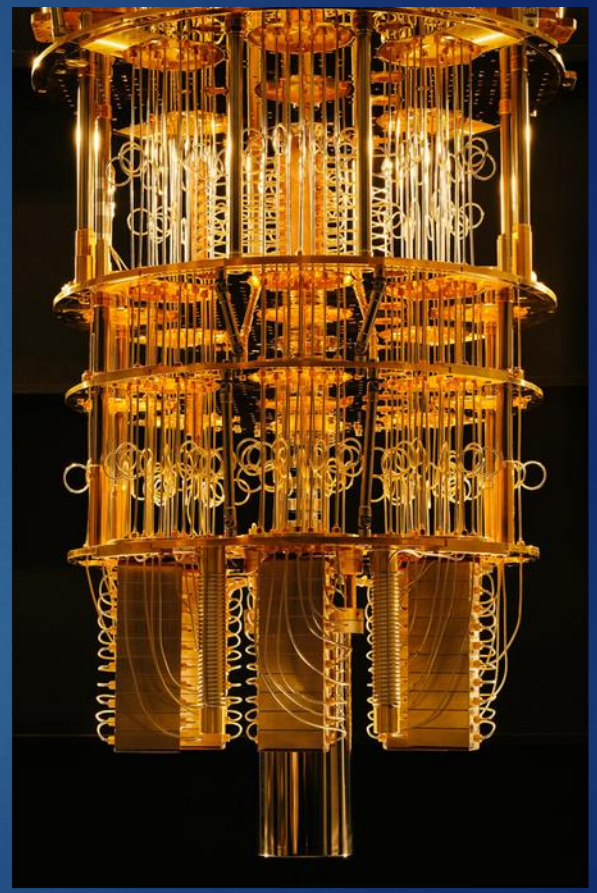
Introduction to Quantum Computing

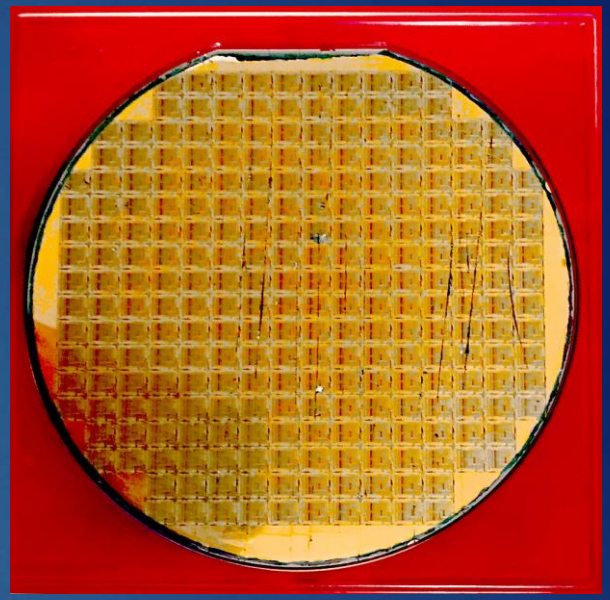
BY ALEX KHAN

2021



Topics

- History of Computing
  - What are classical computers made of?
  - Moore's Law (Is it ending?)
  - High Performance computing
- Quantum Computing
  - Quantum Computers
  - Quantum Advantage
  - The Qubit (Information in superposition)
  - Information storage
  - Different kinds of quantum computers
  - Superconducting vs Ion Traps
  - Annealing vs Universal/Gate quantum computers
  - Comparative history of classical and quantum computers
  - Roadmaps of quantum computing companies
  - Possible Future of quantum computers
  - Funding and revenue expectations
- Quantum Use-Cases
  - Quantum algorithms and their applications
  - Security and post-quantum cryptography
  - Molecule simulation
  - Financial portfolio optimization
- Challenges

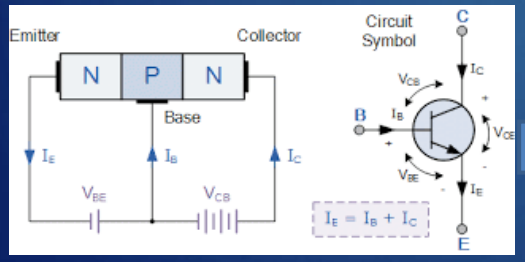


What are classical computers made of?

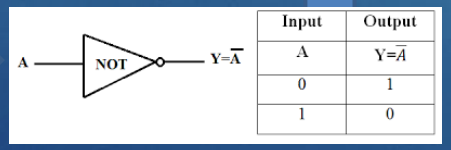
Model of first working transistor made in 1947

