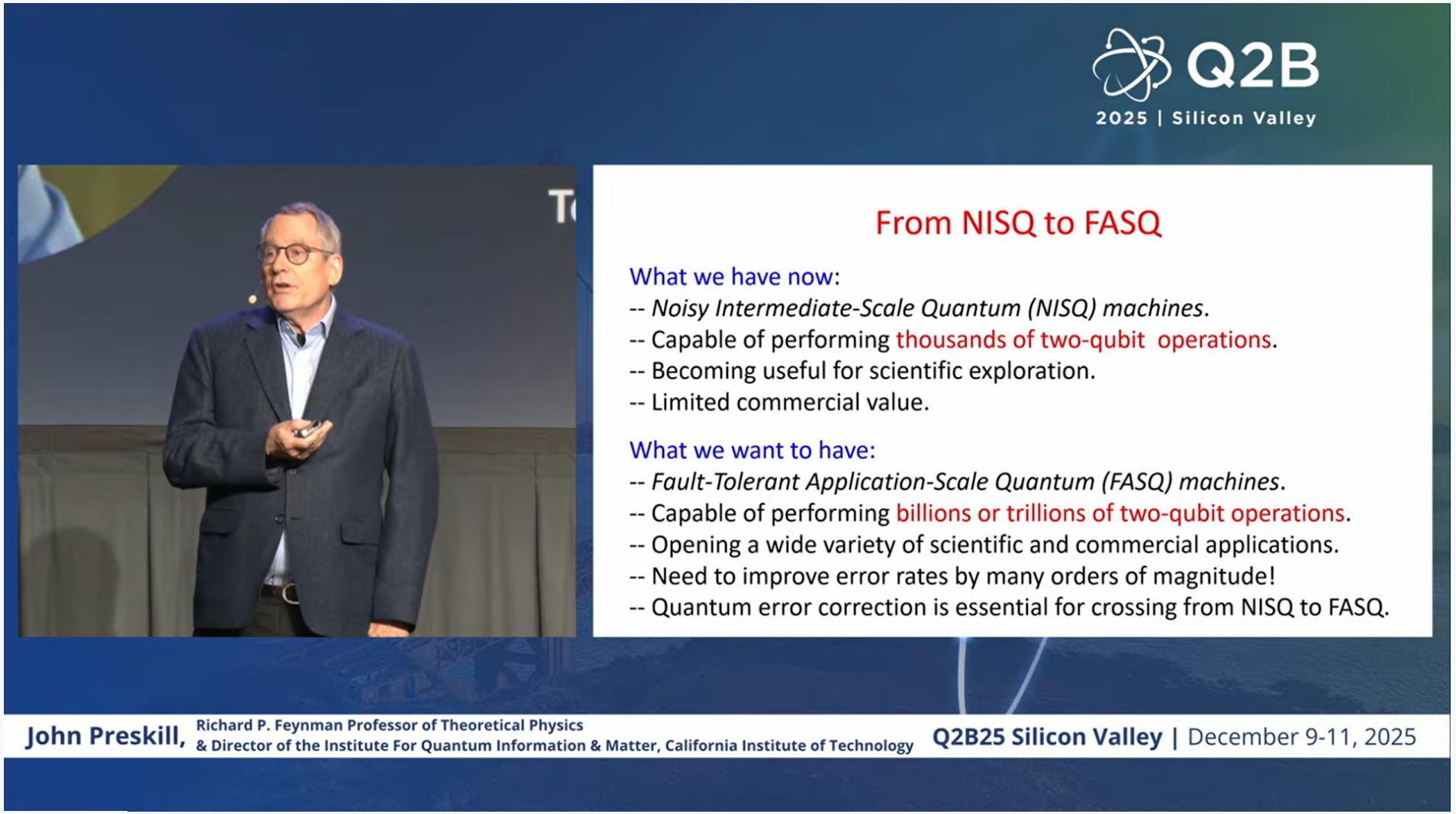
… and the specs we'd need to reach



SOURCE

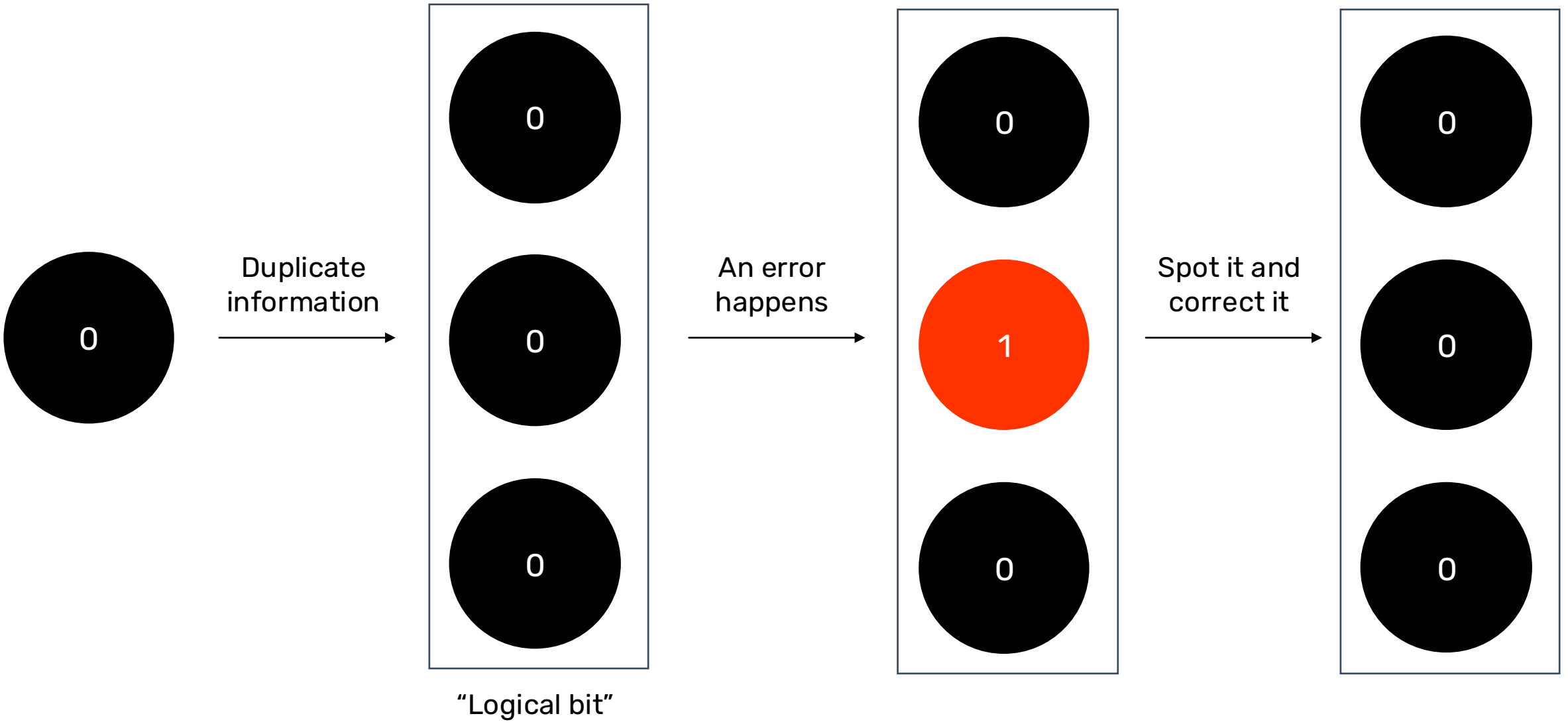
1. Travis Scholten (IBM) et al., arXiv, 2024

NISQ fails to fulfill its promises



NISQ vs FTQC

	NISQ (Today)	FTQC (Future)
Qubit quality	Noisy	Error-corrected
Reliability	Limited	High
Computation length	Short	Long and scalable
Error correction	Minimal/none	Continuous
Main hardware	Physical qubit	Logical qubits
Scale	10-1000 qubits	Millions of physical qubits
Typical use	Experience & prototypes	Practical large-scale applications


0
Duplicate information
0
0
0
“Logical bit”
An error happens
0
1
0
Spot it and correct it
0
0
0

“Redundant” Error Correction is The best Solution to Date to Escape the Paradox

QUANTUM ERROR CORRECTION

(In simple words)

// .01

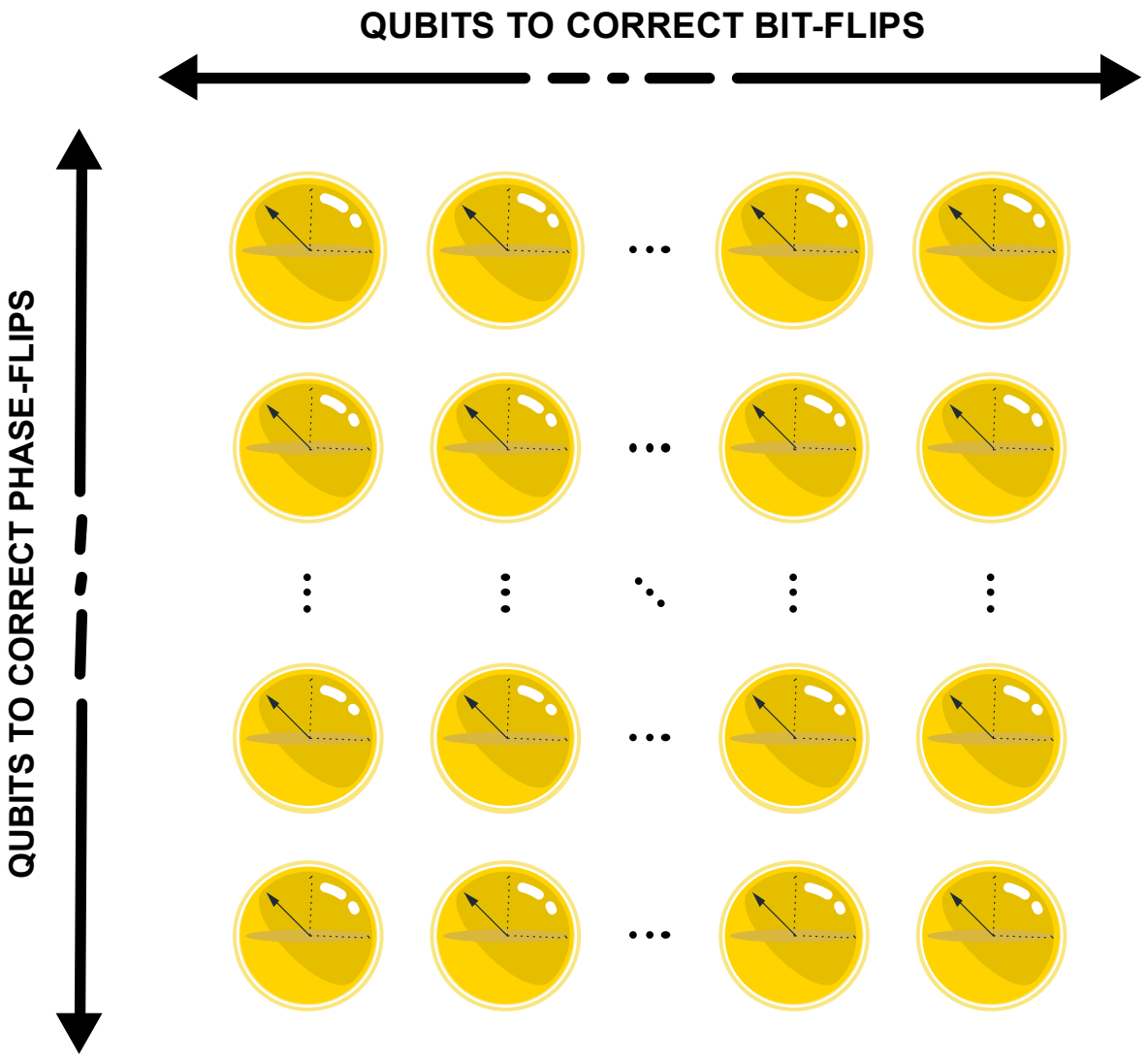
Same information within a **set** of **qubits**

