cambridge consultants
Part of Capgemini Invent

Capgemini

# QUANTUM COMPUTING AND MACHINE LEARNING

James Cruise and Julian van Velzen

August 2022

# Agenda

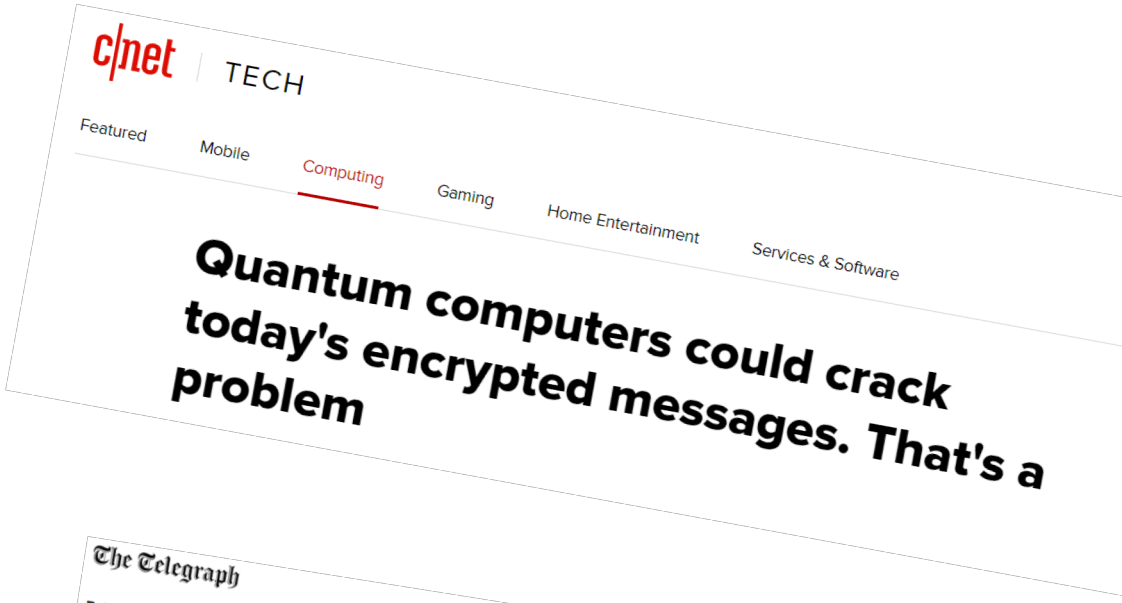
1. **Introduction to quantum computers**
   - Why should you care about quantum computers?
   - What is quantum computing?
   - How quantum computing is different from classical computing
   - Where are we and where are we going
2. **Overview of quantum algorithms**
   - Quantum circuits and circuit diagrams
   - Variational quantum circuits and machine learning
   - Un-structed search and Grover's algorithm
   - Eigenvalues and quantum phase estimation
3. **Quantum Monte Carlo estimation**
   - Extension of Grover's algorithm to amplitude estimation
   - Application to Monte Carlo estimation
   - Quadratic speed up
   - Examples

