USC University of Southern California

Fujitsu Laboratories Advanced Technology Symposium
2017

The Impact of Quantum Computing

Daniel Lidar
University of Southern California

Quantum Computing - Origins

Credit goes to Feynman:

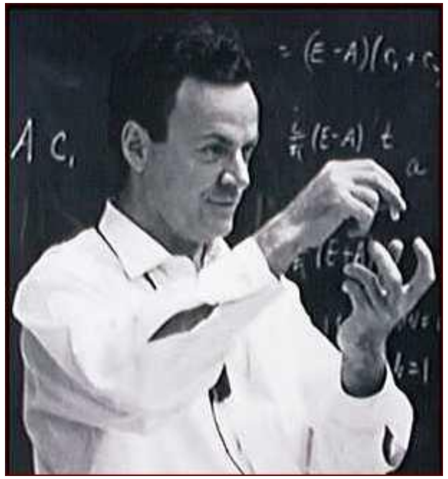
International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981



USC University of Southern California

Quantum Computing - Origins

Credit goes to Feynman:

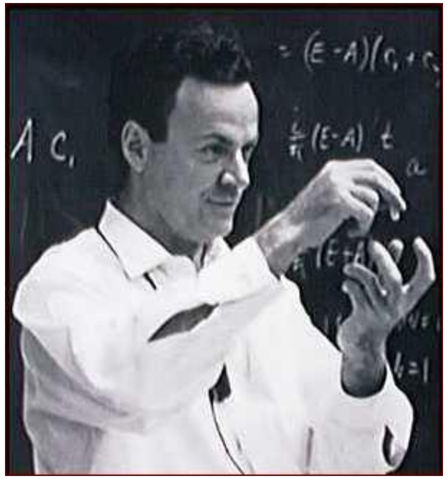
International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

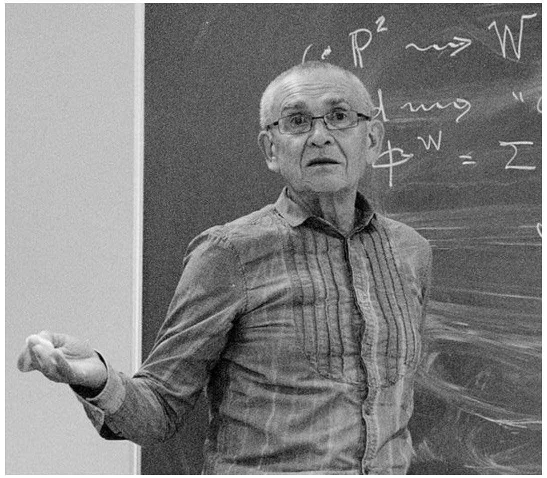
Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981



Yuri Manin



Russian meddling/Fake news?

Russian mathematician
first proposed QCs in 1980
Radio Moscow broadcast

Quantum Computing - Origins

Credit goes to Feynman:

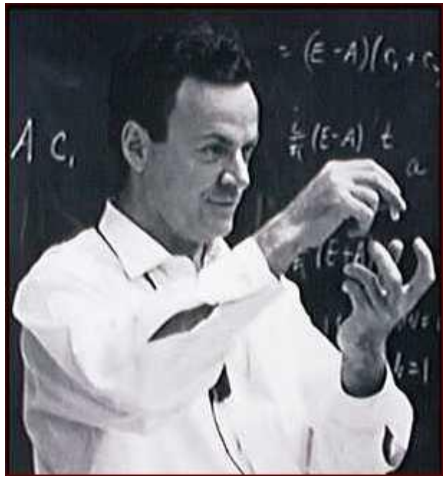
International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981



1. INTRODUCTION

On the program it says this is a keynote speech—and I don't know what a keynote speech is.

USC University of Southern California

Quantum Computing - Origins

Credit goes to Feynman:

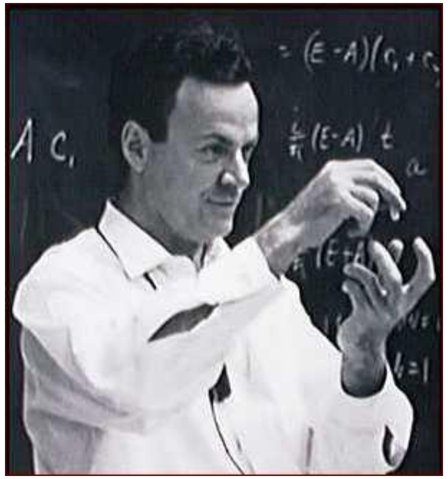
International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981



1. INTRODUCTION

On the program it says this is a keynote speech—and I don't know what a keynote speech is.

This talk will:

- Provide some background on quantum computing
- Plant some seeds for the panel discussions and later talks
- Speculate about where the field is going

Quantum Computing - Origins

Credit goes to Feynman:

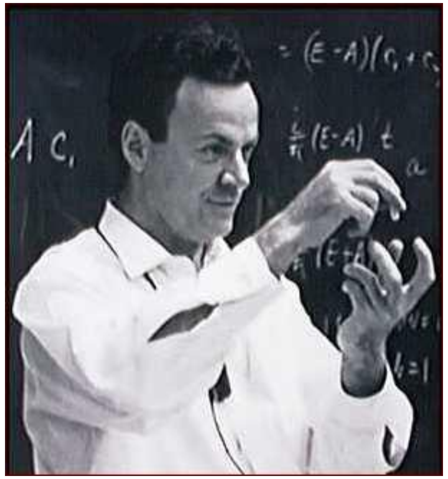
International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981



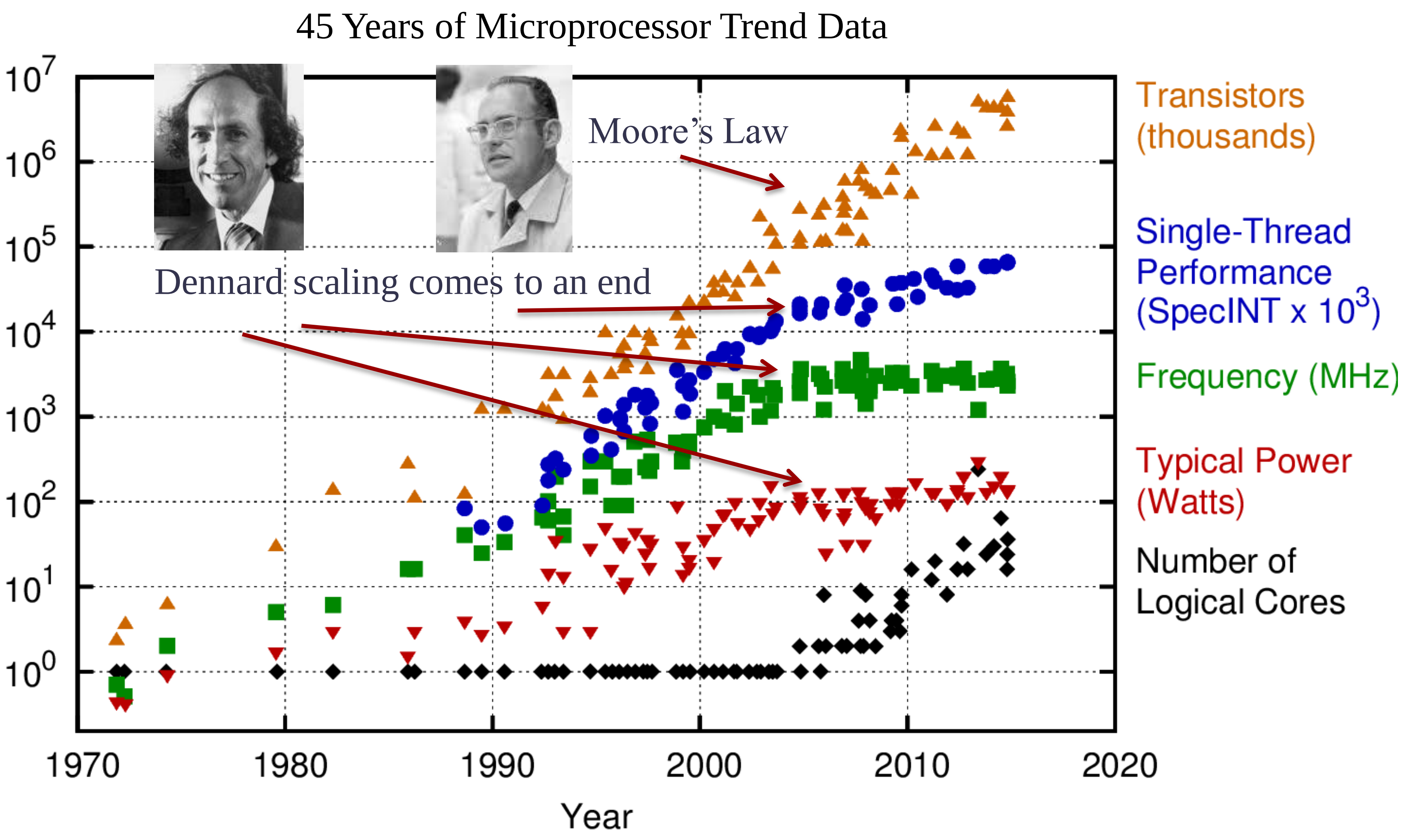
What did Feynman say:

> the problem is, how can we simulate the quantum mechanics?
>
> we can say: Let the computer itself be built of quantum mechanical elements which obey quantum mechanical laws.

Feynman was interested in Quantum Simulation:
when quantum computers simulate other quantum systems

Why else is quantum computing interesting?

