

QUANTUM COMPUTING AND MACHINE LEARNING

James Cruise and Julian van Velzen

August 2022



Agenda

1. Introduction to quantum computers

- Why should you care about quantum computers?
- What is quantum computing?
- How quantum computing is different from classical computing
- Where are we and where are we going

2. Overview of quantum algorithms

- Quantum circuits and circuit diagrams
- Variational quantum circuits and machine learning
- Un-structured search and Grover's algorithm
- Eigenvalues and quantum phase estimation



Introduction to quantum computers



Classical computing has changed our lives

- We hope this is not a controversial point!
- But, some problems are beyond the reach of any achievable classical compute
 - Chemical simulation
 - Resource allocation / path planning
 - Unstructured search
- Quantum computing shows great promise for some of these hard problems





Why should you care about quantum computing?

COMPUTING

How a quantum computer could break 2048-bit RSA encryption in 8 hours

A new study shows that quantum technology will catch up with today's encryption standards much sooner than expected. That should worry anybody who needs to store data securely for 25 years or so.

By Emerging Technology from the arXiv May 30, 2019

CNET | TECH

Featured Mobile Computing Gaming Home Entertainment Services & Software

Quantum computers could crack today's encrypted messages. That's a problem

The Telegraph

US blacklists quantum computing firms over national security fears

James Titcomb · 25/11/2021

Like 9

The White House has blacklisted eight Chinese quantum computing companies amid growing concerns that the technology will allow hackers to easily break into the West's most sensitive national security systems.

- Widely publicised concerns about the cryptographic consequences of quantum computers.
 - White House National Security Memorandum on quantum computing and cybersecurity
 - RSA, Diffie-Helman and related protocols are easily broken by large enough quantum computers.
 - Leading to a move to post-quantum cryptographic (PQC) schemes and quantum key distribution (QKD).
 - But is this all?



There are a wide range of use cases for quantum computers which will change the world

- NO, much broader use cases than just cryptography.
- Potential for polynomial or even exponential speed-ups on computational tasks.
- Making currently impossible tasks possible

Machine learning

- Natural language processing
- Quantum neural networks
- Search decoders

Quantum chemistry

- Drug design
- Material development
- In silico chemical simulation

Optimisation

- Logistics
- Resource allocation
- Scheduling

Simulation

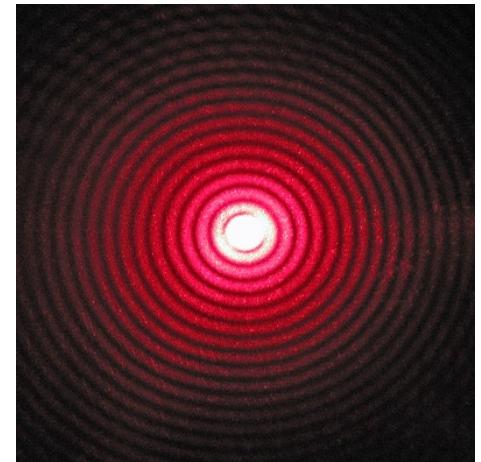
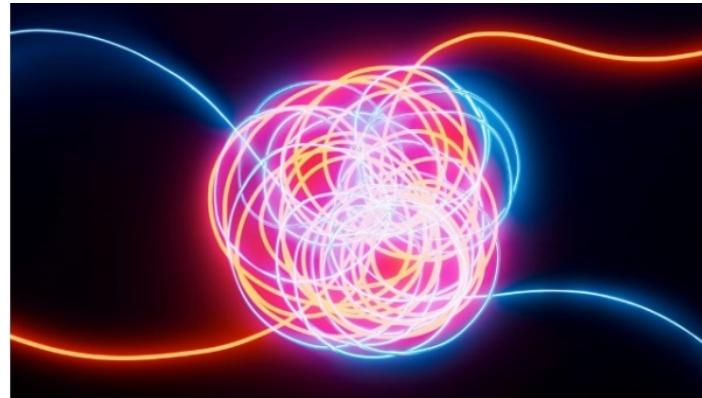
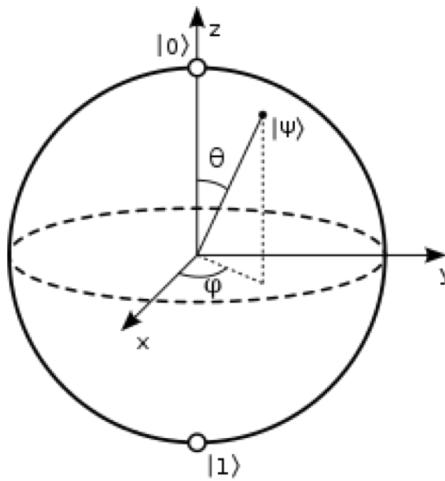
- Synthetic data generation
- Monte Carlo estimation