# 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?

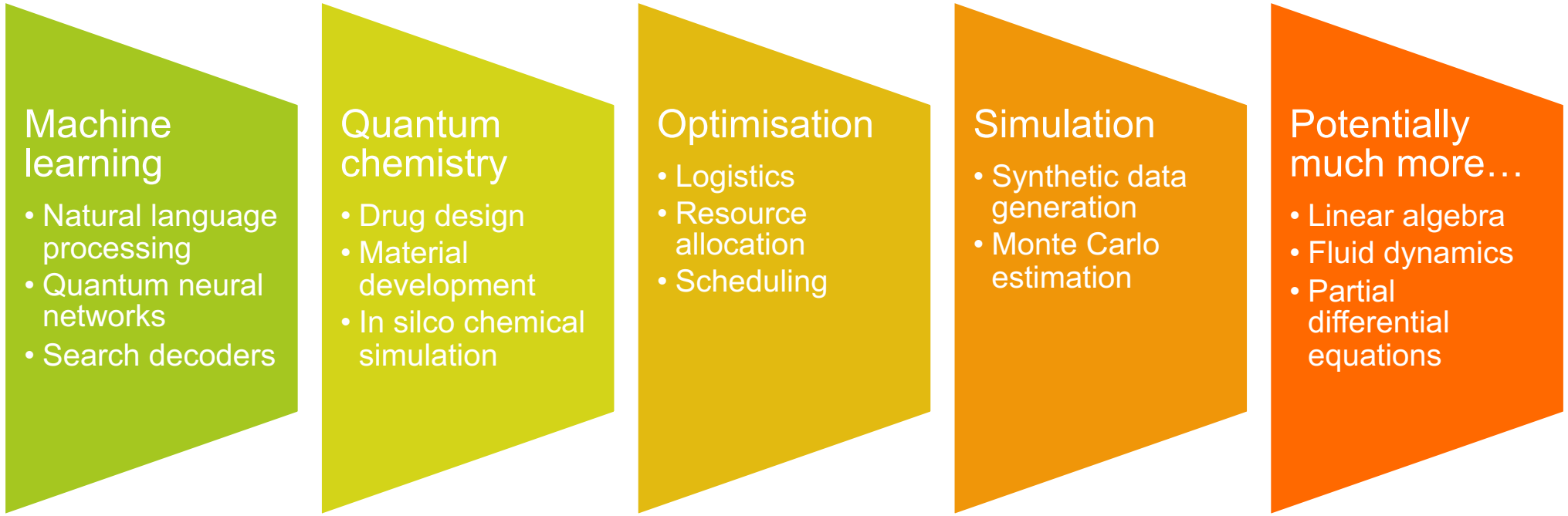





- Widely publicised concerns about the cryptographic consequences of quantum computers.
  - White House National Security Memorandum on quantum computing and cybersecurity
- RSA, Diffie-Helman and related protocols are easily broken by large enough quantum computers.
- Leading to a move to post-quantum 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

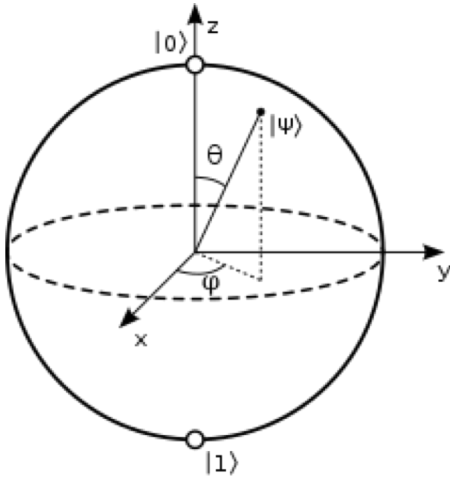
- NO, much broader use cases than just cryptography.
- Potential for polynomial or even exponential speed-ups on computational tasks.
- Making currently impossible tasks possible



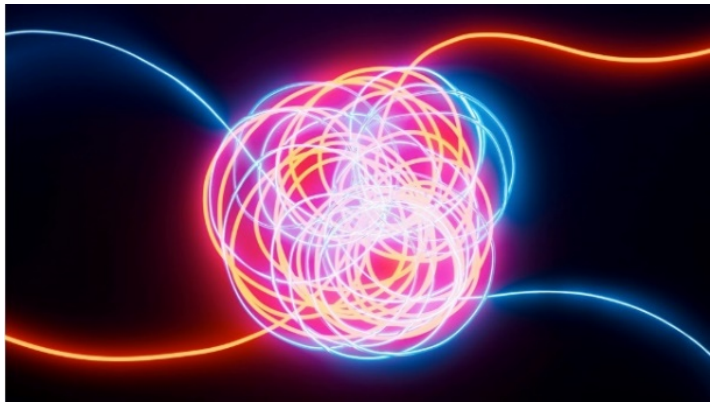
Cambridge Consultants
Part of Capgemini Invent

# What is quantum computing?

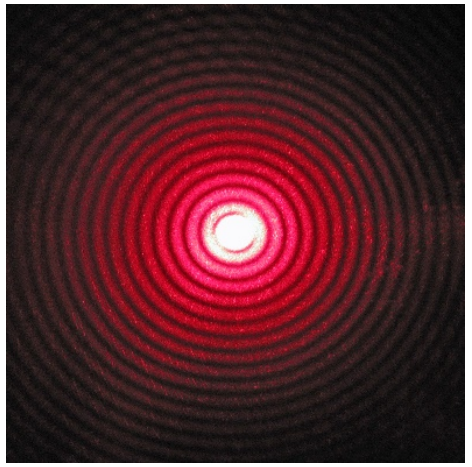
Computation built on Quantum Mechanics rather than Classical Mechanics.




