Quantum Computing: Algorithms and Implementation

Kyle Gordon
Peng Xu
Yichen Zhao

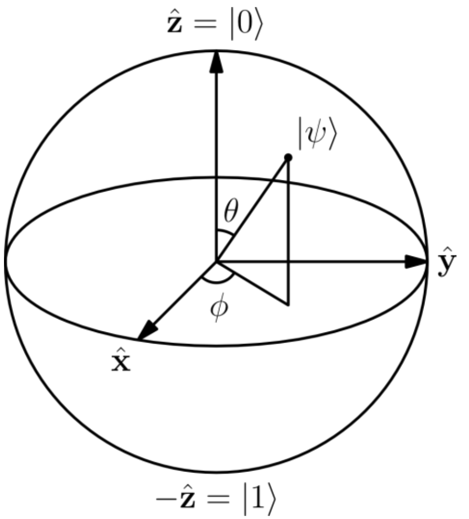
Introduction

Theory
Quantum Parallelism, Decoherence

Algorithms
Factoring, Quantum Fourier Transform

Physical Realization
Quantum Dots, NMR, SQUID, D-Wave

THEORY



$\hat{\mathbf{z}} = |0\rangle$
$|\psi\rangle$
θ
$\hat{\mathbf{y}}$
ϕ
$\hat{\mathbf{x}}$
$-\hat{\mathbf{z}} = |1\rangle$

Motivation

"Quantum Theory is already important in the design of microelectronics components. But soon it will be necessary to harness quantum theory, rather than simply take it into account, to give components their functionality." David Deutsch

Qubit

Probability **a** of being 0

30% = 0.30

Probability **b** of being 1:

70% = 0.70

$$\text{Our Qubit} = \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0.30 \\ 0.70 \end{pmatrix}$$

Qubits exist in a *superposition* of 0 and 1

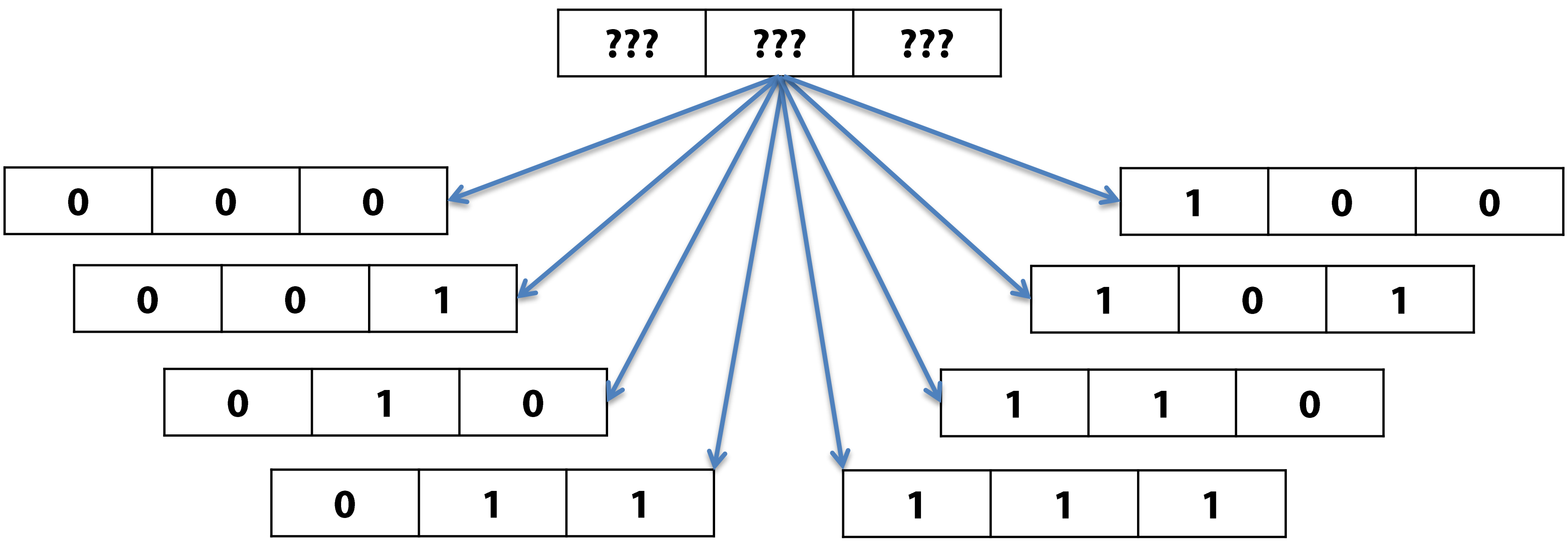
You can't do this classically!

Quantum Parallelism

3 bits in today's computer:

1	0	1

In quantum computer:



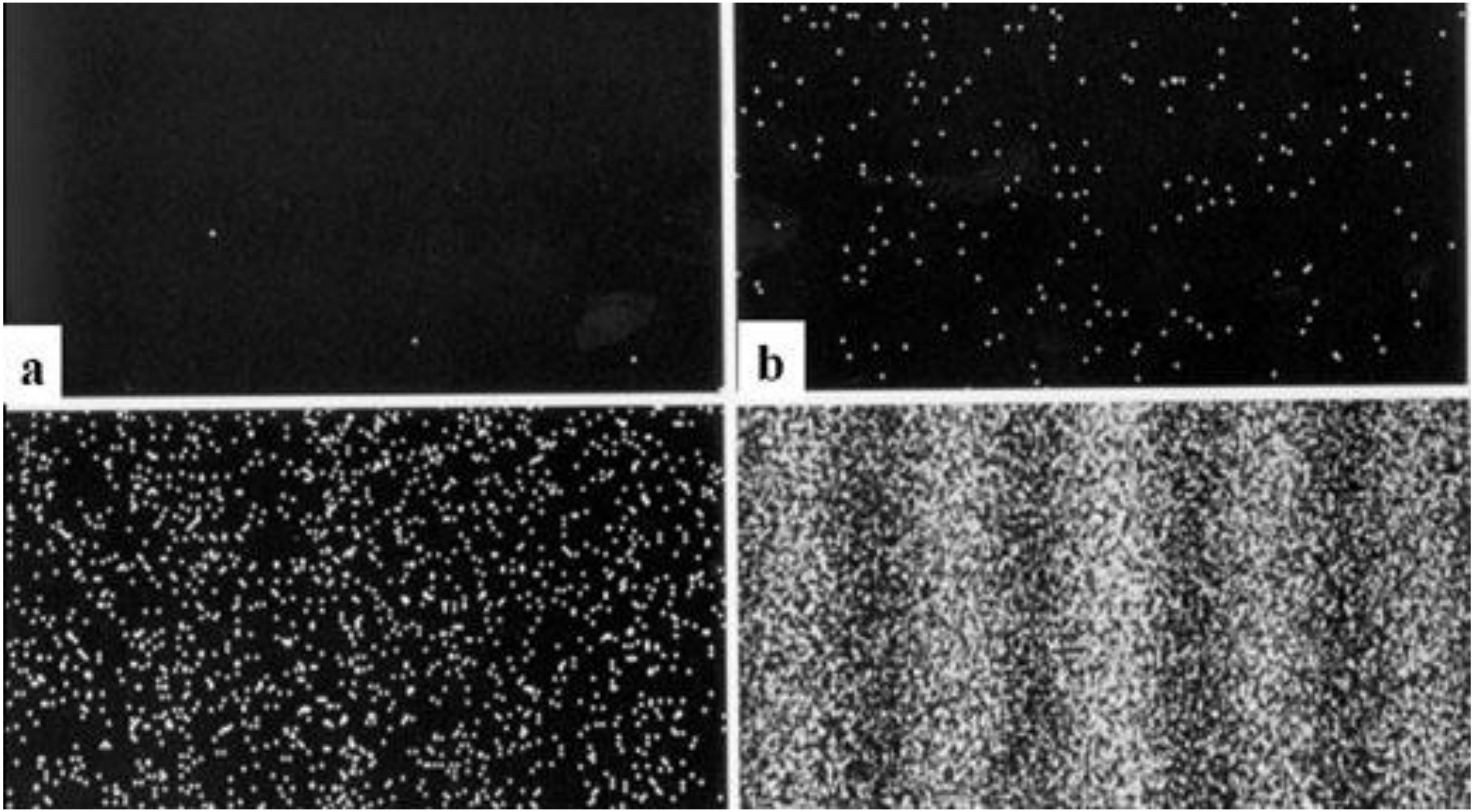
Quantum Parallelism

???	???	???	+ 1

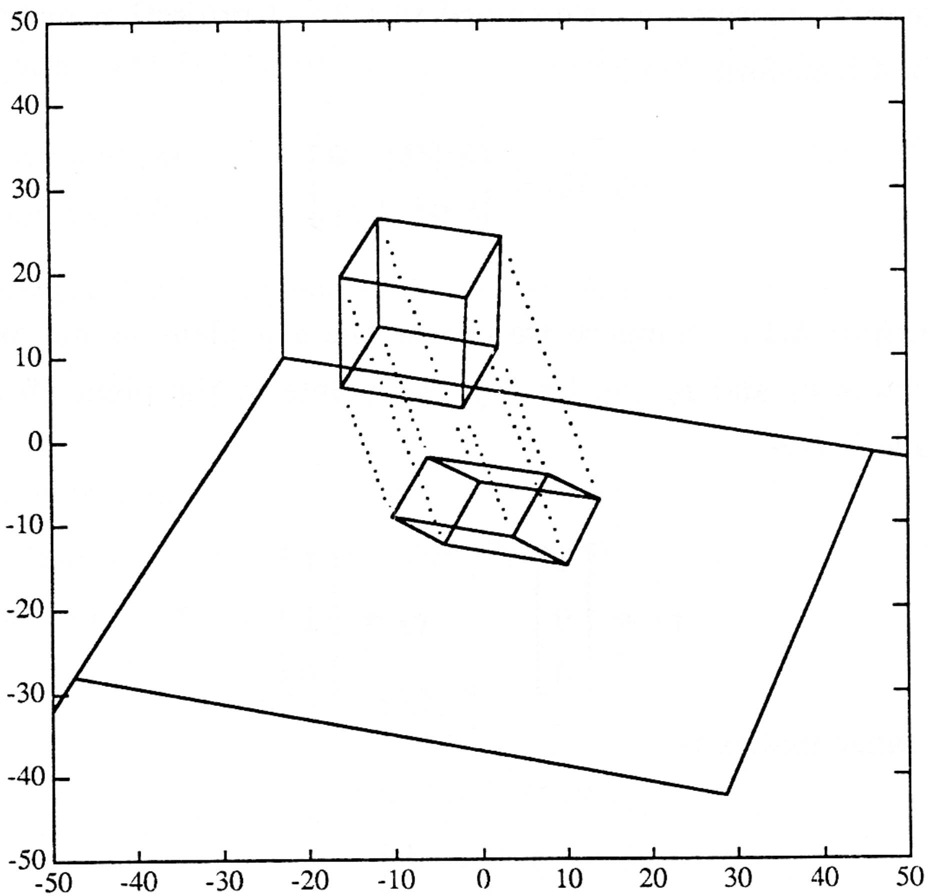
=

0	0	0	+ 1
0	0	1	+ 1
0	1	0	+ 1
0	1	1	+ 1
1	0	0	+ 1
1	0	1	+ 1
1	1	0	+ 1
1	1	1	+ 1

Decoherence

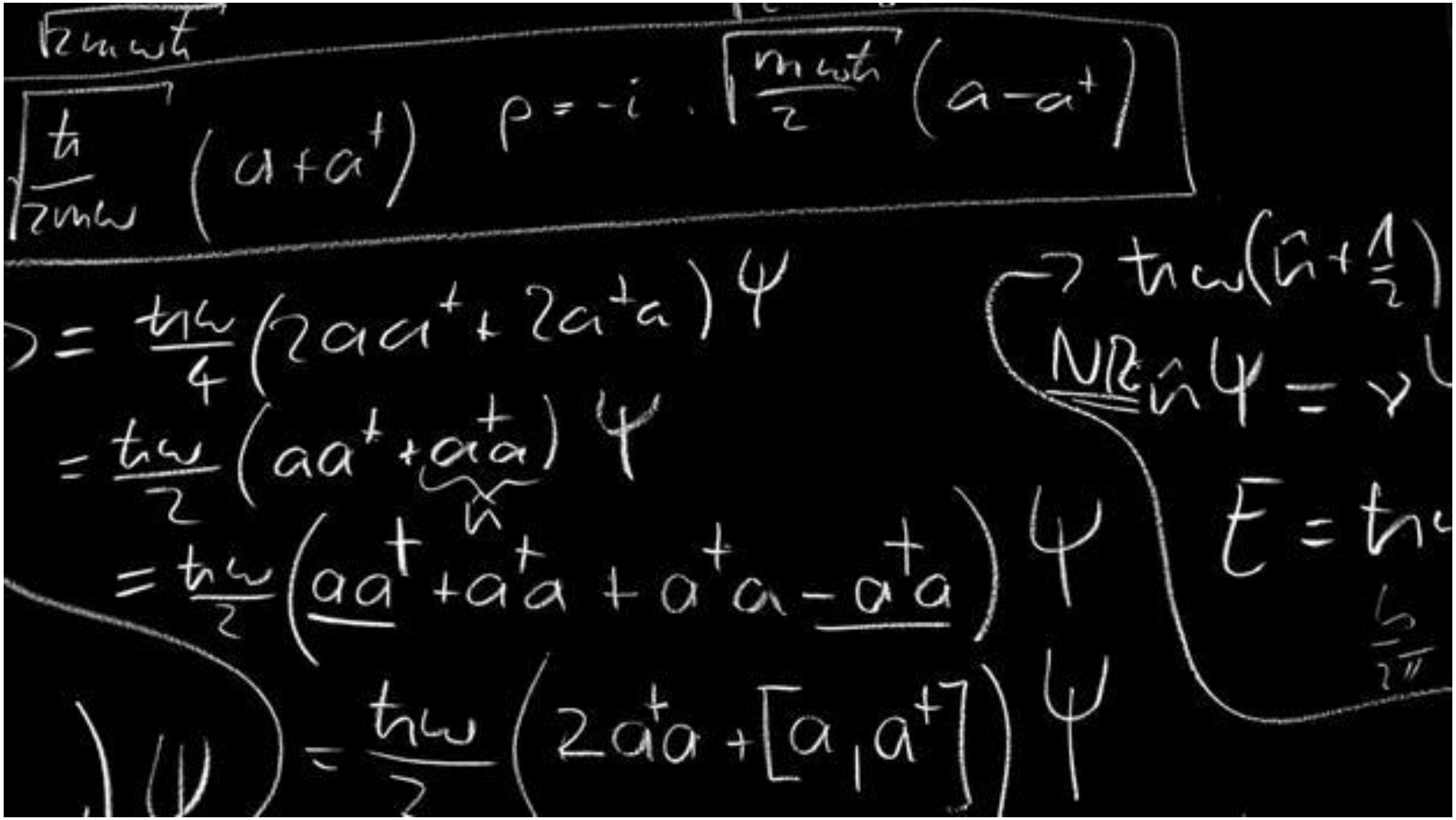


Decoherence



Think of it like projecting a box

It gives us a new representation of the same object, but we lose information about its original state



From: BBC

QUANTUM ALGORITHMS

Why Quantum Computing is fast

- Does it run regular instructions faster?

Why Quantum Computing is fast

- Does it run regular instructions faster?
- Not really

Quantum Algorithm

- An algorithm which runs on a realistic model(e.g. quantum circuit model) of quantum computation