Potentially much more...

- Linear algebra
- Fluid dynamics
- Partial differential equations

What is quantum computing?

Computation built on Quantum Mechanics rather than Classical Mechanics.



Superposition

Entanglement

Interference

Computing with linear algebra instead of Boolean algebra



Models of computation

	Classical computation	Quantum computation
Register	N bits	N qubits
Data	Binary string length N $\{0,1\}^N$	Complex vector length 2^N , indexed by binary strings length N a_i for i in $\{0,1\}^N$ such that $\sum a_i^* a_i = 1$
Data manipulation	Map of binary string to binary string Boolean function	Linear map, preserving length Unitary matrix
Output	Binary string length N Data stored in the register	Binary string length N String i in $\{0,1\}^N$ with probability $a_i^* a_i$



Data manipulation revisited

Boolean functions

Map from binary strings to binary strings

Example:

I ₁	I ₂	O ₁	O ₂
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

Unitary matrix

Condition:

$$U^* U = I$$

Examples:

1 qubit (2 by 2 matrices)

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \quad \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

2 qubits (4 by 4 matrices)

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

For 3 qubits we have 8 by 8 matrices and for N qubits we have 2^N by 2^N matrices



Quantum computing is different to classical computing - Reversible

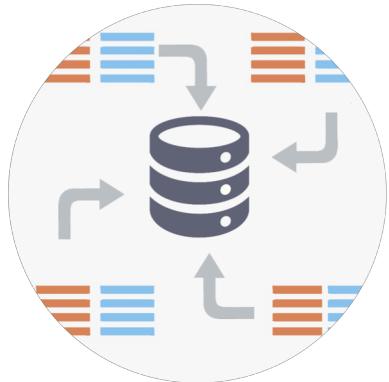
- An operation is reversible if given the outputs we can uniquely determine the inputs
 - As a consequence, no two inputs can generate the same output
- In classical computing, many computations are not reversible

I ₁	I ₂	O ₁	O ₂
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

- In quantum computing all computations are reversible apart from measurement
 - All unitary matrices are invertible
- All classical computations can be made reversible through the inclusion of extra registers



A different perspective is needed to get value from quantum computing



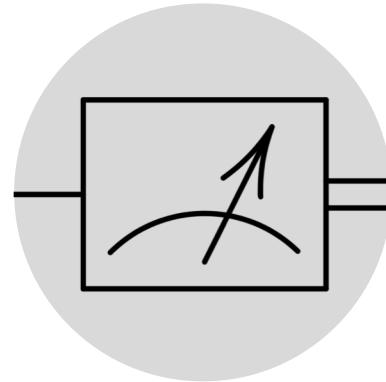
Data loading is a challenge

- Data needs to be repeatedly reload, it can not be copied
- Encoding data on qubits is hard, often requiring long circuits
- Quantum computers do not have memory



Computation is slow

- Underlying physical phenomenon are slow, 10ns to 1μs per gate
- Error correction overheads will significantly increase gate times
- Classical gates are complicated in implement quantumly



Accessing information is hard

- Only tool is measurement, which collapses superpositions
- Provides a single projection of a multidimensional object
- Obtaining an estimate of the full state requires many thousands of measurements



Quantum computing is different to classical computing – No cloning theorem

(Warning: 'Proof')

