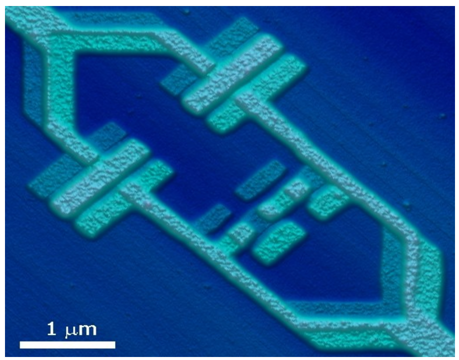
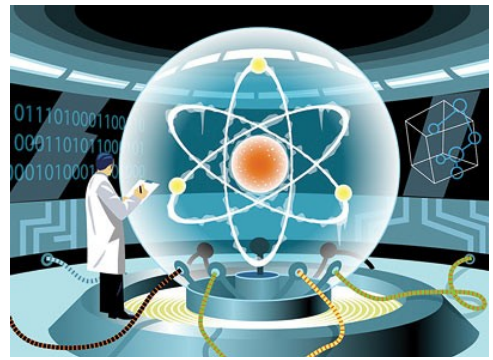
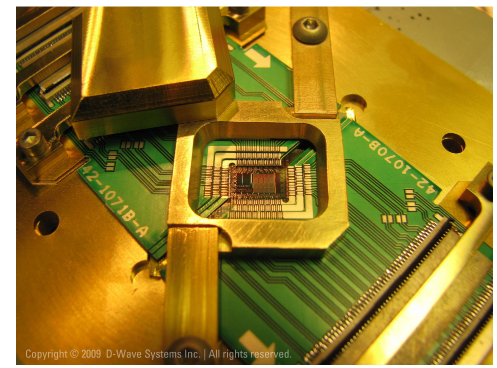
Quantum Computing



Separating the 'hope' from the 'hype'

Suzanne Gildert (D-Wave Systems, Inc)
4th September 2010
10:00am PST, Teleplace

The Hope

- All computing is constrained by the laws of Physics and Mathematics, at a very low level.
- The laws governing quantum objects are different to those that govern the informational content of 'classical' computers
- Therefore quantum computers can do 'some things' that classical computers cannot.

The Hype

- “Quantum Computers can break cryptographic protocols and will disrupt life as we know it”
- “Quantum computers are exponentially faster than classical computers!”
- “Quantum computers can do all the calculations simultaneously!”
- “Quantum computers can solve NP-Complete problems in polynomial time!”
- These statements are all wrong (to varying degrees)

Definition

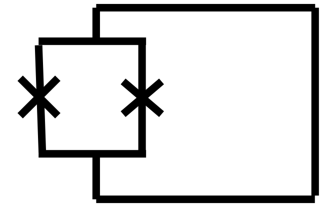
"A quantum computer is a machine which uses the quantum effects of superposition and entanglement as part of its intrinsic computational operation"

Checklist of Quantum Effects!

- Superposition
- Entanglement
- Not so cool: Decoherence

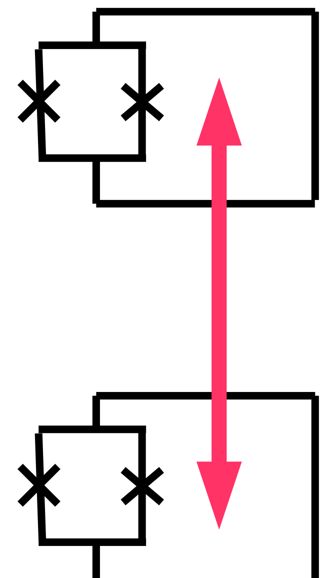
Superposition and entanglement

- Classical bit: 0 or 1
- Superposition state: linear combination of 0 and 1 in varying amounts = QUBIT.



A|0> + B|1>

- Entanglement: Correlations between states
- The ability of two quantum states to become 'locked together', even if physically separated (Einstein thought this was “spooky”)

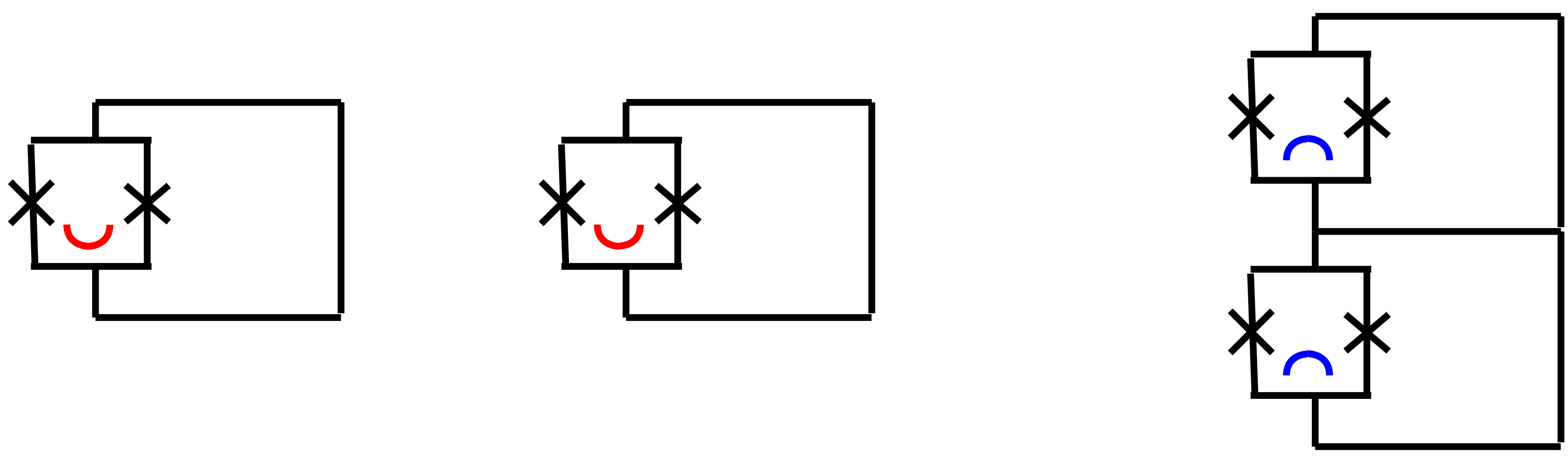


So we have our quantum effects....

What's the problem?