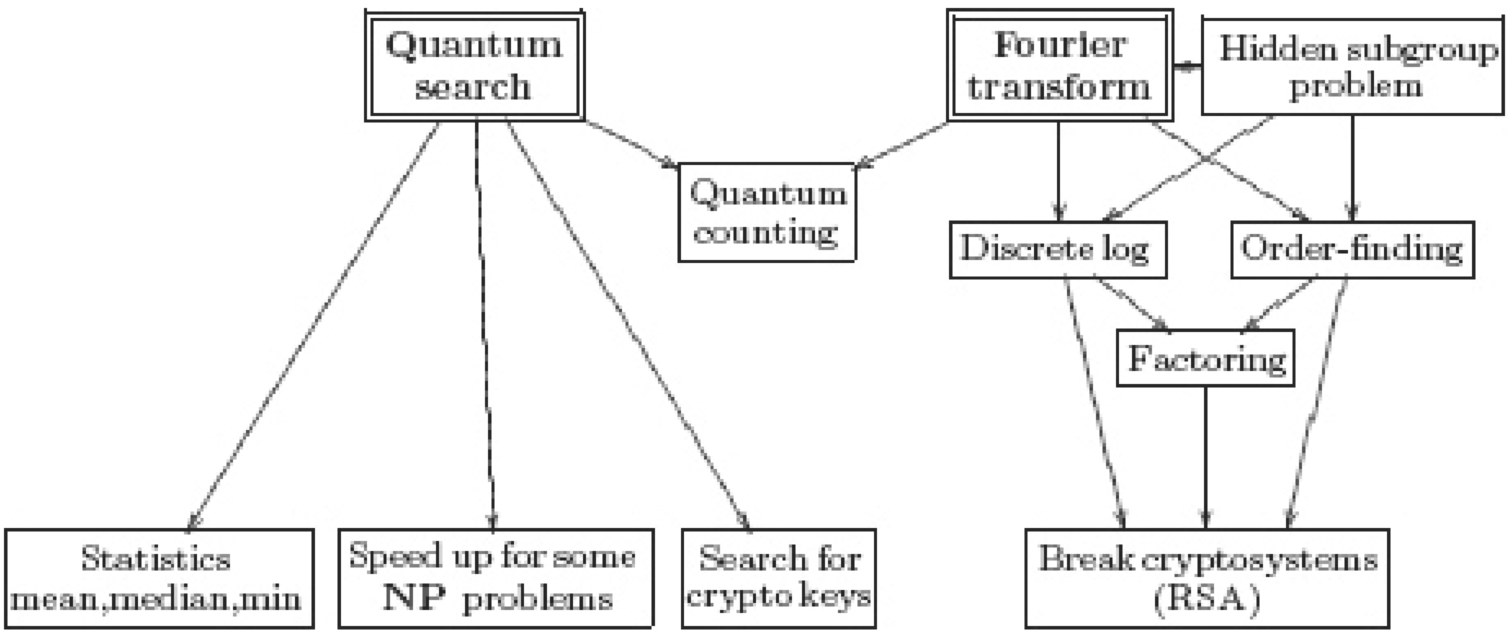


Figure 4.1. The main quantum algorithms and their relationships, including some notable applications.

Intro Problem to Deutsch's Algorithm

- Given a black box f, which transforms one bit input (0 or 1) to another bit output (0 or 1)
- Check if f is constant (always output 0 or 1)

Classical Approach

- We calculate f(0) and f(1), compare the values, and get the result
  - If f(0) = f(1) = 0 or f(0) = f(1) = 1, then f is constant

- Two calculations
  - Calculate f(0)
  - And f(1)

Classical Approach

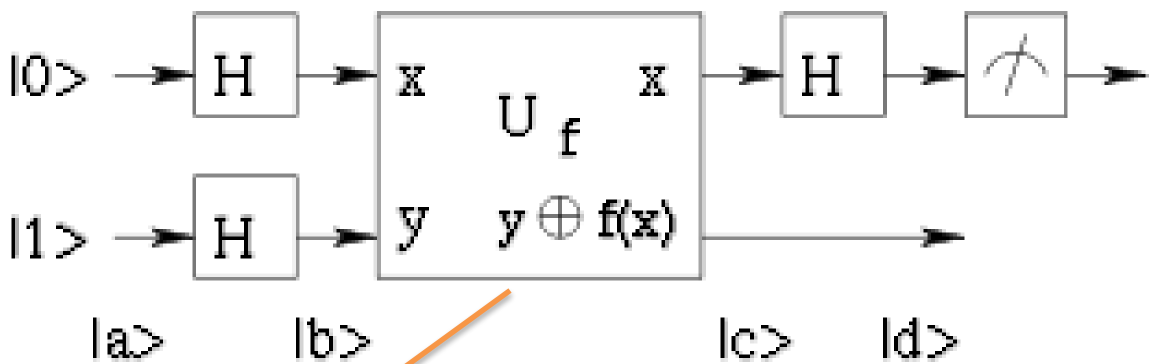
- We calculate f(0) and f(1), compare the values, and get the result
  - If f(0) = f(1) = 0 or f(0) = f(1) = 1, then f is constant

- Two calculations
  - Calculate f(0)
  - And f(1)
- However
  - Redundant information: specific values of f(0) and f(1)

Deutsch's Algorithm

- What Deutsch's Algorithm does:

Hadamard transform $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ **Measuring unit**



Controlled-NOT gate

f(0) = f(1) is equivalent to f(0) xor f(1) = 0

From Wikimedia

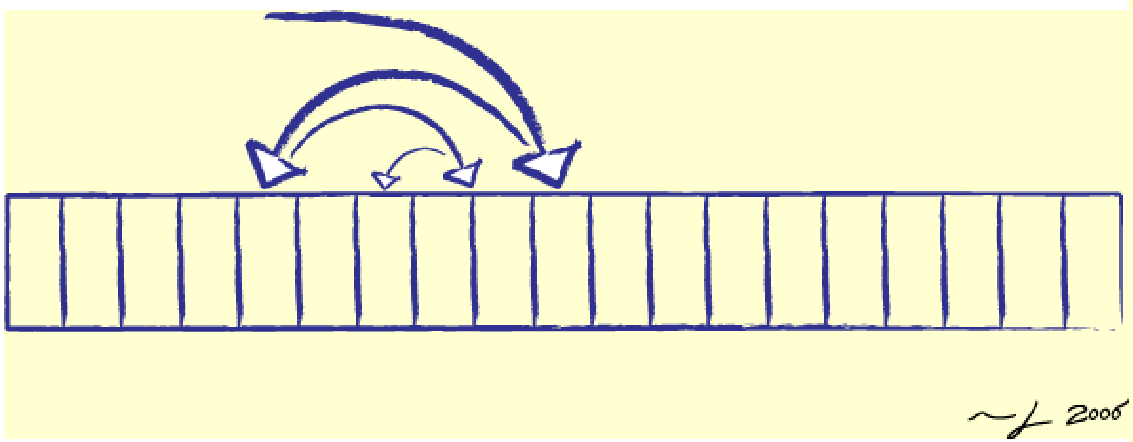
Grover's Searching Algorithm

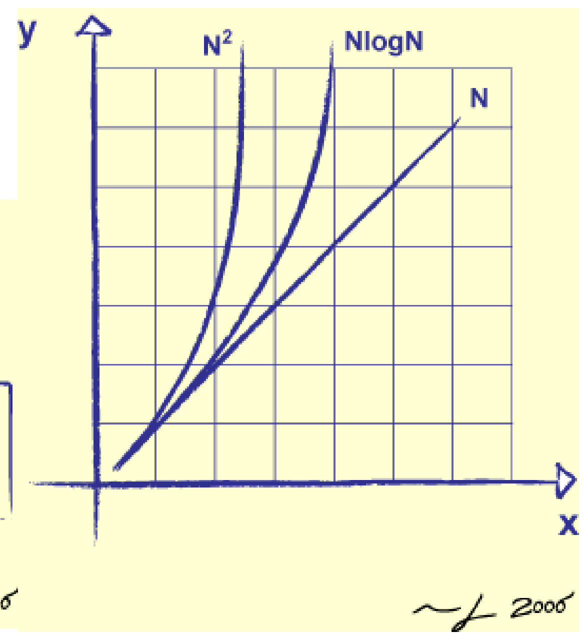
- Introduced in 1996
- Idea:
    - Search an unsorted database with N entries in $O\left(\sqrt{N}\right)$

- Quadratically faster
- Non-deterministic

Grover's Searching Algorithm

- Statistics
  - Mean, median, min, binary search

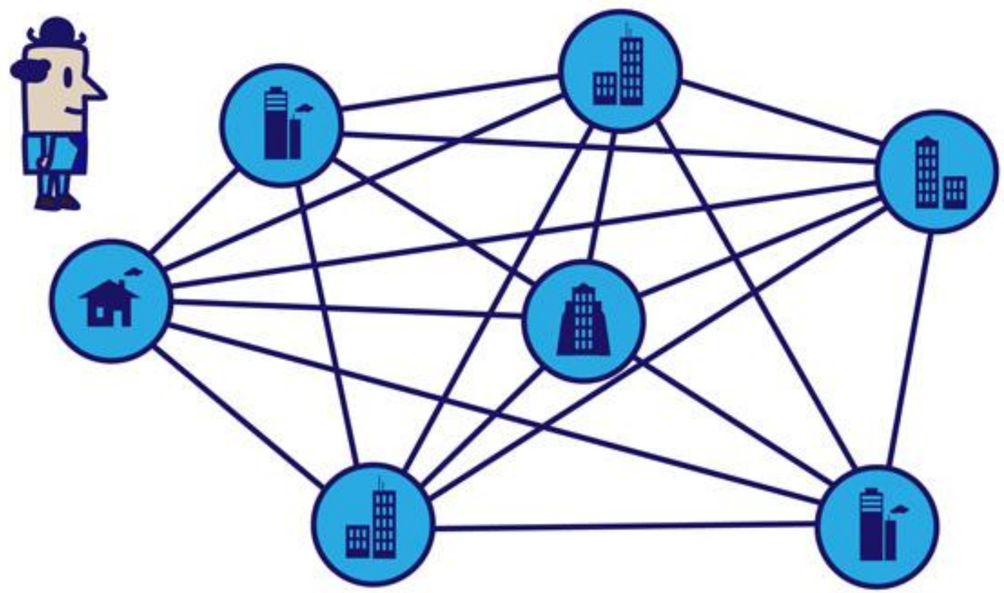




http://www.cgl.ucsf.edu/Outreach/bmi219/slides/swc/lec/py04.html

Grover's Searching Algorithm

- Speed up for some NP problems
  - Optimization (Knapsack problem, Travelling salesman)