1. Transistor

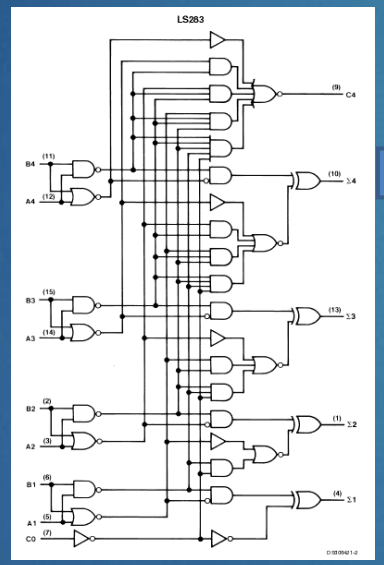
0 or 1



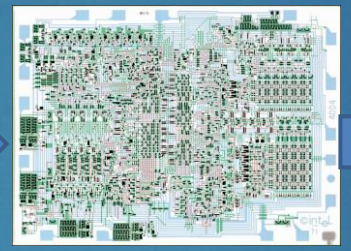
2. NOT Gate



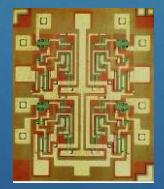
3. Adder Circuit



Intel 4040 chip in production in 1974

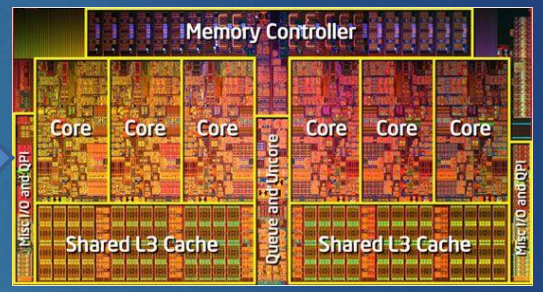


4. Full Circuit of the Intel 4040 Chip



4-input NAND gate

Intel Core i7 Chip

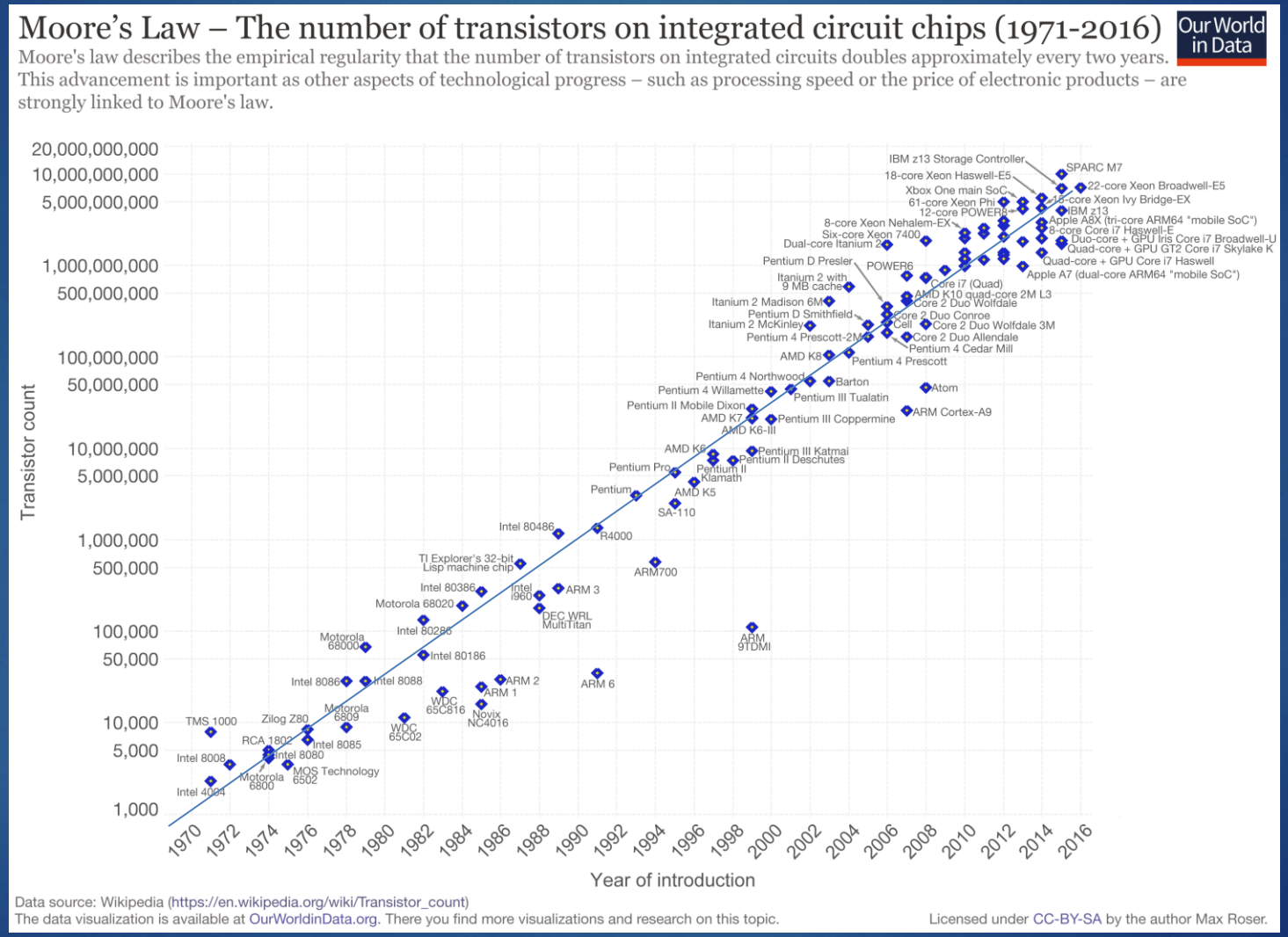


5. Circuit of the Intel Core i7

6. Motherboard

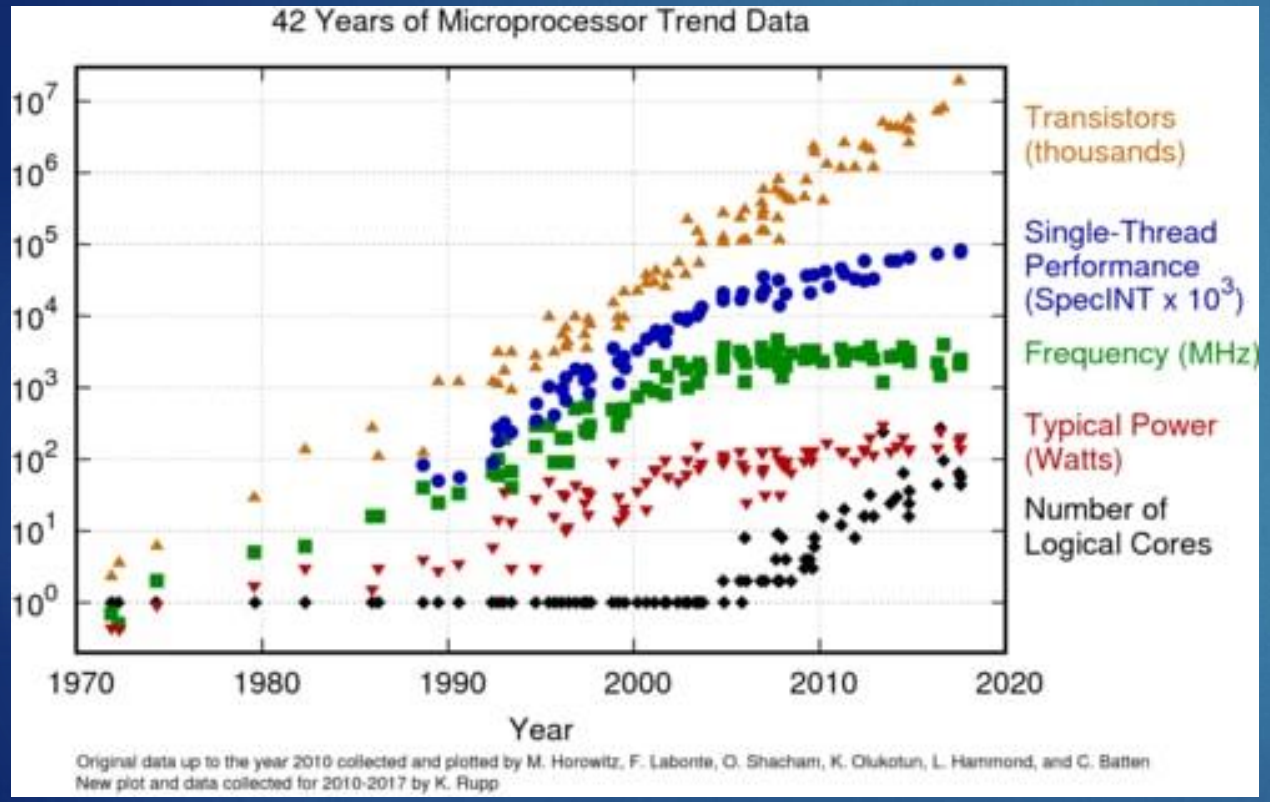
Image of Transistor: https://clintonwhitehouse4.archives.gov/Initiatives/Millennium/capsule/mayo.html NAND Gate: Dgarte - Own work, CC BY-SA 3.0

Moore's Law (Is it ending?)



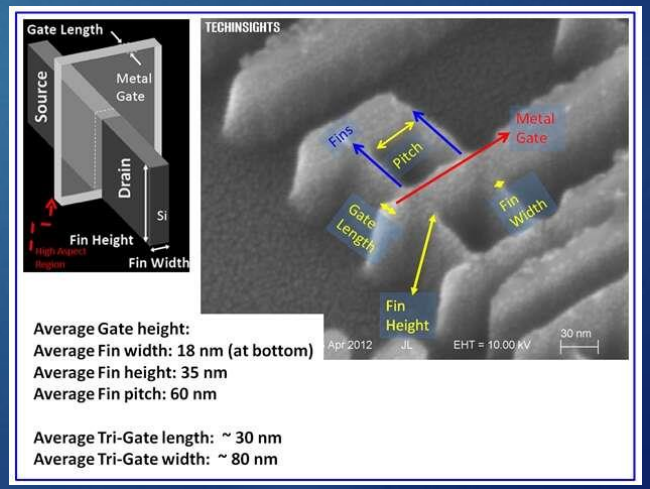
https://commons.wikimedia.org/wiki/File:Moore%27s_Law_Transistor_Count_1971-2016.png

High Performance Computing (HPC)



https://www.infoq.com/news/2020/04/Moores-law-55/

The Summit supercomputer at ORNL, designed by IBM and Nvidia.



https://www.itworldcanada.com/article/big-cat-swims-intel-details-tiger-lake-and-superfin-transistors/434460

Quantum Computing

"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

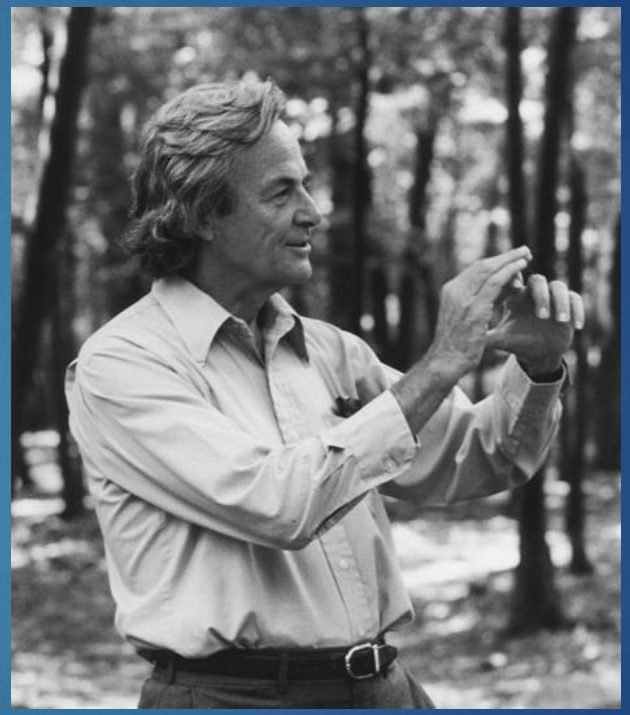


Photo of Richard Feynman, taken in 1984 in the woods of the Robert Treat Paine Estate in Waltham, MA, while he and the photographer worked at Thinking Machines Corporation on the design of the Connection Machine CM-1/CM-2 supercomputer.