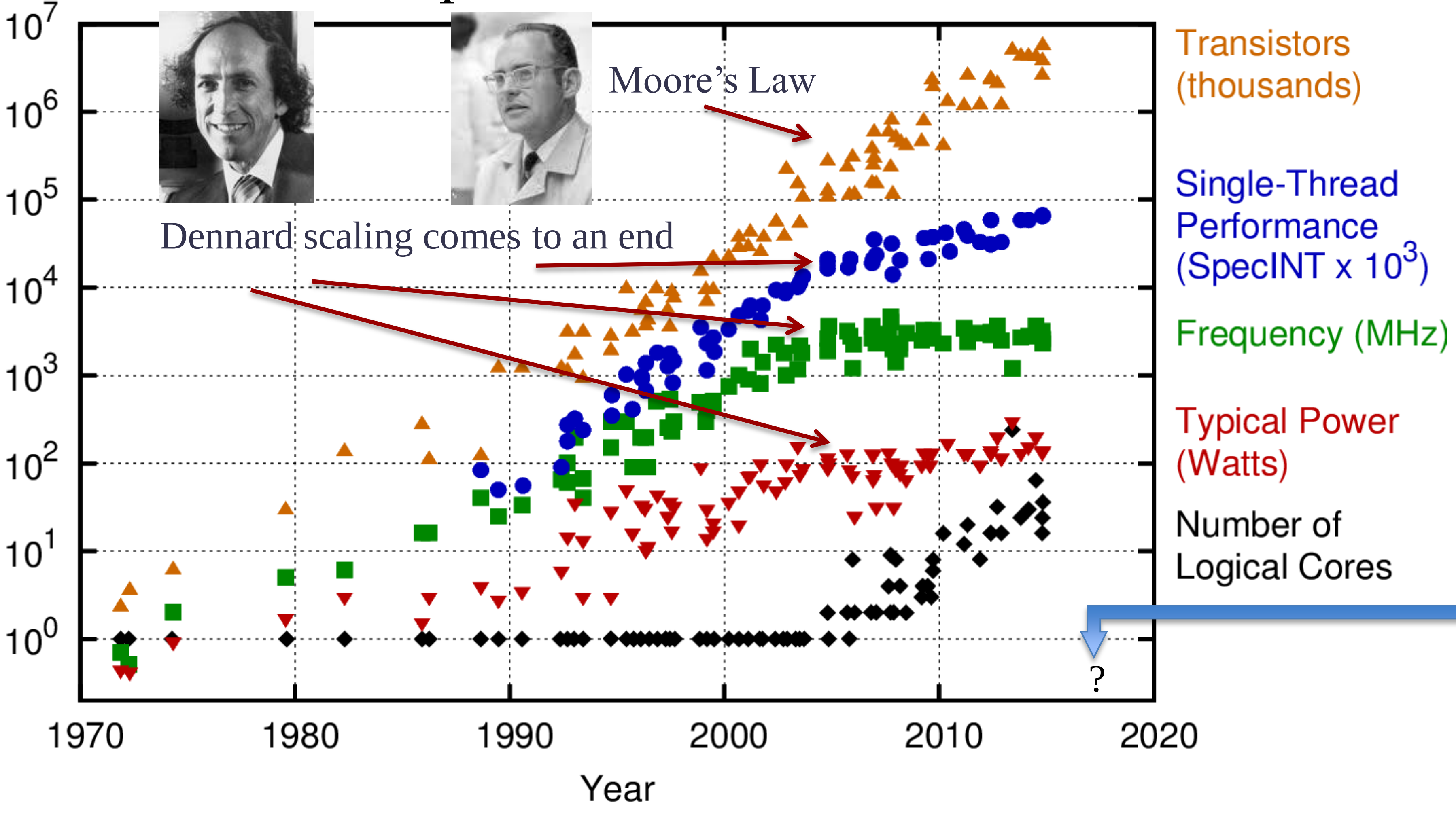
Inevitability



Original data up to the year 2010 collected and plotted by M. Horowitz, F. Labonte, O. Shacham, K. Olukotun, L. Hammond, and C. Batten
New plot and data collected for 2010-2015 by K. Rupp

Inevitability

classical chips hit "the wall of too small"



Si atom radius ~0.2nm;
at 22nm, current
"Ivy Bridge" processors
~100 atoms wide

11nm is on Intel's roadmap
~50 atoms wide;
dielectric thickness ~6 atoms

Quantum effects inevitable!
Anticipated by Feynman…

Original data up to the year 2010 collected and plotted by M. Horowitz, F. Labonte, O. Shacham, K. Olukotun, L. Hammond, and C. Batten
New plot and data collected for 2010-2015 by K. Rupp

Inevitability

"… it seems that the laws of physics present no barrier to reducing the size of computers until bits are the size of atoms, and **quantum behavior holds sway**."

Richard Feynman (1981)

USC University of Southern California

Inevitability → The way out

"… it seems that the laws of physics present no barrier to reducing the size of computers until bits are the size of atoms, and **quantum behavior holds sway**."

Richard Feynman (1981)

- Quantum computers naturally operate at the atomic scale
- They offer a path beyond Dennard scaling
- And so much more…

USC University of Southern California

Amazing algorithmic speedups

When we compute using quantum laws:

Factoring: Shor's algorithm

Factor an n-digit integer

Peter Shor (1994)

Exponential speedup

Best classical: $O(2^{n^{1/3}(\log(n))^{2/3}})$

Best quantum: $O(n^3)$

Simulating Q Field Theory

Compute scattering probabilities

Steve Jordan

Keith Lee

John Preskill

(2011)

Exponential speedup in strong-coupling and high-precision regimes

List search: Grover's algorithm

Find marked item in unsorted list of N items

Lov Grover (1996)

Quadratic speedup

Best possible classical: $\Omega(N)$

Best possible quantum: $O(\sqrt{N})$

Solving linear systems of equations

Solve $Ax = b$ for well-conditioned $A = n \times n$

Aram Harrow

Avinatan Hassidim

Seth Lloyd

(2008)

Exponential speedup

Return x in time $O(\log(n))$

Amazing algorithmic speedups

Hot off the press

Exponential Quantum Speed-ups for Semidefinite Programming with Applications to Quantum Learning

Fernando G. S. L. Brandão, Amir Kalev, Tongyang Li, Cedric Yen-Yu Lin, Krysta M. Svore, Xiaodi Wu

Oct 10 2017 quant-ph cs.DS arXiv:1710.02581v1

Semi-definite programming

Input: m constraint matrices of dimension n and rank r

Exponential speedup in n (for small m and r)

Best classical: $O(n)$

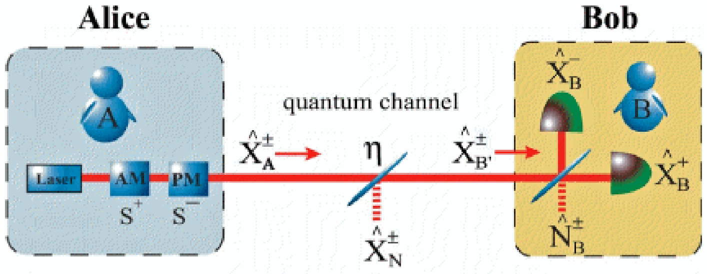
Best quantum: $O(\mathrm{polylog}(n))$

USC University of Southern California

Quantum Killer Aps

- Cybersecurity:
  - **Breaking** public key cryptography (Shor's algorithm)
  - Provably secure **encryption** (guaranteed by the laws of quantum physics)

