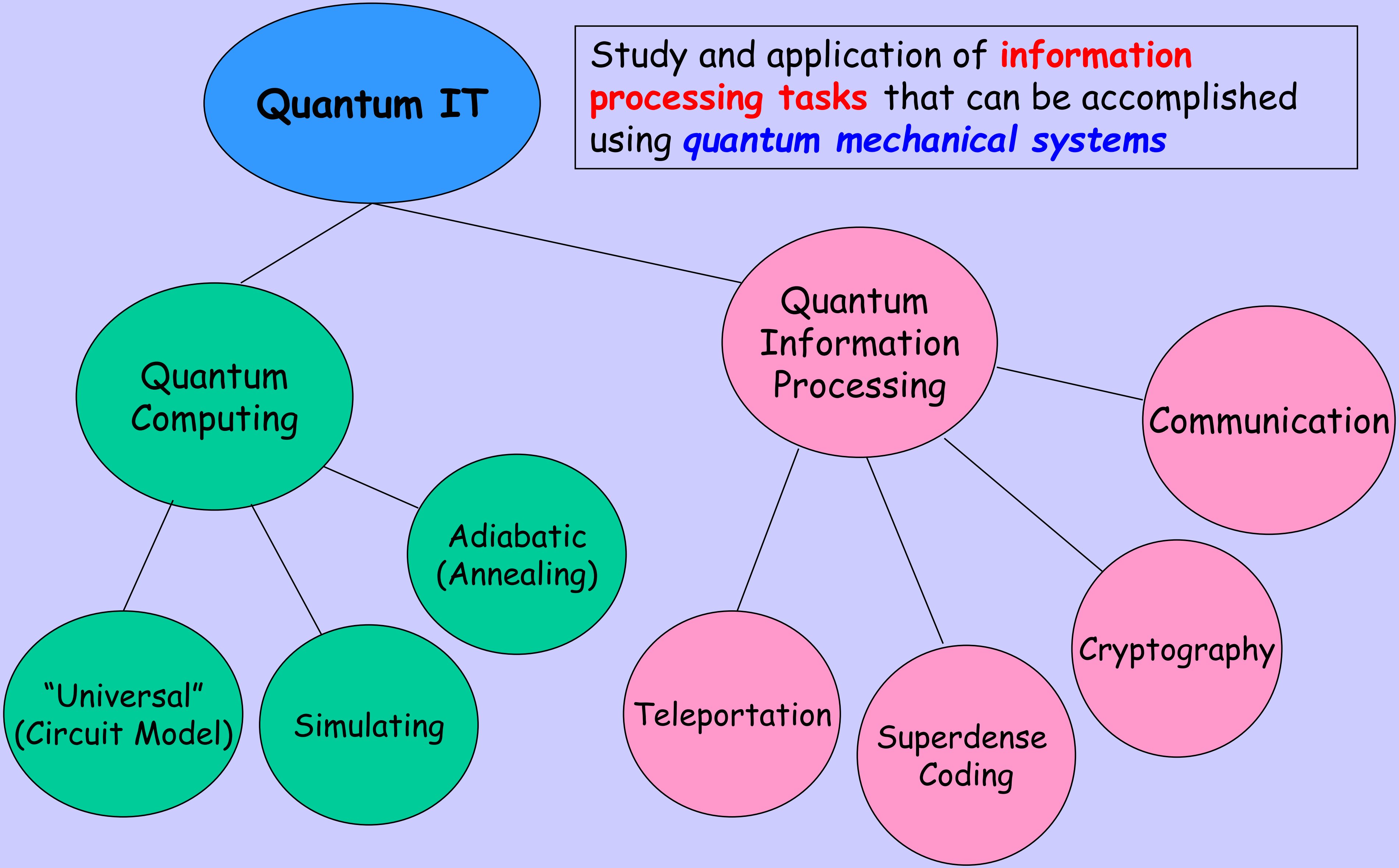
Quantum information technologies: current status and prospects of their applications

Vladimir P. Gerdt

Head of research group (sector) on algebraic and quantum computation
Laboratory of information technologies
Joint Institute for Nuclear Research, Dubna

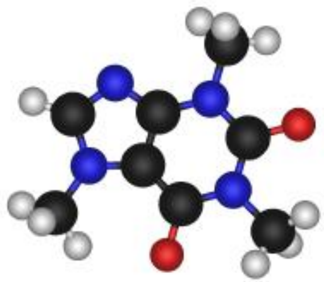
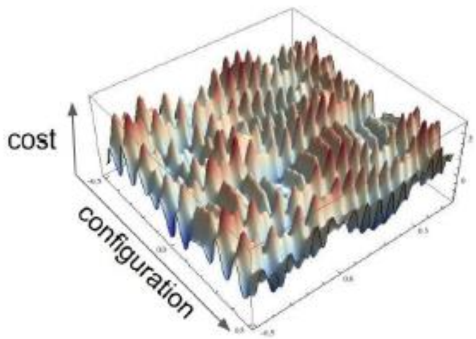
Quantum IT = Quantum Compution + Quantum Information

Study and application of **information processing tasks** that can be accomplished using ***quantum mechanical systems***



Most promising applications of Quantum Computing

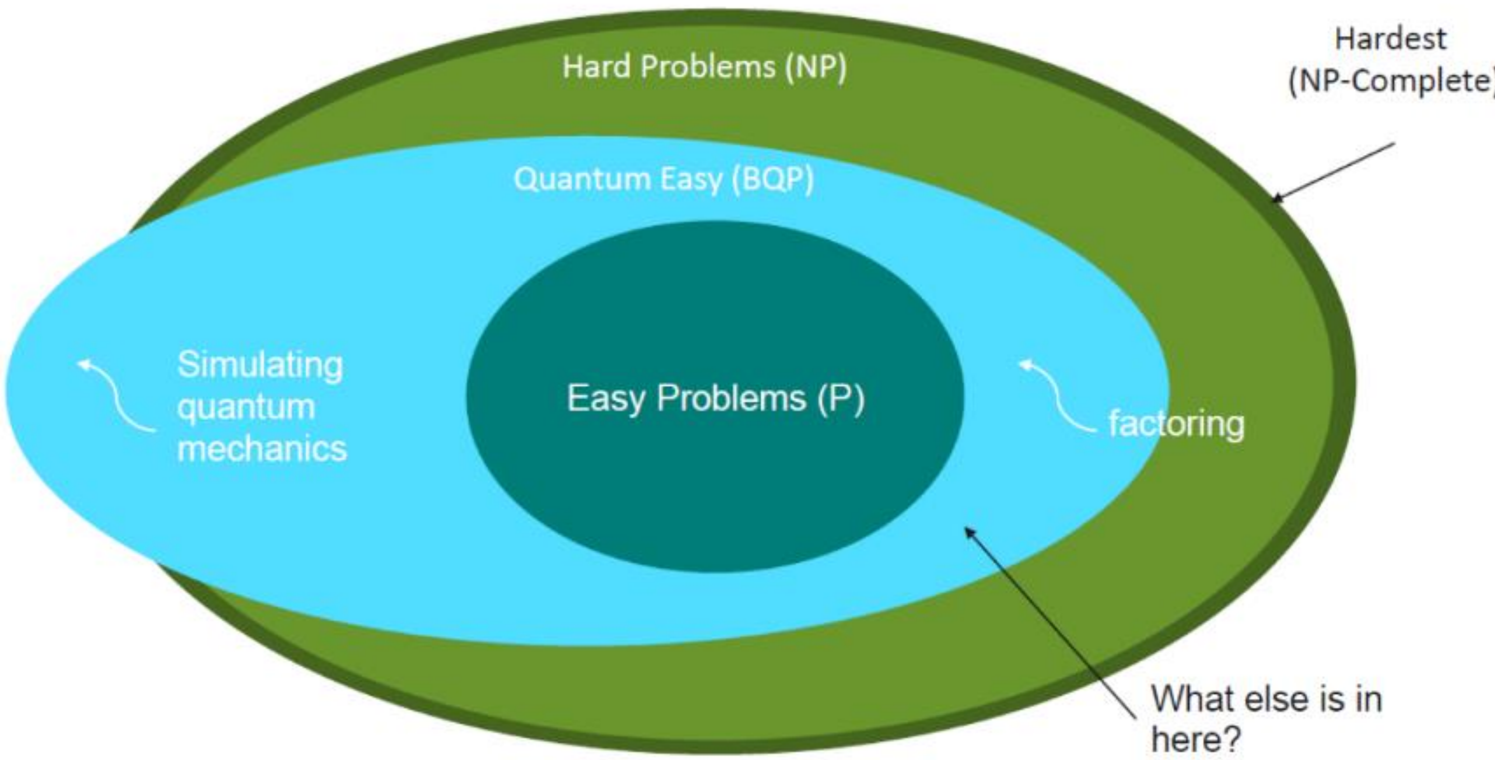
Projected applications of quantum computing

