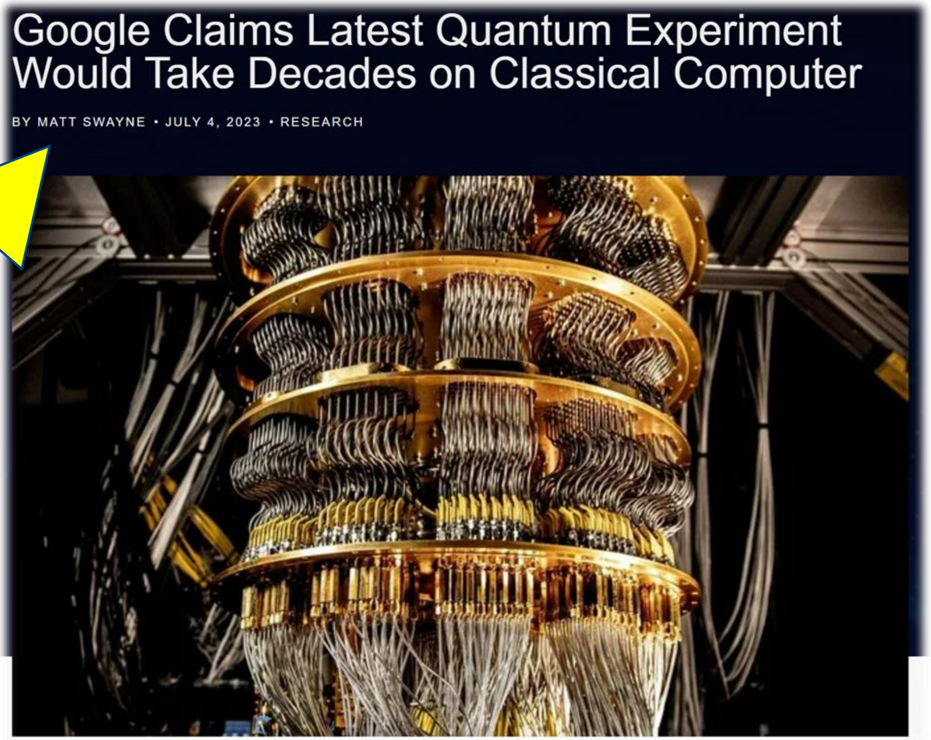
CONTEXT


Google Claims Latest Quantum Experiment Would Take Decades on Classical Computer

BY MATT SWAYNE • JULY 4, 2023 • RESEARCH

- Google scientists are reporting in a new study that **it completed a computational task on a quantum computer that would take a classical supercomputer 47 years to complete**.

- The task was a random circuit sampling calculation.

- The experiment was carried out in the latest version of [Google's Quantum] Sycamore processor that has been boosted to 70 qubits [from 53 qubits].

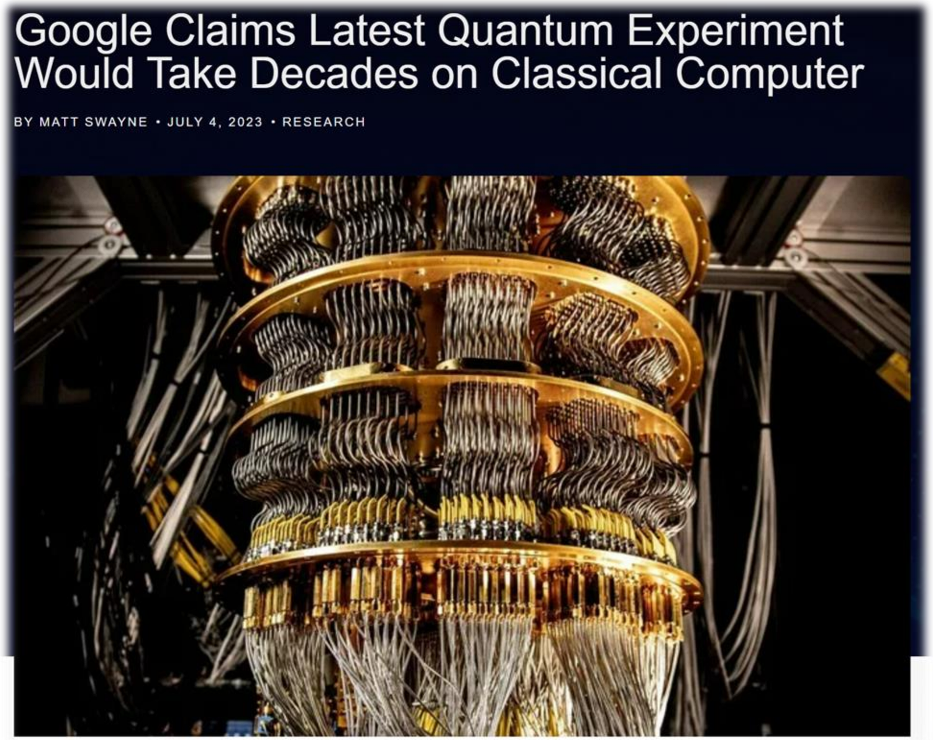
Link: (Quantum Insider)
Source (PDF): arXiv:2304.11119v1 [quant-ph] 21 Apr 2023

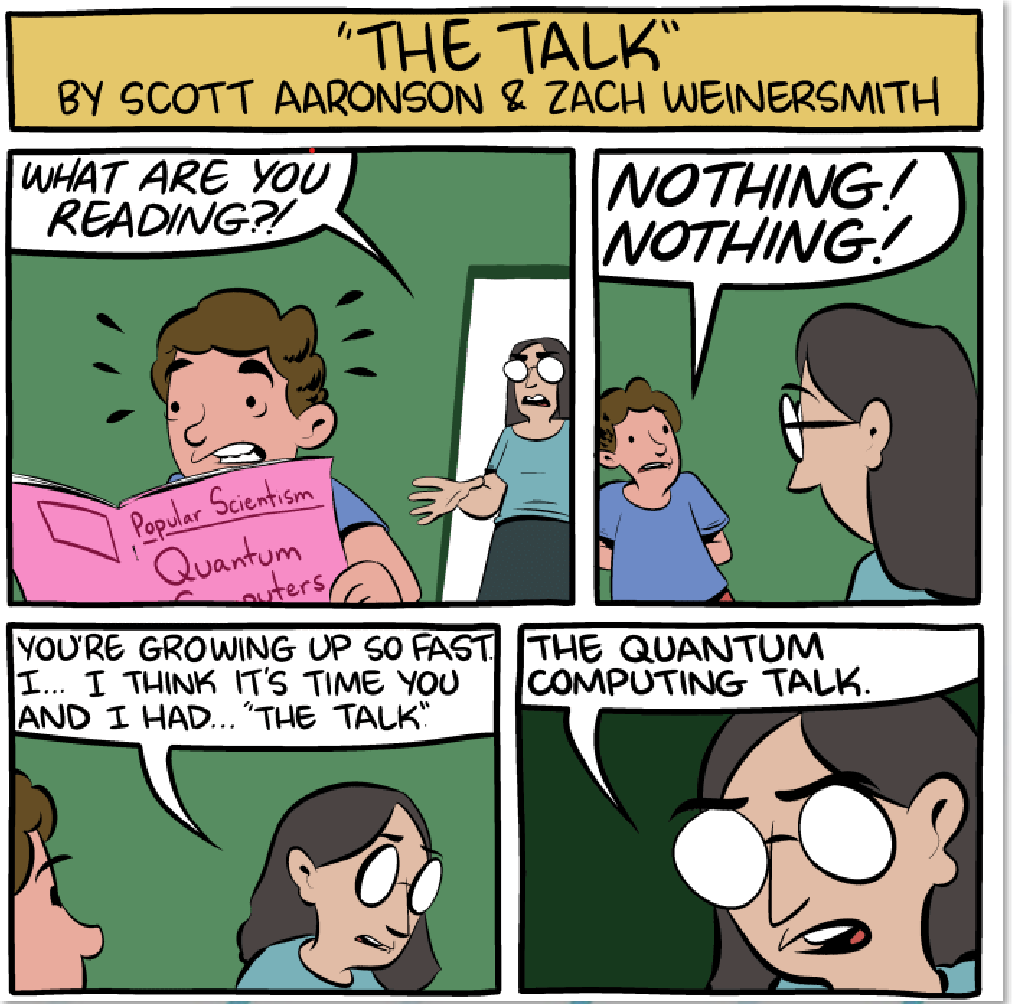
February 1, 2024

Briefing:
Quantum Computing 101

Rick Arthur, Sr. Principal Engineer, Computational Methods Research

(Contributions from Bill Smith, Bogdan Neculaes, Steve Bush, and Annarita Giani)





Link: [The Talk]
Also: [Scott Aaronson Blog]

February 1, 2024

Briefing: Quantum Computing 101

Rick Arthur, Sr. Principal Engineer, Computational Methods Research

(Contributions from Bill Smith, Bogdan Neculaes, Steve Bush, and Annarita Giani)

Quantum Computing

Topics

Preface
- **Executive Summary**
- **Origin Story** [@]: Richard Feynman

Assessments [@]

Building Blocks [@]
- **Data**: What is a bit? → What is a quantum bit (qubit)?
- **Logic**: Binary logic (transistor gate) → Quantum logic
- **Quantum phenomena**: Superposition, Entanglement, Coherence

Hardware & Architectures [@]

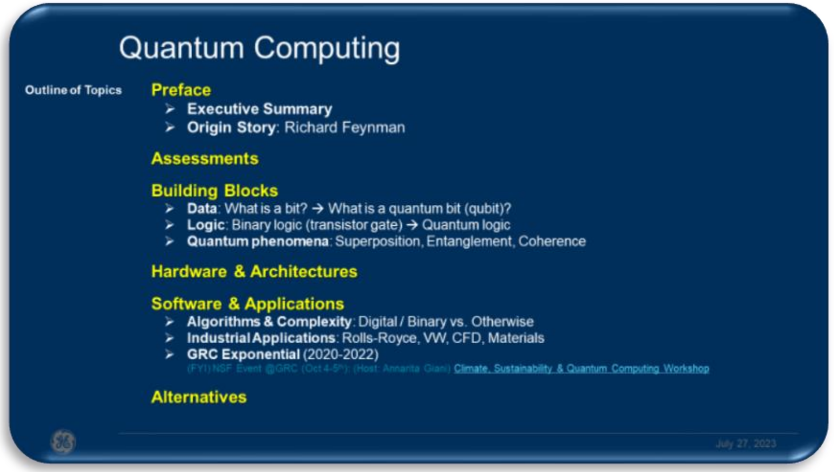
Software & Applications [@]

Alternatives [@]

Quantum Computing 101: What is it?

Motivation (Originally)

- Simulate Quantum Mechanics



Quantum Computers

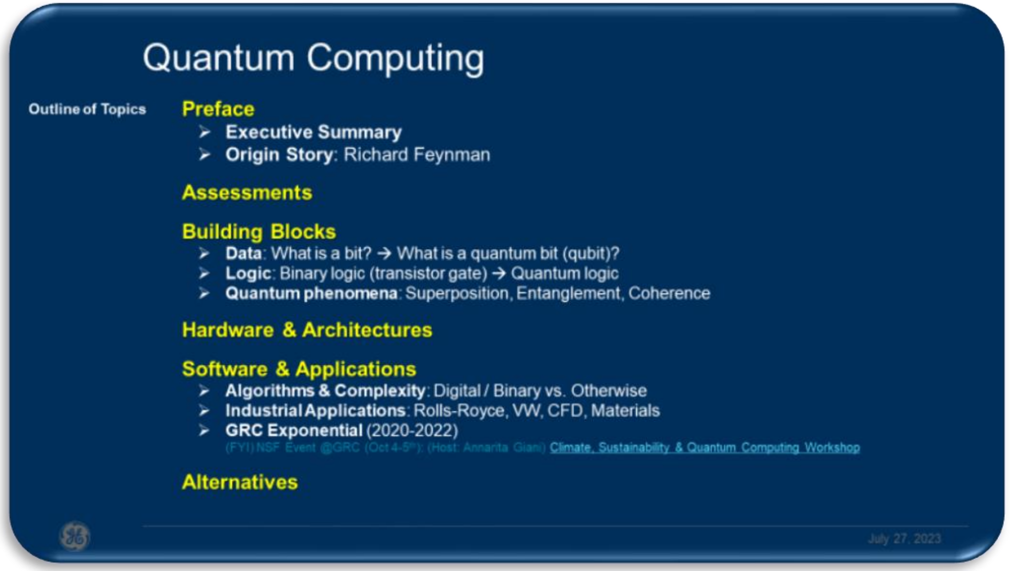
- Quantum Mechanical Architecture
  - ➢ Data
    - ○ classical bits: 0 (=0) or ~5 volts (=1)
    - ❖ quantum bits (“qubits”) = wave functions
  - ➢ Functional Logic
    - ○ classical gate: “clocked” transistors
    - ❖ quantum gate: wave interference
  - ➢ Diverse Hardware Architectures
    - ❖ Address qubit fidelity (noise, stability)
    - ❖ Grow number of qubits (problem size)
- Related Quantum Technology
  - ✓ Communications / Networking
  - ✓ Sensing / Navigation
- Alternative Non-classical Computing
  - ❑ Neuromorphic / AI
  - ❑ Analog (e.g., Optical)
  - ❑ Probabilistic

…

Quantum Computing Applications

- Quantum Computer Execution
  - ○ Set up qubits and qubit relationships
  - ○ ***Instantaneous*** system solution
  - ○ Critical differences vs. Classical
    - ➢ Very small size / data (unless embody as PDE)
    - ➢ No persistent “state” or pipeline sequential processing
    - ➢ Limited algorithms & support toolchain
- Quantum Applications
  - ○ Candidate characteristics:
    - ➢ problem is easy to express (as an ODE or PDE)
    - ➢ but a hard-to-solve problem (complexity taxes classical)
    - ➢ with little to no data to input or output or hold in state during the computation
  - ○ *Essentially,* limited to problems with:
    - ➢ Factorization (e.g., applied to crypto)
    - ➢ Sparsely-constrained high-D linear optimization
    - ➢ Simulation of quantum mechanics – e.g., materials, superconductivity, lasers, photosynthesis

Quantum Computing 101: Executive Summary



Motivating Hype & Hysteria

- Wishful /naïve potential application
- Threat to cryptography
- Foreign (China) investment
- US Government investment
- Startups + big-name R&D

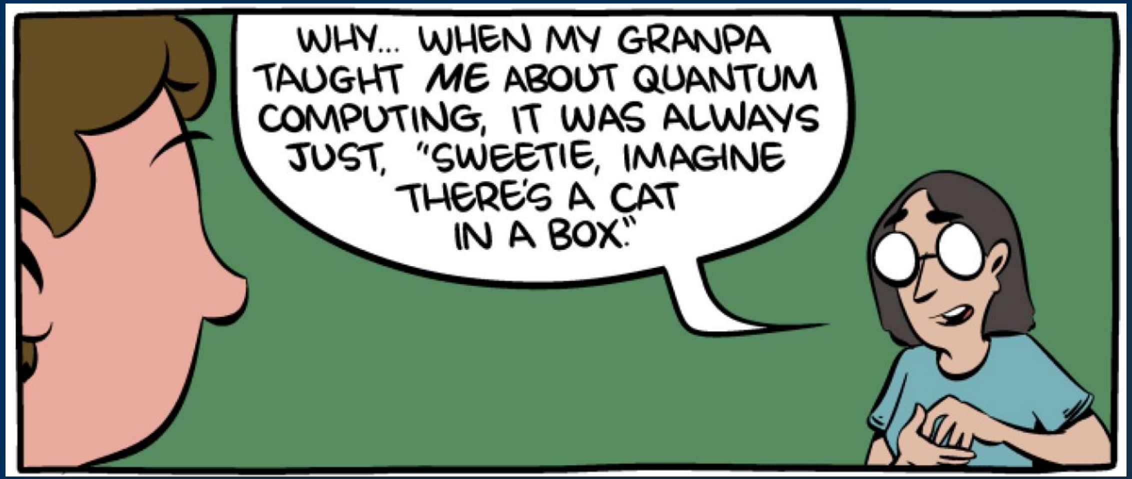
Quantum Computers

- Challenging physics concepts
- Diverse hardware approaches
- Need more qubits (problem size)
- Need error correction (noise)
- Need coherence (stability)
- (Many) need vacuum+super-cold
- Need interface to non-quantum
- Promising related opportunities
  - ✓ Secure communications
  - ✓ Sensing / Navigation
  - ✓ Quantum Mechanics stand-in (e.g., modeling & simulation in chemistry and materials)
- Other computing options exist
  - ❑ Neuromorphic / AI
  - ❑ Analog (e.g., Optical)
  - ❑ Probabilistic, …

Quantum Computing Applications

- Challenging to design programs
- Very narrow advantage applicability
  { *crypto, search, high-D optimization* }
- Instantaneous system solution
  (*no state, pipeline, or time steps*)
- Target: heavy compute + small data
- Need to mature support toolchain

Preface: Origin Story



Quantum Computing's Thought Leader

(How did this all start?)

Richard P Feynman. Simulating physics with computers.
International Journal of Theoretical Physics, 21:467–88, 1981.

Feynman's motive:

"Nature isn't classical, dammit, and if you want to make a simulation of Nature, you'd better make it quantum mechanical"

Richard P Feynman. Simulating physics with computers.
International Journal of Theoretical Physics, 21:467–88, 1981.

Quantum Computing’s Thought Leader

(How did this all start?)

***Problem**: space and time [+ mass, energy, etc] are continuous, but a (classical) computer is discrete.*

***Solution**: assume/hope/pretend that the laws of nature are discrete*
at a level sufficiently fine that no current experimental evidence is contradicted.

***Problem**: “Sufficiently fine” increases exponentially over space-time volumes simulated.*

***Strategy**: Classical physics is causal, so we can simulate the system's time evolution step by step.*

***Problem**: But then “the time is not simulated at all, it is imitated in the computer”*

***Problem**: discretized probabilities cannot be exact.*

The hidden-variable theorem: It is impossible to represent the result of quantum mechanics with a classical universal device.

Feynman’s motive (and the TL;DR re: QC applications):

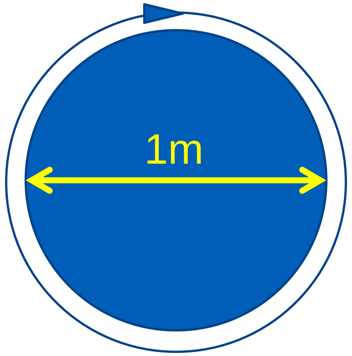
“Nature isn't classical, dammit, and if you want to make a simulation of Nature, you'd better make it quantum mechanical”

Richard P Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–88, 1981.

Quantum Computing's Thought Leader

Classical (binary, Boolean) computer problems

- **Digital = No continuous data** (must "discretize" into finite digits)
  - Loss of precision and numerical sensitivities in measurable quantities (example: spatial measurements into "mesh" or points)
  - Cannot hold a probability distribution as a value, must sample across (discretize)
  - Simulating physical causality by time-stepping introduces implicit (non-explicit) approximation



Circumference = π

FP64 = 3.14159265358979311599796346854 ...???...

Feynman's motive:

"Nature isn't classical, dammit, and if you want to make a simulation of Nature, you'd better make it quantum mechanical"

Quantum Computing’s Thought Leader

Richard P Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–88, 1981.

(1979) Richard **Feynman** famously states:

*“**Will you understand** the theory? […]*

*When I tell you that the first time we really thoroughly explain [**Quantum Mechanics**] to our own physics students is when they're in [third year graduate physics.]*

*Then, you think the answer is going to be **NO**. And that's correct, **you will not understand**. […]*

But […] I want to tell you something: The students do not understand it either.

*And that's **because the professor doesn’t understand**.”*

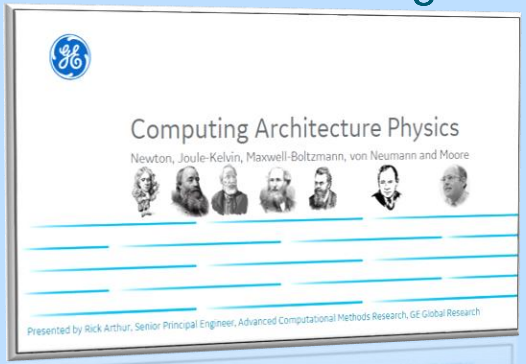
(Therefore) this briefing must trade-off
necessary time to attempt to elucidate vs. pragmatic usefulness
(and all of us accepting incomplete understanding).

Quantum Computing: Fuel for the Fairy Tale

(40yrs later) Richard **Arthur** (*unfamously*) suggests:

When computer clock speeds hit a wall in the mid-2000's
(see HPC 101: Computer Architecture Physics) →
developers of applications/algorithms and their end-users
became frustrated with the halt in computing hardware performance
(having been accustomed to decades of exponentially-improving performance as a side effect of Moore's Law)

Further reading:



HPC 101: Computer Architecture Physics
(PDF) (Webinar)
Nov-2018

Quantum Computing became a "*wish upon a star*" magical fix
to this insatiable demand from software for processing cycles & high-speed storage
(despite – *or more accurately because of* –
Quantum Computing being so inscrutably esoteric!)

(Notably greatly expanding ambitions from Feynman's
motive toward **simulation of quantum mechanics**.)

(1979) Richard Feynman famously states:

"Will you understand the theory? [...]

When I tell you that the first time we really thoroughly explain [Quantum Mechanics] to our own physics students is when they're in [third year graduate physics.]

Then, you think the answer is going to be no. And that's correct, you will not understand. [...]

But [...] I want to tell you something: The students do not understand it either.

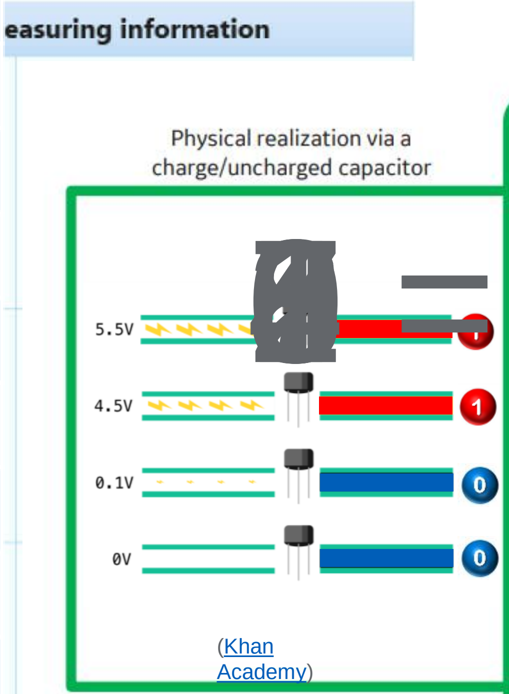
And that's because the professor doesn't understand."

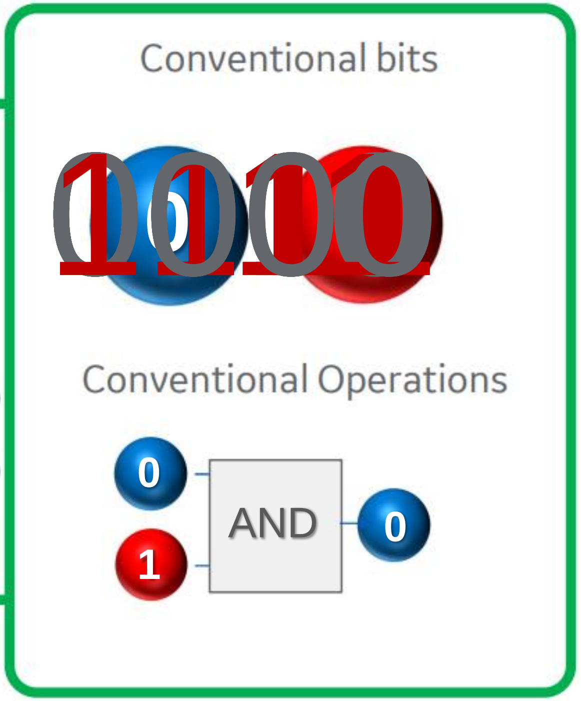
Building Blocks: Data & Logic

Building Blocks (Data): Bits

Conventional binary “Boolean” logic implemented in semiconductors (exploiting band gap)

Binary	Decimal
0 0 0 0	0
0 0 0 1	1
0 0 1 0	2
0 0 1 1	3
0 1 0 0	4
0 1 0 1	5
0 1 1 0	6
0 1 1 1	7
1 0 0 0	8
...	...



