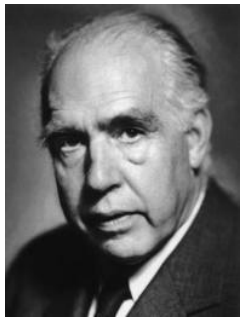
The Potential Impact of Quantum Computers on Society

Ronald de Wolf

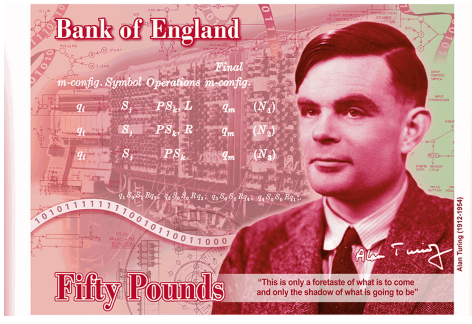
CWI QuSoft Universiteit van Amsterdam

Quantum computers

Quantum mechanics:
developed from 1900



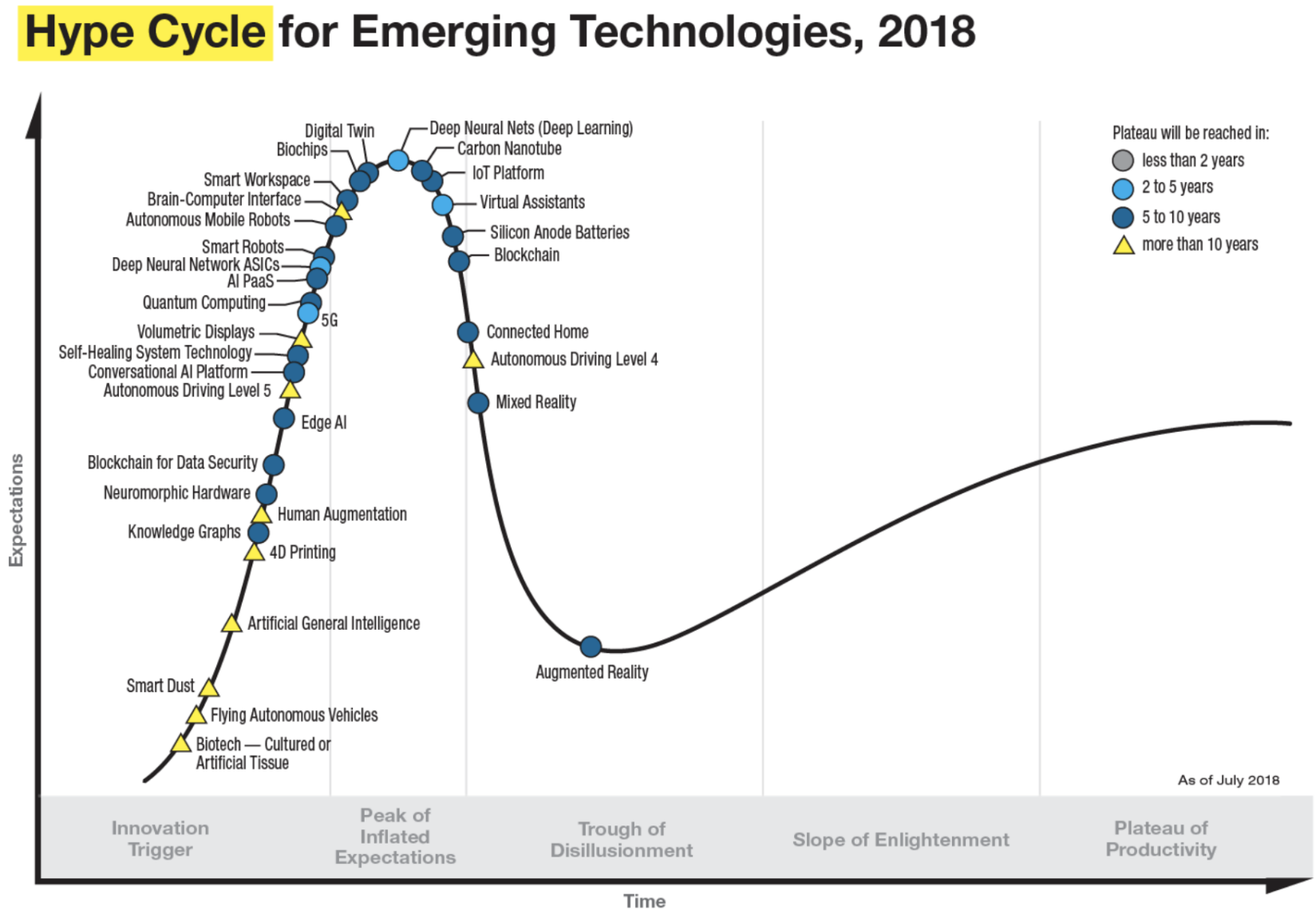
Computer science:
developed from 1930s



Richard Feynman, David Deutsch
in early 1980s:

Harness those quantum effects for useful computations!