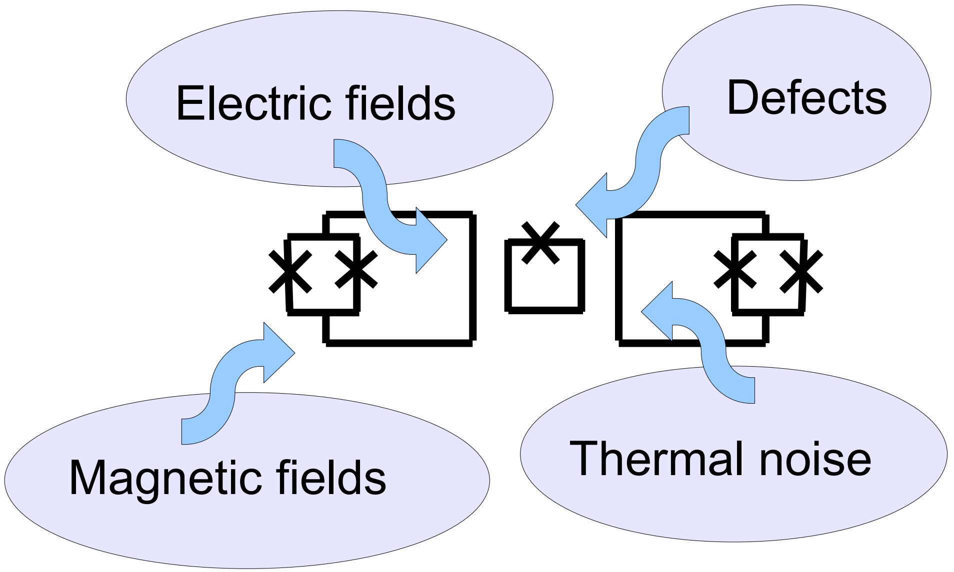
Why it is hard to build a QC

- N Qubits working individually does NOT equal an N-qubit QC.
- This is counter intuitive, as it works with regular circuit components.
- Decoherence plays a big role....



Decoherence – know thy enemy!

- Ways in which the system can exchange energy with the environment are potential sources of decoherence

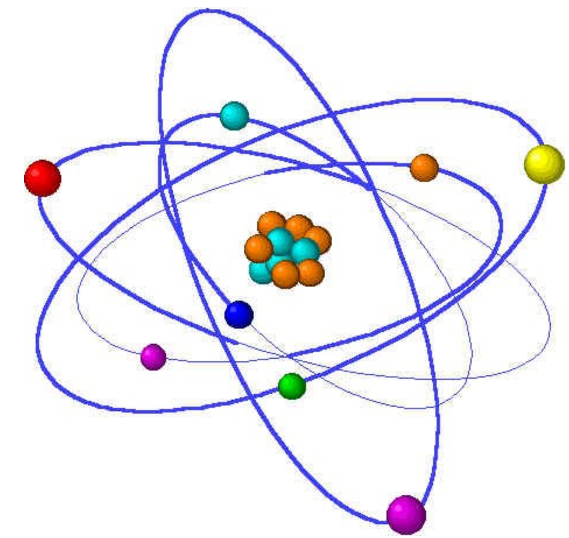


- More qubits = more decoherence

- The main reason why progress in QC has been so slow...

Why we should build one anyway

- Standard computers are not good at modelling quantum systems
- Even if quantum computers have no use for large-scale classical problem solving (which is unlikely), they are still the only way we can feasibly simulate quantum systems.



- This is important for our understanding of the way the world works!

But things are not so simple....

Not all QC are born equal...

You can't just 'build a generic quantum computer' anymore than you can 'build a generic vehicle'

There are different 'ALGORITHMS', 'MODELS' and 'IMPLEMENTATIONS' of QC.

This is VERY IMPORTANT! It is where most of the confusion arises about the power of QC – even amongst researchers ;)

If nothing else, remember this slide.

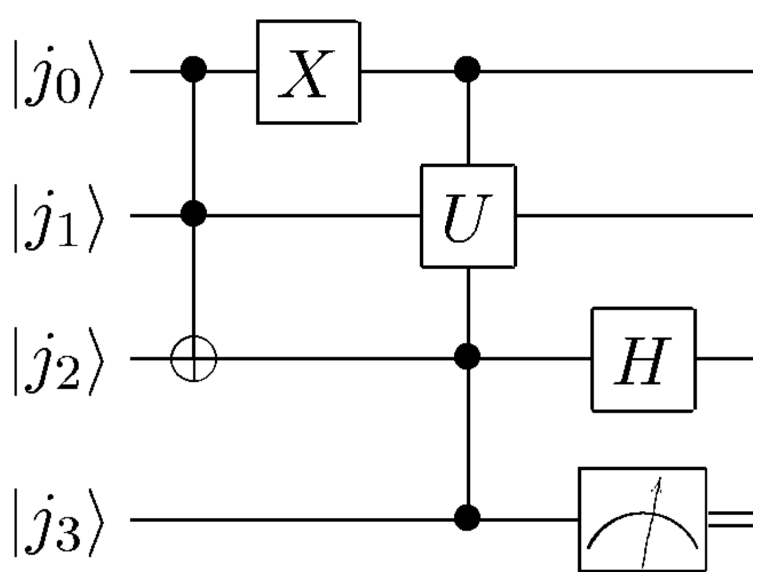
- **Algorithm**: The strategy for solving a problem, e.g. 'how would I invert a matrix?'
- **Models**: Think of this like the different computer architectures: *(Von Neumann, distributed/parallel computing, neural networks).* All good at running particular algorithms...
- **Implementations**: How you actually build it.. Silicon? Water? Beads on a string? Ants?

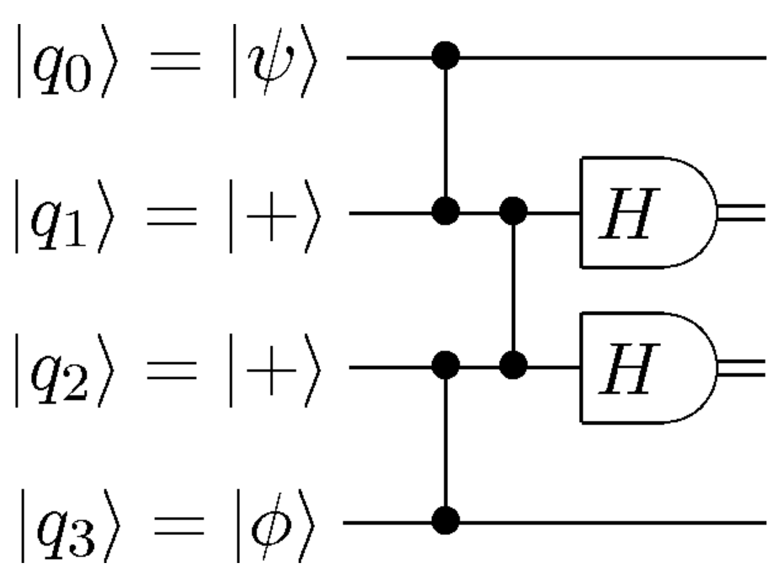
The quantum equivalents...