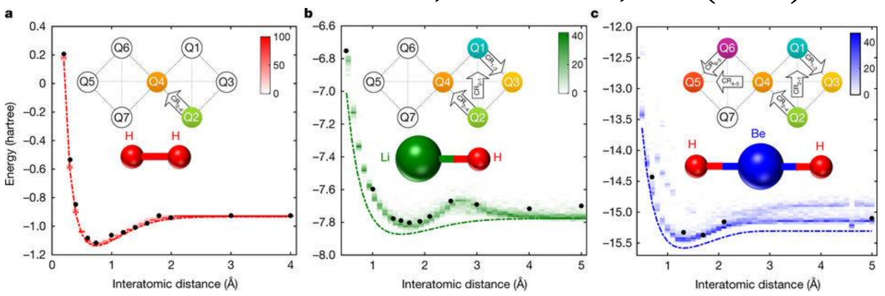
~~RSA SECURITY~~



- Exponentially faster **simulation** of quantum mechanics

→ discovery & first-principles design of novel materials, pharmaceuticals, …

A. Khandala et al., Nature 549, 242 (2017)



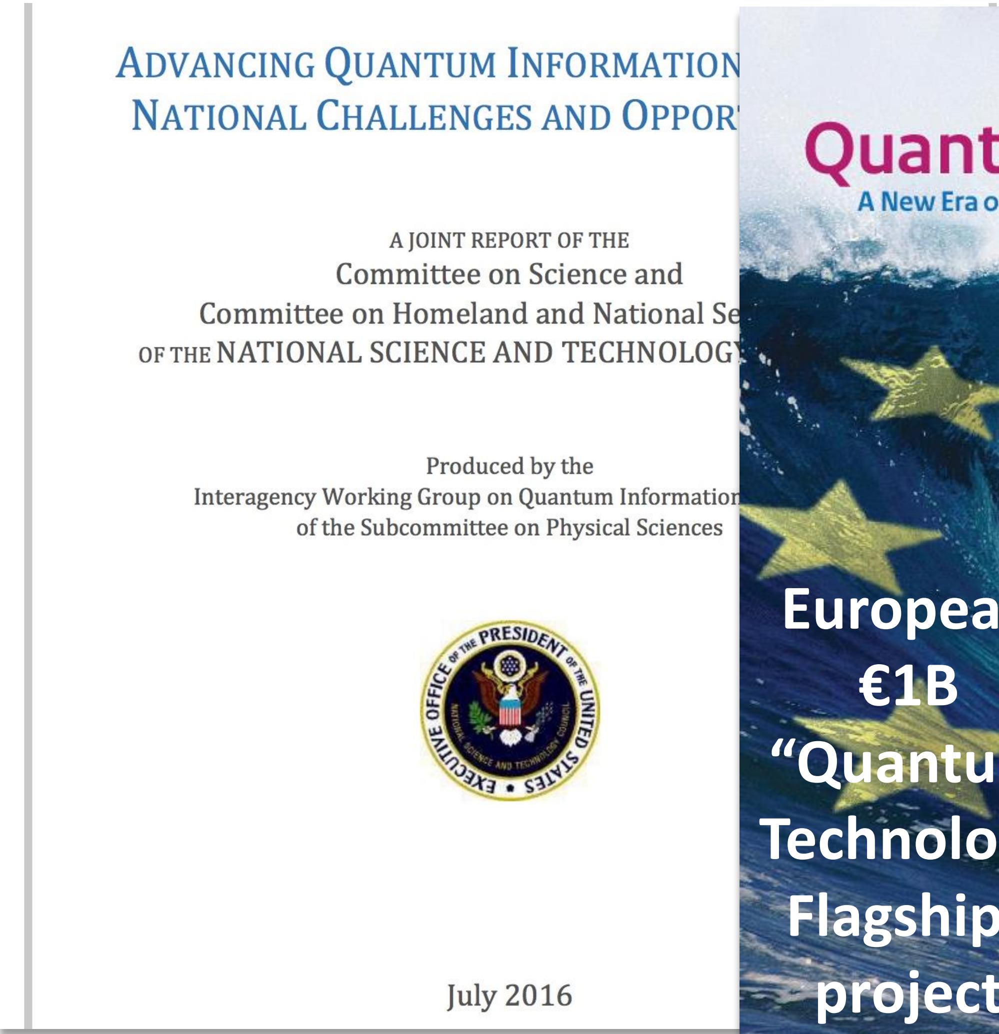
Molecular electronic structure on a superconducting QC

- Quantum speedups in **optimization**

→ machine learning, verification & validation, supply chain & logistics, finance, …

USC University of Southern California

Impact: governments worldwide took notice


ADVANCING QUANTUM INFORMATION
NATIONAL CHALLENGES AND OPPOR

A JOINT REPORT OF THE
Committee on Science and
Committee on Homeland and National Se
OF THE NATIONAL SCIENCE AND TECHNOLOGY

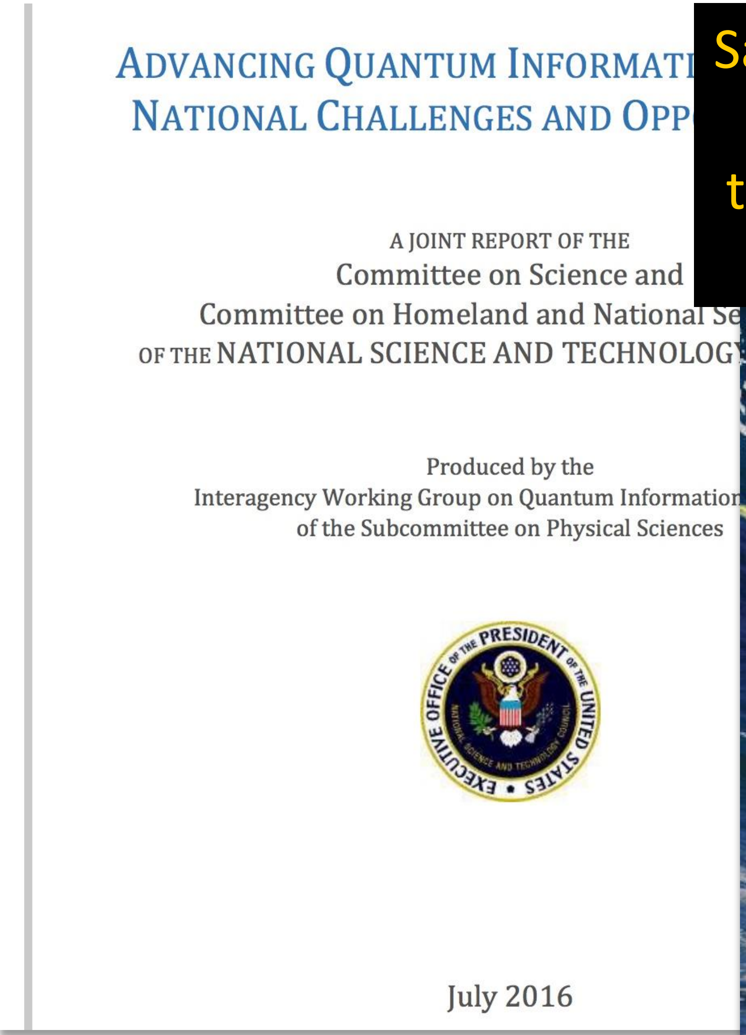
Produced by the
Interagency Working Group on Quantum Information
of the Subcommittee on Physical Sciences

July 2016

European €1B "Quantum Technology Flagship" project

$10B, 4m sq.ft.
source: Popular Science

Impact: governments worldwide took notice + companies


ADVANCING QUANTUM INFORMATI
NATIONAL CHALLENGES AND OPP

A JOINT REPORT OF THE
Committee on Science and
Committee on Homeland and National Se
OF THE NATIONAL SCIENCE AND TECHNOLOGY

Produced by the
Interagency Working Group on Quantum Information
of the Subcommittee on Physical Sciences

July 2016

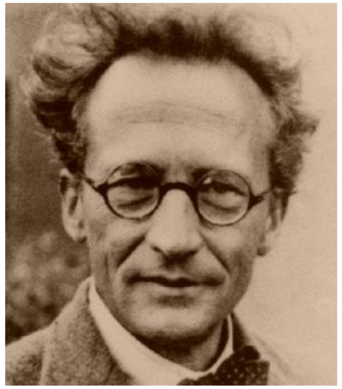
Satya Nadella, Microsoft CEO, in his new 2017 book “Hit Refresh”:

the battle over quantum computing is “an arms race” as important as AI or virtual and augmented reality, though it has “gone largely unnoticed”

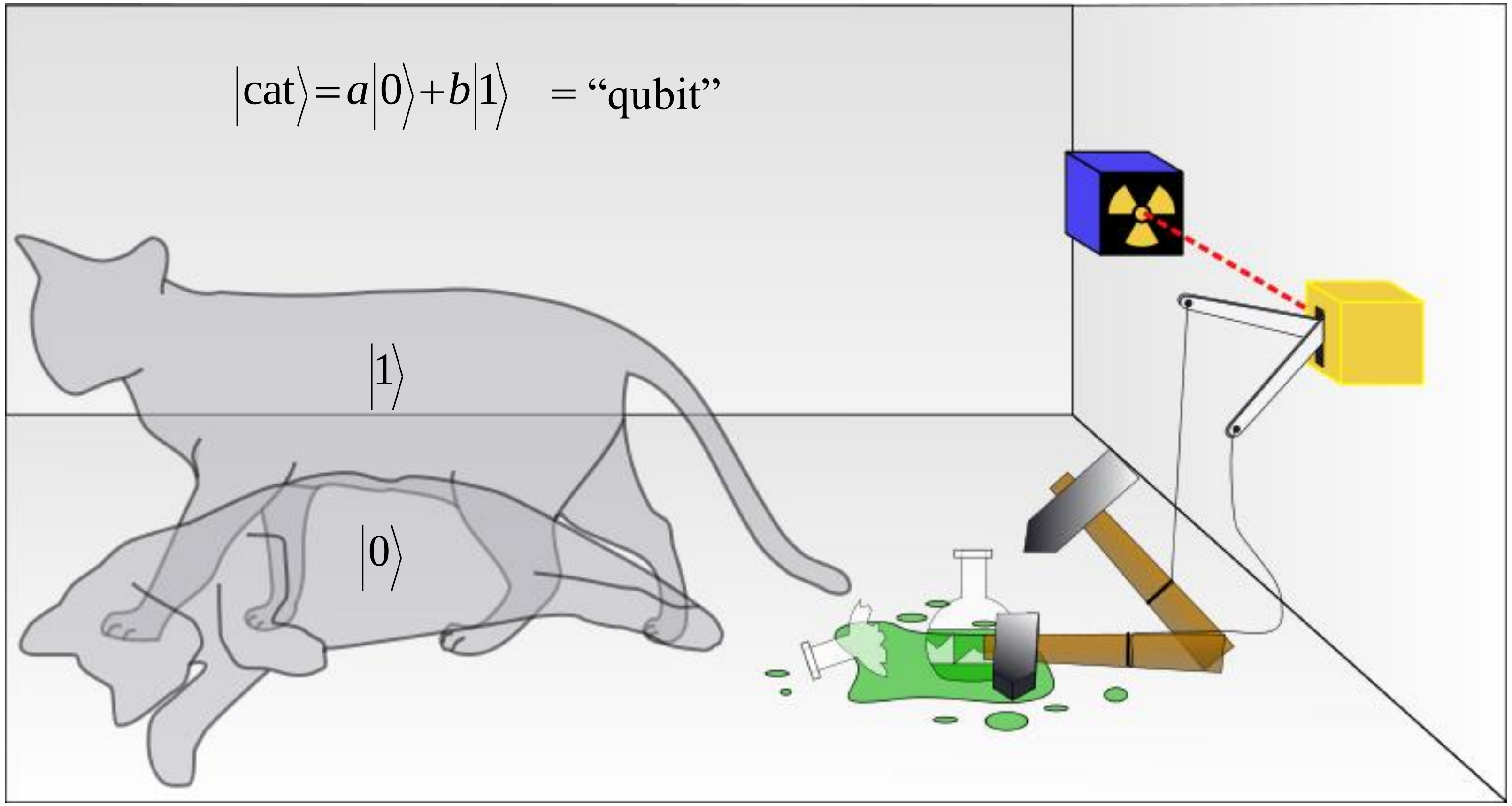
What is the source of this quantum power?