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<br><br>$\{0,1\}^N$ | Complex vector length $2^N$, indexed by binary strings length N<br><br>$a_i$ for $i$ in $\{0,1\}^N$ such that $\sum a_i^* a_i = 1$ |
| Data manipulation | Map of binary string to binary string<br><br>Boolean function | Linear map, preserving length<br><br>Unitary matrix |
| Output | Binary string length N<br><br>Data stored in the register | Binary string length N<br><br>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

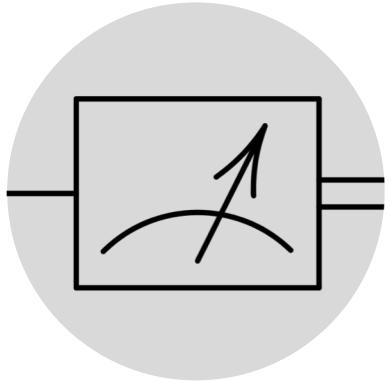
# A different perspective is needed to get value from quantum computing

## 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')

Assume 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 $|\psi\rangle \otimes |0\rangle = \alpha_1 |00\rangle + \alpha_2 |10\rangle$

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

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

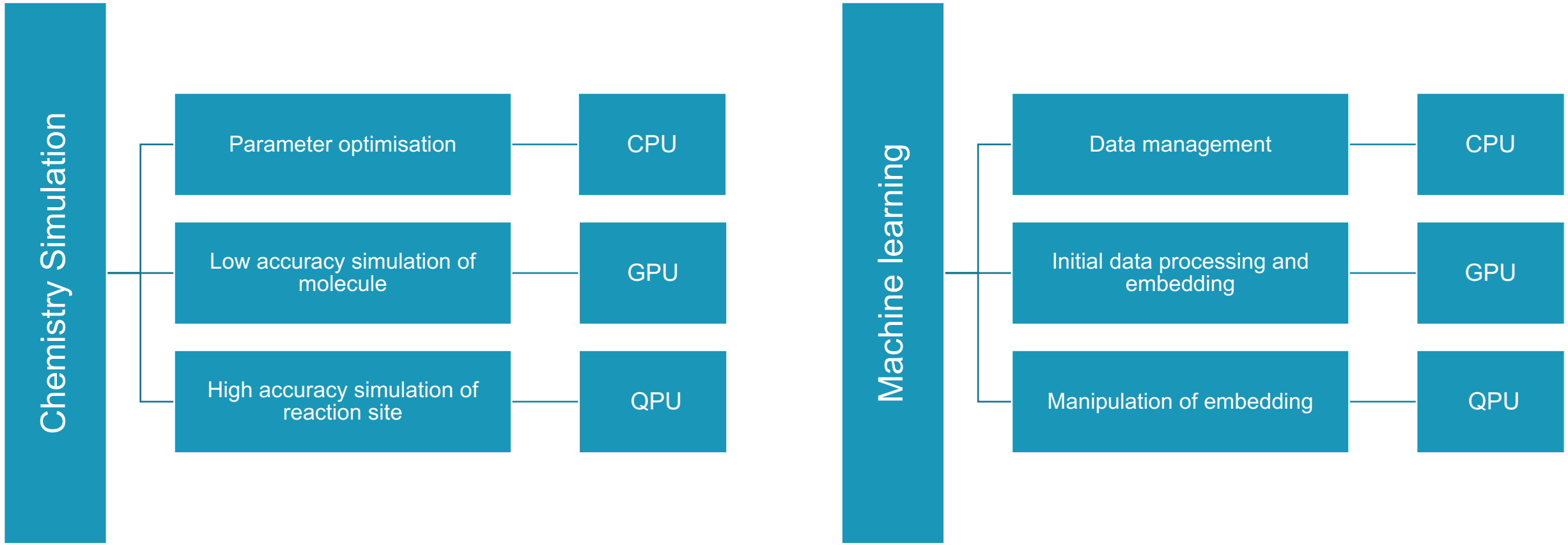
$$= (a\alpha_1 + b\alpha_2)|00\rangle + (e\alpha_1 + f\alpha_2)|10\rangle + (i\alpha_1 + j\alpha_2)|01\rangle + (m\alpha_1 + n\alpha_2)|11\rangle$$