Current Quantum Computers

IBM Quantum Computer

Rigetti Quantum Computer

IonQ Quantum Computer

Xanadu Quantum Computing

Google Quantum AI

Google Image Credit: Stephen Shankland/CNET

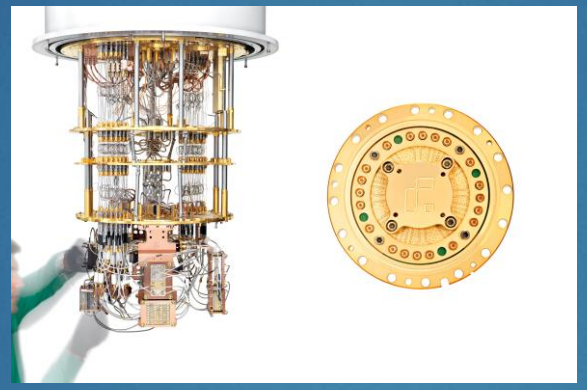
D-Wave Quantum Computer

Note: Images belong to their respective corporations

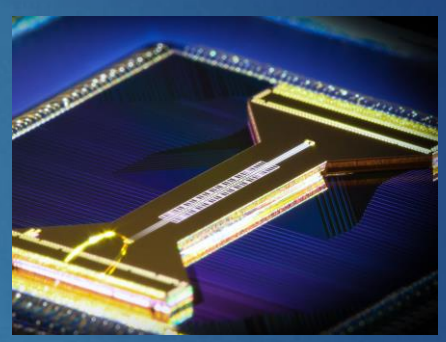
Inside Current Quantum Computers

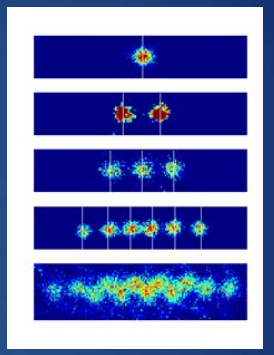
IBM Quantum Computer

Rigetti Quantum Computer

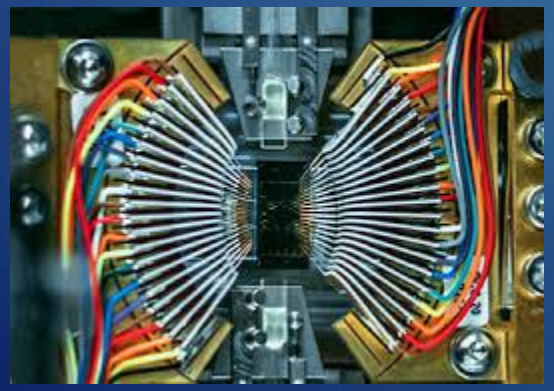


IonQ Quantum Computer





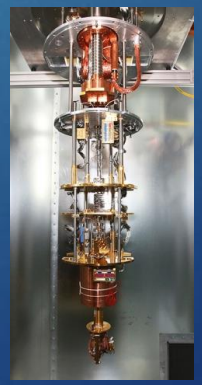
Xanadu Quantum Computing

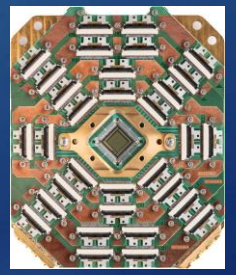


Google Quantum AI

Google Images Credit: Stephen Shankland/CNET

D-Wave Quantum Computer

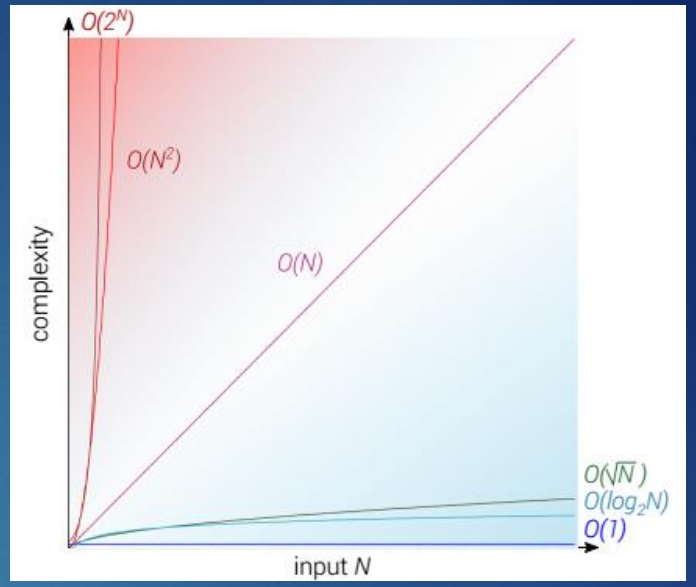


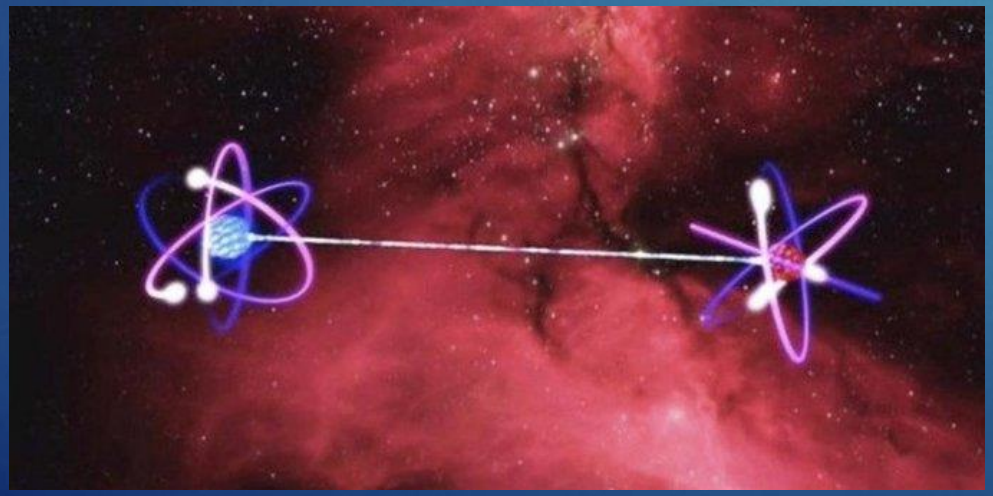


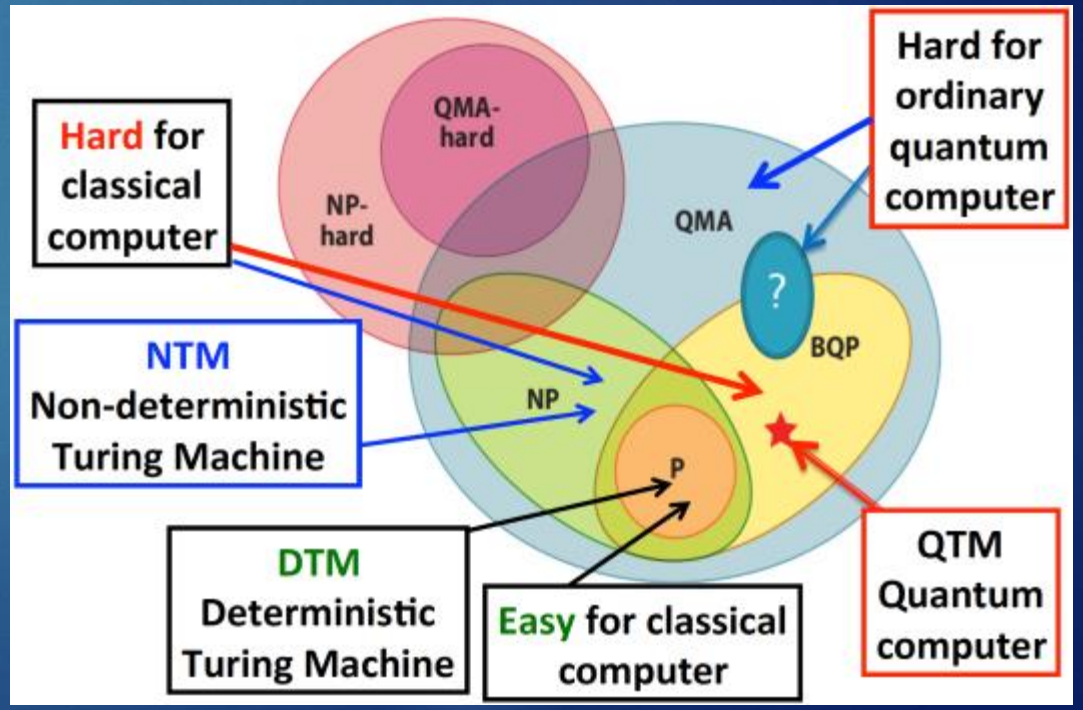
Note: Images below to their respective corporations

Quantum Advantage

- Polynomial and Exponential speedup
- Theoretically can solve some NP problems, and other harder problems.
- D-Wave and Google Quantum Supremacy examples
- Superposition, Parallelism, Entanglement, Hilbert space



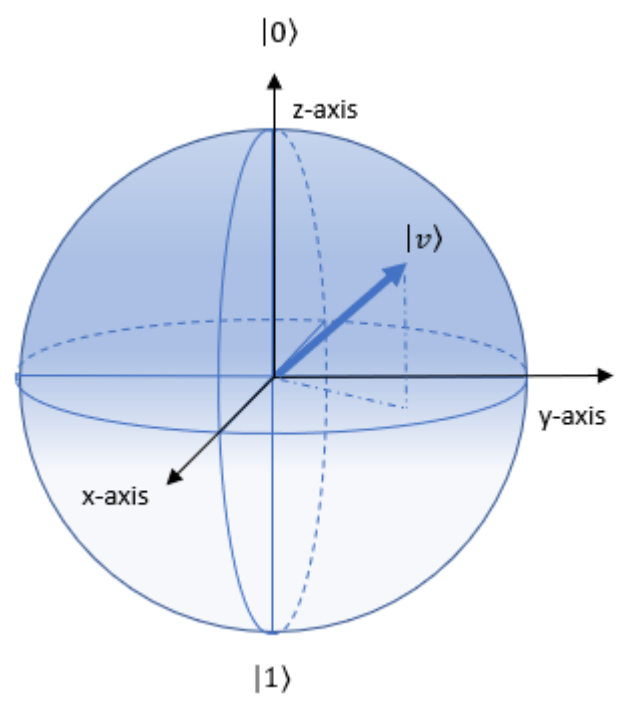




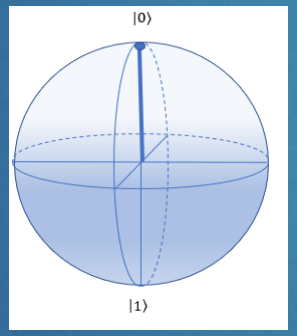
https://www.groundai.com/project/quantum-information-processing-with-superconducting-circuits-a-review/2

The Qubit (Information in Superposition)

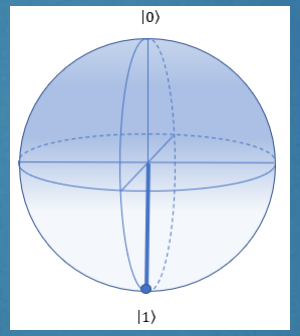
Somewhere from 0 to 1



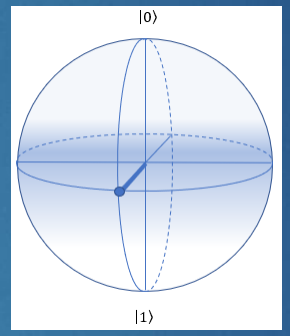
100% 0



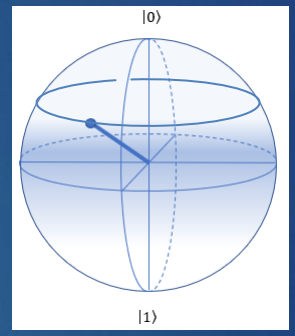
100% 1



50% 0



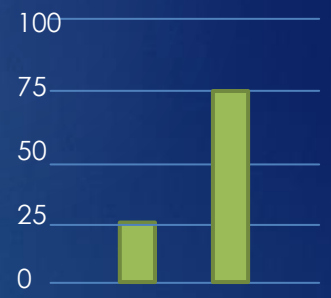
50% 1



~75% 0

~25% 1

Result of measuring 100 times



1 0

$|\rangle$ is a way of representing a quantum state. States on the sphere are pure states, while inside are mixed states or decohered states.

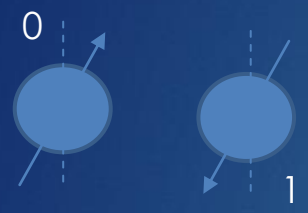
Information Storage (Classical vs Quantum)

Register size (n)	Classical register of n bits. Can only store *one* value at a time.	Quantum register of n high quality qubits in superposition. Can store the individual probability amplitudes of *all* possible values at any given time.
1	1 (eg, 0 or 1)	2 (p0 and p1) (biased coin)
2	1 (00, 01, 10 or 11)	4 (p00, p01, p10 and p11) (4 sided biased dice)
3	1 (000, 001, 010, …… or 111)	8 (p000, p001, p010, … and p111) (8 sided dice)
16	1 out of possible 65,536 values	All 65,536 probability values
32	1 …	4,294,967,296 (> base pairs in human genome)
45	1…	$3.5x10^{13}$ (> number of cells in a human body)
64	1…	$1.8x10^{19}$ (> number of grains of sand on Earth)
100	1…	$1.2x10^{30}$ (number of bacteria on Earth)
167	1…	$1.8x10^{50}$ (> the number atoms on Earth)