- **Algorithm**: E.g. Shor's algorithm, Grovers algorithm
- **Models**: Gate model QC, Adiabatic QC, Measurement based QC, Topological QC
- **Implementations**: Ion traps, NMR, Superconducting Qubits, Nitrogen Vacancies in diamond, Atomic transitions, Photonic systems

Gate model QC

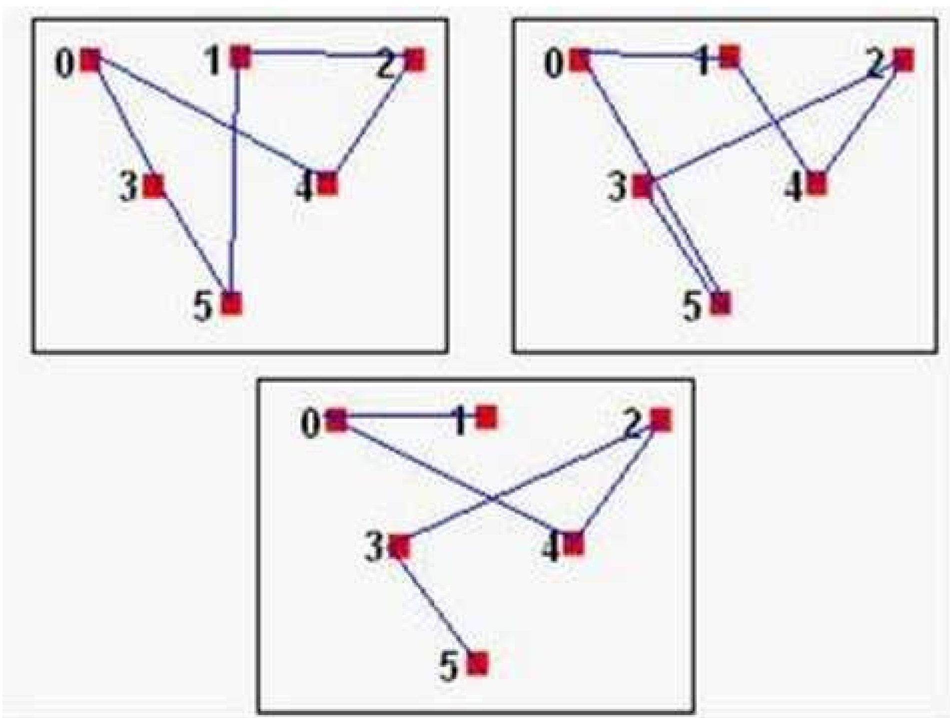
- Gate model – uses qubits like 'quantum logic gates' – but very prone to decoherence
- Easier to understand, a familiar approach

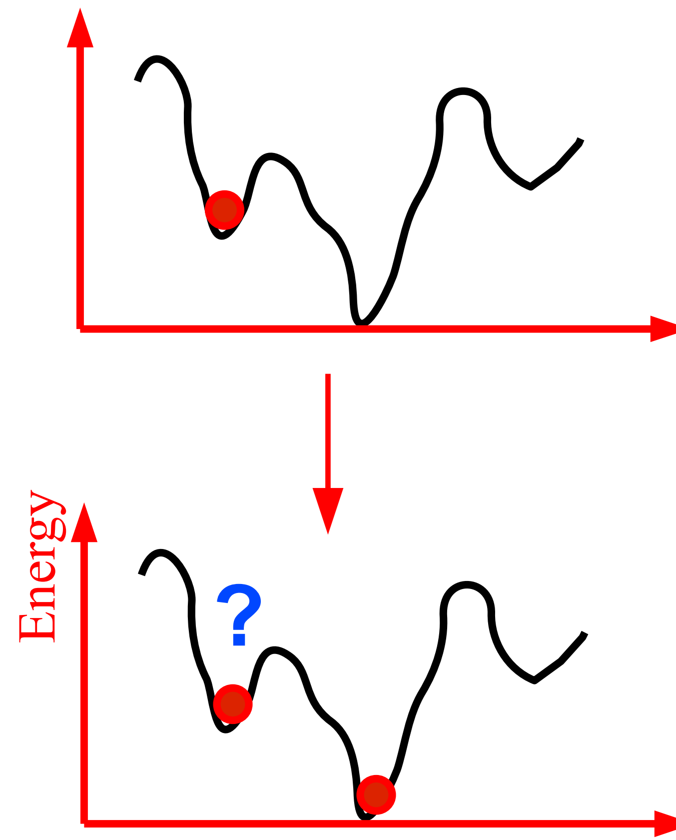




Adiabatic QC

- AQC – uses large numbers of qubits and operates more like simulated thermal annealing...