Quantum Simulation	Optimization	Factoring
		$15 = 5 \times 3$

Google AI Quantum

Complexity Classes

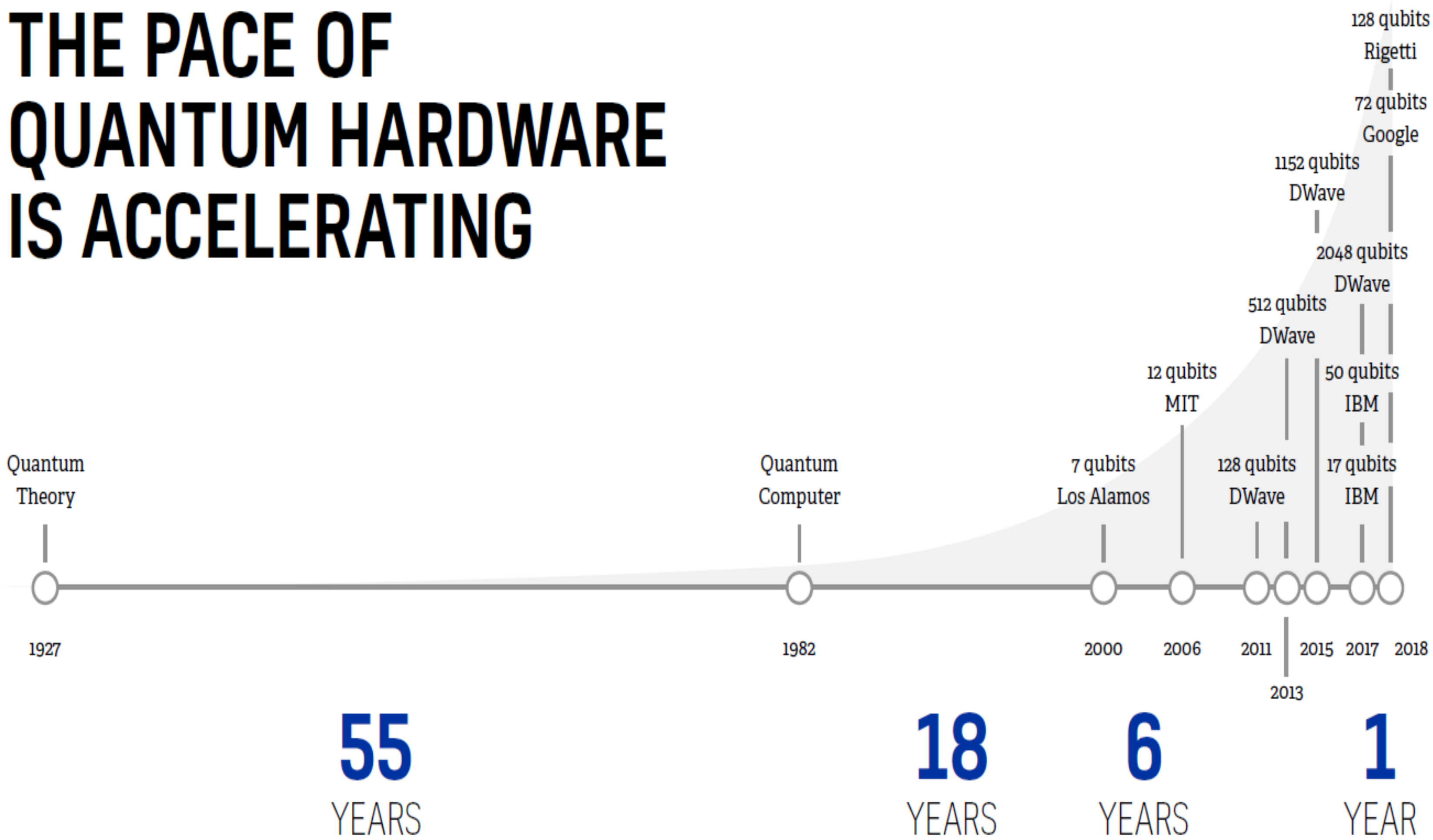
motivation



Lev S. Bishop - https://developer.ibm.com/open/events/dw-open-tech-talk-qiskit-and-quantum-computing/

© 2017 IBM

THE PACE OF QUANTUM HARDWARE IS ACCELERATING



©2018 Strangeworks, Inc. All rights reserved. CONFIDENTIAL

Quantum hardware I

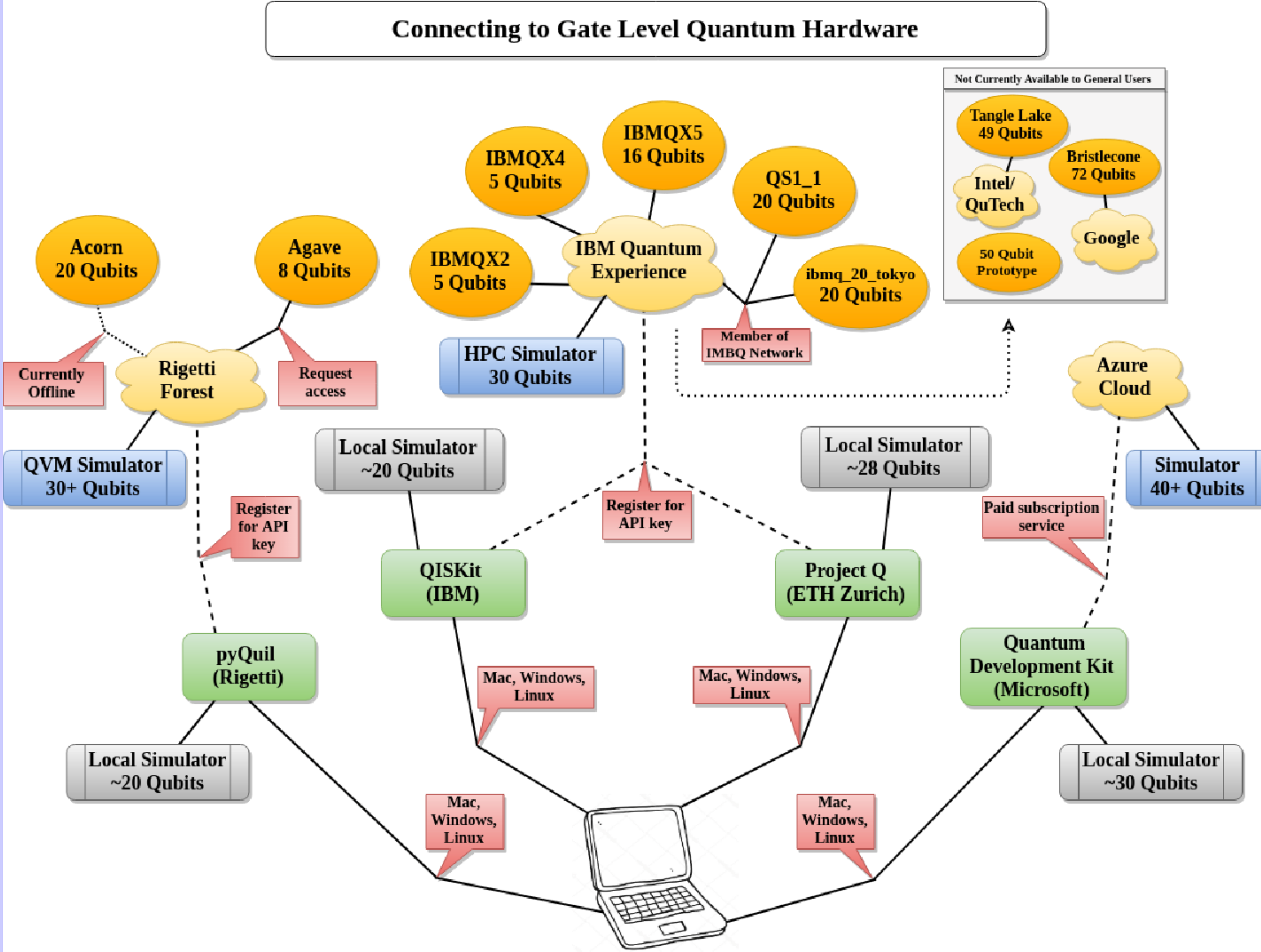
Company	Type	Technology	Now	Next Goal
Intel	Gate	Superconducting	49	TBD
Google	Gate	Superconducting	72	TBD
IBM	Gate	Superconducting	50	TBD
Rigetti	Gate	Superconducting	19	128
USTC (China)	Gate	Superconducting	10	20
IonQ	Gate	Ion Trap	11	79
IQOQI/Univ. Ulm/Univ. Innsbruck	Gate	Ion Trap	20	TBD
NSF STAQ Project	Gate	Ion Trap	N/A	≥64
Intel	Gate	Spin	26	TBD
Silicon Quantum Computing	Gate	Spin	N/A	10
CEA-Leti/INAC/Institut Néel	Gate	Spin	N/A	100
Univ. of Wisconsin	Gate	Neutral Atoms	49	TBD

https://quantumcomputingreport.com/scorecards/qubit-count/

Quantum hardware II

Harvard/MIT	Quantum Simulator	Rydberg Atoms	51	TBD
Univ. of Maryland / NIST	Quantum Simulator	Ion Trap	53	TBD
D-Wave	Annealing	Superconducting	2048	5000+
iARPA QEO Research Program	Annealing	Superconducting	N/A	100
NTT/Univ. of Tokyo/Japan NII	Qtm Neural Network	Photonic	2048	>20,000

https://quantumcomputingreport.com/scorecards/qubit-count/



R. LaRose. Overview and comparison of gate level quantum software platforms. arXiv:1807.02500

Some practical quantum algorithms

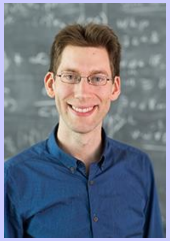
Algorithm: Factoring (1994)
Speedup: Superpolynomial
Description: Given an n-bit integer, find the prime factorization.
The quantum algorithm of **Peter Shor** solves this in $O(n^3)$ time. The fastest known classical algorithm for integer factorization is the general number field sieve, which runs in time $\exp(O(n^{1/3}))$
Shor's factoring algorithm breaks RSA public-key encryption and the closely related quantum algorithms for discrete logarithms break the DSA and ECDSA digital signature schemes and the Diffie-Hellman key-exchange protocol.

P. Shor

Algorithm: Searching (1996)
Speedup: Polynomial
Description: We are given an oracle with N allowed inputs. For one input w ("the winner") the corresponding output is 1, and for all other inputs the corresponding output is 0. The task is to find w.
On a classical computer this requires $\Omega(N)$ queries. The quantum algorithm of **Lov Grover** achieves this using $O(N^{1/2})$ queries, which is **optimal**.

