Quantum Computing

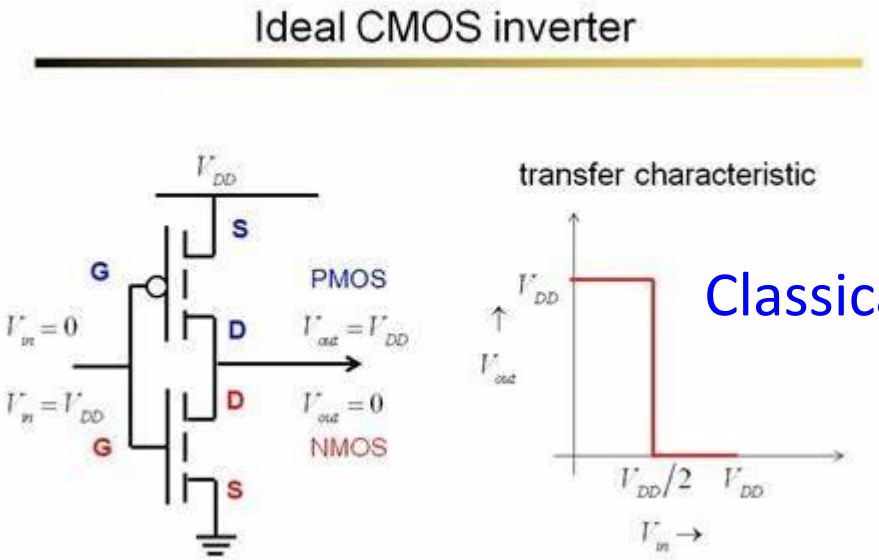
How a Quantum Computer is different?

It is based upon using

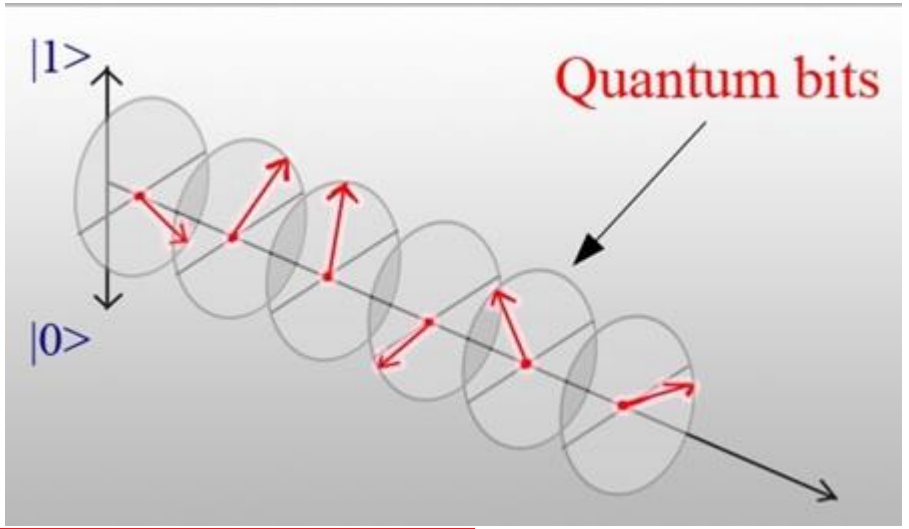
- Qubits
- Superposition/interference
- Entanglement

Superposed state is expressed as:

$|\psi\rangle = a|0\rangle + b|1\rangle$



Classical bits



Classical v/s. Quantum Computers

Classical Computer	Quantum Computer
Uses semiconductor-based CMOS logic gates	May use atomic, electronic, nuclear or photonic properties
ON/OFF state of CMOS transistor determines logic 1/0	Logic 1/0 represented by spin up/down, ground state/excited state, right polarization/left polarization etc.
Bit can be in state 1 or 0 at a given time	Bit (qubit) can be in both 1 and 0 states at a given time
Machine executes operations bit by bit	Machine executes operation on all bits simultaneously*