Quantum computers: hype vs substance



Where do we stand today?

- Noisy Intermediate-Scale Quantum technology era (NISQ, Preskill'18)
- Google, IBM, Intel are close to 50-70 reasonably good qubits.

  But 50-70 qubits is not a lot: classical computers have billions of bits. And "reasonably good" is also not great
- We'll need error-correction to deal with errors, and that will require many more physical qubits
- "Quantum supremacy" reached soon (maybe already reached): some quantum computation that cannot be simulated on today's best supercomputers in a reasonable amount of time
- But useful quantum supremacy is still years away

Quantum computers: hype vs substance

The goal of this talk:

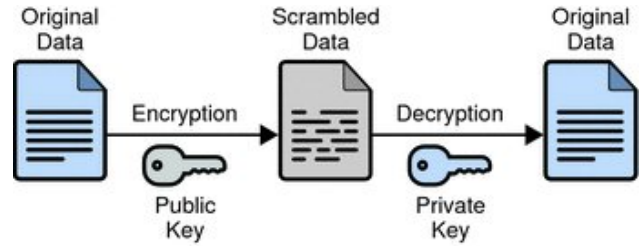
Assume large quantum computers will be built in the next decades.

Where will they have a real impact?

- Probably: Cryptography, optimization, simulation
- Maybe: Machine learning
- Not really: Efficiently solving NP-hard problems, ending climate change, ending world hunger, finding ET, ...

Potential impact area 1: cryptography

- Public-key cryptosystems are great:
  - you choose private key and public key
  - everybody with the public key can send you encrypted messages
  - messages can only be decrypted by someone with the private key (=only you)



. . . unless they can solve some hard math problem

- Most public-key crypto is based on the assumed hardness of
  - factoring large integers (RSA), or
  - finding discrete logarithms (Diffie-Hellman, Elliptic curve)
- Shor's algorithm breaks this using a few thousand good qubits
- Symmetric crypto systems like AES are more secure, but require shared secret key

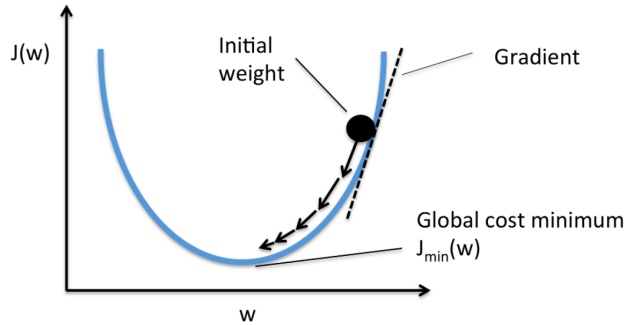
Is this an imminent threat?

- Relax, quantum computers ain't gonna happen anytime soon...
- Maybe, maybe not.

  But many countries have laws requiring top-secret documents to be protected for the next 20-30 years.
- Also, changing our crypto infrastructure will take a long time
- So, how to save cryptography from quantum adversaries?
  - Post-quantum cryptography: public-key crypto, based on other math problems than factoring or discrete log (lattices, codes).
  - Quantum cryptography: use quantum effect to build new type of cryptography (example: quantum key distribution)

Potential impact area 2: optimization

- Optimization is one of the main applications of computers in the real world: allocating resources to jobs, scheduling lectures, optimizing designs, minimizing energy use, etc.
- Quantum computers can help:
  - Grover's search algorithm
  - Finding the shortest path on a map
  - Speed-ups for convex optimization
  - Gradient descent towards minimum



- Typically these only give limited ("polynomial") speed-up; whether that's worthwhile depends on the cost of a QC
- Classical input needs to be accessible in superposition, so needs to be stored in Quantum Random Access Memory

Quantum machine learning

- Machine learning has gotten hugely successful in the last 5 years

- After choosing set $\mathcal{M}$ of possible models & cleaning up data, machine learning boils down to an optimization problem:

  $$\max_{m \in \mathcal{M}} \text{ fit of } m \text{ with the data}$$

  Quantum computers can speed this up (in some cases)

- Often the data consists of vectors in some large dimension d. Can try to prepare those as $\log_2(d)$-qubit states, manipulate those with quantum algorithms. Easier said than done...

Potential impact area 3: simulation

- Much effort on understanding quantum systems for materials, batteries, drugs, high-temperature superconductivity etc.