Grover's Searching Algorithm

- Search for crypto keys
  - Classical encryption (e.g. EDA) is based on the length of key

https://mocana.com/blog/2012/10/24/popular-websites-have-weak-dkim-key-lengths/

Quantum Fourier Transform

- Exponentially faster $O((\log N)^3)$

⇒

- Shor's Algorithm

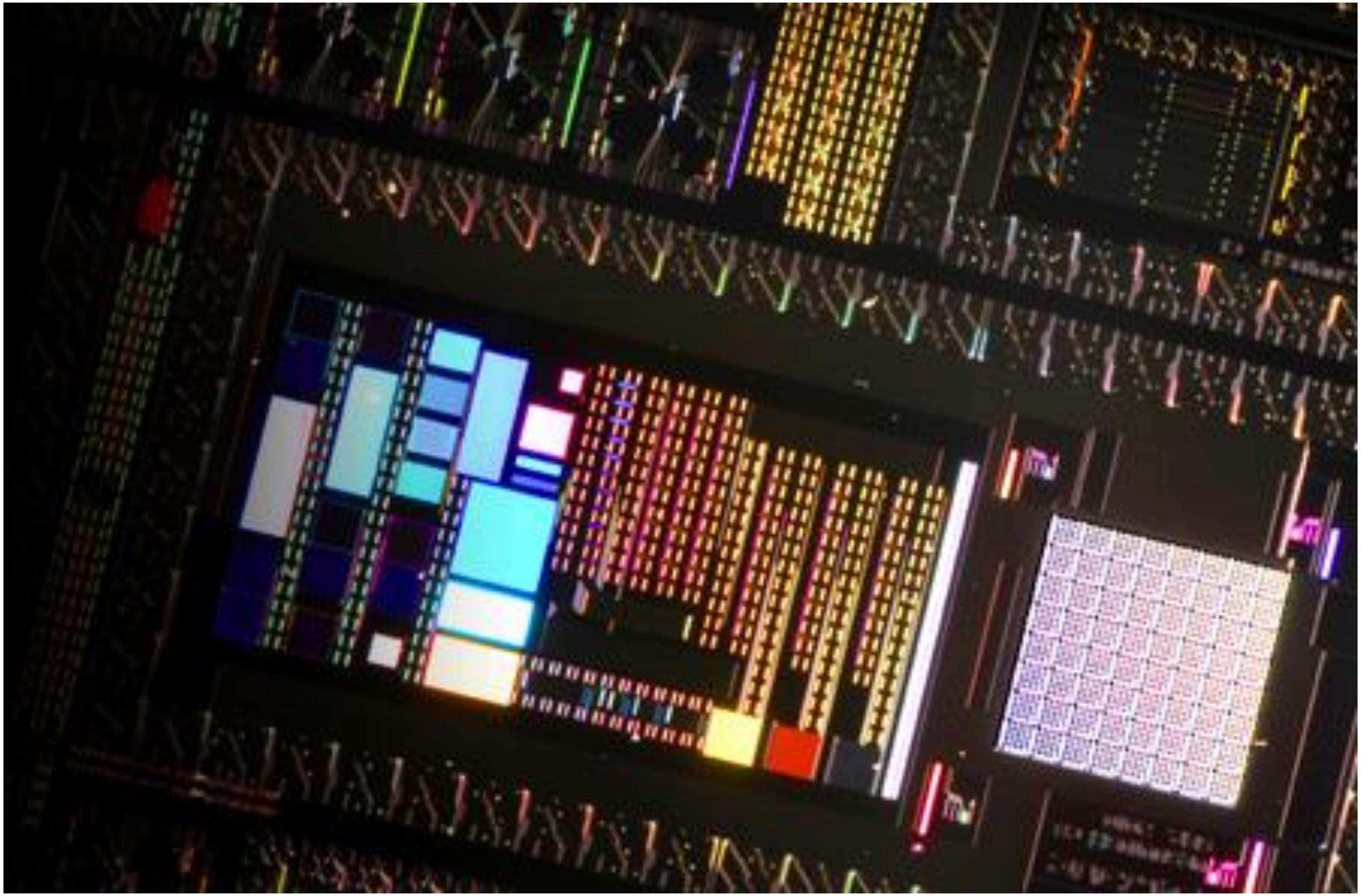
⇒

- Factorization

⇒

- Break cryptosystems (RSA)

⇒ ?