Quantum superposition

Erwin Schrödinger (1887-1961)
quantum pioneer,
inventor of famous cat



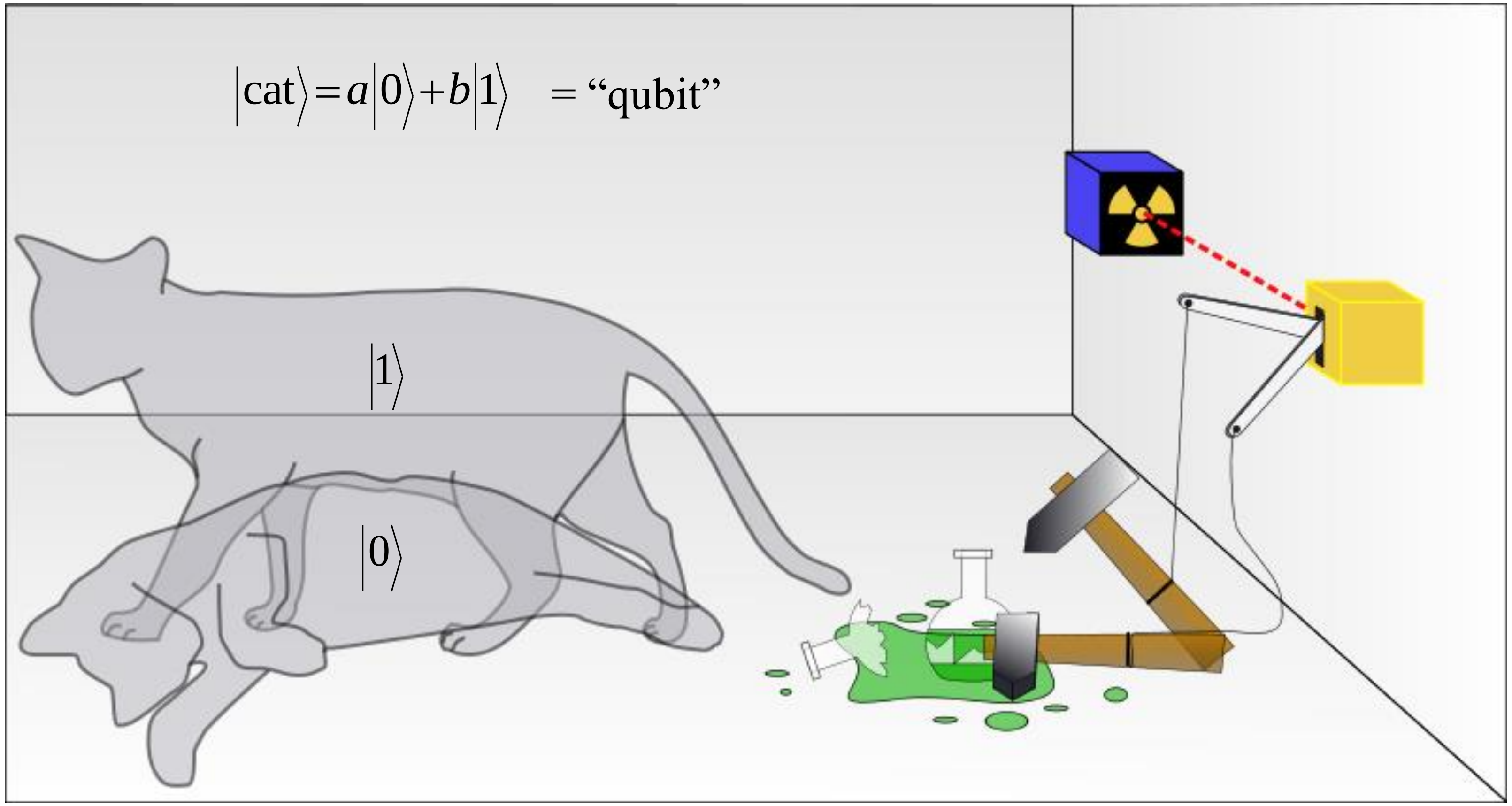
The superposition principle



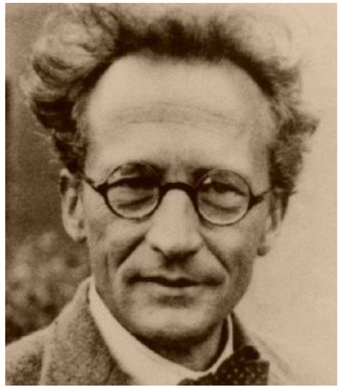
Quantum superposition

~~mystery~~ → useful resource

The superposition principle

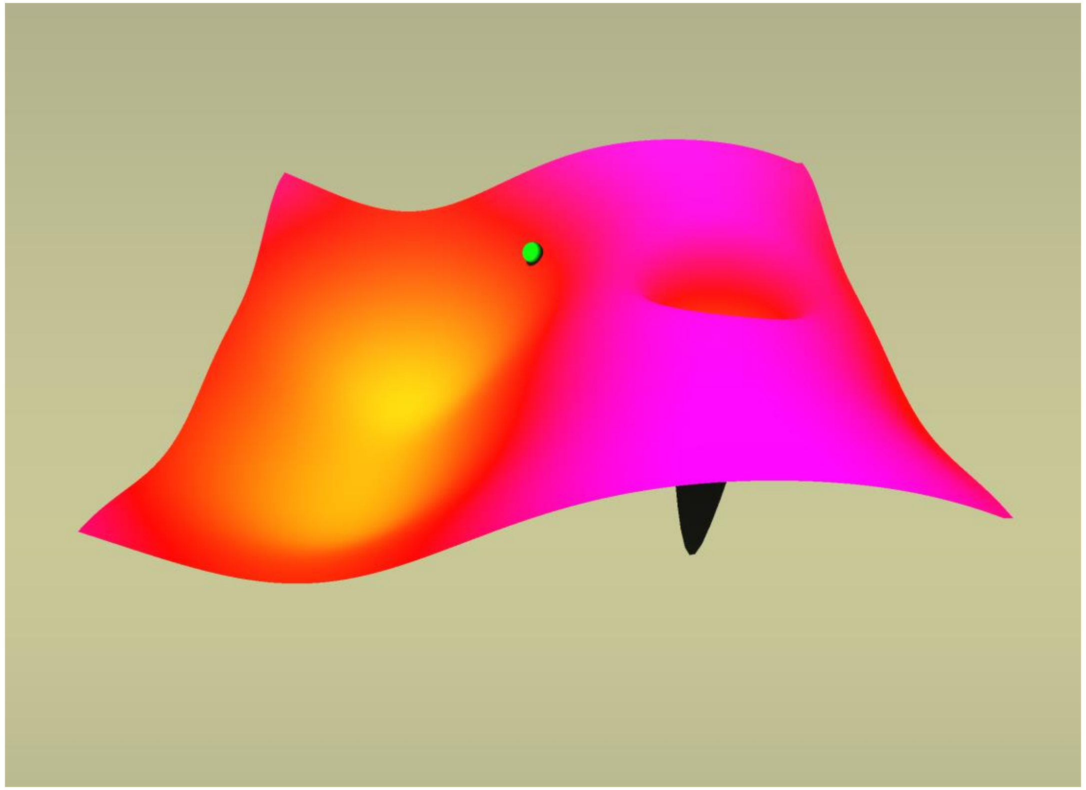


Erwin Schrödinger (1887-1961)
quantum pioneer,
inventor of famous cat



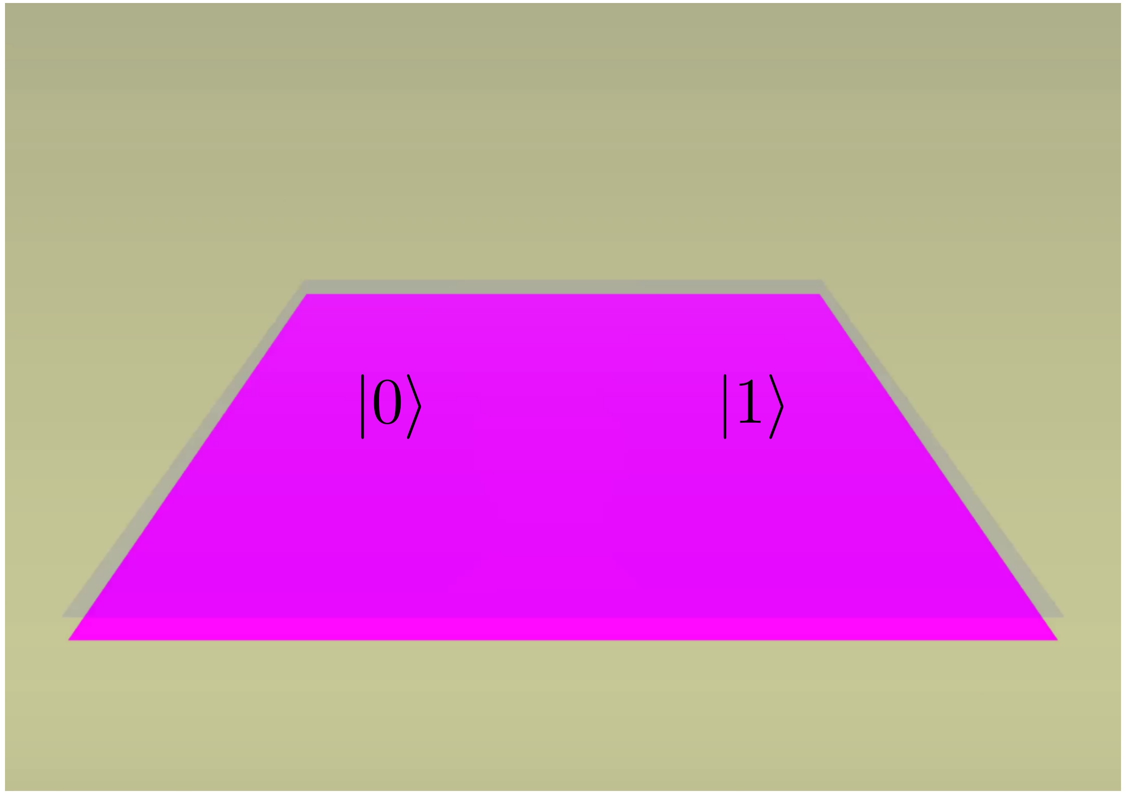
Quantum superposition as a resource

classical



random walk with gradient descent

quantum



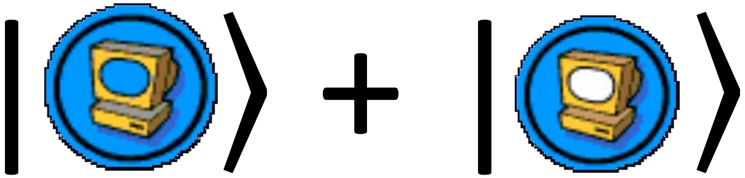
superposition, interference, tunneling

The bad news: Decoherence

Every real quantum computer interacts with its **environment** (don’t we all)

