
Demystifying
Quantum Computing
TAKING THE FIRST QUANTUM LEAP
Peter Flintholm
Security Consultant, Trifork
TRIFORK.
...think software

A few practical notes

1

Recording

We will be recording this Tech Update which you will be able to receive afterwards

2

Chat and Q&A

We will be using the chat to engage with you during the event

3

Post-webinar survey

We will be looking to get your feedback after the Tech Update

TRIFORK
...think software

Please answer this question
and submit your answer in the chat:

What is your industry and do you expect to start using quantum computers in the next 2 years?

TRIFORK
...think software

Agenda

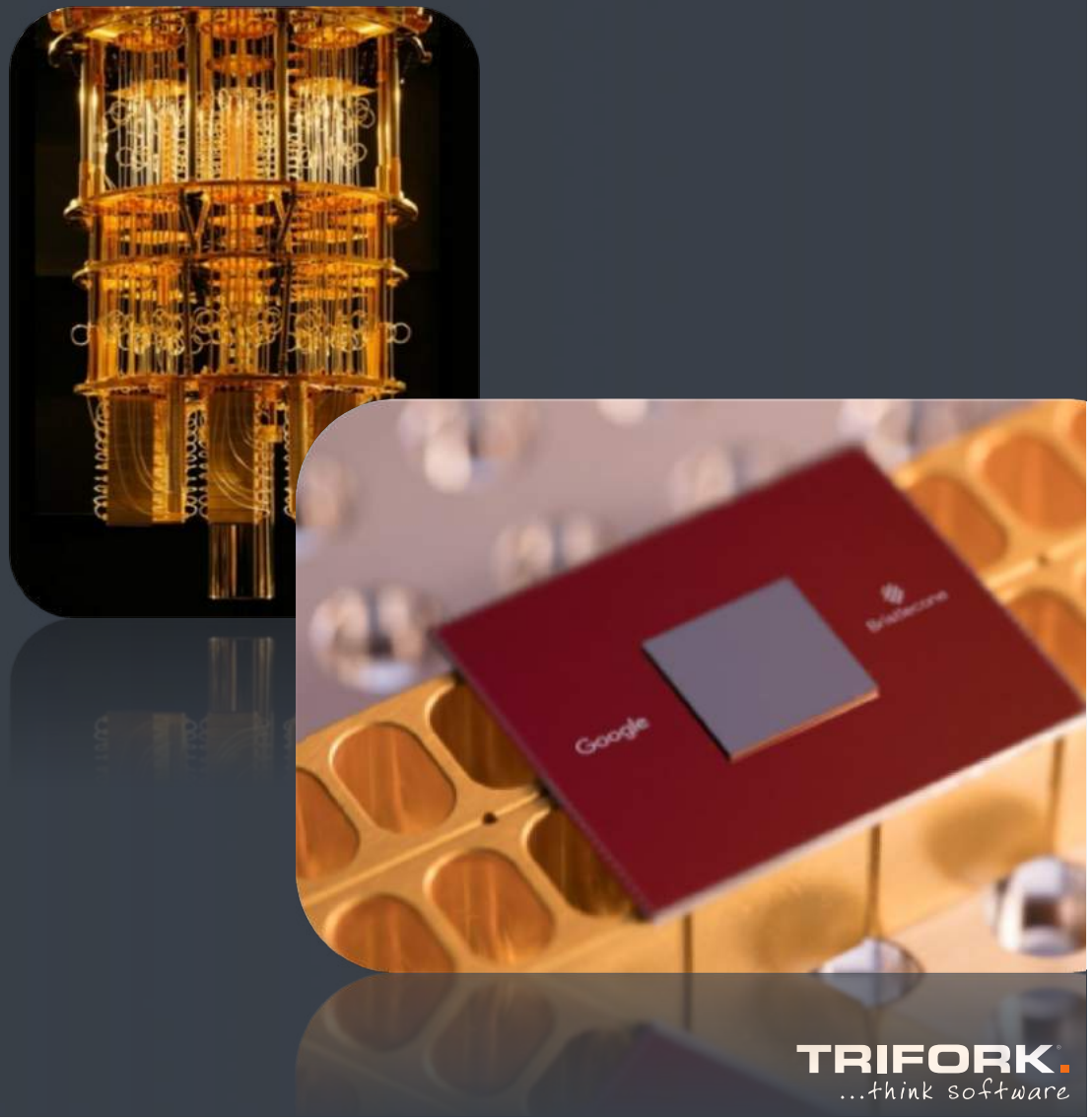
- What is a quantum computer ?
- What is the promise of quantum computers ?
- Do quantum computers have any use your industry ?