// .02

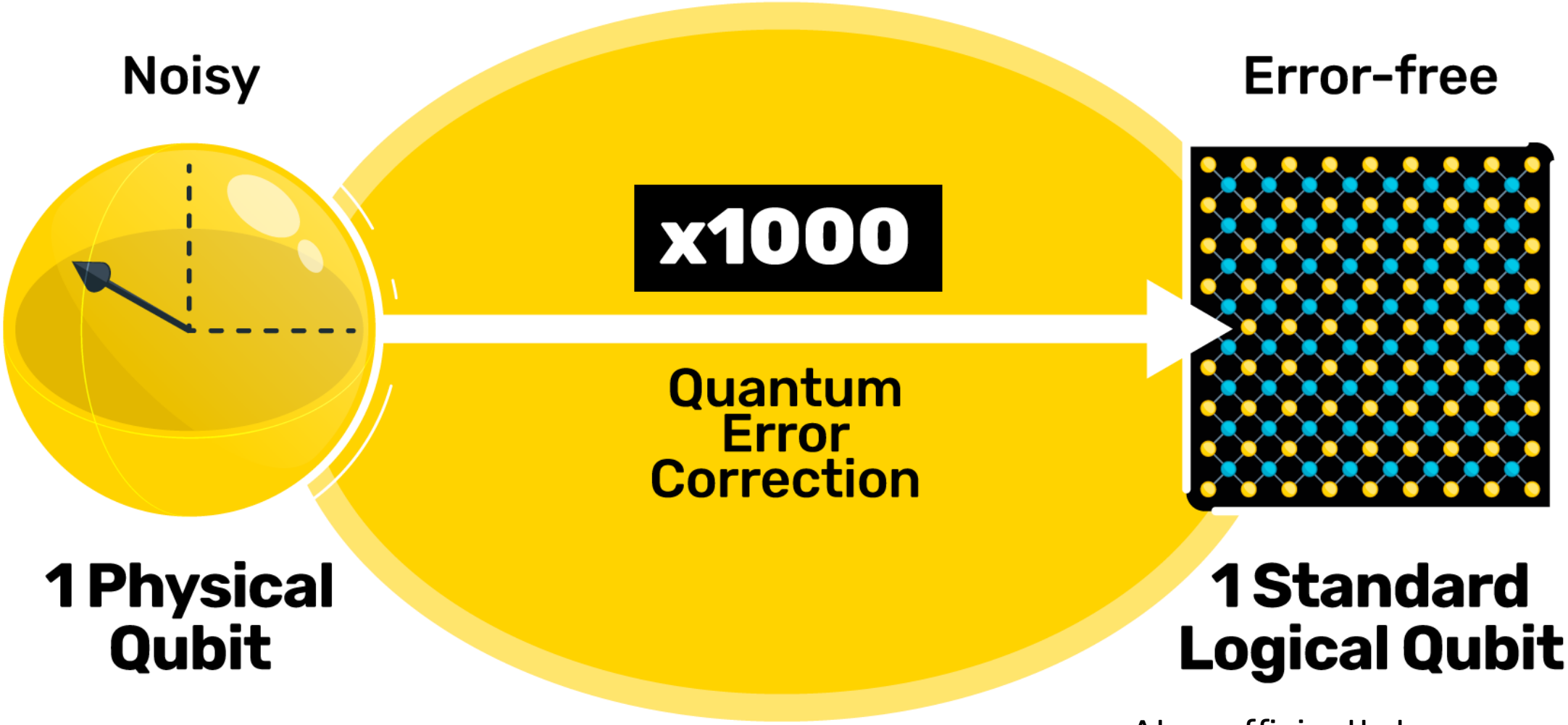
Check if the qubits in the set “**agree**” with each other

// .03

If a **qubit is different** from its neighbors, **correct it**



Quantum error correction is qubit-expensive...

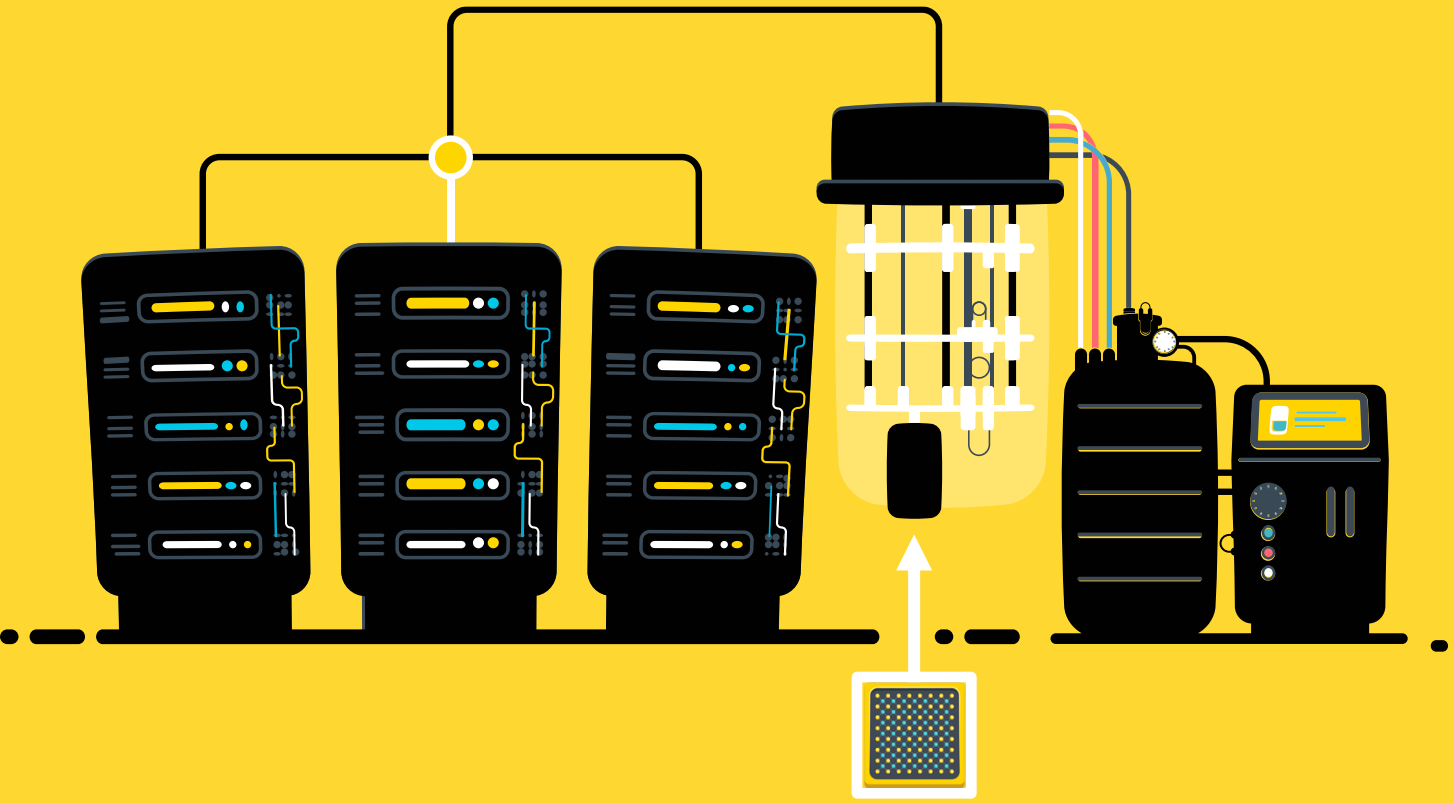


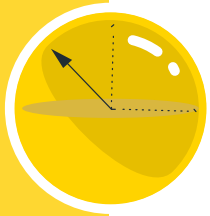
At a sufficiently low error rate to break RSA 2048 [1,2]

1. *Craig G. et al. "How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits." Quantum 5 (2021)*
2. *Rajiv A., et al. "Quantum Error Correction Below the Surface Code Threshold." (2024)*

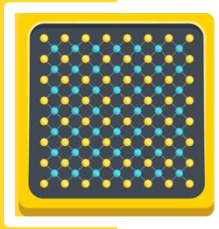
With Today's Technology You Would Need A Full Cryogenic System And 3 Dense Control Racks To run a Logical Qubit