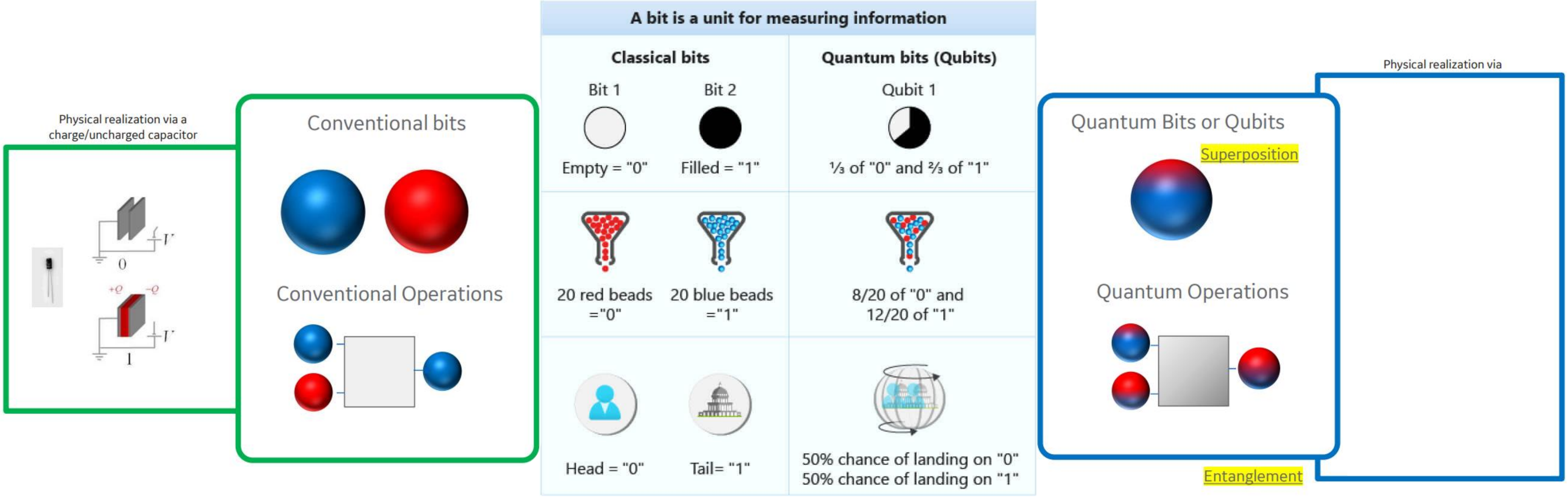


https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-qubit

https://ny-creates.org/wp-content/uploads/NY-CREATES-Talk-Giani-Schnore-June3-2021.pdf

Building Blocks (Data): Bits & Qubits *(quantum bits)*

Exploiting quantum mechanical “Superposition”

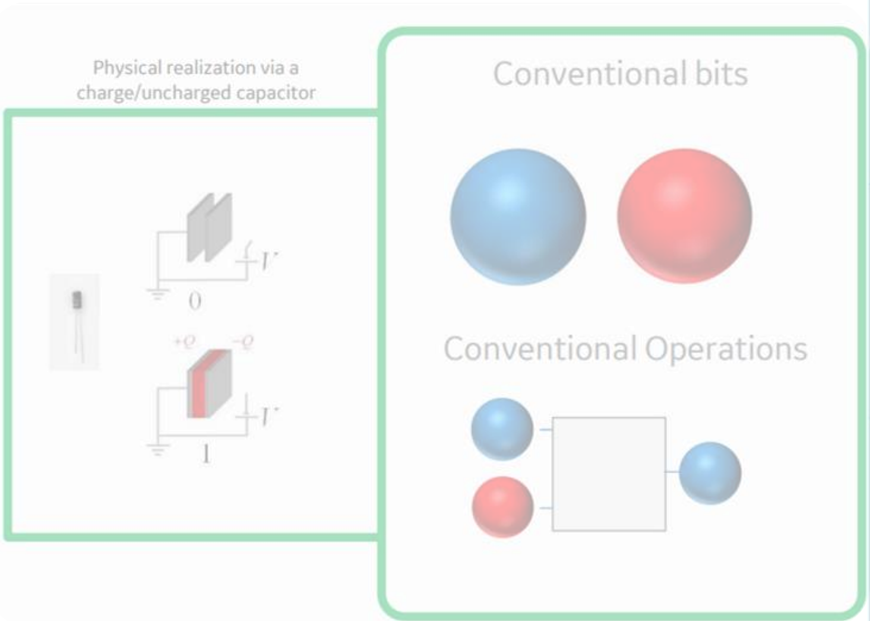


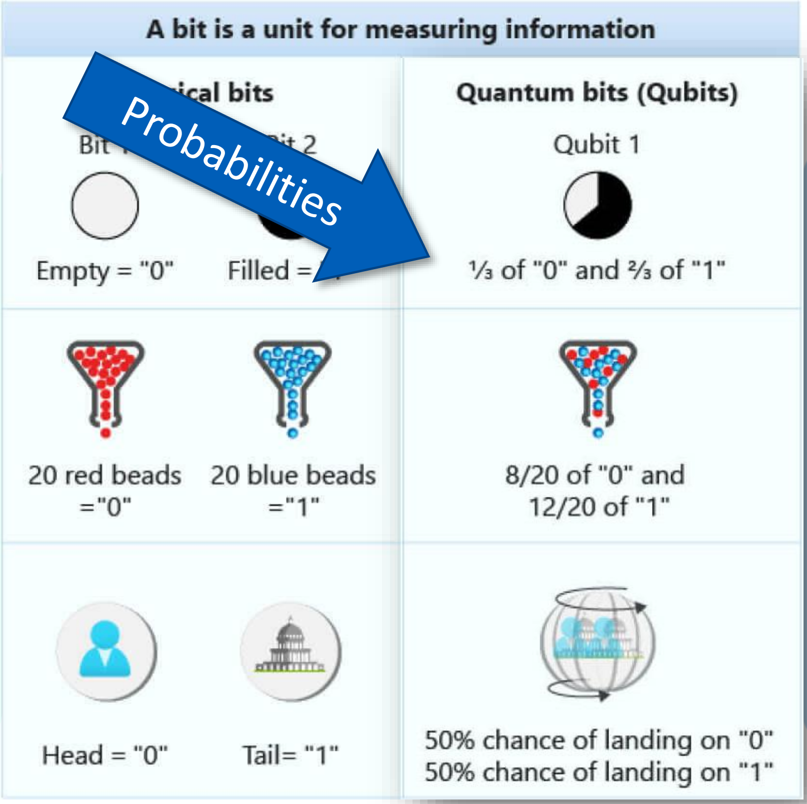
https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-qubit

https://ny-creates.org/wp-content/uploads/NY-CREATES-Talk-Giani-Schnore-June3-2021.pdf

Building Blocks (Data): Bits & Qubits *(quantum bits)*

Exploiting quantum mechanical “Superposition”





https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-qubit

Wave functions describe the behavior of the quantum particles that compose qubits.

Wave characteristics = (phase,) wavelength, and amplitude.

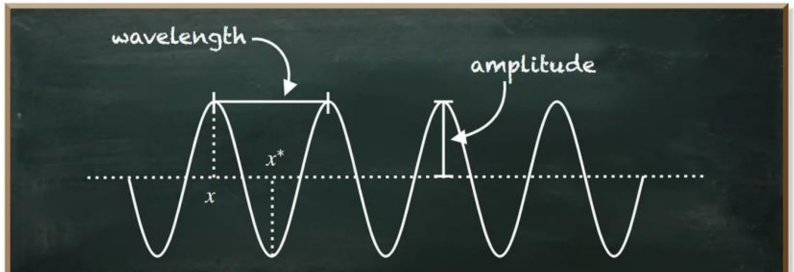


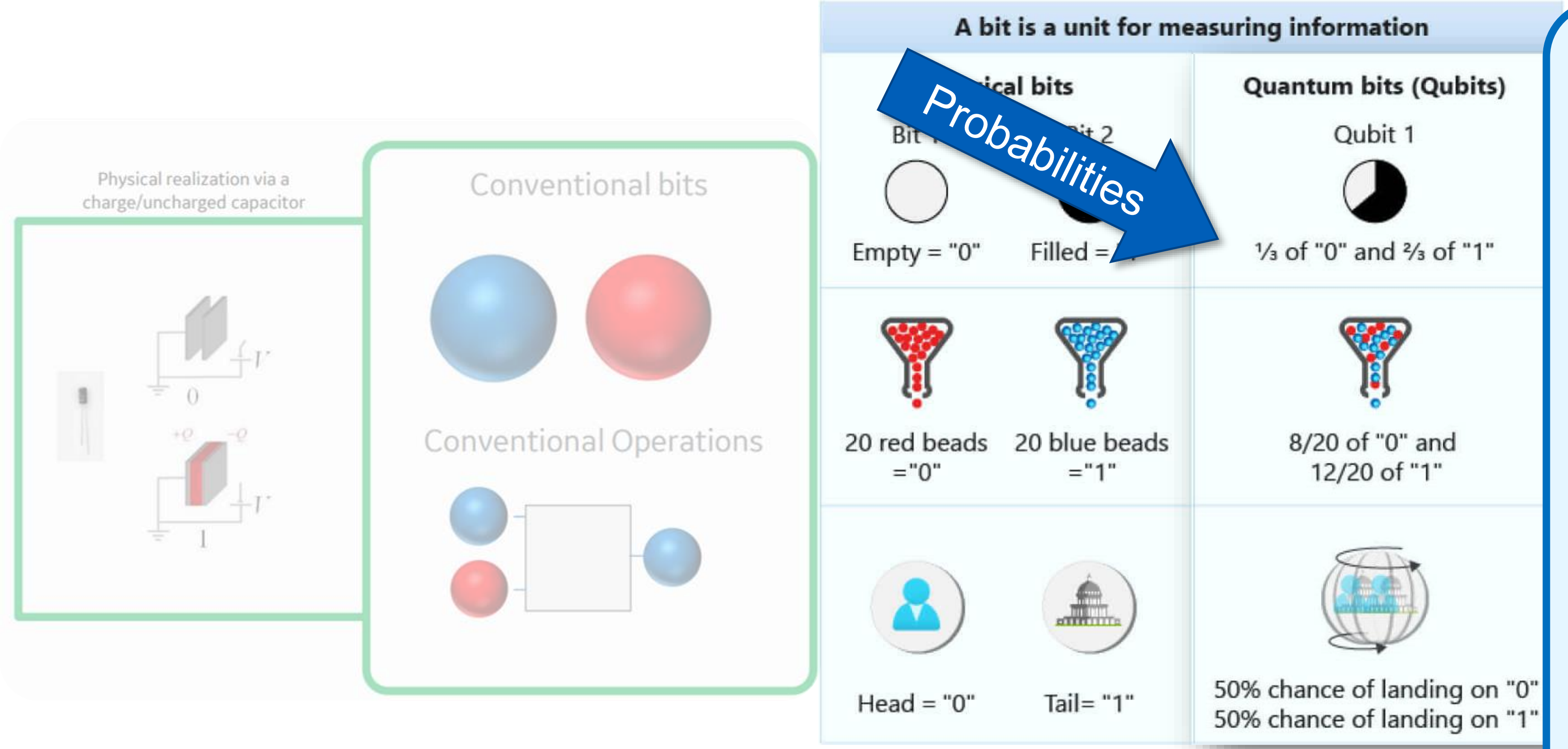
Figure 10.1: Characteristics of a wave

This “probability” of measuring the qubit as a 0 vs. 1 is based upon the measured behavior of particle.

https://towardsdatascience.com/quantum-amplitudes-and-probabilities-b49a6969b0b9

Building Blocks (Data): Bits & Qubits *(quantum bits)*

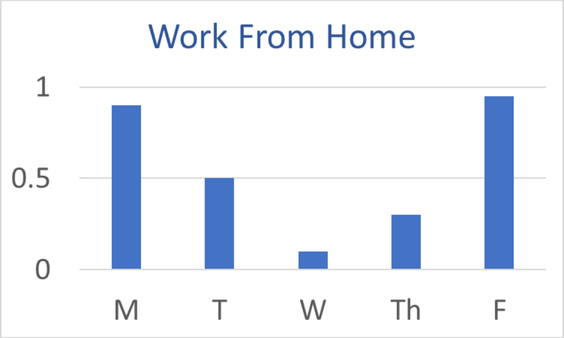
Exploiting quantum mechanical "Superposition"



https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-qubit

Wave functions describe the behavior of the quantum particles that compose qubits.

Consider: "Working at home" distribution over the days of the work week.

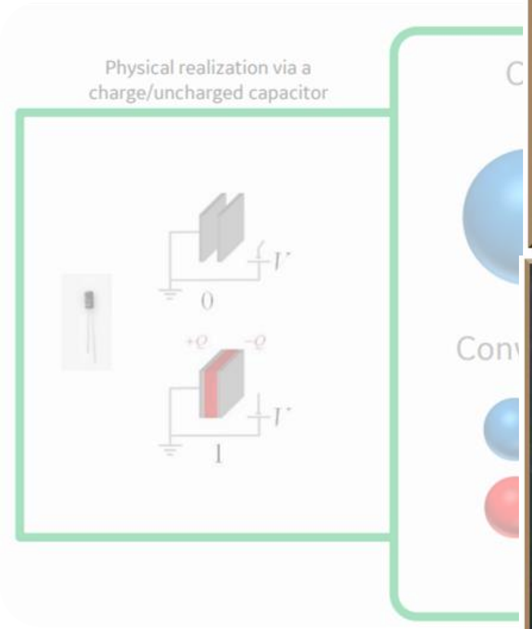


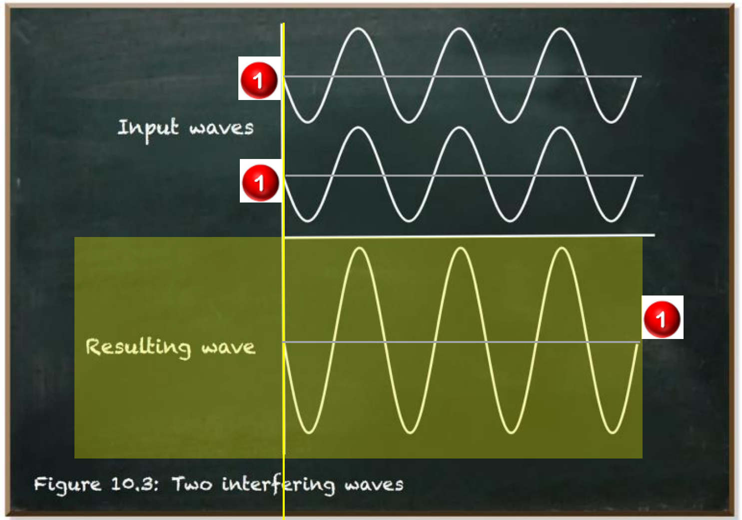
This "probability" of measuring the qubit as a 0 vs. 1 is based upon the measured behavior of particle.

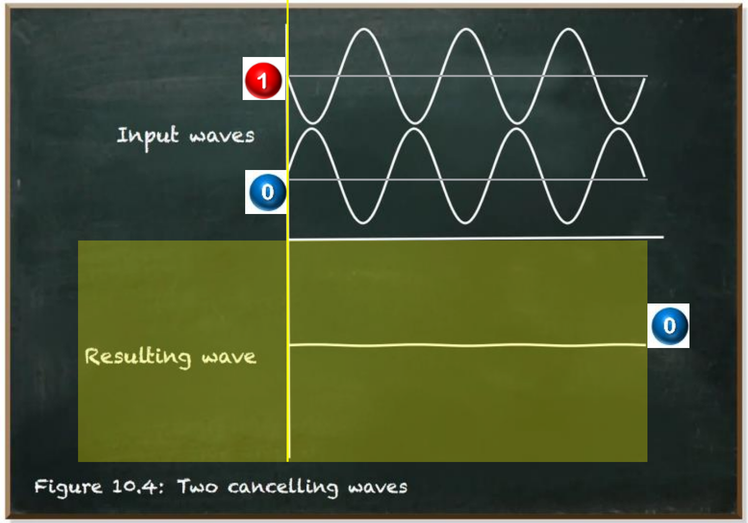
https://towardsdatascience.com/quantum-amplitudes-and-probabilities-b49a6969b0b9

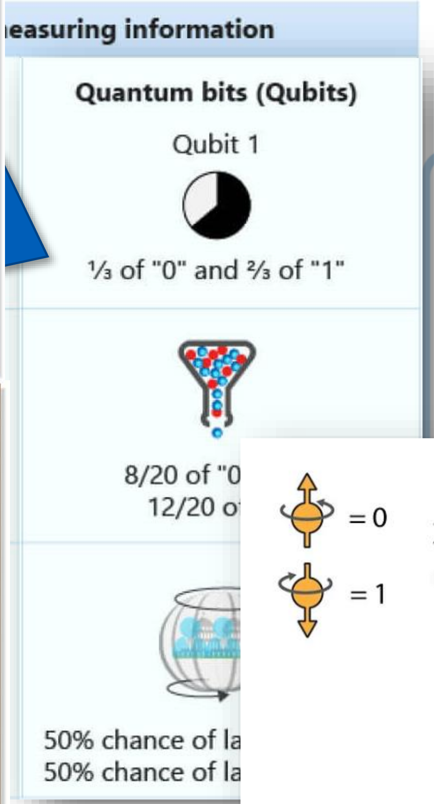
Building Blocks (Data): Bits & Qubits *(quantum bits)*

Exploiting quantum mechanical “Entanglement” between qubits



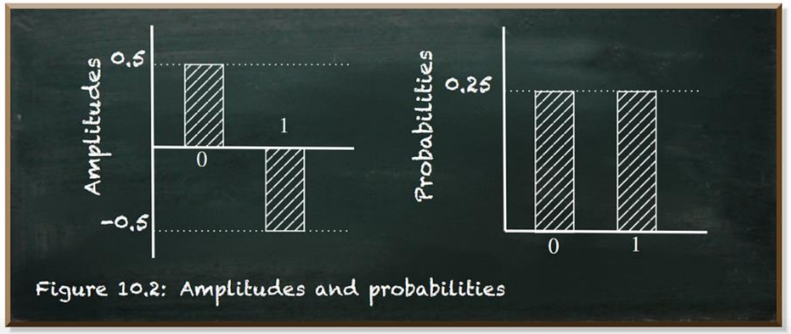


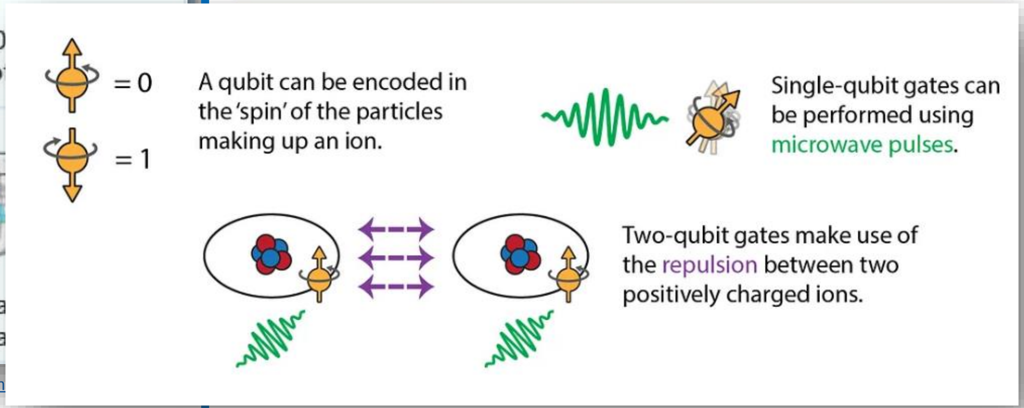




s/cloud-computing-dictionary/wh

Amplitudes ≠ Probabilities





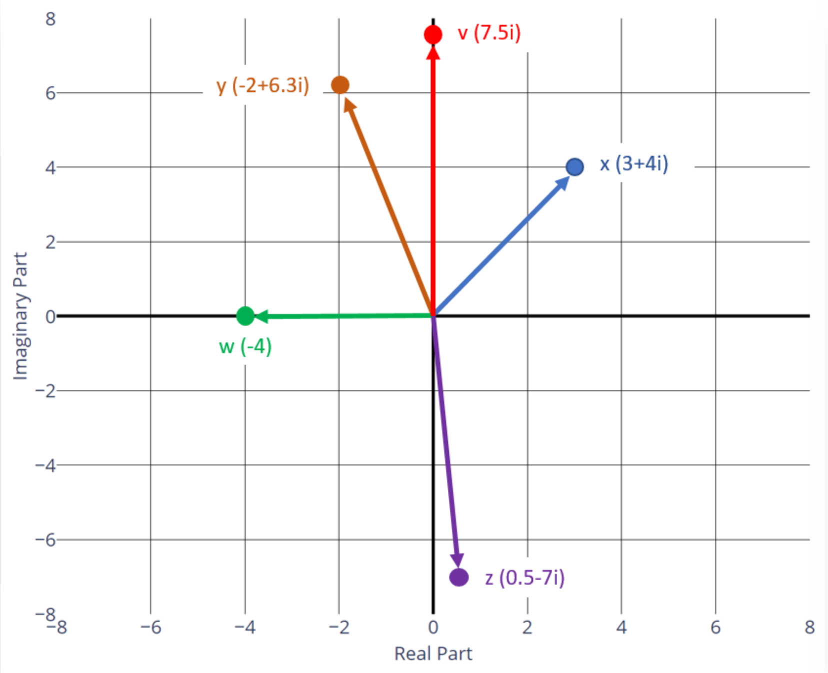
https://towardsdatascience.com/quantum-amplitudes-and-probabilities-b49a6969b0b9

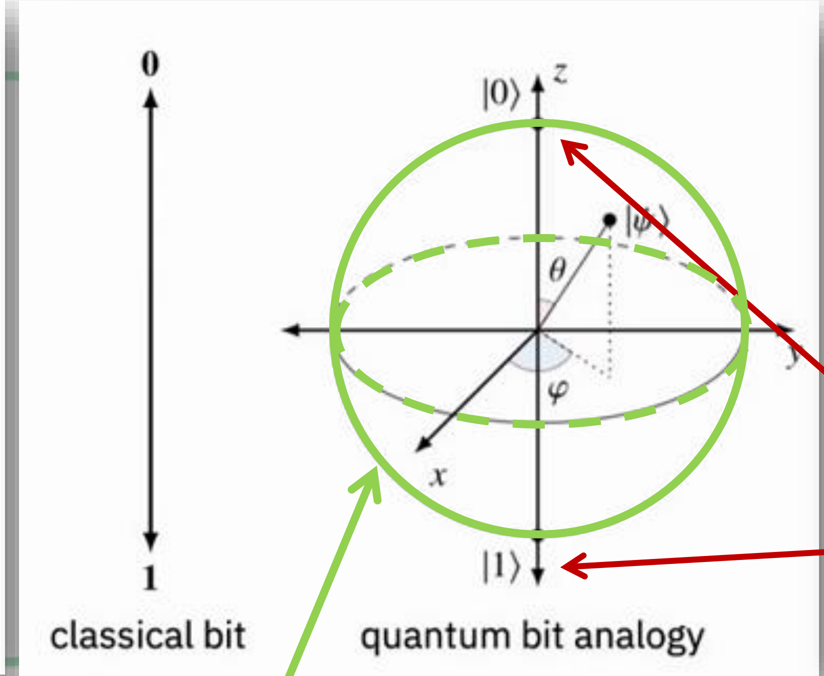
Building Blocks (Data): Bits & Qubits *(quantum bits)*

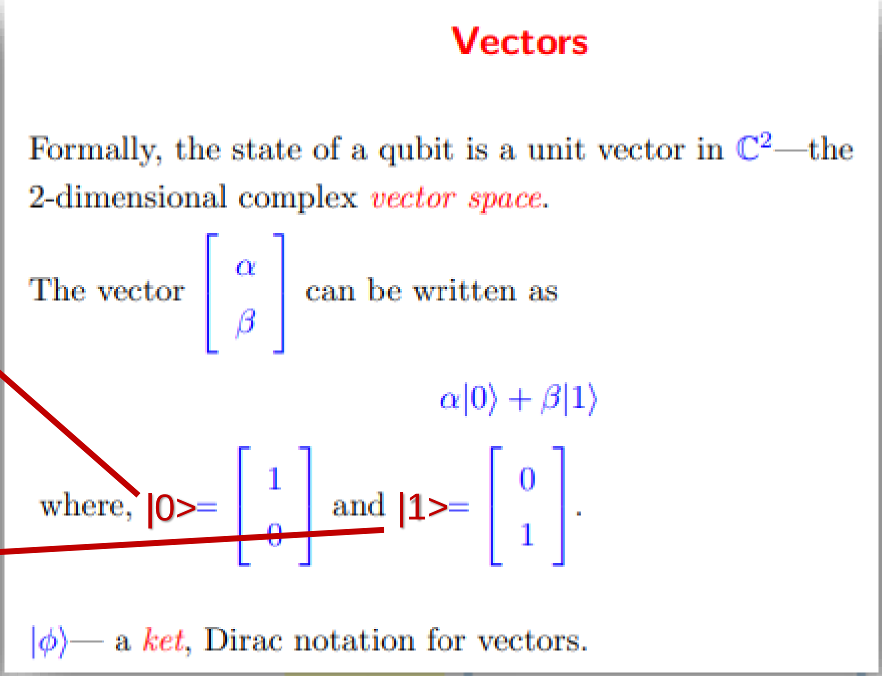
Exploiting quantum mechanical “Entanglement” between qubits

But the mathematics use complex number vectors to characterize the wave function of electron spin...
(See: https://stem.mitre.org/quantum/quantum-concepts/qubits.html)

https://www.cl.cam.ac.uk/teaching/0910/QuantComp/notes.pdf







Vectors

Formally, the state of a qubit is a unit vector in $\mathbb{C}^2$—the 2-dimensional complex *vector space*.

