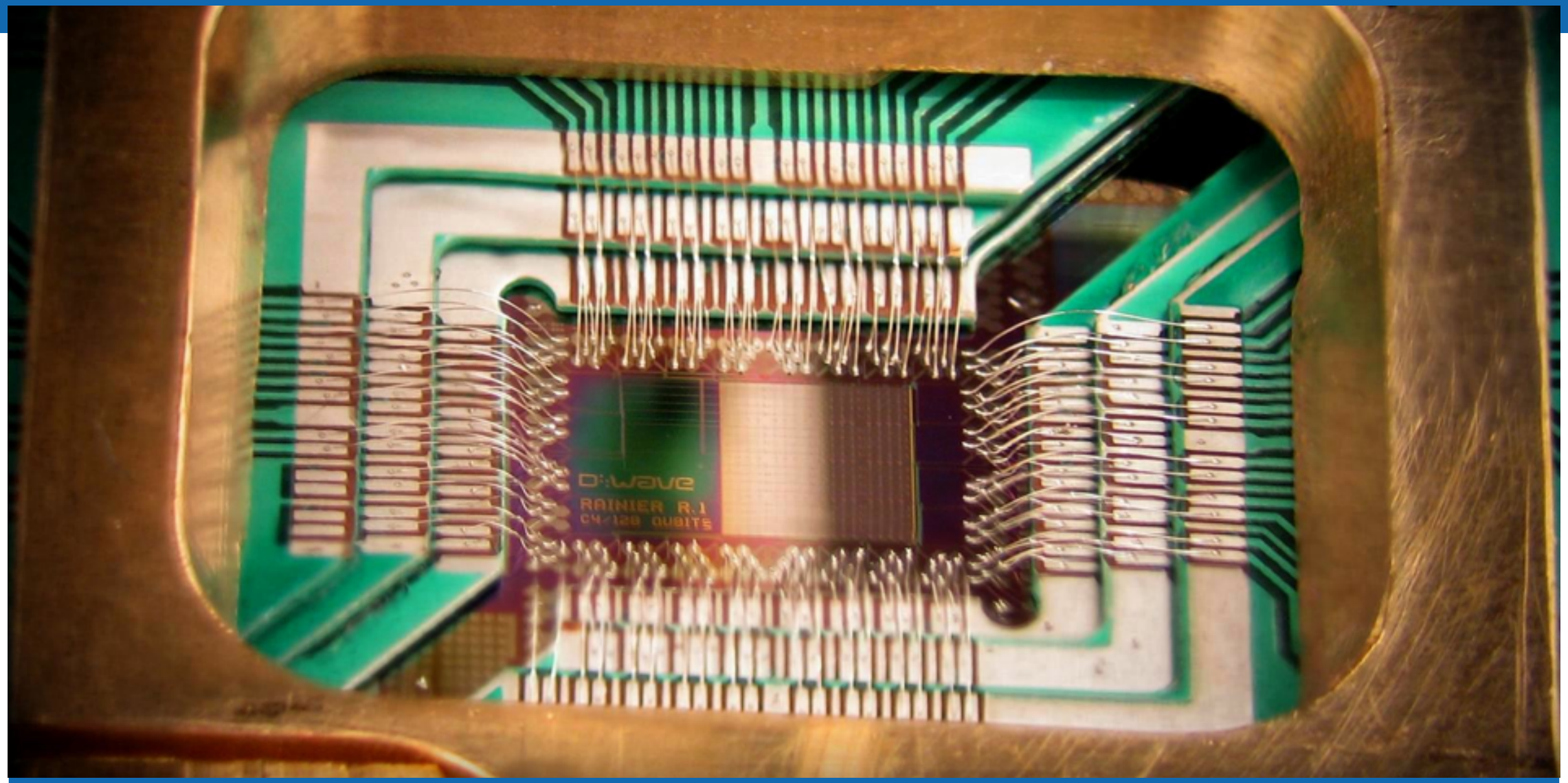
ETH zürich




# High Performance *Quantum* Computing

Matthias Troyer

D PHYS

erc

QSIT Quantum Science and Technology
National Centre of Competence in Research

Microsoft Research

DARPA

# Beyond exascale: quantum devices


Quantum random numbers

perfect randomness

Quantum encryption

secure communication


Quantum computers?

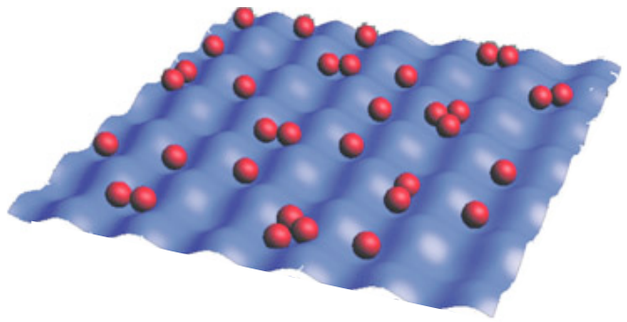
solve quantum models (R. Feynman)

factor integers (P. Shor)