Achñ find U such that $U|\Psi\rangle \otimes |0\rangle = |\Psi\rangle \otimes |\Psi\rangle \quad \forall |\Psi\rangle$

where $U = \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{pmatrix}$

Let $|\Psi\rangle = \alpha_1|0\rangle + \alpha_2|1\rangle$

So $|\Psi\rangle \otimes |0\rangle = \alpha_1|100\rangle + \alpha_2|110\rangle$

and $|\Psi\rangle \otimes |\Psi\rangle = \alpha_1\alpha_1|100\rangle + \alpha_2\alpha_1|110\rangle + \alpha_1\alpha_2|101\rangle + \alpha_2\alpha_2|111\rangle$

C

$$U|4\rangle \otimes |0\rangle = \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} a\alpha_1 + b\alpha_2 \\ e\alpha_1 + f\alpha_2 \\ i\alpha_1 + j\alpha_2 \\ m\alpha_1 + n\alpha_2 \end{pmatrix}$$

$$= (\alpha_1 + b\alpha_2)|00\rangle + (e\alpha_1 + f\alpha_2)|10\rangle + (i\alpha_1 + j\alpha_2)|01\rangle + (m\alpha_1 + n\alpha_2)|11\rangle$$

$$|4\rangle \otimes |4\rangle = \alpha_1\alpha_1|00\rangle + \alpha_2\alpha_1|10\rangle + \alpha_1\alpha_2|01\rangle + \alpha_2\alpha_2|11\rangle$$

$$\alpha_1 + b\alpha_2 = \alpha_1^2$$

$$e\alpha_1 + f\alpha_2 = \alpha_1\alpha_2$$

$$i\alpha_1 + j\alpha_2 = \alpha_1\alpha_2$$

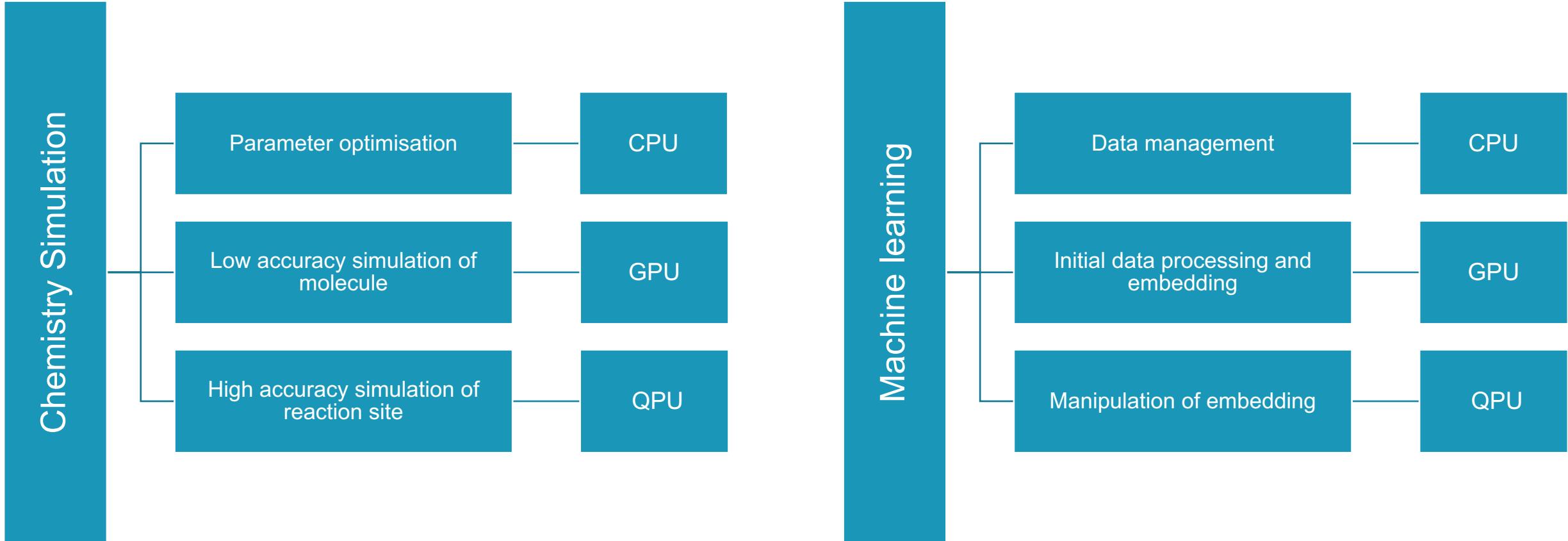
$$m\alpha_1 + n\alpha_2 = \alpha_2^2$$

$$\begin{aligned} a &= \alpha_1 & b &= 0 \\ e &= \alpha_2 & f &= 0 \\ i &= \alpha_2 & j &= 0 \\ m &= 0 & n &= \alpha_2 \end{aligned}$$