~10 M$ | ~50 kW





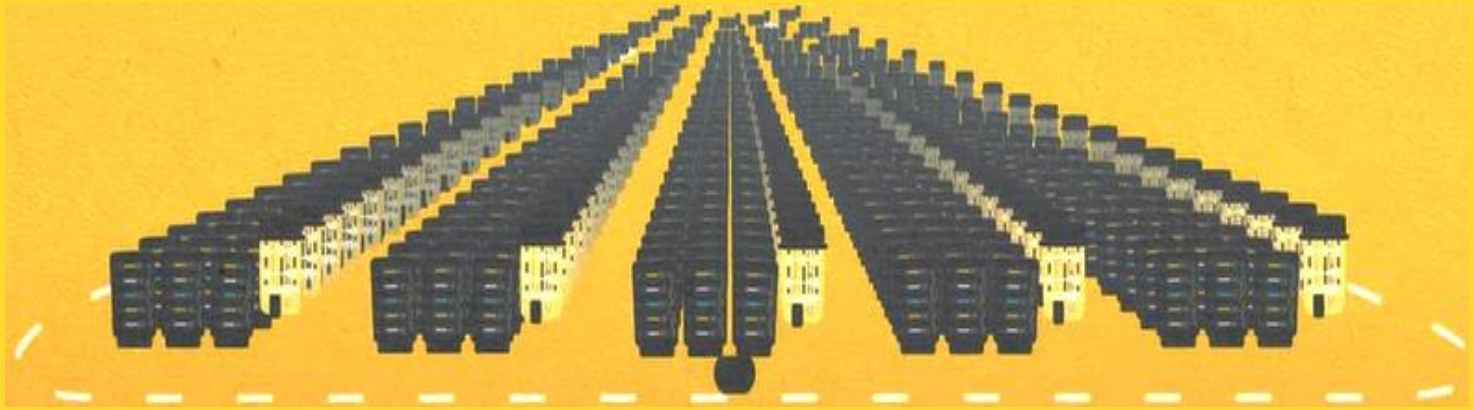
1 000
Physical Qubits

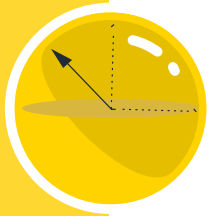


1
Logical Qubit

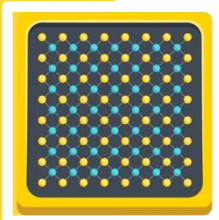
What Does it Mean for Quantum Computing at Scale?

100 CRYOSTATS → **1 B$**
1 000 kW



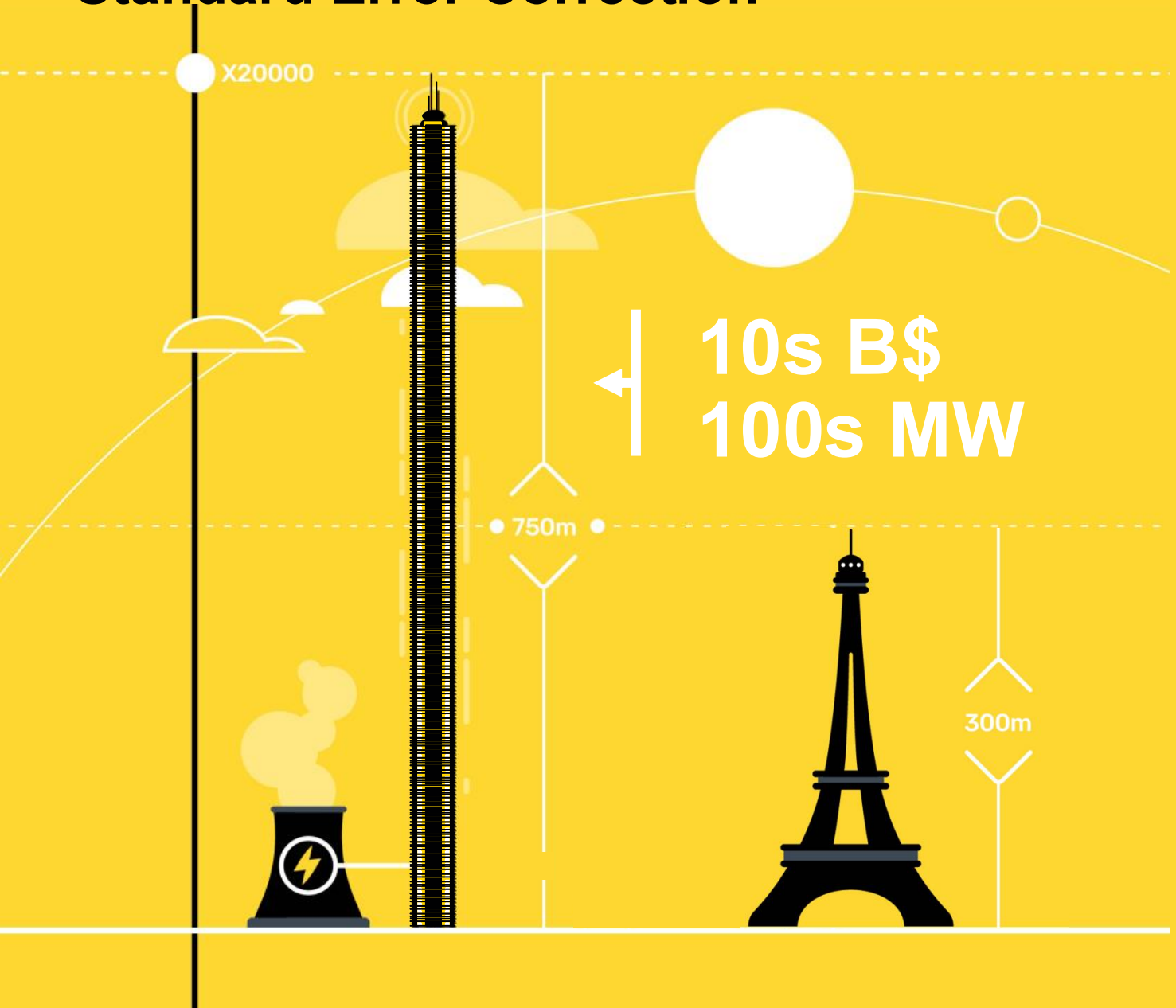


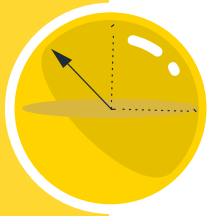
100 000
Physical Qubits



100
Logical Qubits

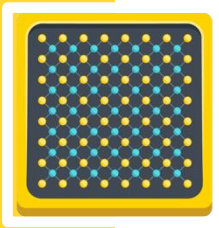
Run Shor's Algorithm on Standard Error Correction





20 000 000

Physical Qubits



20 000

Logical Qubits

Ways of doing a Qubit

	Superconducting	Photonics	Neutral atoms	Trapped ions	Others
Major players	IBM, Google, aws, IQM, rigetti, ALICE & BOB	PsiQuantum, XANADU, QUANDELA	QuEra Computing Inc., Pasqal, atom computing	IONQ, QUANTINUUM, AQT	Microsoft, intel, 12, quobly
Size of investment (M$)	3496	2108	217	1654	920

SOURCES

1. McKinsey
2. Olivier Ezratty

NOTE

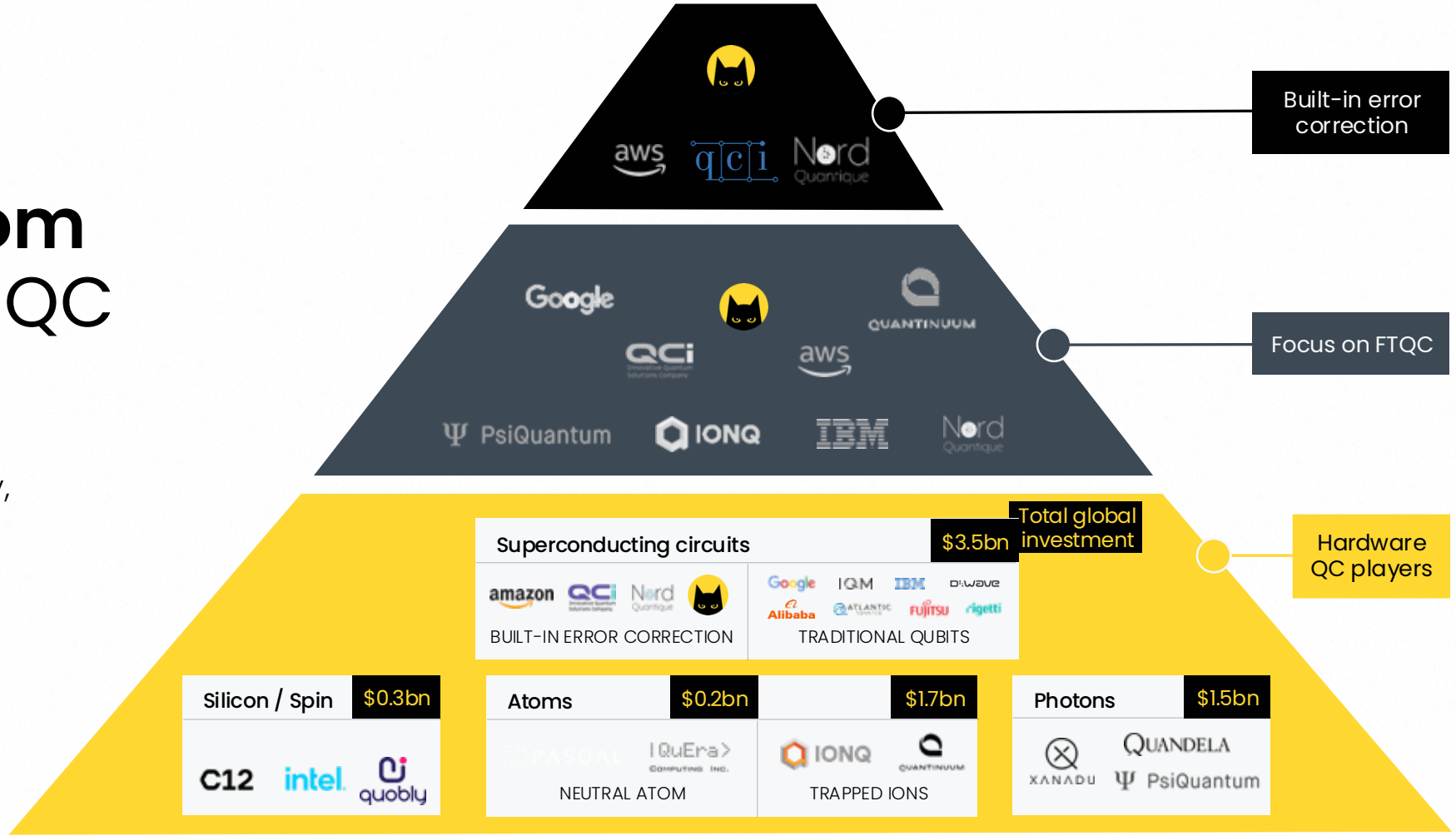
1. Figures need to be updated with the latest 2025 investments
2. These estimations include guesses for companies whose investment figures are not public. We assumed $500M for Google, IBM, Alibaba and AWS in superconducting qubits, $200M for Honeywell in trapped ions and $200M for Intel in silicon spin qubits.