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

$$\begin{aligned} a\alpha_1 + b\alpha_2 &= \alpha_1^2 \\ e\alpha_1 + f\alpha_2 &= \alpha_1\alpha_2 \\ i\alpha_1 + j\alpha_2 &= \alpha_1\alpha_2 \\ m\alpha_1 + n\alpha_2 &= \alpha_2^2 \end{aligned} \longrightarrow \begin{aligned} a &= \alpha_1 \quad b = 0 \\ e &= \alpha_2 \quad f = 0 \\ i &= \alpha_2 \quad j = 0 \\ m &= 0 \quad n = \alpha_2 \end{aligned}$$

Depends on $\alpha_1$ & $\alpha_2$.
No solution exists for all $|\psi\rangle$
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

**Small device**

Less than 100 qubits

**Noisy devices**

Program size and complexity limited by noise

**Slow devices**

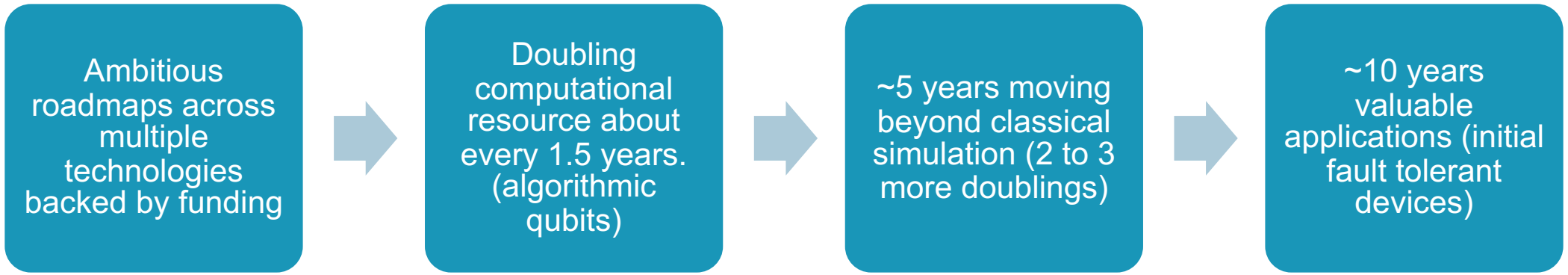
Gates can take microseconds

**Missing features**

Mid-circuit measurement
Active qubit reset
Inter-device communication (comms/networking)

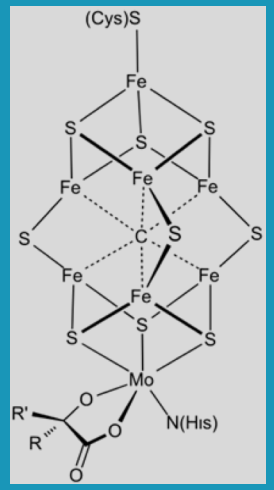
- Fundamentally experimental device on physicists benches

## But rapid development and fast improvements



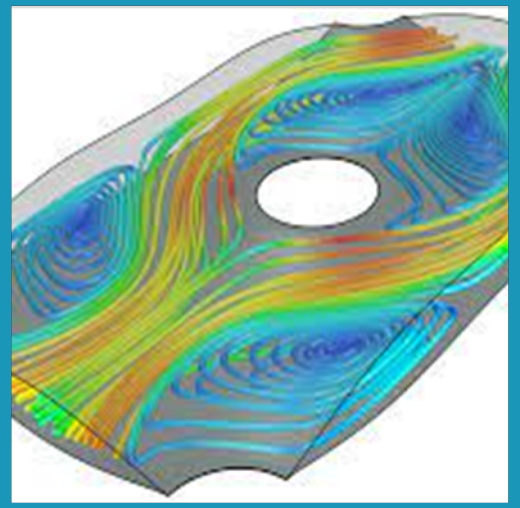

- Substantial engineering challenge but the physics is proven
  - Unexpected challenges along the way, e.g. cosmic rays