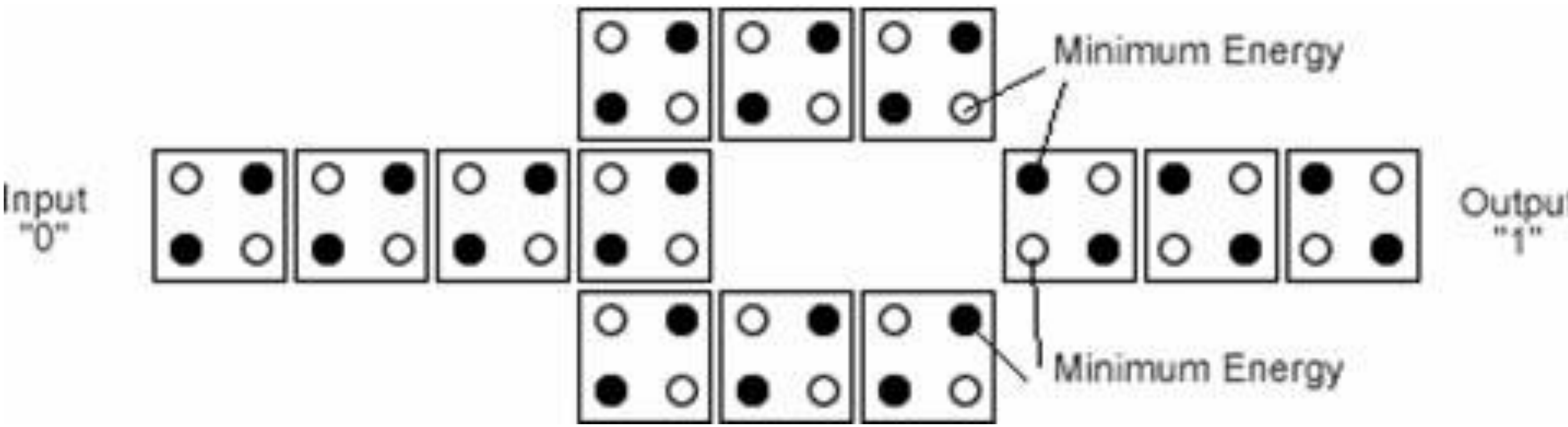


From: D-Wave

PHYSICAL REALIZATION

Quantum Dot Cellular Automata

- Finite-state machine
- **Not** a quantum circuit

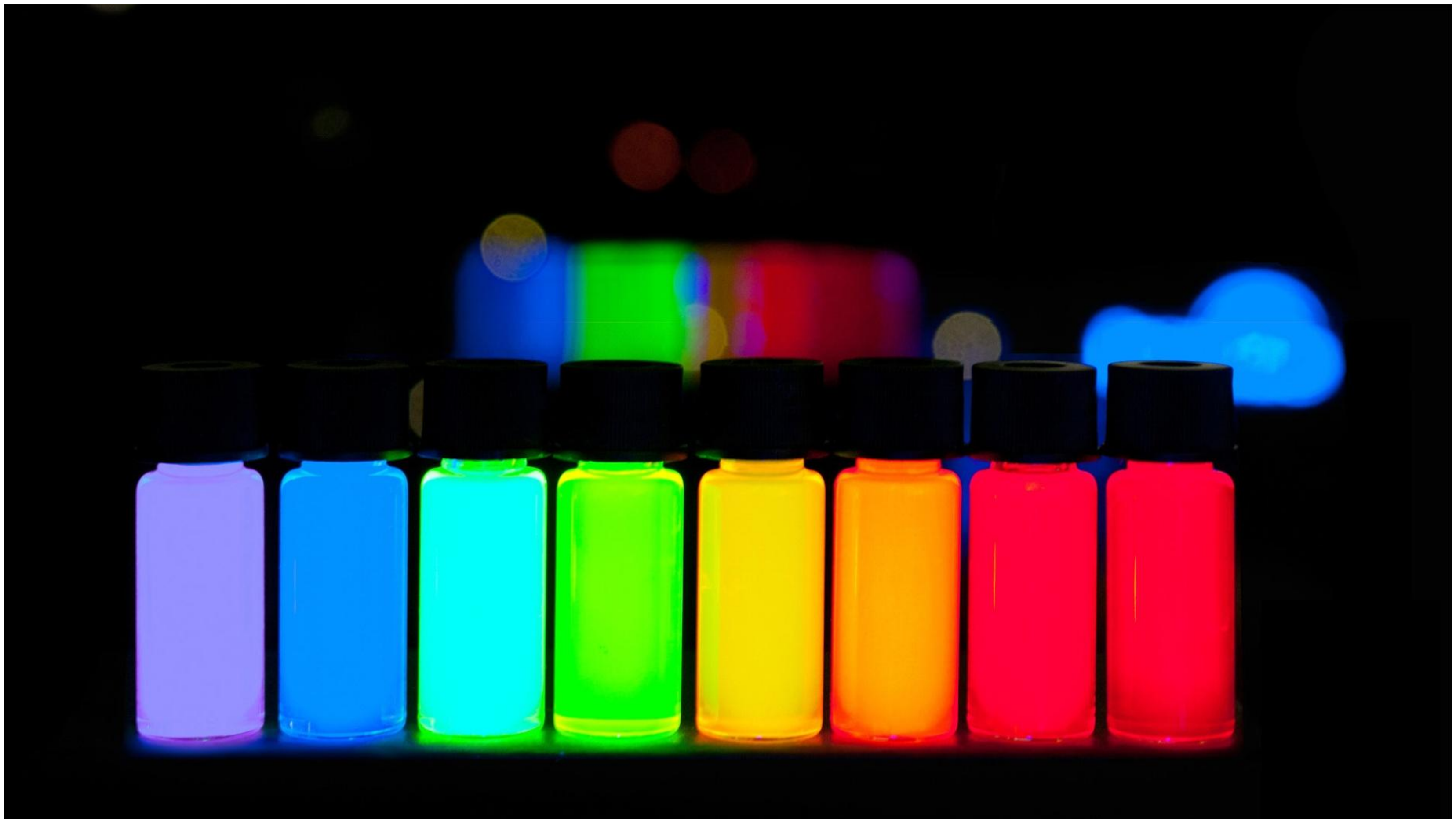


A QCA NOT Gate. From Mariodivece at English Wikipedia

Real Quantum Computer Implementations

- Quantum Dots
- NMR
- SQUID

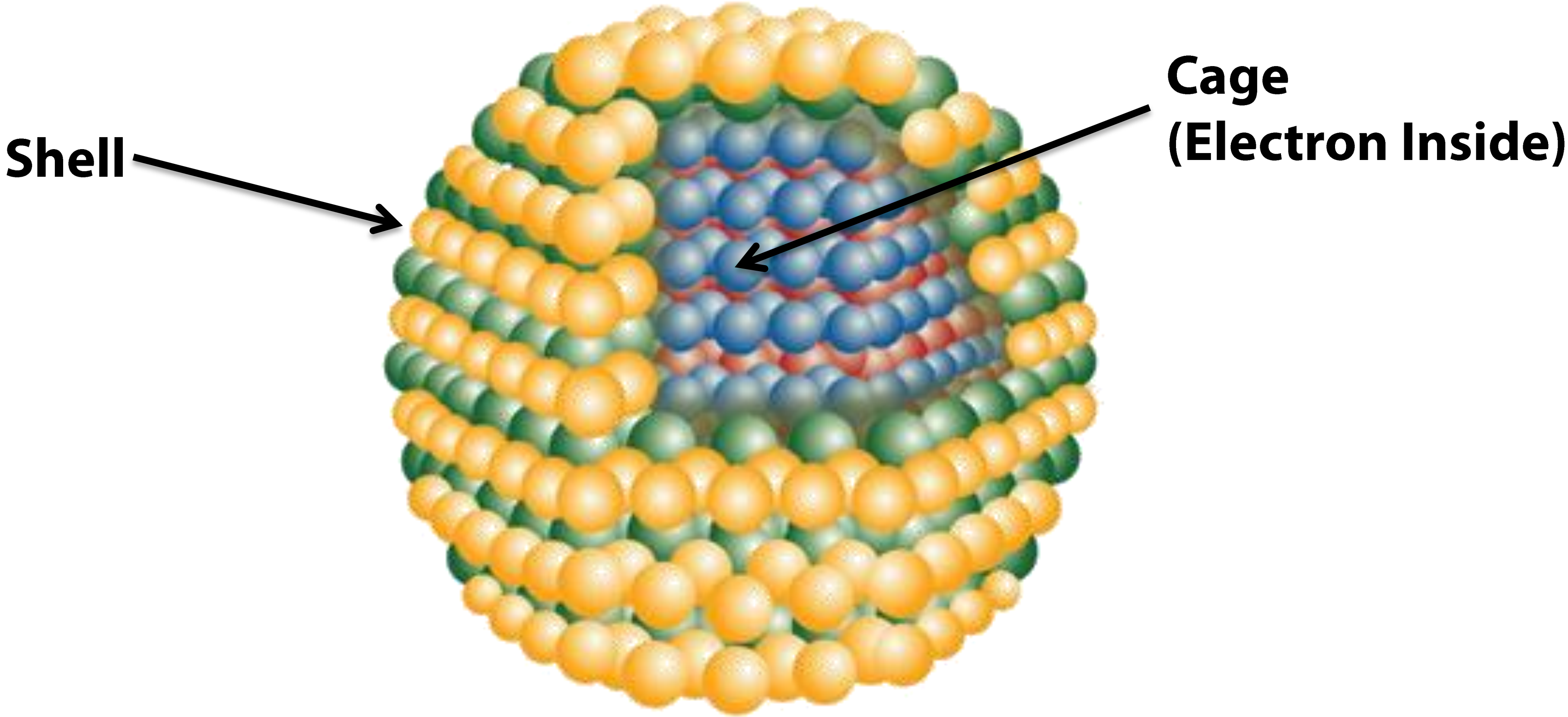
Quantum Dots



From: Antipoff (Wikipedia)

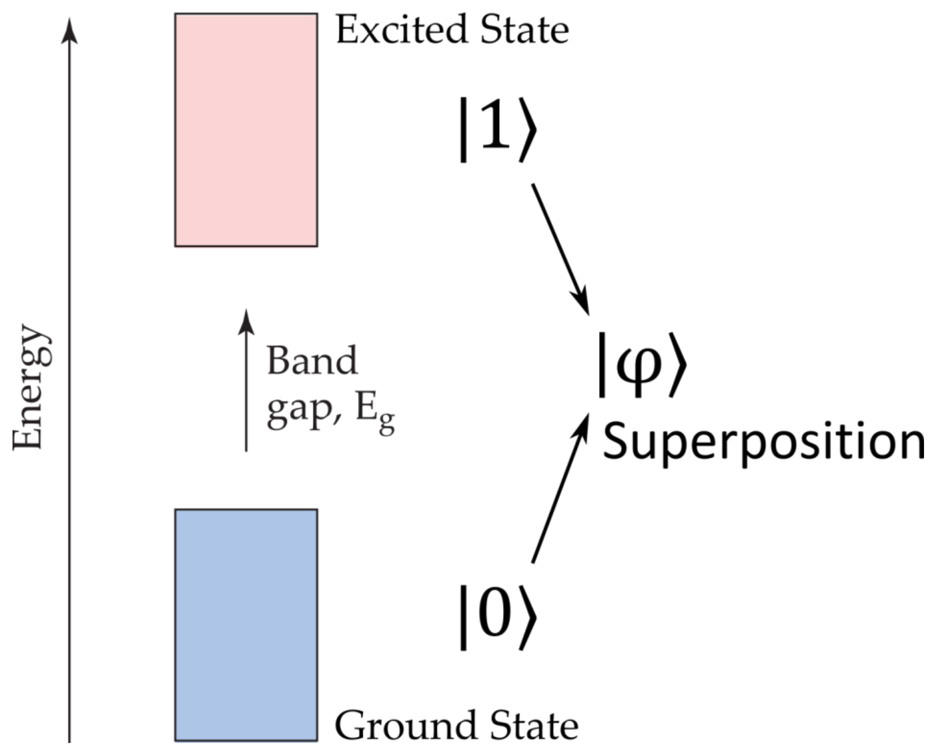
Quantum Dots

- An electron trapped within a cage of atoms



From: Evident Technologies Inc. , via "Are Quantum Dots on the Brink of Their Big Break?" Michael A. Greenwood