The vector $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ can be written as

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

where, $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

$|\phi\rangle$— a *ket*, Dirac notation for vectors.

Entanglement

https://ny-creates.org/wp-content/uploads/NY-CREATES-Talk-Giani-Schnore-June3-2021.pdf

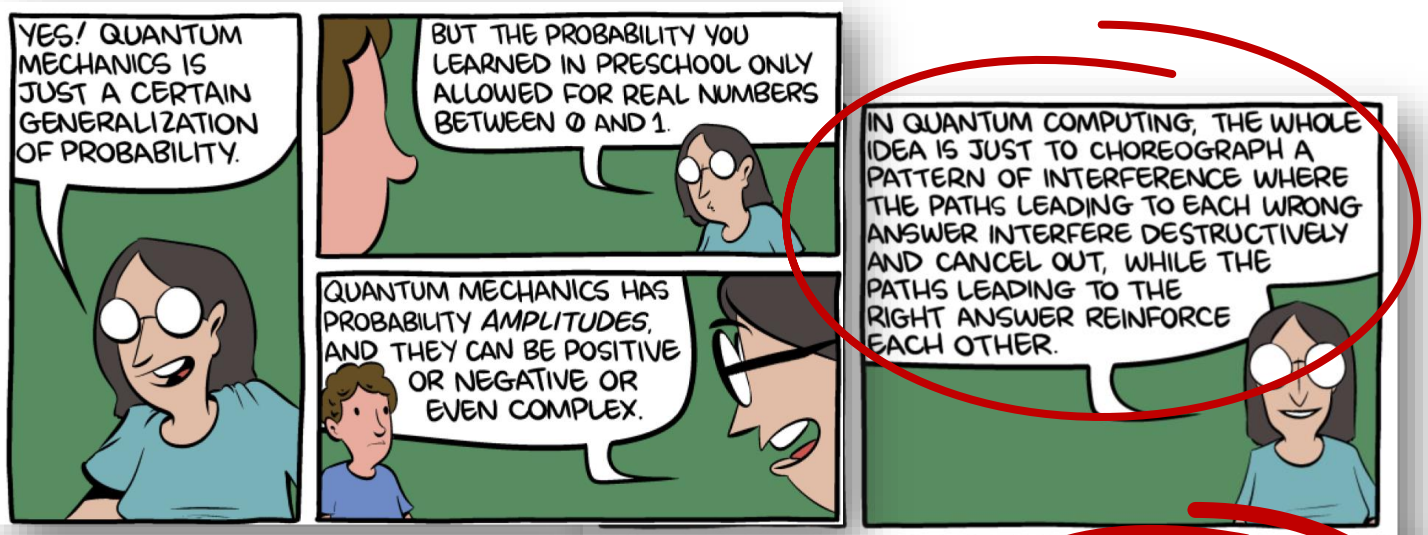
[Topics]

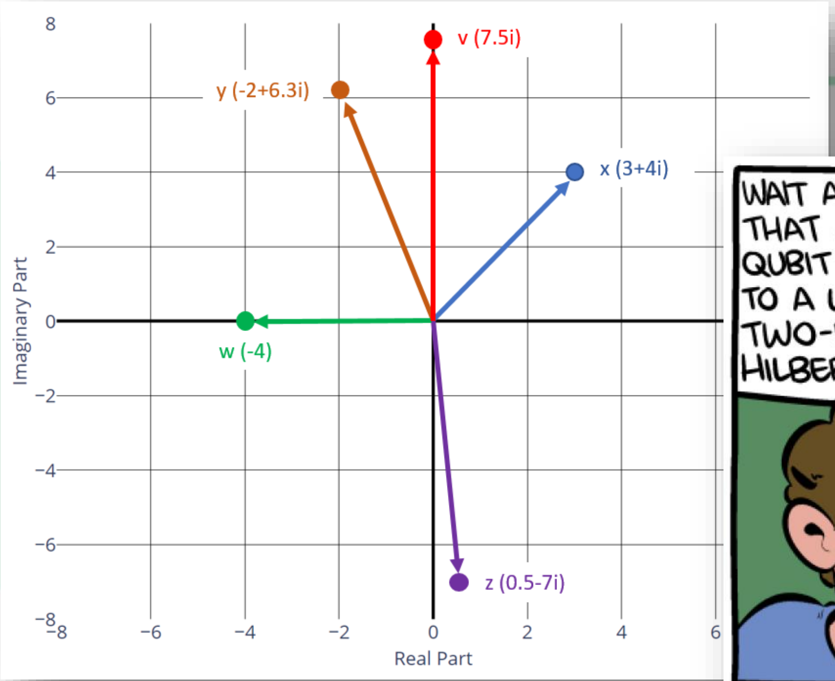
Bloch sphere: geometrical representation of a qubit in spherical coordinates

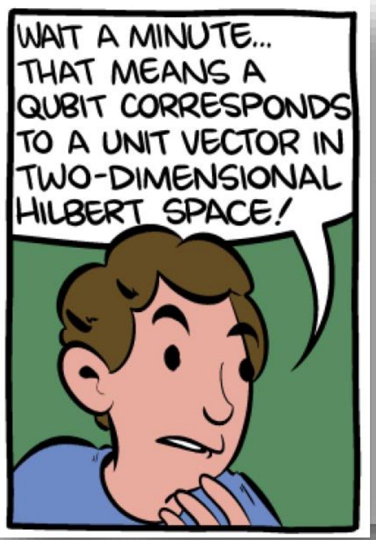
Building Blocks (Data):

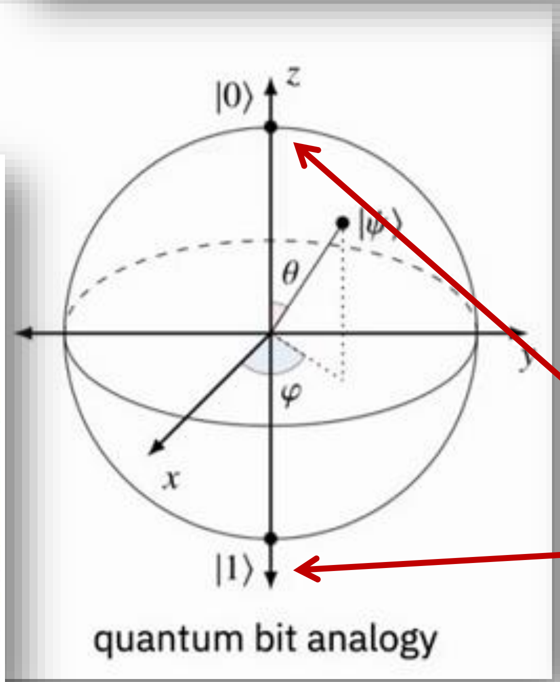
Exploiting quantum mechanical "Enta

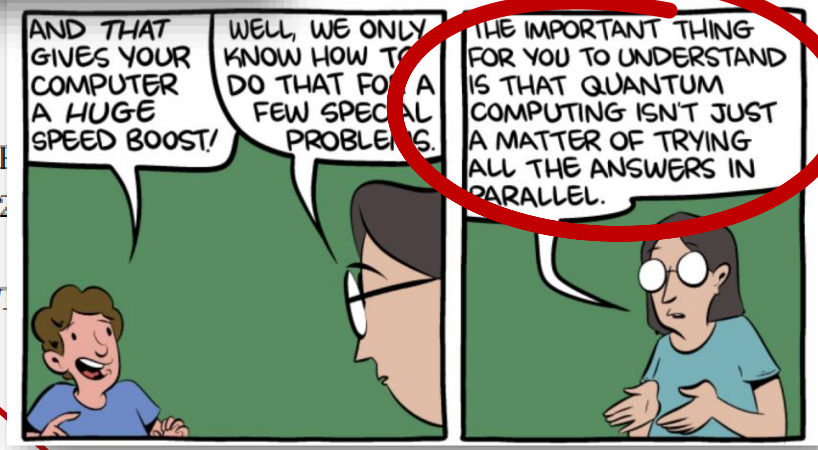
But the mathematics
characterize the wave
(See: https://stem.mitre.org/qua











where, $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

$|\phi\rangle$— a *ket*, Dirac notation for vectors.

Entanglement

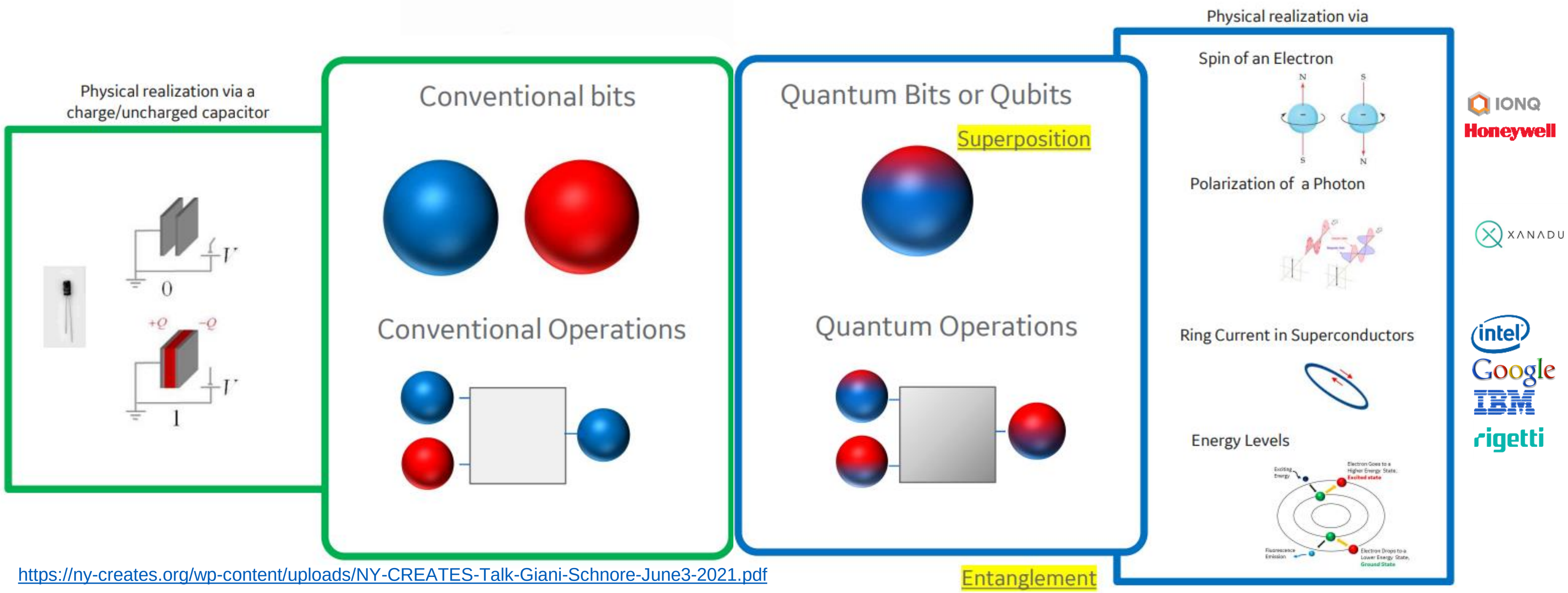
https://medium.com/@brcsomnath/hilbert-space-7a36e3badac2
https://mathworld.wolfram.com/HilbertSpace.html

https://ny-creates.org/wp-content/uploads/NY-CREATES-Talk-Giani-Schnore-June3-2021.pdf

Building Blocks (Data): Bits & Qubits (*quantum bits*)

In a quantum computer:

qubits are joined together and functionally interact like atoms in a molecule



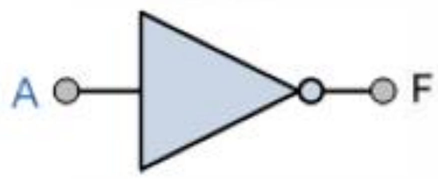
https://ny-creates.org/wp-content/uploads/NY-CREATES-Talk-Giani-Schnore-June3-2021.pdf

Building Blocks (Functional Logic): Gates

Transistors in semiconductors

Classical Boolean Logic

NOT



Input	Output
A	F
0 (NOT) →	1
1 (NOT) →	0

AND

Inputs		Output
A	B	F
0 (&?)	0 (?) →	0
1	0	0
0	1	0
1	1	1

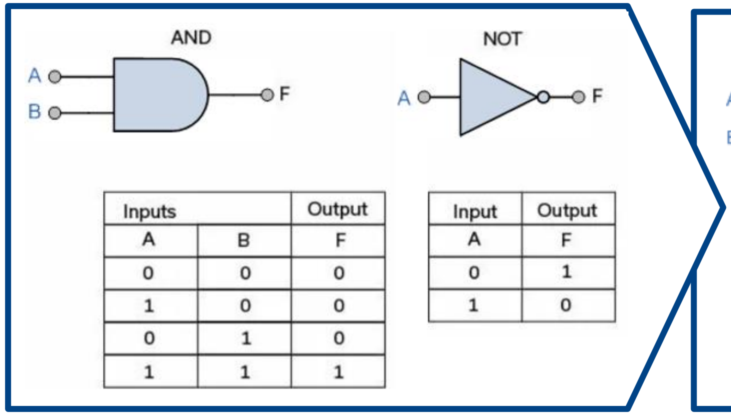
https://www.electronics-tutorials.ws/logic/universal-gates.html

Logic: Gates

Combining gates as building blocks

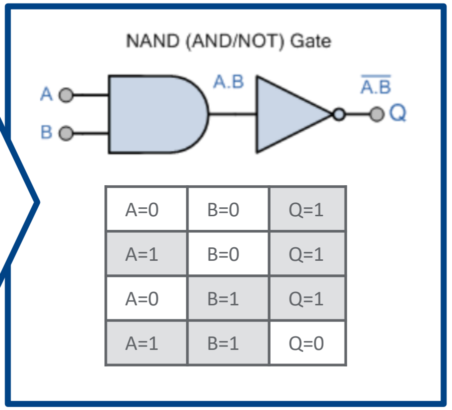
Classical [Boolean](#) Logic

AND + NOT = NAND



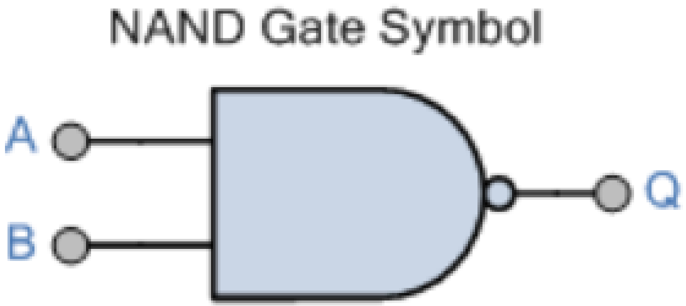
Inputs		Output
A	B	F
0	0	0
1	0	0
0	1	0
1	1	1

Input	Output
A	F
0	1
1	0



A=0	B=0	Q=1
A=1	B=0	Q=1
A=0	B=1	Q=1
A=1	B=1	Q=0

https://www.electronics-tutorials.ws/logic/universal-gates.html

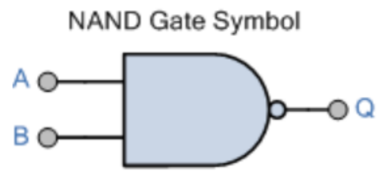


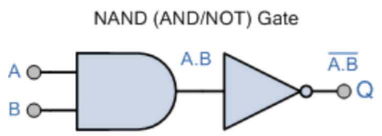
Logic: Gates

Universal logic for computers can be built from NAND building blocks

Example: Add bits A + B

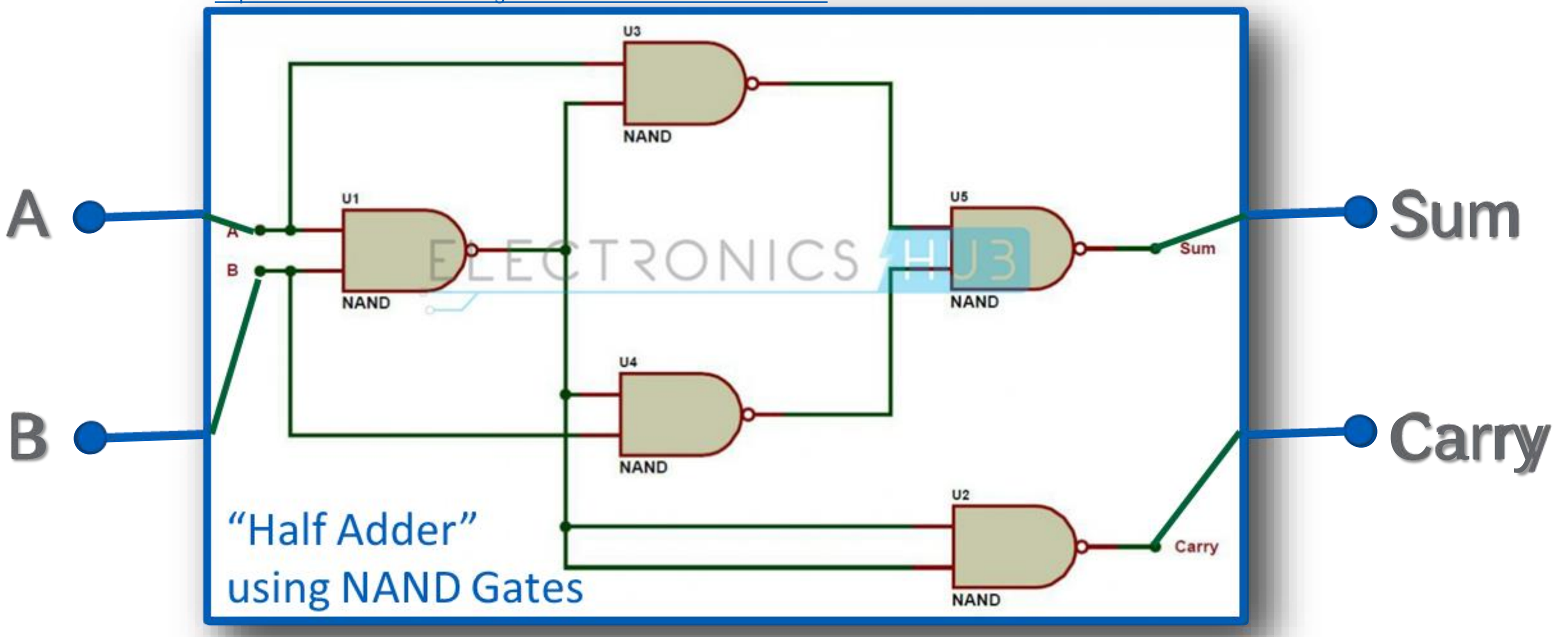
https://www.electronicshub.org/half-adder-and-full-adder-circuits/





A=0	B=0	Q=1
A=1	B=0	Q=1
A=0	B=1	Q=1
A=1	B=1	Q=0

https://www.electronics-tutorials.ws/logic/universal-gates.html



A + B = Sum

0 + 0 = 0

1 + 0 = 1

0 + 1 = 1

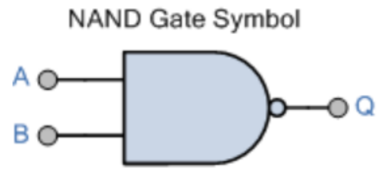
1 + 1 = 0 (Carry 1)

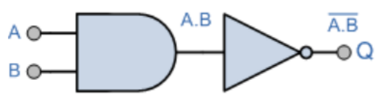
[Topics]

Building Blocks (Logic): Gates into Processors

Assembled into complete microarchitectures of modern semiconductor computers

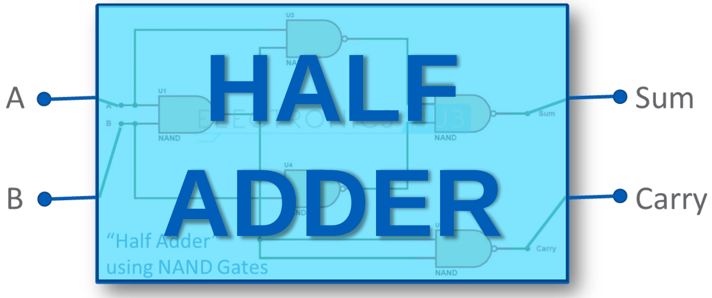
(Classical Boolean) Universal Logic





A=0	B=0	Q=1
A=1	B=0	Q=1
A=0	B=1	Q=1
A=1	B=1	Q=0

https://www.electronics-tutorials.ws/logic/universal-gates.html



https://www.electronicshub.org/half-adder-and-full-adder-circuits/

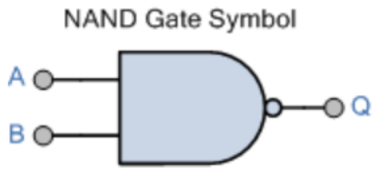
A=0	B=0	Sum=0	Carry=0
A=1	B=0	Sum=1	Carry=0
A=0	B=1	Sum=1	Carry=0
A=1	B=1	Sum=0	Carry=1

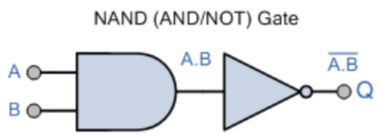
Combining and combining…

Building Blocks (Logic): Quantum Gates

Exploiting quantum mechanical "Entanglement" *(Einstein's "[Spooky action at a distance](#)")*

Classical Boolean Logic

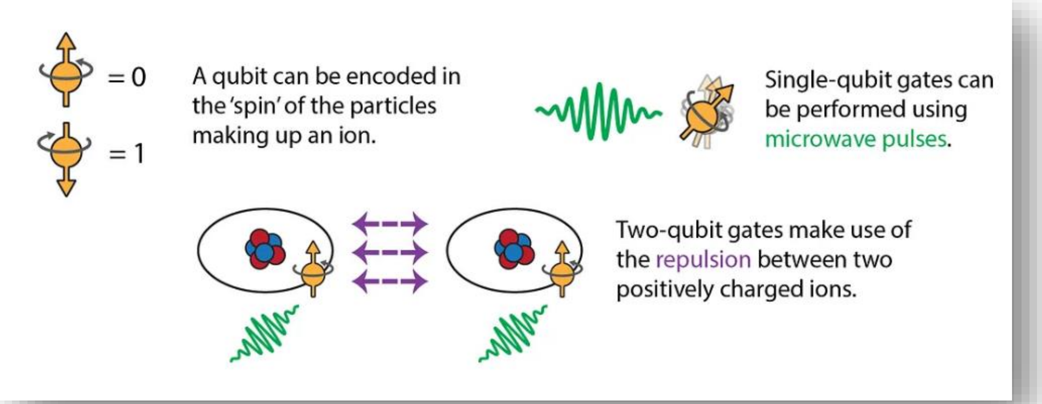


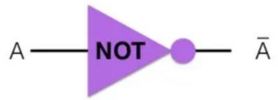


A=0	B=0	Q=1
A=1	B=0	Q=1
A=0	B=1	Q=1
A=1	B=1	Q=0

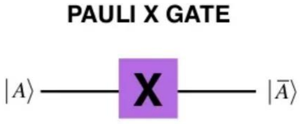
https://www.electronics-tutorials.ws/logic/universal-gates.html

Quantum Logic





A	Ā
0	1
1	0



$\lvert A\rangle$	$\lvert \bar{A}\rangle$
0	1
1	0

(exploiting Pauli's Exclusion Principle)

operate as **vector / matrix operations** relative to spin of 1-2 qubits

(as opposed to Boolean operators)

https://towardsdatascience.com/demystifying-quantum-gates-one-qubit-at-a-time-54404ed80640

Building Blocks (Logic): Quantum Gates

Assemble circuit relationships through physical interaction ("interference") properties

Vectors

Formally, the state of a qubit is a unit vector in $\mathbb{C}^2$—the 2-dimensional complex *vector space*.