What quantum computing is not

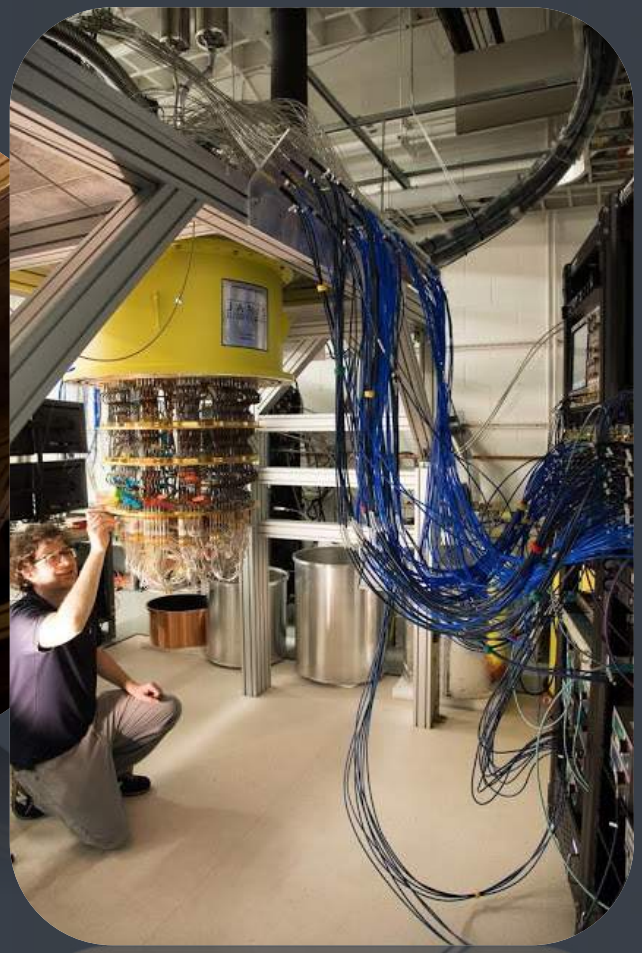
- A smaller and faster generation of classical computers
- A replacement of classical computers
- A magic bullet to solve all problems

A lot of hype, but...

- It is not science fiction
- Quantum computers are real today
- E.g. Googles Bristlecone 72 qubit chip



