Quantum Computing Explained

Table of Contents

1. Introduction 4

2. Types of quantum computers 7

2.1. Direct Quantum Simulator (DQS) 7

2.2. Adiabatic Quantum Computer (AQC) 8

2.3. Quantum Annealer (QA) 8

2.4. Boson sampler 10

2.5. Entropy Quantum Computer (EQC) 11

3. Universal quantum computers 12

3.1. Gate-based quantum computing 12

3.2. Quantum computer components 26

3.3. Quantum emulators 28

3.4. Quantum computing software 29

3.5. Quantum algorithms 30

3.6. Quantum computer benchmarking 32

Appendix A - Qubit technologies and manufacturers 34

A.1 Controlled atom qubits 38

A.2 Superconducting qubits 40

A.3 Electron spin qubits (aka quantum dot qubits) 43

A.4 Cavity spin qubits 44

A.5 Topological qubits 45

A.6 Photonic qubits 49

Appendix B - Dutch quantum R&D ecosystem 54

Appendix C - References 63

Appendix D - Acronyms and abbreviations 64

1. Introduction

As early as 1959 the American theoretical physicist Richard Phillips Feynman noted that, as electronic components began to reach microscopic scales, effects predicted by quantum mechanics do occur which, he suggested, might be exploited in the design of more powerful computers. In 1981, Feynman gave a lecture in which he argued that classical computers cannot adequately represent quantum mechanical systems. He then went on to describe the features that a quantum computer should have to be useful for this purpose. Feynman's idea corresponds with so-called direst quantum simulators (a specific type of analogue quantum computer, see § 2.1). At that time it was unclear to Feynman and the entire physics community how such a machine could be built.

In 1985, the British physicist David Elisier Deutsch developed a comprehensive framework for quantum computing, based on ideas for gate-based quantum computing developed by the Russian mathematician Yuri Manin and the American physicist Paul Benioff. Deutsch described in detail what is a quantum algorithm. Together with the Australian mathematician Richard Jozsa he developed in 1992 an example of a quantum algorithm that would outperform a classical computer.

In 1994, the American mathematician and computer scientist Don Coppersmith invented a quantum algorithm version of the Fourier transform (named after the French mathematician and physicist Jean-Baptiste Joseph Fourier), which claimed an exponential quantum speedup. The Quantum Fourier Transform (QFT) algorithm served as a major component for the American mathematician Peter Shor's quantum algorithms for factoring large integers and for solving the discrete logarithm (dlog) problem, which were published in 1994. The publication of Shor's algorithms stimulated research on quantum algorithms, while other researchers were beginning to make progress on the physical implementation of a quantum computer. It soon became clear that powerful quantum computers, if they were ever to be built, would be capable of solving many problems that are out of reach for classical computers.

What is a quantum computer? Quantum computers are devices that leverage specific properties described by quantum mechanics, such as quantum superposition (Box 1.1), quantum measurement (Box 1.2), the Born rule (Box 1.3), quantum entanglement (Box 1.4) and reversible computation (Box 1.5), to perform computations. Though classical computers can also be described by quantum mechanics, they do not take advantage of these specific properties of quantum mechanics.

A quantum state is a mathematical entity that provides a probability distribution for the outcomes of each possible measurement on a quantum system. Knowledge of the quantum state together with the rules for the quantum system's evolution in time exhausts all that can be predicted about the quantum system's behaviour.

Quantum superposition is a fundamental principle of quantum mechanics. It states that, much like waves in classical physics, any two (or more) quantum states can be added together ("superposed") and the result will be another valid quantum state; and conversely, that every quantum state can be represented as a sum of two or more other distinct quantum states. The principle of quantum superposition states that if a physical system may be in one of many configurations (arrangements of particles or fields) then the most general state is a combination of all of these possibilities. The principle applies to the states that are theoretically possible without mutual interference or contradiction. It requires us to assume that between these states there exist peculiar relationships such that whenever the system is definitely in one state, we can consider it as being partly in each of two or more other states. The original state must be regarded as the result of a kind of superposition of the two or more new states, in a way that cannot be conceived on classical ideas. Any state may be considered as the result of a superposition of two or more other states, and indeed in an infinite number of ways.

Box 1.1: Quantum superposition

A quantum measurement is the testing or manipulation of a quantum system to yield a numerical result. The predictions that quantum mechanics makes about these measurements are in general probabilistic and depends on state of the system that is being measured.

Box 1.2: Quantum measurement

According to the Born rule (named after the German-British physicist Max Born), in a superposition of quantum states, the modulus squared of the amplitude of a state is the probability of that state resulting after measurement, Furthermore, the sum of the square of the amplitudes of all possible states in the superposition is equal to 1.

Box 1.3: Born rule

Quantum entanglement is a physical phenomenon that occurs when a group of particles are generated, interact, or share spatial proximity in a way such that the quantum state of each particle of the group cannot be described independently of the quantum state of the others, including when the particles are separated by a large distance. The topic of quantum entanglement is at the heart of the disparity between classical physics and quantum mechanics.

Box 1.4: Quantum entanglement

Operations used in quantum computation other than for measurement must be reversible (if an irreversible operation would be performed, information would be lost, meaning that a measurement has been performed).

Note: This requirement applies to a theoretical noiseless quantum computer. In a noisy quantum computer quantum states decohere and its operations can therefore not be reversed.

Box 1.5: Reversible computation

The fact that there are currently multiple radically different approaches to quantum computing under development and being marketed, with no assurance that any of them will meet market success (let alone market dominance), speaks to quantum computing's infancy. Quantum computing has not yet reached a point where everybody settled on the use of common technologies, and so there still is a lot of uncertainty about the way forward (this can be compared to the situation in the early days of classical computers when there was a debate on whether computer chips should be made of silicon or germanium). It may also be the case that certain approaches are better for certain types of quantum computing applications and that other approaches are better for other types of applications.

2. Types of quantum computers

A distinction must be made between universal (gate-based) quantum computers and specialised (analogue) quantum computers.

A universal gate-based quantum computer implements a small set of primitive operations (called quantum gates) on qubits. A quantum computation is performed by executing a series of these primitive operations. Universal gate-based quantum computing, qubits and quantum gates are described in the next chapter.

An analogue quantum computer carries out a computation without breaking the operations down into a small set of primitive operations. Instead, analogue quantum computers work by directly representing the task at hand in terms of an Hamiltonian (Box 2.1), which may or may not vary with time. The desired result is encoded in the system's quantum state at the end of the simulation run.

> The Hamiltonian of a quantum system (named after the Irish mathematician and physicist William Rowan Hamilton) is an operator corresponding to the total energy of that system, including both kinetic energy and potential energy. Its spectrum, the system's energy spectrum or its set of energy eigenvalues, is the set of possible outcomes obtainable from a measurement of the system's total energy.
>
> An eigenstate is the measured state of some object possessing quantifiable characteristics such as position, momentum, etc. (the word "eigenstate" is derived from the German word "eigen", meaning "inherent" or "characteristic"). The state being measured and described must be observable (i.e. something such as position or momentum that can be experimentally measured either directly or indirectly), and must have a definite value, called an eigenvalue. In the everyday world, it is natural and intuitive to think of every object being in its own eigenstate; this is just another way of saying that every object appears to have a definite position, a definite momentum, a definite measured value and a definite time of occurrence. However, in quantum mechanics, Heisenberg's uncertainty principle implies that it is impossible to measure the exact value for the momentum of a particle, given that its position has been determined at a given instant and likewise, it is impossible to determine the exact location of that particle once its momentum has been determined at a particular instant. Therefore, it becomes necessary to formulate clearly the difference between the state of something that is uncertain and the state of something having a definite value. When an object can definitely be "pinned down" in some respect, it is said to possess an eigenstate.

Box 2.1: Hamiltonian

Analogue quantum computers may be qubit-based or not. A few examples of analogue quantum computers are described below.

2.1. Direct Quantum Simulator (DQS)

In direct quantum simulation the Hamiltonian created is analogous to that of the quantum system that is being explored. In essence, it means that some controllable quantum system is used to study another less controllable or less accessible quantum system. Direct quantum simulation promises to have applications in the study of many problems in fields such as condensed-matter physics, high-energy physics, atomic physics, quantum chemistry and cosmology.

2.2. Adiabatic Quantum Computer (AQC)

Adiabatic quantum computation is a form of quantum computing which relies on the adiabatic theorem (Box 2.2) to do calculations. In adiabatic quantum computing, a system is slowly evolved from the ground state of a simple initial Hamiltonian to a final Hamiltonian that encodes a computational problem. The appeal of this approach lies in the combination of simplicity and generality. In principle, any problem can be encoded. In practice, however, applications are restricted by limited connectivity, available interactions and noise. Adiabatic quantum computation is used to solve satisfiability problems and other combinatorial search problems.

The adiabatic theorem is a concept in quantum mechanics. Its original form, due to Max Born and the Russian physicist Vladimir Aleksandrovich Fock, was stated as follows: "A physical system remains in its instantaneous eigenstate if a given perturbation is acting on it slowly enough and if there is a gap between the eigenvalue and the rest of the Hamiltonian's spectrum". In simpler terms, a quantum mechanical system subjected to gradually changing external conditions adapts its functional form, but when subjected to rapidly varying conditions there is insufficient time for the functional form to adapt, so the spatial probability density remains unchanged.

Box 2.2: Adiabatic theorem

2.3. Quantum Annealer (QA)

Quantum annealing (Box 2.3), which is a restricted form of adiabatic quantum computing, is a metaheuristic for finding the global minimum of a given objective function (Box 2.4) over a given set of candidate solutions (candidate states). It is used for finding an absolute minimum or maximum size/length/cost/distance from within a possibly very large, but nonetheless finite set of possible solutions (using quantum fluctuation-based computation instead of classical computation). Quantum annealing is used mainly for problems where the search space is discrete (combinatorial optimisation problems) with many local minima.

In metallurgy and materials science, annealing is a heat treatment that alters the physical and sometimes chemical properties of a material to increase its ductility and reduce its hardness, making it more workable. It involves heating a material above its recrystallisation temperature, maintaining a suitable temperature for an appropriate amount of time and then cooling.