The vector $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ can be written as

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

where, $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

$|\phi\rangle$— a *ket*, Dirac notation for vectors.

https://www.cl.cam.ac.uk/teaching/0910/QuantComp/notes.pdf

vector / matrix operations

(*as opposed to Boolean operators*)

Name	Circuit	Matrix	Operation
Pauli-X (Quantum NOT)	X	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\sigma_x\|0\rangle = \|1\rangle$ $\sigma_x\|1\rangle = \|0\rangle$
Pauli-Y	Y	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$\sigma_y\|0\rangle = i\|1\rangle$ $\sigma_y\|1\rangle = -i\|0\rangle$
Pauli-Z	Z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\sigma_z\|0\rangle = \|0\rangle$ $\sigma_z\|1\rangle = -\|1\rangle$
Hadamard	H	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$H\|0\rangle = \frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$ $(\|+\rangle)$ $H\|1\rangle = \frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$ $(\|-\rangle)$
Phase shift	R_ϕ	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$	$R_\phi\|0\rangle = \|0\rangle$ $R_\phi\|1\rangle = e^{i\phi}\|1\rangle$
CNOT		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	$U_{CN}\|00\rangle = \|00\rangle$ $U_{CN}\|01\rangle = \|01\rangle$ $U_{CN}\|10\rangle = \|11\rangle$ $U_{CN}\|11\rangle = \|10\rangle$
SWAP		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$SWAP\|00\rangle = \|00\rangle$ $SWAP\|01\rangle = \|10\rangle$ $SWAP\|10\rangle = \|01\rangle$ $SWAP\|11\rangle = \|11\rangle$
Controlled-phase	R_ϕ	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix}$	$U_{C_\phi}\|00\rangle = \|00\rangle$ $U_{C_\phi}\|01\rangle = \|01\rangle$ $U_{C_\phi}\|10\rangle = \|10\rangle$ $U_{C_\phi}\|11\rangle = e^{i\phi}\|11\rangle$

Table 2.2: Elementary quantum gates

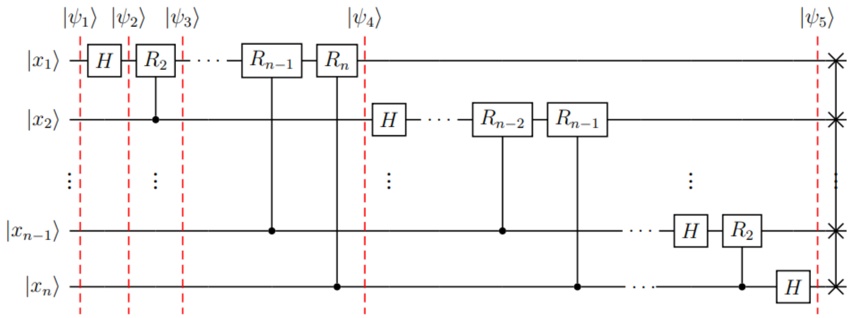
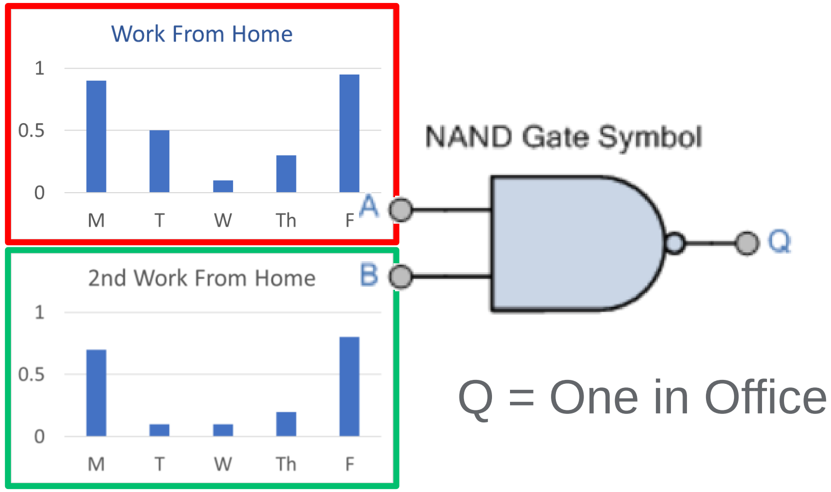


Figure 4.1: Quantum circuit for the quantum Fourier transform.



https://www.imperial.ac.uk/media/imperial-college/research-centres-and-groups/theoretical-physics/msc/dissertations/2021/Chukwudubem-Umeano-Dissertation.pdf

Thought Experiment:
Magnetic + Mechanical Emulator

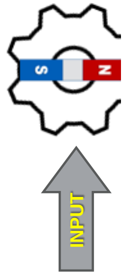
According to ChatGPT:

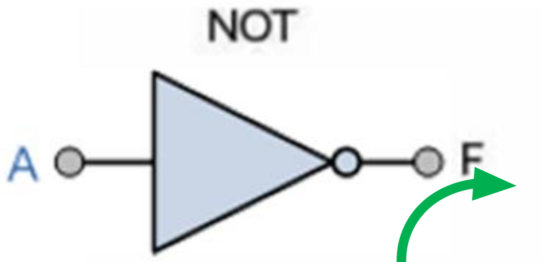
In this humorous presentation, the Clampett family takes it upon themselves to explain the mysteries of quantum computing to Mr. Drysdale and Miss Jane Hathaway. Armed with their unconventional hillbilly wisdom, they compare quantum concepts to moonshine brewing, critter antics, and oil barrel experiments. Through their creative explanations, they manage to demystify quantum computing, making it more relatable and understandable for their puzzled audience. In the end, the presentation emphasizes the value of diverse perspectives and hands-on learning while delivering laughs along the way. The Clampetts once again prove that simplicity and resourcefulness can bridge the gap between the old ways and the technological marvels of the modern world.

Thought Experiment: Boolean Magnet + Mechanical

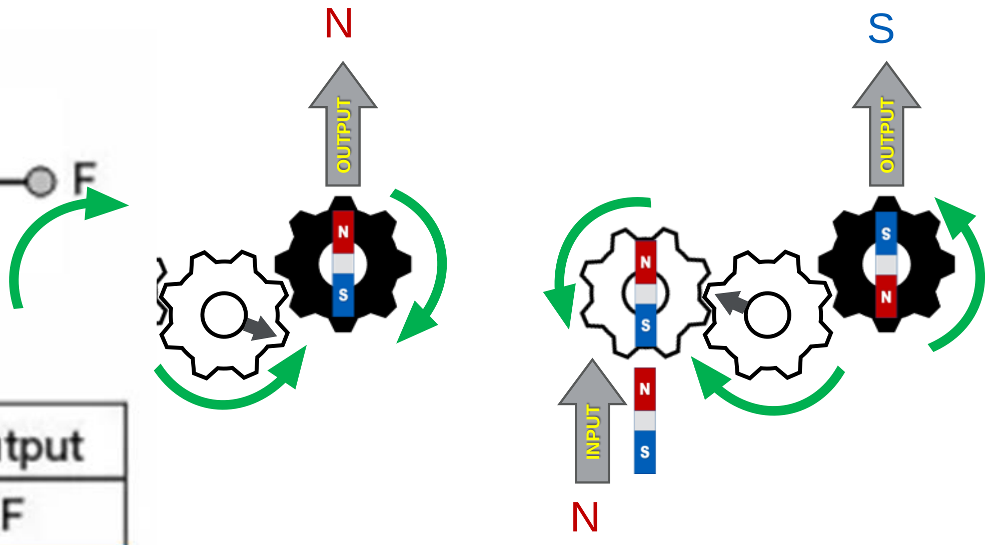
(Electromagnetic force as a *spooky action at a distance*) + (Mechanically can "hold" in position before releasing)

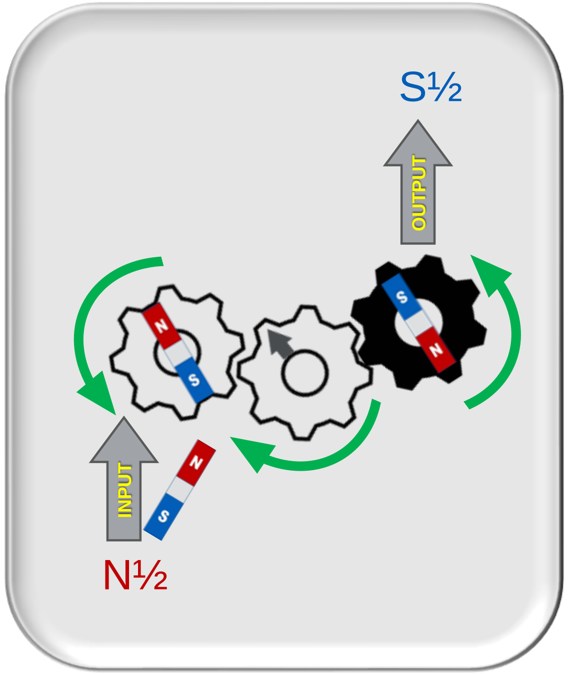
Logical NOT

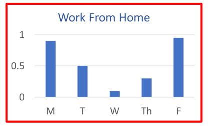




Input	Output
A	F
0	1
1	0





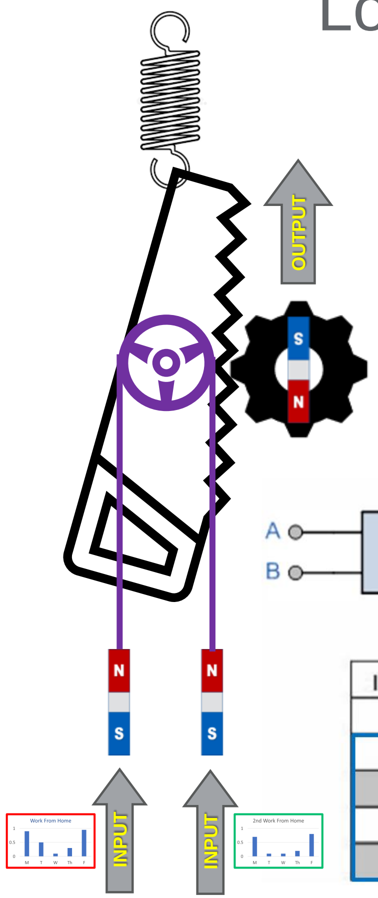


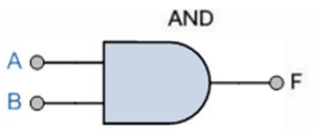
Not intended as an actual working machine: notional operation manifesting at scale of classical physics

Thought Experiment: Boolean Magnet + Mechanical

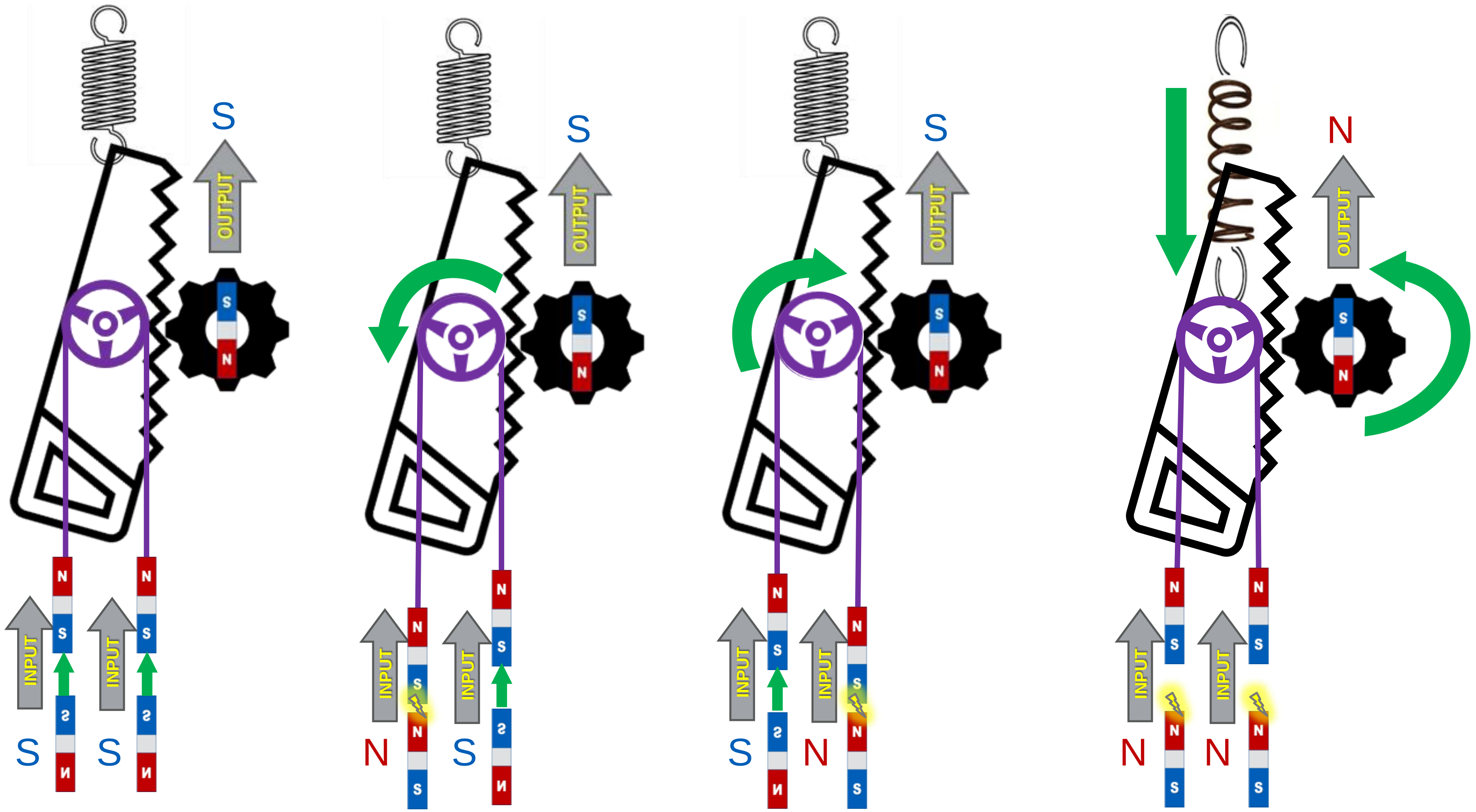
Wheel turns when <u>only one side</u> pulls / Both sides pull = spring extends / Saw blade notches turn the gear

Logical AND





Inputs		Output
A	B	F
0	0	0
1	0	0
0	1	0
1	1	1



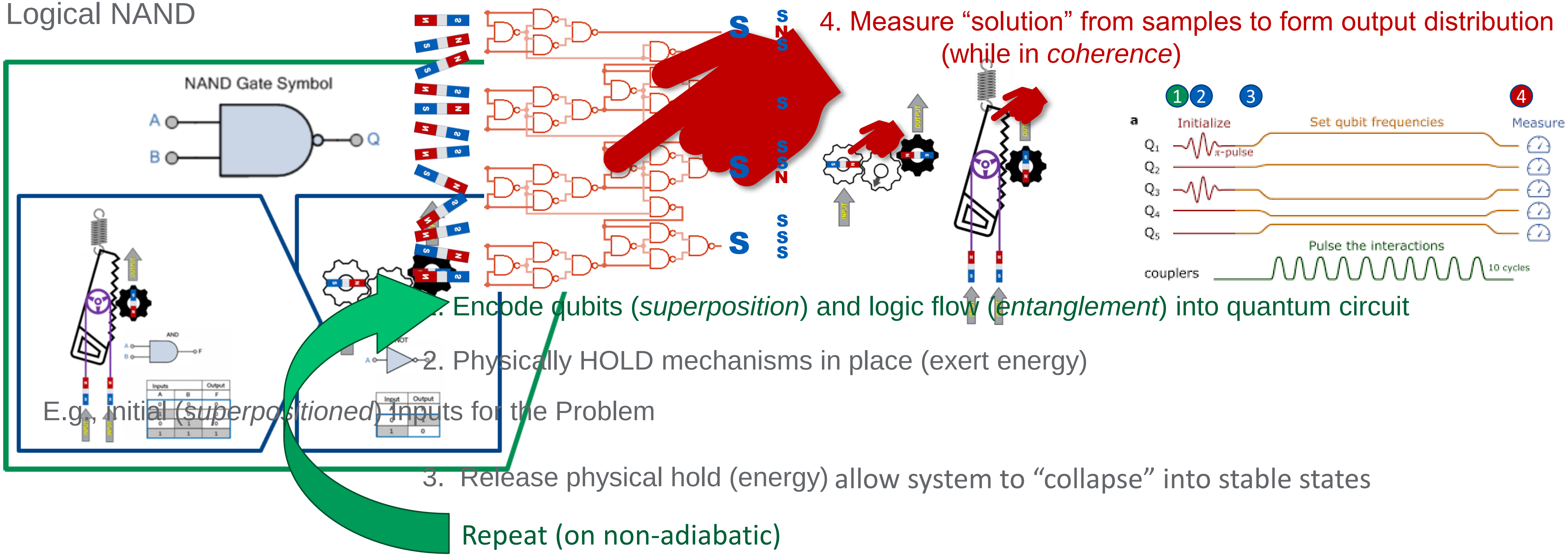
Not intended as an actual working machine: notional operation manifesting at scale of classical physics

Analogy: Magnetic + Mechanical System

(Electromagnetic force as a *spooky action at a distance*) + (Mechanically can "hold" in position before releasing)

Setup problem through inputs (qubits in superposition) and logic gates (entanglement), collapse into low-energy solution state

Logical NAND



4. Measure "solution" from samples to form output distribution (while in *coherence*)

1. Encode qubits (*superposition*) and logic flow (*entanglement*) into quantum circuit

2. Physically HOLD mechanisms in place (exert energy)

E.g., initial (*superpositioned*) inputs for the Problem

3. Release physical hold (energy) allow system to "collapse" into stable states

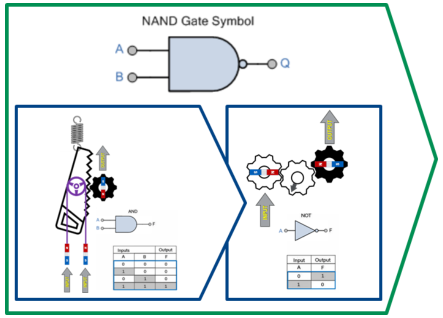
Repeat (on non-adiabatic)

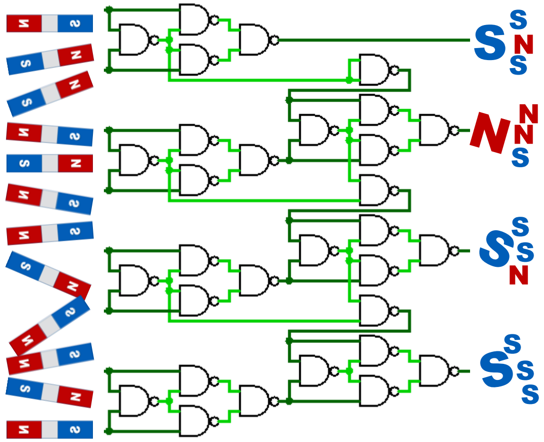
Not intended as an actual working machine: notional operation manifesting at scale of classical physics

Analogy: Magnetic + Mechanical System

(Electromagnetic force as a *spooky action at a distance*) + (Mechanically can "hold" in position before releasing)

Setup problem through inputs (qubits in superposition) and logic gates (entanglement), collapse into low-energy solution state

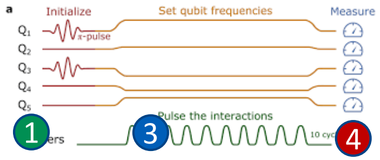




1. Encode inputs into qubits initial state and logic into quantum circuit

Superposition *Entanglement*

2. Physically HOLD mechanisms in place (exert energy)



3. Release physical hold (energy)

allow system to (*quickly ~ ns to ms*) "collapse" into stable state

Repeat (1) → (2) → (3) until completion

4. **Measure "solution"** (sample into probability distribution)

while in Coherence

Note: solution may not be optimal (locally stable) and/or difficult to verify optimality (combine multiple runs)

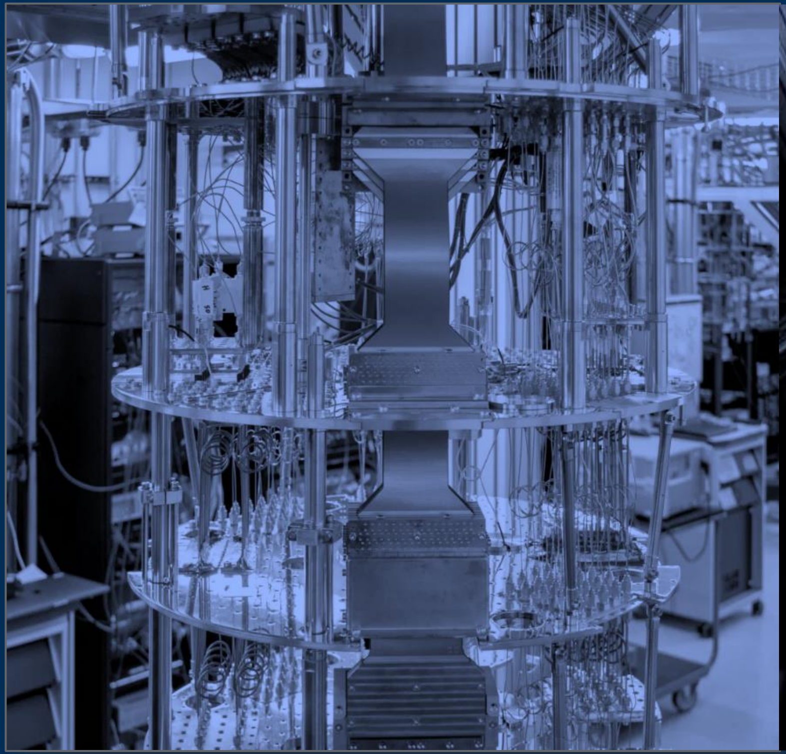
Not intended as an actual working machine: notional operation manifesting at scale of classical physics

Quantum Phenomena

Esoteric but Essential Terminology

- **Superposition**: probability distribution state between 0 and 1 in a qubit until measurement, at which point resolves the qubit’s state to either 0 or 1
- **Entanglement**: one qubit intrinsically linked (correlated) with another qubit, such that when one qubit is acted upon (measured) reveals the other qubit
- **Coherence**: durability vs. environmental interactions, (decoherence irreversibly loses ***superposition*** and/or ***entanglement***)
- **Logical qubit**: multiple *physical* qubits combined to employ quantum error correction to enhance ***coherence*** and other sources of instability and error.