* This concept is different than parallel computing

Advantage of a Quantum Computer

A classical computer

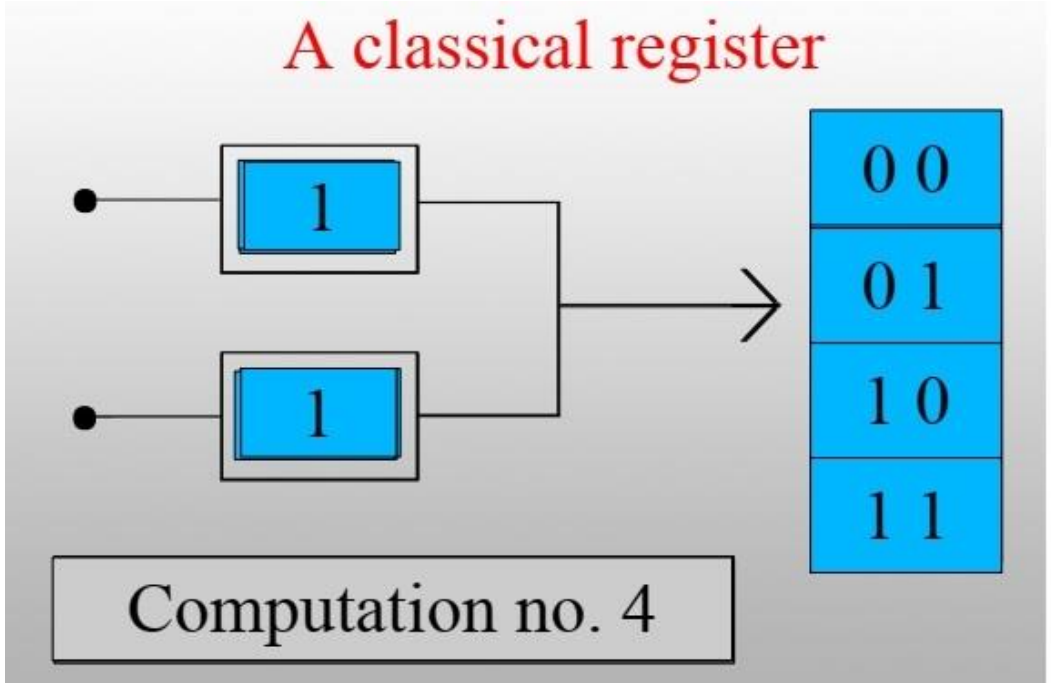
- Each register has unique input

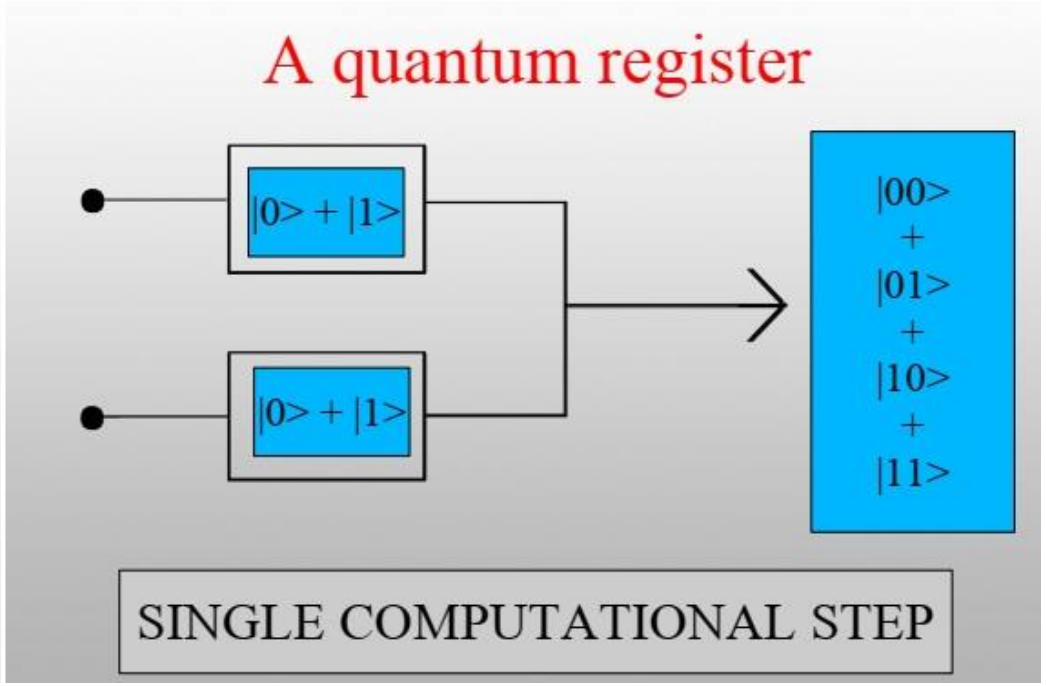
  Executes one operation at a time

A quantum computer

- Each register has both inputs

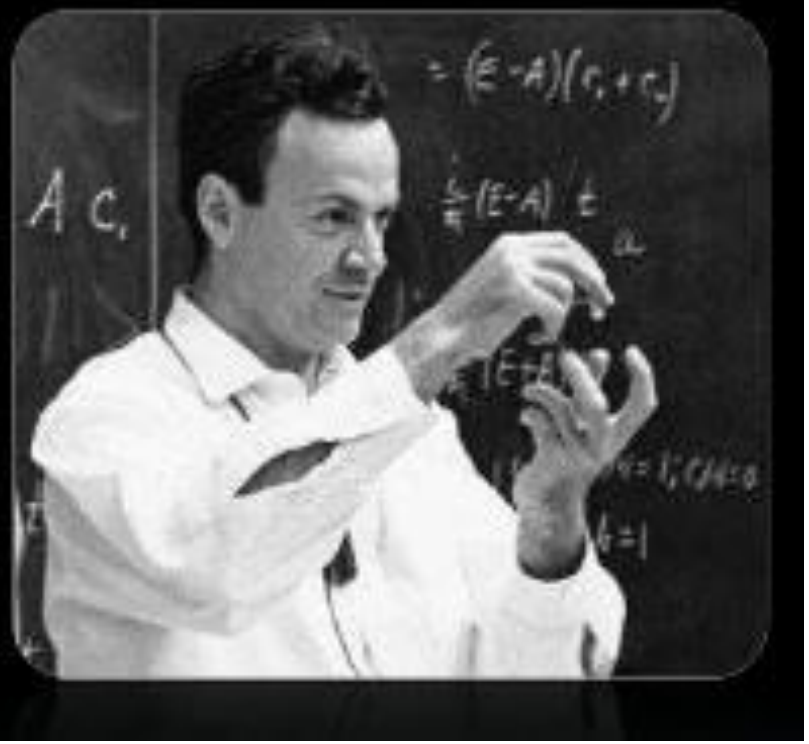
  Executes all operations in one go





Feynman's Proposal of a Quantum Computer

1981 -Richard Feynman determines that it is impossible to efficiently simulate an evolution of a quantum system on a classical computer.



Quantum Algorithms

- Programs that would run on a quantum machine
- Currently, there are no genuine quantum algorithms
- What we have are Qis – Quantum Inspired algorithms
- All use cloud based computing e.g. IBM's Qiskit or IBMQ
- Case study – Shor's algorithm (1994)