Depends on α_1, α_2 .
 No solution exists for all $|4\rangle$
 Need to know the state to copy it



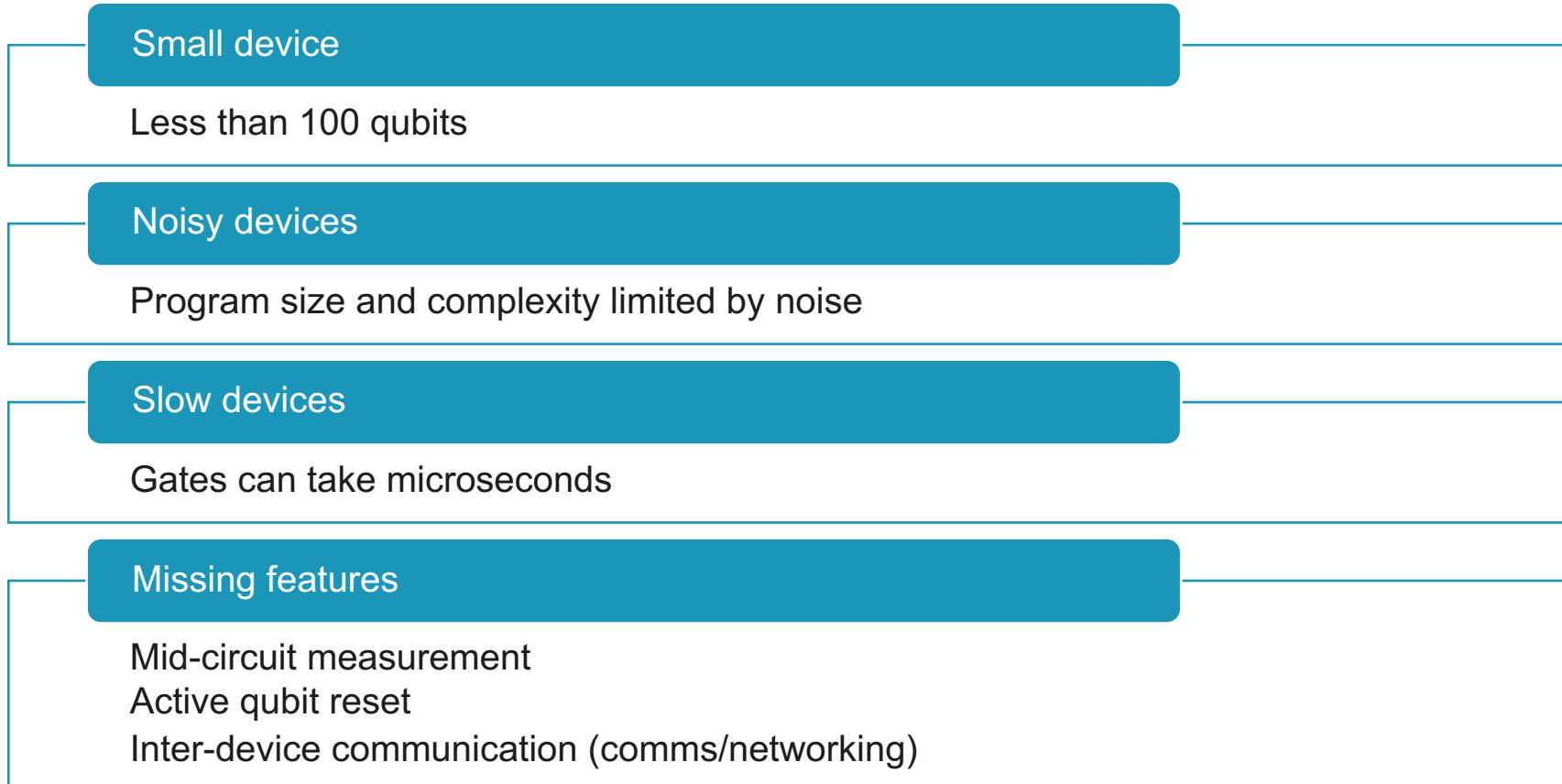
Allocating the correct computation to the correct device is the key to success



