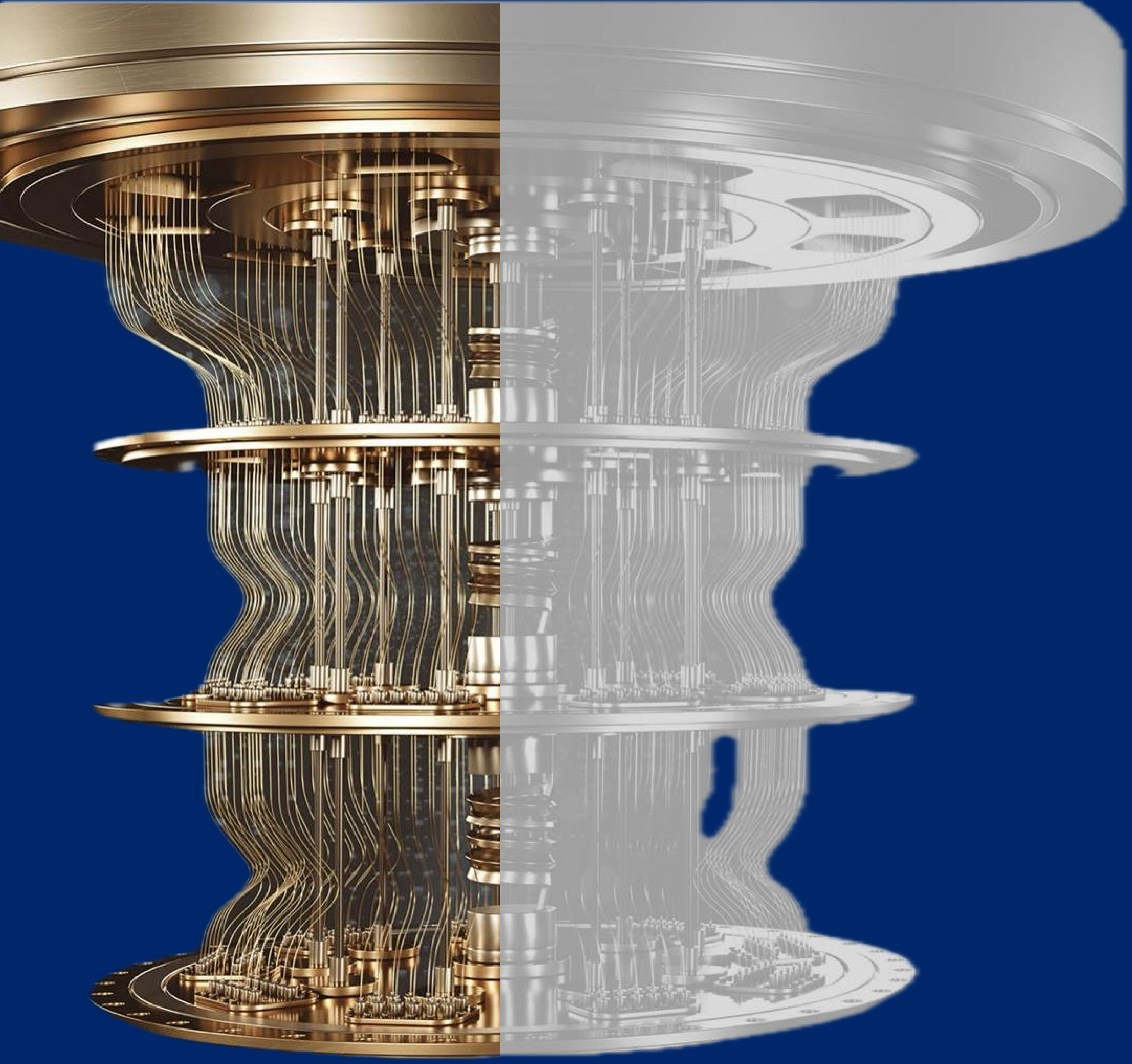


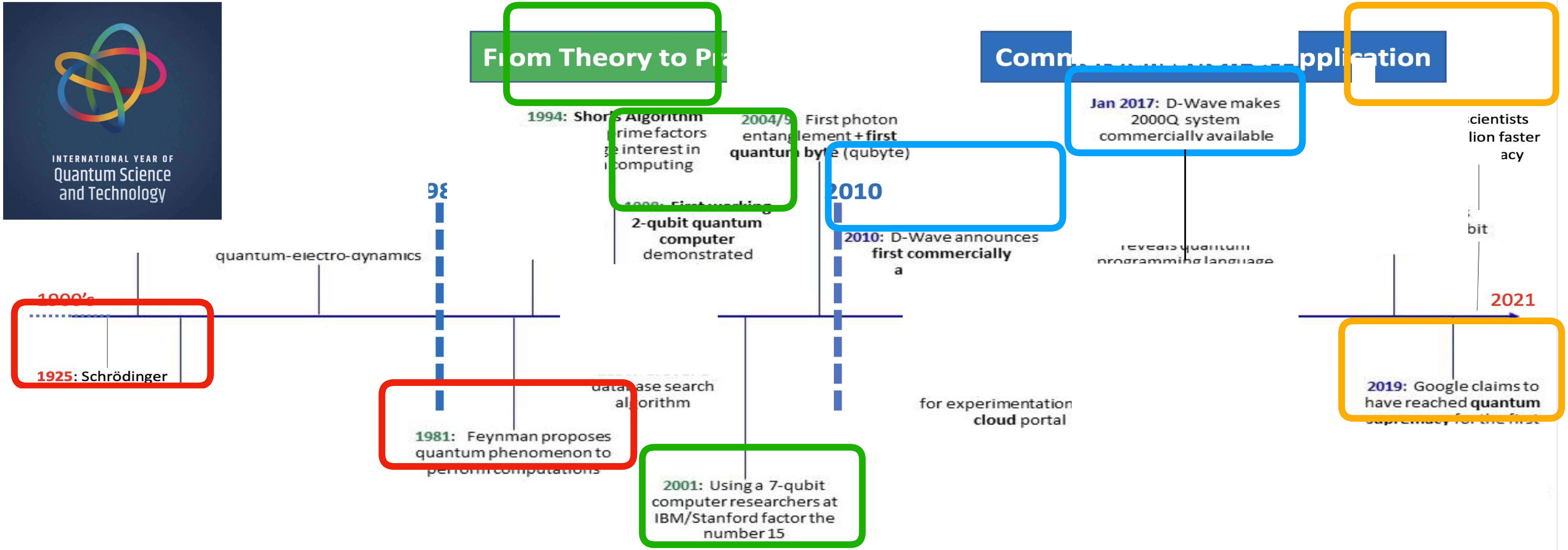
2025

INTERNATIONAL YEAR OF
Quantum Science
and Technology

Quantum Physics and Quantum Computing

Some historical milestones

Evolution of Quantum Theory & Quantum Technology



From classical to quantum computer:

Terminology similarities and differences

"Bit" = single **digit** in binary number

e.g. decimal 5 = 3 bits (101) in binary

"Byte" = a set of 8 bits

State "0" or "1" is usually associated with **voltage levels** in circuit (0 V, 5 V)