break RSA encryption

solve linear equations (A. Harrow *et al)*

**...**



Analog quantum simulators

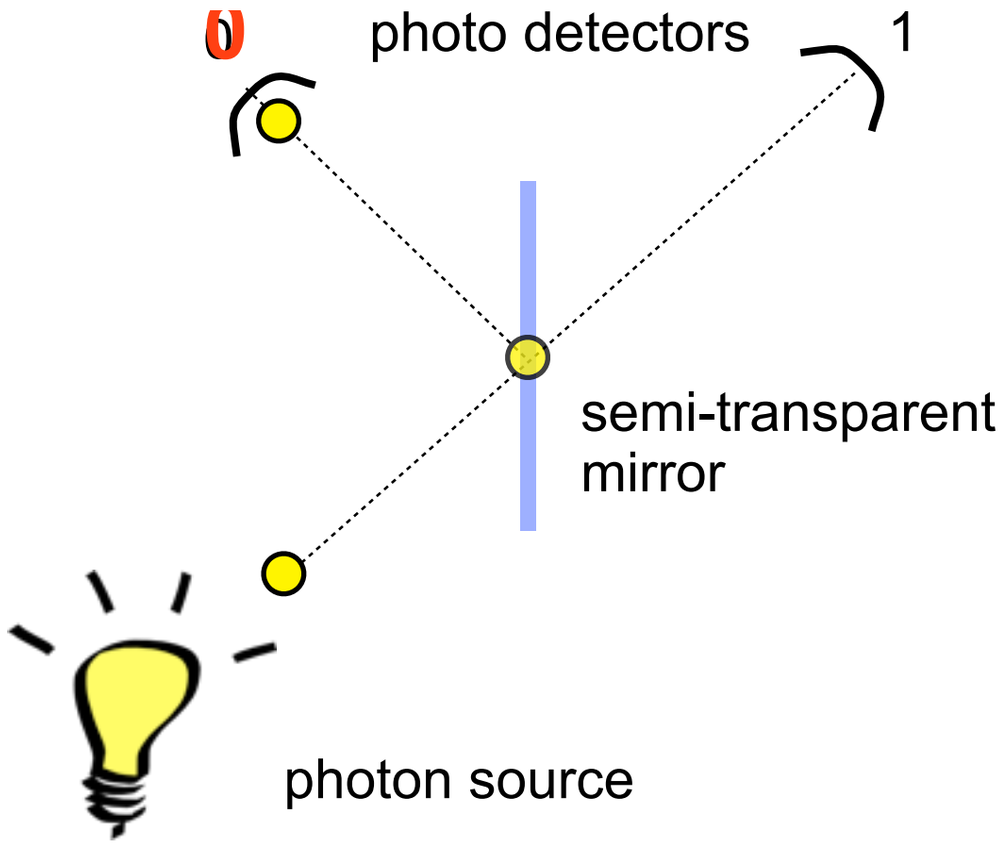
solve quantum models


Quantum annealer

solve hard optimization problems?

# Quantum random numbers

Quantum mechanics can give true and perfect random numbers


1. Photon source emits a photon
2. Photon hits semi-transparent mirror
3. Photon follows both paths
4. The photo detectors see the photon only in one place: **random selection**
5. Record one random bit

# Quantum cryptography

Exchange a secret key to encrypt a message using entangled photons

No eavesdropper can listen without being detected

except for the quantum hacker Vadim Makarov (Waterloo)

Quantum hacking lab

FEBRUARY 17, 2014

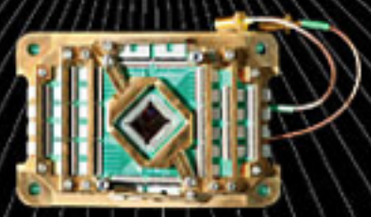
French Advances / My Doctor Fired Me / Love App-tually

# TIME

IT PROMISES TO SOLVE SOME OF HUMANITY'S MOST COMPLEX PROBLEMS. IT'S BACKED BY JEFF BEZOS, NASA AND THE CIA. EACH ONE COSTS $10,000,000 AND OPERATES AT 459° BELOW ZERO. AND NOBODY KNOWS HOW IT ACTUALLY WORKS

## THE INFINITY MACHINE

BY LEV GROSSMAN

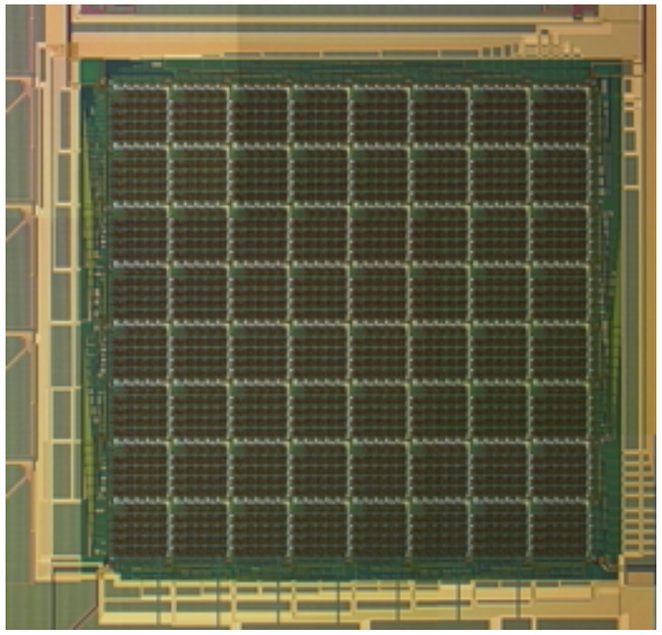


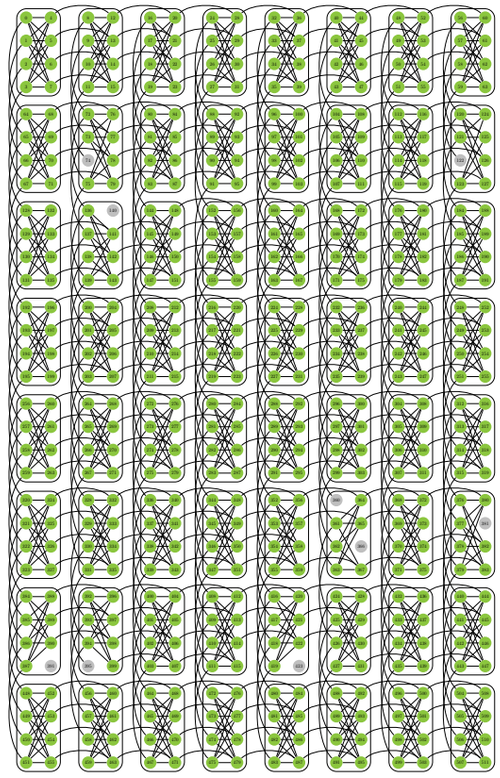
time.com

# D-Wave Two quantum annealer

Solves NP-complete spin glass problem with up to 512 variables

$$H = \sum_{ij} J_{ij} s_i s_j + \sum_i h_i s_i + const. \qquad \text{with} \qquad s_i = \pm 1$$