- Workflows are often complex with many parts with a mixture of suitability for quantum acceleration
- QPUs will be a part of larger heterogenous computers leading to hybrid workflows



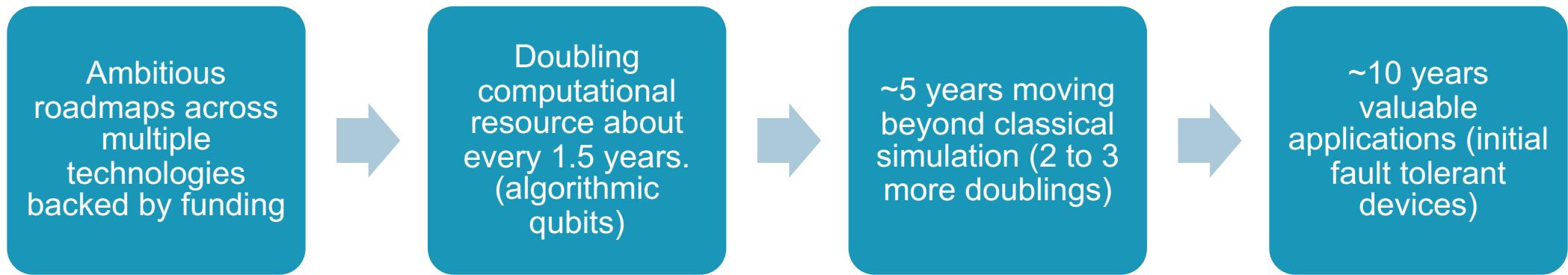
Current status of quantum computers



- Fundamentally experimental device on physicists benches



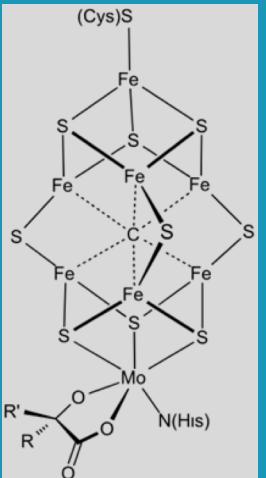
But rapid development and fast improvements



- Substantial engineering challenge but the physics is proven
 - Unexpected challenges along the way, e.g. cosmic rays



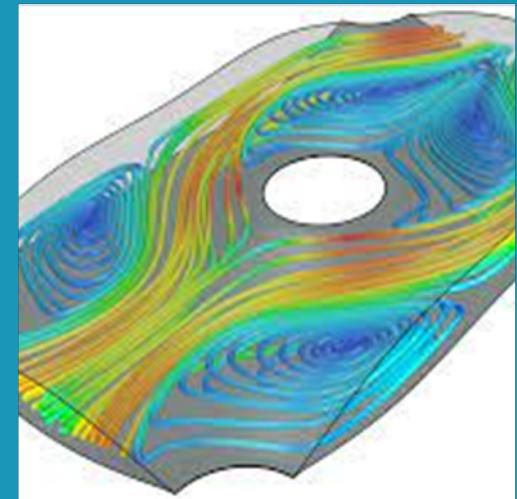
Quantum computers making impossible calculations possible



Drug and material design on computer



Faster simulation for financial services



Improved computational fluid dynamics



Many more yet to be discovered ...