How Alice & Bob differentiates **from other hardware** QC actors

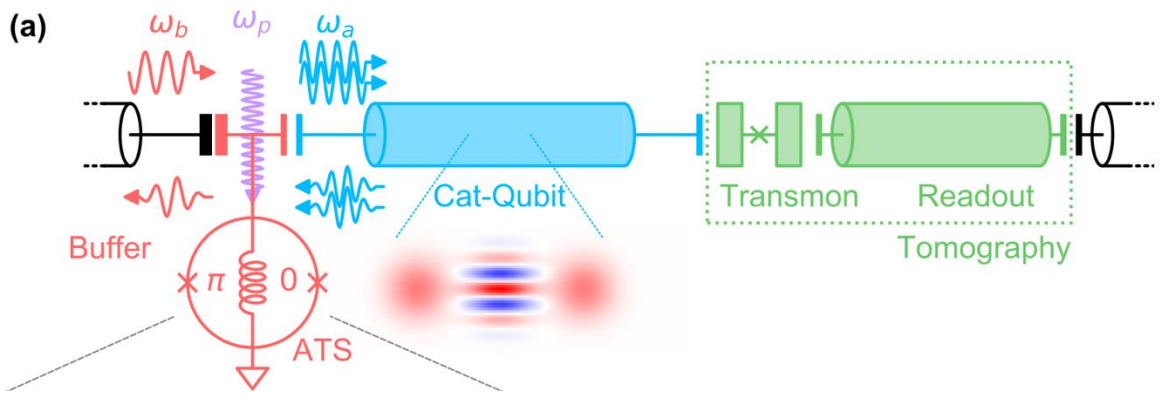
A superconductor-based technology, aiming at FTQC with our built-in error corrected qubit: the cat qubit

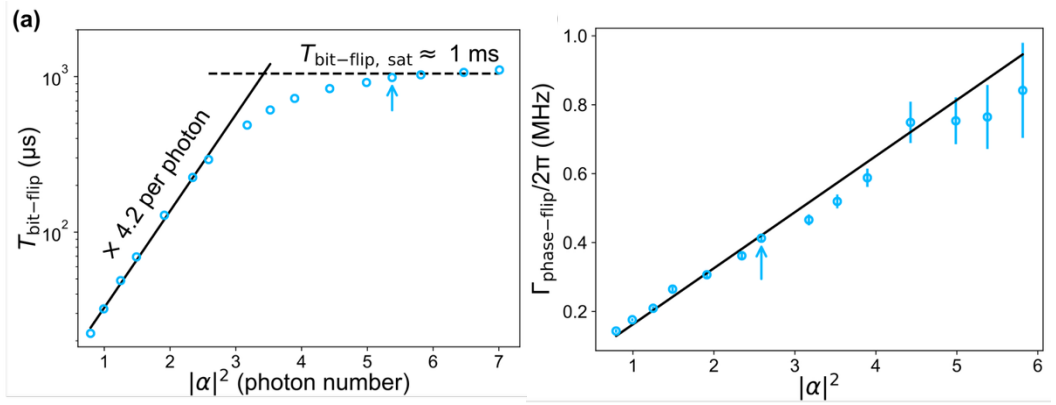
12x

Increase in cat qubit research publications over the past 5 years

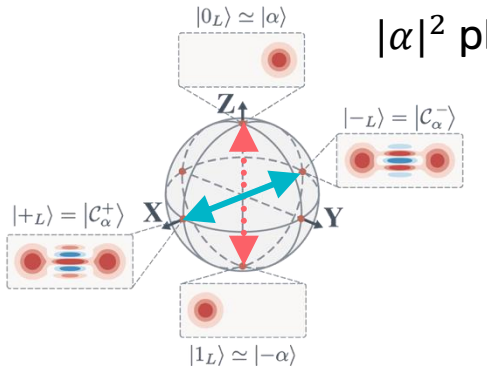


The Cat Qubit





Bit Flips: Autonomous QEC



$|\alpha|^2$ photons

Strong **noise biasing**:

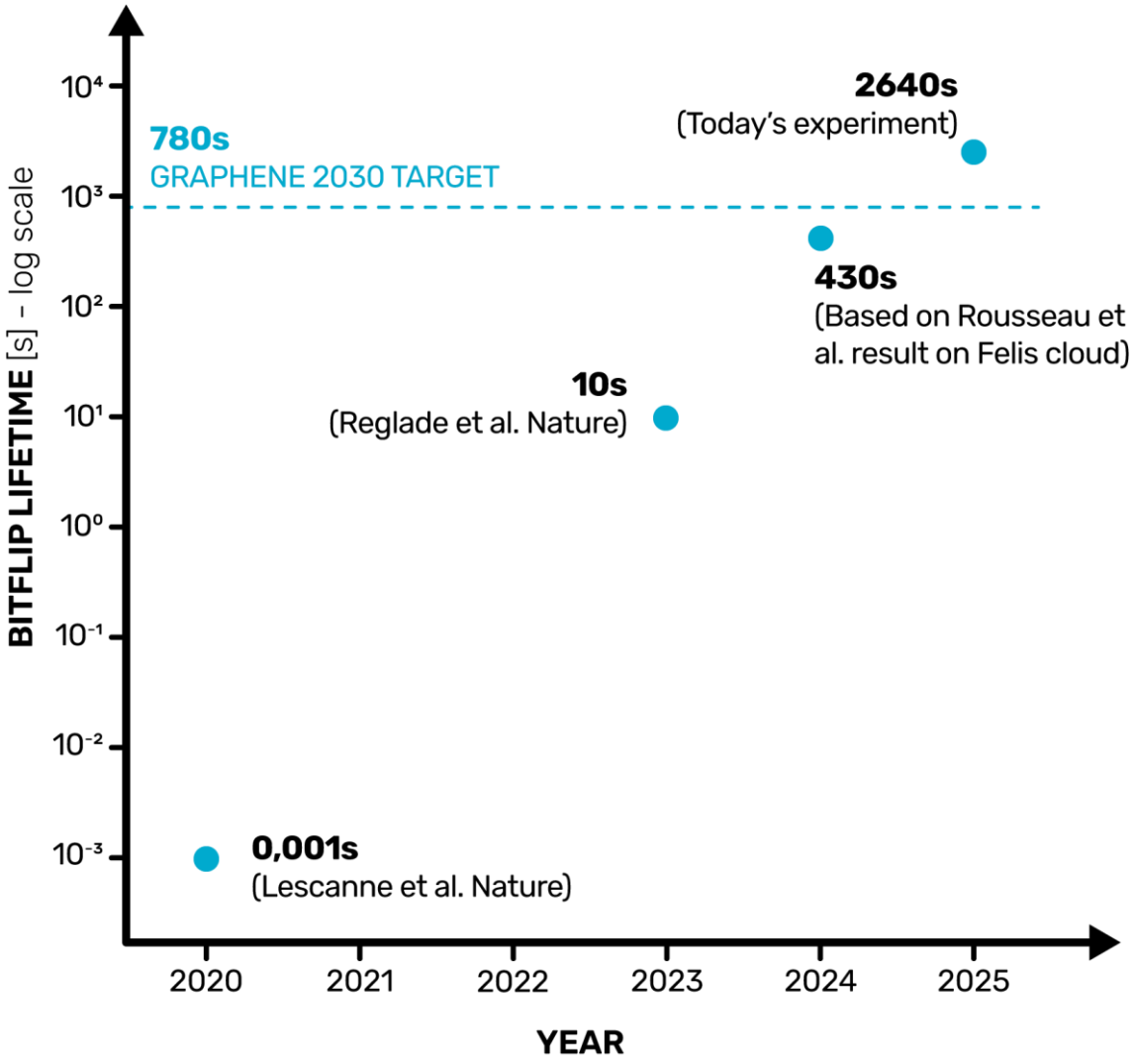
- **Bit-flips** are suppressed **exponentially**