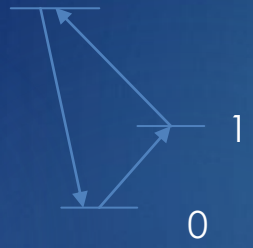
p is the probability of that number

Different Kinds of Quantum Computers

Electron Spins

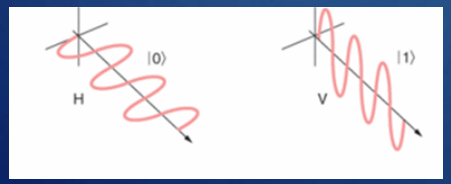


Molecule Energy Levels



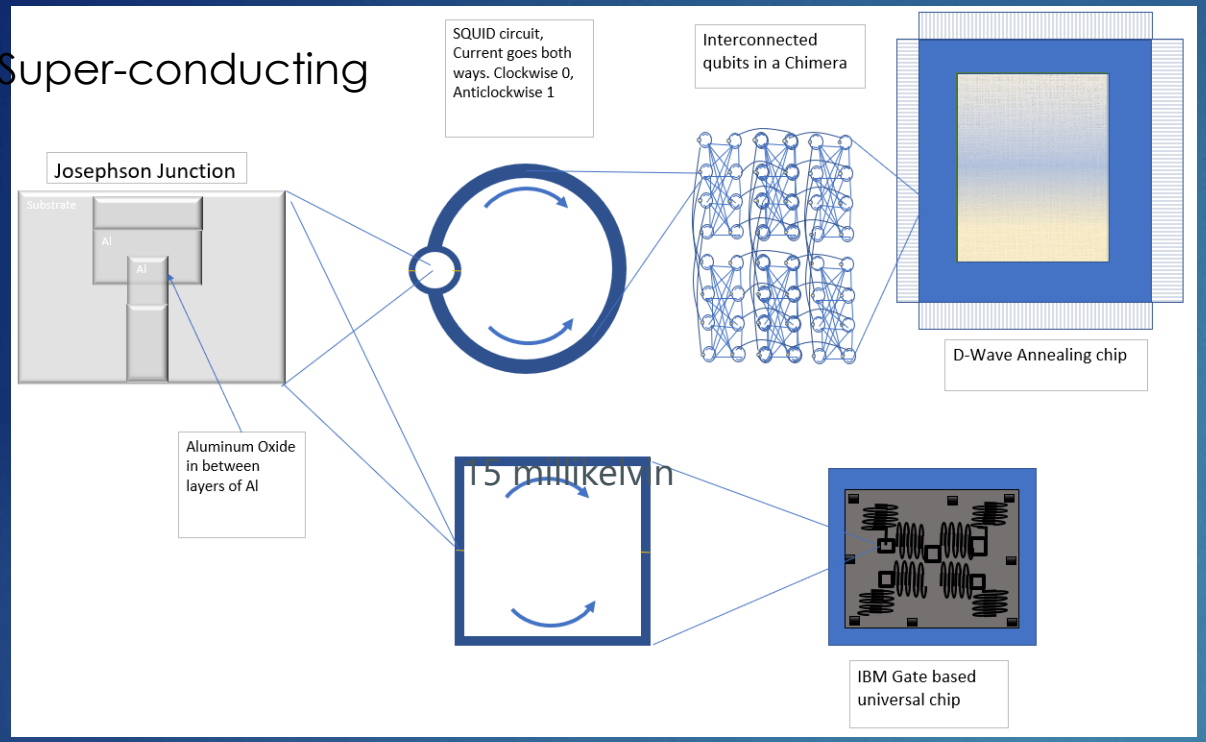
Superconducting Circuits

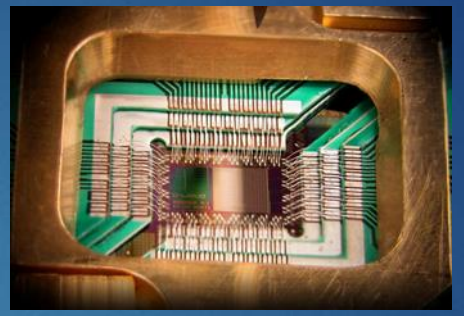
Photons



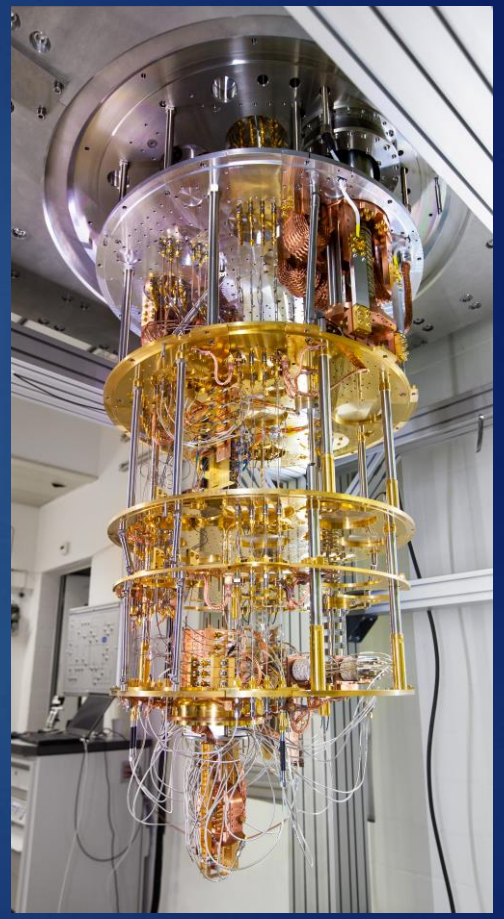
Type	Companies/Universities	Gate/ Annealing
Superconducting	Google IBM Q Rigetti Systems	Gate
Superconducting	D-Wave (Canada)	Annealing
Trapped Ions (Electron energy levels)	IonQ (U of Maryland/Duke) Honeywell (Microsoft/Honeywell)	Gate
Photonics	Xanadu	Gate
Simulators (Emulators)	Many including IBM, Google, Microsoft, ATOS, …	B
Si Si/Ge (undoped quantum Dots)	Johannes Kepler University	?
Doped Si	U of Melbourne and Keio U.	?
Nitrogen Vacancy center in Diamond (Energy Levels)	QuTech/TUDelft (Netherlands)	?
Neutral Atom	Anderson Group/University of Colorado	?
Nuclear Magnetic Resonance	Stanford and other labs	?
Silicon Semiconductor Electron Spin	Intel (Intel/QuTech/TuDelft)	

Superconducting vs Ion Traps

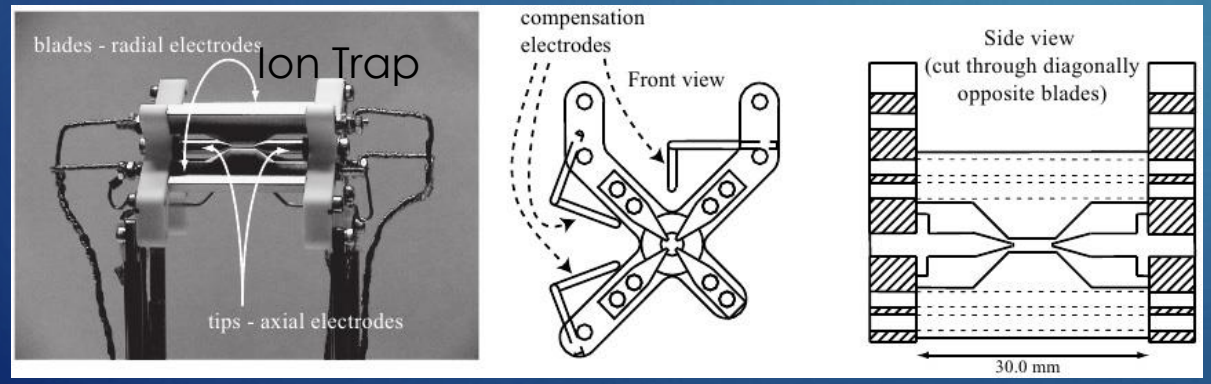


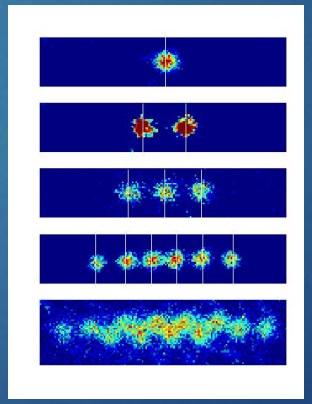


D-Wave 128 Qubit Processor



IBM Quantum Computer





12 ions squeezed into an Ion Trap

A quantum information processor with trapped ions, New J. Phys. 15 123012 (2013). DOI: https://doi.org/10.1088/1367-2630/15/12/123012 Figure 5

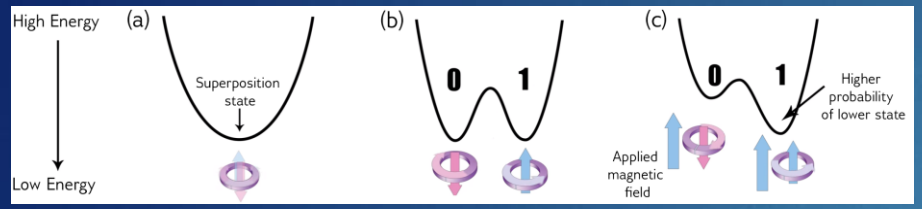
National Institute of Standards and Technology - Planar Ion Trap; Magnesium Ions

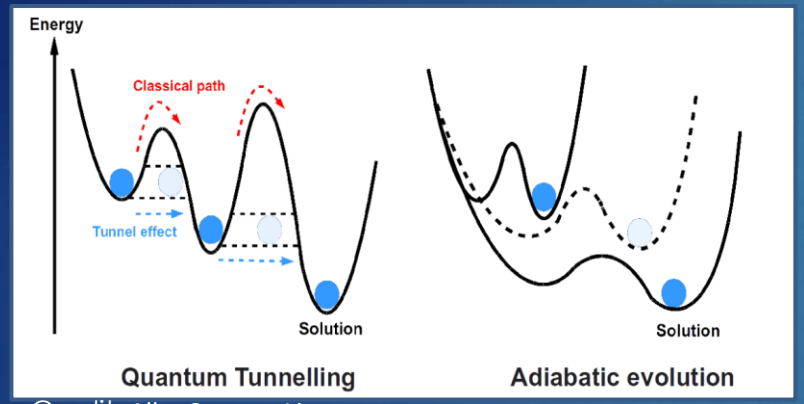
IBM Zurich Lab Quantum Computer

Photograph of a chip constructed by D-Wave Systems Inc., designed to operate as a 128-qubit superconducting adiabatic quantum optimization processor, mounted in a sample holder. D-Wave Systems, Inc. - D-Wave Systems, Inc.