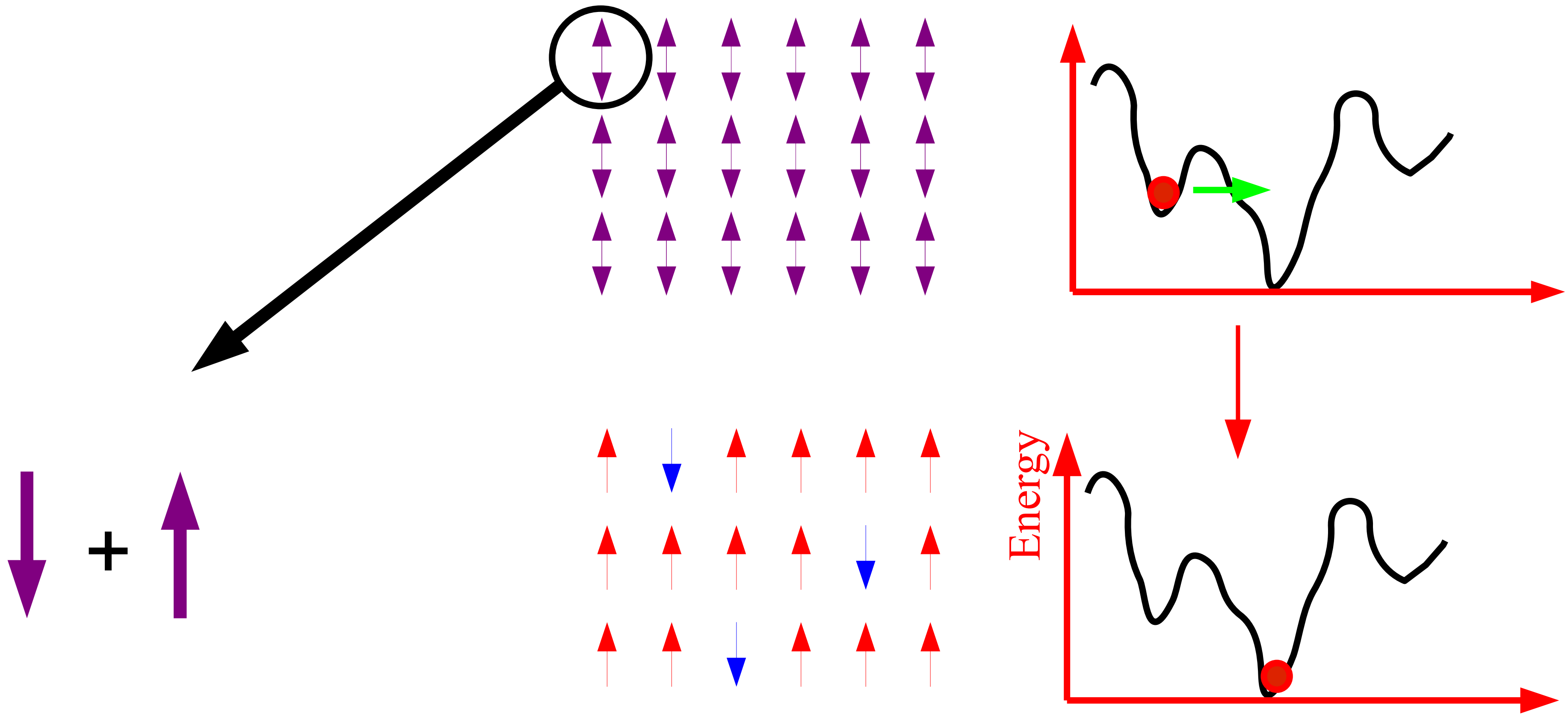




- To solve problems e.g. traveling salesman problem

Adiabatic QC

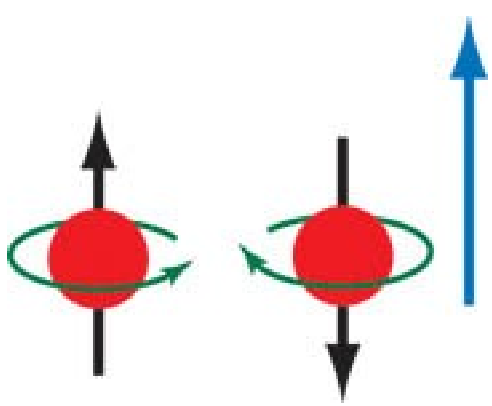
… But with a quantum twist - Use quantum annealing



and a large number of qubits to encode the problem

Enough about models, how do you build one?

- Rule of thumb: Anything small, or cold, usually exhibits quantum mechanical effects!
- Anything with a well defined 'quantum variable'

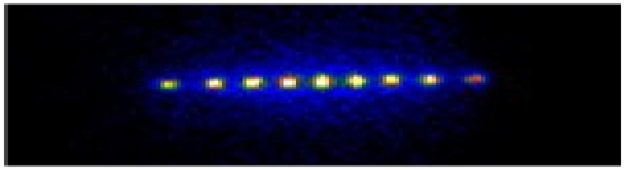


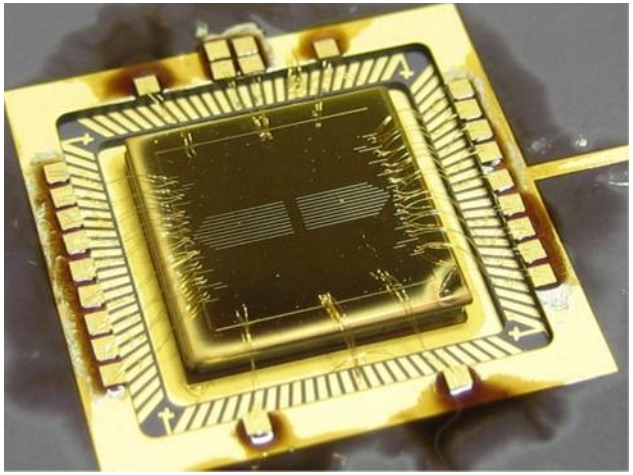
- Many systems exist that have nicely defined 0 and 1 states
- And exhibit quantum effects of superposition and entanglement as required... atoms, electrons, photons...

Implementations

- Ion Trap systems (ions)
- NMR schemes (atoms in a molecule)
- Nitrogen Vacancy (nanotechnology)
- Superconducting electronics (electrons)

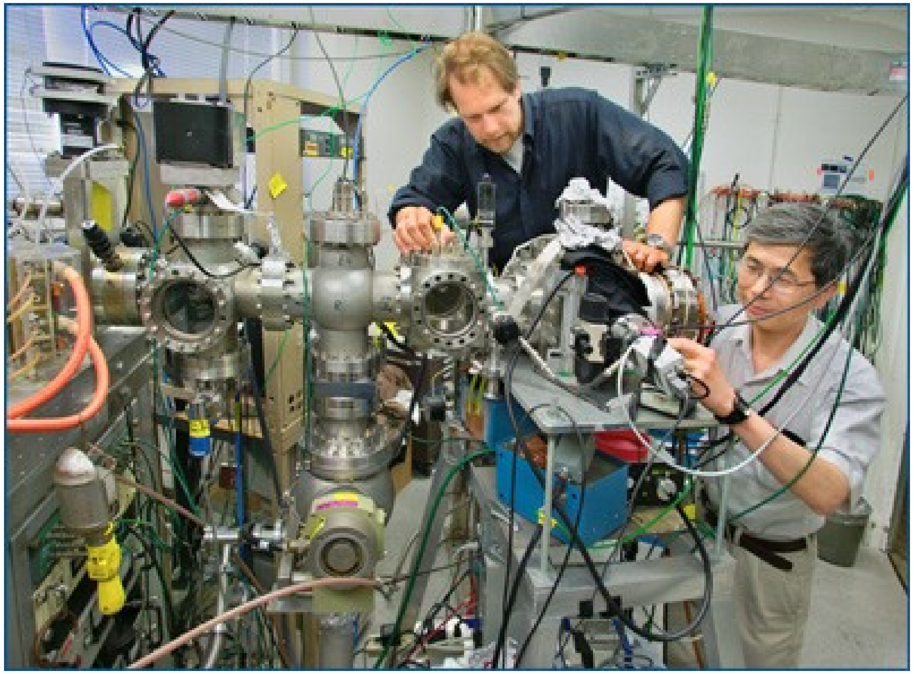
Ion Trap QC





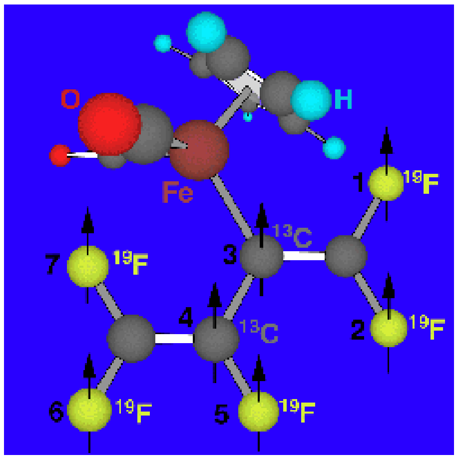
ion-to-surface distance is 150 microns, vibrational frequency for trapped Ca ions is 3.5 MHz

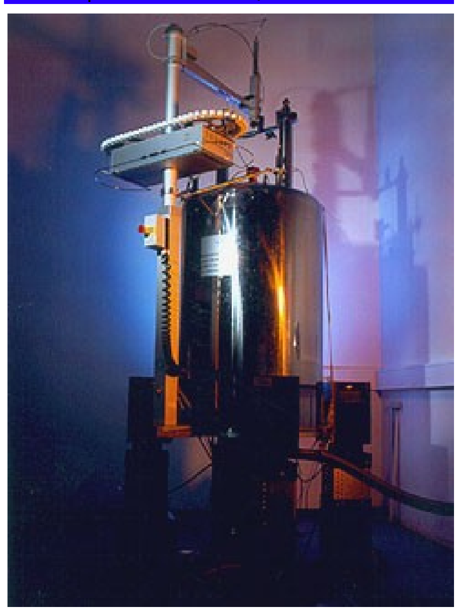
http://www.physics.ox.ac.uk/users/iontrap/