"Gate" = **circuit** with several input wires - one output wire

Computer chip = a circuit made up of many gates

"Qubit" = a **physical object** that exhibits quantum behaviours

e.g. atom, electron, photon

"Register" = several Qubits in a row

State "0" or "1" is associated with **quantum state** that Qubit can be in,

e.g.electron spin UP or DOWN

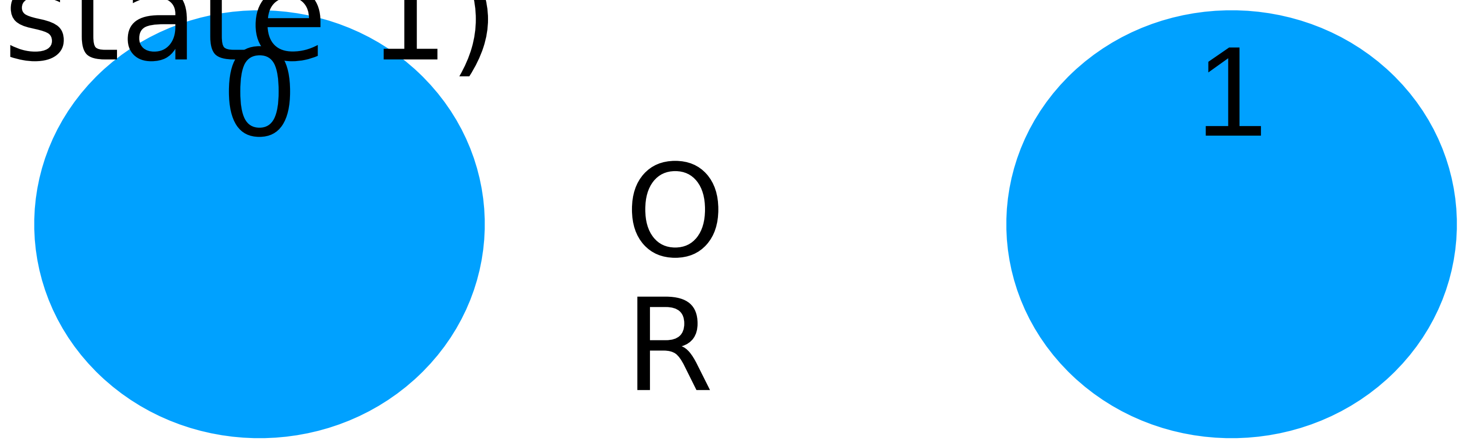
"Gate" = **act of manipulation** of a qubit to change its state

QC-chip = a miniature container in which the qubits are contained with sensors to observe them, manipulators to control the qubit state

Classical Bits (e.g. voltage levels)

Computing is based on electrons flowing in wires and electronic circuits

Voltage levels (e.g. 0 to 2,5V for bit in state 0 and 2,5 to 5V for bit in state 1)



State of Bit is **deterministic**

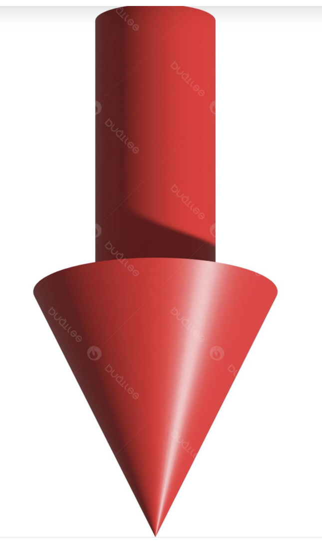
Bits **do not influence each other**

Measuring the state of a Bit does not affect its state - one can make copies

Changing the state of a Bit is **a step of** a classical computing program (or **algorithm**)

Quantum Bits (Qubits)

O
R



with
probabilitie
s attached

State of Qubit is a **superposition** of its possible states e.g. $|UP\rangle$ and $|DOWN\rangle$

Measuring the state of a Qubit changes its state

Therefore a Qubit **cannot be copied** or **cloned**

Measurement will result in definite state $|UP\rangle$ or $|DOWN\rangle$

However the result occurs only with a certain **probability**

Power of Quantum computing**: measured probability is part of the result**

Physical realisations of Quantum Computers

… various candidates for Qubits

Photon based - polarisation state of light

Ion or Atom traps - energy level / spin states of electron

Quantum dots - spin state of electrons in nm-size structures

Superconducting circuits - coil or junction current directions

Nuclear Magnetic Resonance - spin state of nuclei

…

Quantum behaviours underpin Quantum Computing

Superposition of Quantum particle states

Measurement process

Entanglement of Quantum particles

These 3 features follow strict mathematical rules, but are not intuitive

When quantum particles interact with macroscopic world, they become part of a world of many interactions: collective behaviour

Behaviour reverts to classical macroscopic experiences (=“decoherence”)