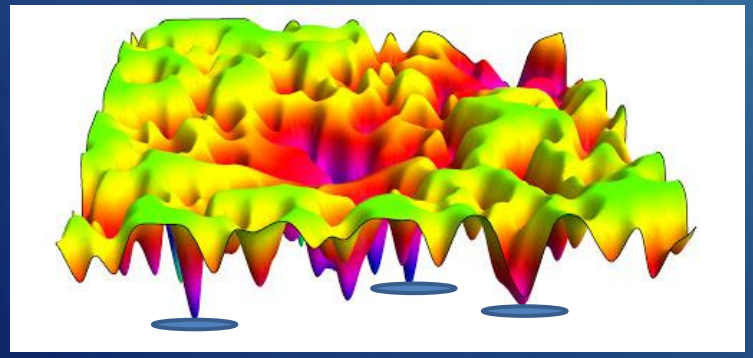
Annealing vs Gate Quantum Computing

Energy Landscape, minimization



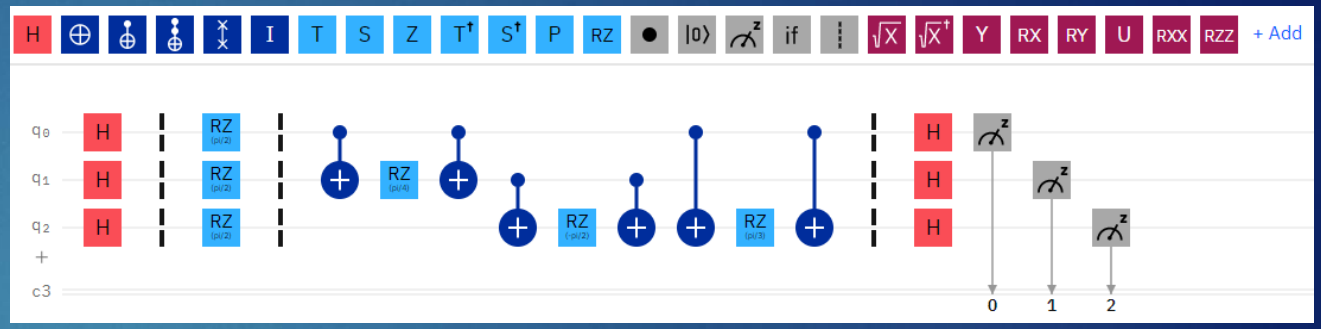


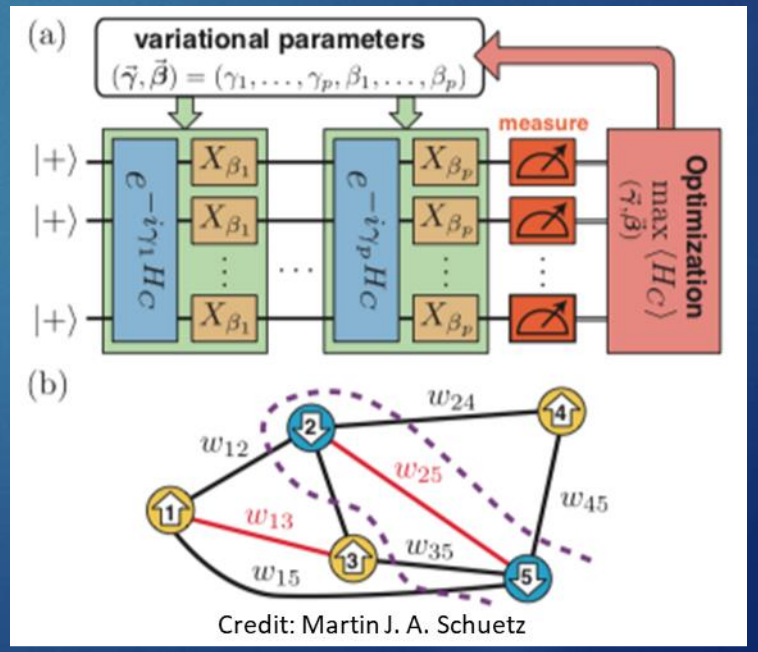
Credit: Alba Cervera-Lierta



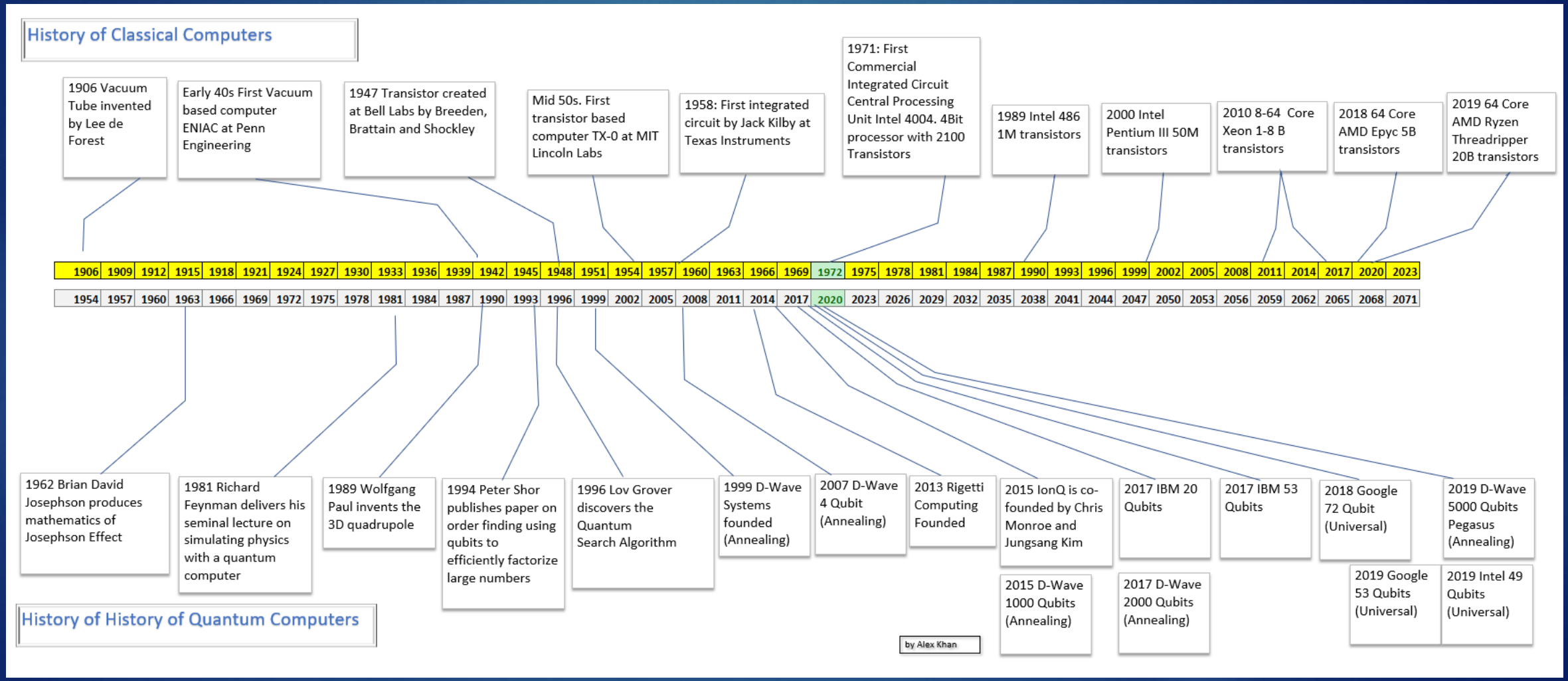
https://medium.com/@quantum_wa/quantum-annealing-cdb129e96601