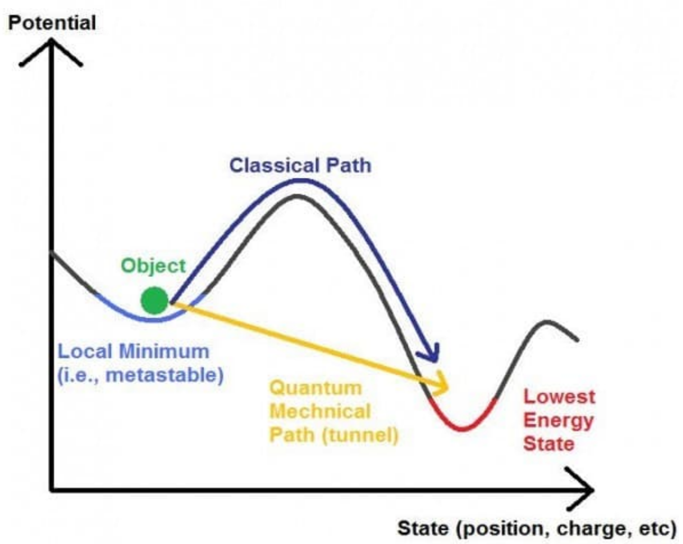
Box 2.3: Annealing

An objective function is either a cost function (aka loss function) or a profit function (aka reward function), which an optimisation problem seeks to minimise (cost function) or maximise (profit function).

Box 2.4: Objective function

Quantum annealing starts from a quantum-mechanical superposition of all possible states (candidate states) with equal weights. Then the system evolves following the time-dependent Schrödinger wave equation (named after the Austrian-Irish theoretical physicist Erwin Rudolf Josef Alexander Schrödinger), a natural quantum-mechanical evolution of physical systems. The amplitudes of all candidate states keep changing according to the time-dependent strength of a magnetic transverse field, which causes quantum tunnelling (Box 2.5) between states.

Quantum tunnelling is a quantum mechanical phenomenon in which a particle passes through a potential energy barrier that, according to classical mechanics, the particle does not have sufficient energy to enter or surmount. Quantum tunnelling is a consequence of the wave nature of matter, where wave equations such as the Schrödinger equation describe the behaviour of a particle. The probability of transmission of a particle wave packet through a barrier decreases exponentially with the barrier height, the barrier width and the particle's mass, so tunnelling is seen most prominently in low-mass particles such as electrons or protons tunnelling through microscopically narrow barriers.



Quantum tunnelling (source: Wikimedia Commons 2025)

Box 2.5: Quantum tunnelling

If the rate of change of the magnetic transverse field is slow enough, the system stays close to the ground state of the instantaneous Hamiltonian. If the rate of change of the magnetic transverse field is accelerated, the system may leave the ground state temporarily but produce a higher likelihood of concluding in the ground state of the final problem Hamiltonian. The magnetic transverse field is finally switched off, and the system is expected to have reached the ground state, which corresponds to the solution to the original optimisation problem.

Note:
Digital Annealers (DAs) are dedicated digital chips that use a non-Von Neumann architecture (see Box 3.6 in Chapter 3) to minimise data movement in solving combinatorial optimisation problems. Such a chip is composed of thousands of bit-updating blocks with on-chip memory that stores weights and biases, logic blocks to perform bit flips, and interfacing and control circuitry. Rather than programming the DA, a problem

is uploaded in the form of weight matrices and bias vectors so as to convert the problem into an “energy landscape”. Problem solving with a DA is very similar to problem solving with a Quantum Annealer (QA).

2.4.Boson sampler

Boson (Box 2.6) sampling is based on the Fock states (Box 2.7) of a beam of photons (Box 2.8) entering an optical circuit, which implements a series of phase shifters and beam splitters that represents a unitary matrix. By sampling from the distribution of photons that passed through the optical circuit, a related matrix can be effectively computed, which is a hard problem for classical computing.

A boson is a subatomic particle whose spin quantum number is an integer value (0 , 1 , 2 , 3 , etc.). There are two types of bosons: elementary bosons and non-elementary bosons. Elementary bosons are elementary subatomic particles. Some elementary bosons, e.g. the photon (associated with the electromagnetic force), the gluons (associated with the strong force) and the W and Z bosons (associated with the weak force), give rise to forces between other particles. One elementary boson, the Higgs boson (with spin 0), named after the British theoretical physicist Peter Ware Higgs, gives rise to the phenomenon of mass (all of space is assumed to be filled with a Higgs field, a background of virtual Higgs bosons that pop in and out of existence). The Higgs boson is different from the other elementary bosons (photon, gluons, W and Z bosons) in that it doesn't involve anything resembling a force.

Non-elementary bosons, e.g. mesons and stable nuclei of even mass number (such as hydrogen-2 and helium-4), are composite subatomic particles made up of smaller constituents. Unlike fermions, bosons are not subject to the Pauli exclusion principle and they can thus occupy the same place at the same time. For example, in a laser beam many photons occupy the same quantum state with the same colour, the same direction and the same spatial profiles. Other well-known examples of bosonic behaviour are superconductivity and superfluidity, where large number sf Cooper pairs of electrons or helium-4 atoms, respectively, occupy the same quantum state and thus flow coherently.

The name boson is in honour of Satyendra Nath Bose, an Indian physicist who developed a quantum theory for these particles (known as Bose-Einstein statistics) together with the Swiss-American theoretical physicist Albert Einstein.

Box 2.6: Boson

A Fock state, named after Vladimir Fock, is a quantum state that is an element of a Fock space within a well-defined number of particles. A Fock space is an algebraic mechanism to construct quantum states from a single-particle Hilbert space.

Box 2.7: Fock state

The photon is an elementary subatomic particle. It is the quantum of the electromagnetic field, including electromagnetic radiation such as light and radio waves, and it is the force carrier for the electromagnetic force. Photons do not have electrical charge, they have zero mass and zero rest energy, and they only exist as moving particles. Photons move at 299,792,458 metres per second in a vacuum, the so-called “speed of light” denoted by *c* (from the Latin celeritas). The speed of photons in a medium depends upon the medium and is always slower than the speed in vacuum *c*.

Box 2.8: Photon

To overcome practical implementation difficulties, Gaussian Boson Sampling (GBS) was introduced, as Gaussian photon input states are much easier to generate and manipulate than Fock photon input states.

2.5.Entropy Quantum Computer (EQC)

Natural quantum states interact freely, influencing and impacting each other as they evolve and change. This natural interaction significantly impacts the accuracy and scale of first generation quantum computers which suffer from loss of information, significant errors and limited scalability.

Entropy quantum computing harnesses the true fundamentals of quantum physics to overcome these limitations. It operates on open quantum systems, carefully coupling a quantum system to an engineered environment, so that its quantum state is collapsed to represent a problem's desirable solution. As a result it solves larger and more complex problems, eliminates errors and can be deployed on room temperature rack-mountable servers that require no special infrastructure.

3. Universal quantum computers

3.1. Gate-based quantum computing

In classical computing the information is encoded in bits (binary digits), where each bit can have the binary value “0” or “1”. In quantum computing the information is encoded in qubits. A qubit (quantum bit) is the quantum mechanical analogue of a classical bit. A qubit is a two-level quantum system where the two basis quantum states are usually expressed using bra-ket notation (Box 3.1) and written as $|0\rangle$ and $|1\rangle$.

The bra-ket notation (aka Dirac notation) is used to denote quantum states. The notation uses the angle brackets ⟨ and ⟩ and the vertical bar | to construct "bras" and "kets". Bra–ket notation was created by the British theoretical physicist Paul Adrien Maurice Dirac.

Box 3.1: Bra-ket notation

A qubit can be in state $|0\rangle$, in state $|1\rangle$ or, unlike a classical bit, in a linear combination $\alpha|0\rangle + \beta|1\rangle$ of both states; the name of this phenomenon is quantum superposition.

<u>Note</u>
Mathematically speaking, the qubit is always in quantum superposition following Schrödinger’s wave equation, but in common parlance the basis quantum states $|0\rangle$ and $|1\rangle$ are not considered superposition states.

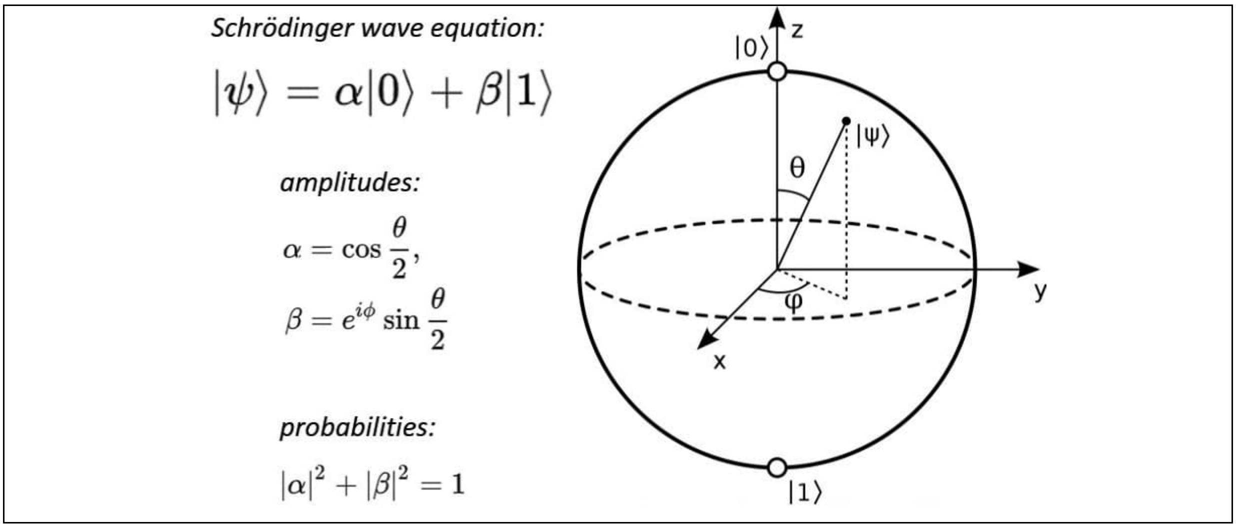
The complex numbers α and β are the probability amplitudes and the sum of the squares of their norms (Box 3.2) equals 1 according to the Born rule: $|\alpha|^2 + |\beta|^2 = 1$.

The vertical bars | and | denote the norm (aka modulus) $\|z\|$ of a complex number $z = a + bi$, which is the length of the vector from the origin to the point (a, b) in a two-dimensional plane. According to the Pythagorean theorem $\|z\|$ is defined as the square root of $a^2 + b^2$.

Box 3.2: Norm of a complex number

The status of a qubit is often visualised with a Bloch sphere (Box 3.3).