# Quantum computers making impossible calculations possible




Drug and material design on computer

Faster simulation for financial services

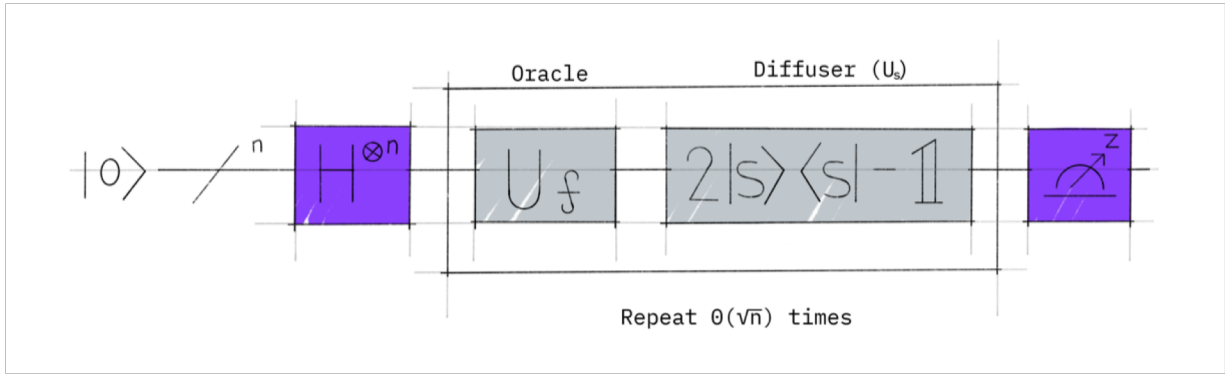


Improved computational fluid dynamics


Many more yet to be discovered …

# Overview of quantum algorithms

# Unstructered search & Grover

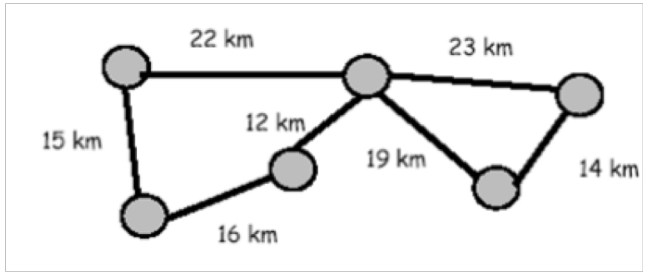



Example: phone book

- Find the name of the person with phone number: 123456
- Takes an average of N/2 queries
- Grover search requries $\sqrt{n}$ 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:

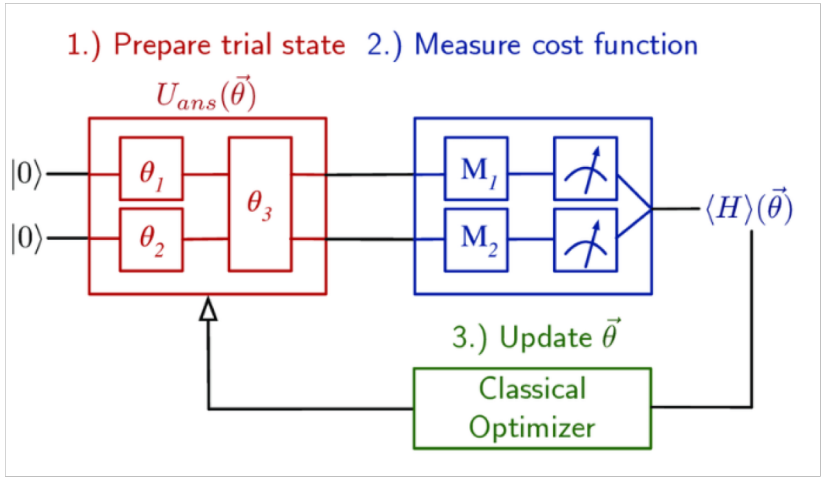
- Input vector b needs to be loaded efficiently
- A has to be sparse
- A has to be well-conditioned
- Getting the data out