  Sophisticated classical methods hit a wall for larger systems.

- That's why Feynman'82 wanted a *quantum* computer:

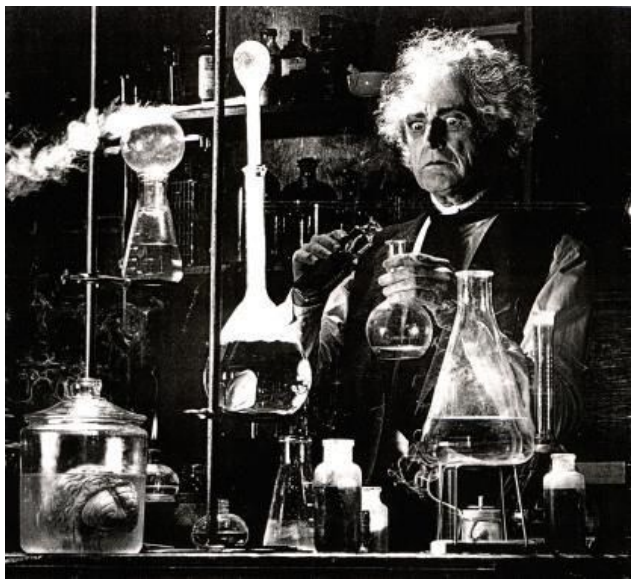
  efficiently simulate evolution of given initial state for time t

- In the last 5 years, such "Hamiltonian simulation" has been optimized, and people are starting to apply this to real physical systems of interest,
  like nitrogen-fixation for more efficient production of fertilizer

Quantum simulation could have huge impact

- A few hundred good qubits (and lots of gates. . .) suffice to do interesting things in quantum chemistry, so this is likely to be among the first real applications of quantum computers

- There could be quantum version of the "maker movement" or SETI: lots of amateurs start to explore and toy around with simulations of large molecules. Who knows what will be discovered!



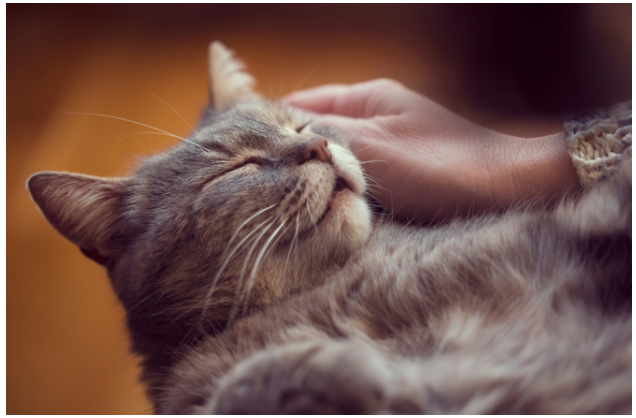
Summary so far

- Quantum computers are great

  not as great as some journalists make you think

  but much stronger than our current computers in some areas

- Should society be happy?



- Or afraid?

Risks to society: breakdown of crypto

- Large quantum computers can break all crypto that's based on factoring and discrete log

- Scenario 1: someone builds a QC, doesn't tell anyone, but uses it to read your email & steal your money
- Scenario 2: someone builds a QC, proudly announces this, and uses it to read your email & steal your money
- Either way, after a while this hacking is detected, and then all confidence in our current crypto schemes will disappear
- Fortunately, by then we should have tools to fix this: post-quantum crypto and quantum crypto

Risks to society: inequality

- Quantum computers are extremely expensive to build, and will probably remain so for a long time
- What if only one or a few parties can afford to build one?
- Inequality between countries: it's possible that only the US government will have a QC (at least for a while), like with the atomic bomb

- Inequality between companies: suppose QC is great for designing new medicines, and only company X has one. All other companies go out of business $\Rightarrow$ monopoly, so medicine prices will go through the roof

Mitigating inequality

- Hopefully quantum computing power becomes available widely through the cloud, like IBM Q Experience

- What if the market doesn't provide this,

  or governments try to prevent it?

  Possible solution:
  Santa Claus gives
  the world a quantum computer

Santa's little helpers: Norway, Gates Foundation, ...

Summary

- Quantum computation & information is wonderful science
- Quantum computers may become powerful practical machines, but that is still years (decades?) away.

  But in the NISQ era we can at least start to experiment
- Main areas where quantum computers may impact society:
  1. Cryptography
  2. Optimization
  3. Simulation of quantum systems
- Main risks to society:
  1. Breakdown of current cryptography
     post-quantum or quantum crypto will save us
  2. Increased inequality between countries, companies
     the cloud will save us (or Santa Claus)