The Bloch sphere (named after the Swiss-American physicist Felix Bloch) is a geometrical representation of the pure quantum state space of a two-level quantum mechanical system, e.g. a qubit. The Bloch sphere has antipodal points corresponding to a pair of mutually orthogonal quantum state vectors. The north and south poles of the Bloch sphere correspond to the standard basis vectors $\|0\rangle$ and $\|1\rangle$ of the qubit.



Box 3.3: Bloch sphere (source: Wikipedia 2023)

A single qubit is represented as a (quantum) state vector in the Bloch sphere, a vertical vector containing 2 (21) entries and represented by |Ψ ⟩ , the ket of the quantum state Ψ:

$$|\Psi\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix}$$

where α and β are complex numbers associated with the basis states |0⟩ and |1⟩ of the qubit.

The value 0 is represented by the ket |0⟩ and the value 1 is represented by the ket |1⟩:

$$|0\rangle = \begin{bmatrix}1\\ 0\end{bmatrix} \quad |1\rangle = \begin{bmatrix}0\\ 1\end{bmatrix}$$

The combined state for a set of n qubits is the tensor product (denoted by the symbol ⊗) of the constituent qubit state vectors, i.e. a vector containing 2^n entries. Example: ket representation of the state Ψ of two qubits:

$$|\psi\rangle = v_{00}|00\rangle + v_{01}|01\rangle + v_{10}|10\rangle + v_{11}|11\rangle \rightarrow \begin{bmatrix}v_{00}\\ v_{01}\\ v_{10}\\ v_{11}\end{bmatrix}$$

In a quantum computers, qubits are organised in qubit registers, like the bit registers in today's classical processors but not quite the same though. A quantum computer has only one qubit register and not many bit registers as current classical processors do have.

The most important difference between an n-qubit register and a classical n-bit register is the amount of information that can be manipulated simultaneously (Figure 3.1). In classical computers, the bit registers store bitstrings, integers or floating-point numbers on which elementary logical or arithmetic operations are performed. In contrast, a register of n qubits is a vector in a 2^n dimensional space of complex numbers.

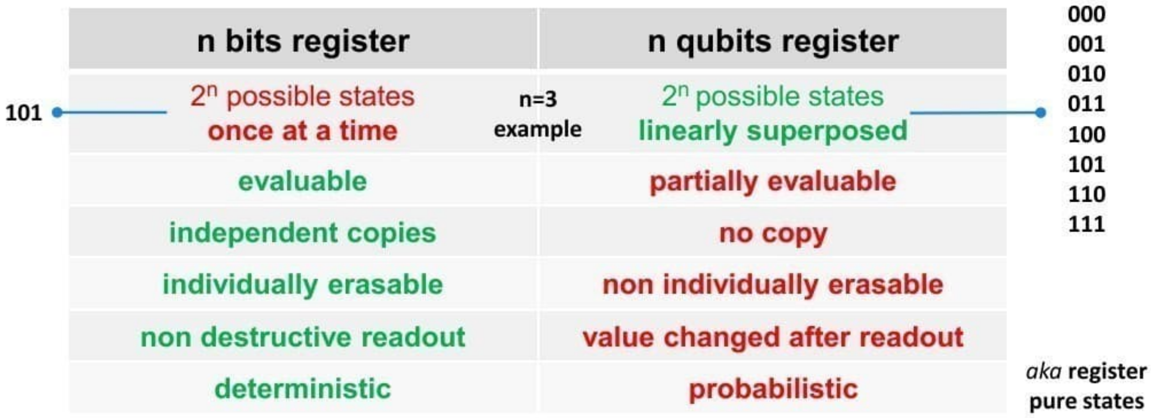


Figure 3.1: Key differences between bit and qubit registers (source: Olivier Ezratty 2023)

These complex numbers are the amplitudes of each computational quantum state and the total of their norms equals 1 since these are probabilities (Born rule). Hence the dimensionality of a n-qubit register is exponentially larger than that of a n-bit register. However, these 2^n computational state amplitudes that occur during a quantum computation are not useful information that we can exploit outside the qubit register, because the information output of a quantum computation (i.e. the qubit register readout result) is just a set of n classical bits corresponding with a single computational state.

Expressing logic in Boolean algebra (Box 3.3) allows us to design machines that can perform logical operations. This is one of the fundamental ideas underlying the design of modern classical computers.

Boolean algebra, named after the British mathematician, philosopher and logician George Boole, makes it possible to treat certain parts of logic algebraically. A Boolean value is a binary digit (bit) that can take on one of two values. These two values are usually represented by “true” and “false” in Boolean algebra, but can also be represented by something else, in particular “0” and “1”. The three basic operations in Boolean algebra, which allow us to express any Boolean function whatsoever, are the not, and and or binary operations.

Box 3.3: Boolean algebra

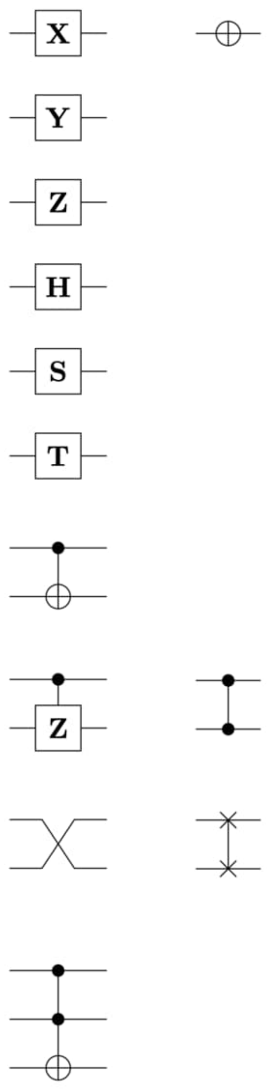
At discrete time intervals (i.e. the clock rate), a pulse of electricity is transmitted (corresponding with the binary value “1” of a bit) or it is not (corresponding with the binary value “0” of a bit) through switches that correspond with binary Boolean operators. These switches are called gates and are the fundamental building blocks of all modern classical computers. Gates are combined together to form a circuit.

Quantum gates and quantum circuits are a natural extension of classical gates and circuits. However, unlike classical gates, quantum gates are not devices located in space made out of some material; they are instead processes applied over time by means of microwave pulses, laser pulses or other means.

Unlike bits, qubits are not pulses of electricity; they are instead devices located in space made out of some material.

Weird as it may sound, in gate-based quantum computing, rather than moving the bits through the gates, as is done in classical computing, the quantum gates are moved through the qubits.

Quantum gates (Figure 3.2) apply a unitary matrix (aka unitary operator, Box 3.4) of complex numbers to qubit(s) state vectors. A quantum gate that acts on n qubits is represented by a 2n x 2n unitary matrix.



Operator	Gate(s)	Matrix
Pauli-X (X)	X	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)	Y	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)	Z	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)	H	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)	S	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)	T	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)	Z	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Figure 3.2: Examples of quantum gates (source: Wikipedia 2025)

An invertible complex square matrix U is *unitary* if its inverse matrix U^{-1} equals its Hermitian adjoint (aka Hermitian conjugate aka Hermitian) $U^{\dagger}$, that is, if $U^{\dagger}U = UU^{\dagger} = I$, where I is the identity matrix (square matrix with ones on the main diagonal and zeros elsewhere). This follows from $U^{-1}U = UU^{-1} = I$ (i.e. the definition of inverse matrix).

The Hermitian adjoint $U^\dagger$ of a square complex matrix is obtained by transposing the matrix, i.e. exchanging its rows and columns and then applying complex conjugation to each entry of the transposed matrix, i.e. replacing $a + \mathrm{i}b$ by $a - \mathrm{i}b$.

An important property of unitary matrices is that they preserve norms, and thus preserve probability amplitudes.

Box 3.4: Unitary matrix

The action of the gate on a specific quantum state is found by multiplying the vector that represents the state by the matrix that represents the gate; the result is another vector that represents the new quantum state.

There are many different types of quantum gates, including:

- single-qubit quantum gates that apply 2 x 2 ($2^1 \times 2^1$) unitary matrices to the qubit state vector containing 2 (2^1) entries:
  - Pauli gates (named after the Austrian physicist Wolfgang Ernst Pauli):
    - X gate (aka NOT gate): performs an inversion (bit flip) from state $|0\rangle$ to $|1\rangle$ and vice versa, corresponding with an 180º rotation around the x-axis of the Bloch sphere. X gates are often used to initialise qubits to $|1\rangle$ (the default initialisation being $|0\rangle$).
    - Y gate: performs an 180º rotation around the y-axis of the Bloch sphere and also turns state $|0\rangle$ into $|1\rangle$.
    - Z gate (aka phase flip gate): applies a sign change to the β component of the qubit state vector (phase inversion), corresponding with an 180º rotation around the z-axis of the Bloch sphere.
  - I (Identity) gate: essentially does nothing and may be used as a “pause” in a quantum circuit.

  Any single-qubit unitary transformation can be decomposed into a linear combination of Pauli gates and I gates.

  - S gate aka P gate (Phase shift gate): generates a phase change (a quarter turn around the z-axis); it is equivalent with half a Z gate.
  - T gate: the equivalent of half an S gate (one eighth of a turn around the z-axis.

- R gates (phase shift gates) are variations of Pauli gates with arbitrary rotation angles (they do not affect the amplitude hence the qubit's measurement outcome is not affected):

  - R_X: rotation around the x-axis;

  - R_Y: rotation around the y-axis;

  - R_Z: rotation around the z-axis (P_{angle} phase change).

  R_Z is meant when X and Y are not specified with R. When $R_X/R_Y/R_Z$ are specified without an angle, it is 90º.

- H (Hadamard) gate, named after the French mathematician Jacques Salomon Hadamard (aka Hadamard-Walsh gate, named after the American mathematician Joseph Leonard Walsh), puts a qubit at state $|0\rangle$ or $|1\rangle$ into a superposed state $(|0\rangle + |1\rangle)/\sqrt{2}$ or $(|0\rangle - |1\rangle)/\sqrt{2}$.

  It is often used to prepare a qubit register before executing an oracle-based quantum algorithm, e.g. Grover's algorithm (named after the Indian-American computer scientist Lov Kumar Grover).

  $H^2 = I$ and therefore, applying the H gate twice to the same qubit has no effect on it.

- $|0\rangle$ reset gate: is sometimes used at the beginning of a quantum circuit (see below).

Single-qubit quantum gates always generate some rotation of the qubit state vector in the Bloch sphere, while the norm stays stable at 1 (before any decoherence happens).