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

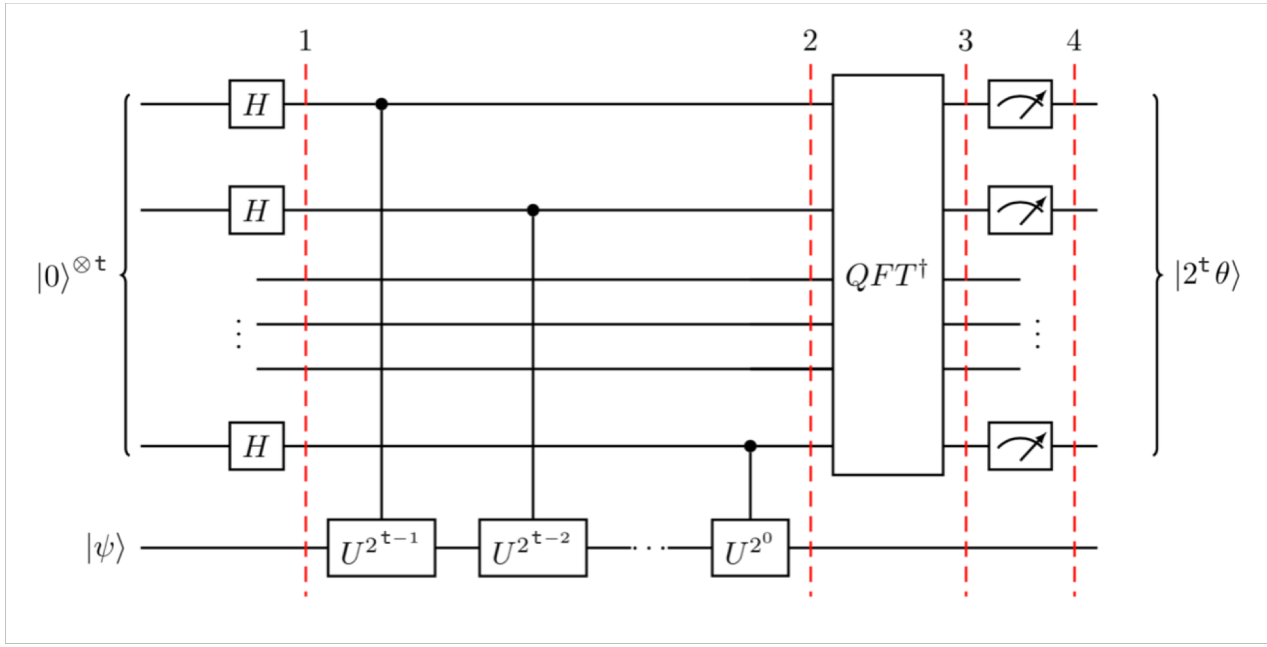
## Quantum simulation

Task: estimate $\theta$ 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 | | • Massive cryptography migration |
| Linear algebra (HHL) | Exponential | Tricky implementation | • Finding applications that satisfy constraints |
| Search algorithms (Grover's, Quantum Monte Carlo, AE, AA) | Quadratic | Limited through overhead and clock speed | • Finding large enough problems<br>• Beating heuristic state-of-the-art solutions |
| Variational algorithms (VQE, QAOA, QML) | Unknown | Many unknowns | • Proving speedup |
| Quantum simulation (QPE) | Exponential | | • Finding first applications with large enough business case |

# Quantum Monte Carlo estimation

## Monte Carlo estimation/integration

- Interested in the problem of estimating the expected value of function of a random variable
- Relevant in a wide range industries including finance
  - Option pricing
  - Premium setting
  - Risk measures, for example CVaR
  - Many more
- Discrete random variable X with probability mass function p, and bounded function f

$$\mathbb{E}\big(f(X)\big) = \sum p(x) f(x)$$

- We can approximate using random samples, $X_1, X_2, \ldots, X_N$ by

$$\mathbb{E}\big(f(X)\big) \approx \frac{1}{N} \sum_{i=1}^{N} f(X_i)$$

- To obtain accuracy $\epsilon$ we require order $1/\epsilon^2$ samples/work

## How can we approach this problem with quantum computers?

- Assume we have two special quantum circuits *P* and *R*
  - *P* loads the probability distribution

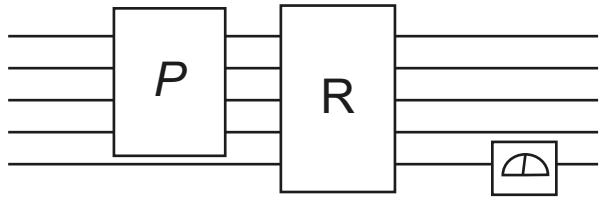
$$\mathcal{P}\left|0>=\sum\sqrt{p(x)}\right|x>$$

  - *R* loads the function of interest

$$\mathcal{R}|x>|0>=|x>(\sqrt{f(x)}\left|1>+\sqrt{1-f(x)}\right|0>)$$

  - Putting these together we have

$$\mathcal{RP}|0>=\sum_x\left((\sqrt{p(x)f(x)}|x>|1>+\sqrt{p(x)\big(1-f(x)\big)}|x>|0>)\right)$$




- Quantity of interest encoded into amplitude of known states
- Probability of measuring a |1> on the last qubit is $p(x)f(x)$, so the proportion of 1 measurements provides an estimate of the expectation of interest.