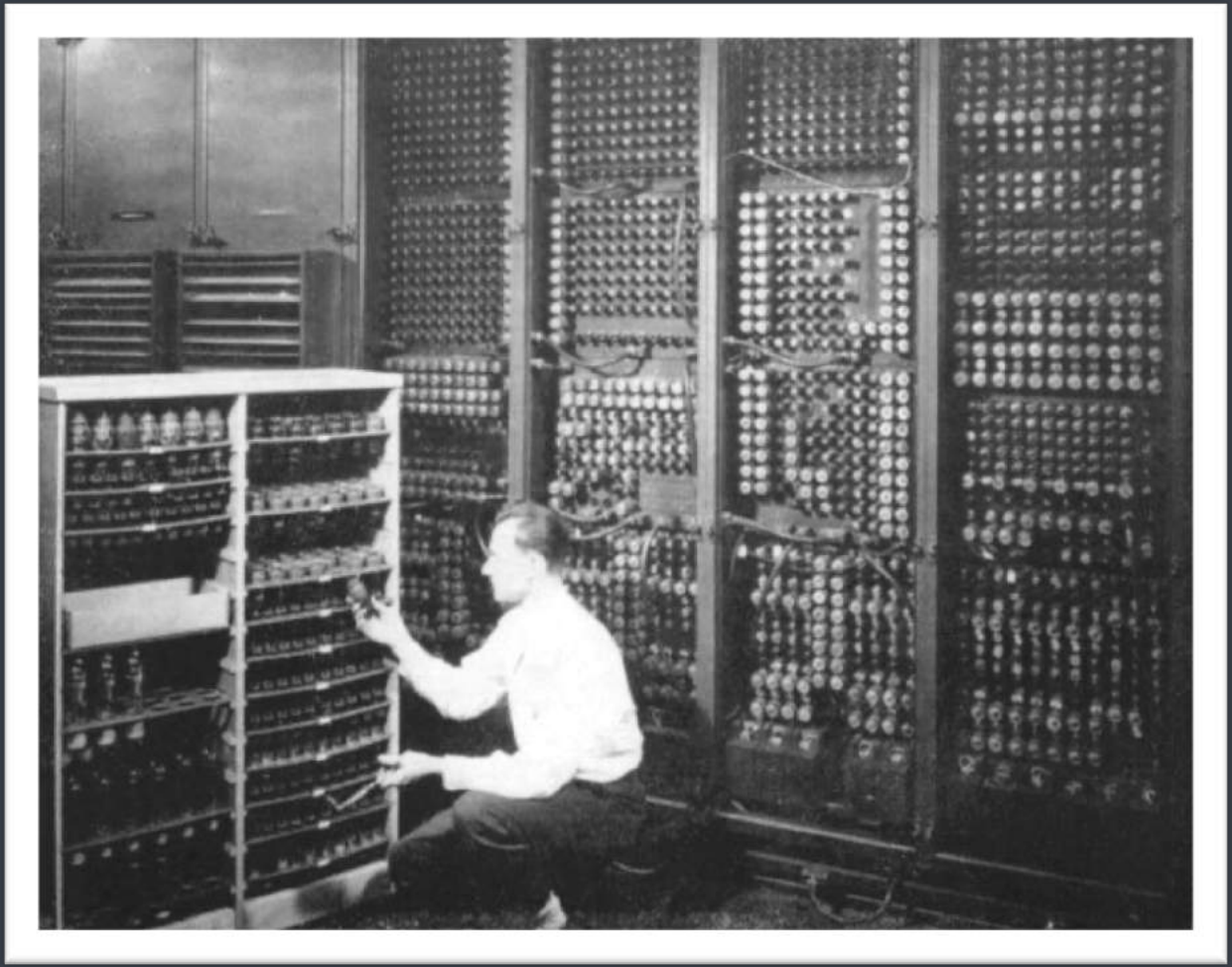
Source : Google



Source : Google

ENIAC ca. 1945

- 30 tons
- 20.000 vacuum tubes



Source : US Army

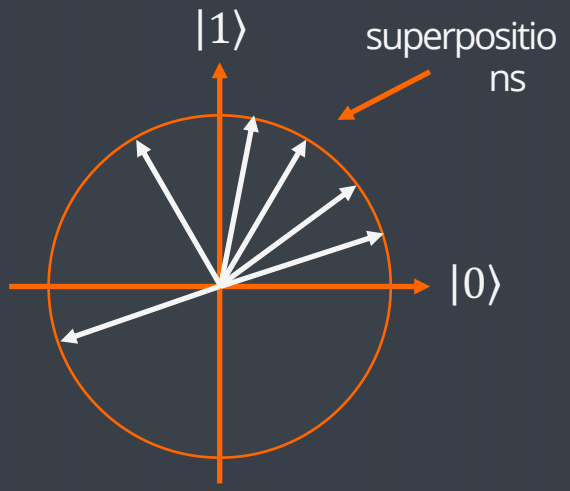
TRIFORK
...think software

How does a quantum computer work ?

By using quantum mechanical phenomenons to solve problems

Qubits and superposition

- A classic bit is either 0 or 1
- Qubits can also be in a ”superposition” of $|0\rangle$ and $|1\rangle$
- When you measure a qubit, it collapses to a classic state
- N qubits can be represented as vector in 2^N dimensional space



$$|01011\rangle$$

step 1

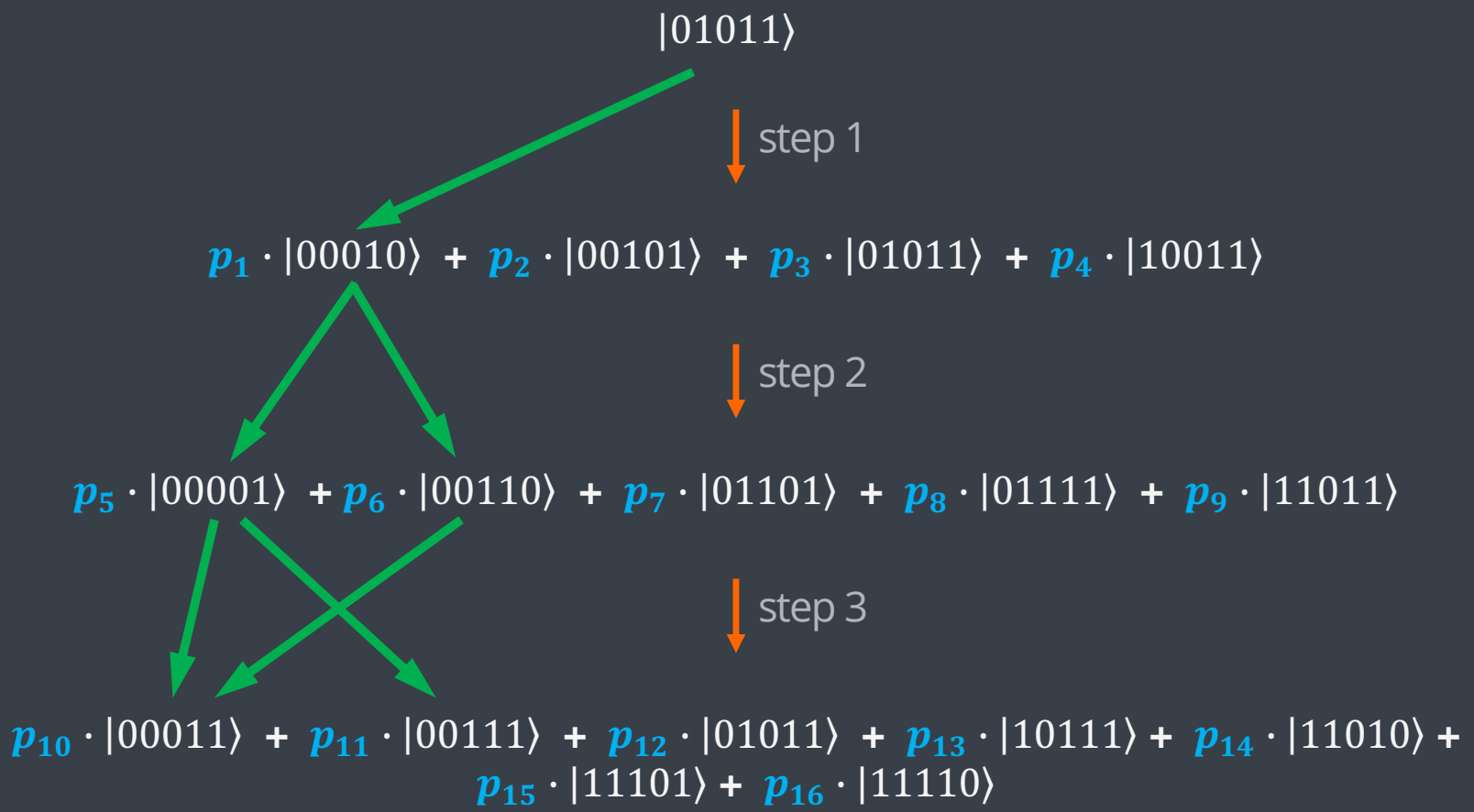
$$p_1 \cdot |00010\rangle + p_2 \cdot |00101\rangle + p_3 \cdot |01011\rangle + p_4 \cdot |10011\rangle$$