- 2-qubit quantum gates that apply 4 x 4 ($2^2 \times 2^2$) unitary matrices to the qubits state vector containing 4 (2^2) entries:

  - CNOT (Controlled NOT) gate aka CX gate: inverts the state of a qubit (target qubit) conditioned by the state of another qubit (control qubit); it is the quantum computing equivalent of the classical computing XOR (eXclusive OR) gate.

    If the control qubit is in a superposition state, the target and control qubits become entangled.

  - CR (Controlled R) gates: R gates conditioned by the state of a control qubit.

  - CS (Controlled S) gate: S gate conditioned by the state of a control qubit.

  - CZ (Controlled Z) gate: Z gate conditioned by the state of a control qubit.

- SWAP gate: inverts the states of two qubits (and may thus also displace entanglement); it is the only 2-qubit gate that is not generating a new entanglement between the two qubits.

  A SWAP gate can be emulated by applying three CNOT gates in succession.

- 3-qubit quantum gates that apply 8 x 8 ($2^3 \times 2^3$) unitary matrices to the qubits state vector containing 8 (2^3) entries:

  - C2NOT (Controlled CNOT) gate aka CCX gate aka TOFF (Toffoli) gate (named after the American electrical and computer engineer Tommaso Toffoli): inverts the state of a qubit conditioned by the $|1\rangle$ state of two other qubits (control qubits).

  - F (Fredkin) gate, named after the American computer scientist, physicist and businessman Edward Fredkin, aka CSWAP (Controlled SWAP) gate: a SWAP gate that is conditioned by the state of a third qubit.

Note
Sometimes “Conditional” is used instead of “Controlled” in the name of certain quantum gates.

The concept of quantum gates has led to the creation of many theorems about different groups of quantum gates. These theorems are mostly associated with the notion of universal quantum gate sets, which are capable of generating all other quantum gates. A universal quantum gate set is a group of quantum gates that has the property of allowing the creation of all unitary operations on a set of qubits. From a practical point of view, it also allows to create all known quantum gates for one, two and three qubits. Such a quantum gate set must be able to create superpositions and entanglement, and it must contain at least one quantum gate with no real parameters (i.e. complex numbers instead of real numbers).

The Special Unitary group $SU(2^n)$ is the space of unitary transformations applicable on n qubits (Box 3.5). It covers all the unitary transformations that can be performed on n qubits. Hence SU(2) denotes the unitary transformations applicable to a single qubit, SU(4) denotes the unitary transformations applicable to 2 qubits, SU(8) denotes the unitary transformations applicable to 3 qubits, and so on.

A complex square matrix U is Special Unitary (SU) if it is unitary and its matrix determinant equals 1. The determinant of an n x n square matrix can be defined in several equivalent ways, the most common being Leibniz formula, which expresses the determinant as a sum of n! signed products of matrix entries. It can also be computed by the Laplace expansion, which expresses the determinant as a linear combination of determinants of submatrices, or with Gaussian elimination, which allows computing a row echelon form with the same determinant, equal to the product of the diagonal entries of the row echelon form.

Box 3.5: Special Unitary

Various classifications of quantum gates have been proposed; Figure 3.3 provides an example classification scheme.

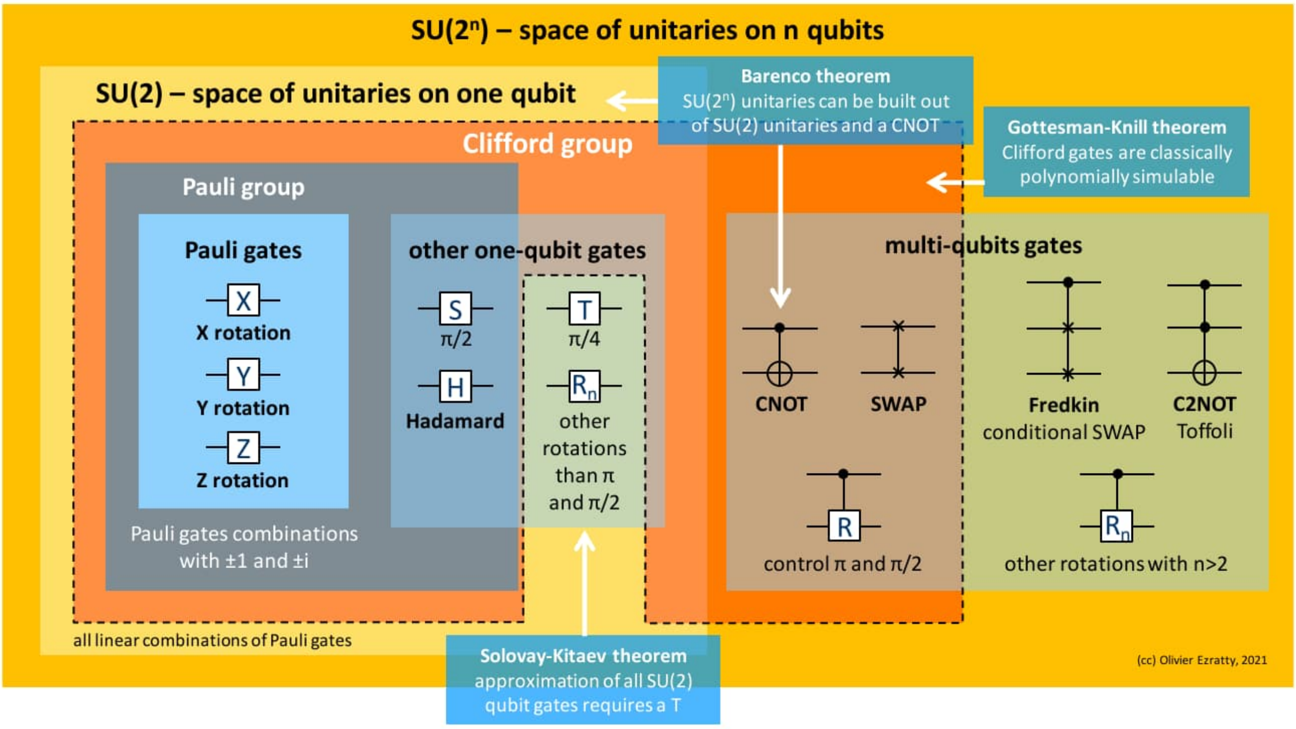


Figure 3.3: Example quantum gate classification scheme (source: Olivier Ezratty 2024)

The Clifford group, named after the British theoretical physicist Clifford Victor Johnson, is a group of single- and multiple-qubit quantum gates (so-called “digital quantum gates”), consisting of: CNOT gate, 90º and 180º CR gates, H gate, 90º and 180º R gates, S gate, SWAP gate, and the X, Y and Z Pauli gates.

The Gottesman-Knill theorem, named after the American physicist Daniel Gottesman and the the American mathematician and computer scientist Emanuel Knill, states that quantum algorithms using only quantum gates belonging to the Clifford group can be emulated in polynomial time on a classical computer. Therefore, non-Clifford gates (so-called “analogue quantum gates”) such as the C2NOT gate, the CR gates other than 180º and 90º, the Fredkin gate, the R gates other than 180º and 90º and the T gate, must be used by a quantum algorithm to obtain quantum speedup.

The Solovay-Kitaev theorem, named after the American mathematician Robert Martin Solovay and the Russian theoretical physicist Alexei Kitaev, states that if a set of single-qubit quantum gates generates a dense subgroup of SU(2), then that set can be used to approximate any desired quantum gate with a short sequence of quantum gates that can also be found efficiently.

The Barenco theorem, named after the Swiss physicist Adriano Barenco, states that the set of single-qubit quantum gates plus the CNOT quantum gate is universal (any n-qubit quantum gate can be implemented with single-qubit quantum gates and CNOT quantum gates).

The quantum computation's main goal is to amplify the computational state amplitudes that will produce the desired result, while at the same time reducing all the other computational state amplitudes to near zero. Gate-based quantum computing is the main quantum computing paradigm. It is based on quantum computation performed by quantum circuits that combine qubits, quantum gates and qubit measurements. See Figure 3.4 for an example.

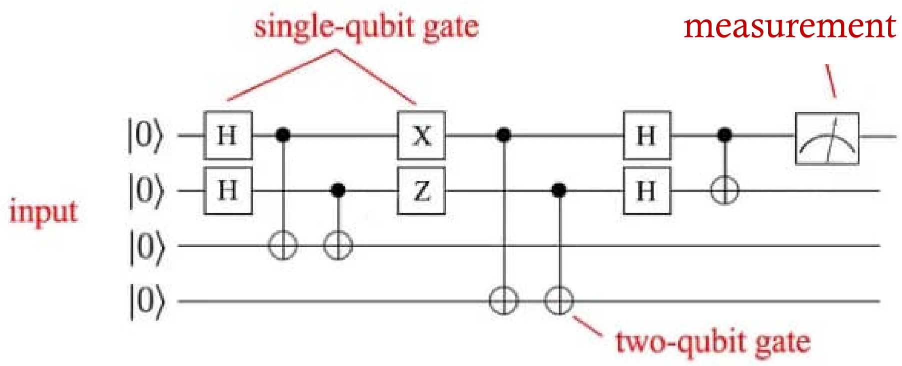


Figure 3.4: Quantum circuit example (source: Jonathan Hui 2022)

The quantum circuit width is the number of qubits; some quantum circuits are narrow while others are wide. The quantum circuit depth is the number of quantum gates; some quantum circuits are shallow while others are deep. Furthermore, some quantum circuits are wide shallow circuits or narrow deep circuits.[1]

In a gate-based quantum computer, a quantum computation is performed in a series of steps that constitute a quantum circuit (see Figure 3.5 for an example).

- The first step ("initialising the system") consists of resetting the set of qubits that will be manipulated (the "quantum register") to the $|0\rangle$ state. This is mostly done by applying a $|0\rangle$ reset quantum gate. This step is not needed if qubits are in the default $|0\rangle$ initialisation state.
- The next step ("preparing the system") is to change the $|0\rangle$ state of selected qubits to the $|1\rangle$ state (by applying X gates) or to a superposition of $|0\rangle$ and $|1\rangle$ (by applying H gates).
- Quantum gates are then sequentially applied to the set of qubits according to the specification of the quantum algorithm to be executed. The quantum information that is manipulated during quantum computation is very "rich", consisting of a vector of two complex numbers α and β for each individual qubit. Quantum gates are reversible operations and therefore, no quantum information is lost during the quantum computation[2]. Applying a sequence of applied quantum gates in reverse order is known as the "uncompute trick".

---

[1] This is a bit confusing because in most graphical representations of quantum circuits, the qubits are shown from top to bottom and the quantum gates are shown from left to right.