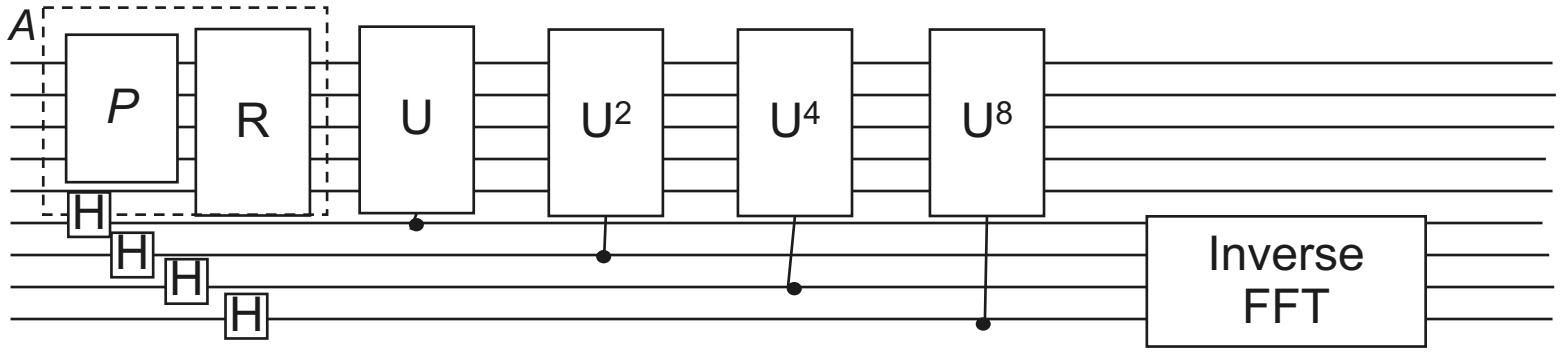
## Amplitude estimation

**Problem:**

- Given an oracle that produces a state $\sqrt{a}\,|\Psi_{good}> + \sqrt{1-a}|\Psi_{bad}>$ estimate $a$

**Solution**

- Use Grover rotation with inverse Fourier transform




- Each controlled unitary contains 2 copies of A, the oracle
- To reach accuracy $\epsilon$ we need $-\log(\epsilon)$ controlled unitaries, so the total oracle calls needed is order $1/\epsilon$.
- **Quadratic speedup**

# Derivative pricing

**What is it**:
- Derivatives are financial products (like options) based on stochastic models

**Market outlook:**
- Giant market of $1 quadrillion dollars on the high end -> 10 times world total GDP

**Why quantum:**
- Complex derivatives can not be simulated analytically, and classical approximations have limitations.

**Business value:**
- new products tailored to clients need (like customisable pay-offs)
- Improved return on equity (lower need for reserves)

**Challenge** → finding quantum advantage

- To complex for classical solvers
  - Path-dependent
  - Correlation-dependent
  - Time-dependent
  - Mix of those
- Doable with quantum computers
  - Efficient loading of data
  - Efficient formulation of payoff functions
  - Efficient algorithms
- Relevant case
  - Is there a business case?

# Risk Management

**What is it**:

- (Conditional) Value-at-risk simulations of credit, operational or other financial risk

**Market outlook:**

- Risk management is crucial for (re) insurance, banking, and many other industries

**Why quantum:**

- Need for faster, more complex models
- Rare events can have big impact

**Business value:**

- Compliance
- Improved return on equity (lower need for reserves)
- Better inputs to the risk strategy

**Challenge** → finding quantum advantage

- To complex for classical solvers
  - Complex risk measures (CVaR)
  - Tail risk
  - Risk interdependence
  - Frequency & accuracy
- Doable with quantum computers
  - Efficient loading of data
  - Efficient formulation of risk model
  - Efficient algorithms
- Relevant case
  - Is there a business case?


UK ▪ USA ▪ SINGAPORE ▪ JAPAN

www.cambridgeconsultants.com

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