Overview of quantum algorithms



Unstructured search & Grover

Example: phone book

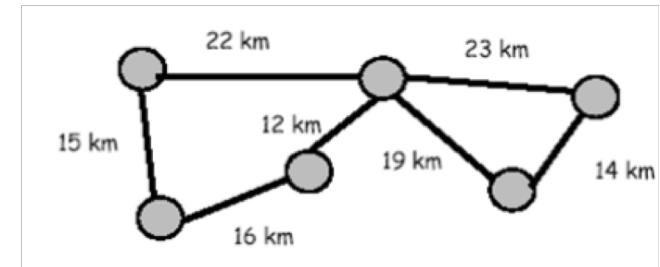
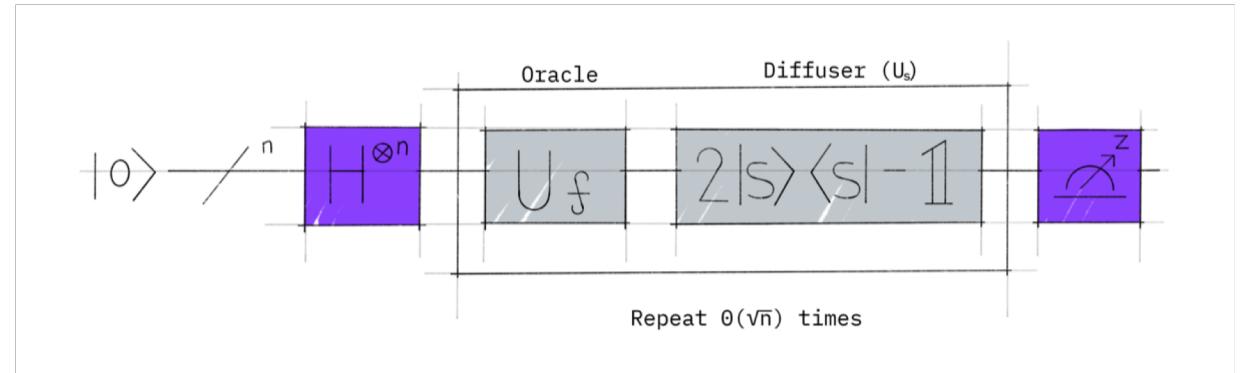
- Find the name of the person with phone number: 123456
- Takes an average of $N/2$ queries
- Grover search requires \sqrt{n} queries
- BUT: inputs scale linearly with size of the problem

Example: traveling salesman

- Hard to find solution, but easy to verify
- Scales $O(n!)$ brute force classically. For $n=20$, $\sim 10^{18}$ queries
- Scales $O(\sqrt{n}!)$ with Grover. For $n=20$, $\sim 10^9$ queries

Challenges

- Finding problems that justify quadratic speedup
- Beating the state-of-the-art classical solutions





Quantum Machine learning

Speeding up with HHL:
solves $Ax = b$ in logarithmic time

Strict conditions:

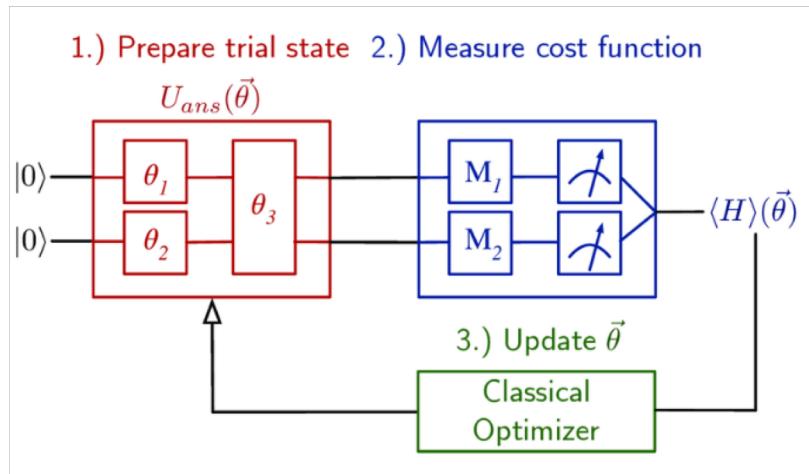
- Input vector b needs to be loaded efficiently
- A has to be sparse
- A has to be well-conditioned
- Getting the data out

Leveraging large space
faster learning with less data

- Better ‘expressibility’
- Variational algorithms like VQE/QAOA

Learning on quantum data

- Quantum native data
- Actual quantum data



Source: https://www.researchgate.net/figure/An-exemplar-VQE-circuit-with-two-qubits-and-an-ansatz-U-ans-th-parameterized-by-the_fig1_351828076