[2] In practice, this will often not be the case because of qubit decoherence.

- The last step of the quantum computation consists of measuring the qubits. While quantum gates are reversible operations based on unitary operators, measuring the state of a qubit is an irreversible operation that collapses its state. When the state of a qubit is measured (“qubit readout”), a classical binary “0” or “1” is obtained, with a probabilistic return depending on the qubit state. It must therefore be repeated multiple times in order to obtain the desired output, i.e. the result which has the highest probability of occurrence, by averaging the results of a series of repeated measurements. The main objective of quantum computing is to execute a quantum circuit to transform the system’s quantum state in such a way that the desired outcome has a high probability of occurring.

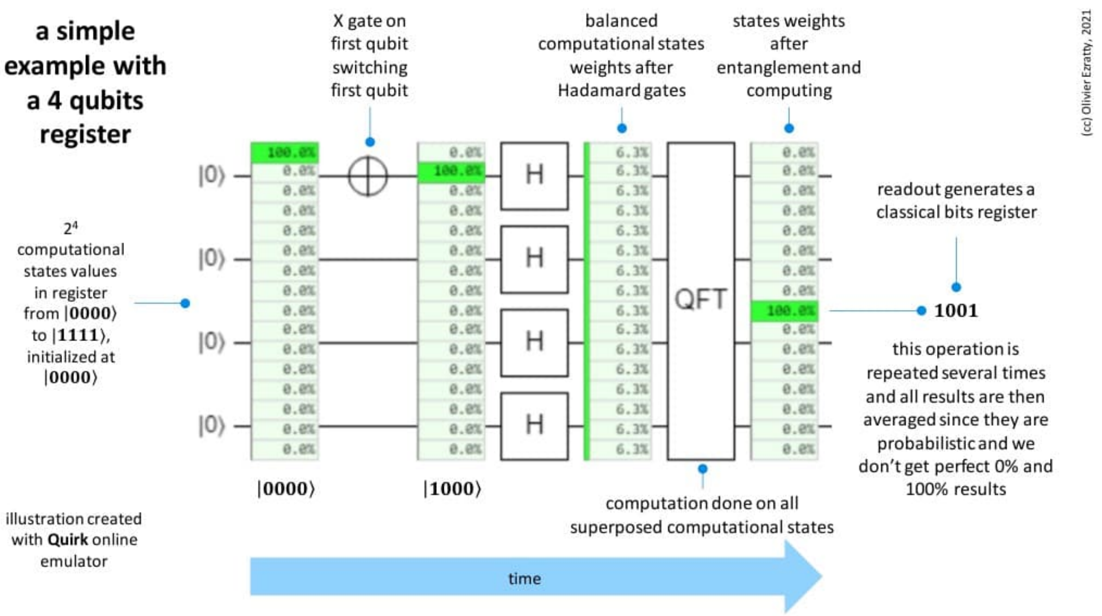


Figure 3.5: Example quantum computing execution flow (source: Olivier Ezratty 2021)

Gate-based quantum computers can have many physical realisations. However, *universal* (i.e. general-purpose) gate-based quantum computers realisations should satisfy the *DiVincenzo criteria* (named after the American theoretical physicist David P. DiVincenzo) for quantum computation, which are the following:

1. The physical system has well-characterised qubits and is scalable.

2. The physical system must be able to have the state of the qubits initialised to a known low entropy state.

3. The decoherence times of the physical system implementing the qubit must be much longer than the quantum gate operation time (Figure 3.6).

4. A physical system as the embodiment of a quantum computer must have available a universal set of quantum gates.

5. The physical system must have a qubit-specific measurement capability (preferably non-destructive).

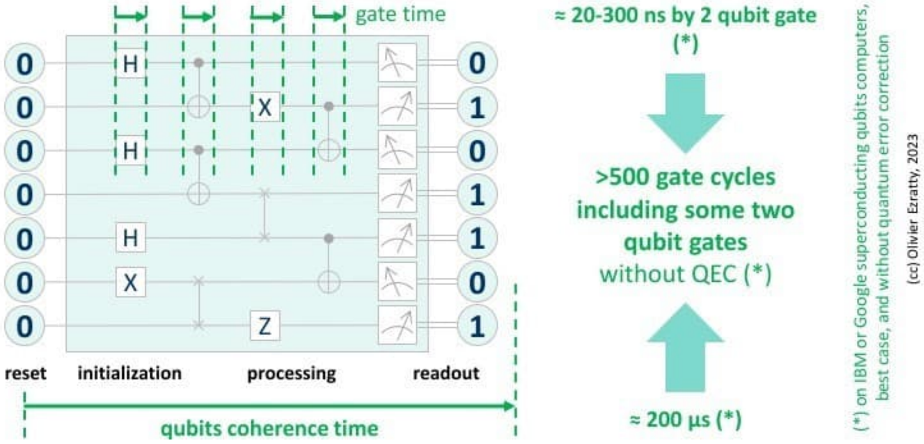


Figure 3.6: Qubit decoherence versus gate operation time (source: Olivier Ezratty 2023)

Qubits are vulnerable to perturbances caused by the environment in which they operate, causing decoherence of the qubit's quantum state. The time it takes for qubits to decohere, i.e. the qubit fidelity, is still very low for all qubit technologies currently being used for building quantum computers (Figure 3.7).

Note

Some renown scientists, including the Dutch theoretical physicist and Nobel Prize winner Gerardus 't Hooft, the Russian physicist Mikhail Dyakonov and the Israeli mathematician and computer scientist Gil Kalai, caution that building a universal quantum computer is most probably unfeasible because it is not an engineering problem but rather a fundamental scientific problem for which there exists no solution.

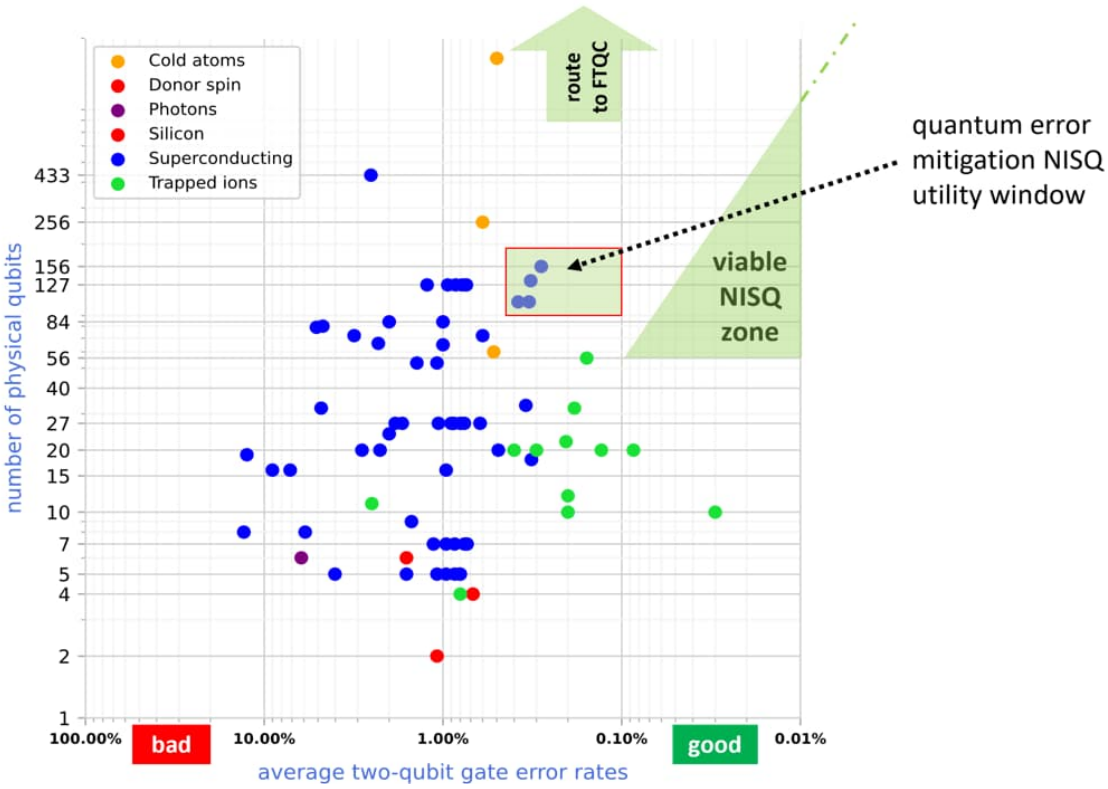


Figure 3.7: Qubit technologies qubit fidelities (source: Olivier Ezratty 2024)

A fundamental property of qubits is that they cannot be copied according to the quantum mechanics no cloning theorem, published by the American physicist James L. Park and independently by the American theoretical physicist William Kent Wootters and the Polish-American theoretical physicist Wojciech Hubert Zurek, at the same time as the Dutch physicist Dennis Geert Bernardus Johan Dieks.

The no-cloning theorem states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state, a statement which has profound implications in the field of quantum computing. This is very different from classical bits: copying bits is heavily used in modern computers which are based on the Von Neumann architecture (Box 3.6). This fundamental difference implies that the design of gate-based quantum computers will not be based on the Von Neumann architecture. It also has severe implications for the design of error correction mechanisms for quantum computers (see QEC below).

The Von Neumann architecture is a computer architecture based on a 1945 description by the American mathematician, physicist, computer scientist and engineer John von Neumann and a few others. It describes a design architecture for a digital computer system with the following components: a processing unit that contains an arithmetic logic unit and processor registers, a control unit that contains an instruction register and program counter, memory that stores data and instructions, external mass storage and input and output mechanisms.

Box 3.6: Von Neumann architecture

Quantum Error Correction (QEC) is seen as the solution to the qubit decoherence problem. QEC enables sets of noisy physical qubits (imperfect qubits) to emulate stable logical qubits (perfect qubits) so that the quantum computer behaves reliably for any quantum computation. However, QEC incurs significant overheads in terms of both the number of physical qubits required to emulate a logical qubit and the number of primitive qubit operations that must be performed on the physical qubits to emulate a reliable quantum operation on the logical qubit. The higher the physical qubit error rate, the more physical qubits must be assembled into one logical qubit. It should also be noted that non-Clifford quantum gates, the use of which is essential for achieving quantum speedup, are difficult to correct with QEC.