L. Grover

Algorithm: Linear Systems (2008)
Speedup: Superpolynomial
Description: We are given oracle access to an $n \times n$ matrix A and some description of a vector b. We wish to find some property of $f(A)b$ for some efficiently computable function f. Suppose A is a Hermitian matrix with $O(\text{polylog } n)$ nonzero entries in each row and condition number k. As it was shown by **Aram Harrow, Avinatan Hassidim and Seth Lloyd** (HHL algorithm) , a quantum computer can in $O(k^2 \log n)$ time compute to polynomial precision various expectation values of operators with respect to the vector $f(A)b$ (provided that a quantum state proportional to b is efficiently constructable). For certain functions, such as $f(x)=1/x$, this procedure can be extended to non-Hermitian and even non-square A. The runtime of this algorithm was subsequently improved to $O(k \log^3 k \log n)$.



A.Harrow

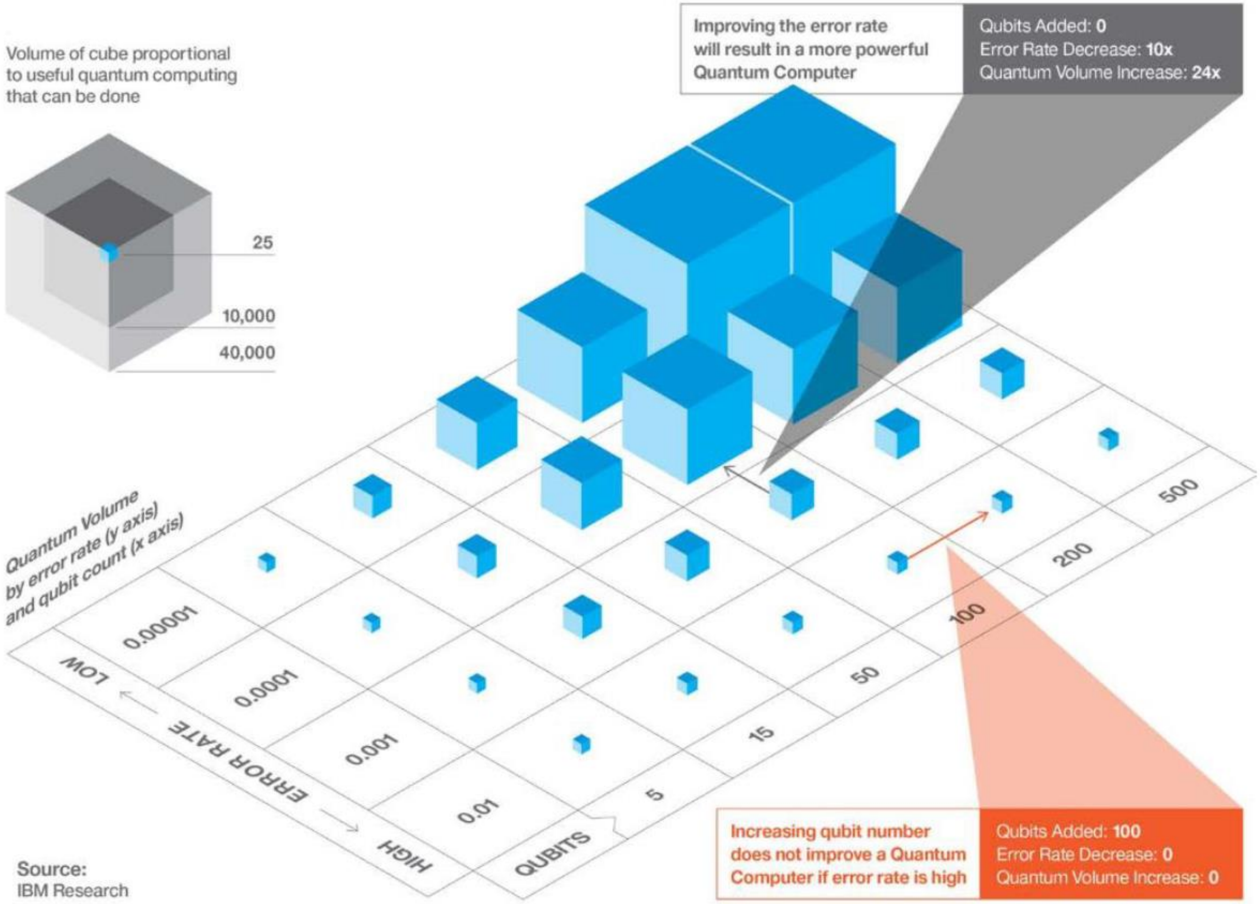
A.Hassidim

S. Lloyd

https://math.nist.gov/quantum/zoo/

Metric of IBM for Performance of Quantum Computing

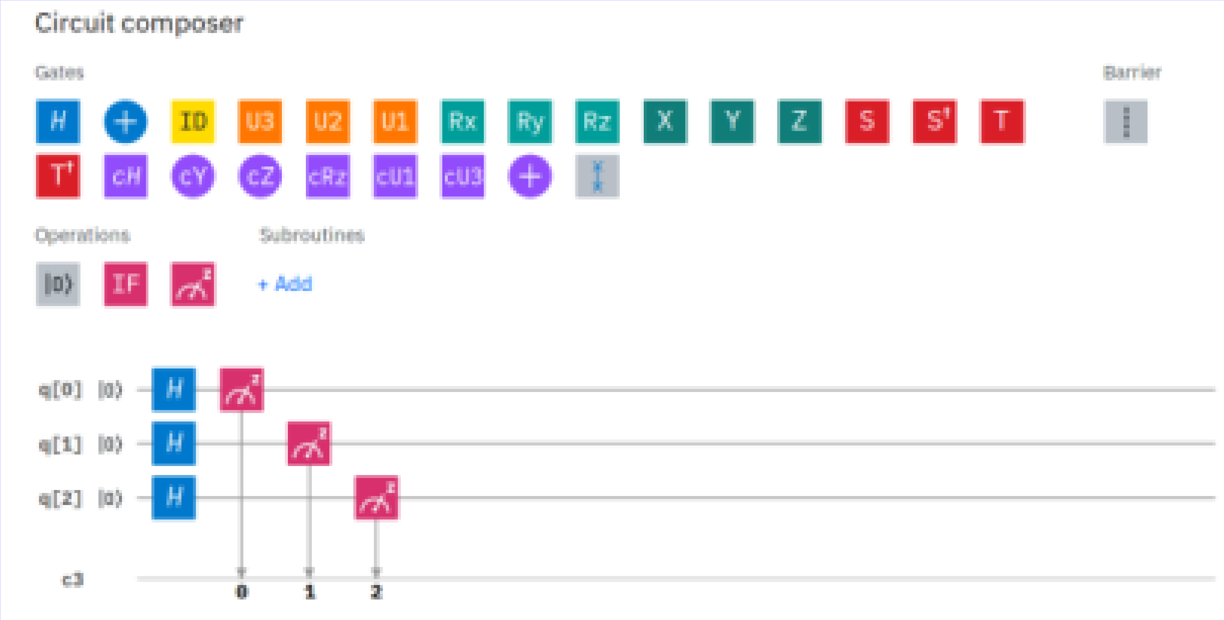
Quantum Volume

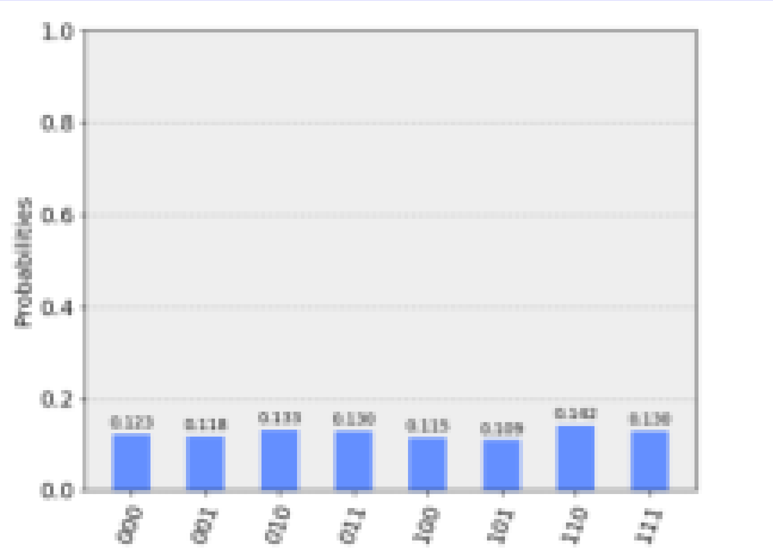


Source:
IBM Research

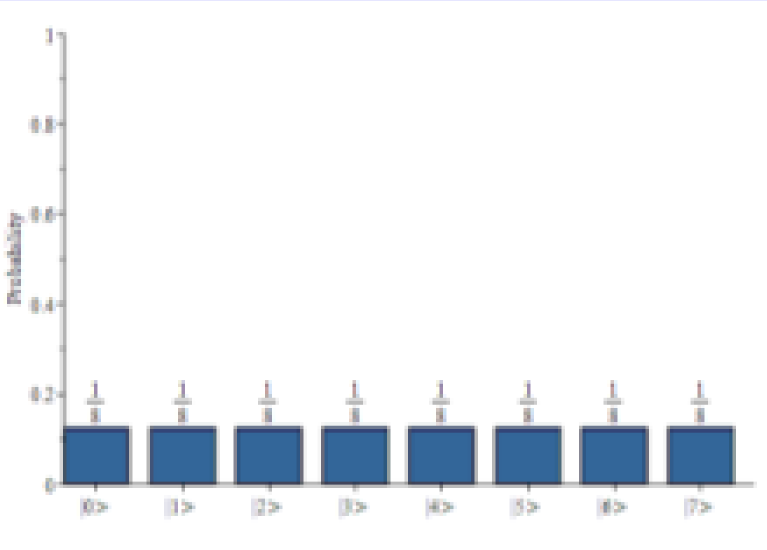
© 2017 IBM

Experimental Errors on IBM Q Yorktown with 5 qubits

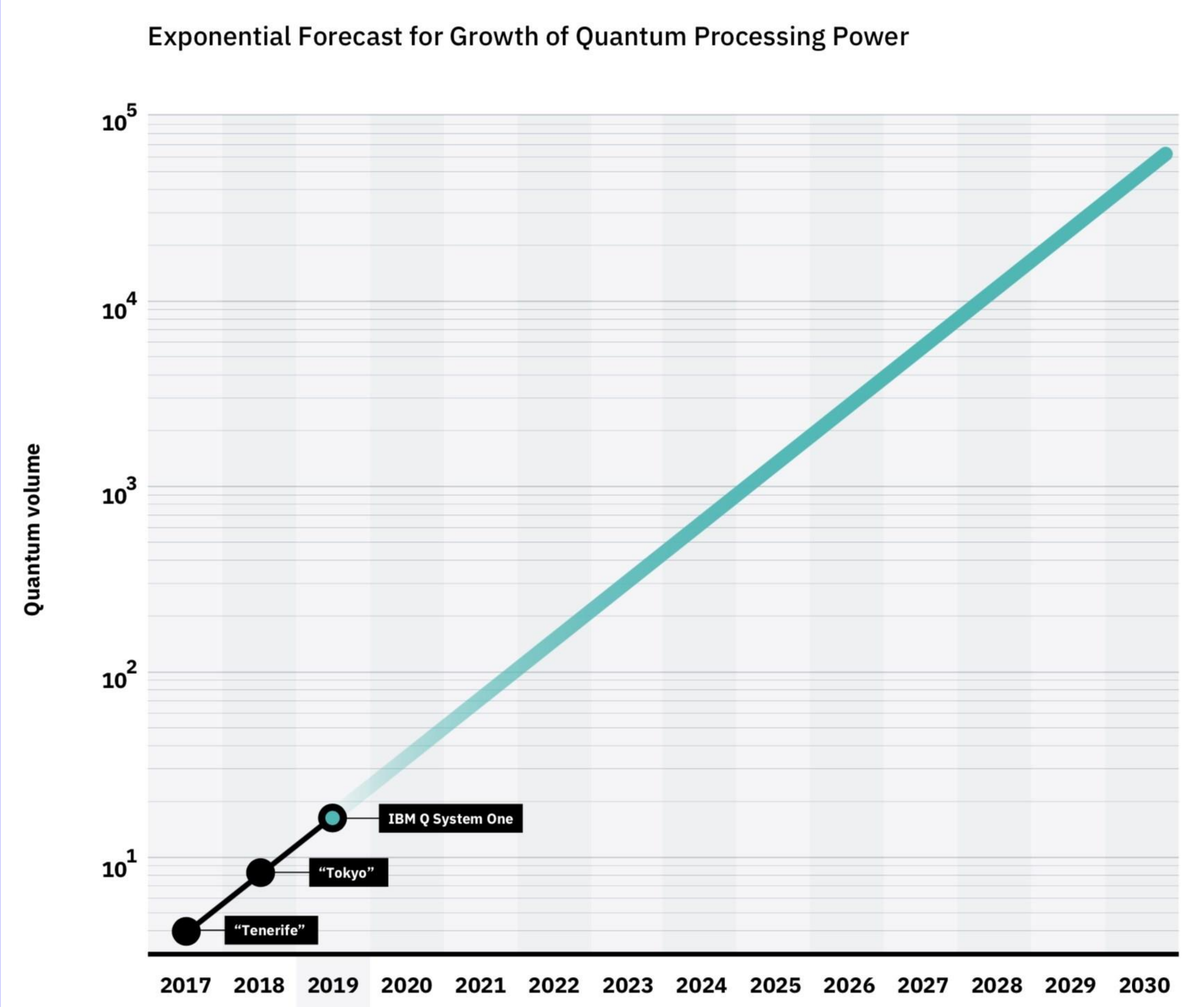




3-qubit equal superposition



Output on classical simulator



https://newsroom.ibm.com/2019-03-04-IBM-Achieves-Highest-Quantum-Volume-to-Date-Establishes-Roadmap-for-Reaching-Quantum-Advantage

Criteria for a universal Quantum Computer

David DiVincenzo
The Physical Implementation of Quantum Computation
***Fortschritte der Physik*. 48 (9–11): 771–783. arXiv:quant-ph/0002077v3**

1. Scalable system with well-defined qubits
2. Initializable to a simple fiducial state
3. Long decoherence time
4. Universal set of quantum gates
5. Permit efficient, qubit-specific measurements

additional criteria for quantum communication:

6. The ability to interconvert stationary and flying qubits