- Uses the interactions between energy levels in ionised atoms as the quantum variable
- Can run several algorithms using the 'gate model'

NMR QC



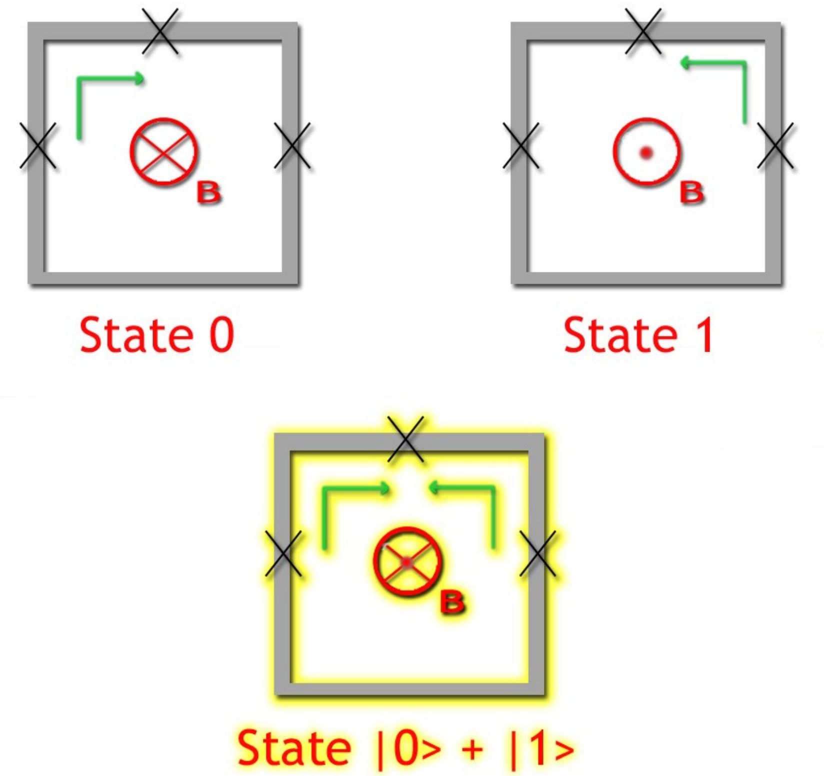


- Uses the interactions between the nuclear spins of atoms at various positions in a molecule
- IBM famously built a 7 qubit 'NMR QC'
- It runs 'Shors algorithm' on a 'Gate Model' system, and was able to factor the number 15

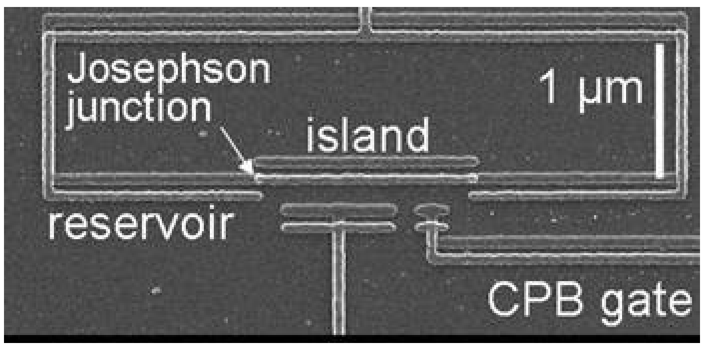
My favourite implementation

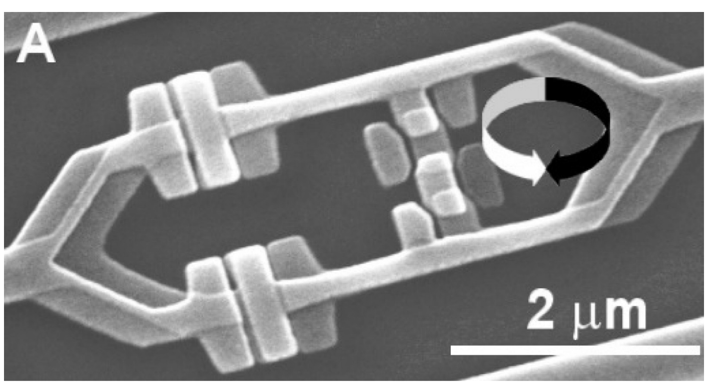
Superconducting QC

- Loops of superconducting metal
- Current flows with no resistance depending upon applied field
- In a superconductor, the current and field become quantum mechanical
- Choose correct field = superposition of currents!



What do superconducting flux qubits look like?

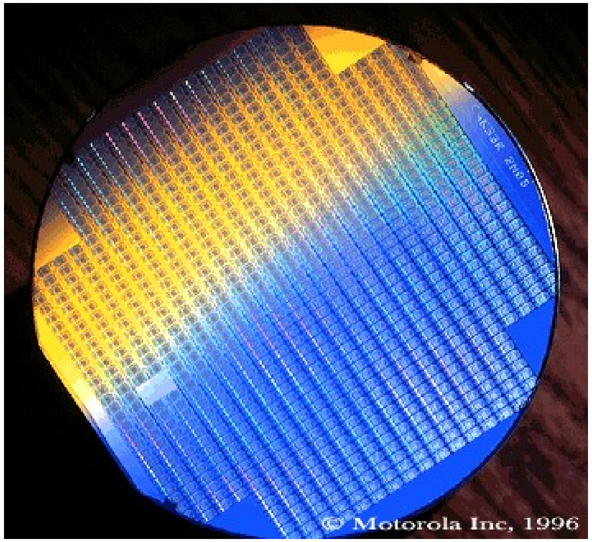




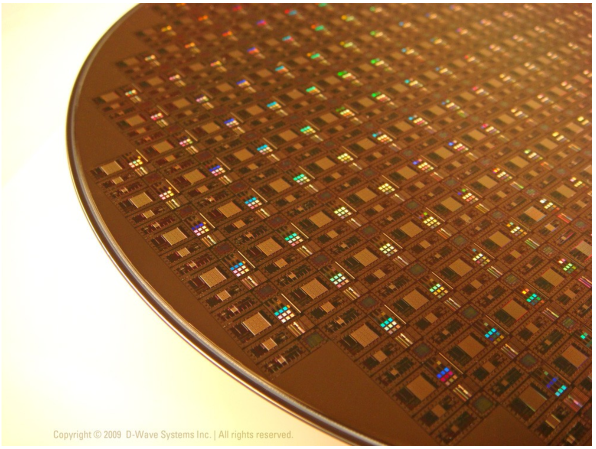
- They are tiny components, like transistors, patterned in a similar way to CMOS devices, but made from Al or Nb.
- Between 0.1 and 10microns in size
- They do not dissipate any power in certain modes of operation

Why Superconducting Flux Qubit?