QEC has become a very rich scientific field of quantum technologies and has been growing regularly since 1995. Important QEC technologies are the Shor code and families of stabilizer codes and topological codes. Topological codes include toric codes, planar codes and surface codes. Currently, most QEC implementations are based on surface codes, many variants of which have been around for some time. Surface codes replicate neighbouring qubits several times with entanglement and then compare the results at the output of algorithms to keep the statistically dominant results; this is done without reading the value of the qubits (which would make the whole system collapse). QEC based on surface codes is implemented with so-called ancilla qubits that are used to detect error syndromes without affecting the qubits used in the calculation; see Figure 3.8 for an example.

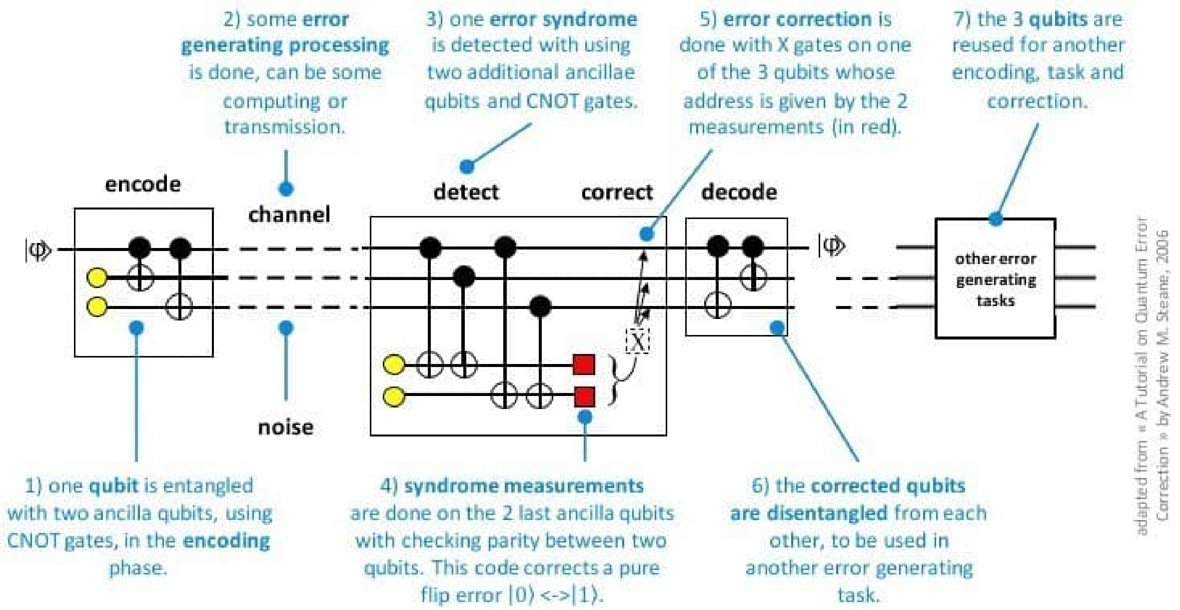


Figure 3.8: Example of a simple QEC code (source: Olivier Ezratty 2024)

Fault-Tolerant Quantum Computers (FTQCs) are quantum computers made more robust through deployment of QEC. It should be noted that non-Clifford quantum gates, which are essential for achieving quantum speed-up, are difficult to correct with QEC.

Noisy Intermediate-Scale Quantum (NISQ) computing is a term, coined by the American theoretical physicist John Phillip Preskill in 2018, that applies to current state-of-the-art quantum computers. The term “noisy” refers to the fact that these quantum computers are very sensitive to perturbances caused by the surrounding environment and may lose their quantum state due to quantum decoherence because they are not sophisticated enough to implement QEC. The term “intermediate-scale” refers to the not-so-large number of qubits.

Quantum Error Mitigation (QEM) denotes a collection of techniques that reduces quantum computing errors by combining classical post-processing (often based on quantum computation results) with quantum circuit modifications (optimisations), running quantum algorithms several times and averaging the single-run results. QEM is an intermediate solution that aims at increasing the computational power of for NISQ quantum computers.

Several QEM techniques are currently being used, including:

- randomized compiling;
- measurement-error mitigation;
- Probabilistic Error Cancellation (PEC);
- Zero-Noise Extrapolation (ZNE).

All of these QEM techniques incur some degree of (classical) computational overhead but they do not require the use of ancilla qubits as QEC does. QEM is <u>not</u> the same as quantum error suppression (Figure 3.9), which can be implemented in the quantum computer firmware and/or taken care of by appropriate quantum algorithm designs.

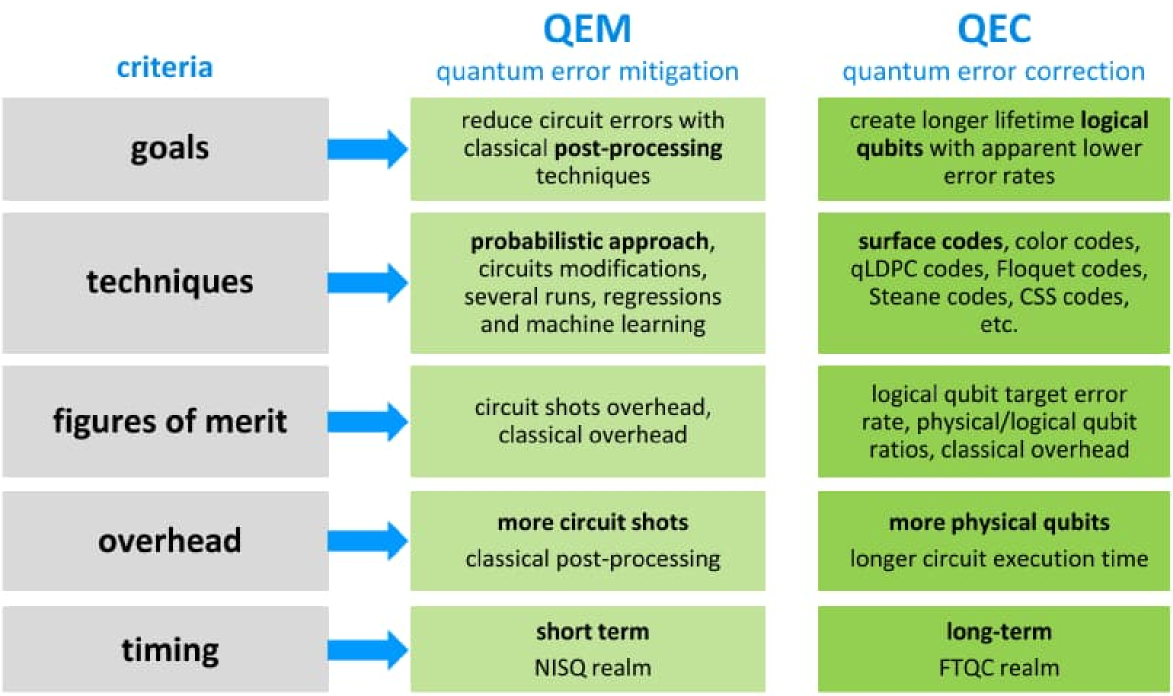


Figure 3.9: QEM compared to QEC (source: Olivier Ezratty 2024)

Regardless of the qubit technology being used, scaling up quantum computers (i.e. increasing the number of physical qubits) will require some sort of Quantum Processing Unit (QPU) interconnection technology (Figure 3.10)

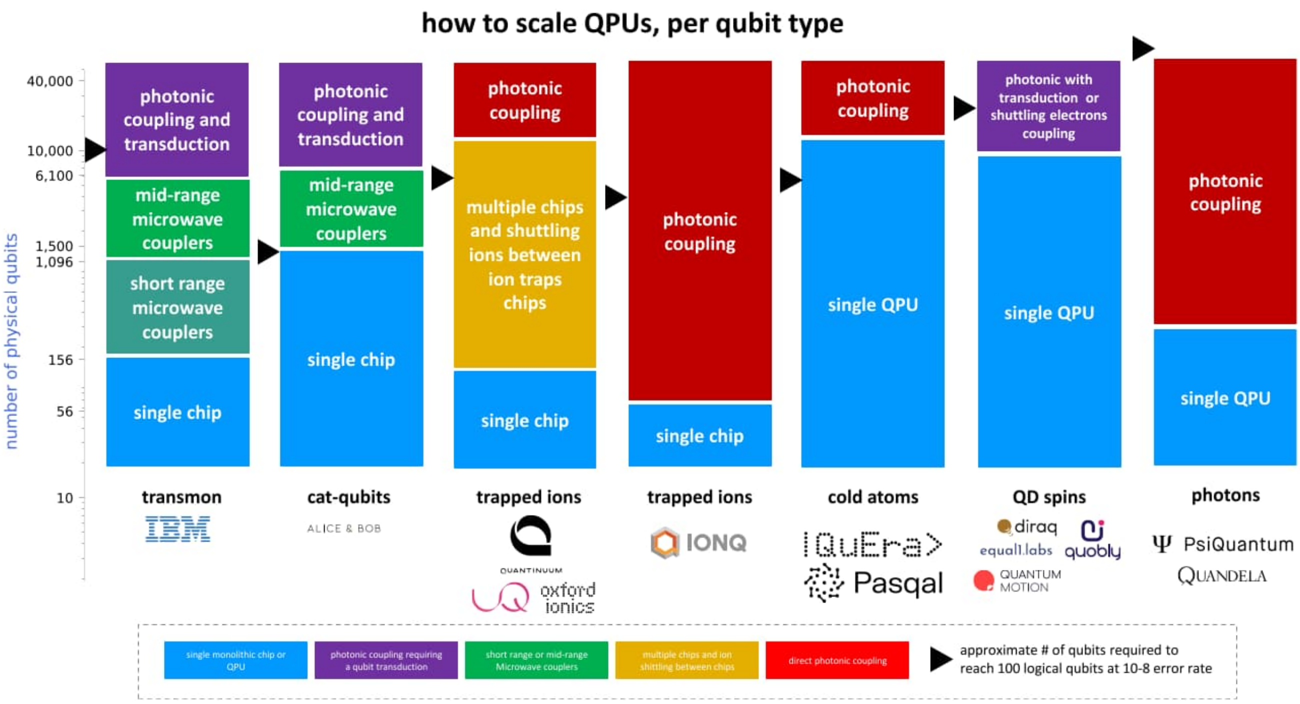


Figure 3.10: QPU interconnection (source: Olivier Ezratty 2024)

3.2. Quantum computer components

A typical quantum computer consists of the following components (Figure 3.11):

- quantum chipset (aka quantum processor): includes quantum register and qubits control devices (qubit reset, quantum gate operations and qubit readout);
- (optional, depending on the qubit technology): cryogenic installation, including a cryostat which keeps the qubit chipset and also part of its qubits control electronics and/or photonics subsystem at a temperature close to absolute zero (to avoid generating disturbances that contribute to qubit quantum state decoherence);
- (external part of) qubits control electronics and/or photonics;
- classical computers;
- networking components.