Quantum Dot



- Laser beam pulse (~1n)
  - Ground → Excited
  - Excited → Ground
  - NOT Gate
- Half pulse
  - Superposition of ground and excited states
- Tunable band gap

Quantum Dot

- Arbitrary quantum gate
- Rapid loss of coherence ~ 1μs
  - Quantum error correction
- Very short laser pulses (~1ns) required
- Frequency tunable laser pulses required
  - Technological advances

NMR

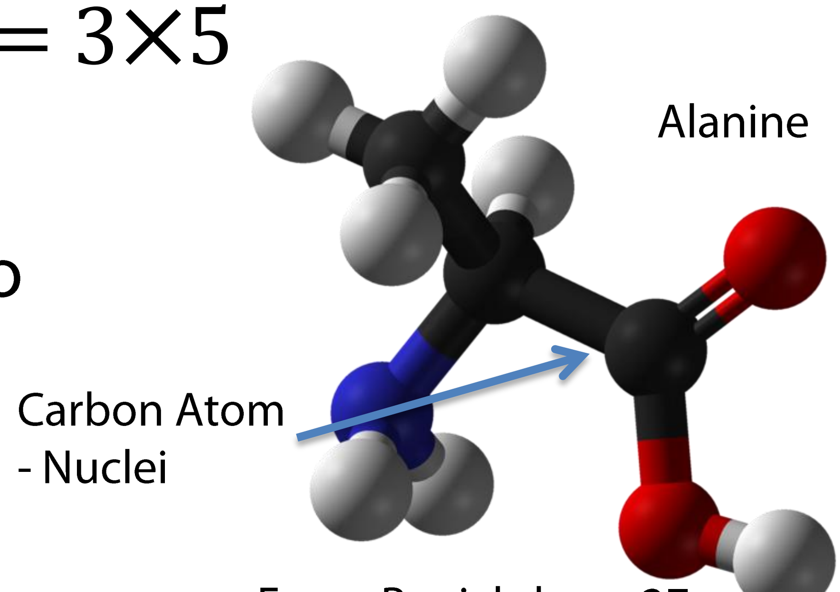
- Nuclear Magnetic Resonance

From: Jan Ainali

The superconducting magnet of an FTNMR spectrometer

NMR Computing Liquids

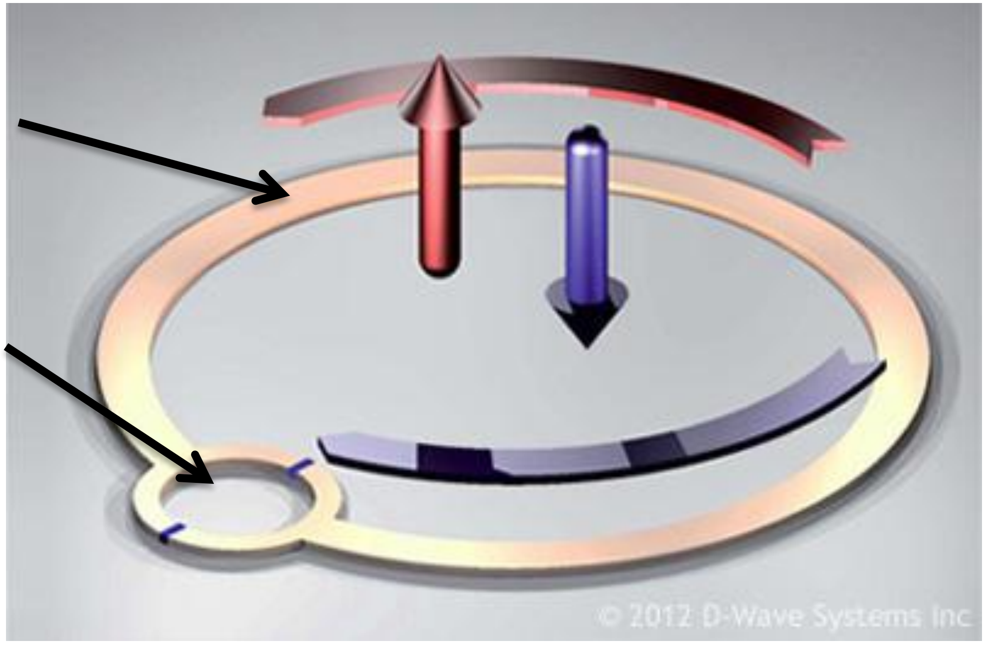
- Detect and manipulate the spin of nuclei in many molecules
  - Longer time before decoherence
- Used by IBM to implement 7-qubit Shor's algorithm. Factored $15 = 3 \times 5$
- Not scalable
  - high signal-to-noise ratio



From: Benjah-bmm27

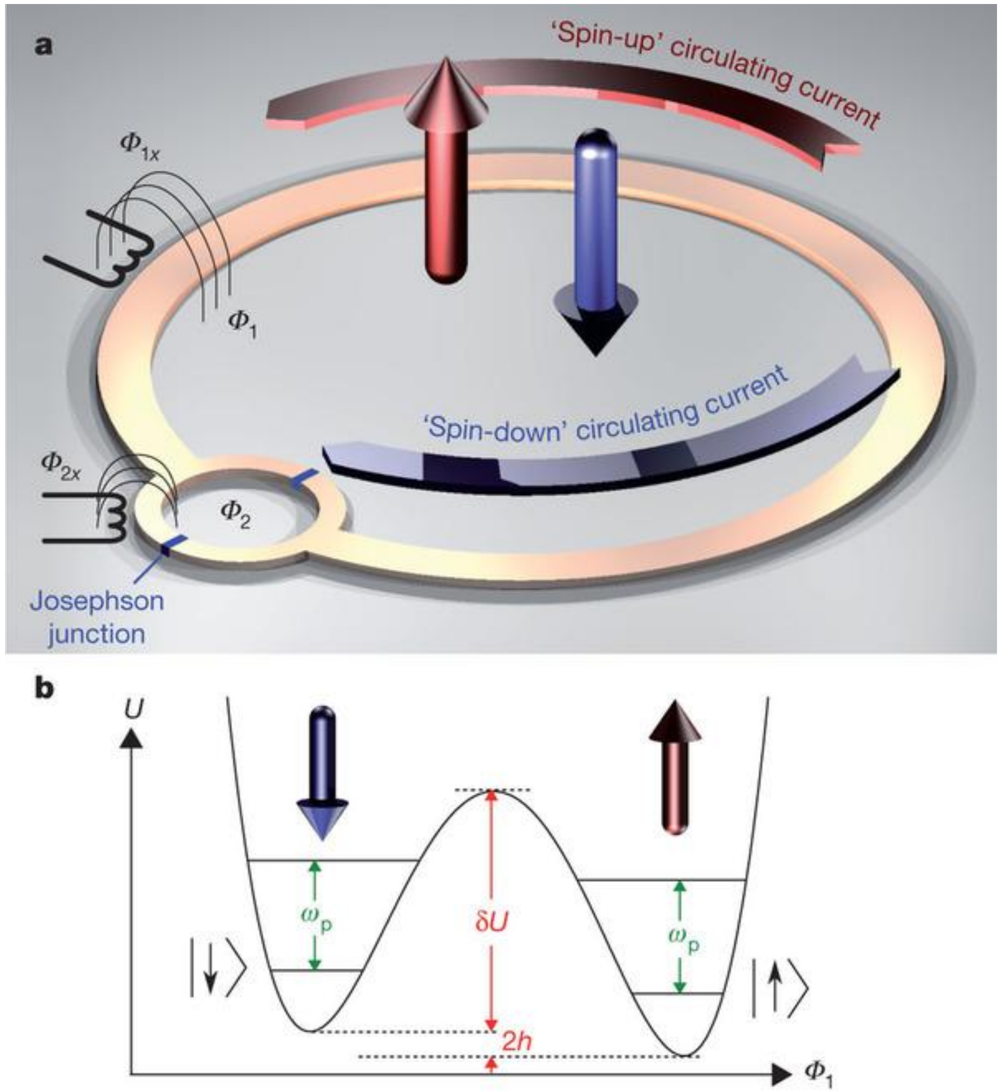
SQUID

- SQUID – Superconducting Quantum Interference Device
- Highly sensitive magnetometer (10^{-12}T)