The environment acts as an uncontrollable observer, making random measurements

Destroys the quantum computer’s superposition states



USC University of Southern California

The bad news: Decoherence

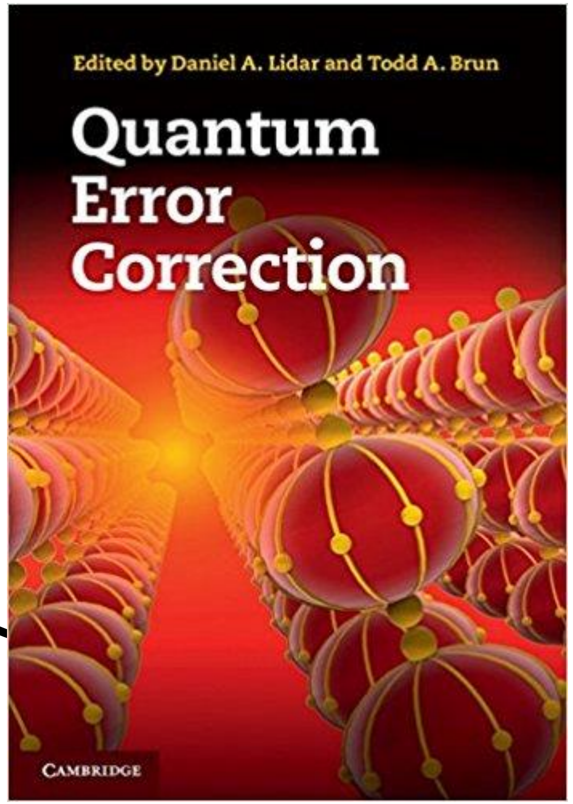
Every real quantum system interacts with its environment.

The environment acts as an uncontrollable observer, making random measurements

Destroys the quantum computer’s superposition states.

Bad news for quantum computation:

Theorem: A sufficiently decohered quantum computer can always be efficiently simulated on a classical computer.



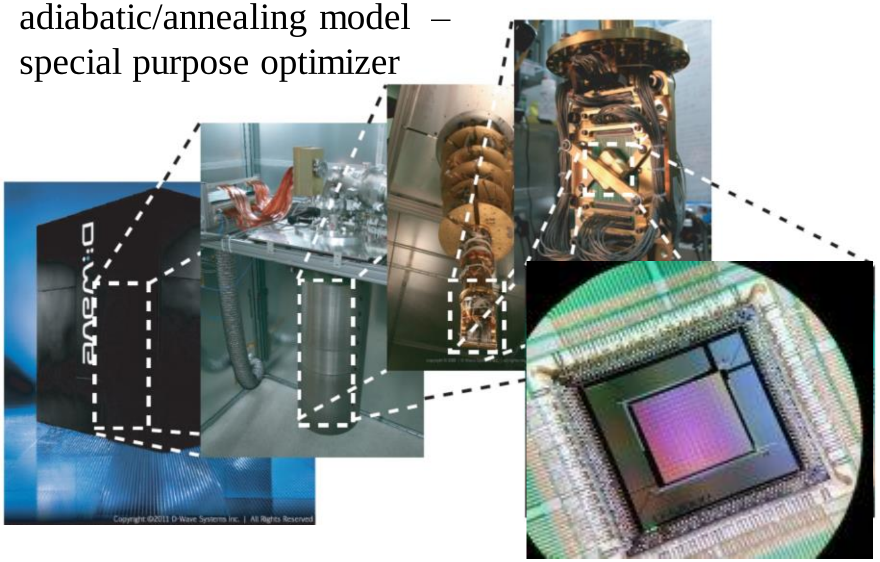
Solution: Quantum Error Correction

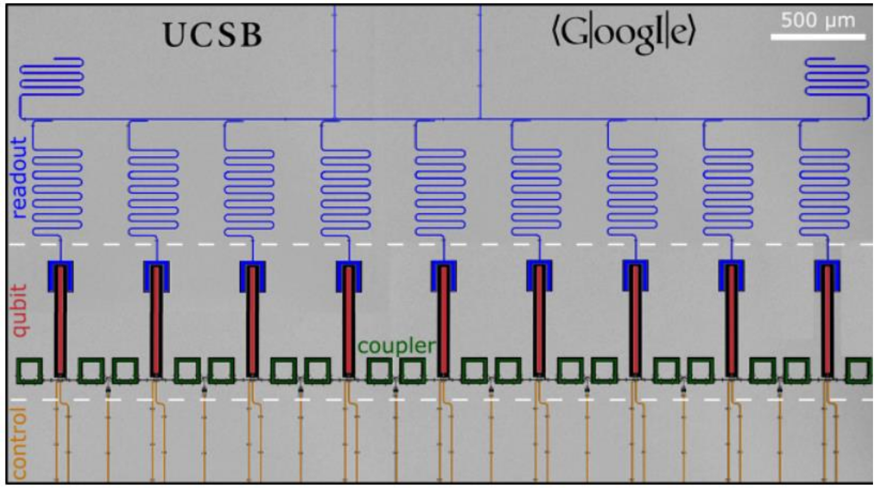
Quantum computers will never scale up without it!

USC University of Southern California

What is a quantum computer – really? A representative sample

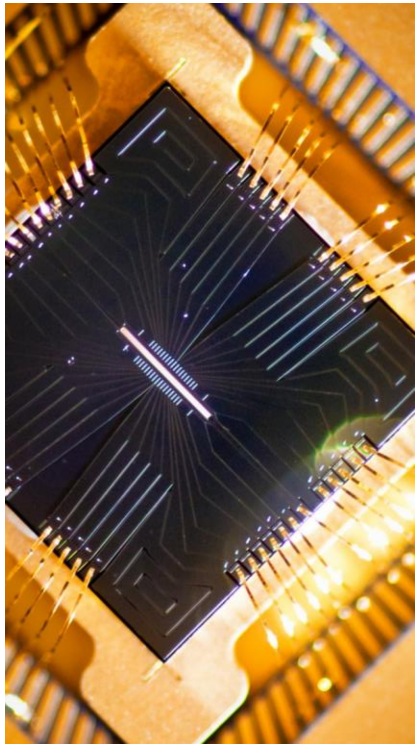
adiabatic/annealing model – special purpose optimizer





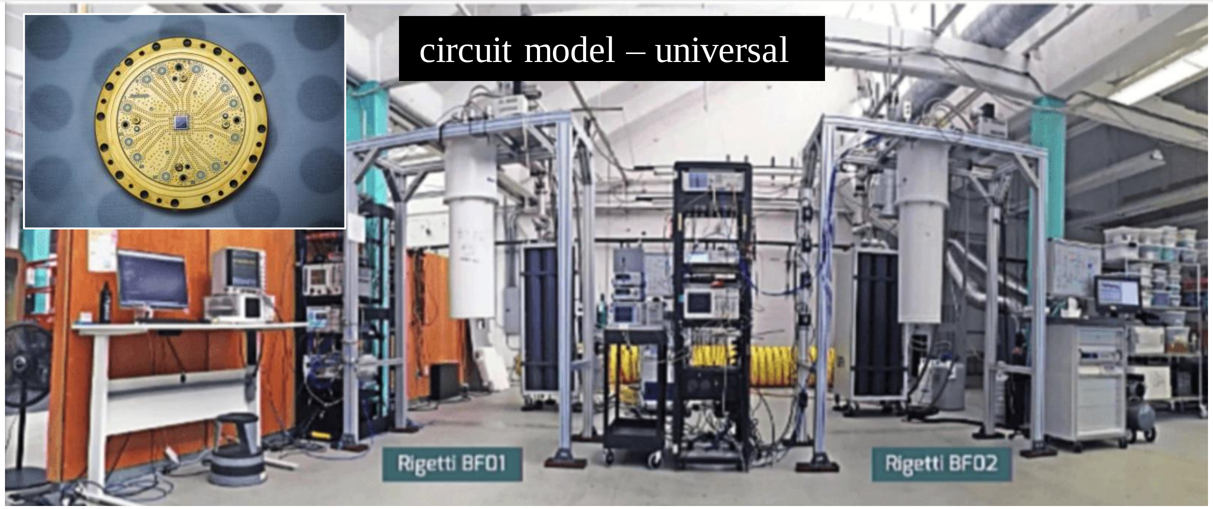
circuit model – universal (general purpose)

circuit model –universal



IONQ

Very unlike classical computers!