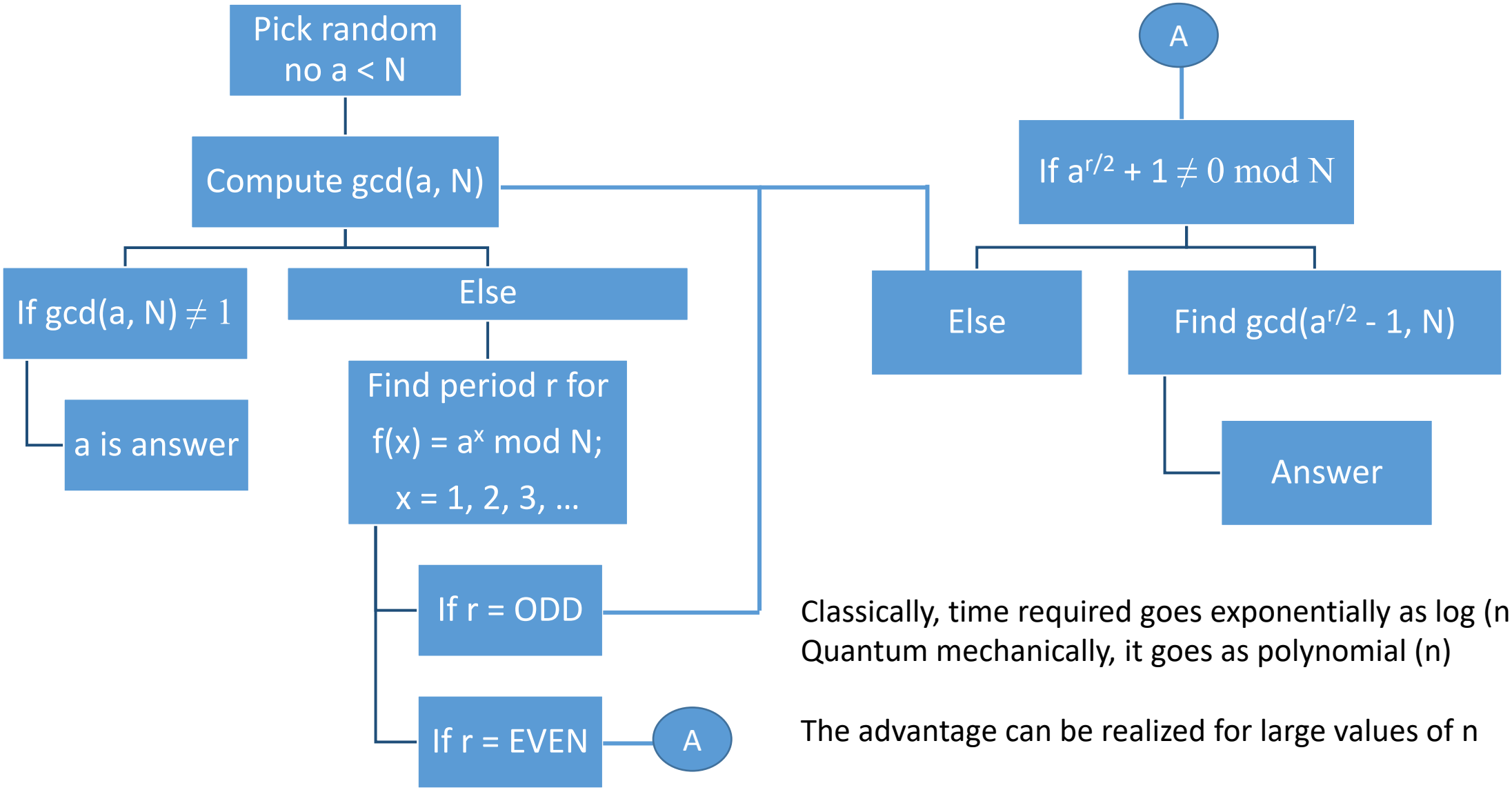
Shor's Algorithm

- To find prime factors of a large number N
- N being some public encryption key*
- Procedure:
- Given an integer N, find another integer p such that $1 < p < N$ and p divides N.
- Steps:

1. Classical part – reduce the factorizing problem to order-finding
2. Quantum part – solve the order finding problem

*RSA (Rivest-Shamir-Adleman) is a public-key cryptosystem that is widely used for secure data transmission