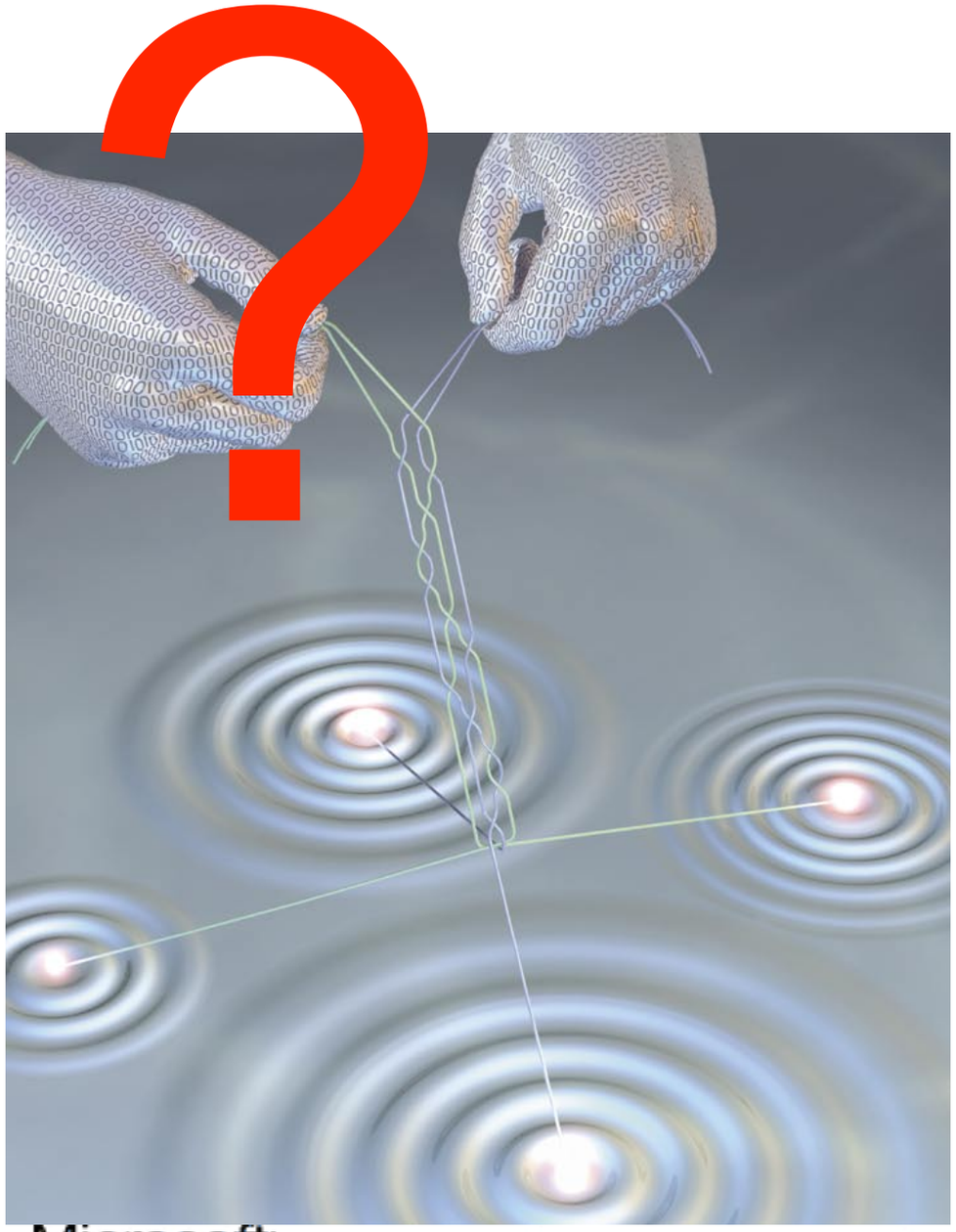


Can be built with imperfect qubits

Suffers form calibration problems like other analog devices

Unknown if this technology can ever scale better than classical devices

# What about quantum computers ?

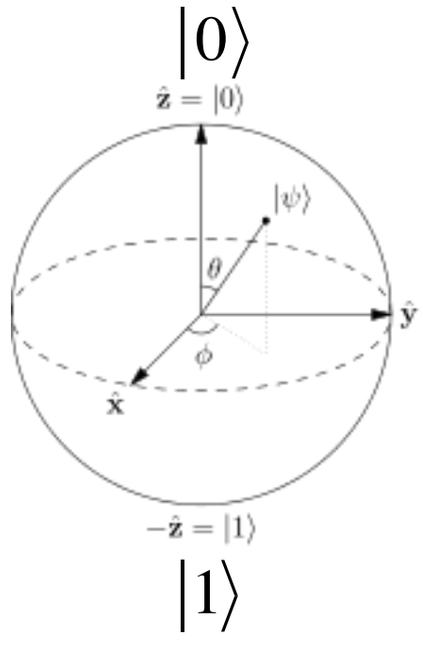


Microsoft Windows Q

# Classical versus quantum bits

- Classical bits can only be either 0 or 1
- Quantum bits can have both values at once, in arbitrary superpositions

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |\alpha|^2 + |\beta|^2 = 1$$