Universal/Gate computers

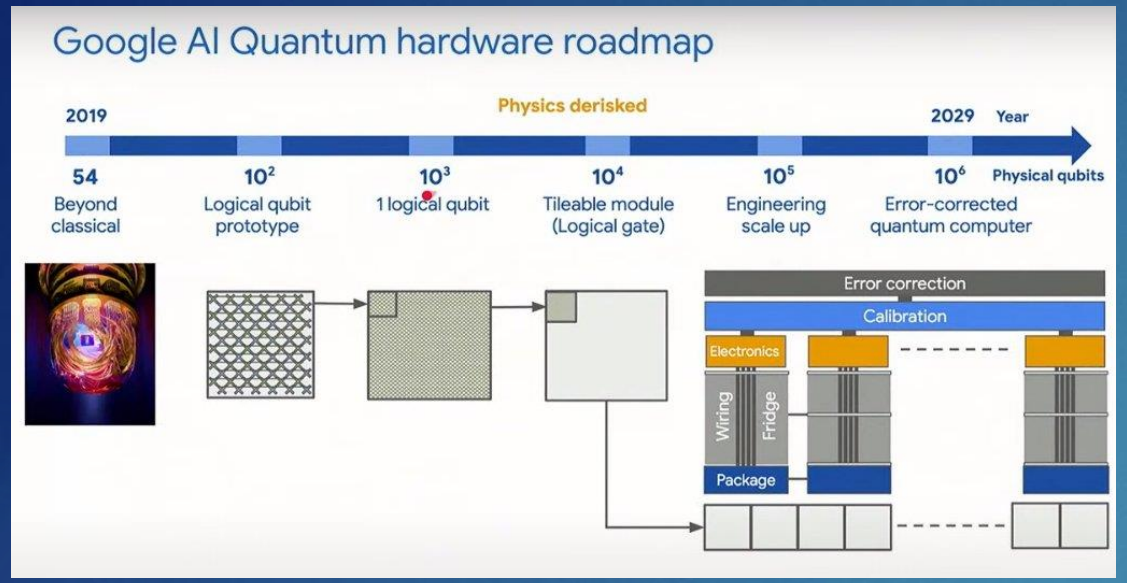


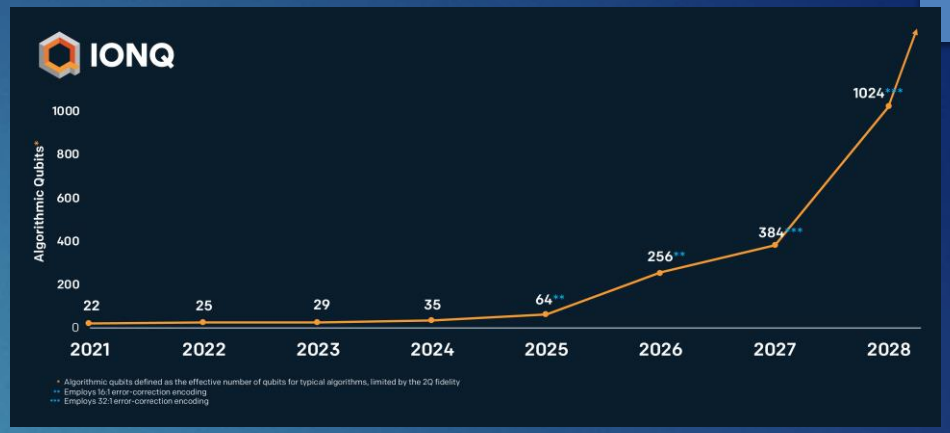


Comparative History of Classical and Quantum Computers



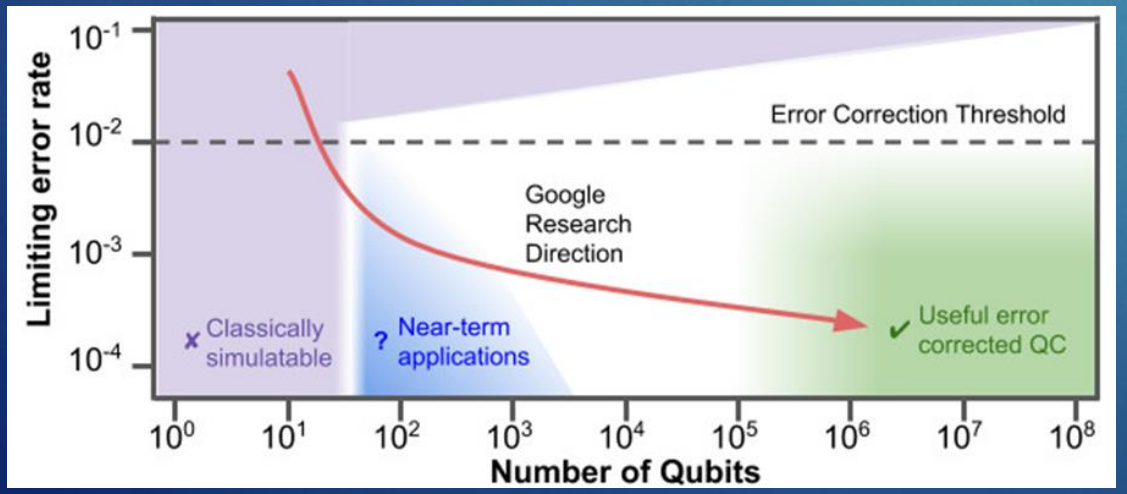
Roadmaps of Quantum Computing Companies



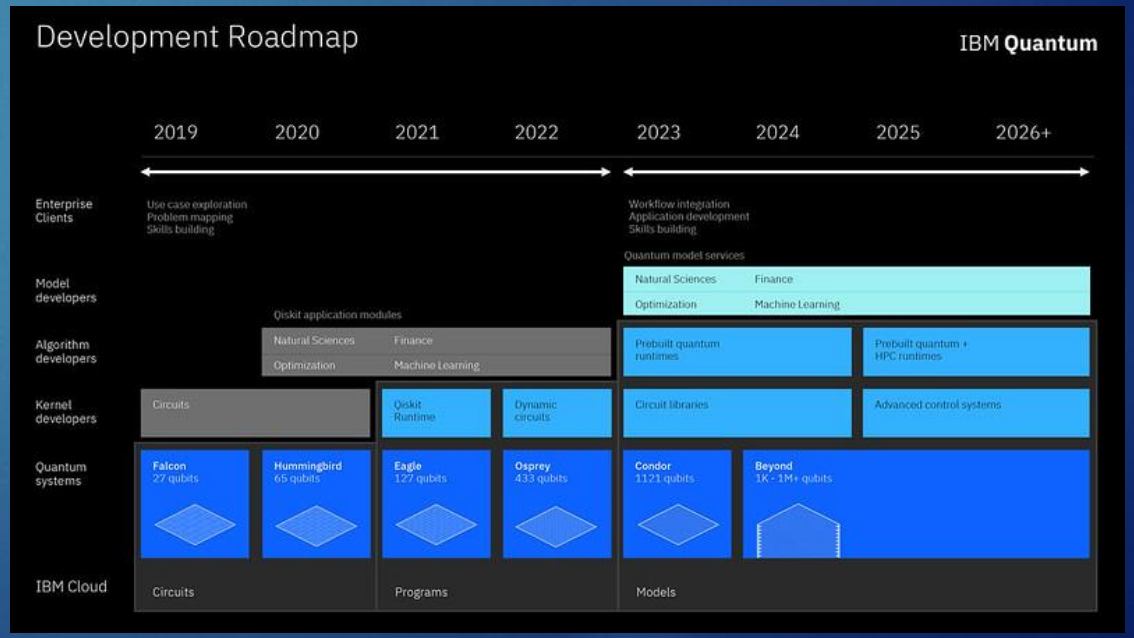


Credit: IonQ

https://ionq.com/posts/december-09-2020-scaling-quantum-computer-roadmap

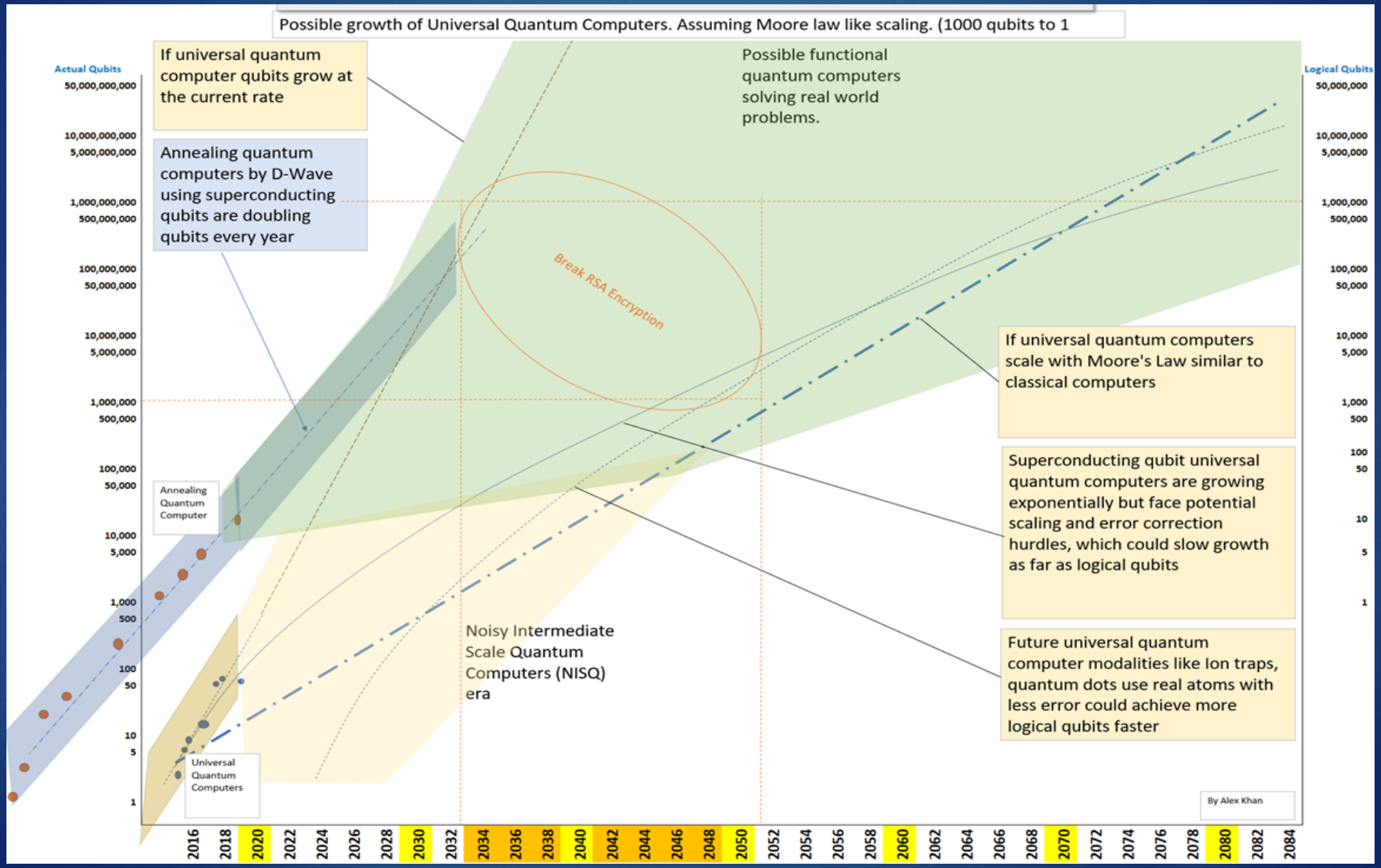


Credit: Google

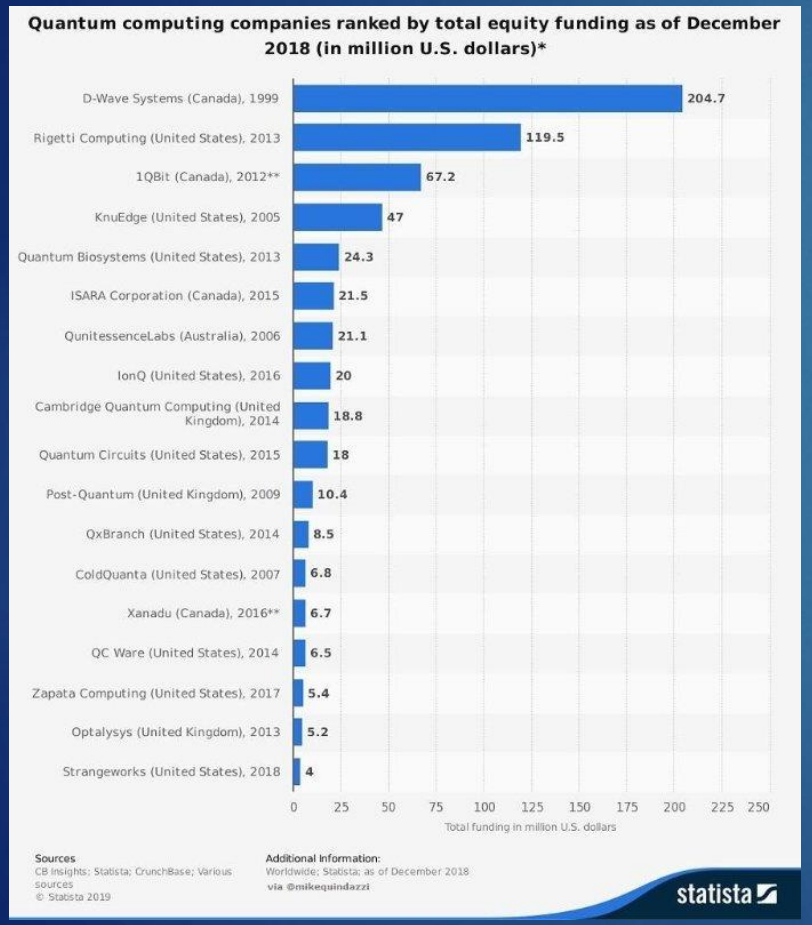


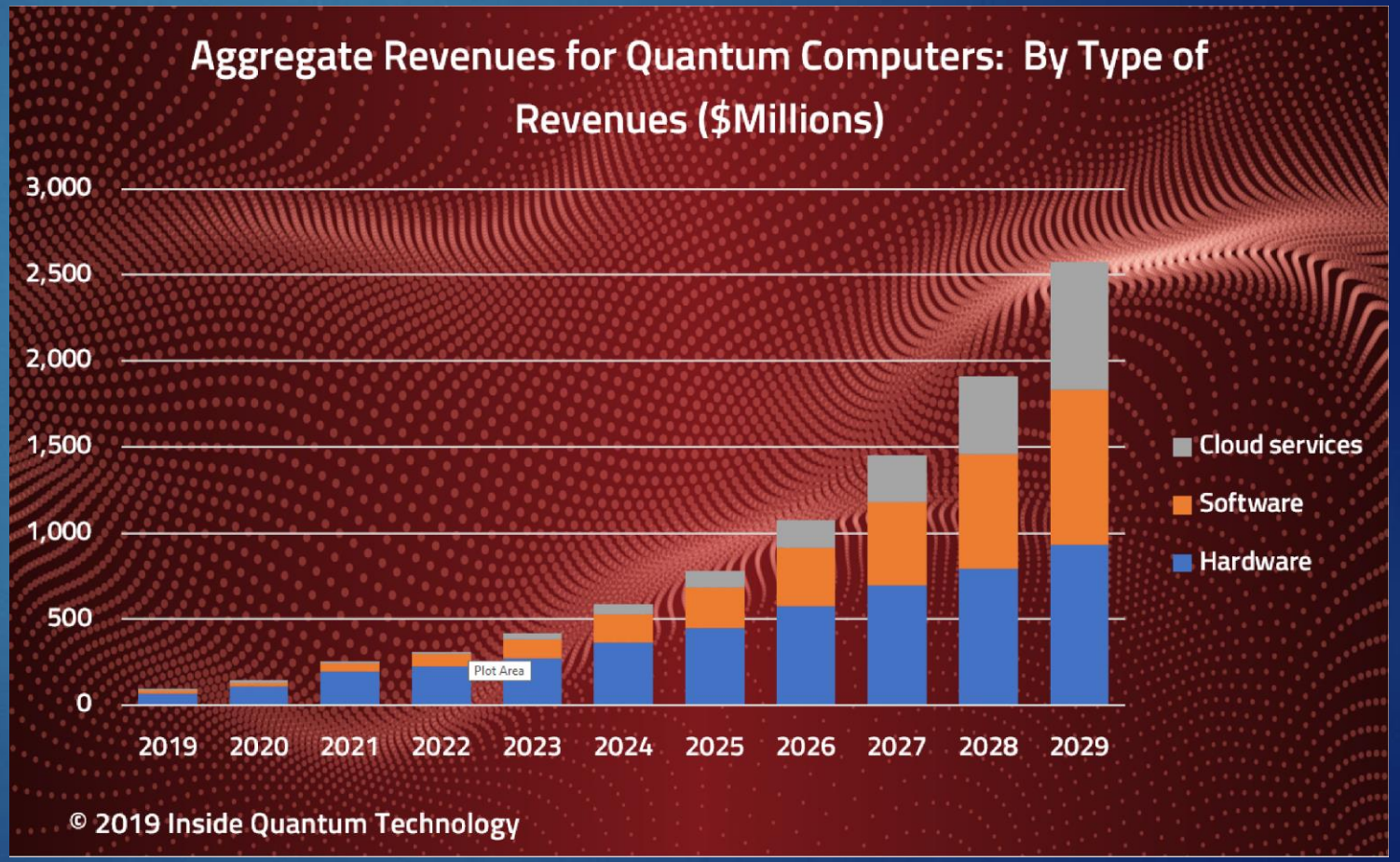
https://www.ibm.com/blogs/research/2021/02/quantum-development-roadmap/