step 2

$$p_5 \cdot |00001\rangle + p_6 \cdot |00110\rangle + p_7 \cdot |01101\rangle + p_8 \cdot |01111\rangle + p_9 \cdot |11011\rangle$$

step 3

$$p_{10} \cdot |00011\rangle + p_{11} \cdot |00111\rangle + p_{12} \cdot |01011\rangle + p_{13} \cdot |10111\rangle + p_{14} \cdot |11010\rangle + p_{15} \cdot |11101\rangle + p_{16} \cdot |11110\rangle$$



Complexity – classes of difficulty

Complexity – or how ”hard” it is to solve a problem given a ”problem size”

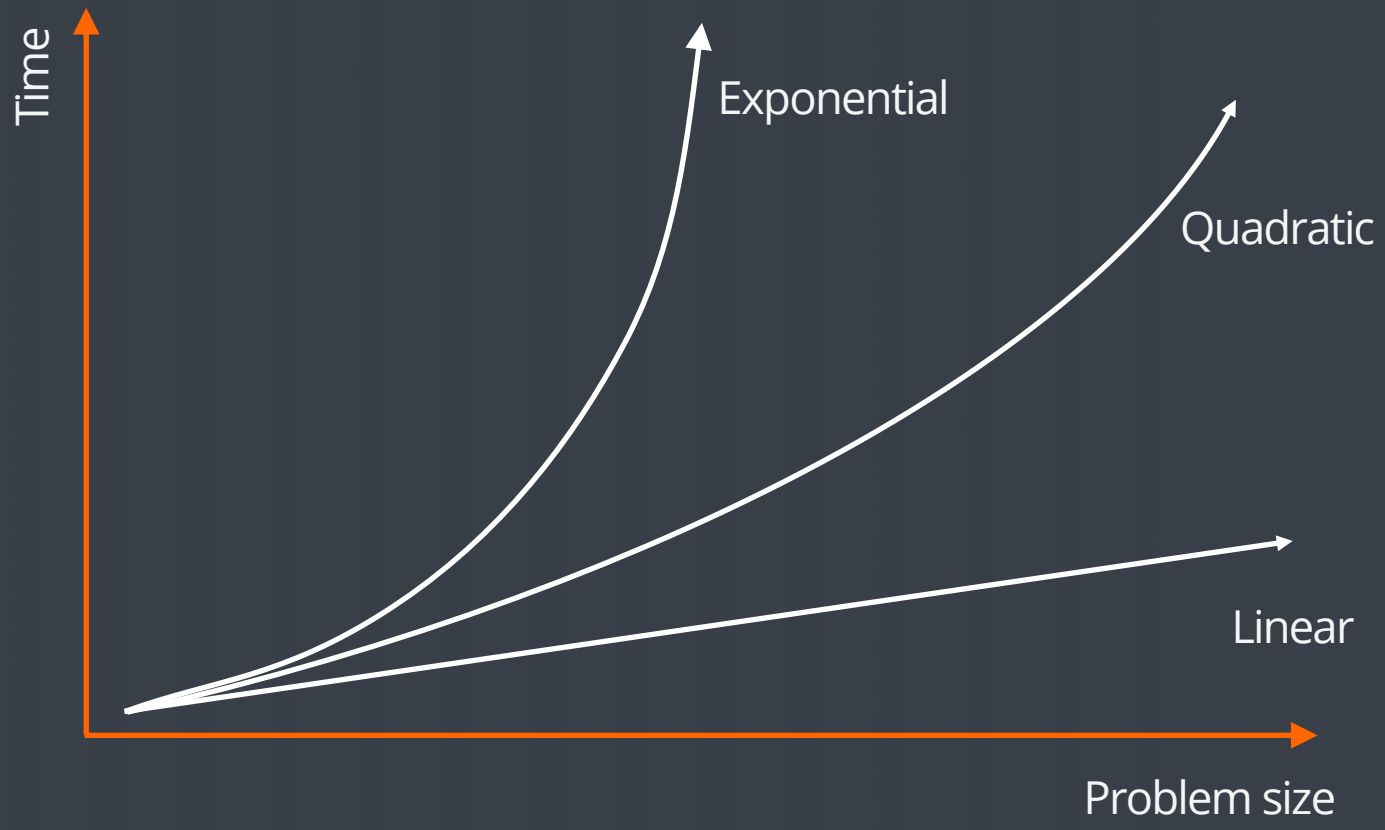
”Easy” problems

- Can be solved in polynomial time
  E.g. problem of size n, takes time n or n^2
- Sorting, searching, arithmetic

”Hard” problems

- Takes exponential time
  Problem size n takes 2^n

It’s a losing battle against exponentials



Assume a problem of size 1 takes 1 second to solve.