- need two complex or three real numbers to describe the state

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \qquad \alpha = \cos\left(\frac{\theta}{2}\right) \qquad \beta = e^{i\phi}\sin\left(\frac{\theta}{2}\right)$$

- but when measuring (looking) I only ever get 1 bit

$$0 \quad \text{with probability } |\alpha|^2$$
$$1 \quad \text{with probability } |\beta|^2$$

# Information content of a quantum register

- The state of an *N* qubit register
  - needs $2^N$ complex numbers to be represented classically
  - but when measured only gives *N* bit of information
- Advantages and limitations of quantum computers
  - Exponential intrinsic parallelism: operate on $2^N$ inputs at once
  - But very limited readout of only *N* bits
- No-cloning theorem: a quantum register cannot be copied

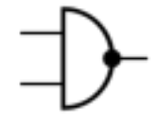
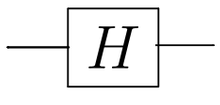
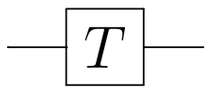
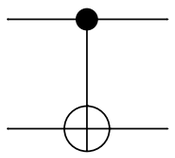
Try to build a cloner for 0 and 1

$$C|0\rangle \rightarrow |0\rangle|0\rangle$$
$$C|1\rangle \rightarrow |1\rangle|1\rangle$$

Linearity of quantum mechanics means it will not clone an arbitrary state

$$C\left(\alpha|0\rangle+\beta|1\rangle\right) \rightarrow \alpha|0\rangle|0\rangle+\beta|1\rangle|1\rangle$$
$$\neq \left(\alpha|0\rangle+\beta|1\rangle\right)\left(\alpha|0\rangle+\beta|1\rangle\right)$$

# Quantum gates

- In classical computing the NAND gate is universal 
- In quantum computing we need three gates
  - Hadamard gate (flips *x* and *z*)  $|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ $|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
  - T gate (applies phase to 1 state)  $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|0\rangle + e^{i\pi/4}\beta|1\rangle$
  - CNOT gate (conditionally flips)  $|x\rangle|y\rangle \rightarrow |x\rangle|x \oplus y\rangle$
- This choice is not unique and having more gates can make a device more efficient

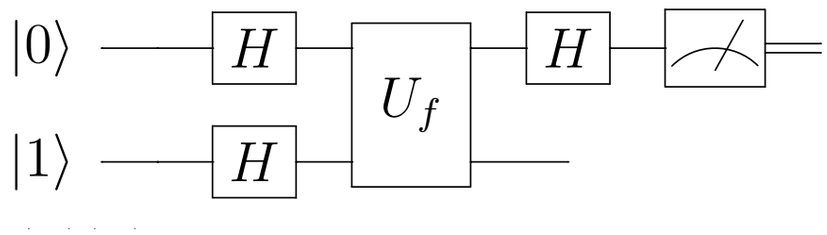
# The Deutsch algorithm: simplest quantum speedup

- Check whether a binary function is constant or not

$$f:\{0,1\}\to\{0,1\}$$

- Classically two function calls are needed: f(0) = f(1)?

- Quantum mechanically only one function call by applying the function to both arguments at once




$$U_f|x\rangle|y\rangle\to|x\rangle|f(x)\oplus y\rangle$$

$$U_f\left(\alpha|0\rangle+\beta|1\rangle\right)|0\rangle\to\alpha|0\rangle|f(0)\rangle+\beta|1\rangle|f(1)\rangle$$

- Smart manipulation needed to read out the answer as one bit

$$\frac{1}{2}\left[\left(1+(-1)^{f(0)\oplus f(1)}\right)|0\rangle+\left(1-(-1)^{f(0)\oplus f(1)}\right)|1\rangle\right]$$

# What would we use it for?

Surprisingly, this question has not been seriously asked until 2012

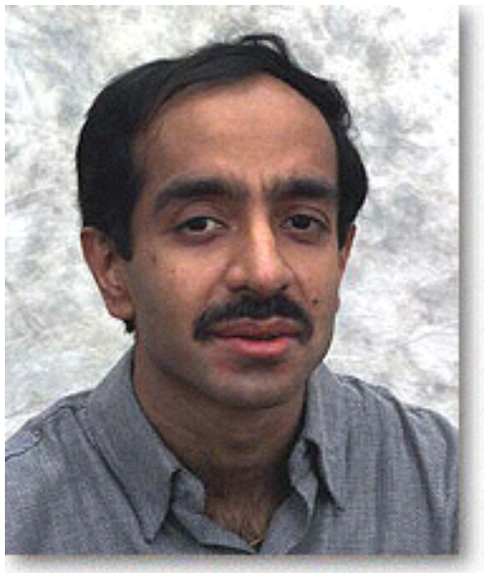
It needs to be an important problem (killer-app) that we cannot solve on an exascale machine

Compare to state-of-the-art on beyond-exascale hardware and not an unoptimized code on a single CPU core

# Grover search

- Search an unsorted database of $N$ entries in $\sqrt{N}$ time
- Rare case of provable quantum speedup given an oracle

- However, the oracle needs to be implemented!
  - $N$-entry database or arbitrary stored data needs at least $O(N)$ hardware
  - Can perform the same search classically in $\log(N)$ time with special purpose hardware



- Grover search is only useful if the database need not be stored but can be calculated on the fly!