$$\Gamma_X \propto e^{-\gamma|\alpha|^2} \qquad (\gamma \lesssim 2)$$

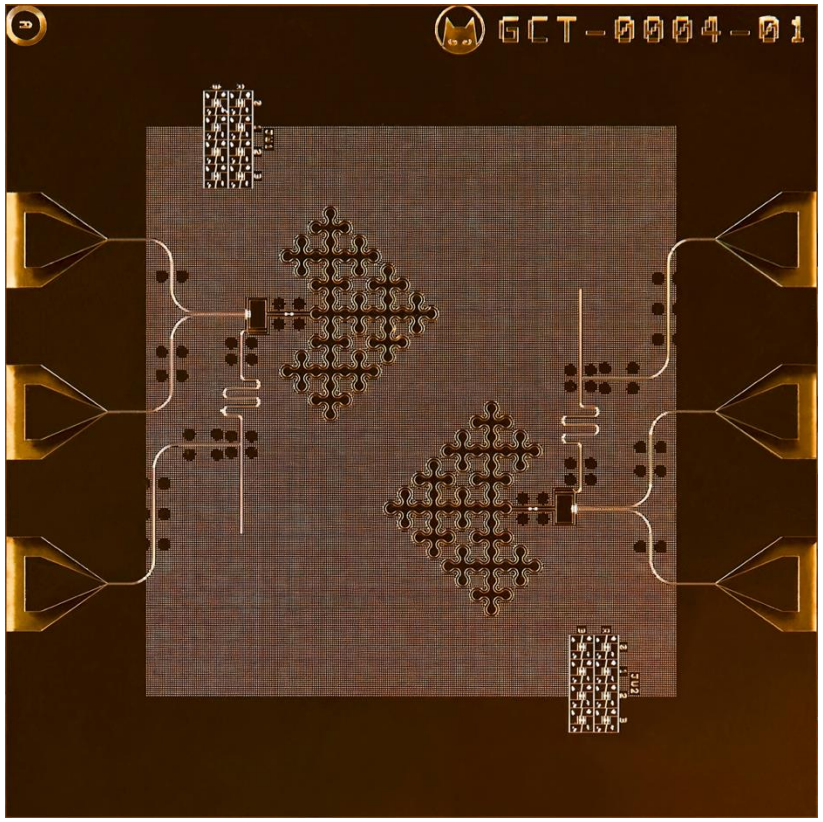
- **Phase-flips** increase **linearly**

$$\Gamma_Z = 2|\alpha|^2\kappa_1 \qquad \text{(single-photon loss)}$$

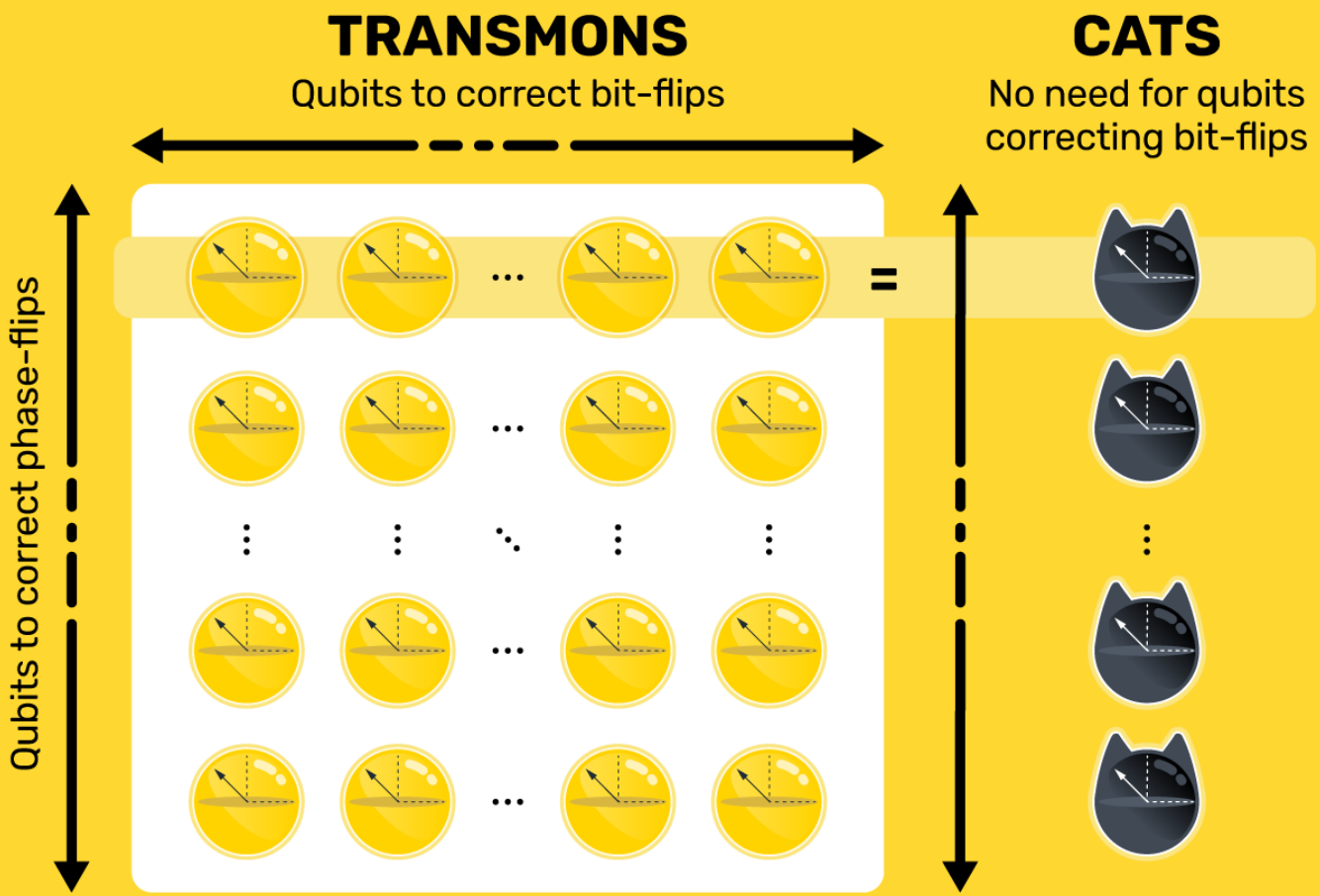
ALICE & BOB BIT-FLIP LIFETIME BY YEAR



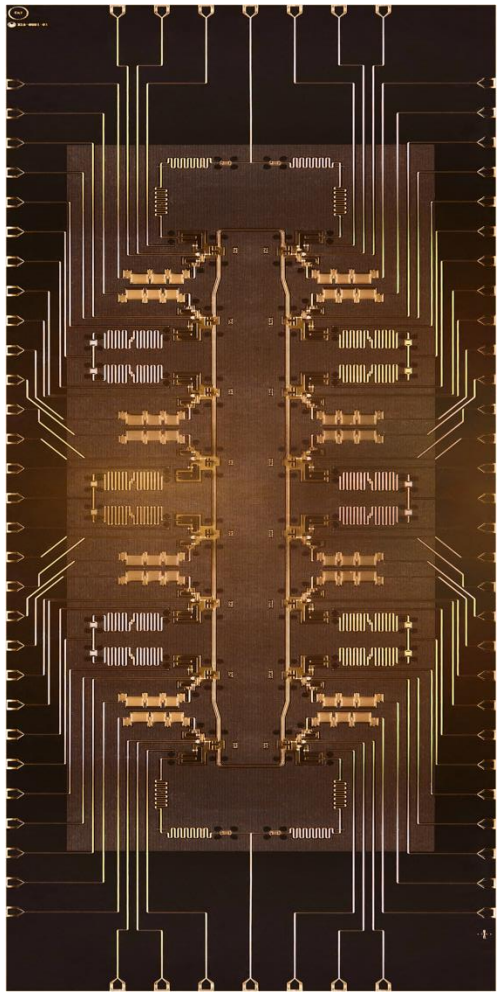
BOSON 4 SINGLE CAT-QUBIT ON THE CLOUD

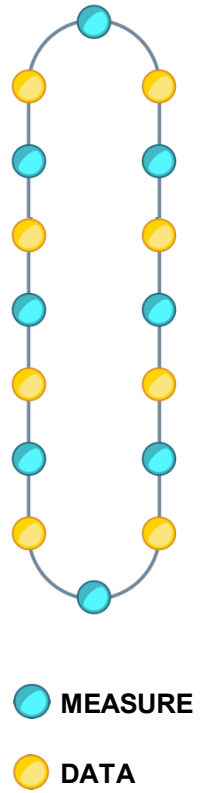


With Only One Error Left, Correction Can Be One-dimensional, Only Taking Care Of Phase Flips



HELIUM, 16 CAT-QUBIT NOW IN TESTING





Low-overhead FTQC with repetition-cat code

Bit-flip suppression*

39 Transmon qubits [1] VS **1** cat qubit [2]

(* hour-long bit flip time)

[1] Google Quantum AI et al., *Nature* 638, 920–926 (2025)
[2] Jezouin, https://alice-bob.com/blog/just-out-of-the-lab-a-cat-qubit-that-jumps-every-hour/ (2025)

100 logical memory qubits*[5]

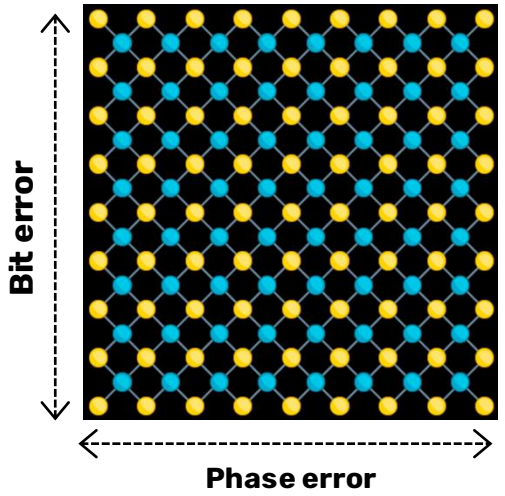
33,700 Transmon qubits w/ surface code VS **2,100** cat qubits w/ repetition code

(* 10^{-8} logical error rate)

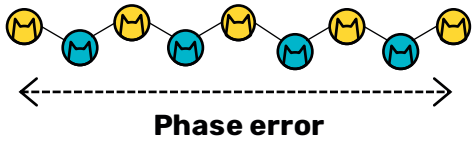
[5] Ruiz, Guillaud, Leverrier et al., Nat. Commun. (2025)

Logical qubit resources drop

Surface code [3]



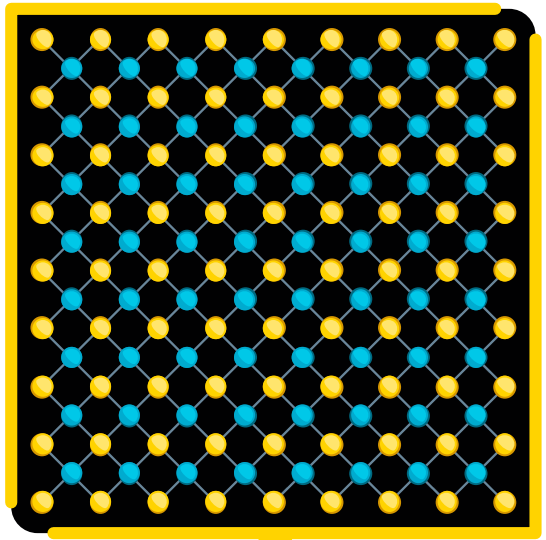
Alice & Bob [4]



[3] Fowler et al., PRA 86 (2012)
[4] Guillaud, Mirrahimi, PRX 9, 10.1103 (2019)

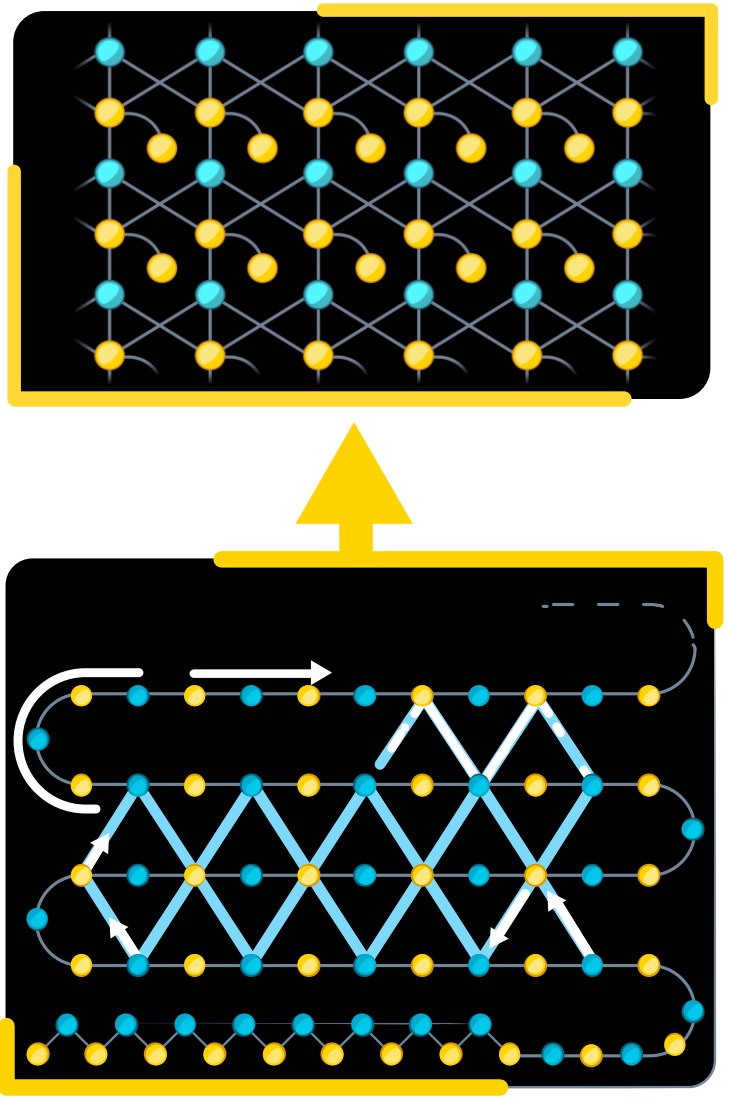
Cats Have One Dimension To Play With, Allowing For More Efficient Codes