7. The ability to transmit flying qubits between specified locations

DiVincenzo Criteria for QC Approaches

QC Approach	#1	#2	#3	#4	#5
NMR	🔴	🟡	🟡	🟢	🟡
Trapped Ion	🟡	🟢	🟢	🟢	🟢
Neutral Atom	🟡	🟢	🟢	🟢	🟢
Cavity QED	🟡	🟢	🟢	🟡	🟢
Photonic	🟡	🟢	🟢	🟢	🟢
Solid State	🟡	🟢	🟢	🟢	🟢
Superconducting	🟢	🟢	🟢	🟢	🟢

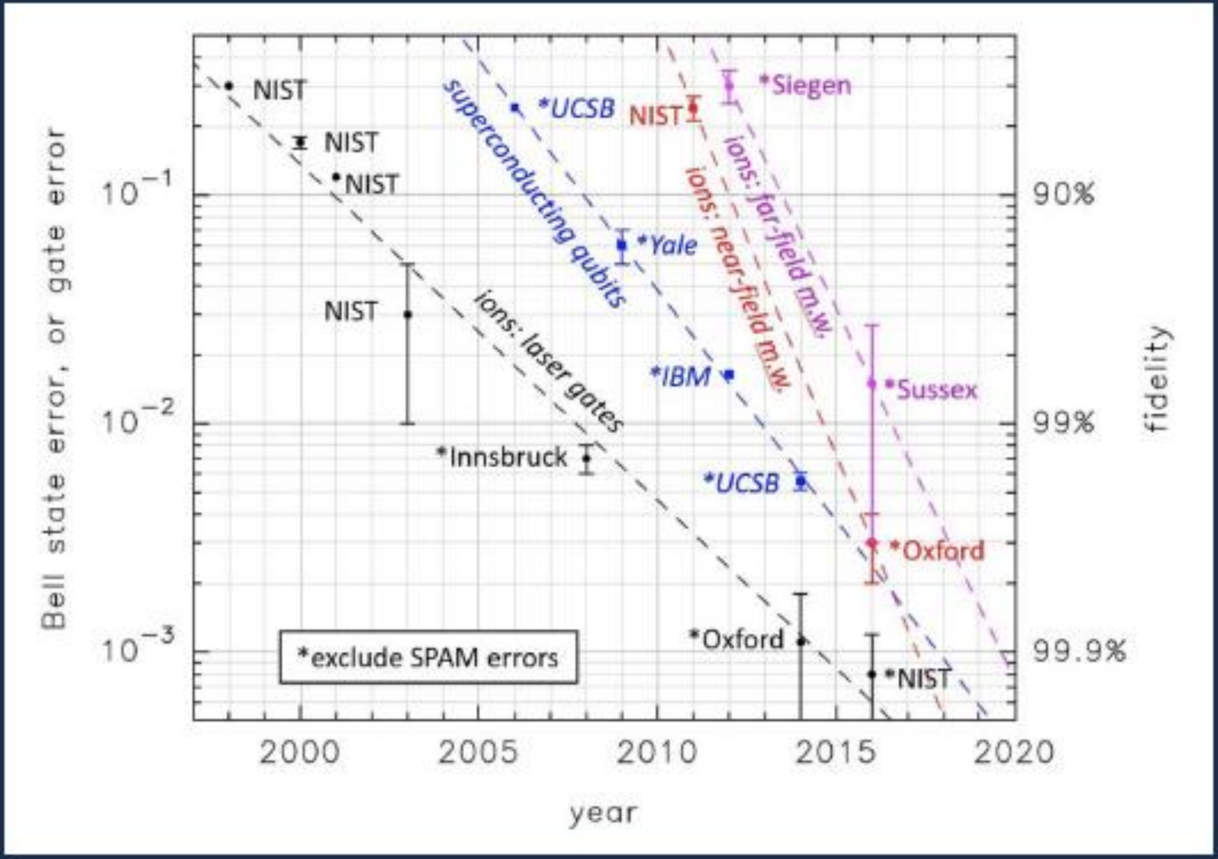
🟢 = a potentially viable approach has achieved sufficient proof of principle

🟡 = a potentially viable approach has been proposed, but there has not been sufficient proof of principle

🔴 = no viable approach is known

Source: Peter McMahon, Q2B 2018
https://q2b2018.qcware.com/videos-presentations

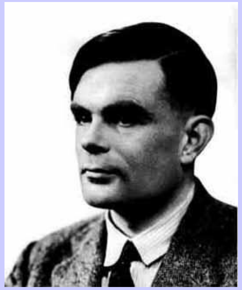
Hardware fidelity progressing rapidly



Source: University of Oxford, NQIT

Source: Peter McMahon, Q2B 2018
https://q2b2018.qcware.com/videos-presentations

The strong Church-Turing thesis



Church-Turing thesis: Any algorithmic process can be simulated on a Turing machine.

Strong Church-Turing thesis (E.Bernstein, U.Vazirani. Quantum Complexity Theory. *SIAM J. Comput.*, 26(5), 1411–1473,1997).

Any physically reasonable algorithmic process can be simulated on a Turing machine, with at most a polynomial slowdown in the number of steps required to do the simulation.

***Ad hoc* empirical justification!**

The strong Church-Turing thesis implies that the problems in **P** are precisely those for which a polynomial-time solution is the best possible, in any *physically reasonable* model of computation.

violation ?

Quantum Supremacy: find a problem **A**, such that
Complexity (**A** | classical computer) >> Complexity (**A** | quantum computer)

Noisy Intermediate Scale Quantum (NISQ) Era

In quantum computers qubits lose their (quantum) state due to the errors caused by noisy gates and decoherence. Quantum Error Correction Codes (QECC) can protect again errors . Unfortunately, QEC requires significant overheads, typically 10-50 extra qubits to encode one fault-tolerant qubit.