# Shor's algorithm for factoring

- Factoring is a hard problem classically: $O(\exp(N^{1/3}))$ for $N$ bits

$$
\begin{aligned}
&5369396836426911946079505415332600518604181838930231166202317318847061358416977798124777554355964649\\
&0445261580420917702924053815614103527255419762537786248302905180961505012704341492726102041142364969 4\\
&6309670910771714302797950221151202416796228494478056509873683502478296830543092162766745097351056392 4\\
&0298977591783205062161915884859331945476609848287512883478098897975108372321438198667838135056716 7\\
&=\\
&4363637625931498167701061252972058930130370651588109946621952523434903606572651613287342123766790024 5\\
&9135372537443549282380180405548453067960658656053548608342707327969894210413710440109013191728001673\\
&*\\
&1230486419064350262435007521990111788816176581586683476039159532309509792696707176253005200766846735 0\\
&6058795416957989730803763009700969113102979143329462235916722607486848670728527914505738619291595079


- Shor's algorithm is polynomial time on a quantum computer
  - $O(N^3)$ using minimal number of $2N+3$ qubits
  - $O(N^2)$ using $O(N)$ qubits
  - $O(N)$ using $O(N^2)$ qubits

- Shor's algorithm suddenly made quantum computing interesting

# Shor's algorithm and encryption

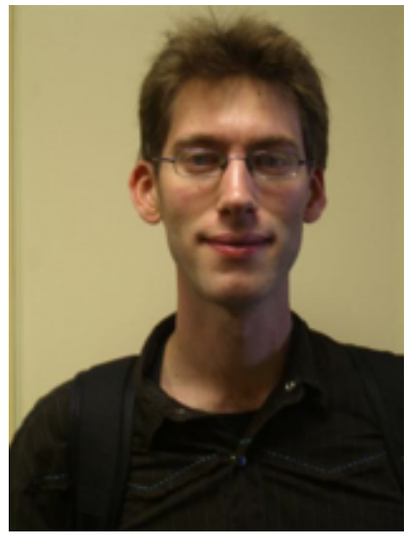
- Shor's algorithm can be used to crack RSA encryption
  - assuming 10 ns gate time and minimal number of 2N+3 qubits
  - much faster (seconds) when using more qubits

| RSA | cracked in | CPU years | Shor |
|---|---|---|---|
| **453 bits** | 1999 | 10 | 1 hour |
| **768 bits** | 2009 | 2000 | 5 hours |
| **1024 bits** | | 1000000 | 10 hours |

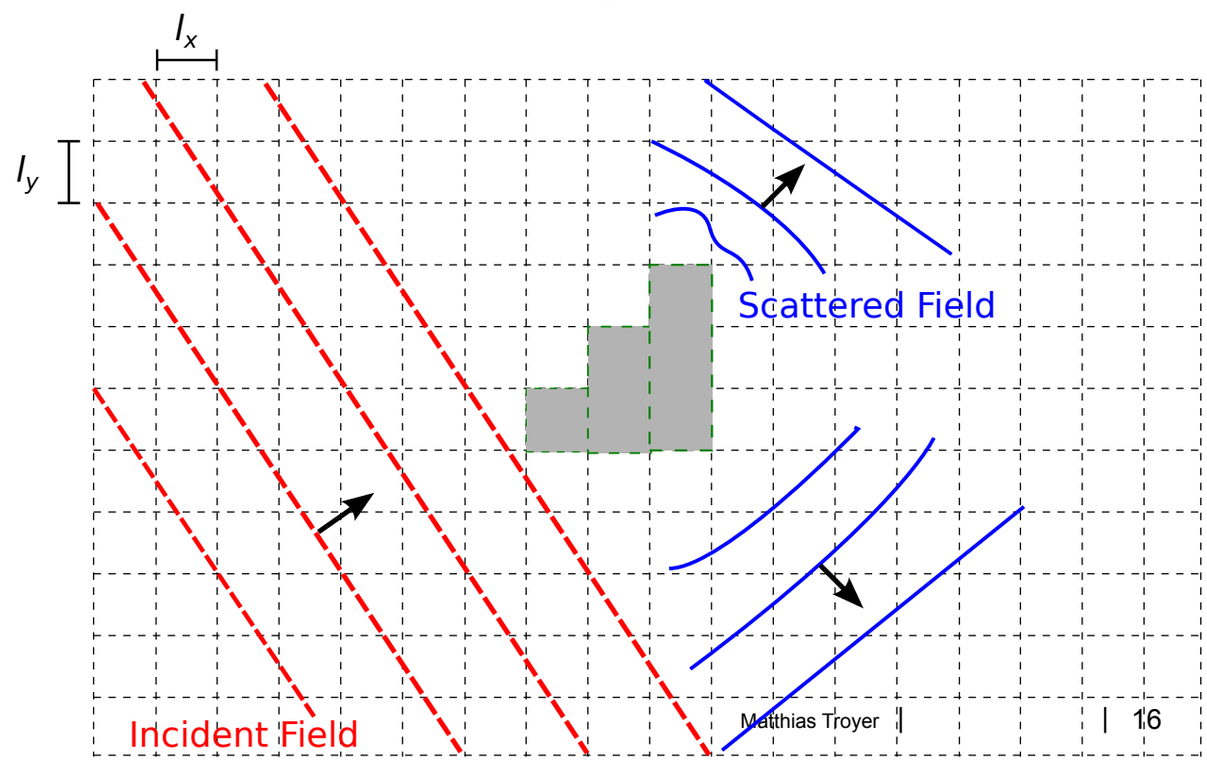
- But use of quantum computers to crack RSA is limited since we can anytime switch to post-quantum encryption
  - quantum cryptography
  - lattice based cryptography

# Solving linear systems of equations (Harrow *et al*)

- Solve linear systems in log(*N*) time if
  - matrix can be computed efficiently and need not be stored
  - only log (*N*) bits of the answer are needed
  - problem is well conditioned



- First application: electromagnetic wave scattering
  - Clader, Jacobs, Sprouse (2013)
  - crossover compared to classical supercomputers is beyond 1000 years wallclock time