How long does it take to solve a problem of size 64 ?

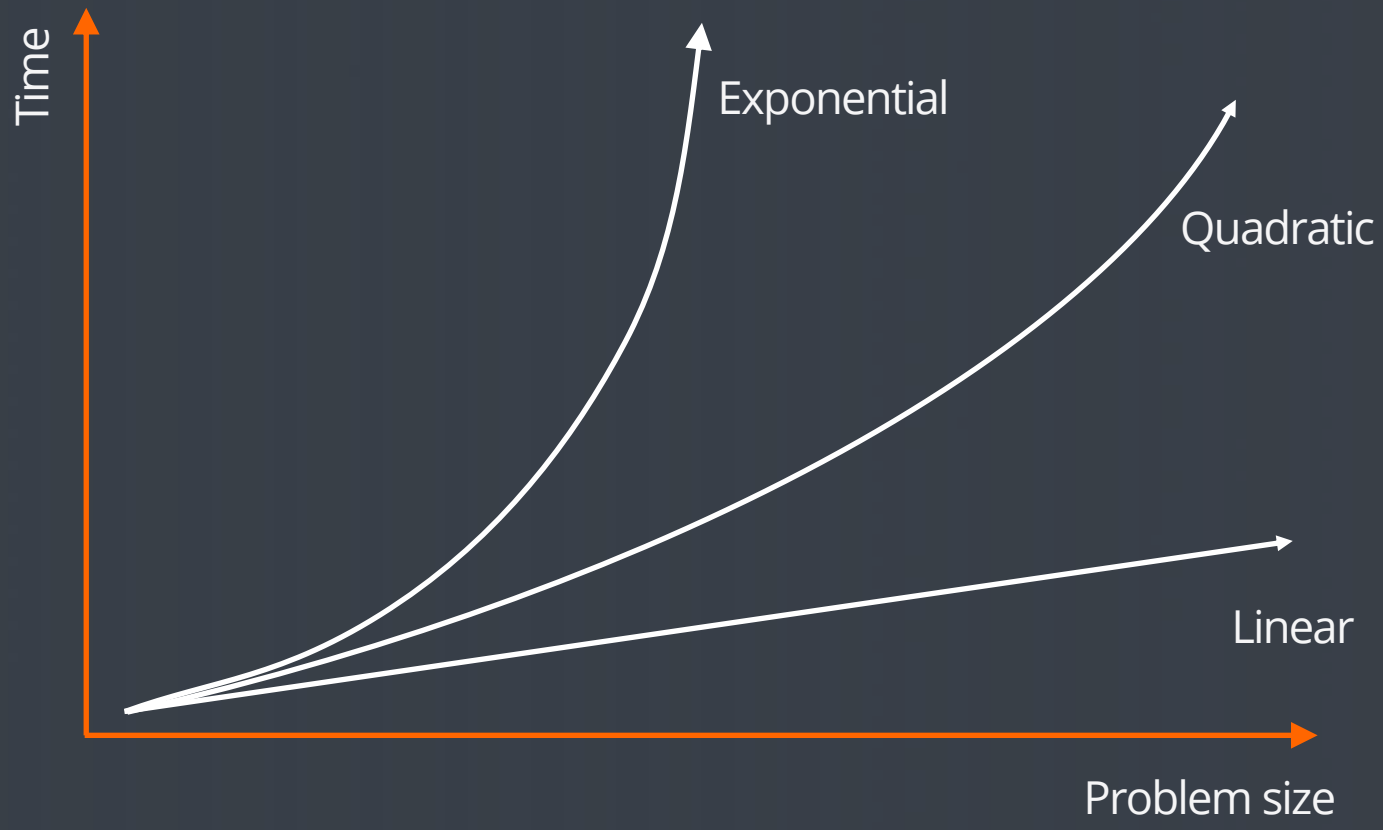
If linear complexity, 64 seconds.

If quadratic complexity, 1h 8m

If exponential complexity, 21 times the age of the universe.

TRIFORK.
...think software

It's a losing battle against exponentials



What about a new super-duper computer that's a billion-billion times faster !

