Imperial College London

AI Summit London – 14 June 2018

Quantum Computing Summit: The Potential of Quantum Computing for Enterprises

Mario Berta – Department of Computing

Imperial College London

Quantum Information Science

- Understanding quantum systems (e.g., single atoms or electrons) is hard

Richard Feynman
The Nobel Foundation

Understanding physics with computers '81

"trying to find a computer simulation of physics seems to me to be an excellent program to follow out (...) nature is not classical, dammit, and if you want to make a simulation of nature, you would better make it quantum mechanical, and by golly it is a wonderful problem, because it does not look so easy"

- Information processing based on quantum physics:
  Quantum Information Science

Imperial College London

Quantum Technologies are growing fast

Main motivation is

that we believe quantum technologies will enable us to do things that we do not know how to do using only (future) classical technology

- Academic interest:
  UK national network of quantum technology hubs (UKNQT) + EU quantum manifesto flagship-scale initiative in quantum technologies

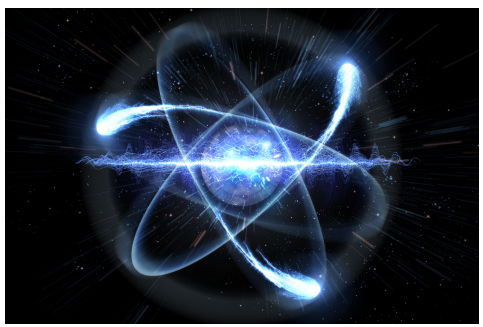
UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

- Central intelligence agencies GCHQ + NSA:
  "we must act now against the quantum computing threat in cryptography"
- Big IT players investing in quantum technologies:
  Alibaba, Google, IBM, Intel, Microsoft, Nokia Bell Labs, NTT Laboratories, etc.
- Explosion of quantum start-ups

Imperial College London

Overview of Quantum Technologies

1. Direct quantum hardware applications:
   - quantum enhanced sensing such as quantum clocks
   - quantum annealing
   - analogue simulations of quantum systems
2. Digital quantum simulation of quantum materials and chemical reactions:



Quantum simulation

Quantum error correction codes

allow to efficiently simulate any (relevant) physical process that occurs in nature

- the design of more efficient solar panels in material sciences
- the design of improved pharmaceuticals and catalysts in computational chemistry

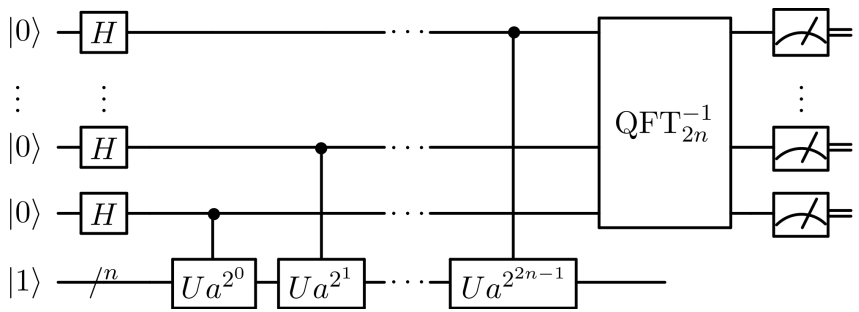
Imperial College London

Overview of Quantum Technologies (continued)

3. Quantum computation with (super-polynomial) speed-ups over classical algorithms, e.g., for
   - finding the prime factorization of large numbers
   - solving certain linear and convex optimization problems
   - recommendation systems

   Quantum algorithm zoo: math.nist.gov/quantum/zoo/

- Important consequences for cryptography and deep learning:



Shor's algorithm for prime factorization '94

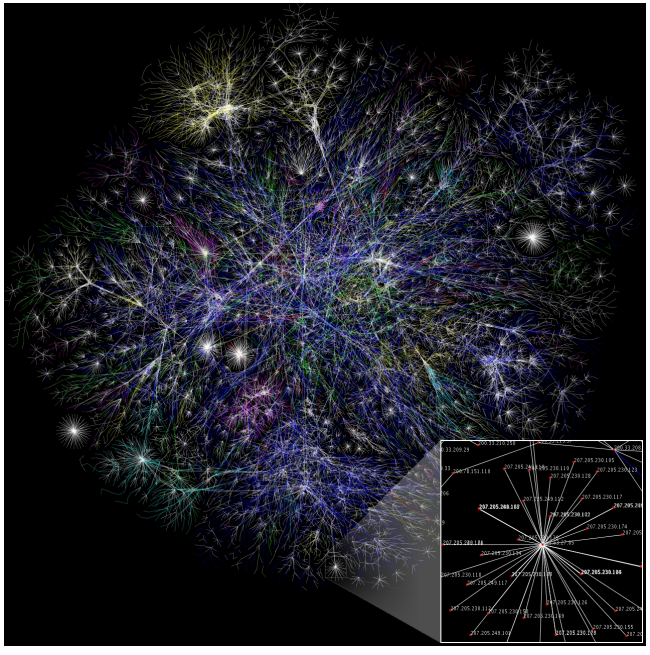
Wikimedia commons

Quantum algorithm

for prime factorization breaks RSA public key cryptosystem – that is, virtually any encryption scheme in use today!

Imperial College London

Overview of Quantum Technologies (continued)



Graphical depiction of network

The Opte Project

4. Quantum cryptography has two aspects:
   - *Quantum-safe cryptography* studies how to protect from adversaries with access to quantum technologies
   - *Quantum-based cryptography* leading to, e.g., quantum random number generators, quantum key distribution schemes, quantum authentication schemes, quantum money, etc.
5. Quantum communication using repeaters for networks leading to the quantum internet
6. Quantum software to run quantum algorithms

Quantum hardware –

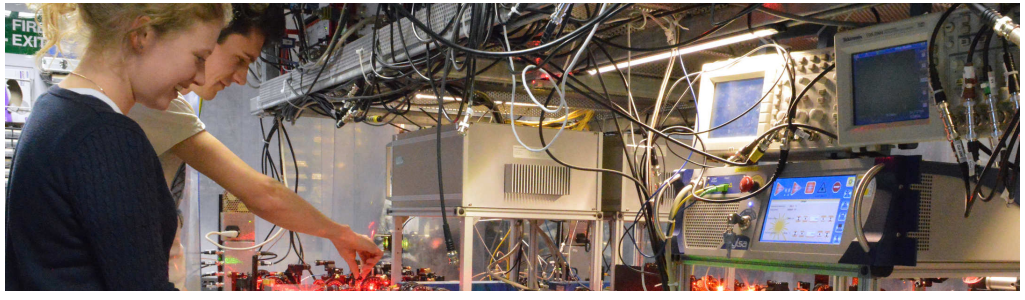
how to build any of this?

Imperial College London

Quantum Engineering for Quantum Hardware

Build well-controlled quantum systems – approaches include

- Cavity quantum electrodynamics
- Optical lattices
- Ion traps
- Superconductors
- Quantum dots
- Linear optics



Imperial Centre for Quantum Engineering, Science and Technology (QuEST)

Noisy Intermediate Scale Quantum (NISQ) Technology

Available now / in the near future

are at most around 50 – 100 qubits with error rates at best around 0.1%

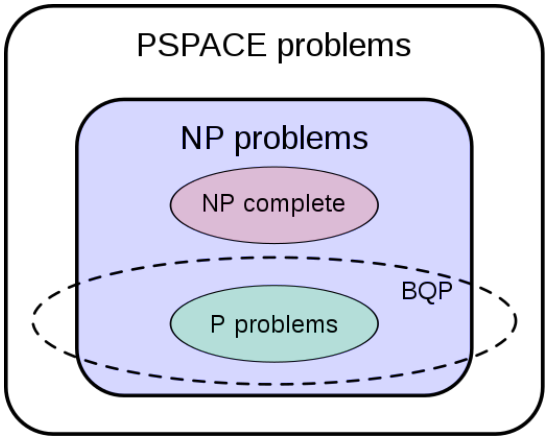
- Examples of superconducting architectures:
  - IBM Q System 50-Qubit Quantum Processor
  - Google Bristlecone 72-Qubit Quantum Processor
- Indications that Moore's law is slowing down, replaced by quantum Moore's law?
- Better metric is quantum volume: number of qubits / error rates of qubits / connectivity of qubits / speed of qubits / etc.
- With NISQ technology quantum error correction is impossible and hence (naively) we can do at most 1000 gates.
- Nevertheless, very exciting frontier of fundamental research at the time: testbed to explore highly correlated quantum systems.