How to imagine / think about superposition & probability

A concept valid both in classical and quantum world

Flipped coin settles showing either **heads** or **tails**

While spinning, effectively in both states “at once” - i.e. either is possible

After landing it is only in one state = **measured outcome**

If coin is fair, 50% probability for either outcome

Repeat to obtain the most probable outcome

How to imagine / think about entanglement

State of each particle in the register is not independent of the state of the others

Coins close to each other interact and “agree” on a measurement result (i.e. **heads** or **tails)**

While spinning, **both coins** are jointly **in both states “at once”**

After one of them has landed - the other will have a predefined **outcome**

EVEN when measured far apart

Measureme
nt

“HEADS
”

o
r

“HEADS
”

“TAILS
”

“TAILS
”

A Qubit manipulation affects ALL states

… while a measurement has not yet happened

Classical bits & bytes

000

001

010

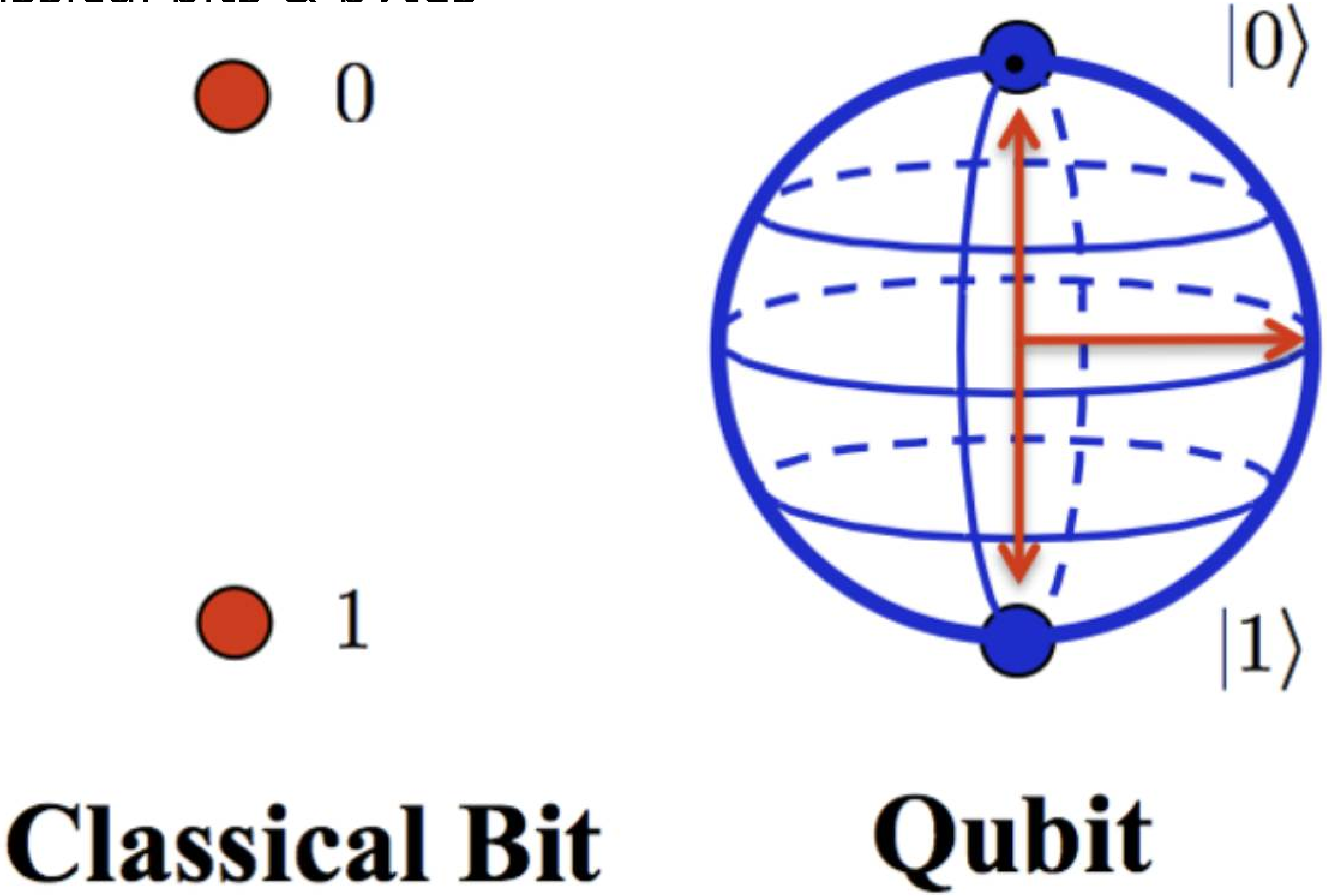
100

101

110

011

111



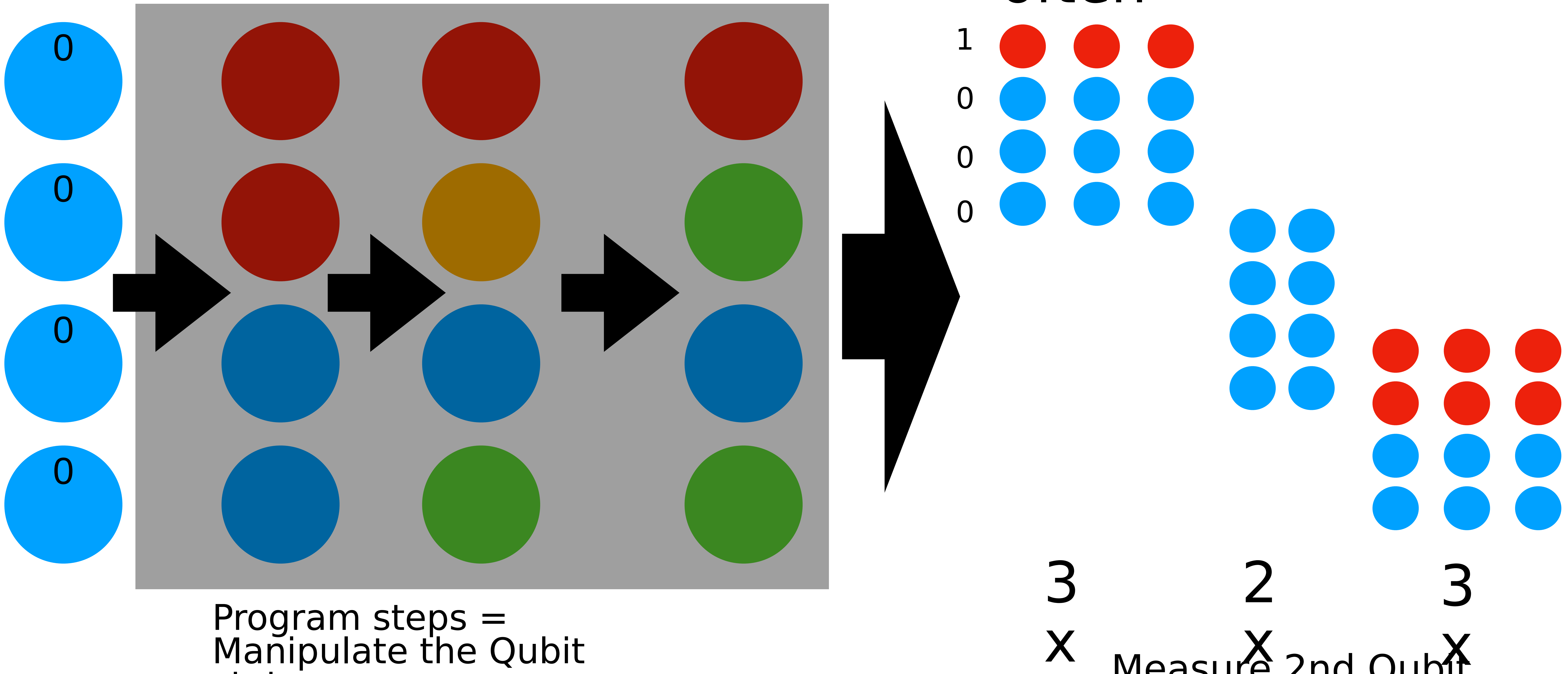
Superposition of states |0 〉 and |1 〉
Arrow pointing to anywhere on a <u>sphere</u>