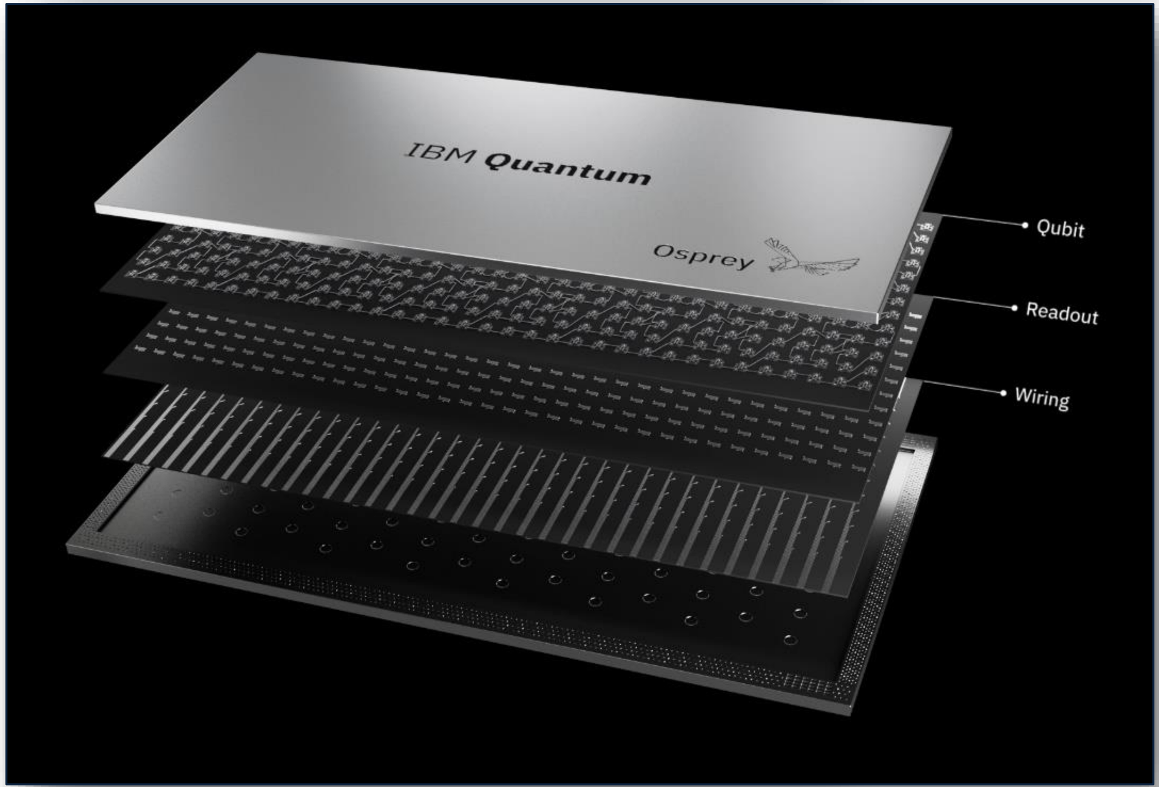
Hardware & Architectures



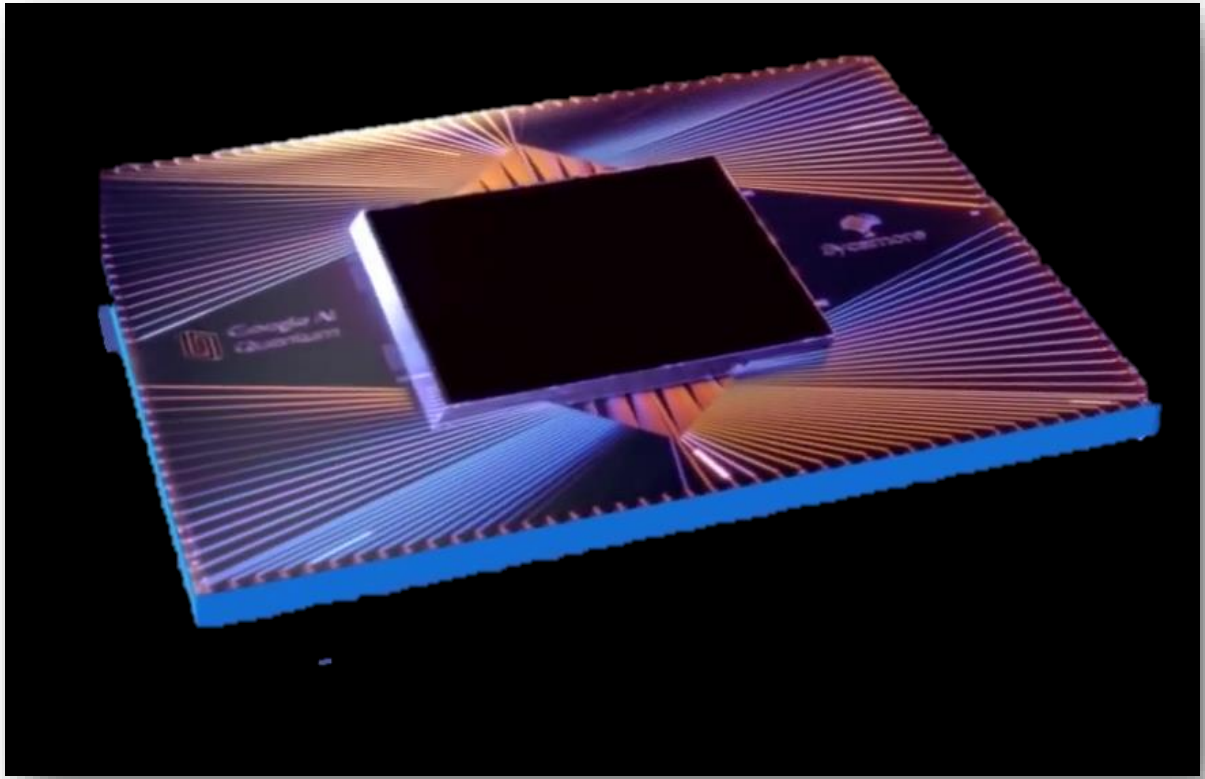

State-of-the-Art Quantum Computers

*Vacuum + cryostat refrigerator + microwave cables required (to cool the quantum chip below -272C: nearly absolute zero) to control for **noise**, resolve to minimal energy state.*

Emphasis on Qubit Scaling

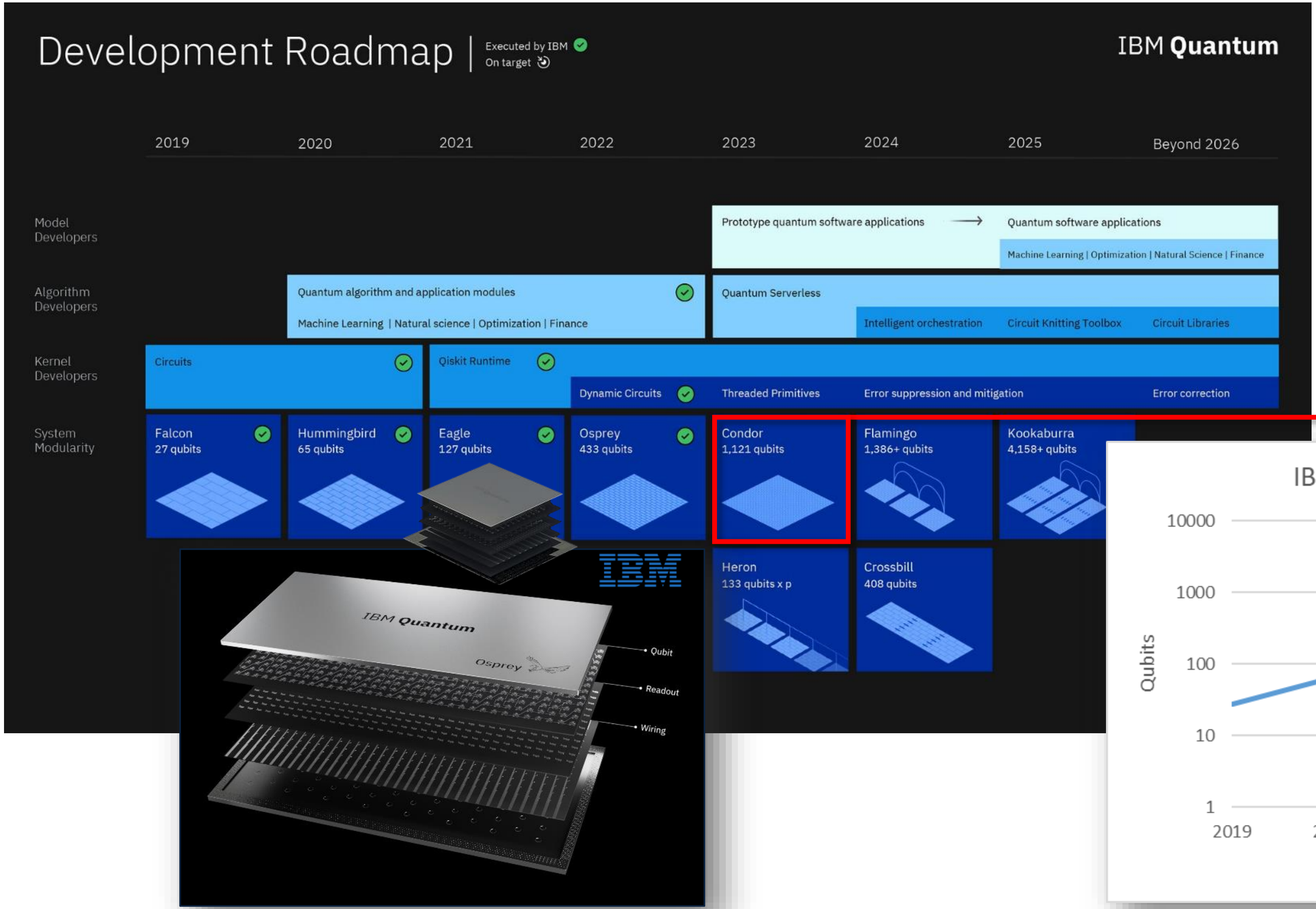


Focus on Qubit Fidelity

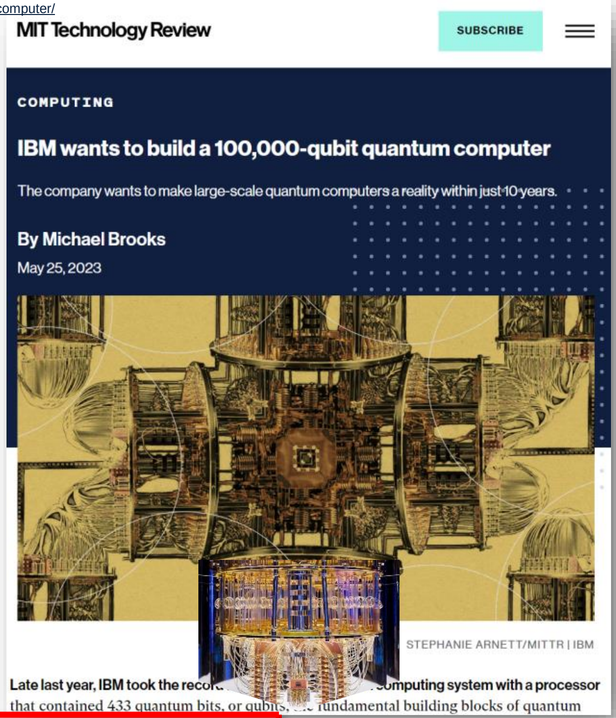


Qubit Scaling: IBM Quantum Computing Roadmap

Source: https://arstechnica.com/science/2022/11/ibm-pushes-qubit-count-over-400-with-new-processor/



https://www.technologyreview.com/2023/05/25/1073606/ibm-wants-to-build-a-100000-qubit-quantum-computer/


MIT Technology Review

SUBSCRIBE

COMPUTING

IBM wants to build a 100,000-qubit quantum computer

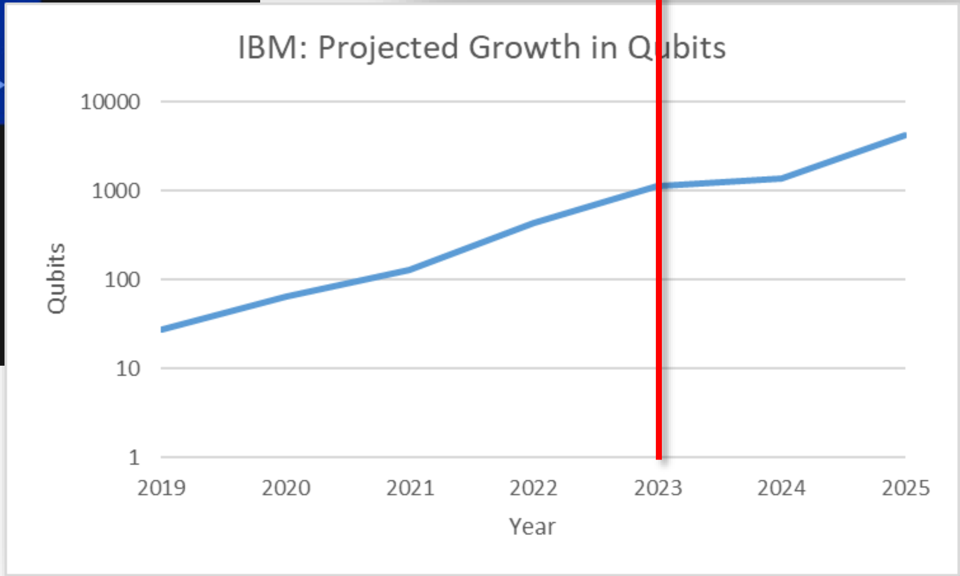
The company wants to make large-scale quantum computers a reality within just 10 years.

By Michael Brooks

May 25, 2023

STEPHANIE ARNETT/MITTR | IBM

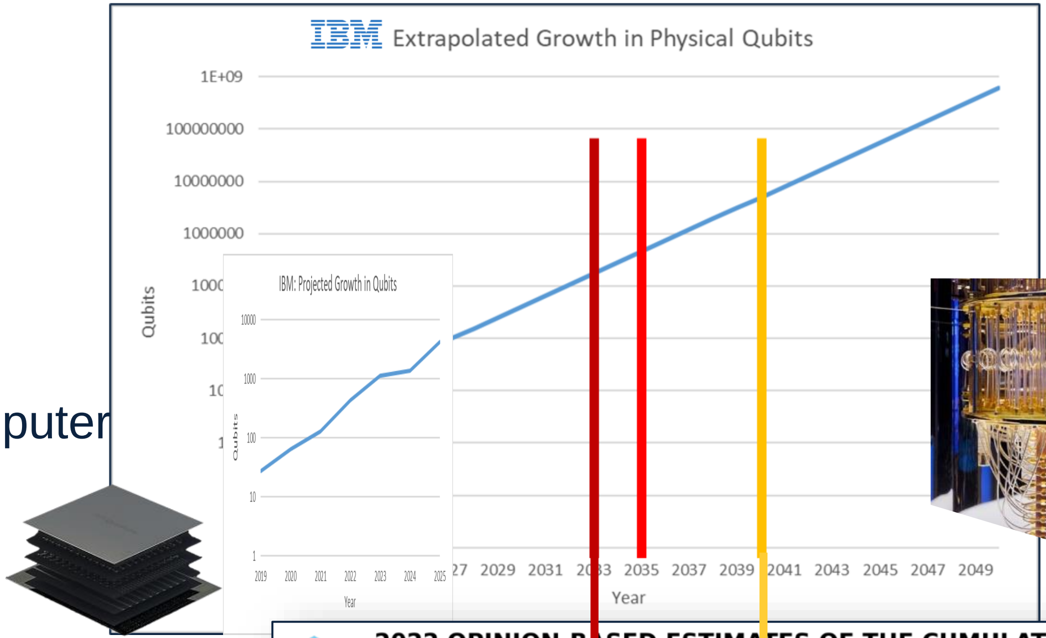
Late last year, IBM took the reco... ...omputing system with a processor that contained 433 quantum bits, or qubits, ... fundamental building blocks of quantum

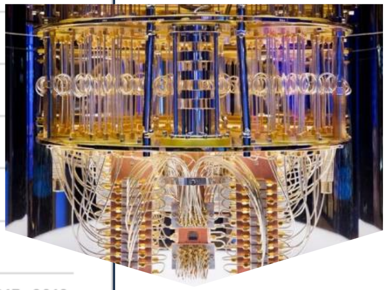


Expert Opinion on Quantum Computing Roadmap

From: GE Aerospace

Post-Quantum Cryptography Tutorial





Towards a Cryptographically Relevant Quantum Computer (CRQC) that can break RSA-2048 in 24 hours

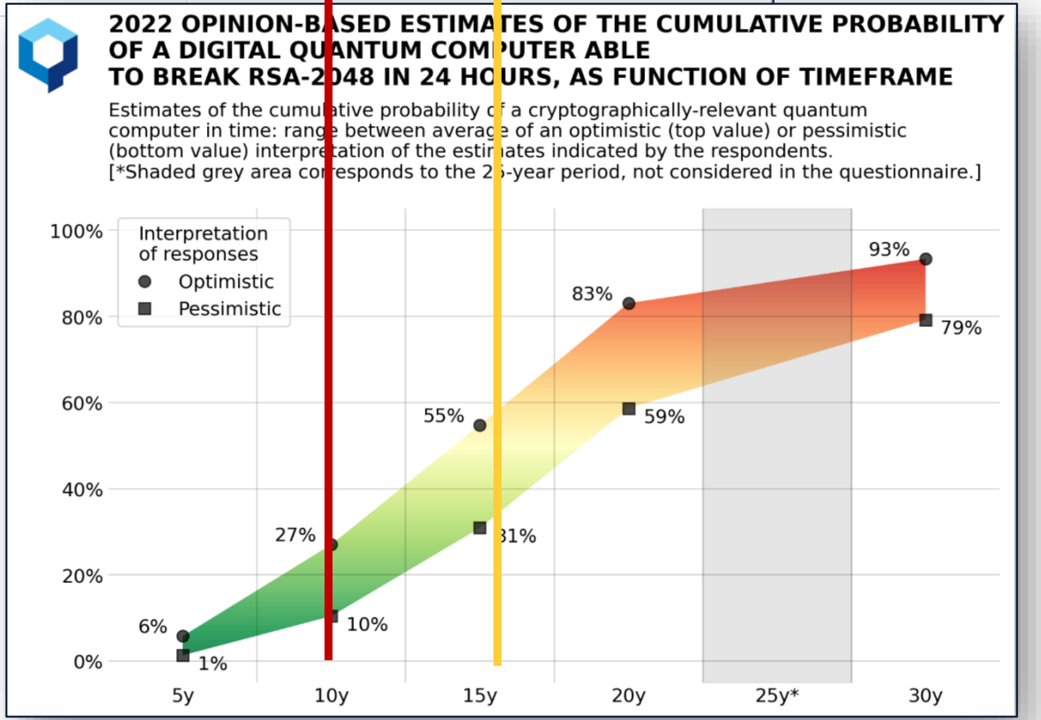
Breaking RSA

- 4096 qubits are required to factor RSA-2048
- Assume continued improvements in:
  - physical qubit error rates, and
  - quantum error correction techniques

Physical Qubits per Logical Qubit	RSA-2048 Qubits	Year of the CRQC	Enabling Technology
50	200K	2033	Improved coding & qubits
100	400K	2035	Improved qubit error rate
1000	4M	2040	IBM roadmap extrapolation

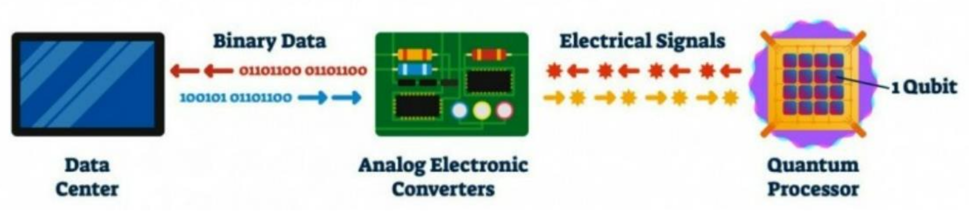
- Hence a CRQC ***may*** be viable before 2035

So many assumptions!



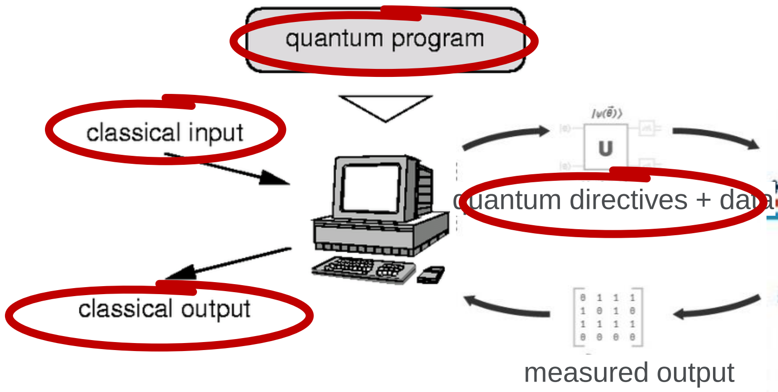
Source: M. Mosca, M. Piani, Quantum Threat Timeline Report, 2022
https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/

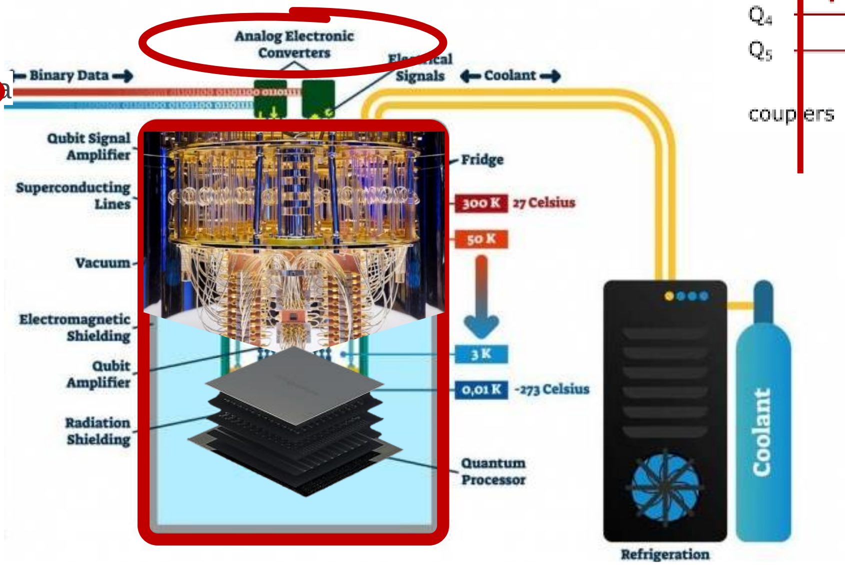
Architecture

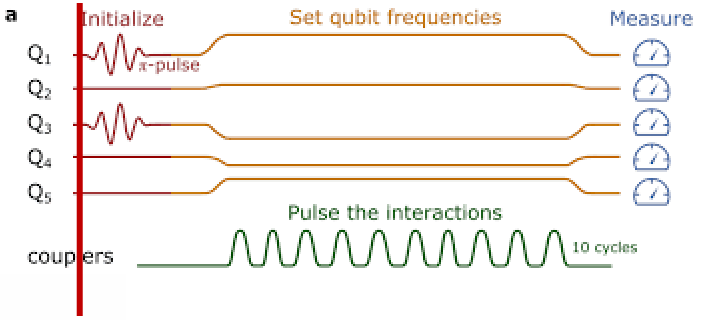


You still need a classical computer to use a quantum computer

https://www.thebroadcastbridge.com/content/entry/14159/instant-answers-from-the-universe







https://www.researchgate.net/publication/2196974_Semantics_and_simulation_of_communication_in_quantum_programming

https://ionq.com/resources/what-is-hybrid-quantum-computing

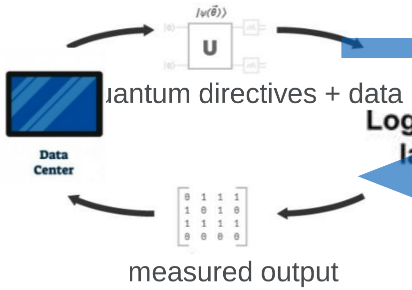
Classical: problem setup + I/O + solution analysis

Quantum: resolution of circuit vs. inputs + measurement

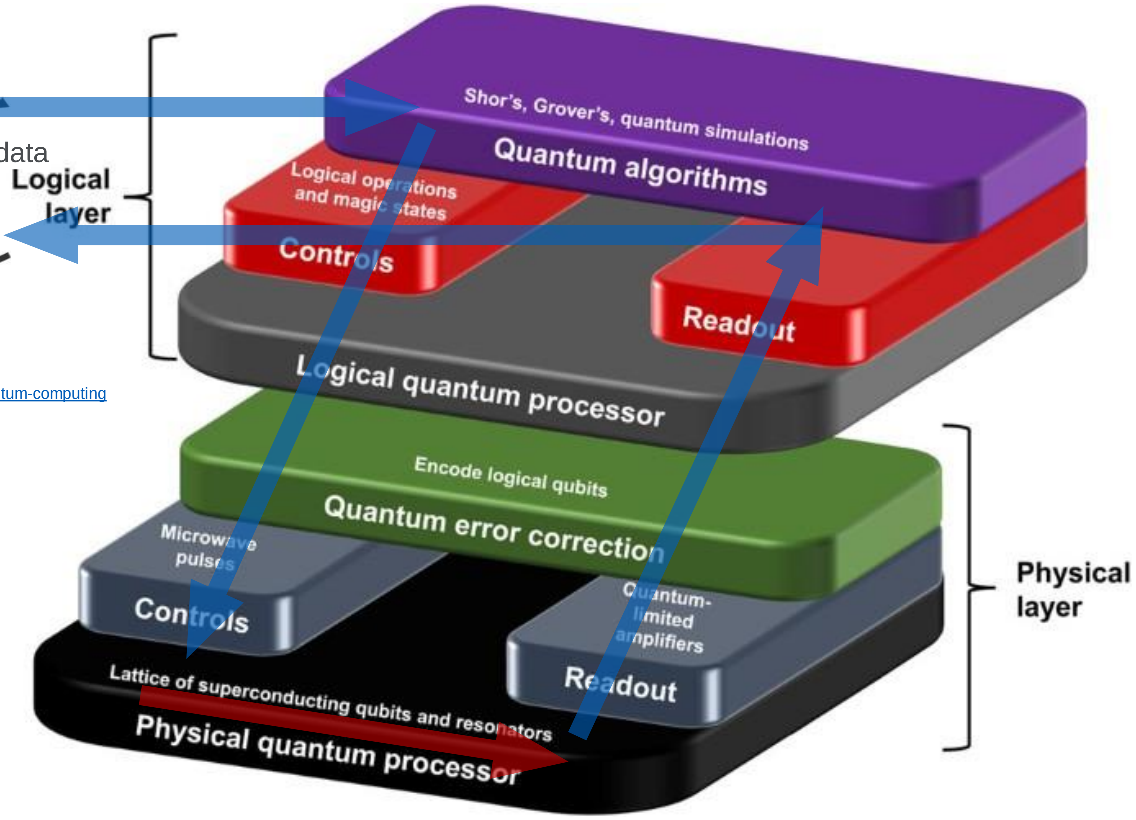
Architecture

You still need a classical computer to use a quantum computer

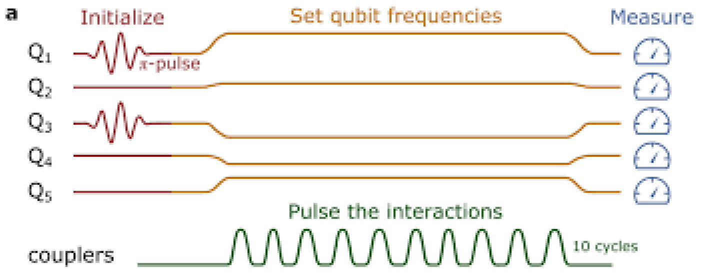
https://www.thebroadcastbridge.com/content/entry/14159/instant-answers-from-the-universe