- Compatible with existing processor fabrication methods
- Scalable
- A logic family based around superconducting hardware already exists
- Disadvantages: Requires extreme environments (temperature, low magnetic field) & prone to decoherence



Standard CMOS processor wafer



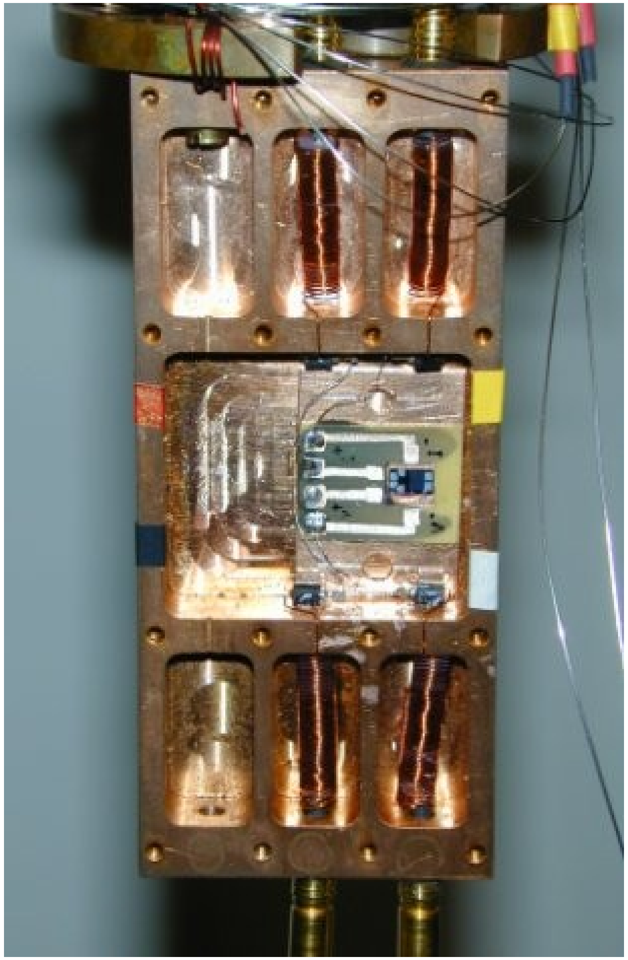
D-Wave superconducting processor wafer

Cooling Flux Qubits

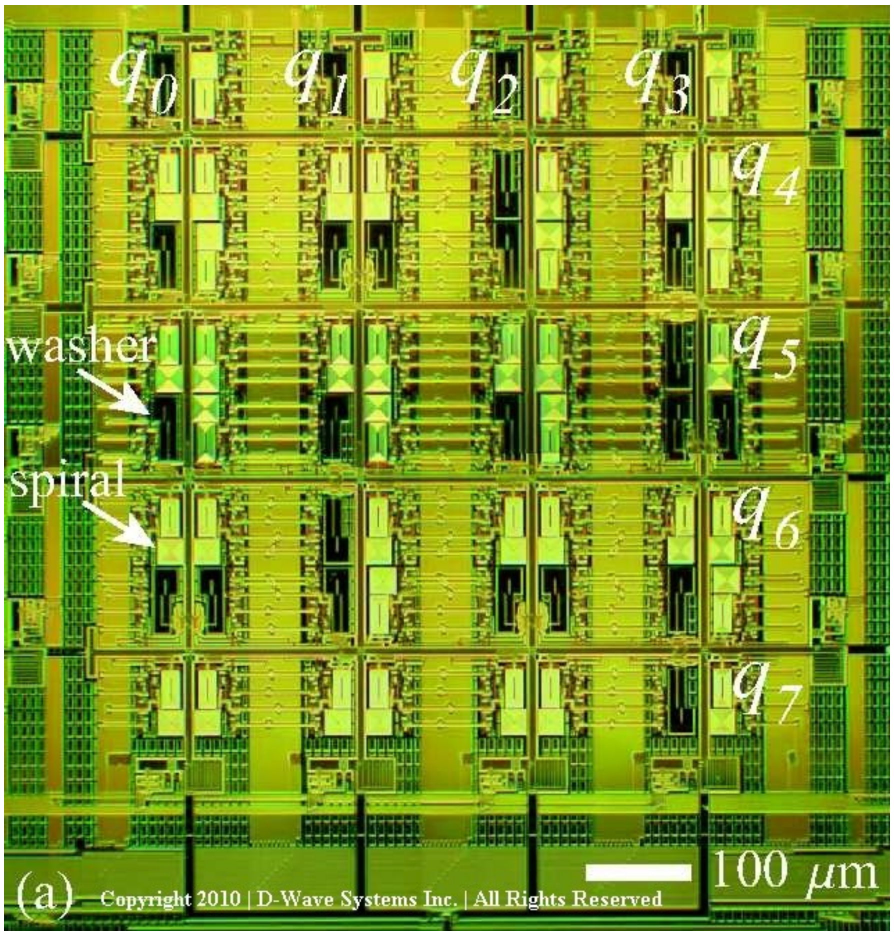
- Temperature – 20mK
- Just above absolute zero
- Extreme magnetic field environments
- EMI shielded room housing
- All to avoid decoherence...

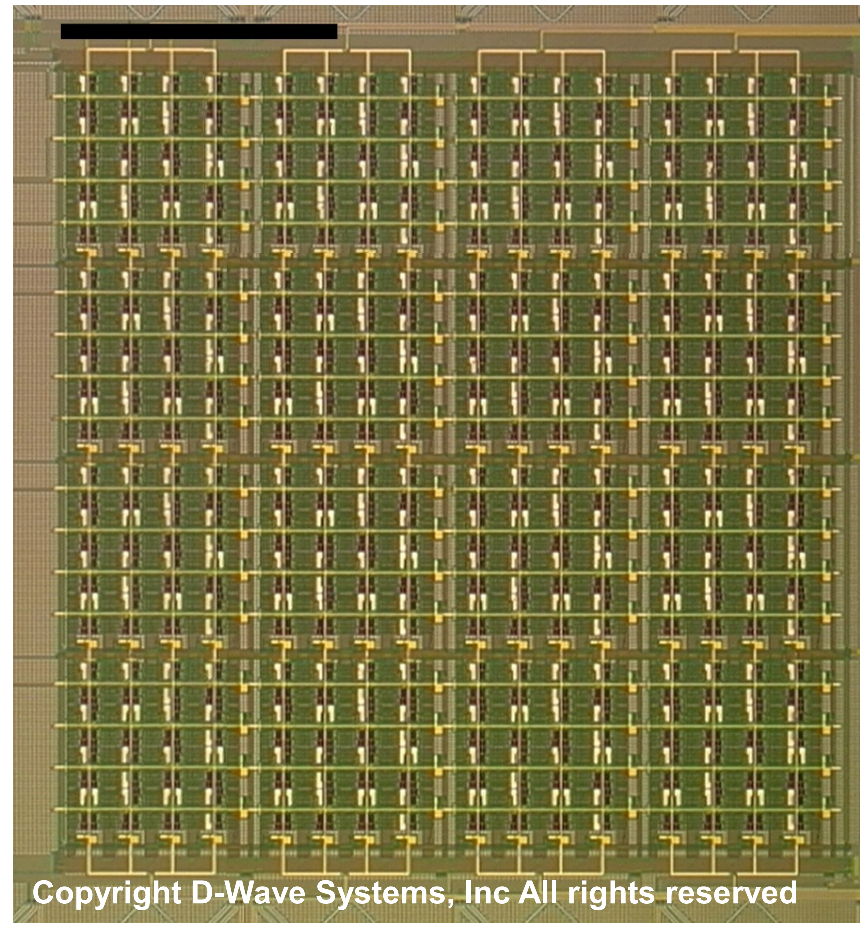
Dispelling a qubit myth...