Quantum simulation

Task: estimate θ in $U |\psi\rangle = e^{2\pi i \theta} |\psi\rangle$

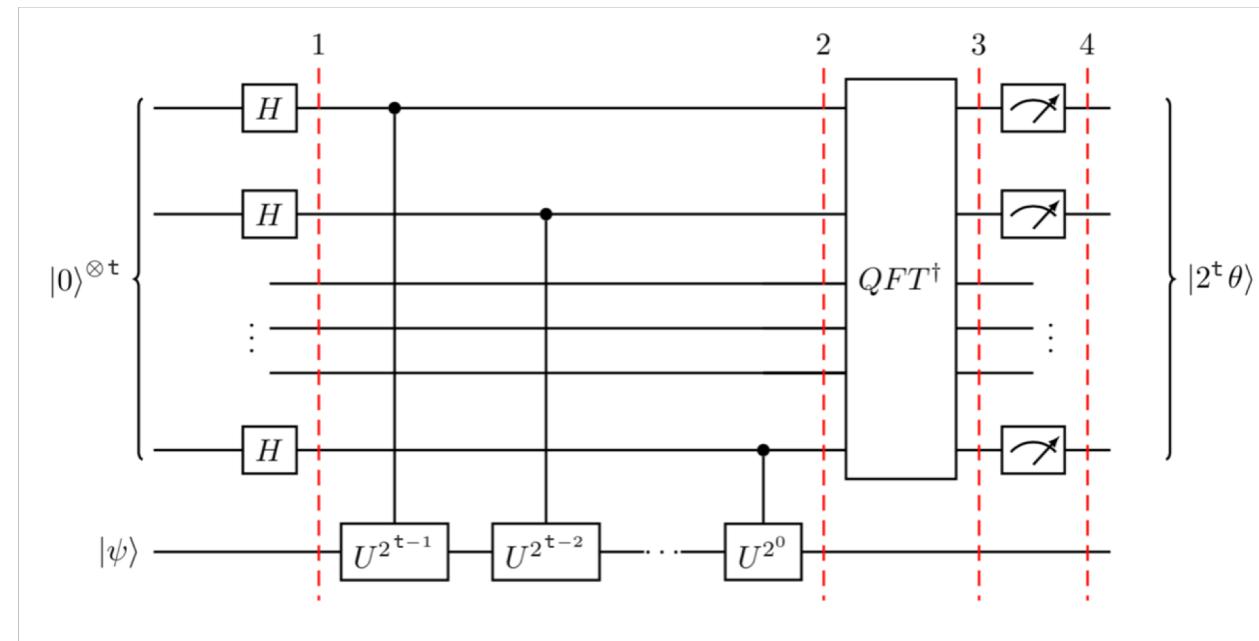
- Exponential speedup
- Complexity depends on size of molecule and basis set

Some potential use cases

- multi-reference quantum chemistry
- Vibrational problems
- Dynamics
- Correlated electronic structure

Research areas

- More efficient ways to describe chemistry
- More efficient algorithms
- Better use cases





Quantum Algorithms: Loads of potential, but not without challenges

Algorithm	Speedup	limitations	Challenge
Shor's algorithm	Exponential		<ul style="list-style-type: none">Massive cryptography migration
Linear algebra (HHL)	Exponential	Tricky implementation	<ul style="list-style-type: none">Finding applications that satisfy constraints
Search algorithms (Grover's, Quantum Monte Carlo, AE, AA)	Quadratic	Limited through overhead and clock speed	<ul style="list-style-type: none">Finding large enough problemsBeating heuristic state-of-the-art solutions
Variational algorithms (VQE, QAOA, QML)	Unknown	Many unknowns	<ul style="list-style-type: none">Proving speedup
Quantum simulation (QPE)	Exponential		<ul style="list-style-type: none">Finding first applications with large enough business case



cambridge
consultants

Part of Capgemini Invent

UK • USA • SINGAPORE • JAPAN
www.cambridgeconsultants.com

Cambridge Consultants is part of Capgemini Invent, the
innovation, consulting and transformation brand of the
Capgemini Group

© Cambridge Consultants 2022

The contents of this presentation are commercially confidential
and the proprietary information of Cambridge Consultants