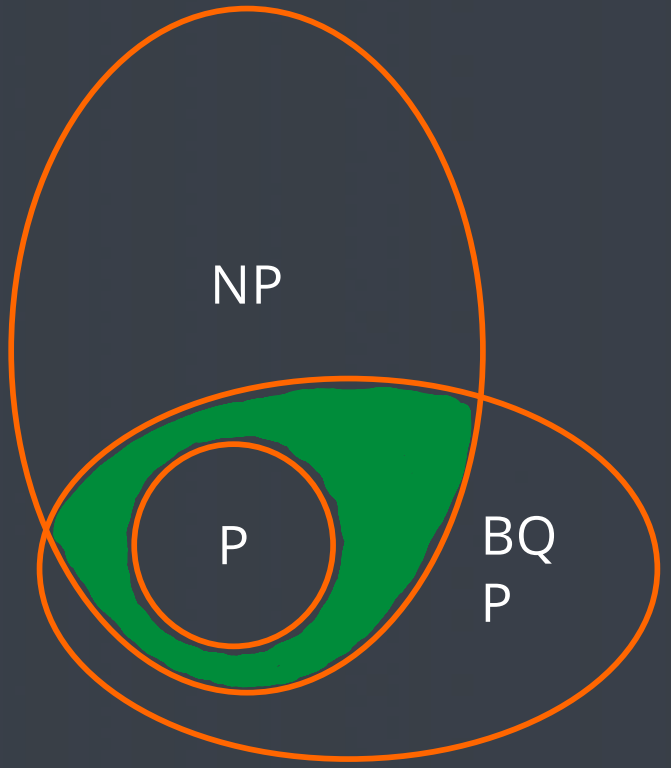
Now we can solve the problem with exponential complexity of size 64 in 9 seconds ☺

What if the problem size grows to 128 ?

396 times the age of the universe...

A little more formally

- P (polynomial time)
  - E.g. it takes n, n^2, n^3 to solve the problem of size n
- NP (Non deterministic polynomial time)
  - We can verify a solution in polynomial time
- BQP (Quantum polynomial time)
  - Polynomial time using a quantum computer



What can it be used for?

- Chemistry - simulating quantum mechanics
  - Pharmaceuticals - drug design
  - Material science (better solarcells, batteries etc)
  - Catalysts – e.g. for green energy development
- Break classic cryptography (Shor's algorithm)
  - Factoring goes from (sub)exponential to polynomial complexity
- Optimization problems - Quantum annealing
- Very secure communications (Quantum Key Distribution)

Quantum Annealing vs Universal Gate Quantum Computing

- Quantum Annealing
  - D-Wave
  - +2000 qubits
  - Optimization problems
- Universal Gate Quantum Computing
  - Everybody else (IBM, Google etc)
  - More general problems
  - E.g. Shor's algoritm
  - 72 qubits (Google's Bristlecone)
- Equivalent in theory by a polynomial fact

TRIFORK
...think software

What is the problem ?

Why can’t we build a quantum computer with 1 million qubits today ?

- Because of noise – decoherence

- Experts argue that error-correction is the biggest impediment to crossing the 100-qubit barrier for the universal gate model type of quantum computers. (Google, IBM, Microsoft)

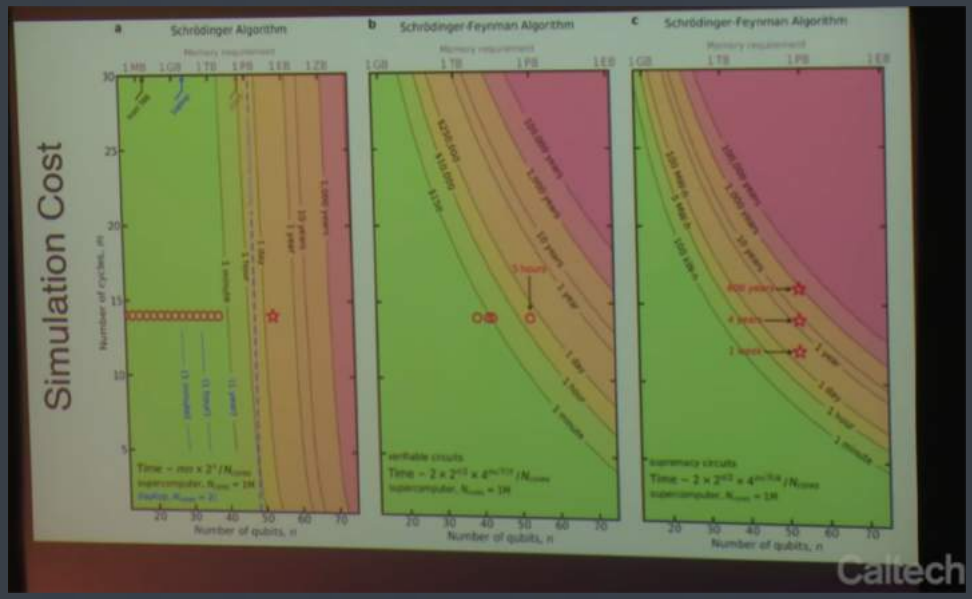
”Quantum supremacy”

- John Preskill, Caltech

Solve a problem with a quantum device that is not practically solveable with a classic computer

”Quantum supremacy”

Has been achived by Google – published October 23th 2019 !