- Room temperature superconductors won't help!



128 Qubit Processor



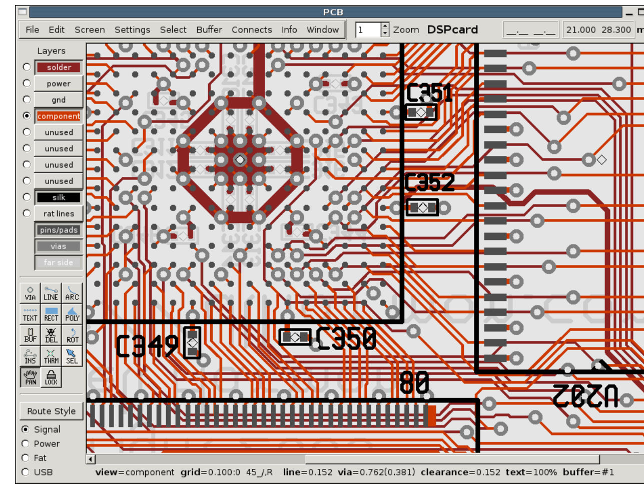


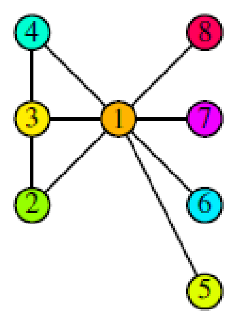
- This chip runs the 'adiabatic quantum optimization' algorithm, using an 'AQC model', and is implemented with 'superconducting qubits'

Applications

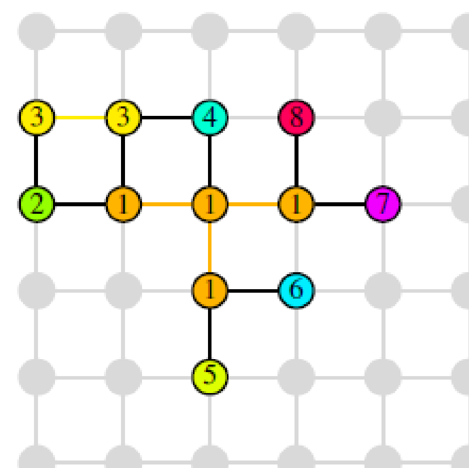
Graph Applications

- Congestion simulation
- Microprocessor design
- Traveling salesman
- Network routing
- Circuit routing