Possible Future of Quantum Computers



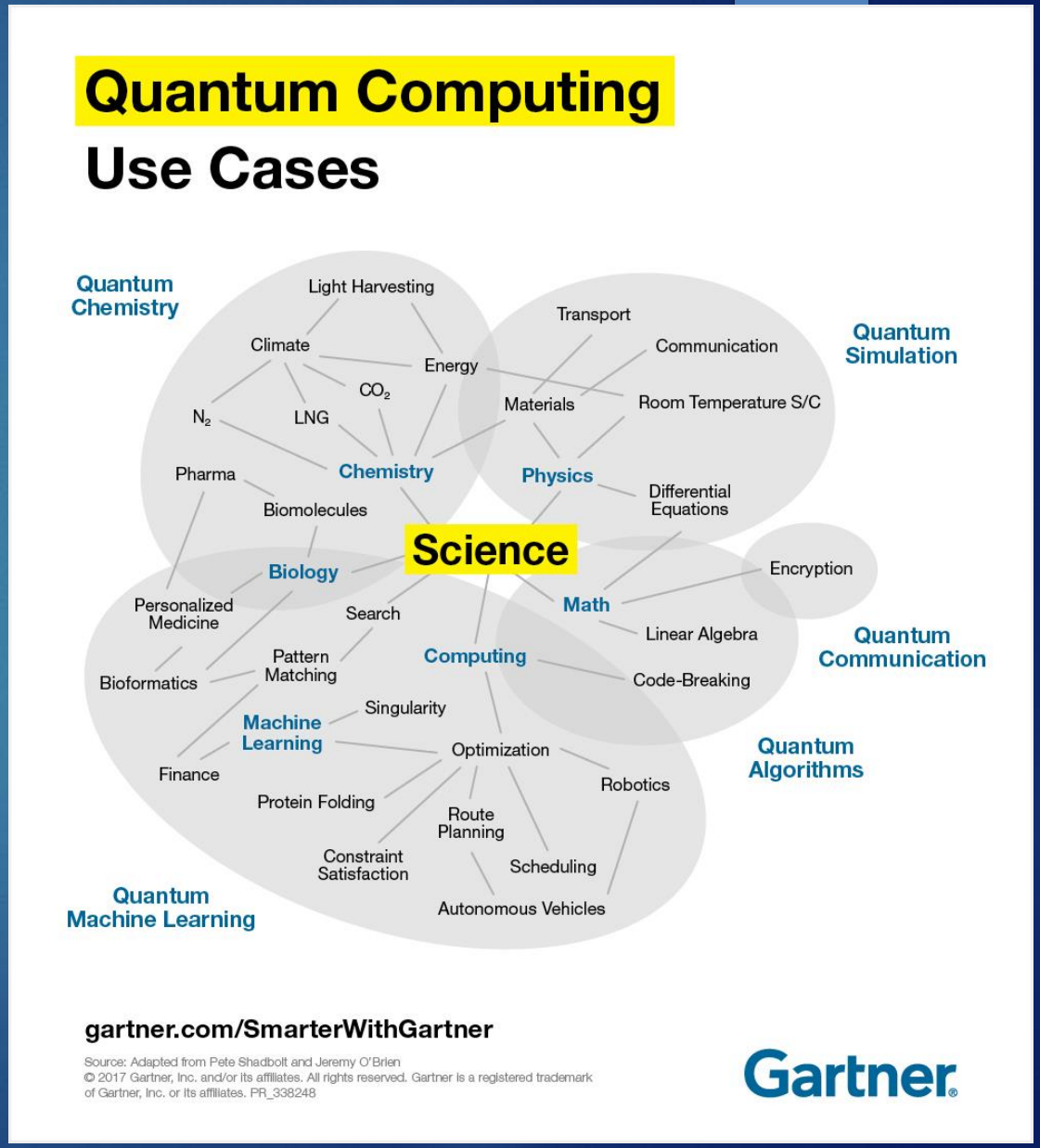
Funding for Quantum Computing





Quantum Computing Use-Cases

- Optimization using annealing or universal quantum computers
  - Financial stock portfolio, fixed asset optimization, traffic, medical, etc.
- Quantum cryptography, quantum Network and communication
- Quantum Machine Learning (and using ML to aid in error correction)
- Sensors and quantum devices (atomic clocks)
- Quantum chemistry and molecule simulation (new medicines)
- Quantum Random Number Generation (QRNG)
- More being discovered each day

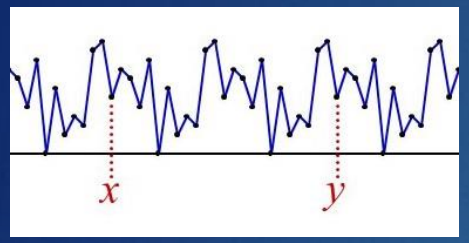


Quantum Algorithms and their Applications

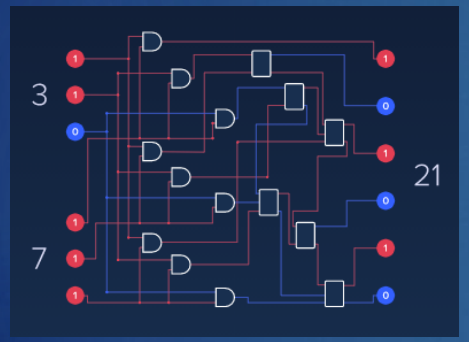
Quantum Algorithm	Uses
Grover's	Search and has quantum advantage
Shor's	Period finding with quantum speedup (this is used to find factors and thus breaks RSA encryption)
Quantum Annealing	Find solutions (minimum, maximum) of optimization problems. Quantum Speedup not proven, though demonstrated.
Harrow, Hassidim and Lloyd (HHL)	Find solutions to a linear set of equations
Quantum Approximate Optimization Algorithm (QAOA)	To help speedup finding solution to combinatorial problems
Variational Quantum Eigensolver (VQE)	Speed up the process of finding the minimum energy states of molecules
Quadratic Unconstrained Binary Optimization (QUBO)	Finding energy minimum of optimization problems.

Security and Post Quantum Cryptography

Shor's – Period finding – gate QC



Reverse Multiplication - Annealing



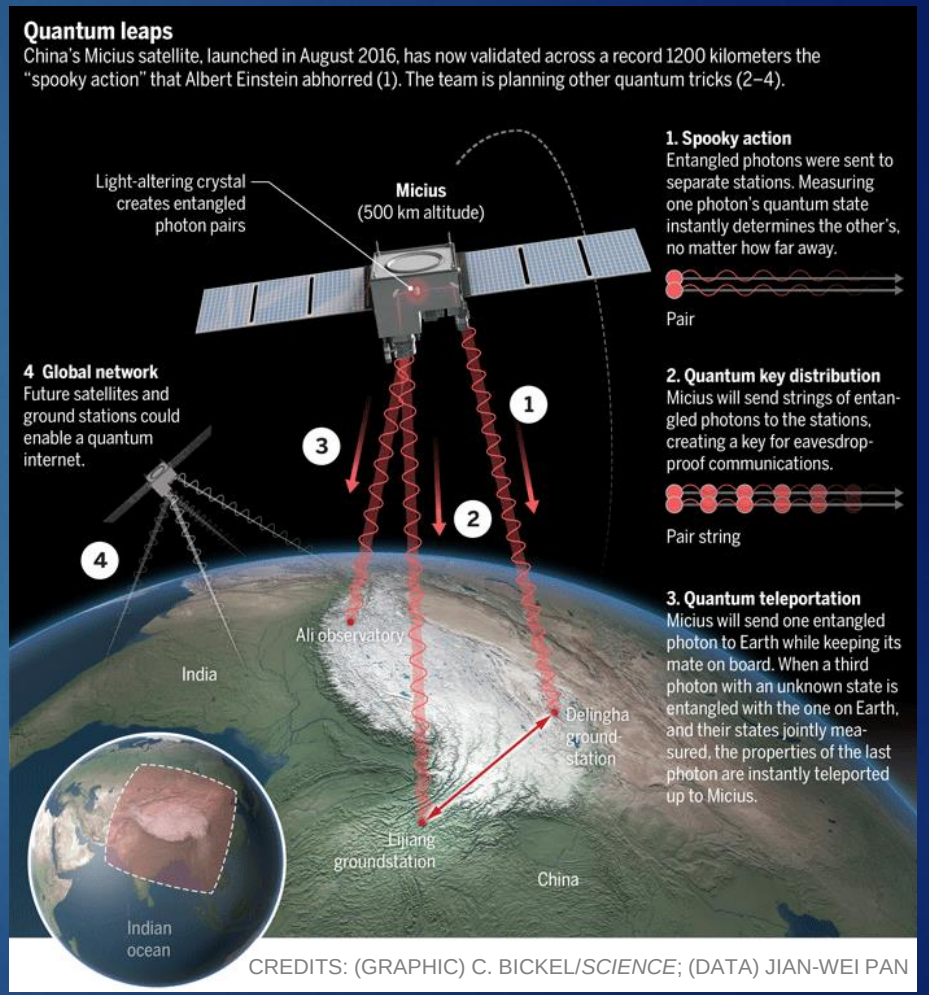
Grover Search, Siev and others

Impact of QC on Common Crypto Algorithms. From NISTIR 8105: Report on Post-Quantum Cryptography, 2016.

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Post Quantum Cryptography

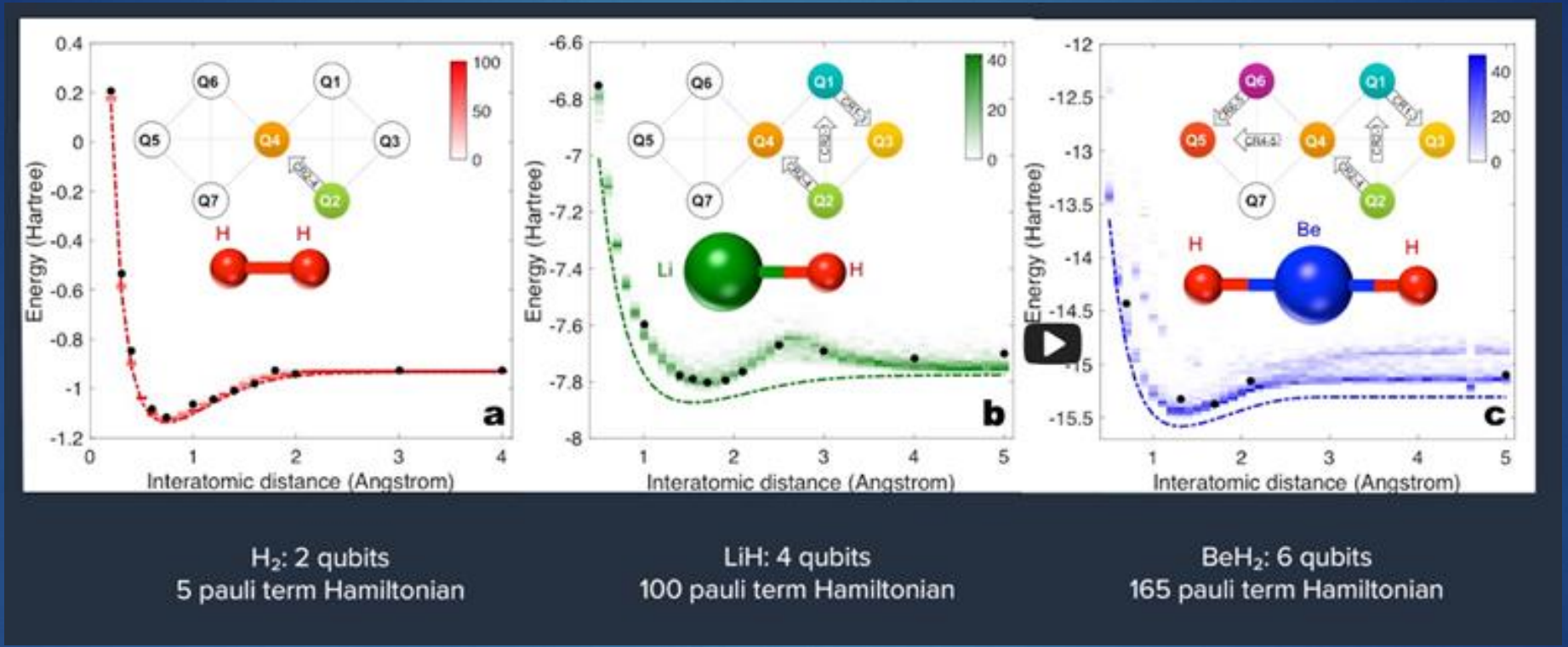
BB84, E92 using entangle qubits



https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

https://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance

Molecule Simulation – Gate (VQE)