SURFACE CODE – 2D



CAT REPETITION CODE – 1D

CAT LDPC CODE – 2D[1]



1. *Diego R., et al."LDPC-cat codes for low-overhead quantum computing in 2D" (2024)*

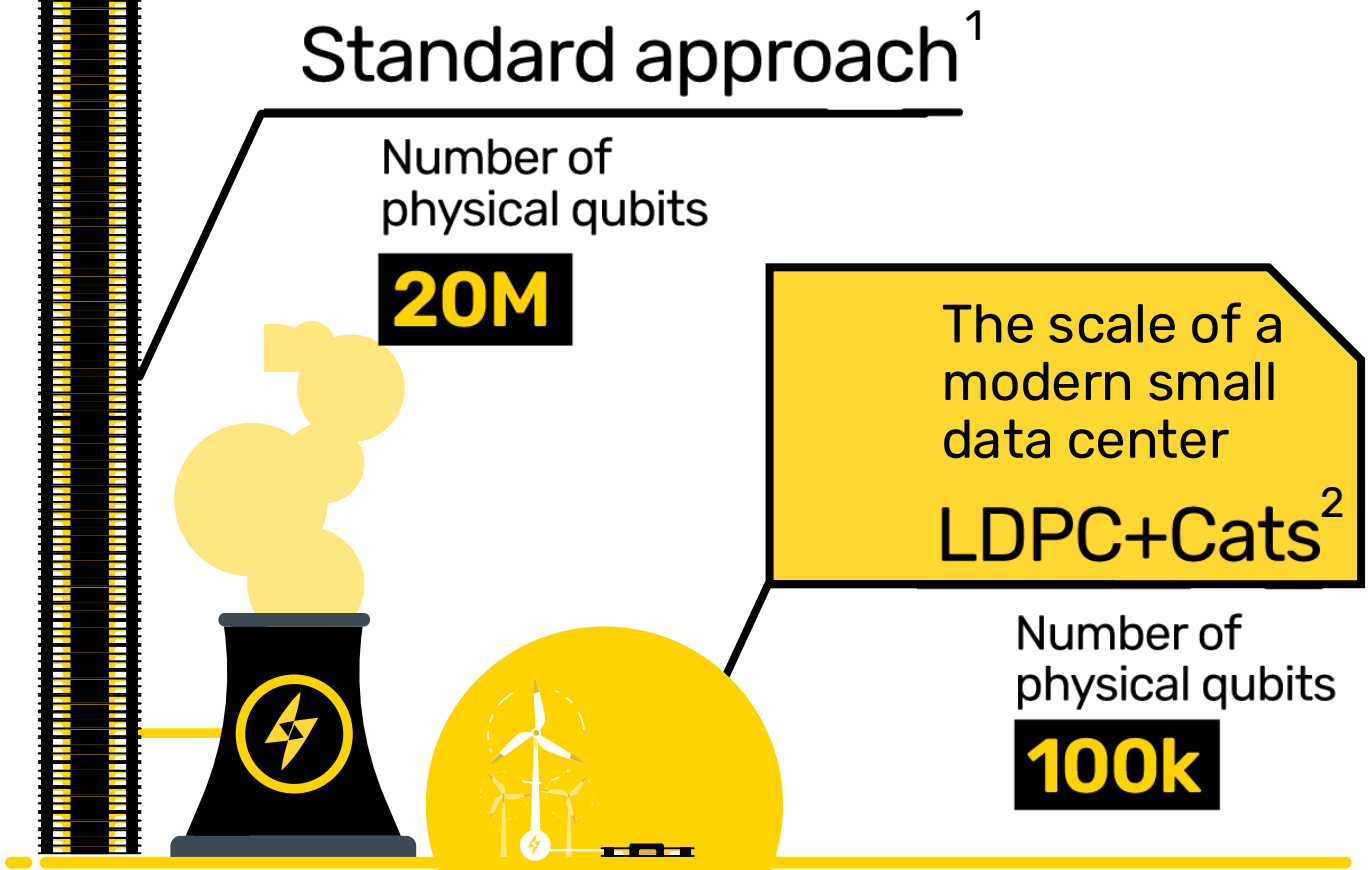
EXTRA CONNECTIONS BETWEEN DISTANT QUBITS

LESS PHYSICAL QUBITS PER LOGICAL QUBIT

200x REDUCTION

VS STATE-OF-THE-ART SURFACE CODE FOR SHOR

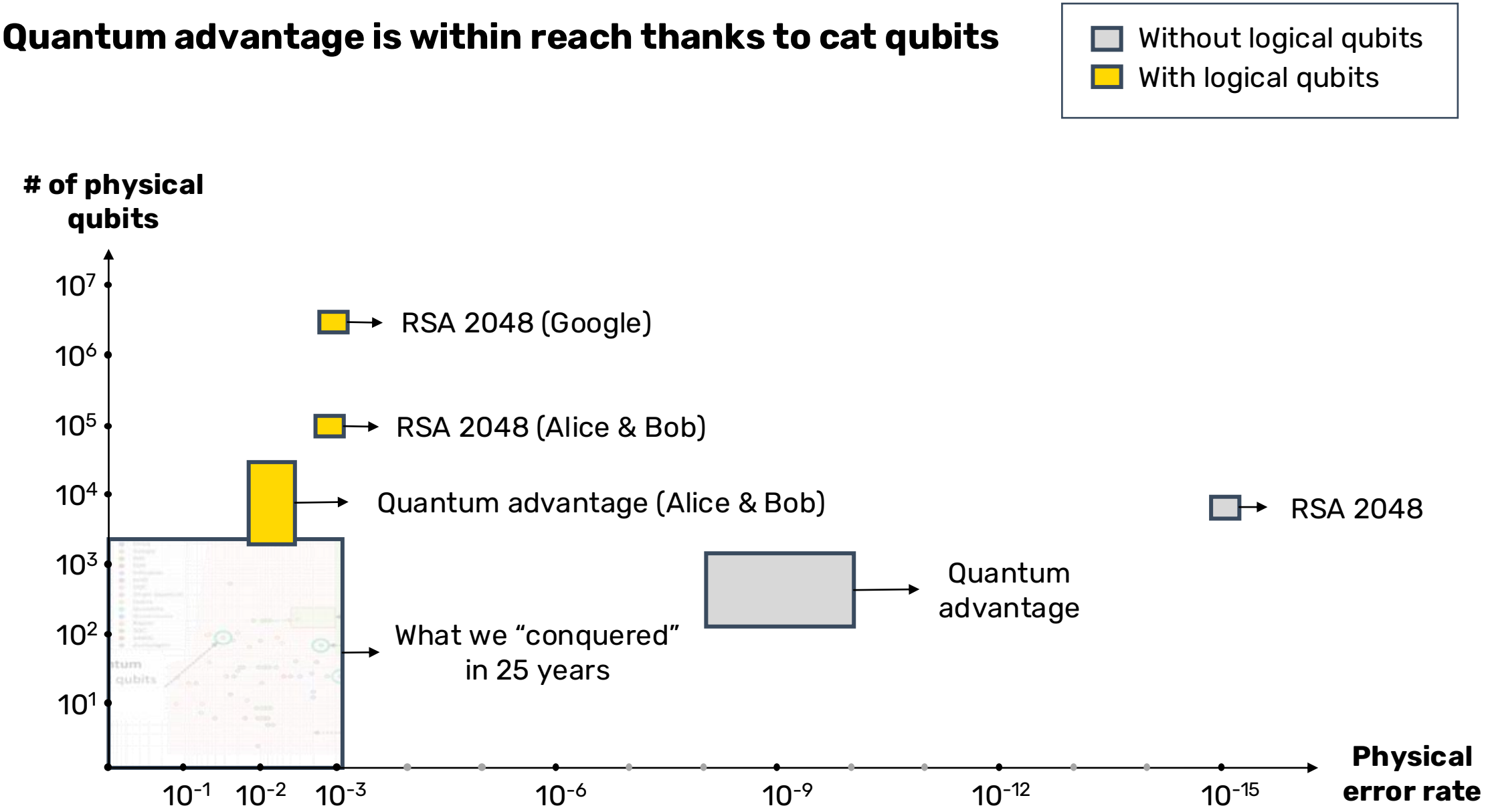
This is How a Useful Quantum Computer Could Become Practical Sooner



Read the full story: Alice&Bob roadmap
alice-bob.com/whitepaper-download

1. *Craig G. et al. "How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits." Quantum 5 (2021)*
2. *Diego R. et al."LDPC-cat codes for low-overhead quantum computing in 2D" (2024)*

Quantum advantage is within reach thanks to cat qubits



SOURCE

1. [É. Gouzien *et al.*, Phys. Rev. Lett. **131**, 040602 (2023)] & [D. Ruiz *et al.*, arXiv:2401.09541 (2024)]