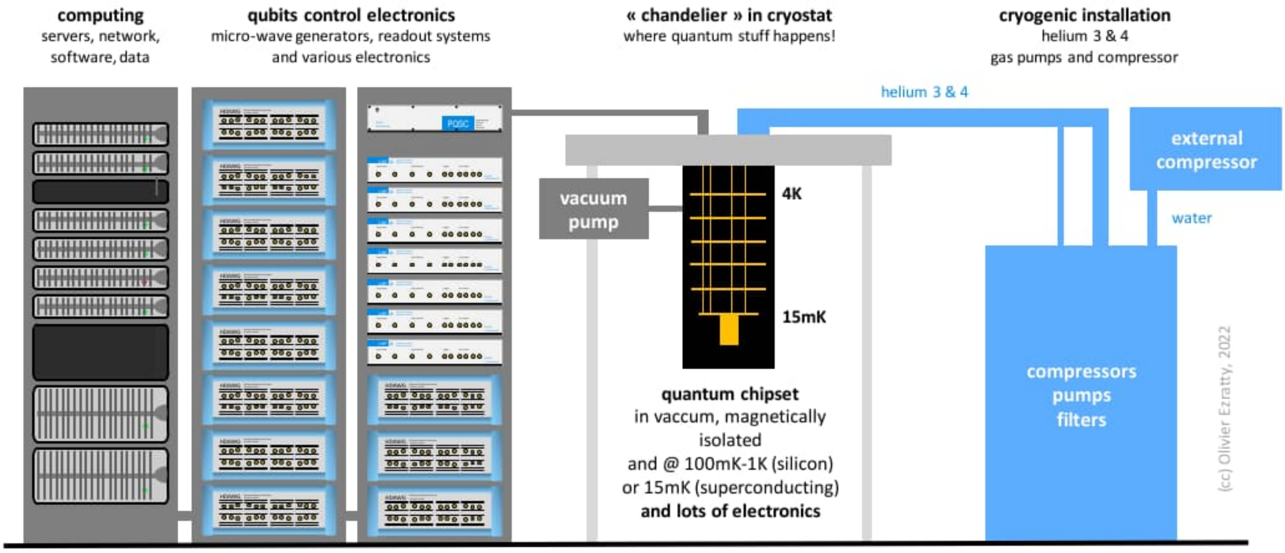


Figure 3.11: Components of a typical superconducting qubit-based quantum computer

The qubits control electronics and/or photonics subsystem closely controls the operation of the quantum processor by triggering at a precise rate the qubit resets, quantum gate operations (Figure 3.12) and qubit readouts (Figure 3.13) that are performed by the qubits control devices. This is done by creating various direct current, microwave or laser signals that are sent to these devices. It also takes into account quantum gate execution time and the known qubit coherence time, i.e. the time during which the qubits remain in a state of superposition and entanglement. A classical computer system is always needed to orchestrate all of these tasks.

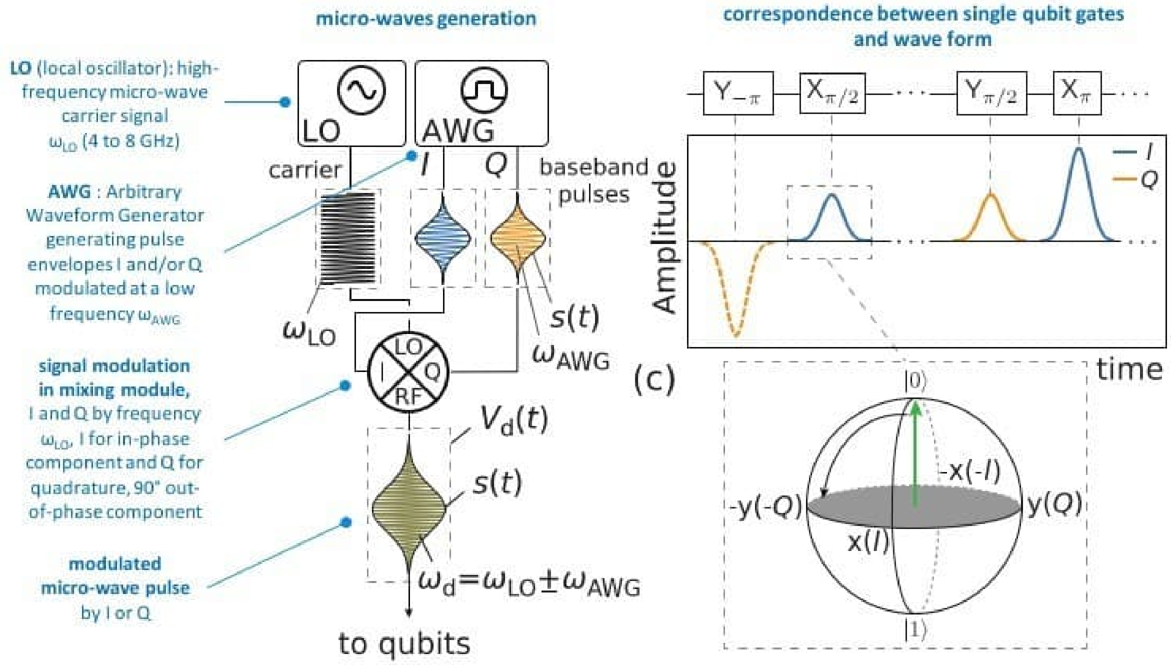


Figure 3.12: Typical control signals for superconducting quantum gate operations (source: P. Krantz et al. 2019)

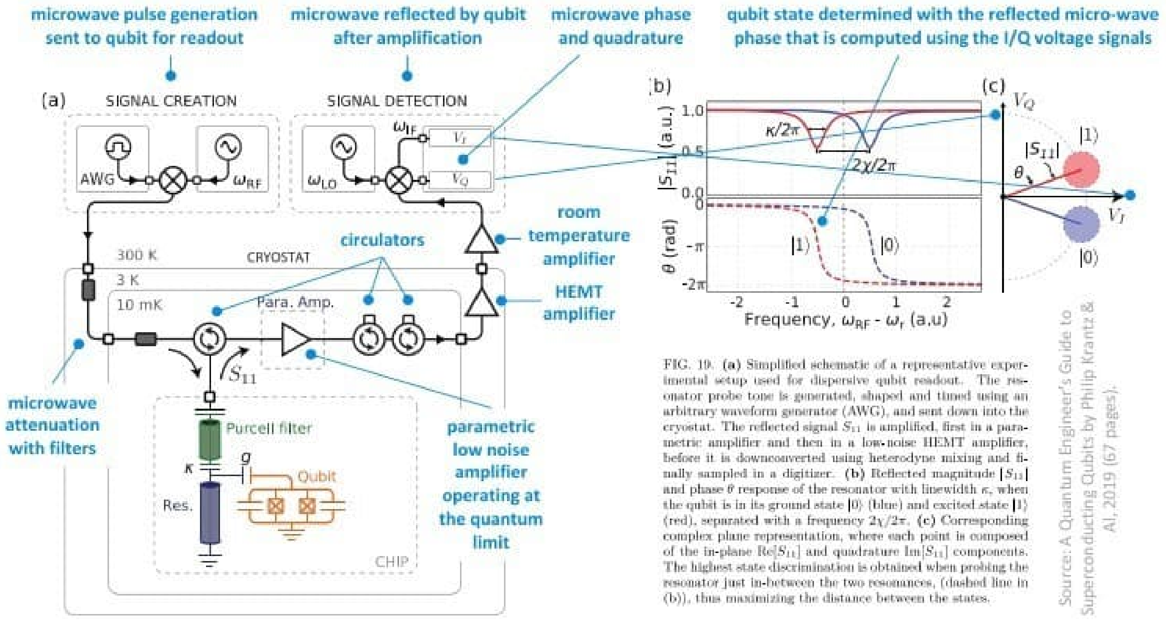


Figure 3.13: Typical control signals for superconducting qubit readouts

The classical computer system is also needed when performing hybrid classical/quantum computing. This will typically involve the combination of quantum computing tasks with High-Performance Computing (HPC) and/or AI (Artificial Intelligence) computing tasks.

Networking, possibly including internet connectivity, is handled by the networking components.

3.3.Quantum emulators and resource estimators

Due to the difficulty of building quantum computers and the limited access to the few real quantum computers currently available, a growing body of quantum emulators has emerged to assist in the tasks of designing quantum algorithms and associated quantum circuits. When new quantum algorithms are being developed, it is generally advisable to conduct the initial proof-of-concept validation with a quantum emulator.

Note

Quantum emulators are often called “quantum simulators” but this is not the right term. Simulation is the imitation of the operation of a system over time and is based on a model which represents its key characteristics and behaviours. Simulation is used for various purposes, e.g. testing, optimising, performance tuning, etc. of technology being designed, the study of physical systems based on scientific modelling of these systems, etc. Emulation is a technique that enables one system (the emulator) to behave (almost) exactly like another system (the target). The Church-Turing thesis (named after the American computer scientist, mathematician, logician and philosopher Alonzo Church, and the British mathematician, computer scientist, logician, cryptanalyst, philosopher and theoretical biologist Alan Mathison Turing) implies that, in theory, any computing environment can be emulated within any other computing environment, assuming memory limitations are ignored. Use of the term “quantum simulator” creates confusion with quantum simulator systems, i.e. analogue quantum computers used for simulating quantum mechanical systems (the quantum computers that Richard Feynman had in mind when he introduced the term “quantum computer” in 1981).

There are several types of quantum emulators, including:

- Density Matrix (DM)-based: using DMs for representing mixed quantum states, which allows for the emulation of imperfect qubits (i.e. qubits affected by noise and decoherence) but is also the most resources-hungry emulation method.
- State Vector (SV)-based: representing pure quantum states by quantum state vectors, which only allows for the emulation of perfect qubits (i.e. qubits that are not affected by noise and decoherence) but is far less resources-hungry.
- Tensor Network (TN)-based: using TN compression techniques, which significantly reduces the complexity of the emulation software and also allows for the distribution of the emulation program execution over a cluster of classical computing nodes.

The amount of computing resources required for the emulation of a quantum circuit heavily depends on the number of qubits to be emulated and also on the depth of the quantum circuit (i.e. the number of quantum gates). The main limitation of classical computers for quantum circuit emulation is the amount of available computer memory (RAM) rather than CPU capacity.