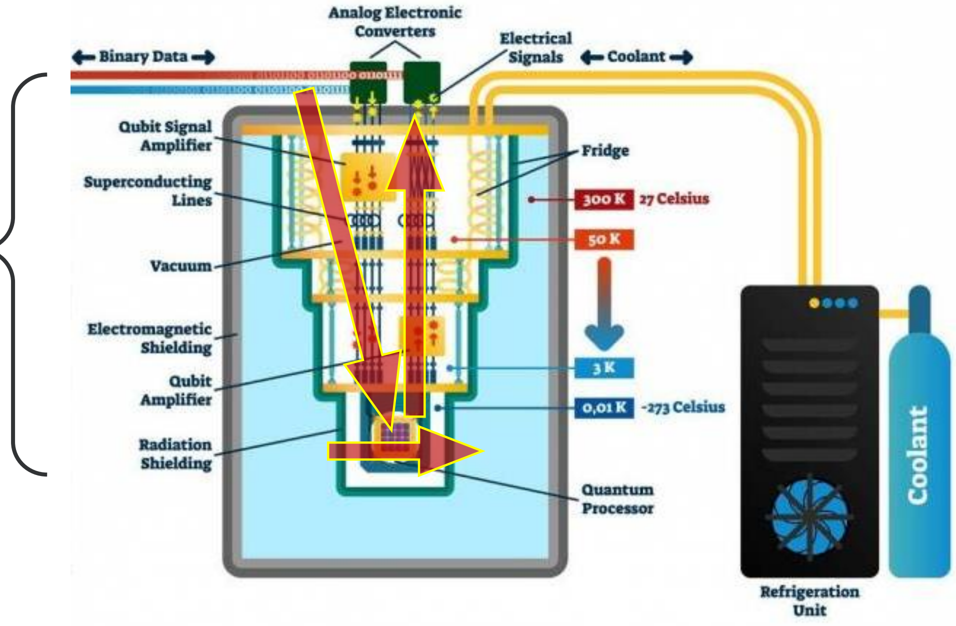


https://ionq.com/resources/what-is-hybrid-quantum-computing



https://www.nature.com/articles/s41534-016-0004-0





Hardware Architectures

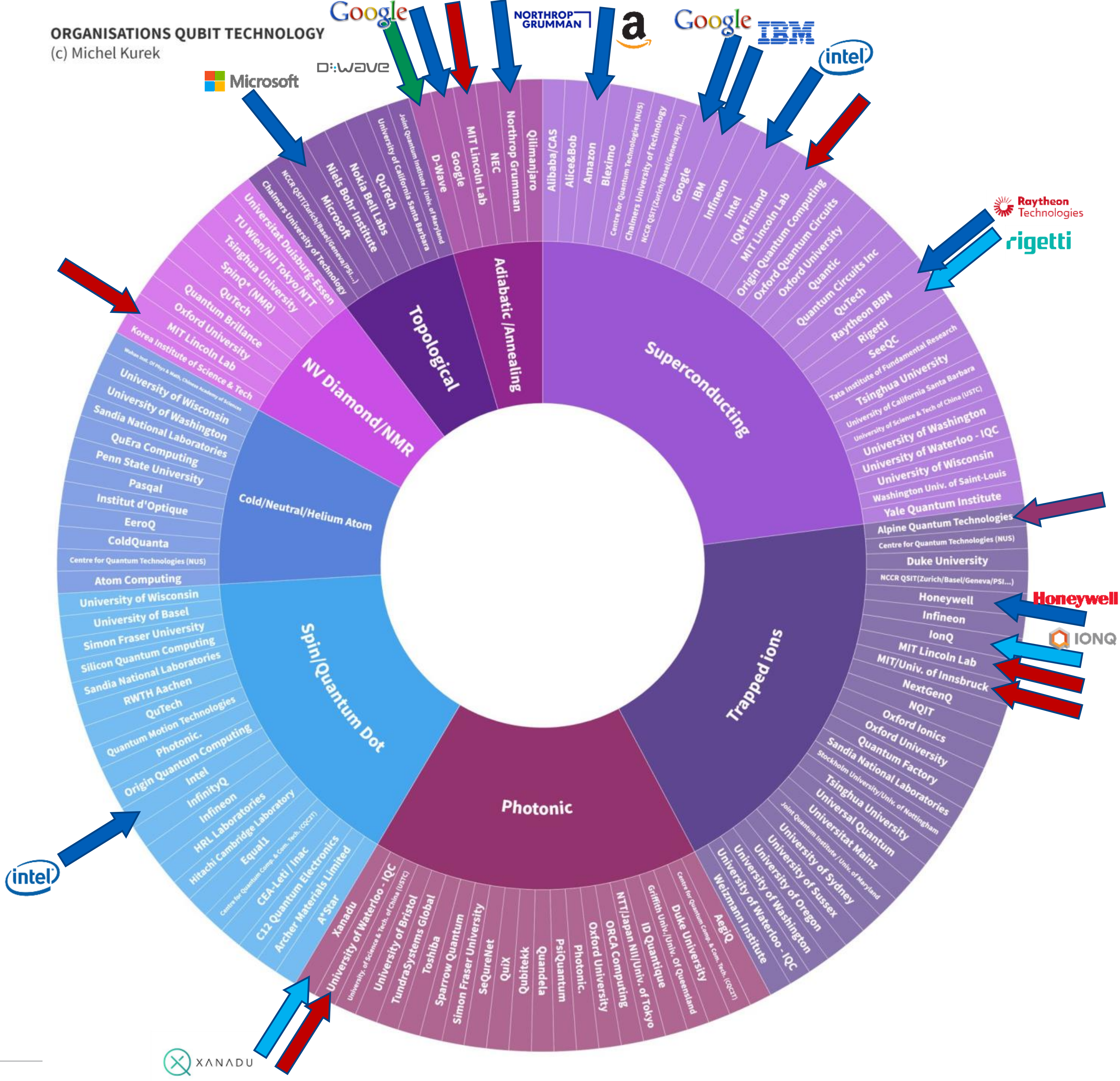
Diversity of physical approaches to superposition / entanglement / coherence

D-Wave

"The O.G."

Amazon
Google
Honeywell
IBM / UK STFC NQCC
Intel
IonQ
Microsoft
Northrop Grumman
Raytheon BBN
Rigetti
Xanadu

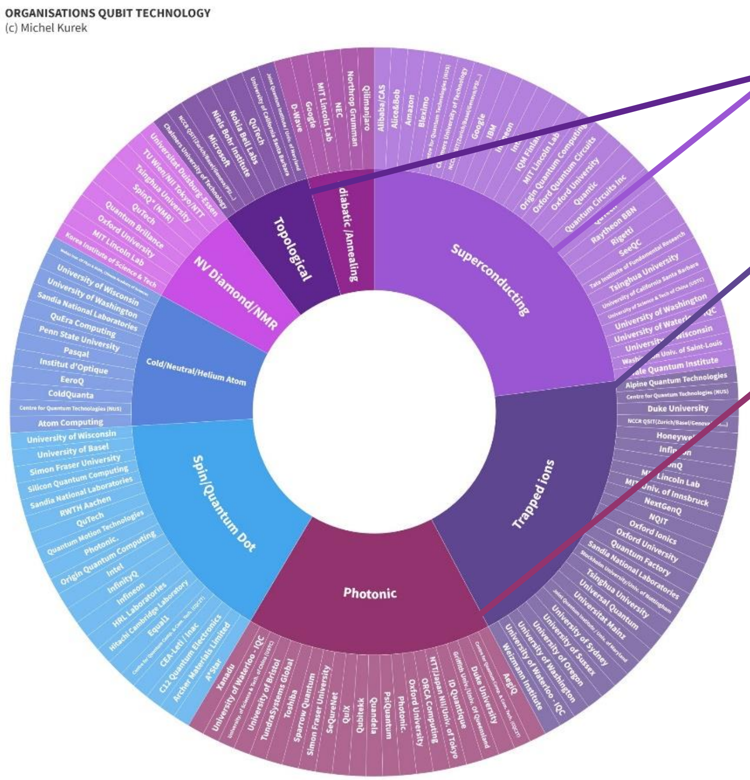
MIT Lincoln Lab
U Waterloo
U Innsbruck / AQT

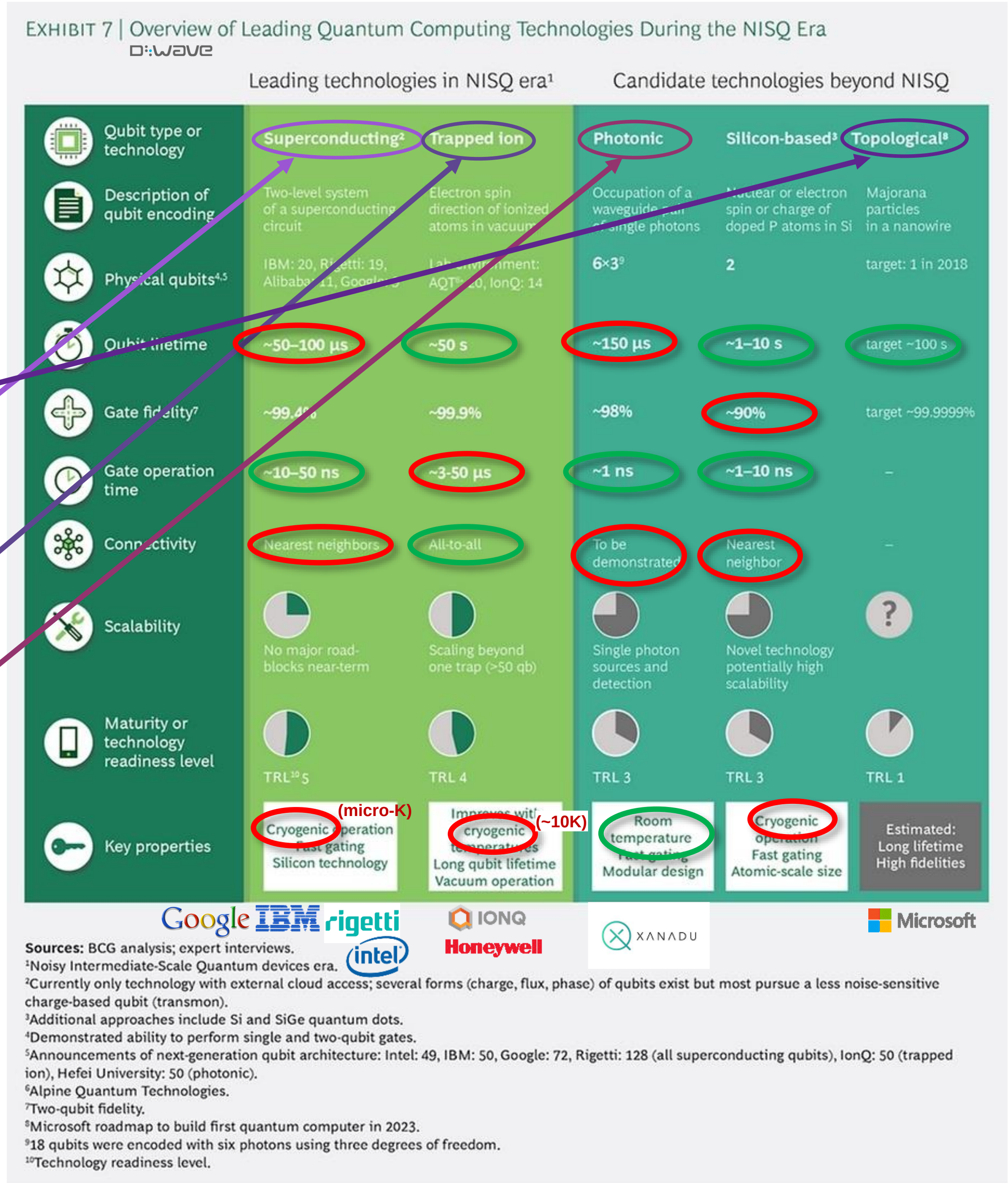


[Topics]

Hardware Architectures: *Trade-offs*

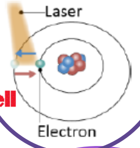
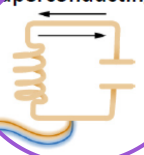
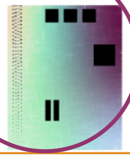
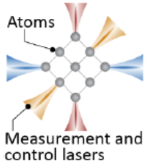
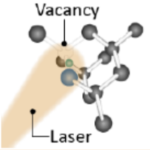
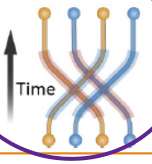
Diversity of physical approaches to
superposition / entanglement / coherence





Hardware Architectures: *"How it works / Status"*

Table 1: Example qubit technologies used in quantum computers and how they work

Qubit Technology	How it works	Status
Trapped Ion 	Single ions (charged atoms) are trapped in electric fields, or electric and magnetic fields and laser-cooled to near absolute zero, the lowest possible temperature. Trapped ion qubits are manipulated with lasers or microwave pulses.	**Size of demonstration computers:** up to a few dozen noisy qubits. **Entities with platforms available:** IonQ, Honeywell, and Sandia National Laboratory's Quantum Scientific Computing Open User Testbed, among others.
Superconducting 	An artificial atom circuit loop made of superconductors cooled to almost absolute zero. These qubits are controlled with microwave electronics and can operate quickly.	**Size of demonstration computers:** up to dozens of noisy qubits. **Entities with platforms available:** IBM, Rigetti, D-Wave,[a] Google, and Lawrence Berkeley National Laboratory's Advanced Quantum Testbed, among others.
Photonic 	Encodes qubits in light that travels through optical chips or fiber. These qubit systems can operate at room temperature but some may require technologies at near absolute zero temperatures to detect qubits.	**Size of demonstration computers:** up to dozens of noisy qubits. **Entities with platforms available:** Xanadu.
Neutral Atoms 	Neutral, or uncharged, atoms are similar to trapped ions and are controlled by lasers or microwave pulses.	**Size of demonstration computers:** up to dozens of noisy qubits. **Platform availability:** late 2021 or early 2022, according to Cold Quanta.
Quantum Dot 	An artificial atom, similar to a transistor, consisting of a small semiconducting crystal controlled with microwaves or electrical signals. Quantum dot qubits require temperatures of approximately -272 degrees Celsius—one degree above absolute zero—to operate.	**Size of demonstration computers:** a few noisy qubits. **Platform availability:** no plans announced as of June 2021.
Color Centers 	An artificial atom in diamond or another crystal composed of a defect in the crystal often created by an added atom or a vacant space. Color center qubits are controlled with light and optically detected.	**Size of demonstration computers:** up to approximately two dozen qubits. **Platform availability:** no plans announced as of March 2020.
Topological 	Topological qubits may be created by, for example, channeling electrons along the boundary between two different materials. Topological qubits are composed of "quantum braids" in time.	Not yet demonstrated.

ources: GAO analysis of a National Academies of Sciences, Engineering, and Medicine report, white papers, journal articles, and industry documents, mage Source: From 'Scientists are close to building a quantum computer that can beat a conventional one', G. Popkin, Science, December 1, 2016 doi:10.1126/science.aal0442). Redrawn and modified with permission from AAAS (all other images). Image courtesy of Oak Ridge National Laboratory, Department of Energy. Carlos Jones, Oak Ridge National Laboratory Photographer (photonic), Dana Anderson, University of Colorado Boulder (neutral atoms) | GAO-22-104422

[a] According to D-Wave, their quantum annealing machines may contain more than 5,000 qubits. However, these qubits cannot be directly compared to those in noisy quantum computers.

Source: GAO + National Academies

Software & Applications

Algorithms and Software

Classical Program Architecture

- Data Storage
  - Multi-tiered (***Massive***/Slower to Tiny/Ultrafast)
  - Data State can ***Persist*** across execution / to years
- Sequential & Parallel Pipeline Execution
- Synchronized by system “***clock***” ticks
  - ($Clock_0$) load control instruction →
  - ($Clock_1$) load inputs to function →
  - ($Clock_2$) execute function →
  - ($Clock_3$) store outputs from function →
  - ($Clock_4$) advance to next control instruction → REPEAT

Quantum Application Execution

- Data
  - classical bits: 0 (=0) or ~5 volts (=1)
  - quantum bits (“qubits”) = wave functions
- Functional Logic
  - classical gate: “clocked” transistors
  - quantum gate: wave interference
- Encode qubit superpositions
- Encode qubit entanglements
- Collapse into stable solution state → REPEAT
- Sample qubits for solution
- Critical differences vs. Classical
  - Very small size / data (unless embody as PDE)
  - Limited persistent “state” or pipeline sequential processing
  - Limited algorithms & support toolchain

Algorithms and Software

Quantum Algorithm "Zoo"

Discussion with maintainer: Stephen Jordan (Microsoft)

Algorithm Categories:

- Algebraic & Number Theoretic (e.g., Shor)
- Oracular (e.g., Grover)
- Approximation and Simulation (of Quantum Mechanics)
- Optimization, Numerics, & Machine Learning (Constraint Satisfaction)

Quantum Algorithms: A Review (Imperial College London 2021)

(Compare vs. general: Stony Brook Algorithm Repository)

Example Software Stacks

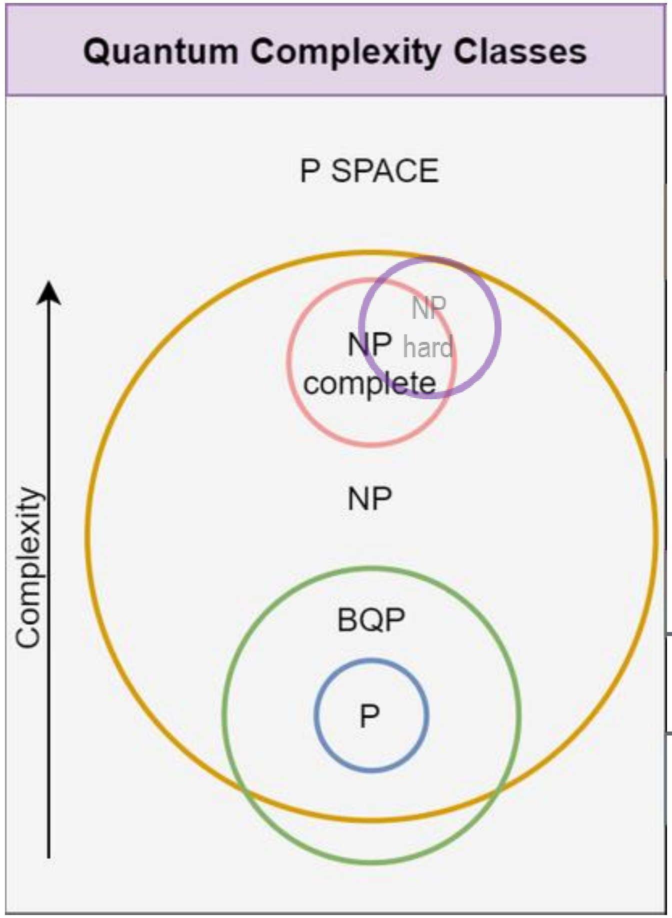
- Qiskit (IBM)
- Cirq (Google)
- Ocean (D-Wave)
- Q# and QDK (Microsoft)
- CUDA Quantum cuQuantum (NVIDIA)
- Quantum SDK (Intel)
- Forest SDK (Rigetti)
- Strawberry Fields and Penny Lane (Xanadu)

Algorithm Complexity

Persistent computer science challenge: solving problems that scale with non-polynomial complexity

HARD

EASY



MAX-CUT
3D Ising Model

Satisfiability
Sudoku
Automated Theorem Proving
Graph Coloring

Graph Isomorphism
Unknotting

Factoring
Discrete Logarithm

Primality Test
Pattern Matching
Multiplication
Adding

Notation	Name	Example problem
$O(1)$	Constant	Calculating $(-1)^n$
$O(\log n)$	Logarithmic	Binary search
$O(n)$	Linear	Linear search
$O(n \log n)$	Linearithmic	Merge sort
$O(n^2)$	Quadratic	Bubble sort
$O(n^c)$	Polynomial	AKS primality test
$O(c^n)$	Exponential	Traveling salesman problem using dynamic programming
$O(n!)$	Factorial	Traveling salesman problem using brute-force search

Quantum computing cannot overcome the exponential scaling of computational time required for NP/NP complete/NP hard problems.

Problems with polynomial scaling complexity are well-behaved in classical computing architectures.

(Clever strategies are employed to allow solution of non-worst case non-polynomial problems.)

Two Pillar Quantum Algorithms

Shor's algorithm (1994)
exponential speed-up over classical computers

- ➢ Factoring large integers (e.g., Cryptography)
- ➢ Finding discrete logarithms

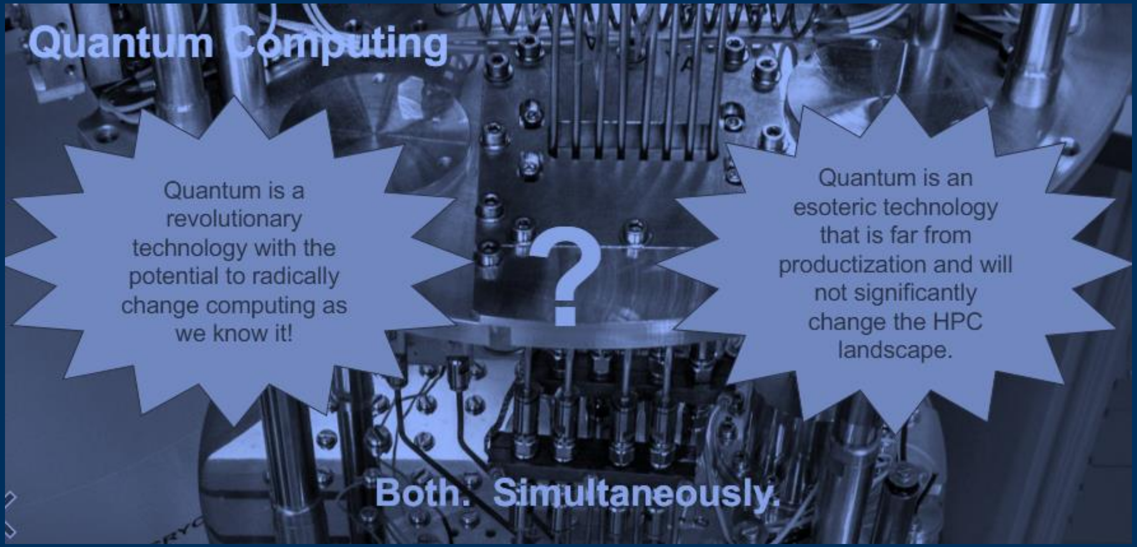
Grover's algorithm (1996)
polynomial speed-up over classical computers from O(N) to O($\sqrt{N}$)

- ➢ Unstructured Search
- ➢ Even though not exponential, advantageous for large N problems

[Topics]

From: GE Aerospace Post Quantum Cryptogrpahy Tutorial

Assessments



Cray CTO (2019) Steve Scott (now at Microsoft Azure)

Booz Allen Assessment

(Dec 2021) Booz Allen: Quantum Threats Report

Concerns: IP theft, decryption, novel quantum uses

Quantum Computers may be good at solving:

- **Factorization** (impacting public-key encryption) - hard to find pair of large prime factors / easy to confirm solution (Schor's Algorithm)
- **Optimization** (sparsity-constrained linear optimization problems - simple solution but complex dimensionality)
- **Search** (over unstructured data)
- **Simulation** (of quantum mechanical phenomena in materials, superconductivity, lasers, photosynthesis, etc.)

Common Belief	Reality
*Quantum computers are **faster or more powerful than classical computers.***	**Only sometimes**. Quantum computers can model and solve certain problems in fundamentally different ways than classical computers. These novel methods can be much more efficient. We currently only know a few, but very important types of problems that can be solved faster on quantum computers.
*Quantum computers will **replace classical computers**.*	**Unlikely**. For the foreseeable future, quantum computers will likely work alongside classical computers, solving the parts of problems most suited to quantum computing. This setup is analogous to classical computers using dedicated graphics processors (GPU) for 3D rendering, cryptocurrency mining, and video editing.
*Quantum computers are **here today.***	**Sort of**. Quantum computers exist but are very rudimentary—somewhat comparable to traditional computers in the 1940s. They can only process very short algorithms and minuscule datasets. Many challenges must be overcome in engineering, computer science, and other disciplines before they are more generally useful.
*Quantum computers will **revolutionize every field & industry.***	**Unknown**. Quantum computers' specific utility for most fields is largely theoretical. Substantial investment globally is directed toward identifying and testing novel uses for quantum computers.
*Quantum computers will **break all encryption.***	**Partially true**. Eventually, all current-generation, public-key cryptography will be vulnerable to decryption with quantum computers. This type of encryption is ubiquitous—variously securing financial transactions, stored data, and telecommunications. The quantum algorithms for breaking this encryption exist, but quantum computers capable of implementing them do not yet.