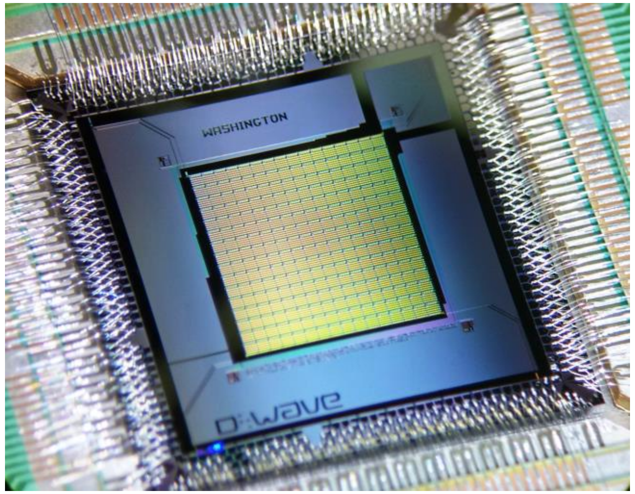
circuit model – universal

USC University of Southern California

Quantum Computing @ USC - highlights

USC-Lockheed Martin Quantum Computing Center

- multi-$M investment by Lockheed Martin in three generations of D-Wave quantum annealers
- Operational at USC since 2011. Followed by Google/NASA Google/NASA (2013), Los Alamos National Lab (2016), (2016), &TDS/ORNL/UofT



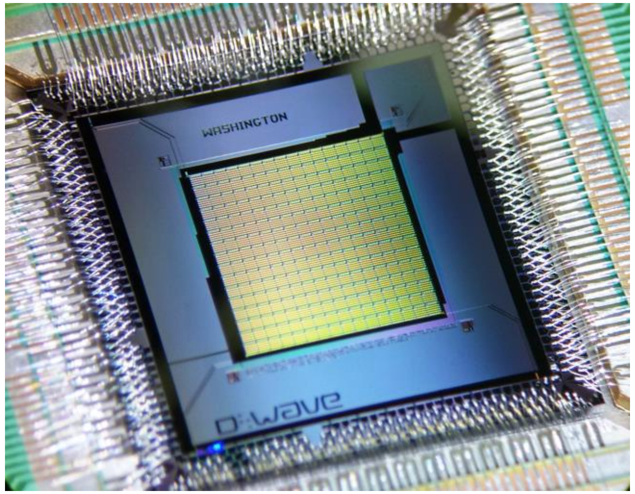
D-Wave 2X, 1098 qubits

USC University of Southern California

Quantum Computing @ USC - highlights

USC-Lockheed Martin Quantum Computing Center

- multi-$M investment by Lockheed Martin in three generations of D-Wave quantum annealers
- Operational at USC since 2011. Followed by Google/NASA Google/NASA (2013), Los Alamos National Lab (2016),



D-Wave 2X, 1098 qubits

IARPA Quantum Enhanced Optimization Program

- multi-$M / 5yr contract awarded to USC this year
- Goal: build a new 100-qubit quantum annealer using high-coherence (Al) superconducting flux qubits, for quantum optimization and sampling applications

MIT

MIT Lincoln Laboratory

HARVARD UNIVERSITY

California Institute of Technology 1891

Berkeley UNIVERSITY OF CALIFORNIA

USC University of Southern California Information Sciences Institute

UCL

UNIVERSITY OF WATERLOO

UNIVERSITÄT DES SAARLANDES

東京工業大学 Tokyo Institute of Technology

LOCKHEED MARTIN

NORTHROP GRUMMAN

The impact of quantum computing: short (<5yrs), and longer term (>5yrs)

Factoring, the holy grail: A long road ahead

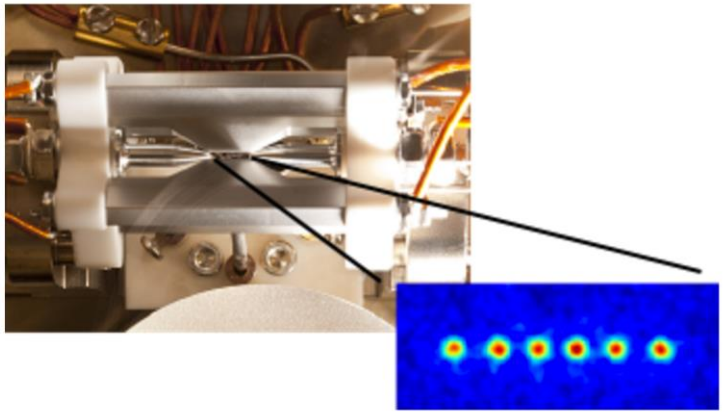
Factoring state of the art:
using 5 Ca^+ trapped ions…

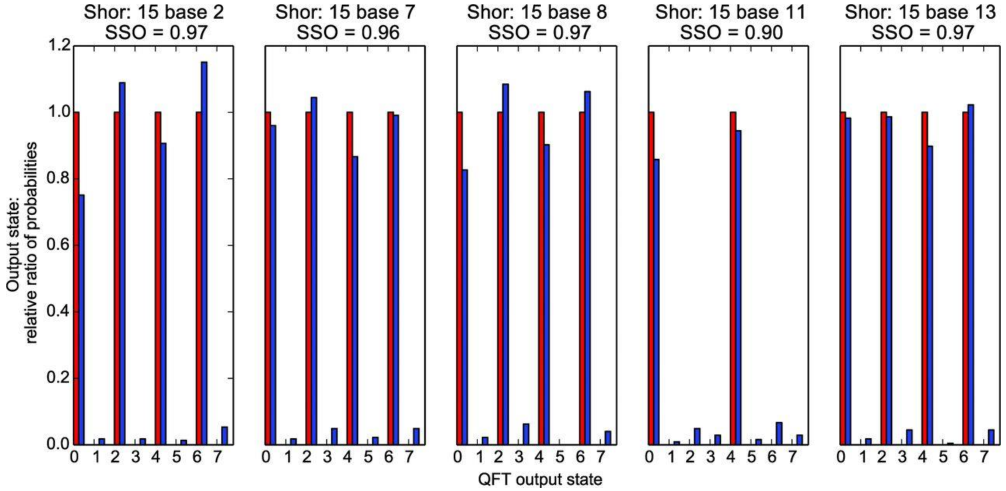
$$15 = 3 \times 5$$

with 99% confidence

143 has also been factored ($= 11 \times 13$), but using liquid-state nuclear magnetic resonance -- a non-scalable QC technology

Focus on more attainable near-term goals





T. Monz *et al*. Science **351** ,1068-1070 (2016)
(Blatt group)

The impact of quantum computing: short (<5yrs)

- Quantum simulation
- Quantum supremacy

The impact of quantum computing: short term (<5yrs)

Advantage in Quantum Simulation

Goal: Demonstrate that a quantum computer performs a useful simulation task of another quantum system that is beyond the capability of any classical computer

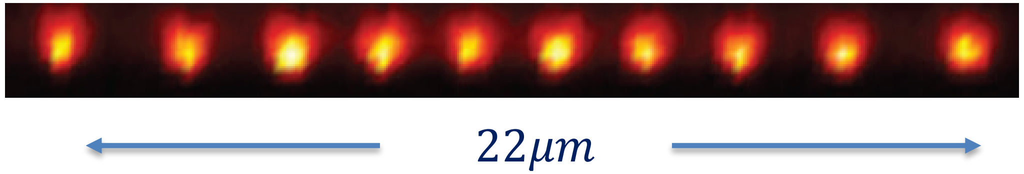
USC University of Southern California

The impact of quantum computing: short term (<5yrs)

Simulation of quantum magnetism, using trapped ions

Quantum phase transition from **paramagnet** to **antiferromagnet** in the transverse field Ising model

A



The impact of quantum computing: short term (<5yrs)

Simulation of quantum magnetism using trapped ions

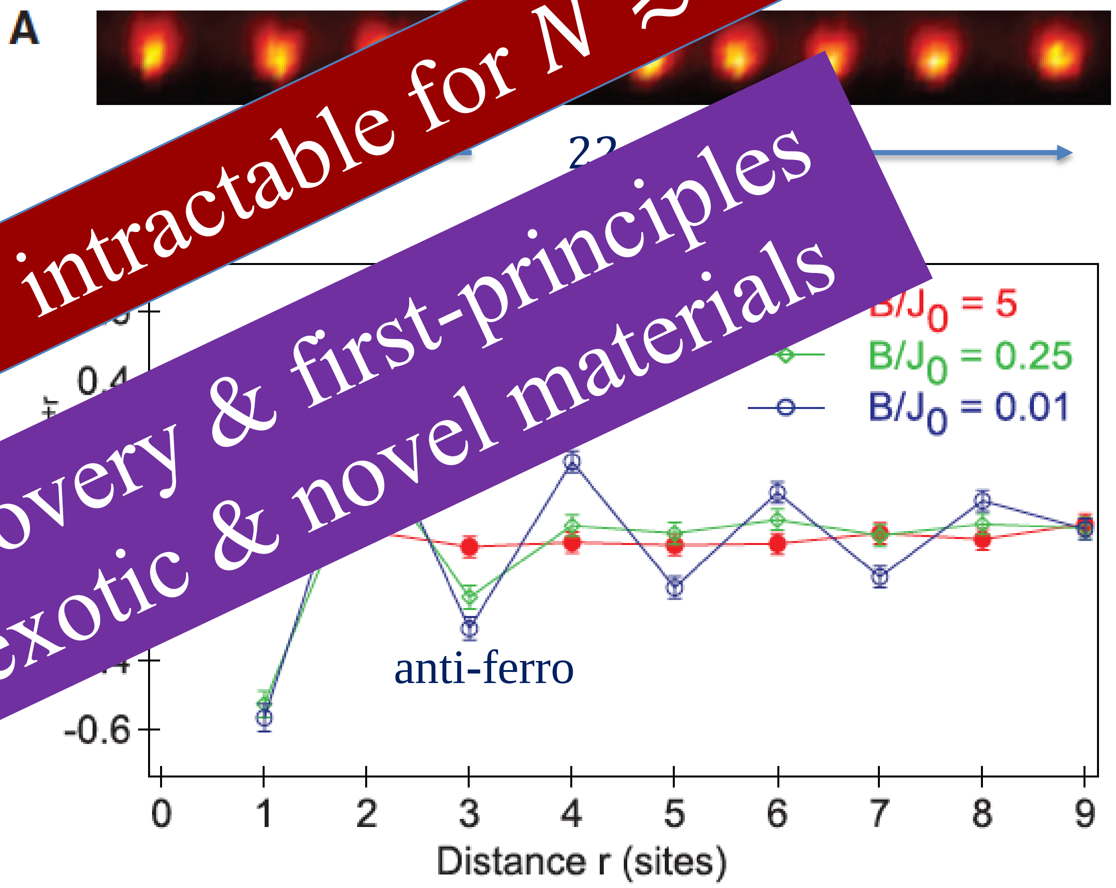
Quantum phase transition from **paramagnet** to **antiferromagnet** in the transverse field Ising model