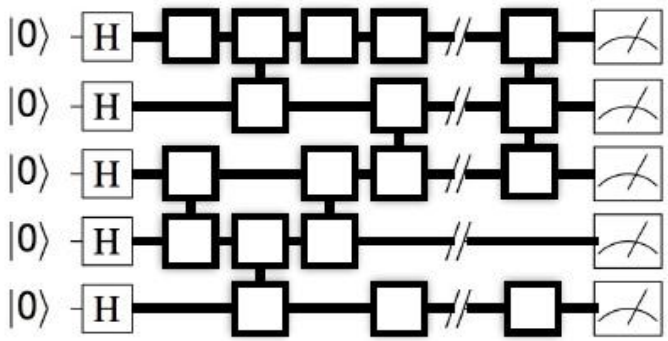
"Quantum Supremacy": a first step

- **Quantum Supremacy:** A practical demonstration of a quantum computation that is prohibitively hard for classical computers
- Needs to be
  - NISQ feasible
  - Exponential speedup over classical
  - No requirement to be useful
- There are several candidates for this experiment:
  - BosonSampling [AA'11], IQP [BJS'11], RCS [BISBDJBMN'18, BFNV'18],...

Source: Adam Bouland, Q2B 2018
https://q2b2018.qcware.com/videos-presentations

Random Quantum Circuit Simulation benchmark

Formulate quantum circuit by randomly picking 1-qubit or 2-qubit gates from a universal gate set acting on the global superposition state.



ArXiv:1905.00444

$$|0\rangle^{\otimes n} \mapsto H^{\otimes n}|0\rangle^{\otimes n} = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n} \mapsto U\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n} = \sum_{i=1}^{2^n} c_i\,|x_i\rangle$$

$$p_U(x_i) = |c_i|^2$$

Task

Produce samples $\{x_1, \ldots, x_m\}$ from distribution $p_U(x)$.

Recent result from complexity theory

(Nat. Phys 14 595 (2018) / arXiv:1803.04402):

It is #P-hard to compute $p_U(x_i)$.

Google AI Quantum

		Runtime (hours)			Energy cost (MWh)		
Circuit size	Target fidelity (%)	Electra	Summit	QPU	Electra	Summit	QPU
$7 \times 7 \times (1 + 40 + 1)$	0.5	59.0	2.44	0.028	96.8	21.1	4.2×10^{-4}

QPU

NASA ORNL 281 Pflops/s

NASA ORNL 281 Pflops/s

49 qubits @ depth 40

10^3 advantage

10^5 advantage

How many qubits can be simulated?

Surpasses IBM's 56 qubit simulation announced in October

George Nott (CIO)
27 June, 2018 11:19

Researchers at the University of Melbourne say they have set a new world record by simulating the output of a 60-qubit quantum computer.

The previous record was set in October by IBM which classically simulated 56 qubits in carefully chosen states.

"In terms of the number of qubits, this represents one of the largest simulations of a non-trivial quantum circuit ever performed," the researchers said.

Simulating qubits using classical computers is tricky. While classical computers work with binary bits, programmed to encode and process data, a quantum computer's qubits are quantum mechanical objects like atoms.

Quantum states can be binary and put in one of two possibilities, or effectively both at the same time. Quantum superposition means that two qubits can, in a sense, be all four combinations of 0 and 1 at the same time. That unique data crunching power is further boosted by entanglement where the state of one qubit when measured mysteriously dictates the state of another qubit.

That quality gives a 50 qubit machine – about the limit of current quantum computer hardware – in principle the ability to simultaneously represent about a million billion number combinations.

"In order to simulate a quantum computer I need to store every one of these possible binary combinations that a quantum computer can effectively represent. If you have a simple question – can a classical computer simulate a quantum computer – then already at 50 qubits I need 2^{50} numbers to be represented in my classical simulation," explains the University of Melbourne's Professor Lloyd Hollenberg.

"Each of those numbers is essentially a complex number, 128 bits, so the counting then is in petabytes. Supercomputers with thousands of nodes are around about that limit," he says.

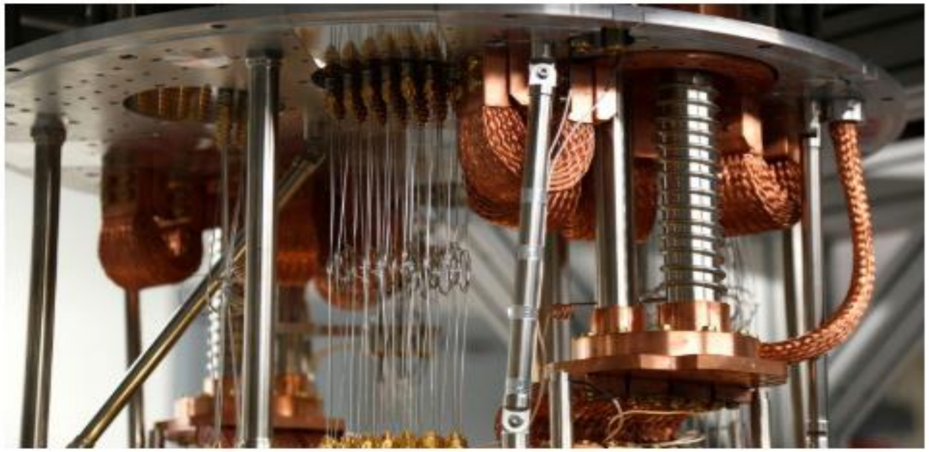
In other words, to simulate a random quantum state of a 50 qubit machine would chew up some 18 petabytes of classical computer memory, or the equivalent of more than a million 16 gigabyte RAM laptops.

One can simulate ≤ 60 qubits

MIT Technology Review

Computing Sep 18

IBM's new 53-qubit quantum computer is the most powerful machine you can use



The machine will be available for researchers and companies to run applications via the cloud.

The news: IBM's new computer, due to launch next month, will boast 53 quantum bits, or qubits, the elements that are the secret to quantum machines' power (see our explainer for a description of qubits and the phenomena that make quantum computers so powerful). Google has a 72-qubit device, but it hasn't let outsiders run programs on it; IBM's machine, on the other hand, will be accessible via the cloud.

Cloud power: IBM has been promoting quantum computing via the cloud since 2016. To boost those efforts, the firm is opening a new center in New York state to house even more machines. Other companies developing quantum computers, like Rigetti Computing and Canada's D-Wave, have also launched cloud services. Behind the scenes, there's a race on to demonstrate quantum supremacy.

Quantum what? That's the point at which a quantum computer can perform a task beyond the reach of even the most powerful conventional supercomputer. Google is rumored to be the closest to achieving this milestone—but hitting it won't mean the machines will be ready for mainstream use. The task is likely to be a very narrow one, and plenty more work will be needed to create quantum computers capable of tackling a wide range of problems.

MIT Technology Review

Computing Sep 20

Google researchers have reportedly achieved "quantum supremacy"

The news: According to a report in the Financial Times, a team of researchers from Google led by John Martinis have demonstrated quantum supremacy for the first time. This is the point at which a quantum computer is shown to be capable of performing a task that's beyond the reach of even the most powerful conventional supercomputer. The claim appeared in a paper that was posted on a NASA website, but the publication was then taken down. Google did not respond to a request for comment from MIT Technology Review.

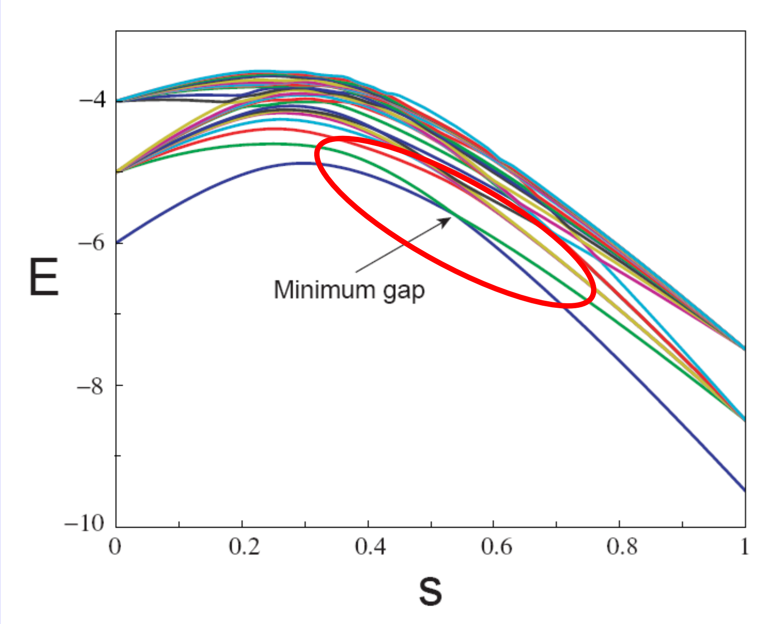
Why NASA? Google struck an agreement last year to use supercomputers available to NASA as benchmarks for its supremacy experiments. According to the Financial Times report, the paper said that Google's quantum processor was able to perform a calculation in three minutes and 20 seconds that would take today's most advanced supercomputer, known as Summit, around 10,000 years. In the paper, the researchers said that, to their knowledge, the experiment "marks the first computation that can only be performed on a quantum processor."

And another but: Quantum computers are still a long way from being ready for mainstream use. The machines are notoriously prone to errors, because even the slightest change in temperature or tiny vibration can destroy the delicate state of qubits. Researchers are working on machines that will be easier to build, manage, and scale, and some computers are now available via the computing cloud. But it could still be many years before quantum computers that can tackle a wide range of problems are widely available.