Article

Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-1666-5

Received: 22 July 2019

Accepted: 20 September 2019

Published online: 23 October 2019

The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor. A fundamental challenge is to build a high-fidelity processor capable of running quantum algorithms in an exponentially large computational space. Here we report the use of a processor with programmable superconducting qubits to create quantum states on 53 qubits, corresponding to a computational state-space of dimension 2^{53} (about 10^{16}). Measurements from repeated experiments sample the resulting probability distribution, which we verify using classical simulations. Our Sycamore processor takes about 200 seconds to sample one instance of a quantum circuit a million times—our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years. This dramatic increase in speed compared to all known classical algorithms is an experimental realization of quantum supremacy for this specific computational task, heralding a much-anticipated computing paradigm.

https://www.nature.com/articles/s41586-019-1666-5

TRIFORK
...think software

IBM's "quantum advantage"

"We define QA as when we will have systems that are powerful enough, and, of course, programmable, that would allow us to solve problems that matter, right, something of relevance to your business or science that we couldn't do before. So my best estimate is that we're still years away."

Dario Gil, IBM Research Director, September 2019

Portfolio Optimization

- Better optimization result than with classical methods
- Faster for small problem sizes, but not so much for larger problem sizes. Overhead cancels out advantage.
- Next-gen D-Wave architecture with 5000 qubits expected to improve significantly
- Conclusion :

  ”Bearing all these considerations in mind, while it is not clear if quantum annealing is going to be the most compelling solver for portfolio optimization, our results indicate that as technology and theory progresses it could represent a viable choice”

USRA Research Institute for Advanced Computer Science and Standard Chartered Bank, London.

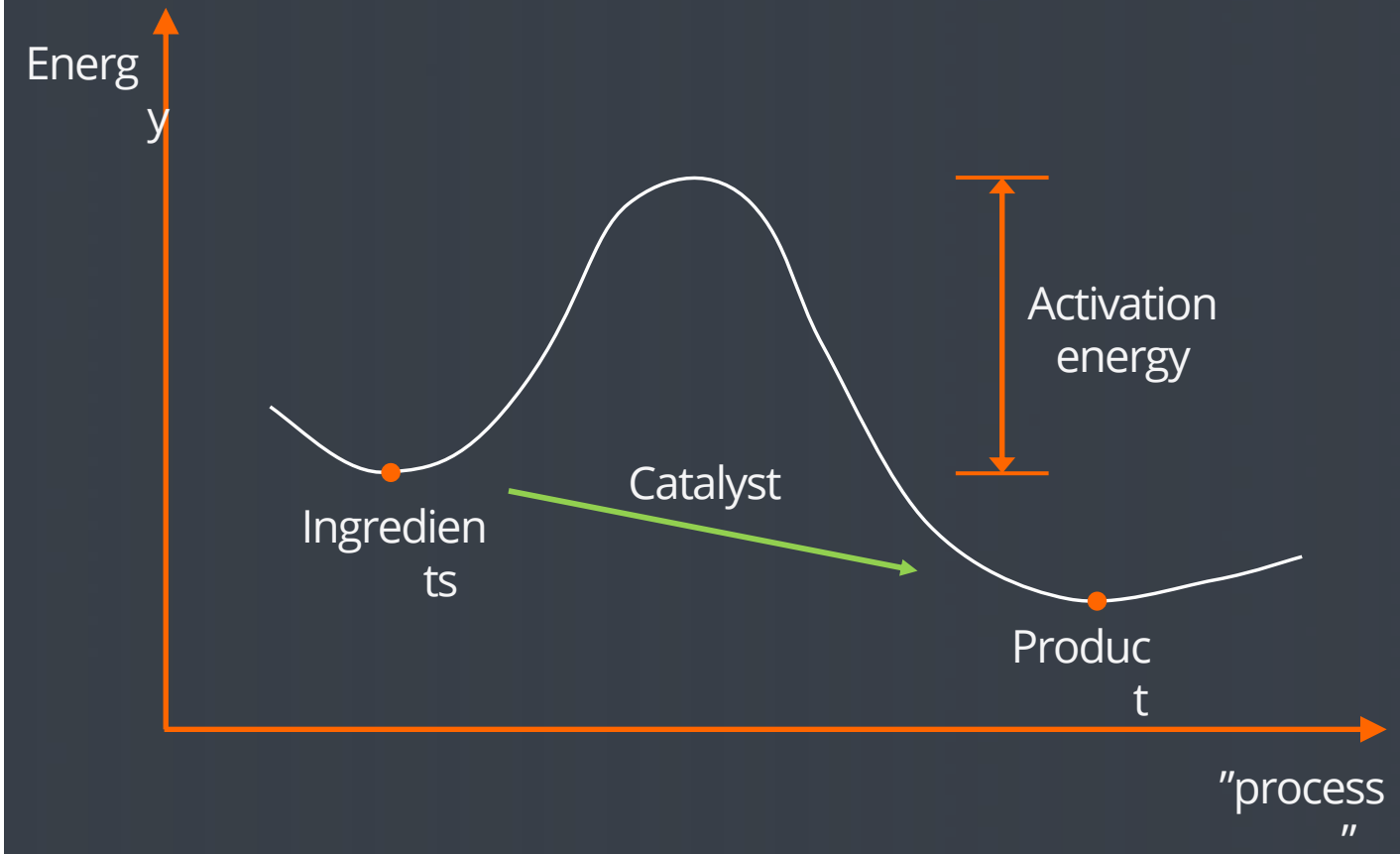
Ref. Venturelli, Davide, and Alexei Kondratyev. “Reverse Quantum Annealing Approach to Portfolio Optimization Problems.” Quantum Machine Intelligence 1.1-2 (2019): 17–30. Crossref. Web.