Science AAAS

Emergence and Frustration of Magnetism with Va... Interactions in a Quantum Simulator
R. Islam *et al.*
Science **340**, 583 (2013);
DOI: 10.1126/science.1232296

$$H = \sum \ldots - B\sum \ldots$$

$$J_{ij} \approx \frac{J_0}{|i-j|^{\alpha}}$$



Classically numerically intractable for $N \gtrsim 40$

Impact: discovery & first-principles design of exotic & novel materials

The impact of quantum computing: short term (<5yrs)

More ambitious goal: "Quantum Supremacy"

Demonstrating that a quantum computer performs a (possibly useless!) computational task that is beyond the capability of any classical computer

Relies on a complexity-theoretic assumption of the form:

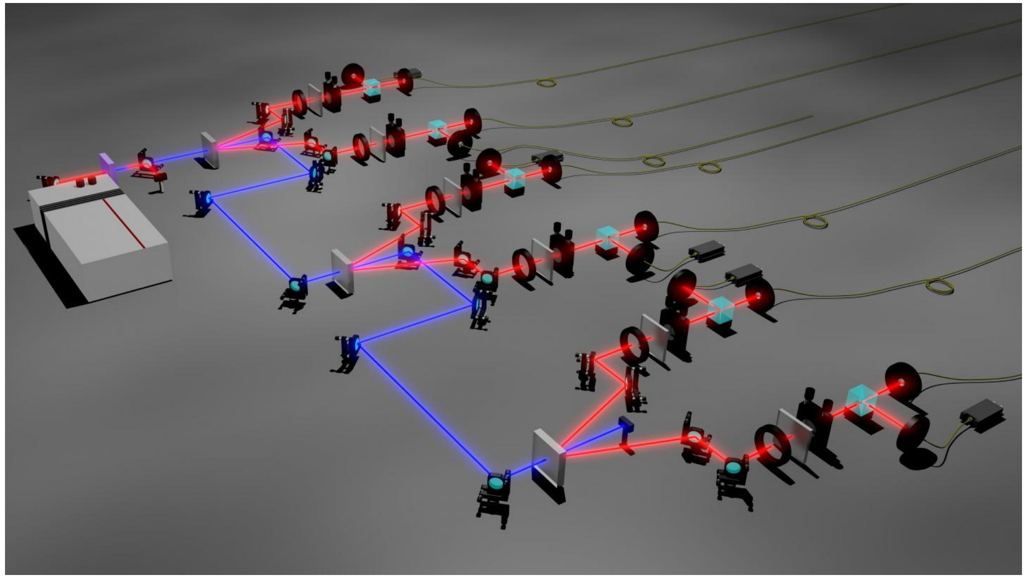
"If this task could be executed efficiently on a classical computer then the polynomial hierarchy would collapse (e.g., $P = NP$)"

Why is this important?

- Foundational: would refute the 'extended Church–Turing thesis', that classical computers can simulate any physical process with polynomial overhead
- Practical: would greatly increase our confidence in the eventual feasibility of large-scale quantum computing

The impact of quantum computing: short term (<5yrs)

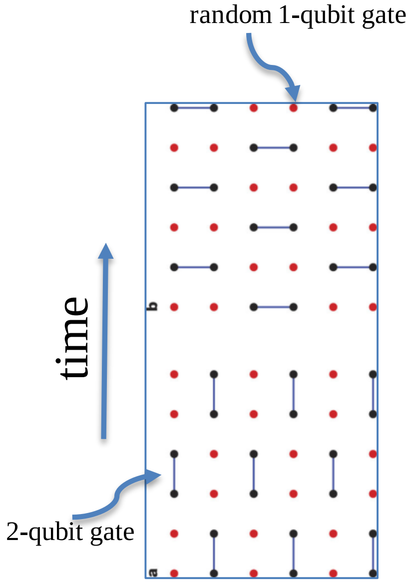
Quantum supremacy example: **Boson Sampling**

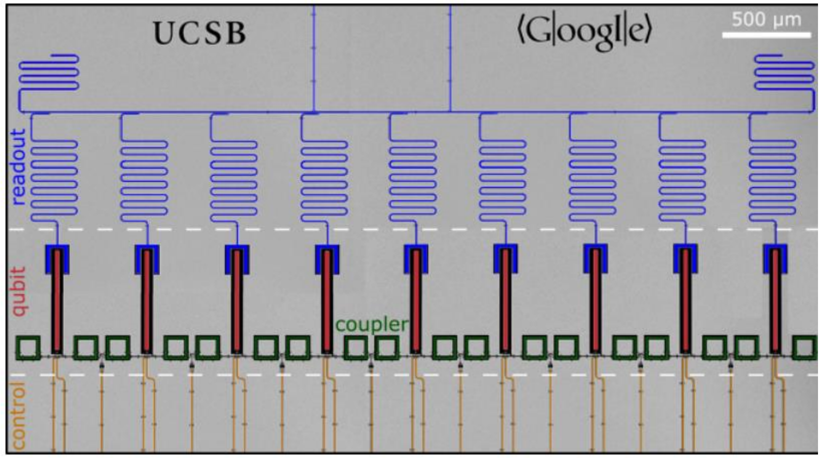


- **Problem:** Sample from the distribution of detections of non-interacting photons propagating through a random linear optics circuit
- Estimated to be classically hard already for 7 photons (Latmiral et al., New J. Phys. (2016))
- 5 photons already demonstrated (Wang et al., Nature Photon. (2017))
- New estimates for beating current-best classical algorithms (Neville et al., Nature Phys. (2017)):
  - >50 photons in well-defined modes
  - low-loss photon propagation in thousands of modes
  - thousands of high-efficiency detectors
  - precise setting of millions of phase shifters
- May not be practical in <5yrs after all

Quantum supremacy example: **Random Circuit Sampling**

- **Problem:** Sample from the distribution of strings output by a random circuit
- Estimated to be classically hard for ~50 qubits (Boixo et al., arXiv:1608.00263)
- Current 9 qubit "gmon" experiments on track (Neill et al., arXiv:1709.06678)
- Google hopes to reach 50 qubits and a quantum supremacy demo in <1yr



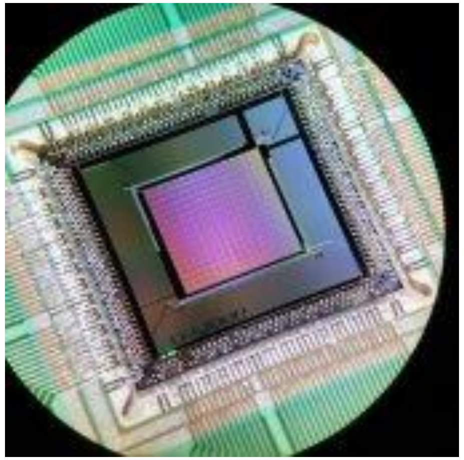


The impact of quantum computing: short term (<5yrs)

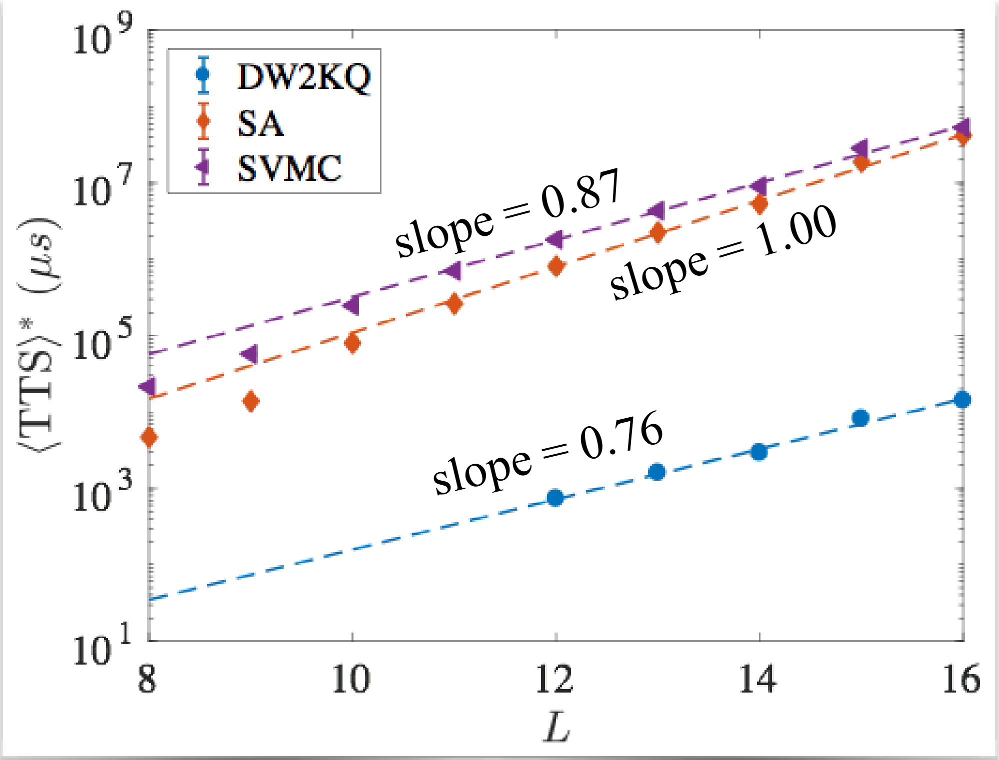
Partial quantum supremacy: **limited quantum speedup**