BCG https://www.bcg.com/publications/2021/building-quantum-advantage

QUANTUM COMPUTING / REPORT

What Happens When 'If' Turns to 'When' in Quantum Computing?

JULY 21, 2021

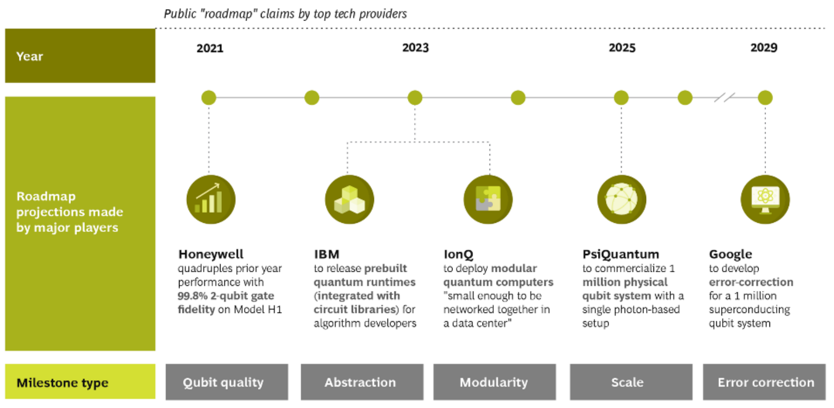
By Jean-François Bobier, Matt Langione, Edward Tao, and Antoine Gourévitch

Boston Consulting Group on Quantum Computing / see also:

- The Coming Quantum Leap in Computing (2018)
- The Next Decade in Quantum Computing—and How to Play (2018)
- Where Will Quantum Computing Create Value—and When? (2019)
- Will Quantum Computing Transform Biopharma R&D? (2019)
- A Quantum Advantage in Fighting Climate Change (2020)
- It's Time for Financial Institutions to Place Their Quantum Bets (2020)
- TED Talk: The Promise of Quantum Computers (2021)
- Ensuring Online Security in a Quantum Future (2021)

"Perhaps no previous technology has generated as much enthusiasm with as little certainty around how it ultimately will be fabricated."

Exhibit 5 - The Path to Broad Quantum Advantage over the Next Decade, According to Major Tech Providers



Sources: IBM, IonQ, desk research (Forbes, TensorFlow, Rigetti), BCG analysis.

Exhibit 6 - The Current State of Progress of the Leading Hardware Technologies

		Superconductors	Ion traps	Photonics	Quantum dots	Cold atoms
% of potential users who consider technology "promising"		61%	35%	34%	26%	16%
Qubit quality[1]	Qubit lifetime	~1 ms	~50+ s	N/A	~1-10 s	~1 s
	Gate fidelity	~99.6%	~99.9%	~99.9%	~99%	~99%
	Gate operation time	~10-50 ns	~1-50 µs	~1 ns	~1-10 ns	~100 ns
Connectivity		Nearest neighbors	All-to-all	All-to-all[2]	Nearest neighbors	Near neighbors
Strengths		✓ Engineering maturity ✓ Scalability[3]	✓ Stability ✓ Gate fidelity ✓ Connectivity	✓ Horizontal scalability ✓ Established semiconductor tech	✓ Stability ✓ Established semiconductor tech	✓ Horizontal scalability ✓ Connectivity
Challenges		× Near absolute zero temperatures × Connectivity limitation in 2D	× Gate operation times × Horizontal scaling beyond one trap	× Noise from photon loss	× Requires cryogenics × Nascent engineering	× Gate fidelity × Gate operation time
Example players		IBM, Google	Honeywell, IonQ	PsiQuantum, Xanadu	Intel, SQC	ColdQuanta, Pasqal

Sources: Expert interviews, Science, Nature, NAE Report, Hyperion Research.

[1]Best reported performance available for all dimensions.

[2]PsiQuantum publication (March 2021).

[3]IBM and Google have announced 1M qubit roadmaps for between 2025 and 2030.

Exhibit 8 - The Value of Quantum Computing Through the Three Stages of Development

	NISQ *(before 2030)*	Broad quantum advantage *(after 2030)*	Full-scale fault tolerance *(after 2040)*
Total annual value creation for end-users (in operating income)	$5B-$10B	$80B-$170B	$450B-$850B
Total annual value for providers (in revenue, ~20% of value creation)	$1B-$2B	$15B-$30B	$90B-$170B
	Before quantum advantage (2023-25), providers' revenues will stem entirely from end-user research investment. Gradually from there, user value-generating spend will take over.		Share of value creation captured by providers includes hardware, software and services. It is subject to decrease as the technology becomes a commodity.

Source: BCG analysis.

https://www.bcg.com/publications/2021/building-quantum-advantage

QUANTUM COMPUTING / REPORT

What Happens When 'If' Turns to 'When' in Quantum Computing?

JULY 21, 2021

By Jean-François Bobier, Matt Langione, Edward Tao, and Antoine Gourévitch

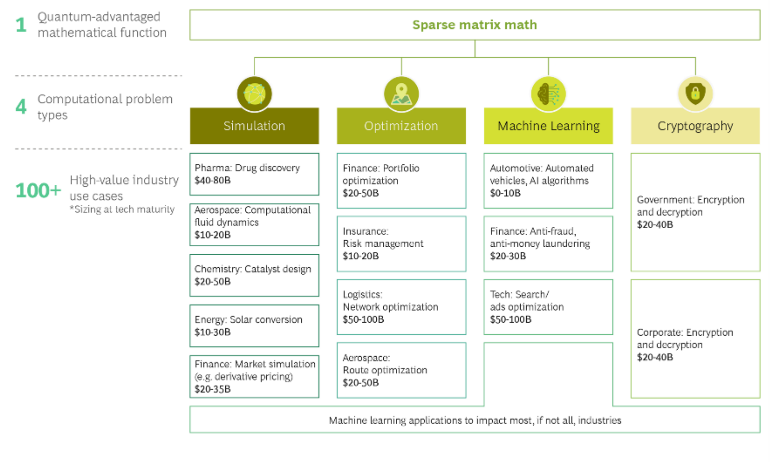
Boston Consulting Group on Quantum Computing / see also:

- The Coming Quantum Leap in Computing (2018)
- The Next Decade in Quantum Computing—and How to Play (2018)
- Where Will Quantum Computing Create Value—and When? (2019)
- Will Quantum Computing Transform Biopharma R&D? (2019)
- A Quantum Advantage in Fighting Climate Change (2020)
- It's Time for Financial Institutions to Place Their Quantum Bets (2020)
- TED Talk: The Promise of Quantum Computers (2021)
- Ensuring Online Security in a Quantum Future (2021)

Research is concentrated on the following types of computational problems:

- **Simulation**: Simulating processes that occur in nature and are difficult or impossible to characterize and understand with classical computers today. This has major potential in drug discovery, battery design, fluid dynamics, and derivative and option pricing.
- **Optimization**: Using quantum algorithms to identify the best solution among a set of feasible options. This could apply to route logistics and portfolio risk management.
- **Machine learning (ML)**: Identifying patterns in data to train ML algorithms. This could accelerate the development of artificial intelligence (for autonomous vehicles, for example) and the prevention of fraud and money-laundering.
- **Cryptography**: Breaking traditional encryption and enabling stronger encryption standards, as we detailed in a recent report.

Exhibit 2 - Four Quantum-Advantaged Problem Types Unlock Hundreds of Use Cases at Tech Maturity



Sources: Industry interviews, BCG analysis.

Exhibit 9 - How Each Type of Player Can Prepare for Quantum Advantage

Technology providers

- ☐ Maintain a clear, milestone-defined **"tech maturity" roadmap** informed by competitor benchmarks
- ☐ Determine what **core and auxiliary business model(s)** will allow you to capture the most value over time (e.g., where to play in the stack)
- ☐ Select **priority industries and use cases** to develop solutions for (and prioritize potential companies to partner with in each industry)
- ☐ Solve for the **complementary layers of the stack** (e.g., hardware companies must develop a delivery mechanism, and software companies must develop a provisioning strategy)
- ☐ Develop an **engagement and ecosystem strategy**

End users

- ☐ Conduct an **impact of quantum ("IQ") assessment**
  - **Workflow analysis** to discover pain points and bottlenecks that lead to cost outlays and missed revenue opportunities
  - **Solution mapping** to identify how these pain points can be mitigated with quantum computing
  - **Path to value assessment** estimating the potential value created at critical breakpoints as the tech matures
- ☐ **Partner with a vendor** to benefit from IP, skills development and implementation readiness
- ☐ Incorporate quantum computing into your **digital transformation roadmap**

Potential investors

- ☐ Invest the time to **understand the technology** and types of industry problems it can uniquely address
- ☐ Get a complete picture of the **market landscape and value flows**
  - Value creation
  - Value capture (division of value among providers and users, by layer of the tech stack)
- ☐ Conduct a comprehensive **risk burndown**
  - Timeline
  - Hardware uncertainty (ions vs. superconductors)
  - Compute and non-compute alternatives
- ☐ Do thorough **diligence** into investment hypotheses and targets

Source: BCG analysis.

Tech Providers, especially hardware makers, should

- develop (or maintain) a clear milestone-defined quantum maturity roadmap informed by competitor benchmarks and intelligence.
- determine the business model(s) that will allow them to capture the most value over time
- develop an engagement and ecosystem strategy and prioritize the industries, use cases, and potential partners in each sector where they see the greatest opportunities for value. These opportunities will evolve over time based on the actions of other players, so early movers will have the most open playing field.

End Users should

- start now with an impact of quantum (IQ) assessment [to] map potentially quantum-advantaged solutions to issues or processes in their businesses
- assess the value and costs associated with building a quantum capability
- incorporate quantum computing into their digital transformation roadmaps.

References re: Supremacy & Hype

Videos

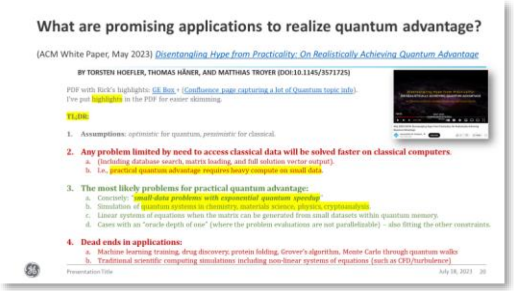
- The Quantum Hype Bubble: Sabine Hossenfelder (YouTube video, Nov-2022)
- Short-take: Quantum Computing Myths (IBM)

Assessments

- (Jun 2021) Quantum Computing 40 Years Later - Preskill (arXiv:2106.10522v3)
- (Sep 2022) State of Quantum Computing: Building a Quantum Economy (World Economic Forum)
- (Oct 2021) Tech Assessment: Quantum Computing and Communications / Status and Prospects
  US General Accountability Office (GAO)
- (April 2022) Quantum Threat Timeline Research Report (EvolutionQ)

Opinions

- (May 2023) Disentangling Hype from Practicality: On Realistically Achieving Quantum Advantage



What are promising applications to realize quantum advantage?

(ACM White Paper, May 2023) Disentangling Hype from Practicality: On Realistically Achieving Quantum Advantage

BY TORSTEN HOEFLER, THOMAS HÄNER, AND MATTHIAS TROYER (DOI:10.1145/3571725)

PDF with Rick's highlights: GE Box + (Confluence page capturing a lot of Quantum topic info).
I've put highlights in the PDF for easier skimming.

TL;DR:

1. Assumptions: optimistic for quantum, pessimistic for classical.
2. Any problem limited by need to access classical data will be solved faster on classical computers.
   a. (Including database search, matrix loading, and full solution vector output).
   b. I.e., practical quantum advantage requires heavy compute on small data.
3. The most likely problems for practical quantum advantage:
   a. Concisely: "small-data problems with exponential quantum speedup"
   b. Simulation of quantum systems in chemistry, materials science, physics, cryptoanalysis.
   c. Linear systems of equations when the matrix can be generated from small datasets within quantum memory.
   d. Cases with an "oracle depth of one" (where the problem evaluations are not parallelizable) – also fitting the other constraints.
4. Dead ends in applications:
   a. Machine learning training, drug discovery, protein folding, Grover's algorithm, Monte Carlo through quantum walks
   b. Traditional scientific computing simulations including non-linear systems of equations (such as CFD/turbulence)

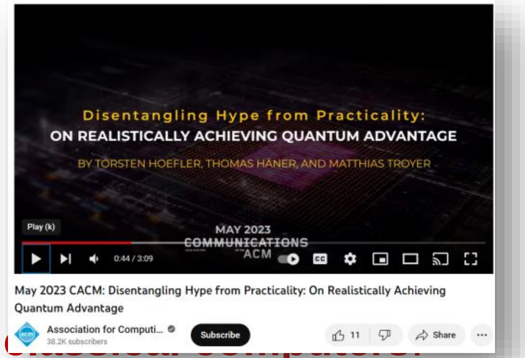
Presentation Title July 18, 2023 20

- (May 2023) Quantum Computers: what are they good for? For now, absolutely nothing (Nature)
- (Sep 2021) Scott Aaronson: Quantum Computational Supremacy (ACM Tech Talk)
- (Mar 2018) Quantum Computing vs. Our 'Caveman Newtonian Brain': Why Quantum Is So Hard (HPCwire)

What are promising applications to realize quantum advantage?

(ACM White Paper, May 2023) [*Disentangling Hype from Practicality: On Realistically Achieving Quantum Advantage*]

BY TORSTEN HOEFLER, THOMAS HÄNER, AND MATTHIAS TROYER (DOI:10.1145/3571725)



TL;DR:

1. **Assumptions**: *optimistic* for quantum, *pessimistic* for classical.

2. **Any problem limited by need to access classical data will be solved faster on classical computers.**
   a. (Including database search, matrix loading, and full solution vector output).
   b. I.e., practical quantum advantage requires heavy compute on small data.

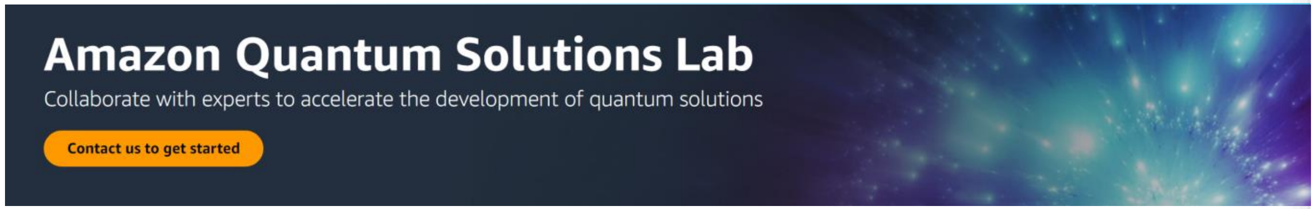
3. **The most likely problems for practical quantum advantage:**
   a. Concisely: "***small-data problems with exponential quantum speedup***"
   b. Simulation of quantum systems in chemistry, materials science, quantum physics, cryptoanalysis.
   c. Linear systems of equations when the matrix can be generated from small datasets within quantum memory.
   d. Cases with an "oracle depth of one" (where the problem evaluations are not parallelizable) – also fitting the other constraints.

4. **Dead ends in applications:**
   a. Machine learning training, drug discovery, protein folding, Grover's algorithm, Monte Carlo through quantum walks
   b. Traditional scientific computing simulations including non-linear systems of equations (such as CFD/turbulence)

AWS Exhaustive Survey

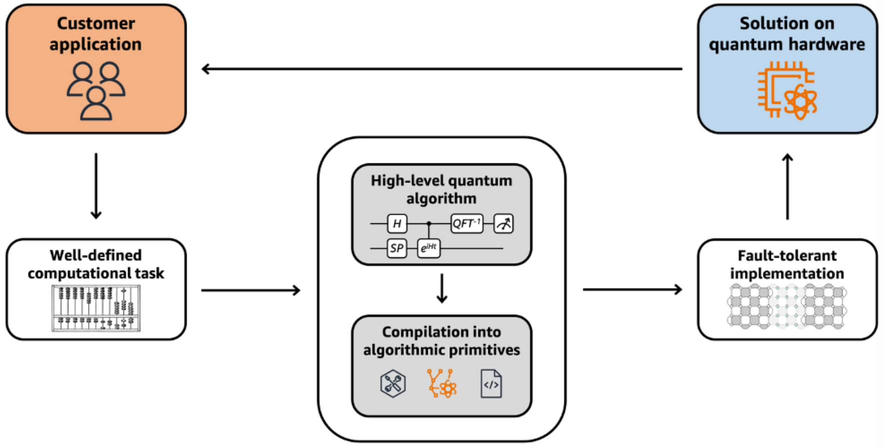
(296 pages plus Bibliography references)

https://arxiv.org/pdf/2310.03011.pdf



https://aws.amazon.com/blogs/quantum-computing/constructing-end-to-end-quantum-algorithm/

Areas of application
Condensed matter physics
Quantum chemistry
Nuclear and particle physics
Combinatorial optimization (Grover)
Continuous optimization
Cryptanalysis
Solving differential equations
Finance
Machine Learning w/ Classical Data
Quantum linear algebra
Hamiltonian simulation
Quantum Fourier transform
Quantum phase estimation
Amplitude estimation .
Gibbs sampling
Quantum adiabatic algorithm
Loading classical data
Quantum linear system solvers
Quantum gradient estimation
Variational quantum algorithms
Quantum tomography
Quantum interior point methods
Multiplicative weights update method
Approximate tensor network



Quantum algorithms:

A survey of applications and end-to-end complexities

Alexander M. Dalzell*[1], Sam McArdle*[1], Mario Berta[1,2,3], Przemyslaw Bienias[1], Chi-Fang Chen[1,4], András Gilyén[5], Connor T. Hann[1], Michael J. Kastoryano[1,6], Emil T. Khabiboulline[1,7], Aleksander Kubica[1], Grant Salton[1,4,8], Samson Wang[1,3] and Fernando G. S. L. Brandão[1,4]

[1] *AWS Center for Quantum Computing, Pasadena, CA, USA*
[2] *Institute for Quantum Information, RWTH Aachen University, Aachen, Germany*
[3] *Imperial College London, London, UK*
[4] *Institute for Quantum Information and Matter, Caltech, Pasadena, CA, USA*
[5] *Alfréd Rényi Institute of Mathematics, Budapest, Hungary*
[6] *IT University of Copenhagen, Copenhagen, Denmark*
[7] *Department of Physics, Harvard University, Cambridge, MA, USA*
[8] *Amazon Quantum Solutions Lab, Seattle, WA, USA*

Abstract

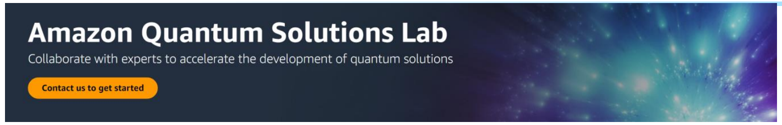
The anticipated applications of quantum computers span across science and industry, ranging from quantum chemistry and many-body physics to optimization, finance, and machine learning. Proposed quantum solutions in these areas typically combine multiple quantum algorithmic primitives into an overall quantum algorithm, which must then incorporate the methods of quantum error correction and fault tolerance to be implemented correctly on quantum hardware. As such, it can be difficult to assess how much a particular application benefits from quantum computing, as the various approaches are often sensitive to intricate technical details about the underlying primitives and their complexities. Here we present a survey of several potential application areas of quantum algorithms and their underlying algorithmic primitives, carefully considering technical caveats and subtleties. We outline the challenges and opportunities in each area in an "end-to-end" fashion by clearly defining the problem being solved alongside the input-output model, instantiating all "oracles," and spelling out all hidden costs. We also compare quantum solutions against state-of-the-art classical methods and complexity-theoretic limitations to evaluate possible quantum speedups.

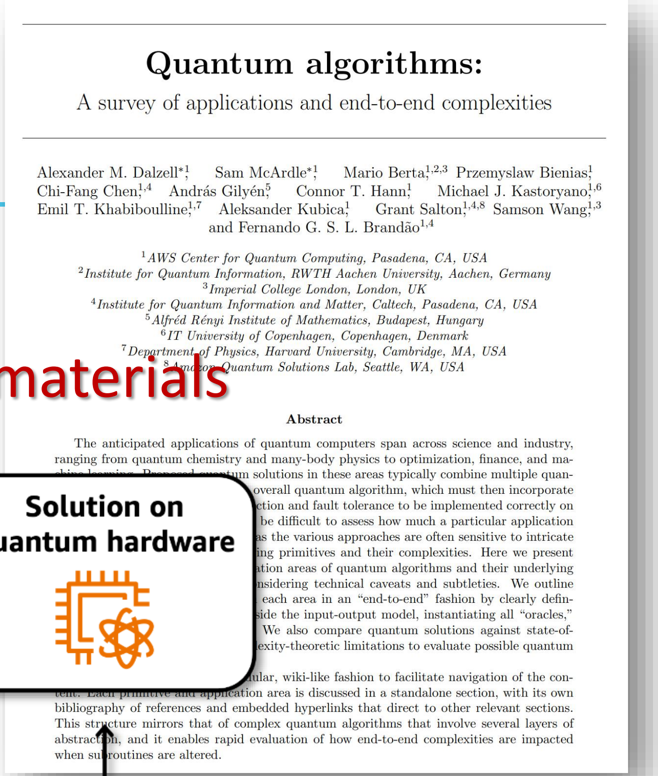
The survey is written in a modular, wiki-like fashion to facilitate navigation of the content. Each primitive and application area is discussed in a standalone section, with its own bibliography of references and embedded hyperlinks that direct to other relevant sections. This structure mirrors that of complex quantum algorithms that involve several layers of abstraction, and it enables rapid evaluation of how end-to-end complexities are impacted when subroutines are altered.

AWS Exhaustive Survey

(296 pages plus Bibliography references)

https://arxiv.org/pdf/2310.03011.pdf





Quantum algorithms:

A survey of applications and end-to-end complexities

Alexander M. Dalzell*[1], Sam McArdle*[1], Mario Berta[1,2,3], Przemyslaw Bienias[1], Chi-Fang Chen[1,4], András Gilyén[5], Connor T. Hann[1], Michael J. Kastoryano[1,6], Emil T. Khabiboulline[1,7], Aleksander Kubica[1], Grant Salton[1,4,8], Samson Wang[1,3] and Fernando G. S. L. Brandão[1,4]

[1] *AWS Center for Quantum Computing, Pasadena, CA, USA*
[2] *Institute for Quantum Information, RWTH Aachen University, Aachen, Germany*
[3] *Imperial College London, London, UK*
[4] *Institute for Quantum Information and Matter, Caltech, Pasadena, CA, USA*
[5] *Alfréd Rényi Institute of Mathematics, Budapest, Hungary*
[6] *IT University of Copenhagen, Copenhagen, Denmark*
[7] *Department of Physics, Harvard University, Cambridge, MA, USA*
[8] *Amazon Quantum Solutions Lab, Seattle, WA, USA*

Abstract

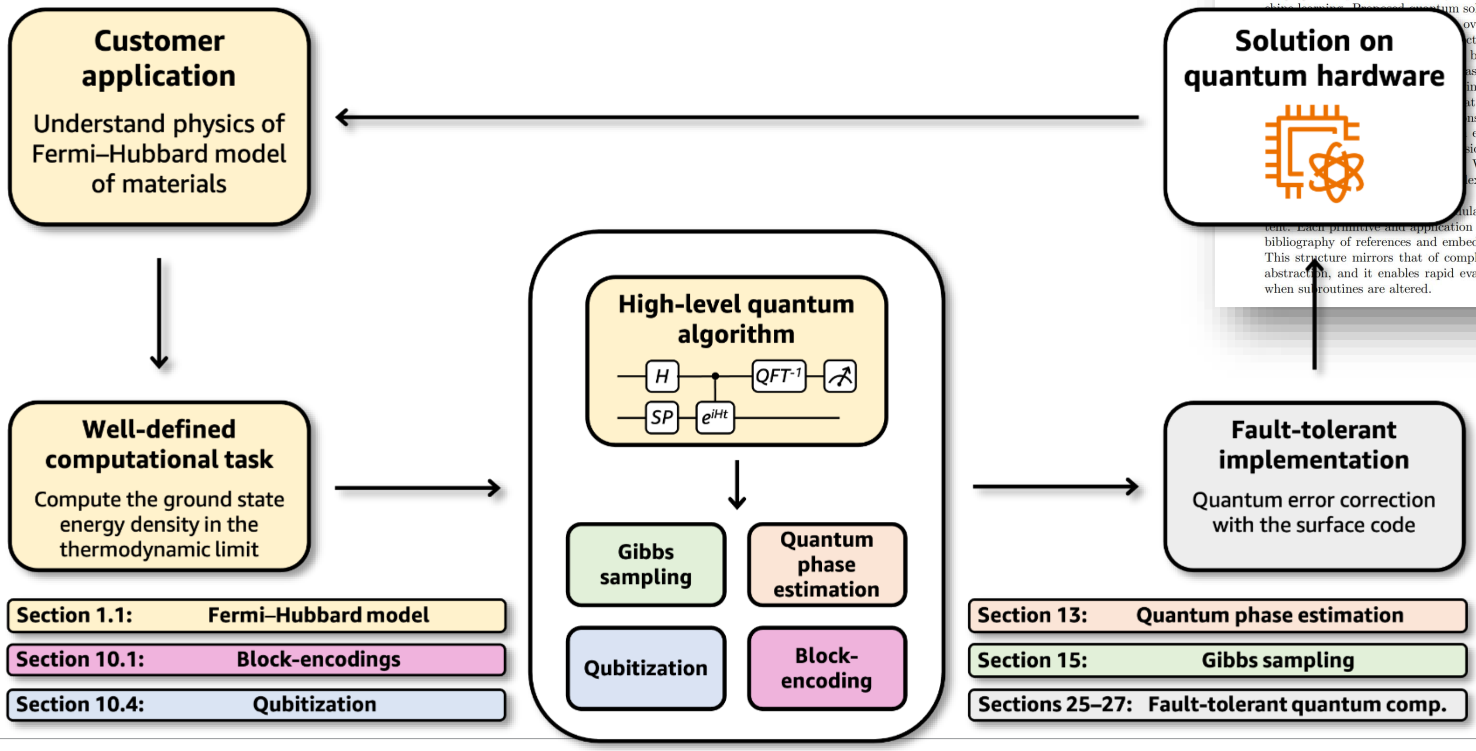
The anticipated applications of quantum computers span across science and industry, ranging from quantum chemistry and many-body physics to optimization, finance, and ma-
…um solutions in these areas typically combine multiple quan-
…overall quantum algorithm, which must then incorporate
…ction and fault tolerance to be implemented correctly on
…be difficult to assess how much a particular application
…as the various approaches are often sensitive to intricate
…ing primitives and their complexities. Here we present
…ation areas of quantum algorithms and their underlying
…nsidering technical caveats and subtleties. We outline
…each area in an "end-to-end" fashion by clearly defin-
…side the input-output model, instantiating all "oracles,"
…We also compare quantum solutions against state-of-
…lexity-theoretic limitations to evaluate possible quantum

…ular, wiki-like fashion to facilitate navigation of the con-
…ation area is discussed in a standalone section, with its own bibliography of references and embedded hyperlinks that direct to other relevant sections. This structure mirrors that of complex quantum algorithms that involve several layers of abstraction, and it enables rapid evaluation of how end-to-end complexities are impacted when subroutines are altered.