Imperial College London

Quantum Speed-up?

Quantum supremacy means

computational tasks performable by quantum devices, where one could argue that no existing (or easily foreseeable) classical device could perform the same task



Computational Complexity Theory

Wikimedia commons

Comparison of quantum versus classical difficult in practice:

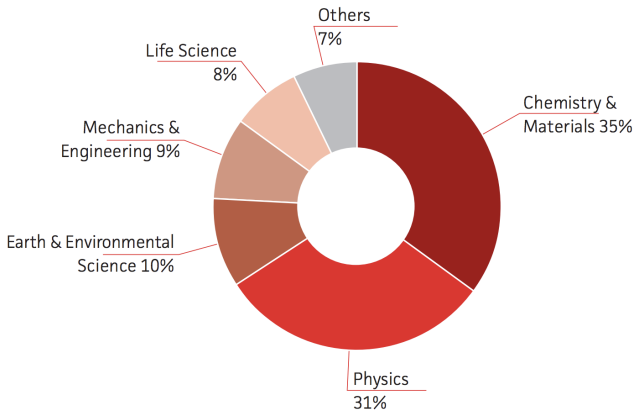
- classical moves along – future hardware
- fine-tuned classical algorithms and technology
- difficulty of benchmarking quantum computers

- Quantum supremacy claims might come soon. However, from a scientific (and even a business perspective) quantum supremacy is not so interesting by itself: stepping stone to move technology further

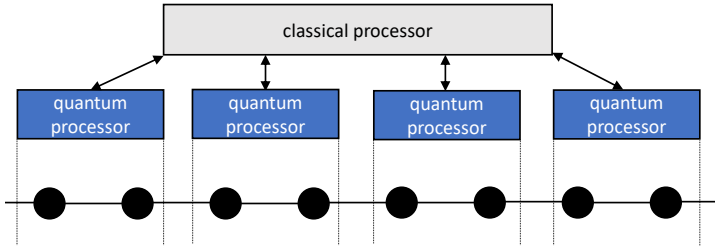
Imperial College London

What are the high impact applications?

1. Quantum cryptography is short-term answer:
   - privacy business is huge, quantum technology largely available
   - migration to quantum-safe cryptography needs to happen now, ongoing NIST "Post-Quantum Cryptography Standardization"
2. Quantum simulation is long-term answer:
   - for chemistry and material sciences
   - highly specialized quantum hardware managed by classical routines (heuristics)



Swiss National Supercomputing Centre
Annual Report 2017



Example: thermal state of one dimensional chain of atoms – local versus global degrees of freedom

Our work at Imperial: marioberta.info

Imperial College London

Outlook on Quantum Computing

- Funding a business versus funding fundamental science:
  - faster / better means in terms of resources = money, computational power per dollar
  - "solve relevant problems" instead of "demonstrate quantum supremacy"

  Except for quantum-safe cryptography – which we should worry about now (!) – we might not be there (yet). However, soon to be available NISQ quantum hardware will allow to experimentally explore the power of quantum computing.
- Quantum technology will be used for very specialized tasks and in parallel to classical computers, at least for a long time.

Take home message is

to remember the revolution that came with classical computing and what long-term influences it had. Quantum computing has similar potential – and you want to be on board early.

- Further reading: Quantum Computing in the NISQ era and beyond (John Preskill)

Thank you for your attention. Our work at Imperial: marioberta.info