- **Problem:** Find the lowest-energy spin configurations of spin glasses
- A notorious NP-hard problem (Barahona, 1982)
- We've demonstrated a speedup for D-Wave against classical simulated annealing and "spin-vector Monte Carlo" (T. Albash & DL, arXiv:1705.07452)

D-Wave 2000Q processor



time-to-solution as a function of problem size



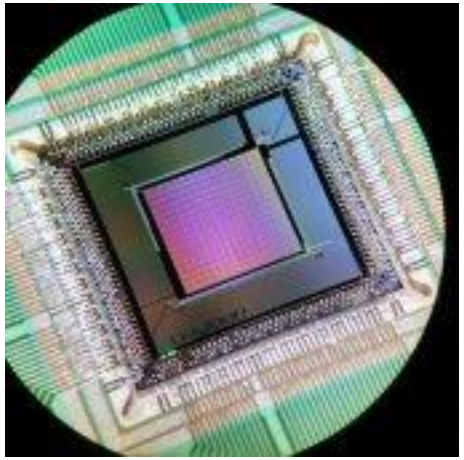
number of qubits = $8 \times L^2$

The impact of quantum computing: short term (<5yrs)

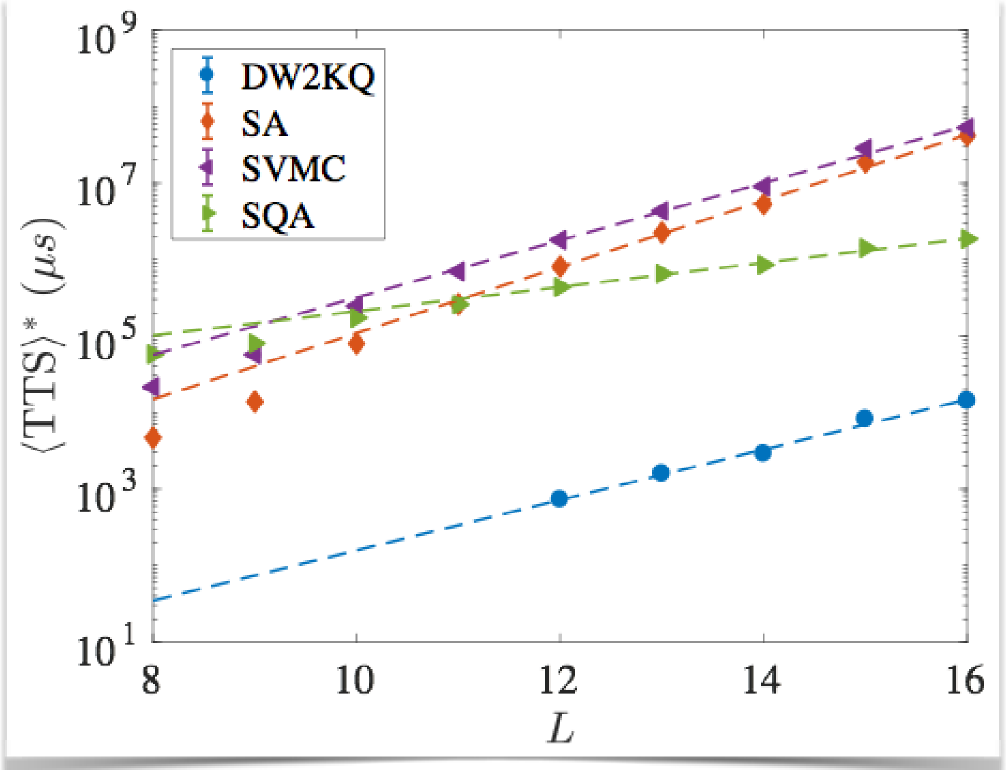
Partial quantum supremacy: **limited quantum speedup**

- **Problem:** Find the lowest-energy spin configurations of spin glasses
- A notorious NP-hard problem (Barahona, 1982)
- We've demonstrated a speedup for D-Wave against classical simulated annealing and "spin-vector Monte Carlo", but not against quantum simulated annealing (T. Albash & DL, arXiv:1705.07452)

D-Wave 2000Q processor



time-to-solution as a function of problem size



number of qubits = $8 \times L^2$

We remain hopeful we're on the right track!

The impact of quantum computing: short term (<5yrs)

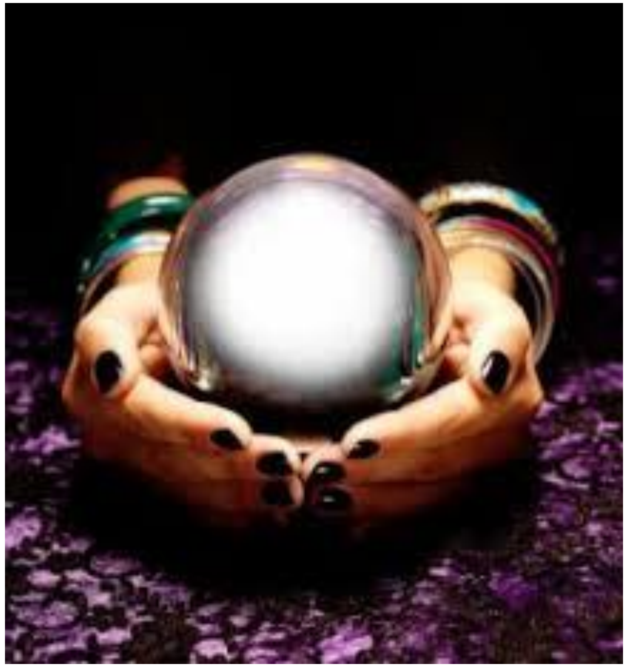
Quantum Supremacy – the race is on

However it is achieved:

Quantum computation that exceeds
the reach of classical computers
will mark the beginning of a
new era of quantum science

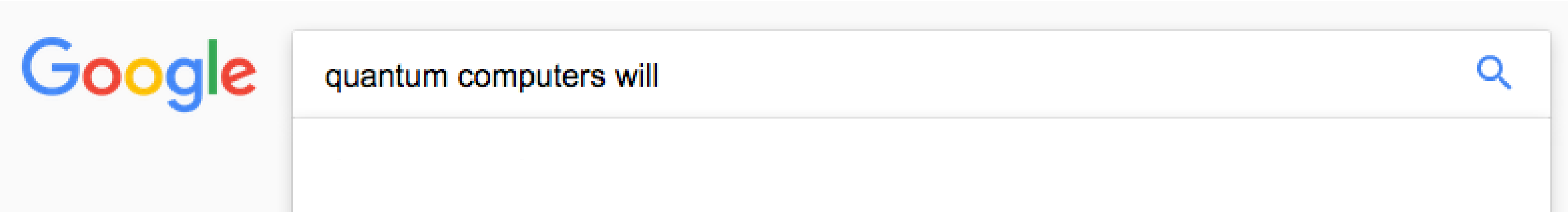
Feasible in < 5 years

The impact of quantum computing: longer term (>5yrs)



The impact of quantum computing: longer term (>5yrs)

I’m no oracle; let’s ask PageRank



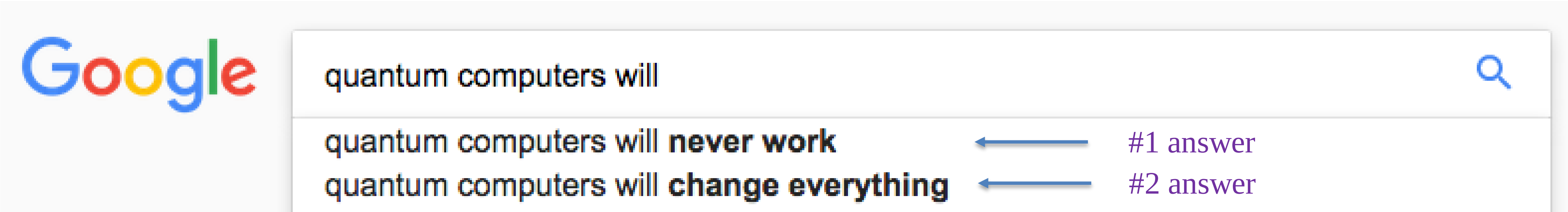
The impact of quantum computing: longer term (>5yrs)

Google

quantum computers will

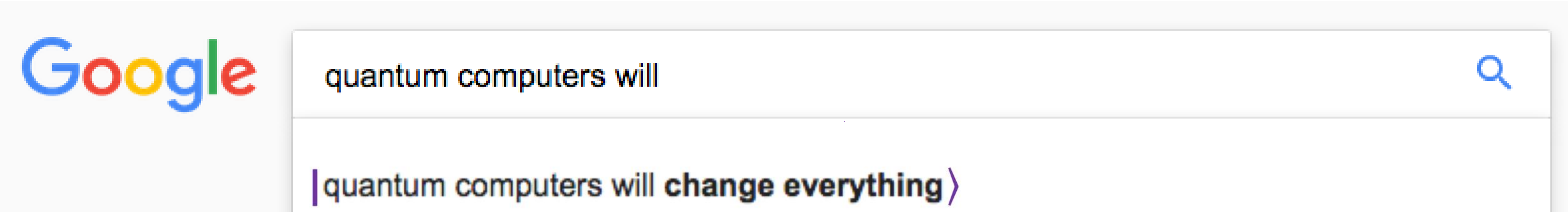
quantum computers will **never work** ← #1 answer

The impact of quantum computing: longer term (>5yrs)



USC University of Southern California

The impact of quantum computing: longer term (>5yrs)



Thanks!