// MILESTONE 1

MASTER THE CAT QUBIT

2024
COMPLETE

Cat Qubits	1
Logical Qubits	0

// MILESTONE 2

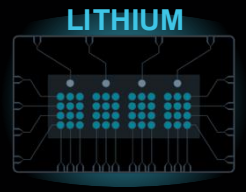
BUILD A LOGICAL QUBIT

WE ARE HERE

Cat Qubits	16
Logical Qubits	1
Clock Speed (µs)	1.5
Logical Error Rate	10^{-2}

// MILESTONE 3

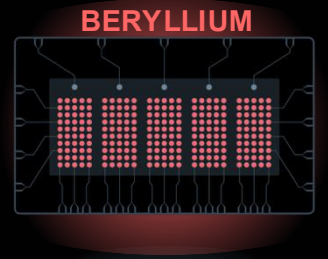
FAULT-TOLERANT QUANTUM COMPUTING



Cat Qubits	48
Logical Qubits	4
Clock Speed (µs)	0.8
Logical Error Rate	10^{-3}

// MILESTONE 4

UNIVERSAL QUANTUM COMPUTING

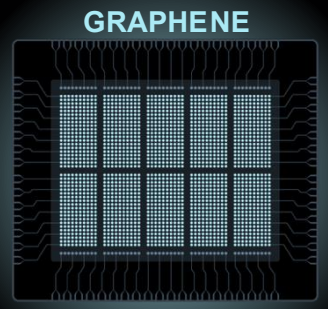


Cat Qubits	250
Logical Qubits	5
Clock Speed (µs)	0.8
Logical Error Rate	10^{-4}

// MILESTONE 5

USEFUL QUANTUM COMPUTING

BY 2030



Cat Qubits	2 000
Logical Qubits	100
Clock Speed (µs)	1
Logical Error Rate	10^{-6}

Focusing on proven computational advantage

	Problem Solved	Quantum Complexity	Classical Complexity	Computational speedup	Comments on logical qubit requirements for solving relevant-scale problems
QPE algorithm	Estimate eigenvalues of unitary operator	Polynomial for Hamiltonian simulation	Exponential in the general case for Hamiltonian simulation	**Up to exponential but context-dependent**	Condensed matter physics (e.g. Hubbard model with ≈100 logical qubits)[2-3] Quantum chemistry simulations with ≈1000 logical qubits[4]
Time evolution algorithm	Study dynamics of quantum systems	Polynomial	Exponential in the general case	**Exponential**	Evolution of system with ≈200 logical qubits for well-chosen problems[5-6]
Shor's algorithm	Integer factorization, discrete logarithm	$O(\{\log N\}^3)$ (basic implementation)	$\exp[\tilde{O}(\{\log N\}^{1/3})]$	**Superpolynomial[2]**	Cryptanalysis with ≈1000 logical qubits[7-8]
HHL algorithm	Solve system of linear equations	$O(\log N)$ (under assumption)	Polynomial, typically $O(N^3)$	**Exponential (under restrictive conditions)**	Potential applications in data analysis or differential equations, but difficult to preserve exponential speedup in end-to-end settings[9-10]
Grover's algorithm	Unstructured search	$O(\sqrt{N})$	$O(N)$	**Quadratic**	Quadratic speedups are not enough for practical advantage[11-12]

2. The speedup provided by Shor's algorithm is exponential for discrete logarithms on elliptic curves, but superpolynomial for integer factorization.

Materials science simulations are the strongest candidates to benefit from eFTQC

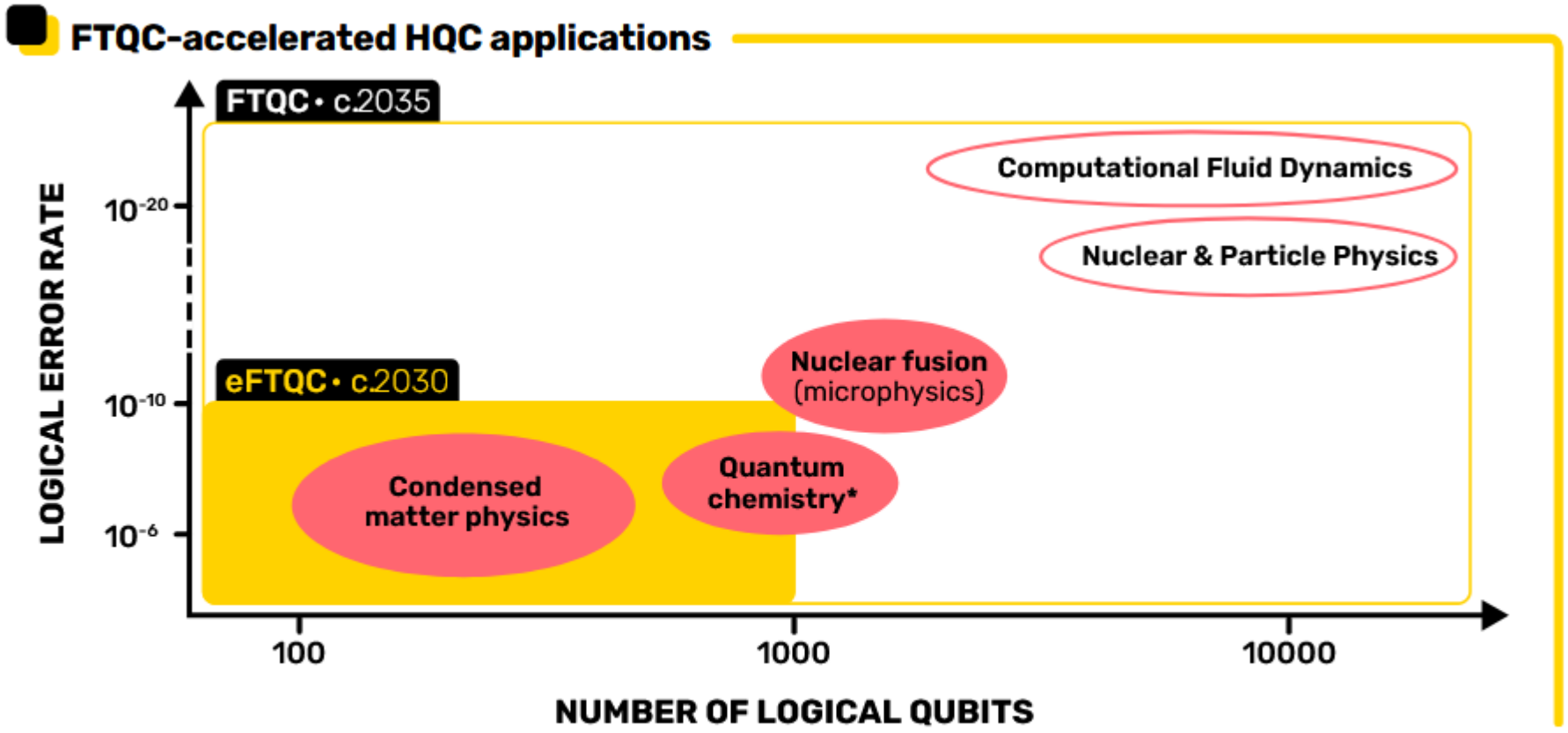
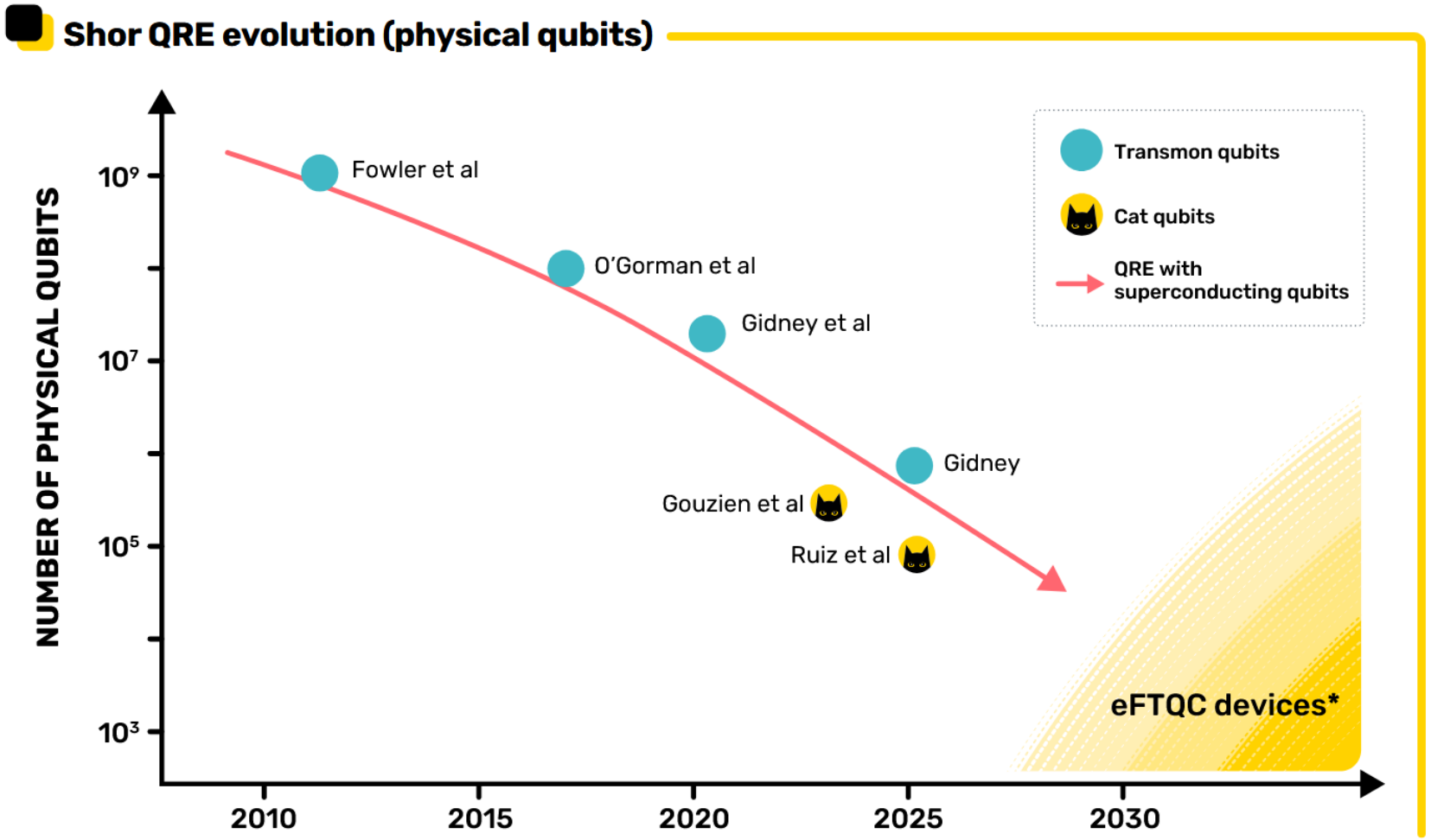


Figure 3 - FTQC acceleration roadmap: anticipated HPC application domains and timelines based on logical qubit counts and error rate thresholds. Timelines are based on quantum computing vendor roadmaps.