Shor's Algorithm – Classical Computation

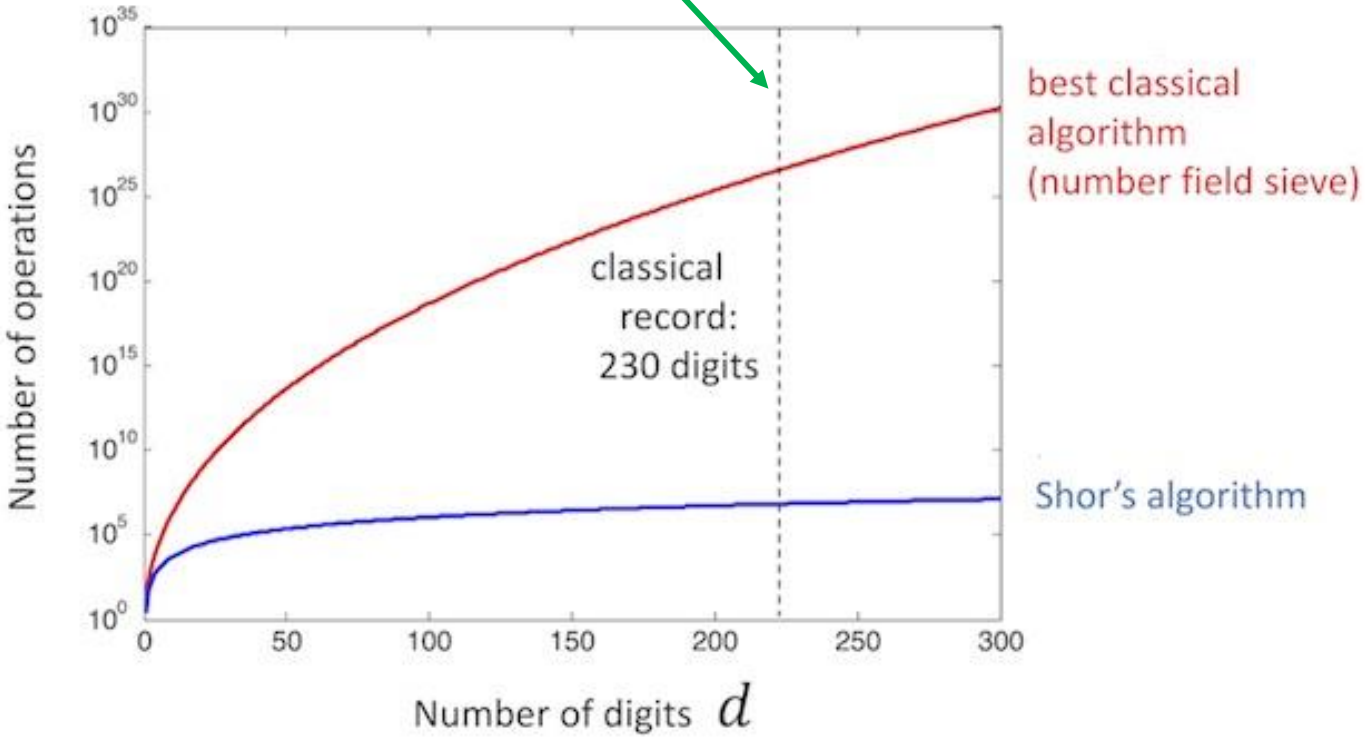


Classically, time required goes exponentially as log (n)
Quantum mechanically, it goes as polynomial (n)

The advantage can be realized for large values of n

Advantage of Quantum Algorithm

Took ≈ 2000 CPU years (OR 2000 parallel processors x 1 year)

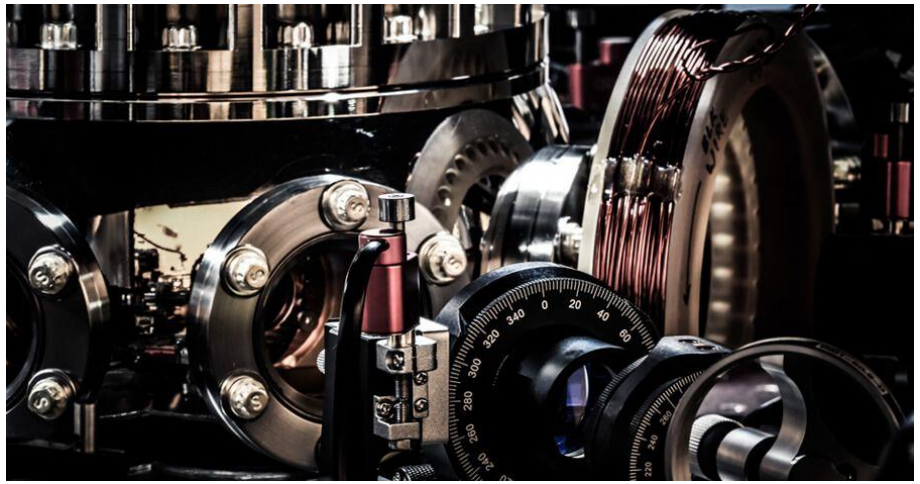


- 2001 IBM demonstrated Shor's algorithm by factorising number 15 using 7 qubits in a NMR system
- 2012,factorized 21
- 2019, tried for 35

Graph credit: IBM Quantum Computing

Quantum Hardware

- Ion trap – uses atomic energy levels
- SQUIDs – uses magnetisation
- NMR – uses nuclear spin
- QD/SET – uses electron energy states
- Examples:
- D-wave Technologies using SQUID
- Honeywell using Ion trap
- IBM using NMR
- Google using superconductors



Quantum Computing

- Using Quantum Mechanical effects for solving computing problems
- Particularly useful for problems involving operations on massive data:

1. Cryptography/Cybersecurity
2. Accurate weather forecasting
3. Traffic optimisation
4. Financial models
5. Drug development
6. Astronomical data analysis