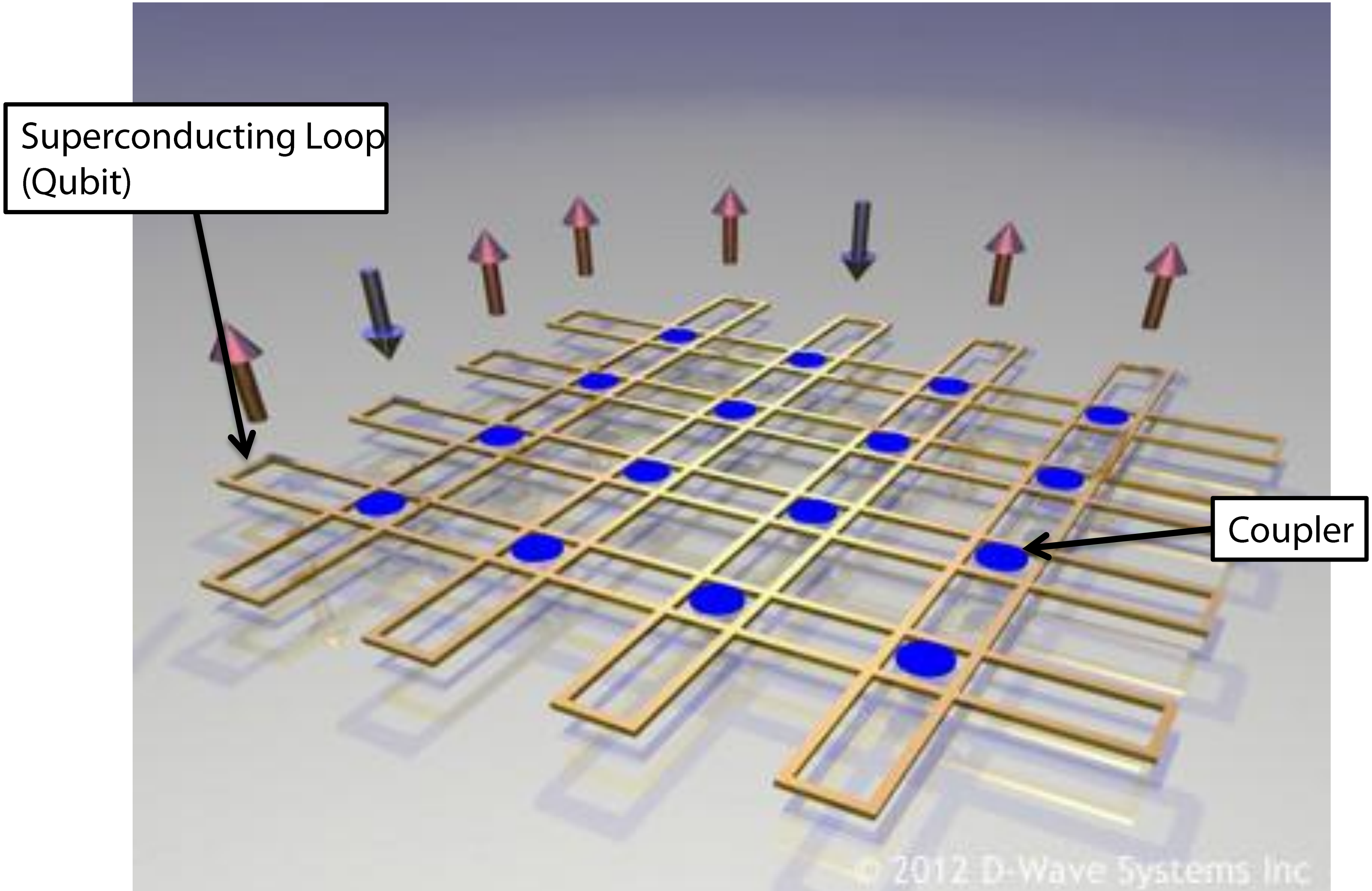
From: D-Wave

Quantum Annealing



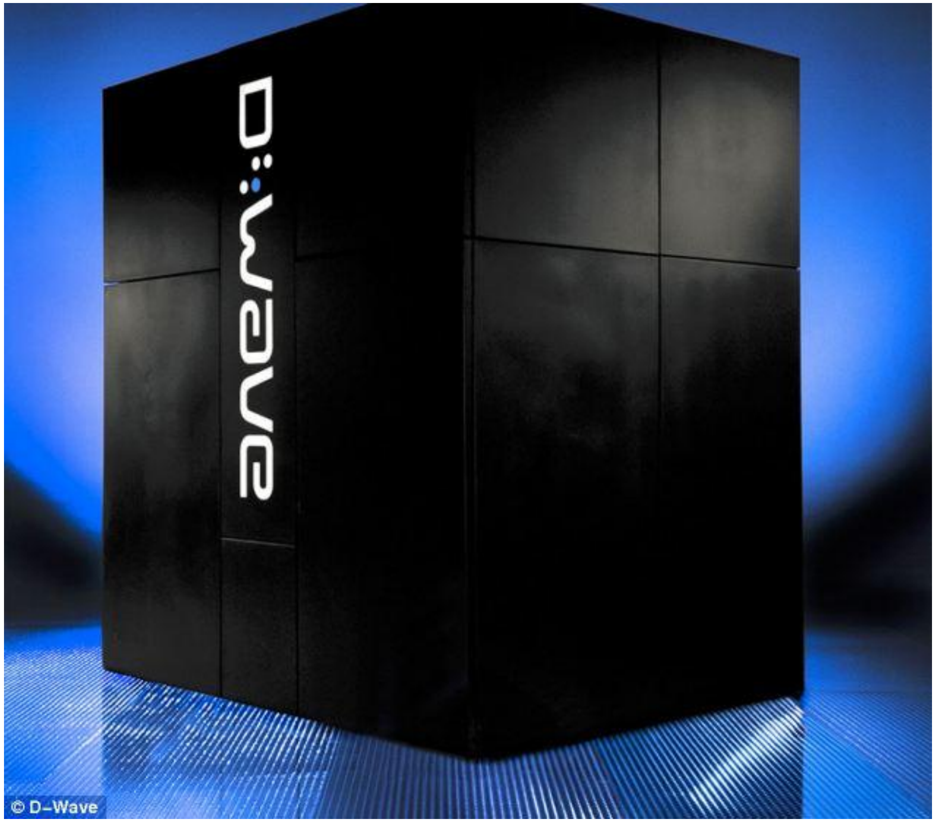
"Quantum annealing with manufactured spins" Johnson et al.