* Cryptanalysis using Shor's algorithm demands quantum hardware resources on par with those required for quantum chemistry workloads.

The quantum frontier is moving:
more HPC applications could enter the reach of eFTQC



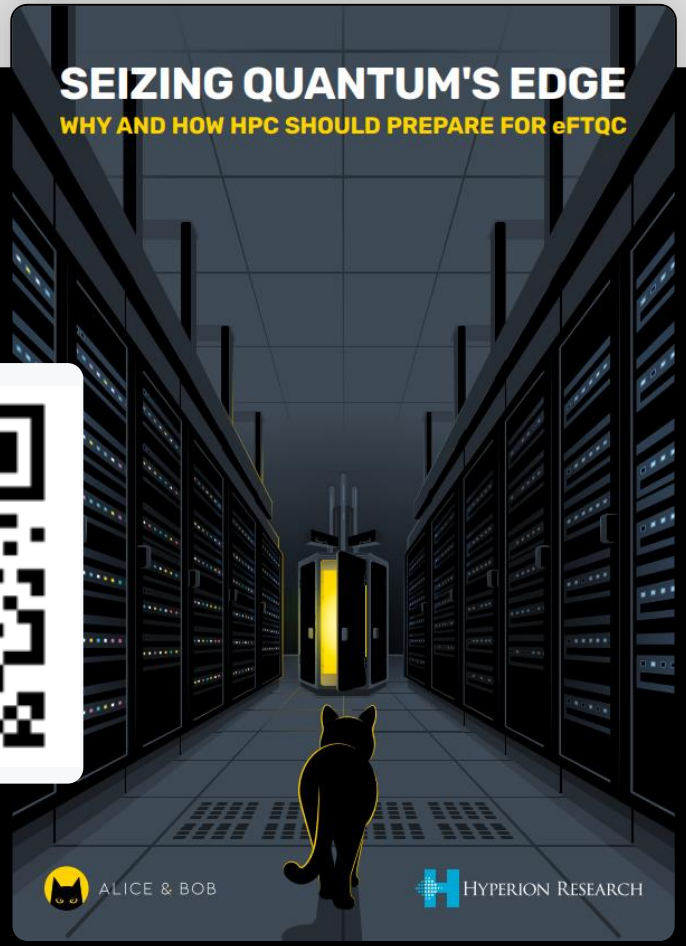
Resource estimations to break ECDSA with a n-bit key

Best known classical algorithms: **O(exp(n/2))**
Shor's algorithm: **O(n^3)**

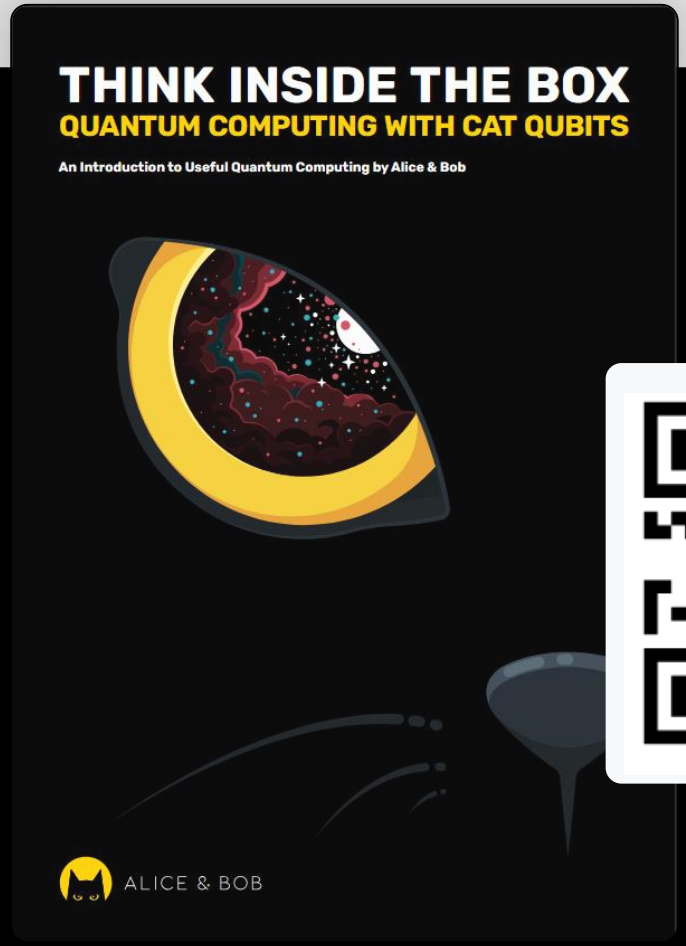
	Qubit type	Logical qubits	Physical qubits	Toffoli gates	Run time
Litinski 2023 (n=256)	Superconducting	6000	9.4 x 10^6	1.1 x 10^8	3.8 hours
Gouzien 2023 (n=256)	Cat qubits	2316	1.3 x 10^5	7.3 x 10^8	9 hours
Garn 2025 (n=233)	Photonic	3036	?	4.4 x 10^6	18 seconds to 4 minutes
Babbush 2026 (n=256)	Superconducting	1450	5 x 10^5	7.0 x 10^6	9 minutes

Litinski 2023: https://arxiv.org/abs/2306.08585
Gouzien 2023: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.131.040602
Garn 2025: https://ieeexplore.ieee.org/document/11072281
Babbush 2026: https://quantumai.google/static/site-assets/downloads/cryptocurrency-whitepaper.pdf

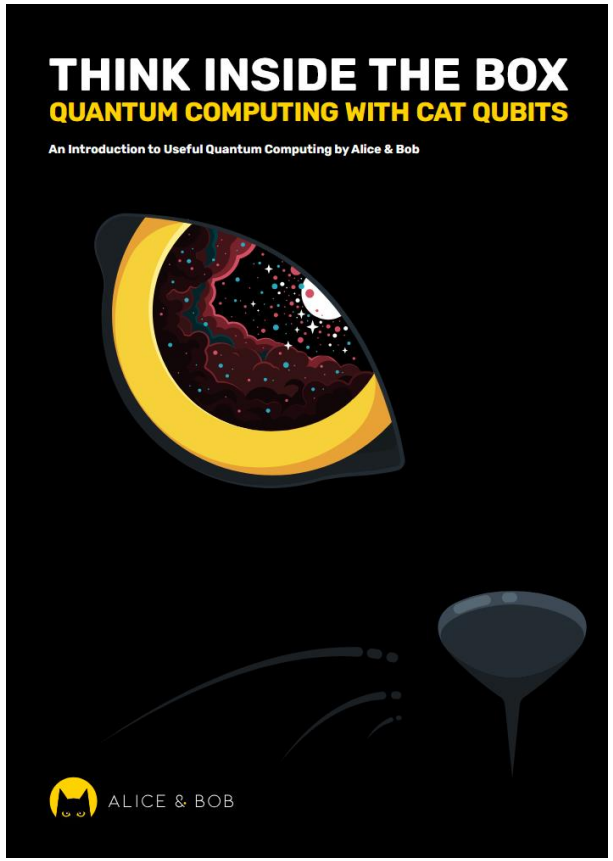
Our
Latest Report



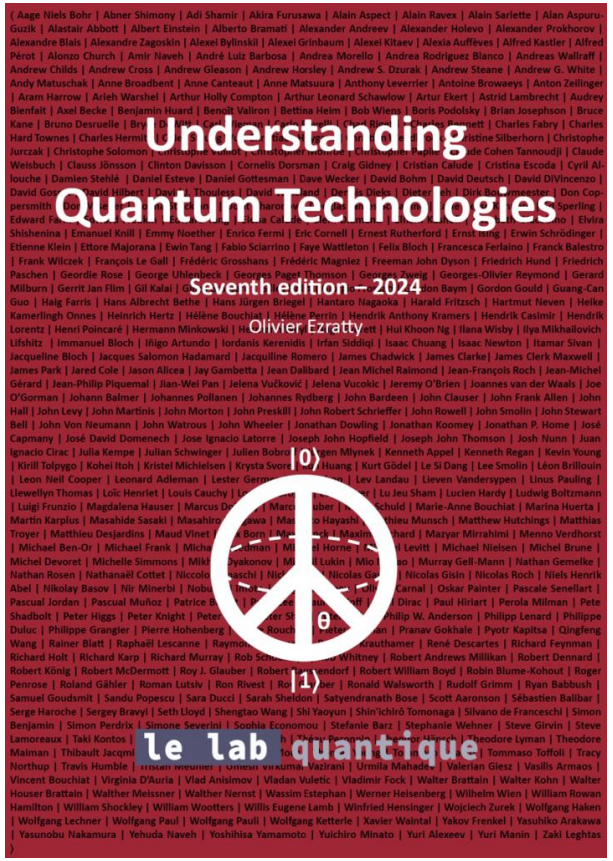
Our
Roadmap



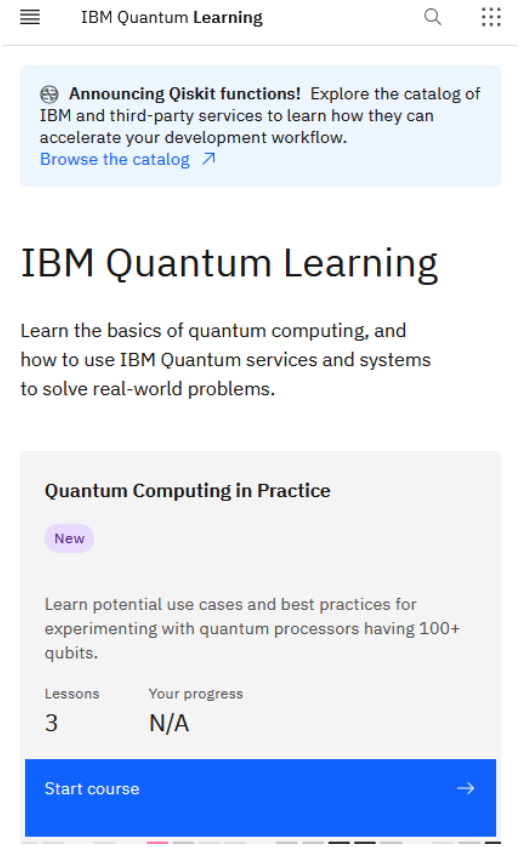
To learn more about quantum computing…



Alice & Bob's white paper



Olivier Ezratty
Understanding
Quantum Technologies



IBM Quantum Learning


Questions?