# Applications running at scale on Jaguar @ ORNL

| Domain area | Code name | Institution | # of cores | Performance | Notes |
|---|---|---|---|---|---|
| Materials | DCA++ | ORNL | 213,120 | **1.9 PF** | 2008 Gordon Bell Prize Winner |
| Materials | WL-LSMS | ORNL/ETH | 223,232 | **1.8 PF** | 2009 Gordon Bell Prize Winner |
| Chemistry | NWChem | PNNL/ORNL | 224,196 | 1.4 PF | 2008 Gordon Bell Prize Finalist |
| Materials | DRC | ETH/UTK | 186,624 | 1.3 PF | 2010 Gordon Bell Prize Hon. Mention |
| Nanoscience | OMEN | Duke | 222,720 | > 1 PF | 2010 Gordon Bell Prize Finalist |
| Biomedical | MoBo | GaTech | 196,608 | 780 TF | 2010 Gordon Bell Prize Winner |
| Chemistry | MADNESS | UT/ORNL | 140,000 | 550 TF | |
| Materials | LS3DF | LBL | 147,456 | 442 TF | 2008 Gordon Bell Prize Winner |
| Seismology | SPECFEM3D | USA (multiple) | 149,784 | 165 TF | 2008 Gordon Bell Prize Finalist |

Source: T. Schulthess

# Solving quantum chemistry on a quantum computer

- A killer-app for quantum computing is solving quantum problems
  - Design a room-temperature superconductor
  - Develop a catalyst for carbon sequestration

  - Develop better catalysts for nitrogen fixation (fertilizer)

- These problem need better accuracy than we get by using approximate classical algorithms
  - exponentially hard classically
  - polynomial complexity on quantum hardware

# Quantum algorithms for quantum chemistry

Microsoft Research

- Assume the fastest imaginable quantum computer and consider smallest problem we cannot solve classically: $N$=50 orbitals, $O$(100) qubits

| | Scaling | Run time for $N=50$ |
|---|---|---|
| **State of 12/2013** | $N^{10}$ | 100 000 years |
| **1/2014 pipelining and optimisations** | $N^{9}$ | 3 years |
| **6/2014 faster convergence** | $N^{5.5}$ | 1 hour |
| **parallel with with** | $N^{1.6}$ | seconds? |

- Quantum information theorists declare victory proving the existence of polynomial time algorithms
- We need HPQC specialists to develop better algorithms!

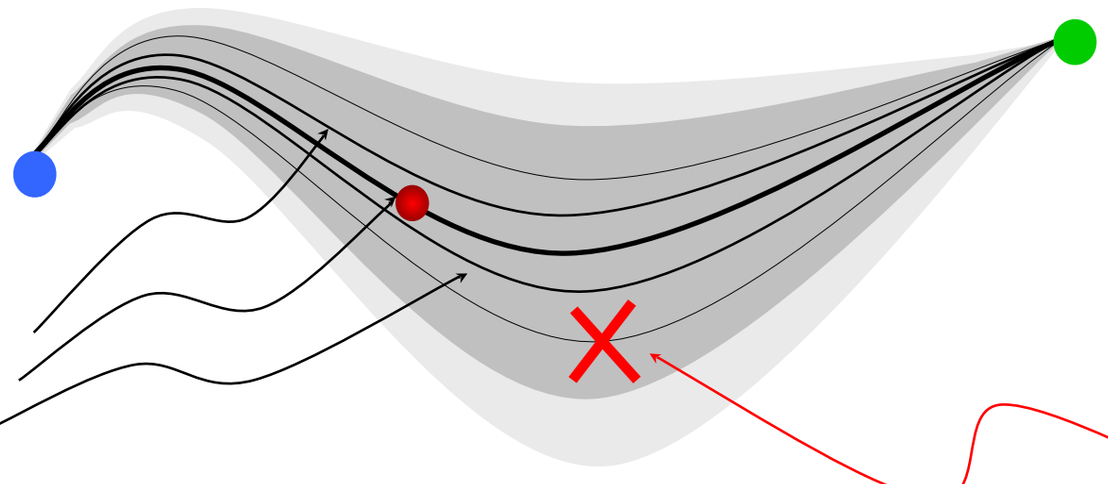
# State of the art of hardware

many proposals but few are scalable …

# Physical realizations and decoherence

- Coupling to the environment easily destroys the quantum superposition
- Qubits need to be designed to be well isolated from the environment

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

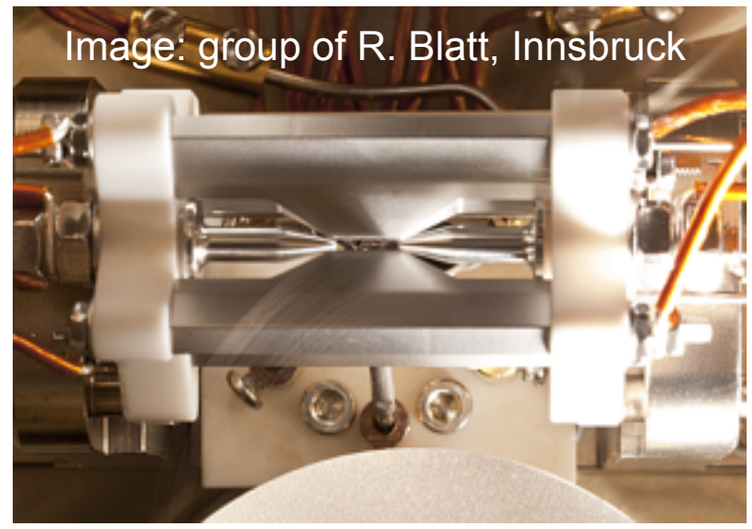



Parallel evolution providing the quantum speedup.