Adiabatic Quantum Computation (AQC)

E. Farhi et al., Science 292, 472 (2001)

Energy Spectrum



System Hamiltonian:

$$H = (1-s)\, H_i + s\, H_f$$

Linear interpolation: $s = t/t_f$

$0 \leq s \leq 1$

- **Ground state of H_i is easily accessible.**
- **Ground state of H_f encodes the solution to a hard computational problem.**

http://qserver.usc.edu/qec07/QEC07/MohammadAmin.ppt

Adiabatic Quantum Computation (AQC)

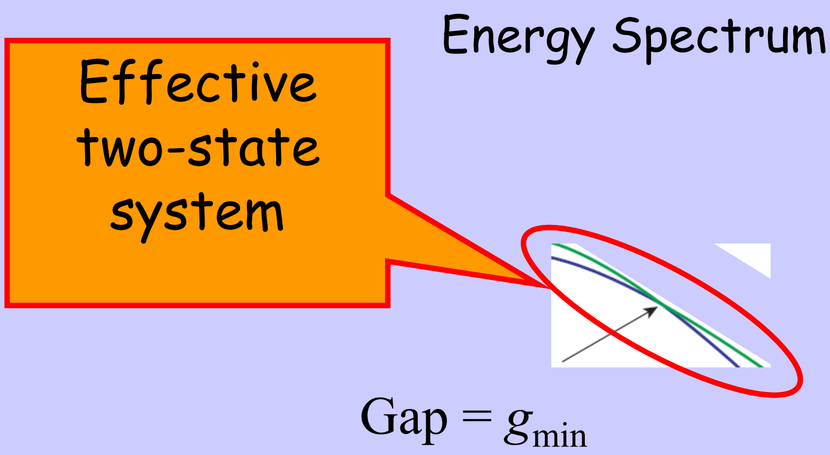
E. Farhi et al., Science 292, 472 (2001)

System Hamiltonian:

$$H = (1-s)\,H_i + s\,H_f$$

Linear interpolation: $s = t/t_f$

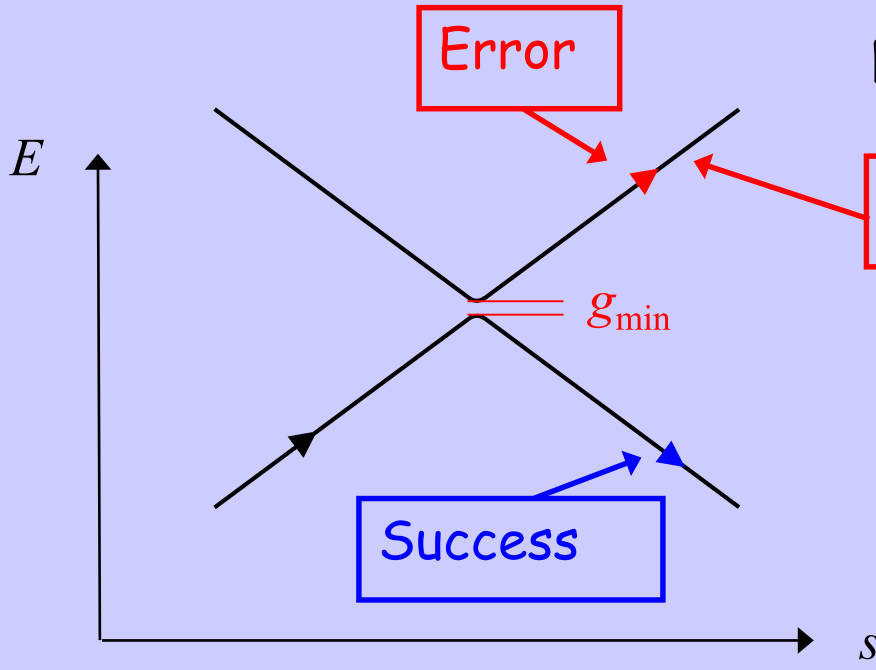
$0 \le s \le 1$



- **Ground state of H_i is easily accessible.**
- **Ground state of H_f encodes the solution to a hard computational problem.**

http://qserver.usc.edu/qec07/QEC07/MohammadAmin.ppt

Adiabatic Theorem



Landau-Zener transition probability:

$$\boxed{P_{LZ} = e^{-\pi g_{\min}^2/2\nu}}$$

$$\nu \sim \dot{s} \sim 1/t_f$$

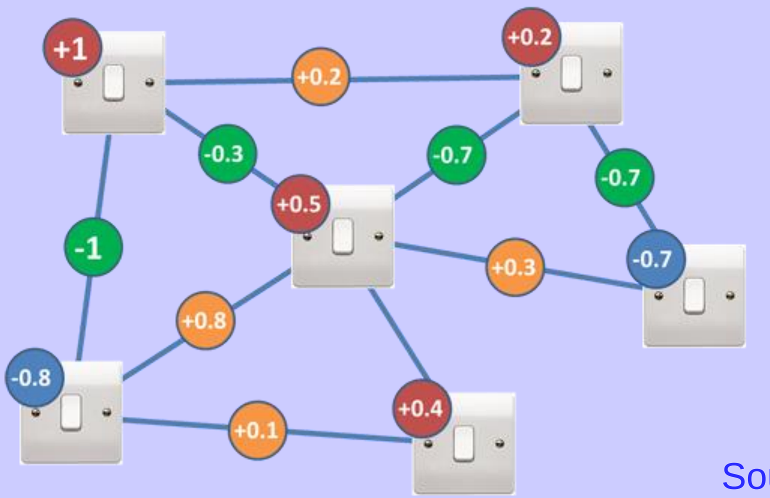
To have small error probability: $t_f >> 1/g_{\min}{}^2$

http://qserver.usc.edu/qec07/QEC07/MohammadAmin.ppt

What is an Adiabatic Quantum Computer?

Solver for Quadratic Unconstrained Binary Optimisation Problems (QUBOs)

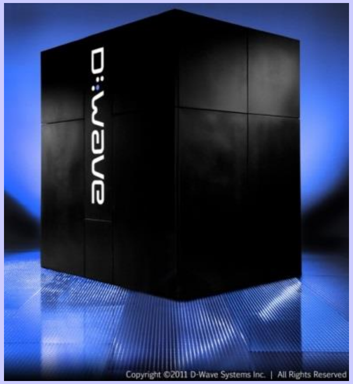
$$E(s_1, s_2, \ldots, s_n) = \sum_i h_i s_i + \sum_{ij} J_{ij} s_i s_j \qquad \text{with } s_i \in \{0,1\}$$



$h_i \in \mathbb{R}$ On-site strength

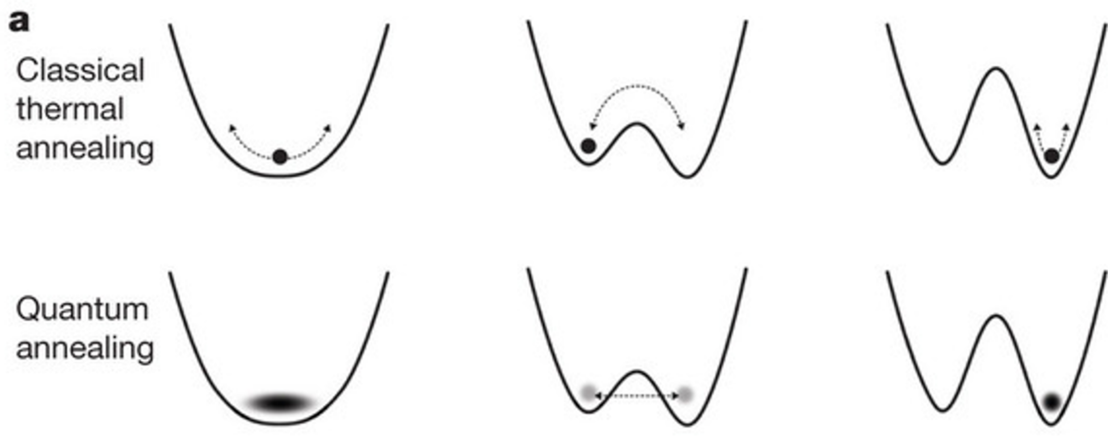
$J_{ij} \in \mathbb{R}$ Coupling

Source: D-Wave Sys.



https://slideplayer.com/slide/9262338/

Quantum Annealing



- Many problems can be mapped onto the question: What is the ground state?
  1) Initialize a known problem in its ground state.
  2) Transform into a problem of interest. Go slowly so that you stay in the ground state.
  3) Nature has solved the problem for you!

M. W. Johnson *et al.*, *Nature* **473**, 149 (2011).

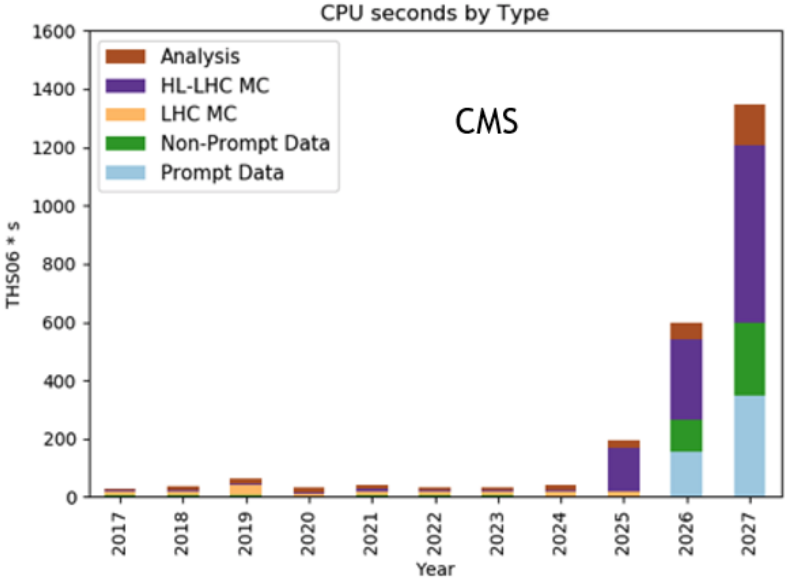
ATLAS and CMS @ HL-LHC
Computing models and CPU needs

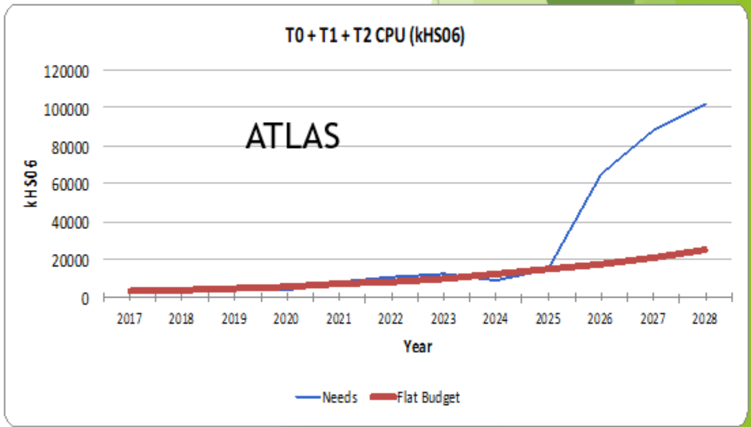
Last known estimates for 2027 (with already a lot of cuts)

- CPU:
  - If we stay with plain old CPUs (think of Intel Xeons), and assume more and more computing cores with roughly today's speed
    - **~15M Cores needed per experiment**
- Disk:
    - **~3 EB per experiment**
- Tape:
    - **~10 EB per experiment**

- There are differences between the 2 experiments estimates, but mostly due different R&D paths.