Essence of Quantum computing

Prepare a number of Qubits in a register

All in a defined start state

probability = how often



Program steps = Manipulate the Qubit states

Do not measure, allow system to relax after each manipulation

Measure 2nd Qubit state

Result ‘1’= 3/8 = 37,5%

Long (relevant) Quantum coherence times

The need for cryogenic temperatures

Qubits need to be well isolated from surrounding macroscopic world

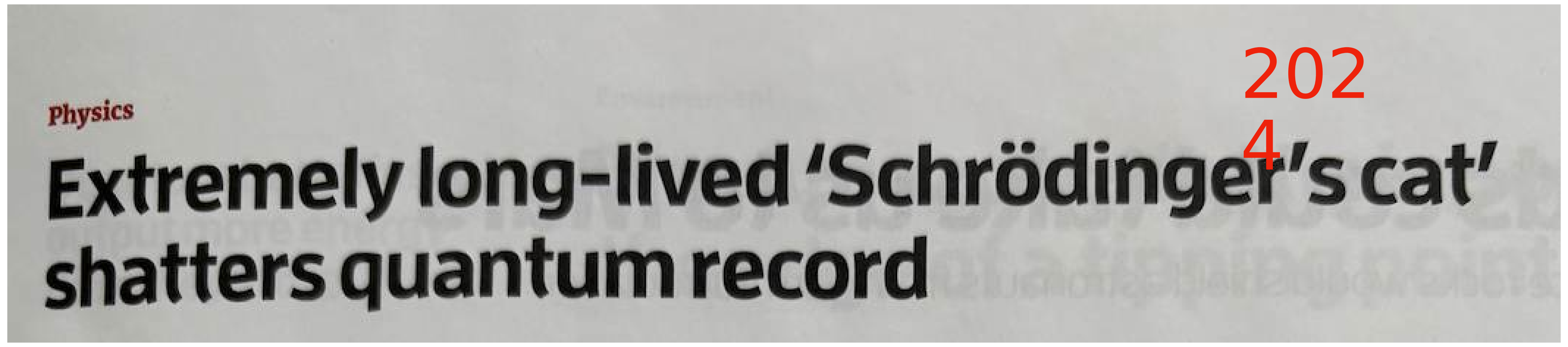
Qubits interact with surroundings via heat and electromagnetic radiation

Additionally temperature of qubit itself needs to be lowered:

- Thermal vibration states in case of atom/ion in a gas, or
- Current fluctuations in case of an electrical circuit element (superconducting junction)

Preserving delicate quantum states - avoid ‘decoherence’ - need to cool the system down to temperatures close to absolute zero (- 273℃)

Record coherence time = **23 minutes**


Physics

Extremely long-lived ‘Schrödinger’s cat’ shatters quantum record

2024

Limitations and practical problems of QC

Physics

Dec 2024

Cracking the Challenge of Quantum Error Correction

Researchers at Google Quantum AI have demonstrated "below-threshold" error correction, a necessary condition for building noise-resistant quantum computers that are sufficiently large to perform useful computations.

By Matteo Rini and Michael Schirber

Quantum computing

2025

Quantum computer is first to correct its own errors

Decoherence time is practical limit - current record is 23 minutes before qubit became decoherent i.e. interacted with surroundings

Calculation is still marred by errors (decoherence effects, quantum noise) which need to be detected and avoided

Quantum error correction techniques are major research area

What is Quantum Computing (QC) good for?

Identified use cases

Large optimisation problems have been shown to be solved efficiently by **Quantum annealing,** but a proof of supremacy is outstanding

Random nature of sequence of measurements & ‘no cloning’ theorem make QC an attractive technology for **Quantum Key Distribution**

Shor’s algorithm for factorisation of prime number products makes it a most desirable technology for those that want to break asymmetric (private/public) key encryption

HHL for solving Simultaneous Linear Equations (exponential speed-up)

All other algorithms ? … watch the news carefully