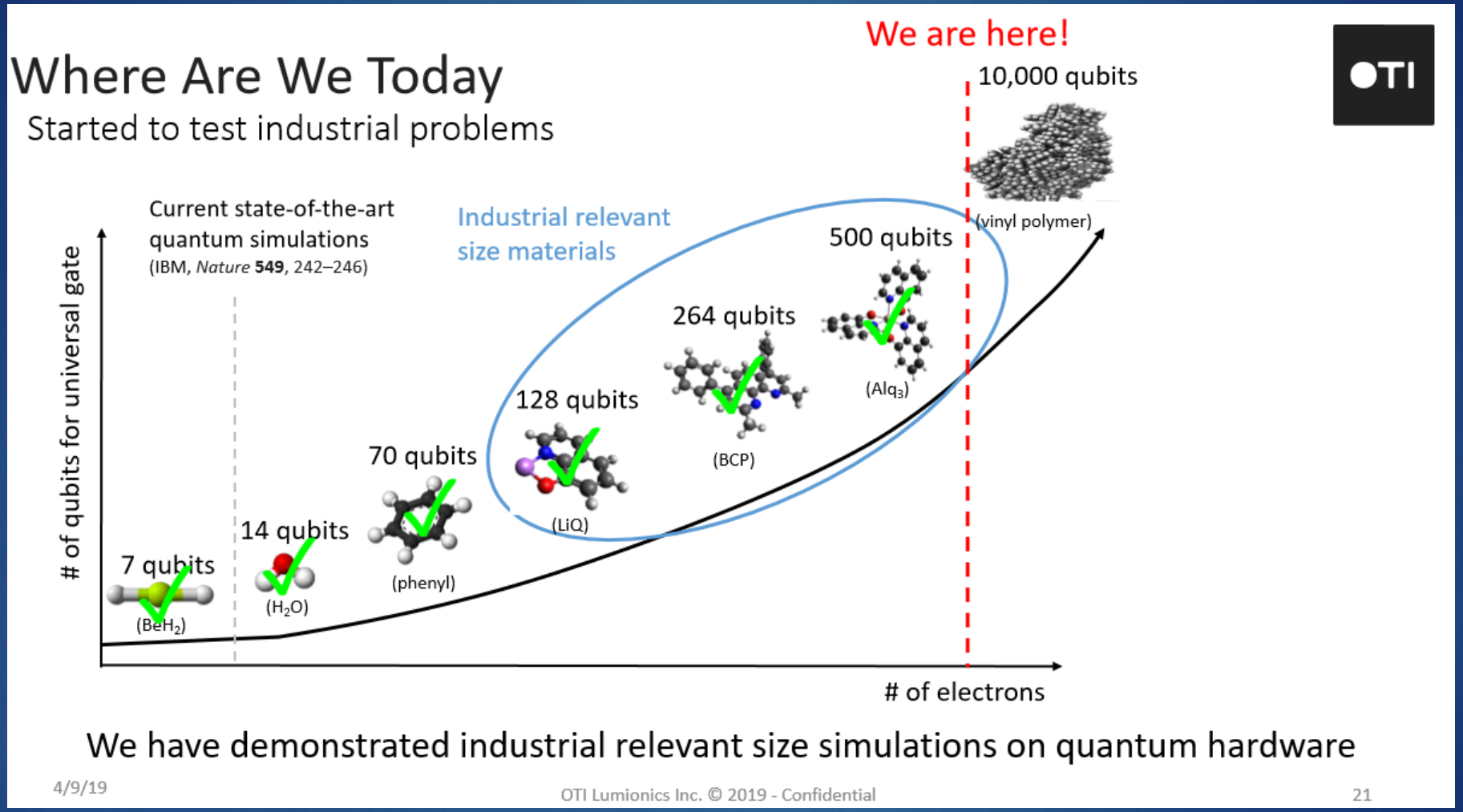
H_2: 2 qubits
5 pauli term Hamiltonian

LiH: 4 qubits
100 pauli term Hamiltonian

BeH_2: 6 qubits
165 pauli term Hamiltonian

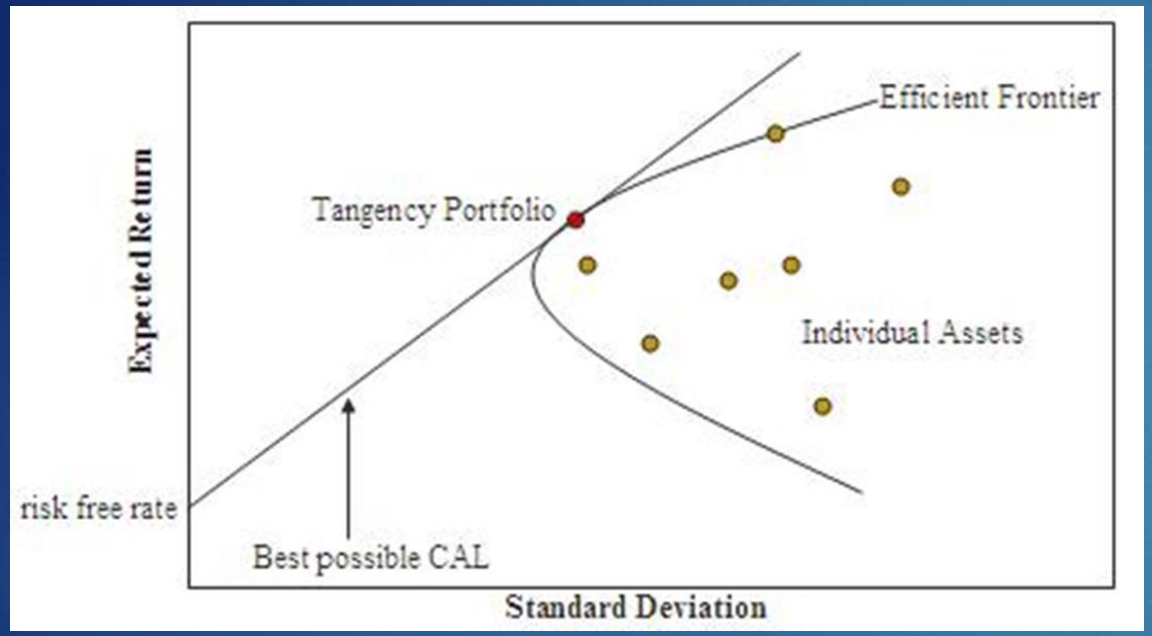
https://arxiv.org/abs/1704.05018

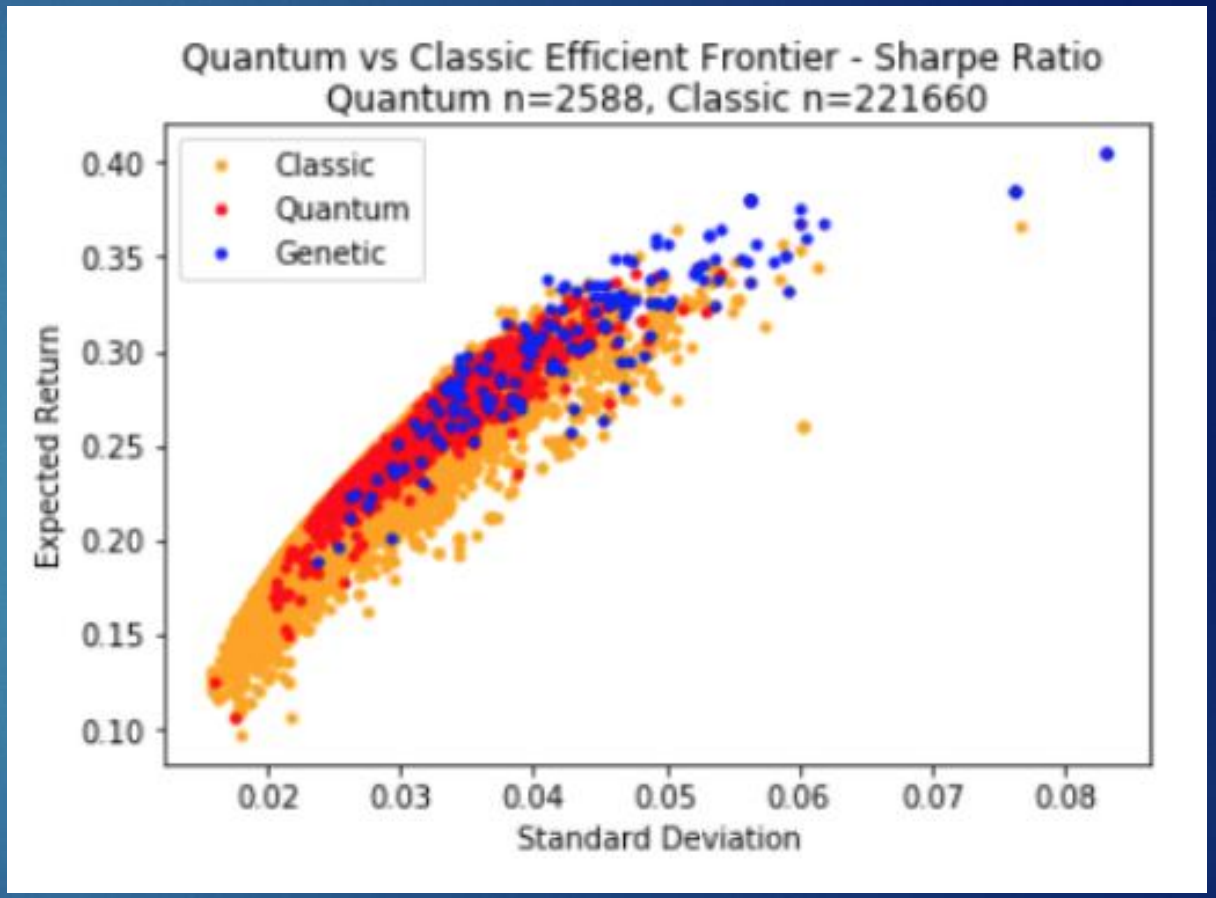
Molecule Simulation - Annealing



https://www.dwavesys.com/sites/default/files/34_Thurs_AM_OTI.pdf

Portfolio Optimization - Annealing





https://www.researchgate.net/publication/343786420_Portfolio_Optimization_of_60_Stocks_Using_Classical_and_Quantum_Algorithms

Some of the challenges

- Low number of qubits
- Isolating qubits and reducing noise from the environment
- Errors in maintaining quantum state and controlling qubit rotations
- No-cloning
- Low number of gates before decoherence
- Data loading problem
- Scaling the systems and adding RAM
- Measurement destroys the quantum state
- Requires multiple shots (measurements) to get probabilistic answer
- Most do not have fully connected qubits (Ion Traps are exception)
- Considerable technical, engineering, and scientific research needed
- Software and use-cases still need to be developed
- Information cannot go faster than light (limitation on entanglement)

Questions