Quantum Annealing



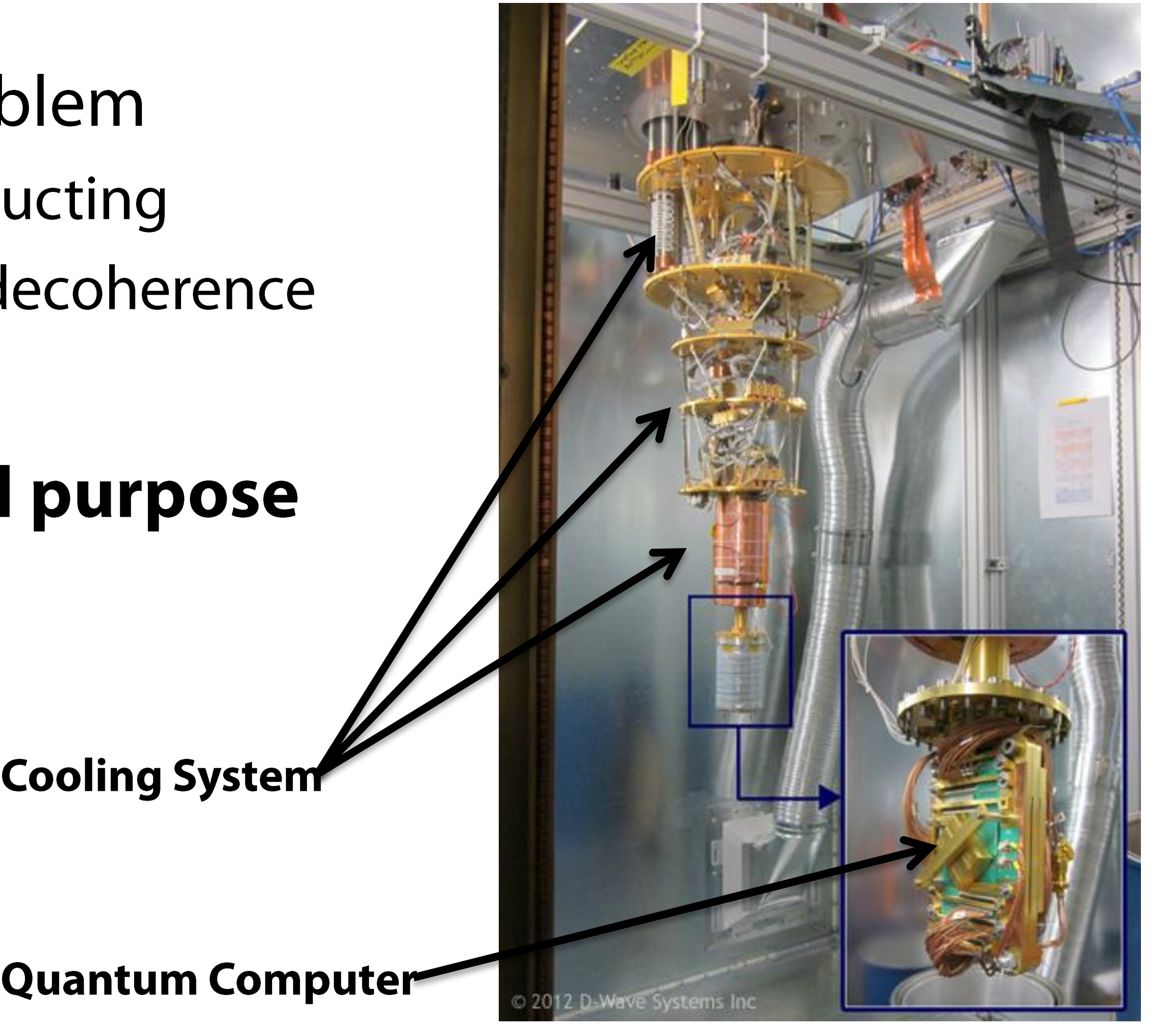
D-Wave One

- SQUID-based quantum annealing computer
- D-Wave One (2011): 128 qubit



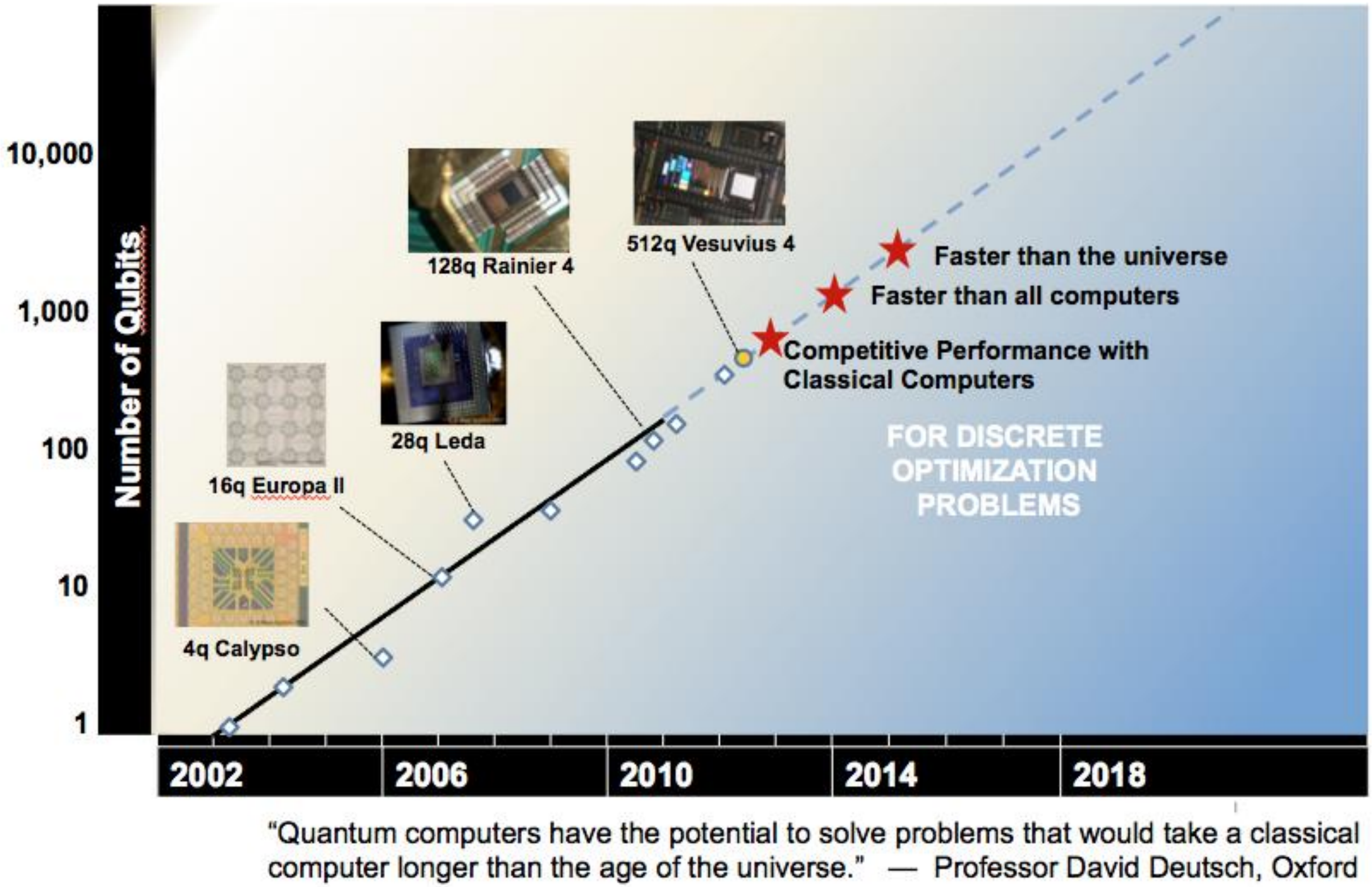
D-Wave One

- Cooling problem
  - Superconducting
  - Reducing decoherence
- Shielding
- **Not general purpose**



Interior of D-Wave One

Rose's Law



From: jurvetson on Flickr

Problems

- Decoherence
- Quantum Interference
- Probabilistic output
- Qubit state initialization

Potential of QC

- Performance
  - Optimization Problem
  - Physical Simulation
  - Artificial Intelligence
- Cryptography
  - RSA & PKI
  - Other symmetric ciphers

References

- Bone, Simon and Matius Castro. *A brief history of quantum computing*. 1997.
- Clayden, J., Greeves, N., & Warren, S. (2012). *Organic Chemistry*. OUP Oxford.
- Deutsch, David. *Quantum Computation*. Physics World. 1992.
- Kloeffel, Christoph and Daniel Loss. *Prospects for Spin-Based Quantum Computing in Quantum Dots*. Annual Review of Condensed Matter Physics. February 4, 2013.
- Nielson, Michael A. *Quantum computation and quantum information*. 2000.
- http://www.bbc.com/future/story/20130124-will-we-ever-get-quantum-theory
- http://www.360doc.com/content/09/1130/09/111971_10044866.shtml
- http://www.photonics.com/Article.aspx?AID=29421
- http://www.dwavesys.com/en/dev-tutorial-hardware.html
- http://www.dwavesys.com/en/dev-tutorial-software.html
- http://robertdick.org/eecs312/lectures/dic-l6.pdf
- http://en.wikipedia.org/wiki/Quantum_cellular_automatahttp://www.scientificamerican.com/article.cfm?id=what-are-josephson-juncti
- http://en.wikipedia.org/wiki/Quantum_annealing

Photo Credits

- Brown, T. L., LeMay, H. E., & Bursten, B. E. (2009). *Chemistry: The Central Science*. Pearson Education International.
- http://ichef.bbci.co.uk/wwfuture/624_351/images/live/p0/14/67/p01467wg.jpg
- http://www.flickr.com/photos/jurvetson/8054771535/sizes/o/in/photostream/
- http://en.wikipedia.org/wiki/File:L-alanine-3D-balls.png
- http://commons.wikimedia.org/wiki/File:Deutsch_algorithm_circuit.svg
- http://en.wikipedia.org/wiki/File:CA06.jpg
- http://en.wikipedia.org/wiki/File:Quantum_Dots_with_emission_maxima_in_a_10-nm_step_are_being_produced_at_PlasmaChem_in_a_kg_scale.jpg
- http://www.hitachi.com/rd/portal/image/fig2.jpg
- http://cnx.org/content/m21493/latest/pic010.png