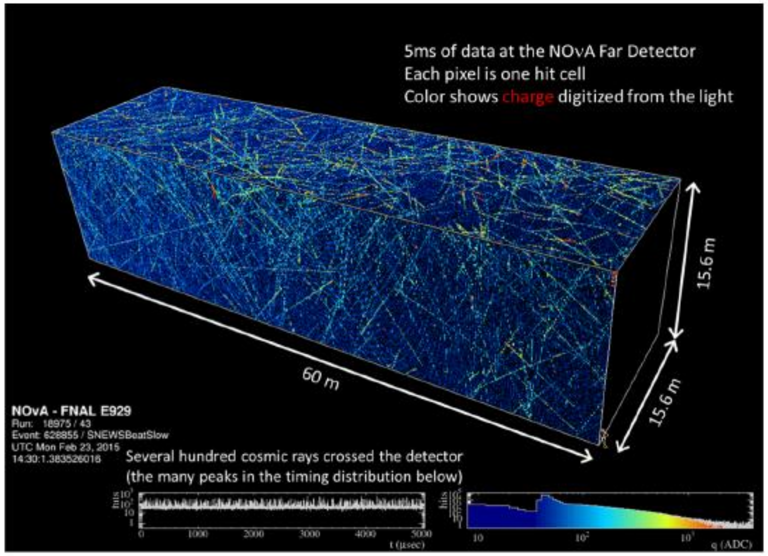
- **Take home message for this venue: we are OFF by ~5x on CPU power when considering Moore's law**

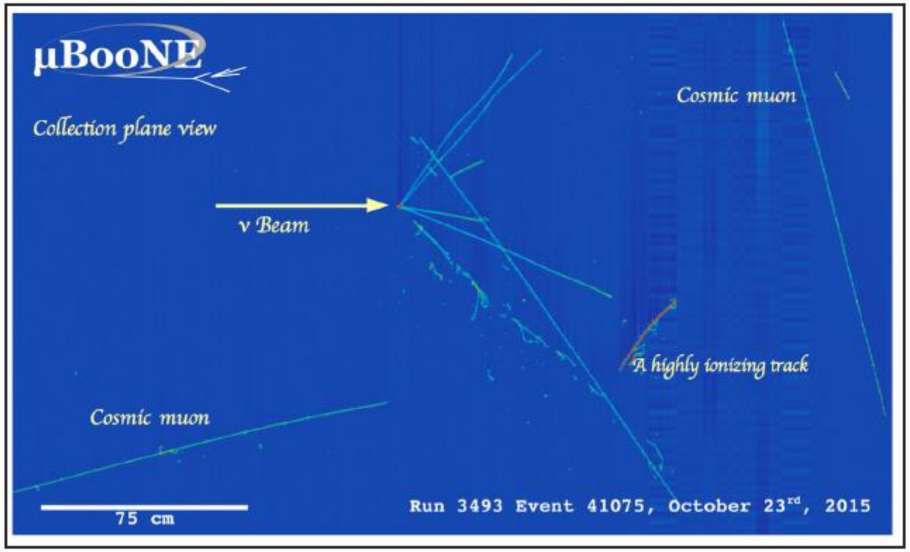




HEP applications on near-term Quantum Computers: Machine Learning (ML)

- Many experiments already using ML to better classify, e.g. neutrino-induced interactions in particle detectors. Fully quantum or hybrid (classical/quantum) approaches could improve performance.
- Some standard ML techniques, e.g. Boltzmann machines, involve estimating the ground state of a Hamiltonian that has many local minima; quantum ML may have advantages
- Quantum ML algorithms could be essential to improve sensitivity for sensor applications





Fermilab

Quantum speedup for machine learning

Box 1 Table | Speedup techniques for given quantum machine learning subroutines

Method	Speedup	Amplitude amplification	HHL	Adiabatic	qRAM
Bayesian inference[106,107]	$O(\sqrt{N})$	Yes	Yes	No	No
Online perceptron[108]	$O(\sqrt{N})$	Yes	No	No	Optional
Least-squares fitting[9]	$O(\log N)$*	Yes	Yes	No	Yes
Classical Boltzmann machine[20]	$O(\sqrt{N})$	Yes/No	Optional/No	No/Yes	Optional
Quantum Boltzmann machine[22,61]	$O(\log N)$*	Optional/No	No	No/Yes	No
Quantum PCA[11]	$O(\log N)$*	No	Yes	No	Optional
Quantum support vector machine[13]	$O(\log N)$*	No	Yes	No	Yes
Quantum reinforcement learning[30]	$O(\sqrt{N})$	Yes	No	No	No

*There exist important caveats that can limit the applicability of the method[51].

Table from: Biamonte, Jacob, et al. "Quantum machine learning." Nature 549.7671 (2017): 195.

commentary

Read the fine print

Scott Aaronson

New quantum algorithms promise an exponential speed-up for machine learning, clustering and finding patterns in big data. But to achieve a real speed-up, we need to delve into the details.

For twenty years, quantum computing has been catnip to science journalists. Not only would a quantum computer harness the notorious weirdness of quantum mechanics, but it would do so for a

HHL attacks one of the most basic problems in all of science: solving a system of linear equations. Given an $n \times n$ real matrix, A, and a vector, $\mathbf{b}$, the goal of HHL is to (approximately) solve the system $A\mathbf{x} = \mathbf{b}$ for $\mathbf{x}$,

of interest, and then carefully analyses the resulting performance against that of the best-known classical algorithm for that case. To my knowledge, so far there have been two attempts to work out potential

Aaronson, Scott. "Read the fine print." Nature Physics 11.4 (2015): 291.

Caveats

1. The input problem: Quantum algorithms provide dramatic speedups for processing data, they seldom provide advantages in reading data. The cost of reading in the input can dominate the cost of quantum algorithms. This cost can be exponential!

2. The output problem. Obtaining the full solution from some quantum algorithms as a string of bits requires learning an exponential number of bits.

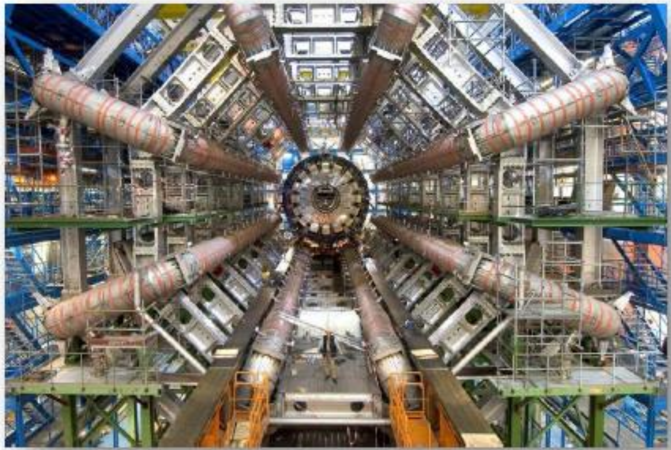
nature
International journal of science

Solving a Higgs optimization problem with quantum annealing for machine learning

Alex Mott, Joshua Job, Jean-Roch Vlimant, Daniel Lidar & Maria Spiropulu

"We show that the resulting quantum and classical annealing-based classifier systems perform comparably to the state-of-the-art machine learning methods that are currently used in particle physics[9,10]. However, in contrast to these methods, the annealing-based classifiers are simple functions of directly interpretable experimental parameters with clear physical meaning…"

*Nature **volume 550**, pages 375-379 (19 October 2017)
doi:10.1038/nature24047



Bo Ewald (D-Wave)

Quantum Computing & Cryptography

Why all the hype?

Shor's algorithm(1994): Efficient quantum algorithm for factoring integers

- Exponentially faster than best known classical algorithm!

This allows (ideal) quantum computers to break most cryptosystems in use today

- RSA
- Diffie-Hellman
- Elliptic curve crypto

Source: Adam Bouland, Q2B 2018
https://q2b2018.qcware.com/videos-presentations

Quantum Computing & Cryptography

Do I need to panic?