EXAMPLE: Fermi–Hubbard model of electrons in materials

https://aws.amazon.com/blogs/quantum-computing/constructing-end-to-end-quantum-algorithm/

Areas of application
Condensed matter physics
Quantum chemistry
Nuclear and particle physics
Combinatorial optimization (Grover)
Continuous optimization
Cryptanalysis
Solving differential equations
Finance
Machine Learning w/ Classical Data
Quantum linear algebra
Hamiltonian simulation
Quantum Fourier transform
Quantum phase estimation
Amplitude estimation .
Gibbs sampling
Quantum adiabatic algorithm
Loading classical data
Quantum linear system solvers
Quantum gradient estimation
Variational quantum algorithms
Quantum tomography
Quantum interior point methods
Multiplicative weights update method
Approximate tensor network



Actionable Strategy for Quantum Adoption Readiness

(Derived from discussions between Peter Lorraine & Rick Arthur)

Map GE Problems to Quantum Technology Readiness Levels

Caveat

If we believe we are now in a regime where we have stopped repeating the annual statement "*Quantum Computing is only 10 years off*" and this technology is maturing to be feasible in a relevant timeframe.

Goal

Better inform decision-makers regarding potential impact and adoption timelines, rather than reacting speculatively.

(Right now, the IBM QE can do toy problems through a Jupyter notebook API. But current QC capability is comparable to computers pre-1950).

Result

Similar to the NIST's Quantum Zoo (link) – we select critical problems for GE and corresponding characterizations that adequately describe the minimum required quantum computing technology to apply to those problems.

This then becomes a watch-list for "trigger points" to usefulness on problems, and reference as the capabilities offered through the IBM Quantum Experience (or Google, Microsoft, Intel, etc.) advance.

Underlying component: Quantum Computing Readiness Estimator

This need not be a simulator – it only needs to be a model that can:

1. **INPUT**: a problem of interest – it could be something we do already using traditional computing methods and algorithms,
   or something we cannot feasibly compute presently, but can at least state parameters for the next steps
2. **MODEL**: the tool then characterizes the problem's requirements in the context of a quantum architecture – it could range from the D-Wave quantum annealing device to weighing attributes of the quantum computer (has_entaglement, has_coherence, has_error-correction, …) – and possibly also notate unknowns or limitations
3. **OUTPUT**: description of the minimal capability of a quantum computer necessary to be applied on the problem input

Example: input a description of a 20-degrees of freedom search space, output is "QC with 85 error-corrected qubits, full entanglement – solution will not be provably optimal"

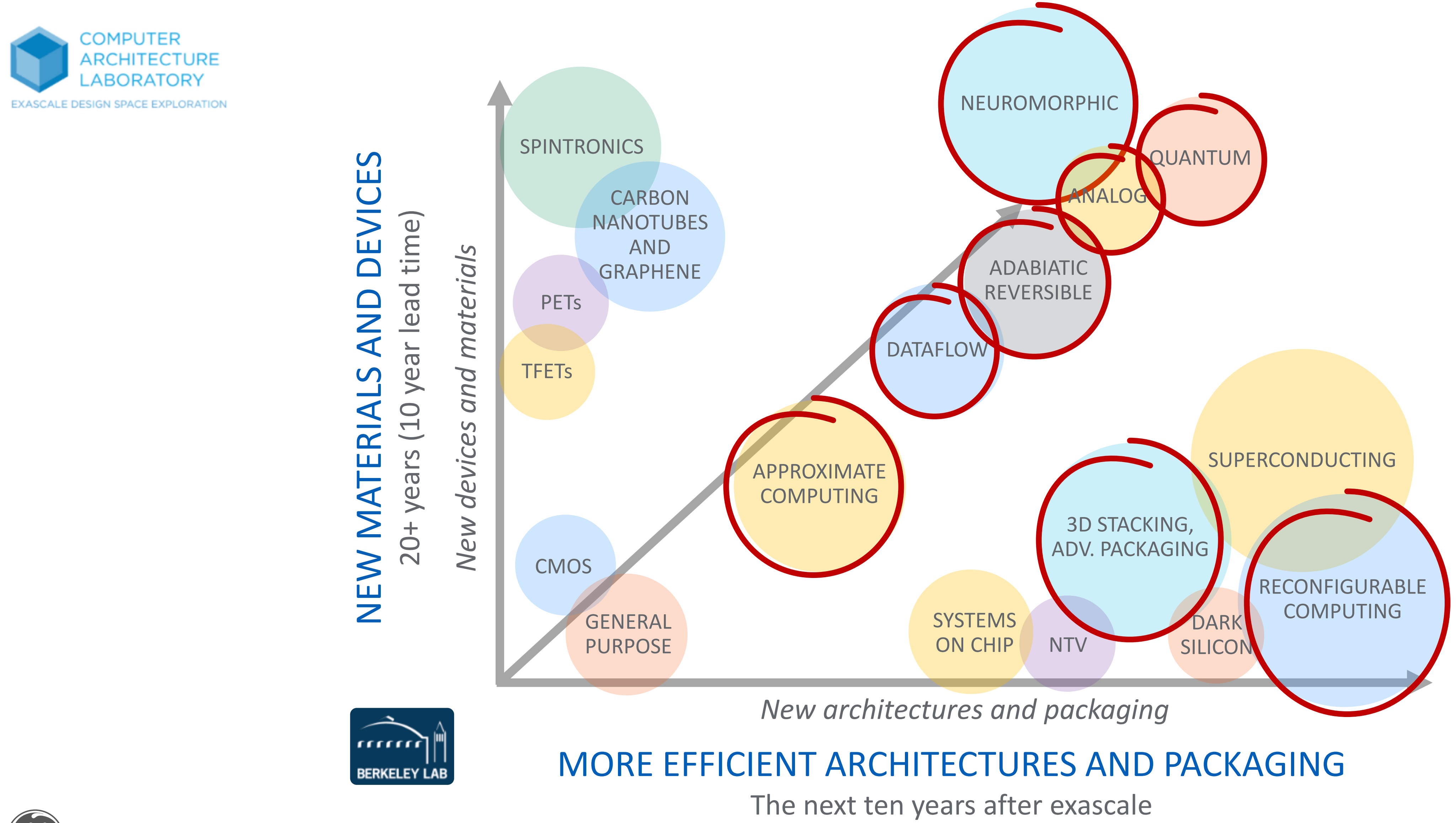
It may not make sense for GE to build this vs. somehow coax it out of someone else (IBM, Intel, Microsoft, Google, NASA, DOE, etc.).

Rick has suggested the idea to leaders at the National Science Foundation (NSF) and DOE Office of Science.

[Topics]

Alternatives

Computing Architecture Alternatives

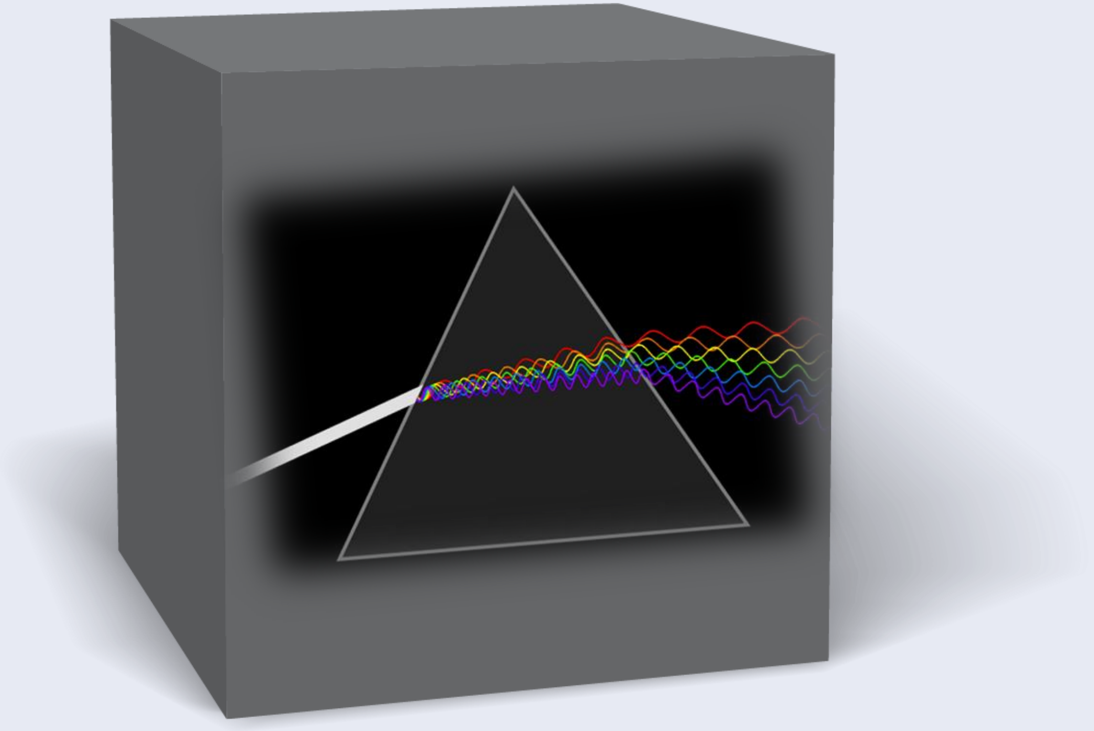


[Topics]

Going Beyond Digital

[Topics]

Analog



[Topics]

See also: Analog Computing

Input/Output: Still Digital

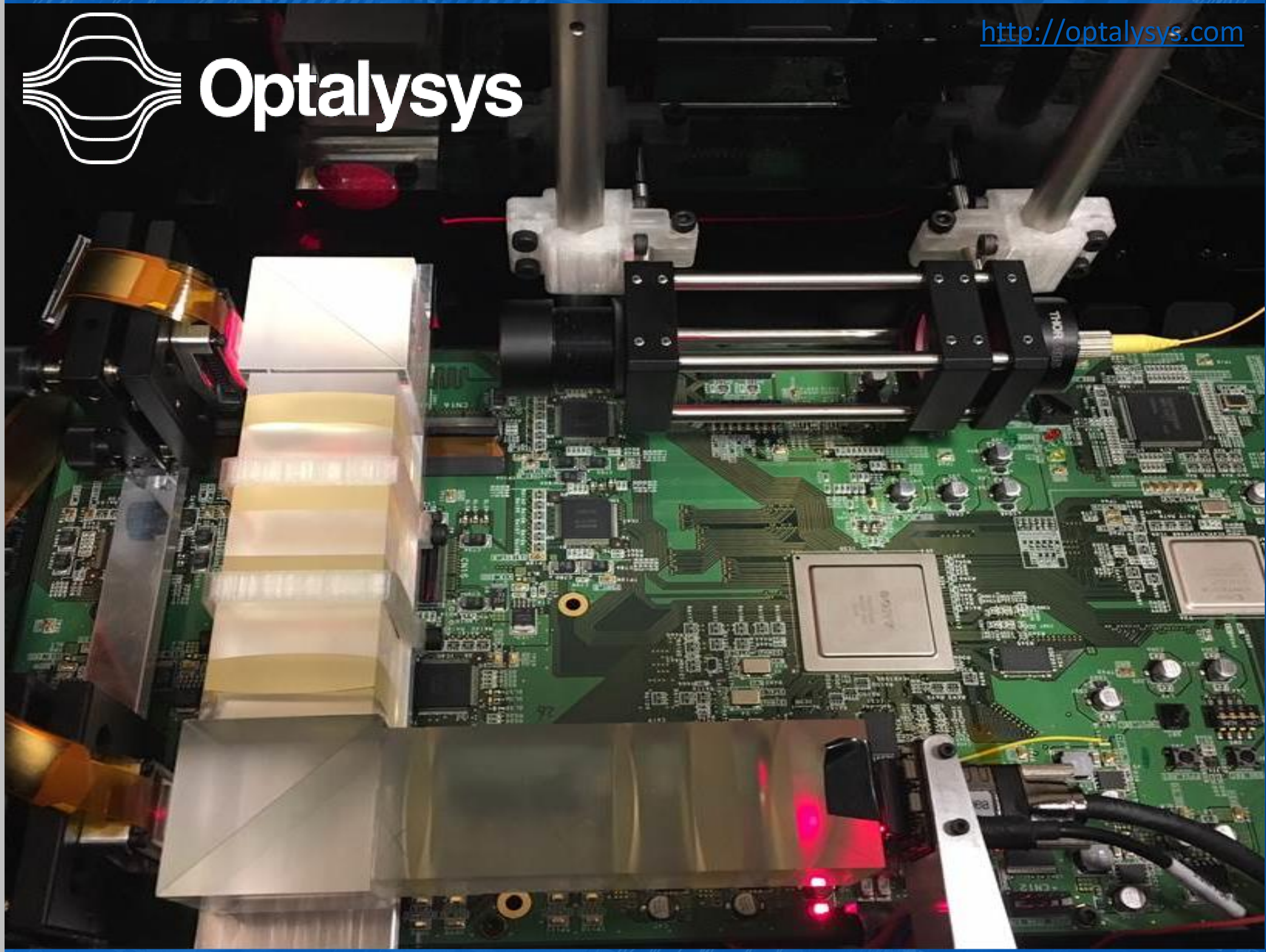
OPTICAL PROCESSING

Lightmatter

LIGHTELLIGENCE

MYTHIC

[Topics]



http://optalysys.com

See also: Analog Computing

COGNITIVE & NEUROMORPHIC PROCESSORS

RAIN

cerebras

groq

SambaNova SYSTEMS

Quadric

Graphcore

Numenta

[Topics]

MEMS / NEMS DEVICES

PROBABILISTIC COMPUTING

E.g., MIT Probabilistic Computing Project (http://probcomp.csail.mit.edu/)
An optical parametric oscillator (OPO), which is essentially a pair of mirrors that bounce light back and forth between them, forms a "p-bit"
Also: Normal.AI (founders from Google Brain, Alphabet X, and Palantir)
~ A First Demonstration of Thermodynamic Matrix Inversion

Also:
Waiting For Q'uantum Computing? Try Probabilistic Computing
(IEEE Spectrum, March 2021)
& (https://spectrum.ieee.org/probabilistic-computing)

THERMODYNAMIC COMPUTING

E.g., Extropic.AI ("*Self-assembling intelligence from the future*")
(in stealth – see https://twitter.com/lexfridman/status/1740815481043320975)

[Topics]

BIOLOGICAL (DNA) COMPUTING

[Topics]

Backup Slides

The Feynman Lectures on Physics

Hosted by CalTech

- Vol 1: Mechanics, Radiation, and Heat
- Vol 2: Electromagnetism and Matter
- Vol 3: Quantum Mechanics
- Messenger Lectures (Gravitation, Conservation Principles, Probability & Uncertainty – Quantum Mechanical Nature, Math/Physics, Symmetry, Past/Future, New Laws)

Algorithms & Complexity

Exploiting quantum logic to overcome computational "explosion" in problem sizes

Notation	Name	Example problem
$O(1)$	Constant	Calculating $(-1)^n$
$O(\log n)$	Logarithmic	Binary search
$O(n)$	Linear	Linear search
$O(n \log n)$	Linearithmic	Merge sort
$O(n^2)$	Quadratic	Bubble sort
$O(n^c)$	Polynomial	AKS primality test
$O(c^n)$	Exponential	Traveling salesman problem using dynamic programming
$O(n!)$	Factorial	Traveling salesman problem using brute-force search

Class	Informal definition	Formal criteria
BQP	Problem can be **solved** by a quantum computer in polynomial time	$A \in \mathrm{BQP}(a,b)$ iff, for functions $a, b : \mathbb{N} \to [0,1]$, there exists a polynomial-time generated family of quantum circuits $Q = \{Q_n : n \in \mathbb{N}\}$, where each circuit Q_n takes in n input qubits and produces one output qubit, with the following properties: • If $x \in A_{yes}$ then $\Pr[Q \text{ accepts } x] \geq a(\lvert x\rvert)$ • If $x \in A_{no}$ then $\Pr[Q \text{ accepts } x] \leq b(\lvert x\rvert)$ Define BQP = BQP(2/3, 1/3)
QMA	Solution can be **checked** by a quantum computer in polynomial time	$A \in \mathrm{QMA}_p(a,b)$ iff, for a polynomial function p and functions $a, b : \mathbb{N} \to [0,1]$, there exists a polynomial-time generated family of quantum circuits $Q = \{Q_n : n \in \mathbb{N}\}$, where each circuit Q_n takes in $n + p(n)$ input qubits and produces one output qubit, with the following properties: • For all $x \in A_{yes}$, there exists a $p(\lvert x\rvert)$-qubit quantum state ρ such that $\Pr[Q \text{ accepts } (x,\rho)] \geq a(\lvert x\rvert)$ • For all $x \in A_{no}$ and all $p(\lvert x\rvert)$-qubit quantum states ρ it holds that $\Pr[Q \text{ accepts } (x,\rho)] \leq b(\lvert x\rvert)$ Define QMA = $\cup_p \mathrm{QMA}_p(2/3, 1/3)$

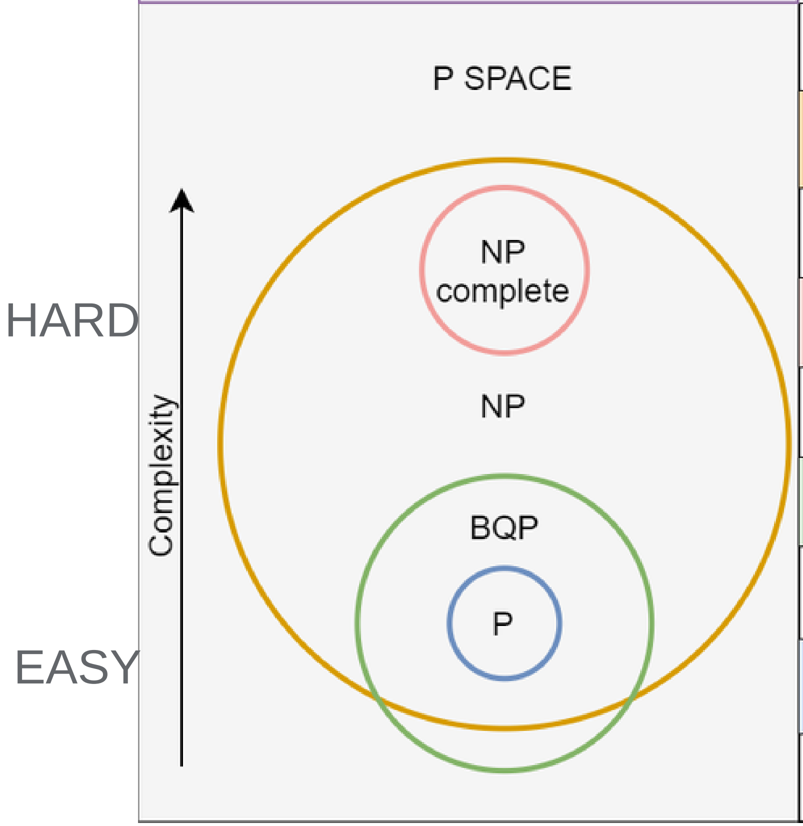
Class	Informal definition	Formal criteria
P	Problem can be **solved** by a **deterministic** classical computer in polynomial time	Problem A for which a polynomial time deterministic TM accepts/rejects all strings in A_{yes}/A_{no}
NP	Solution can be **checked** by a **deterministic** classical computer OR problem can be **solved** by a **nondeterministic** classical computer in polynomial time	Problem A for which there exists a polynomial function p and a polynomial time deterministic TM M with the following properties: • For every string $x \in A_{yes}$, M accepts (x, y) for some string y of length $p(\lvert x\rvert)$ • For every string $x \in A_{no}$, M rejects (x, y) for all strings y of length $p(\lvert x\rvert)$
BPP	Problem can be **solved** by a **probabilistic** classical computer in polynomial time	Problem A for which a polynomial time probabilistic TM accepts all strings in A_{yes} with probability **at least 2/3**, and accepts all in strings in A_{no} with probability **at most 1/3**
P-SPACE	Problem can be **solved** by a **deterministic** classical computer in polynomial space	Problem A for which a deterministic TM running in polynomial space accepts/rejects all strings in A_{yes}/A_{no}

https://www.imperial.ac.uk/media/imperial-college/research-centres-and-groups/theoretical-physics/msc/dissertations/2021/Chukwudubem-Umeano-Dissertation.pdf

Algorithm Complexity

Persistent computer science challenge: solving problems that scale with non-polynomial complexity

Quantum Complexity Classes



Polynomial Space Problem (PSPACE)	Space requirements are polynimial bound e.g. NxN Chess
Non Deterministic Polynomial Time (NP)	Solutions can be guessed and verified in polynomial time e.g. Graph Isomorphism
Non Deterministic Polynomial Time Complete (NP Complete)	Class of problem for which no efficient solution is available e.g. Travelling Sales Person
Bounded-error quantum polynomial time (BQP)	Problems can be efficienltly solved by quantum computer e.g. Factoring Discreet Log
Polynomial Time Solvalbe (P)	Efficiently solved by both quantum and classical computer e.g. Graph Connectivity

https://www.researchgate.net/publication/368652284_Quantum_Computing_Toolkit_From_Nuts_and_Bolts_to_Sack_of_Tools

HPE / Cray re: Quantum Computing

(April 2019) Why HPE Abandoned Quantum Computing Research

Quantum computers are best applied to problems that are simple to state and have an answer that's simple enough to check and look at and understand. Of course, in between that simple beginning and end is an insanely complicated calculation that just cannot be done in the classical universe. They don't handle very large datasets or complex outputs and they are just not good at doing ordinary algebra—you have to actually do all the algebra and not just statistically analyze a linear algebra problem.

Another practical barrier for quantum in enterprise: there is no such thing as a quantum hard drive so anytime a calculation happens using a database for analytics or a neural network there is a conversion that is currently not possible. This is especially true for deep learning training since it would require ridiculous numbers of iterations to do simple things like grab weights at each execution.

(March 2019) Quantum Computing No Threat to Supercomputing

Cray is not pursuing any kind of quantum strategy at the moment following a detailed evaluation.

There are only a small number of core algorithms, some have suggested there are six, that are amenable to quantum and because of this input problem, you have to concentrate on problems that have exponential, not just polynomial or quadratic advantage; it has to be exponential advantage to beat classical machines.

[The problem] "must be defined to a certain number of qubits which means that there needs to be a very compact problem description but an exponential amount of computation followed by a very small output that can be checked with a classical computer."

This further limits the problem space that could be tackled by quantum systems, already complicated by the code base issue.

The fundamental limits of physics