Nitrogen fixation – ammonia production

- Industrial production of ammonia requires high temperature and pressure.
- High energy consumption. Uses approx. 1% of global energy consumption.
- Causes approx. 1% of global CO_2 emissions

The Nitrogenase enzyme in nature produce ammonia at ambient temperatures and pressure.

Nitrogen fixation



The catalyst is the enzyme nitrogenase which lowers the energy level of the activation energy, but the process requires a very high activation energy industrially.

Summary

- Quantum computers create new opportunities to solve problems that are really hard for classical computers.
- As of today, no clear advantage yet of using quantum computers.
- You can start today to solve problems using real quantum computers available online, and prepare to take advantage of near-term quantum computers.
- Consider when is the time to switch (some of) your cryptography to post quantum cryptography

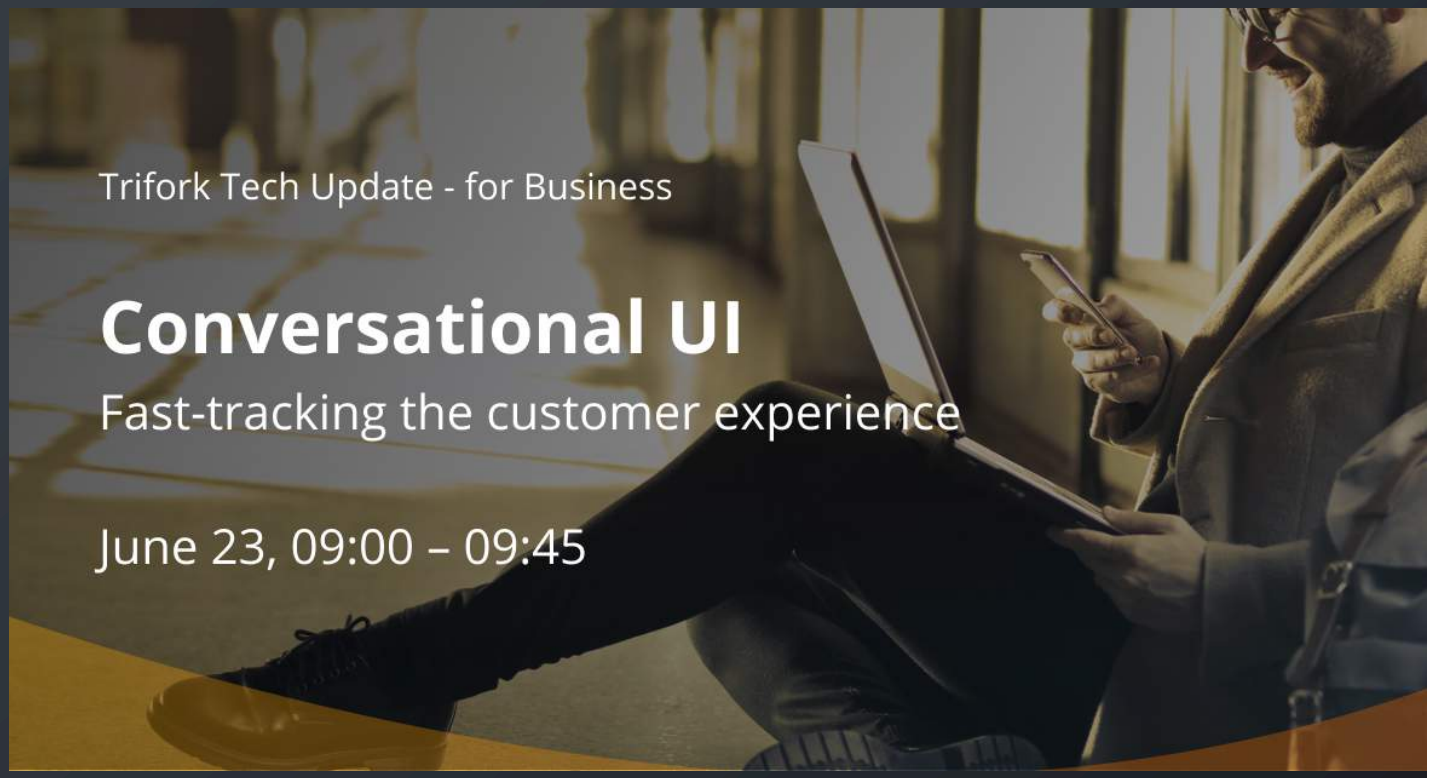
Thank you

Questions ?

Peter Flintholm
pfs@trifork.com

TRIFORK.
...think software

Thank you and see you next time!



TRIFORK
...think software