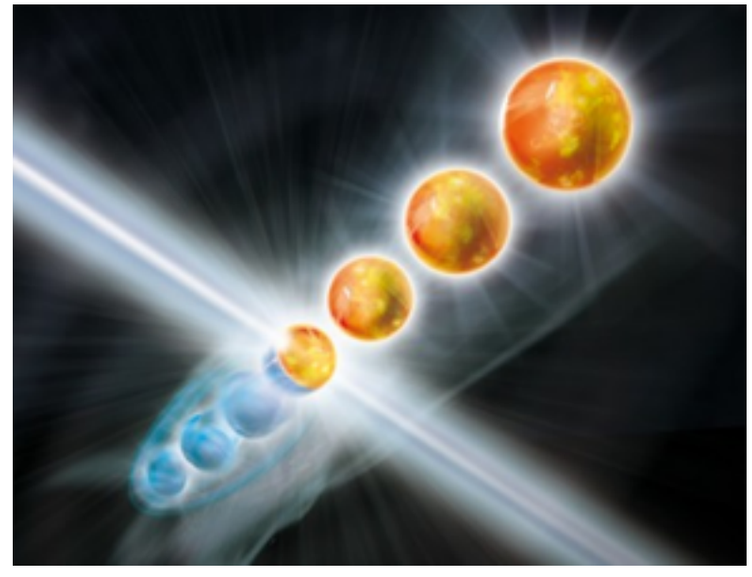
Perturbations from the environment destroy the parallel evolution of the computation

# The best qubits: ion traps (universities)

- Use the motional states of well isolated ions to encode a qubit
  - up to 14 qubits
  - coherent for several seconds
  - about 100 gate operations
  - 10 µs gate times

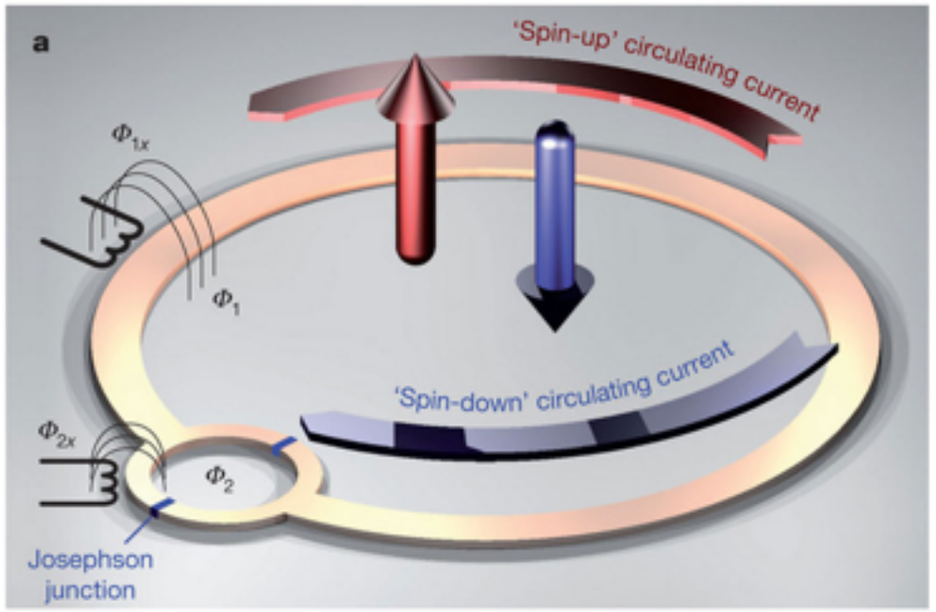



- Advantages and disadvantages
  - Well isolated from environment
  - Relatively slow
  - Hard to scale  beyond O(20) qubits

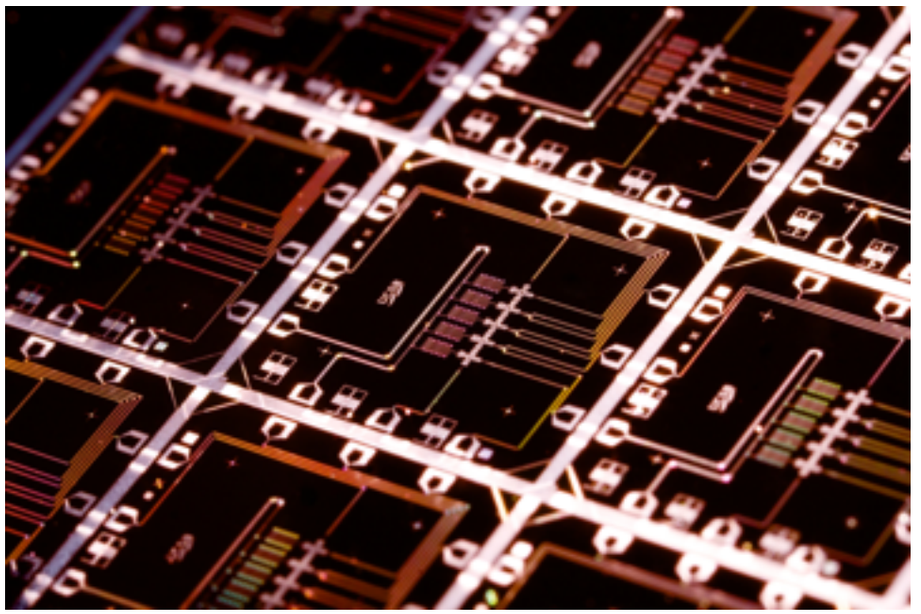


# Superconducting qubits (IBM and universities)

- Use superconducting current loops to encode a qubit
- State of the art
  - 5 qubits
  - 100 µs coherence times
  - 10 ns gate times
  - about 100 gate operations