Not yet…

Shor's algorithm requires many qubits with error-correction – it is not readily implementable on near-term machines

But it is a concern for the long-term future: NIST call for post-quantum cryptography standard

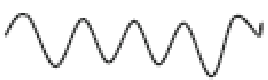
This will eventually replace RSA

Source: Adam Bouland, Q2B 2018
https://q2b2018.qcware.com/videos-presentations

Quantum Computing & Cryptography

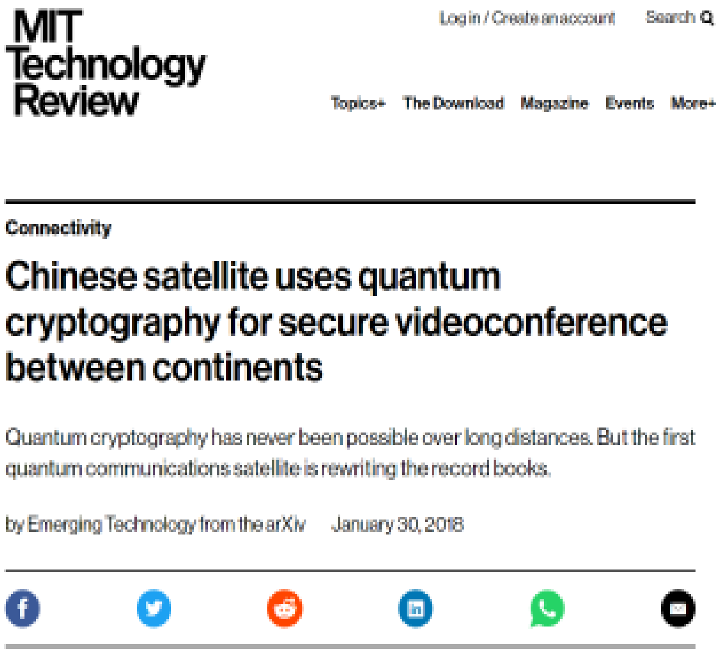
Quantum benefits to cryptography:

Quantum Key Distribution (QKD) [BB'84]:
cryptography which is secure only assuming quantum mechanics is correct



Secret Key

A double edged sword: destroys old crypto, creates new



MIT Technology Review

Log in / Create an account Search

Topics+ The Download Magazine Events More+

Connectivity

Chinese satellite uses quantum cryptography for secure videoconference between continents

Quantum cryptography has never been possible over long distances. But the first quantum communications satellite is rewriting the record books.

by Emerging Technology from the arXiv January 30, 2018

Quantum Information : No-Go Theorems

- Quantum information is fundamentally different than classical information. Quantum theory allows new ways of storing and processing information which are not there in the classical world.

- Copying, deleting, flipping, and partial erasure, etc....are impossible in quantum world.

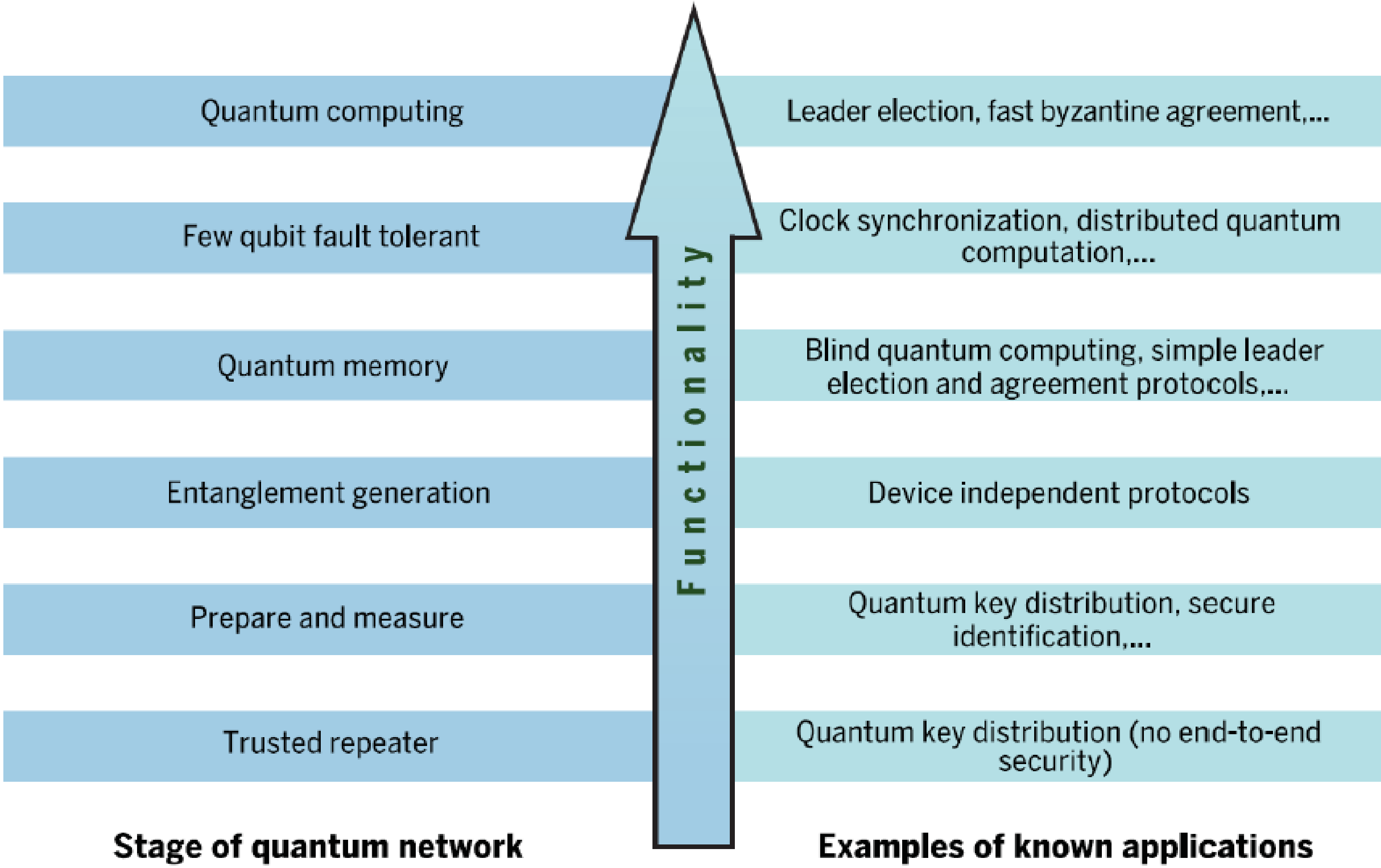
- No-hiding theorem provides new insight into the different laws governing classical and quantum information.

- Unlike classical information, QI cannot be completely hidden in correlations.

- Applications: Randomization, Quantum teleportation, Thermalization, Black hole evaporation and many more.

- Whenever information disappears from one system it moves to somewhere else.

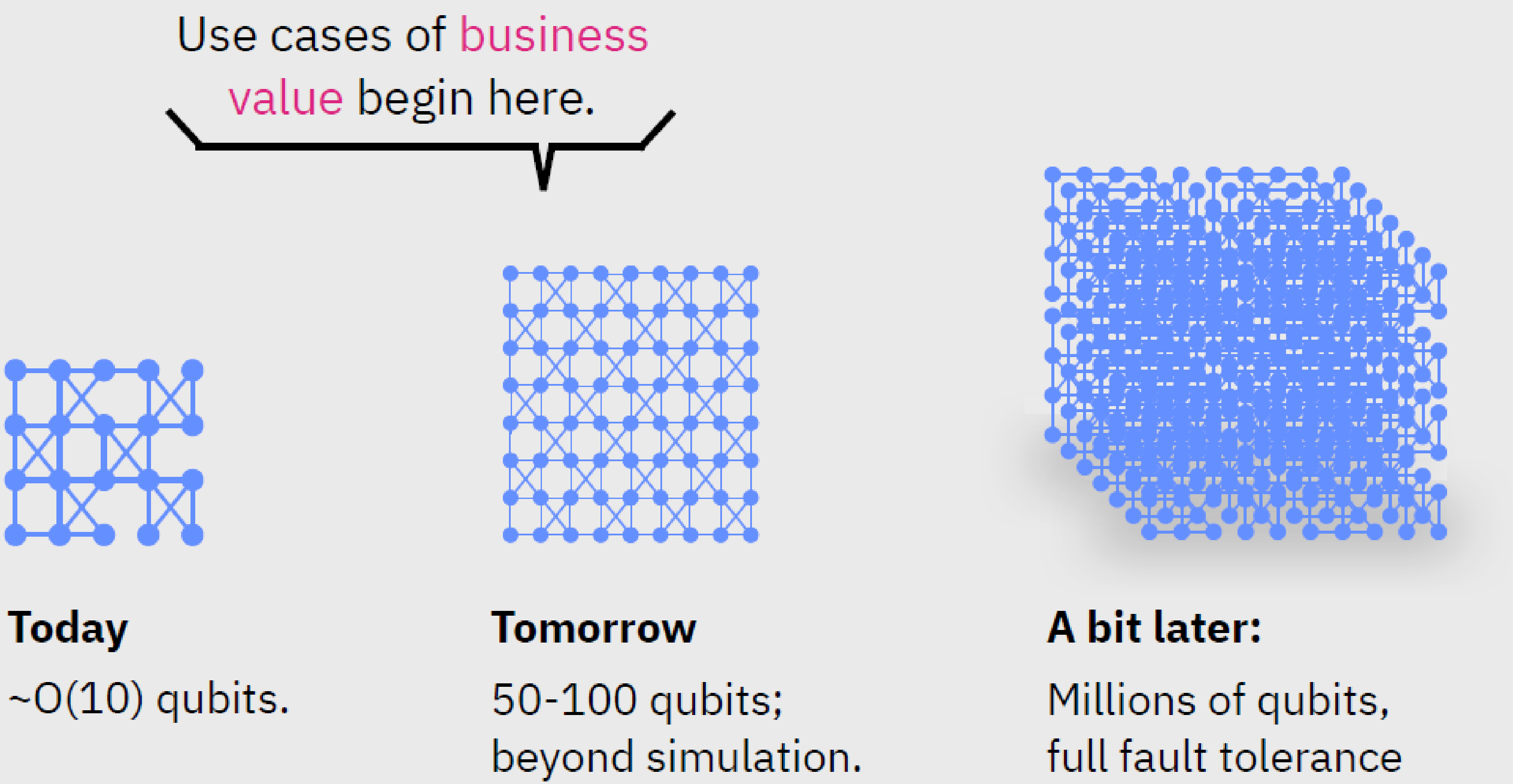
Quantum Internet



Wehner, Elkouss, Hanson 2018

Source: John Preskill, Q2B 2018
https://q2b2018.qcware.com/videos-presentations

Conclusion



Source: Paul Nation, Q2B 2018
https://q2b2018.qcware.com/videos-presentations