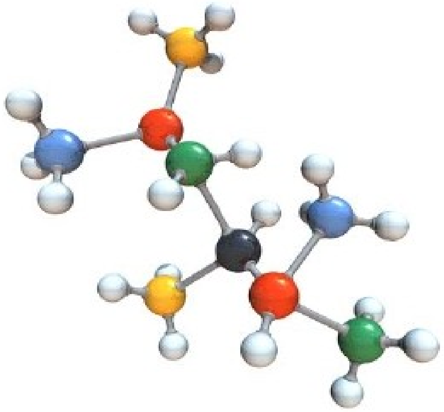
G

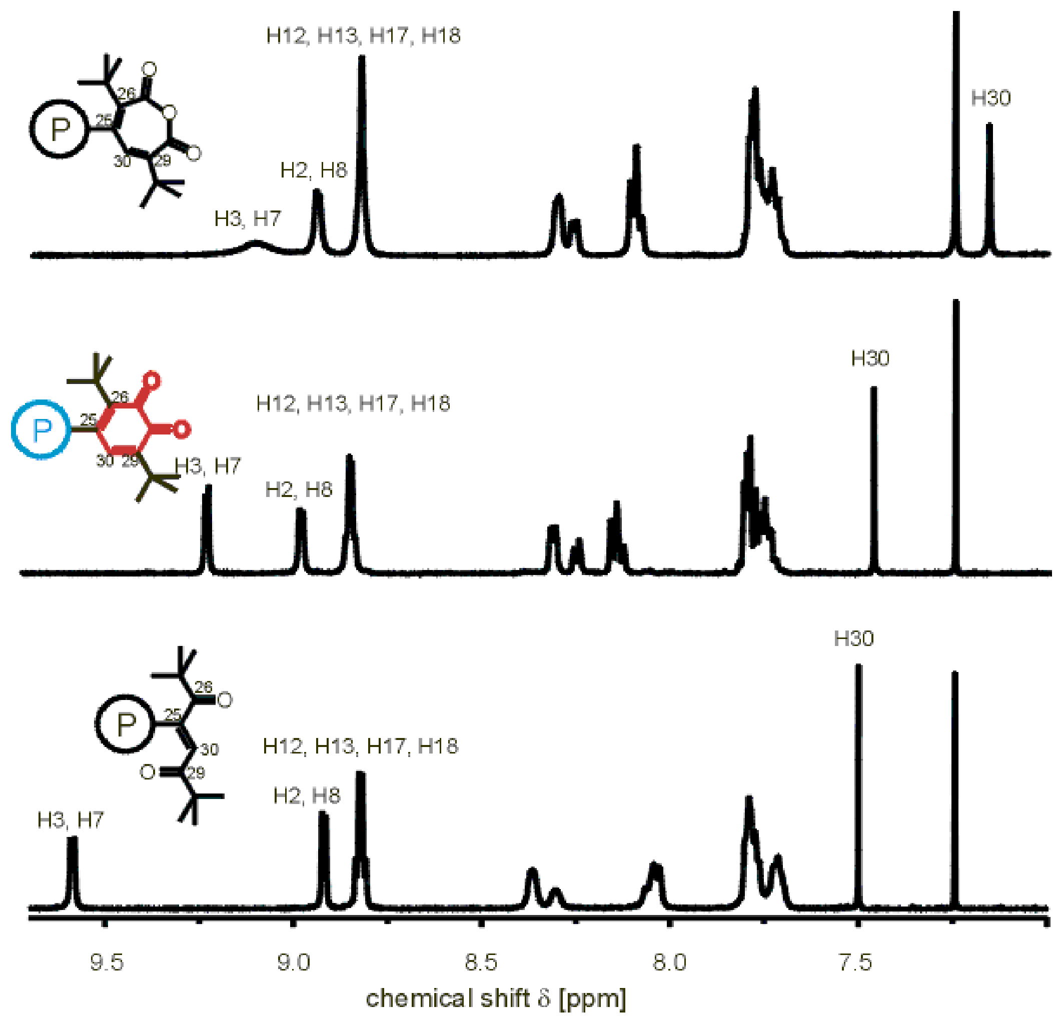


G_{emb}

Bio Applications

- Metabolomics
- Gene sequencing
- Protein folding
- Bioinformatics





Security Applications

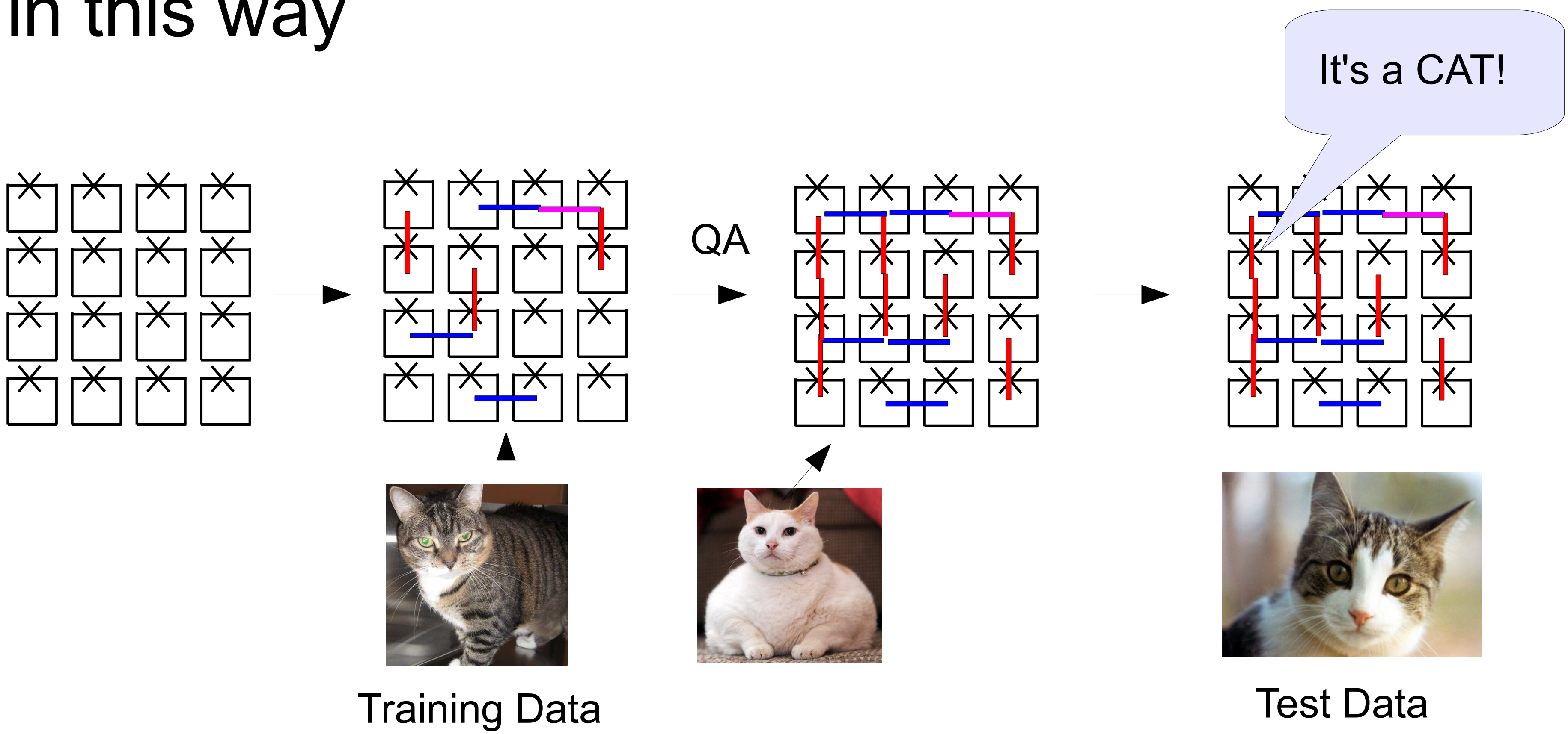
- Cryptography
- Biometrics
- Image recognition
- Database searching
- Scanning network traffic

AI applications

- Machine learning
- Pattern recognition
- Neural networks
- Building synthetic brains!

Neural networks

- AQC is very well suited to neural networks
- DWave chips were used to train a 'car detector' in this way



Timeframes and predictions!

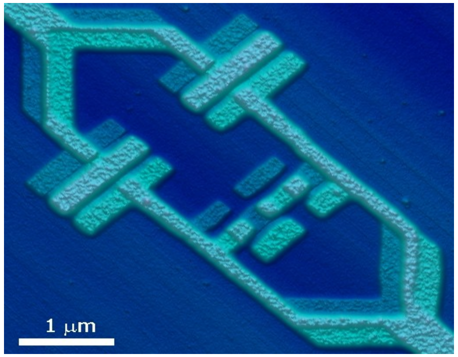
- AQC commercially applicable within the next few years
- Gate model quantum computing is much further away, perhaps 10 years.
- Superconducting hardware will be a strong candidate, followed by Ion trap QC and (possibly) Nitrogen Vacancy QC.

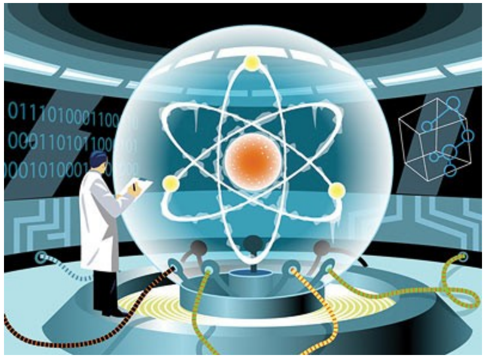
Take away message

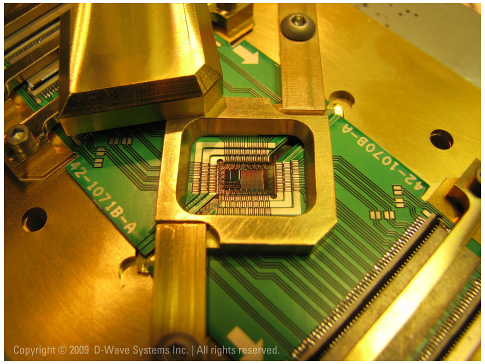
"Quantum Computers are not a magic bullet to solve all hard problems, nor are they by any means easy to build!

...Yet they have interesting applications, and from a computational point of view will allow us to perform simulations based on our best understanding of the nature of the universe."

Quantum Computing







Separating the 'hope' from the 'hype'

Suzanne Gildert

4th September 2010

10:00am PST, Teleplace