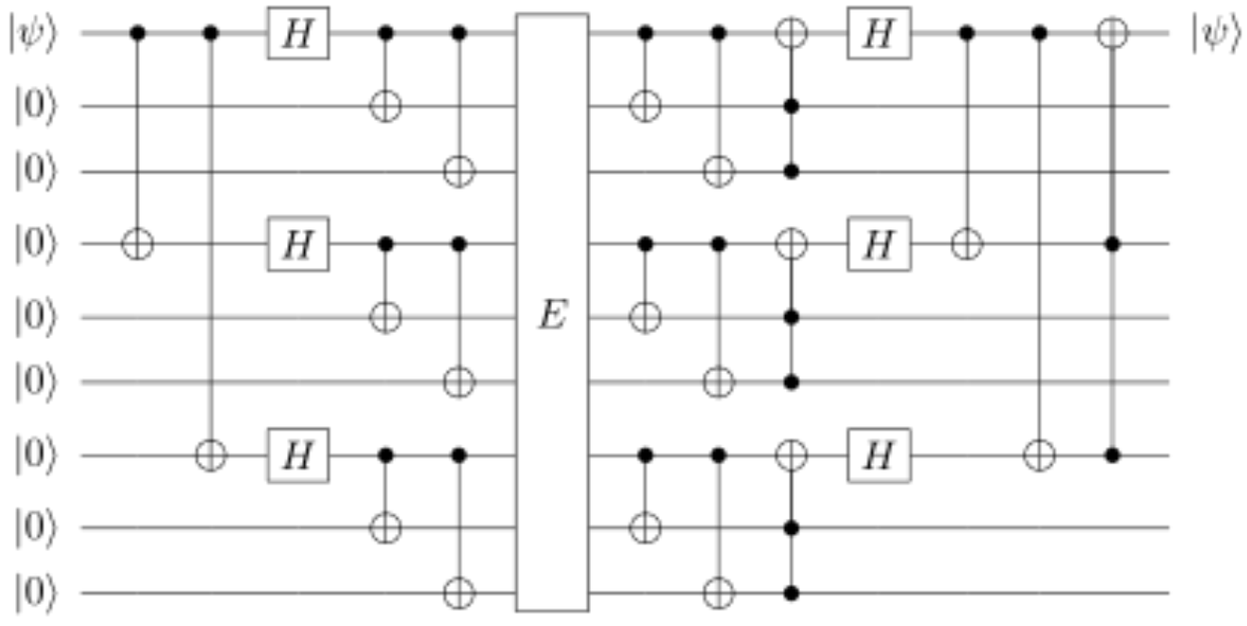



- Advantages and disadvantages
  - scalable
  - fast
  - can be built in semiconductor foundries
  - lots of decoherence in a solid state device



# Quantum error correction

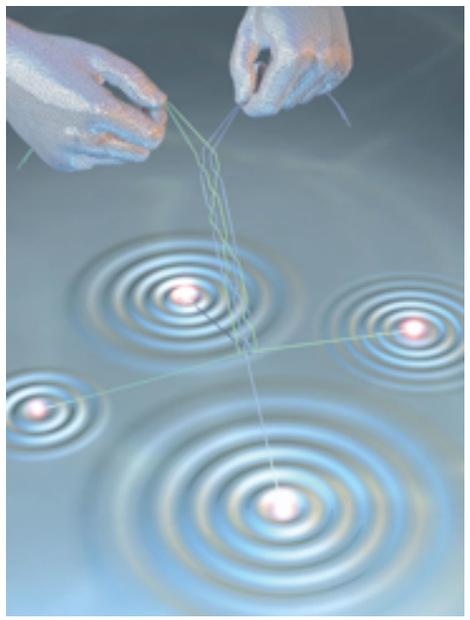
- **Example: Shor's code** protects a against sign or bit flip errors
- Needs nine qubits and substantially increases  number of gates



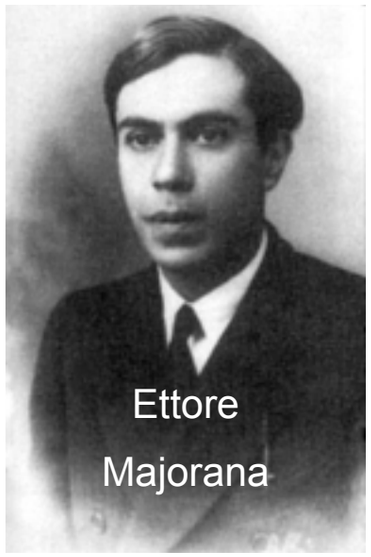

- Codes need to be recursively iterated to protect against multiple errors
- Quantum error correction overhead is at least 1000x more qubits and gates for any reasonable computation

# Topological qubits (Microsoft and universities)

- Encode the qubit in a topological property of a quantum state
  - Intrinsic protection due to topology
  - No local noise can decohere the qubit
  - No expensive error correction needed
  - Operations done by “braiding” isolated particles



- Most promising: Majorana particles
  - may exist at ends of superconducting nanowires
  - hope to confirm their existence within 5 years

# (Optimistic) road map for quantum computers

- First quantum devices exist, but computational power is limited
  - quantum random numbers
  - quantum encryption
  - quantum simulators
  - quantum optimizers



- General-purpose quantum computers will always remain special purpose accelerators for selected tasks
- My optimistic road map
  - Today: 14 qubits allowing up to 100 operations
  - 2020: a long-time stable quantum bit with quantum error correction
  - 2025: matching classical CPUs on selected applications
  - 2030: outperforming any hypothetical classical computer on selected applications
- Huge potential for classical spin-off technology (e.g. superconducting)

# Quantum computing applications

- Identifying killer-apps for quantum computing is challenging
  - the problem has to be hard enough that it cannot be solved on a PC
  - the problem has to be amenable to quantum acceleration
  - the crossover scale has to be short enough to make it useful
  - CMOS technology is a tough competitor
  - we need to consider special purpose classical devices as competitors

- Potential applications
  - factoring and code breaking (limited use)
  - quantum chemistry and material simulations (challenging but enormous potential)
  - solving linear systems (can't we solve them well enough already?)
  - machine learning???

- It is time to move quantum computing research from theoretical computer science to high performance computing