Resource estimators are software tools designed to estimate the quantum computing hardware resources using as inputs a given algorithm and the various hardware characteristics.

3.4.Quantum computing software

When developing quantum applications, the problem to be solved by the use of quantum computing must be determined first. After the problem has been analysed and properly understood, the next step is to design the quantum algorithm (see § 3.5) and then design and specify the corresponding quantum circuit, i.e. the set of qubits, the sequence of operations (quantum gates) to be performed on these qubits, and the qubit measurements yielding the (classical) outcome of the quantum computation. Many different quantum software development tools can be used for this purpose. Most of these tools can produce the source code of the quantum circuit according to one of the available quantum programming languages.

After the quantum source code has been obtained, it is usually integrated into a classical program by embedding it in a program developed with a quantum programming language derived from a classical programming language. The resulting program source code must then be compiled into machine language for execution on the physical classical/quantum computing platform.

Quantum computers are complex systems that should typically not be directly handled by quantum software developers. Instead, to take advantage of the power of these devices, a stack of software layers that abstracts the quantum computer from these developers is required (Figure 3.14).

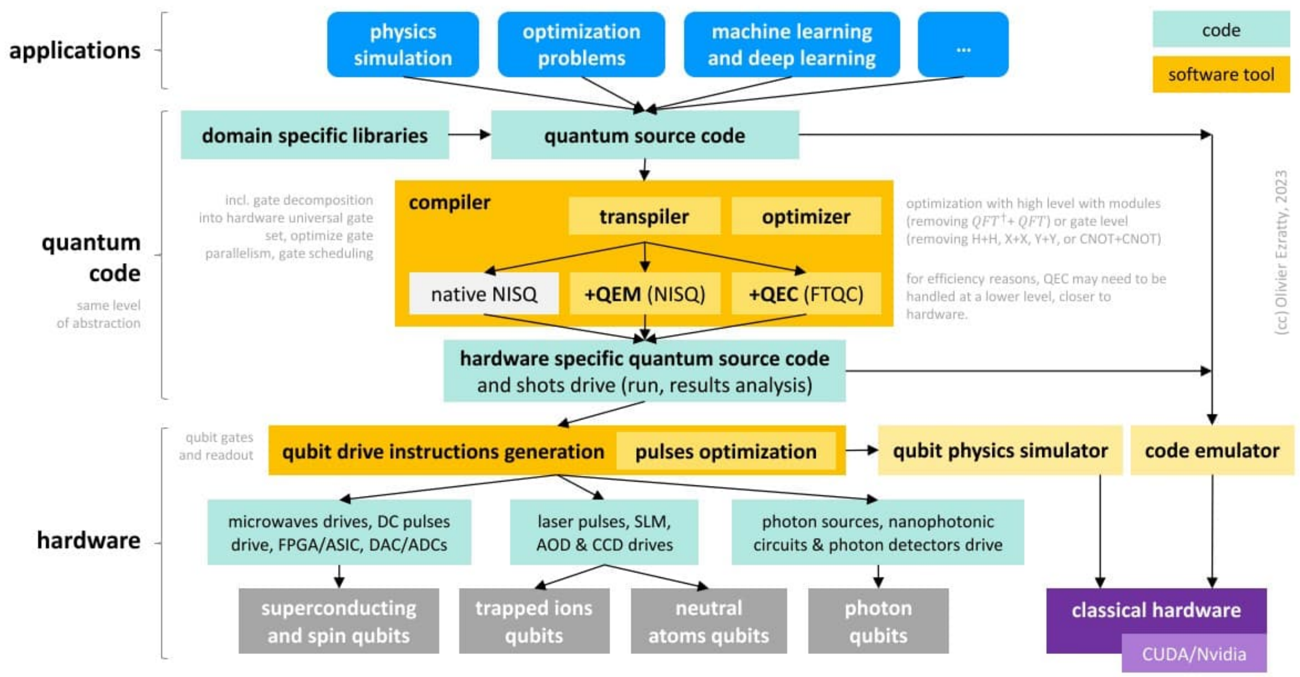


Figure 3.14: Quantum computing stack (source: Olivier Ezratty 2023)

Programming and compilation are the nontrivial tasks of converting an algorithm's abstract mathematical description to an implementation that is executable on a physical computer. Programming languages support this process by offering syntax to support the natural expression of key concepts and operations. Programming for quantum computers requires very different concepts and operations than programming for classical computers, and as such requires new languages and a distinct set of tools. For example, designing a language that enables a programmer to exploit quantum interference in a quantum algorithm is a unique and nontrivial challenge.

There are several levels of abstraction in quantum software, so several layers of programming languages are required. At the highest level, a programming language should enable a user to easily and rapidly program an algorithm, while ideally shielding the programmer from detailed underlying hardware specifications. This abstraction of detail is helpful both because it can help mitigate the massive complexity of these systems and also because it can lead to more device-independent and portable software. Current prototype languages enable developers and programmers to interact with quantum hardware through a high-level language that is at least somewhat device independent.

At the lowest level, a language must be able to interact seamlessly with the hardware components and give a complete specification of the physical instructions necessary to execute a program at speed. While some low-level languages are used at present to program devices directly, the long-term vision and goal for quantum computing is to absorb such languages into automated tool flows. As in classical computers, the goal is to have lower-level quantum computer device orchestration be automatically generated, and to abstract such low-level information away from the programmer.

Similar to early stages of a classical computing ecosystem, the current state of play in quantum computer software includes many languages and tools in development both commercially and academically (several of them being open-source efforts). With the recent industry push toward larger quantum computer prototypes (including availability on public clouds for broad use), there is an increased awareness of the need for full-stack quantum computing software and hardware in order to encourage usage and nurture a developer community around quantum software and hardware. Thus, it is reasonable to expect that quantum programming languages and software ecosystems will receive considerable attention and may see significant changes in coming years.

3.5.Quantum algorithms

The qubits of a quantum computer have amplitudes for the possibility that their measured value is “0”, and different amplitudes for the possibility that it is “1”. The trick in devising an algorithm for a quantum computer is to choreograph a pattern of constructive and destructive interference for its qubits, so that for each wrong answer the contributions to these qubit amplitudes cancel each other out, whereas for the right answer the contributions reinforce each other. If, and only if, that can be arranged, the right answer will be obtained with a large probability when reading the quantum computer’s qubits. The difficulty is to do this without knowing the answer in advance and, of course, significantly faster than could be done with a classical computer.

Quantum computing is inherently probabilistic, requiring executing several times a quantum calculation and averaging the obtained results. One run of a quantum algorithm is probabilistic but by running the quantum algorithm many times, progressive convergence to a deterministic solution will be achieved (the solution being the average of all run results). The number of runs needed is typically in the order of hundreds or thousands. Experience shows that this number will grow with the number of qubits (hopefully only linearly).

In general, three types of problems are well-suited for solving with quantum computing: simulation, optimisation and machine learning. A large number of (generic) quantum algorithms have already been conceived.

Today, many of the quantum algorithms that have been invented are not yet executable on a large problem scale on current NISQ quantum computers or on quantum emulators. There are simply not enough qubits with high fidelity (error-corrected qubits) available for NISQ quantum computers to be more powerful than classical computers.

Instead of waiting for the availability of powerful FTQC quantum computers, researchers have investigated approaches for taking advantage of currently available NISQ quantum computers. A promising approach is to forgo the desire to obtain an exact solution for the computational problem and instead use an approximate, or heuristic, approach to solve the problem. This approach has given rise to a number of quantum and hybrid quantum-classical algorithms for tasks that range from the simulation of many-body systems such as molecules and materials, to combinatorial optimisation and machine learning applications. The goal of these approaches is to provide approximate but nevertheless useful solutions to the problem at hand, with significantly lower quantum resource requirements than other approaches. The most famous of these algorithms are the so-called Variational Quantum Algorithms (VQAs).

The quantum speedup, i.e. the acceleration provided by a quantum algorithm compared to the best-in-class classical algorithm for solving a particular "hard" problem, depends on the types of quantum gates used by the quantum algorithm. Besides using non-Clifford quantum gates, quantum algorithms also provide exponential speedup if they handle maximally entangled states, which means that there is a correlation of states between a set of qubits in the qubit register until the end of the quantum computing.

To outperform their classical counterpart(s), quantum algorithms must demonstrate polynomial speedup or superpolynomial speedup, either weakly superpolynomial or strongly superpolynomial (aka exponential). There are only a few dozen known quantum algorithms supposed to be capable of achieving such speedups and furthermore, only a small fraction of these algorithms is commonly used in quantum applications.

The term quantum supremacy was introduced in 2012 by John Preskill as "the point where quantum computers can do things that classical computers can't, regardless of whether those tasks are useful". According to Preskill's definition, quantum supremacy refers to a point in time rather than an ongoing phenomenon, but it is of course still a moving target as quantum computing technology is evolving. Quantum advantage on the other hand is the goal of demonstrating that a quantum computer can solve a practical problem that no classical computer can solve in any feasible amount of time. Conceptually, quantum advantage involves both the engineering task of building a powerful quantum computer and the computational complexity-theoretic task of finding a problem that can be solved by that quantum computer and has more than polynomial speedup over the best known or possible classical algorithm for that task.

While quantum computers give us the opportunity to directly explore a variety of quantum algorithms and applications, currently available quantum computers have not yet demonstrated quantum advantage with real-world impact, and we are not confident that we have identified an application that will allow us to demonstrate quantum advantage in the short term.

3.6.Quantum computer benchmarking

The goal of quantum computer benchmarking is to evaluate quantum computers for multiple purposes in different contexts:

- comparing commercially available quantum computers;
- determining suitability for specific problem-solving quantum algorithms;
- comparing quantum computing with classical computing[3], e.g. for assessing potential quantum advantage and for cost-benefit analysis;
- estimating the rate of technological progress over time (e.g. to estimate short/medium term projections);
- etc.

Three different types of quantum computer benchmarking are distinguished:

1. component-level benchmarking aka device benchmarking or subsystem benchmarking

   Component-level benchmarking is concerned with metrics related to the performance of quantum computers at the physical level. These low-level metrics address the various characteristics of a quantum computer's qubits.

2. system-level benchmarking aka aggregated benchmarking

   Most system-level benchmarks are based on determining the performance metrics of a quantum computer by measuring its behaviour while executing a set of carefully selected

[3] It should be noted that both are “moving targets”!

quantum circuits, which is believed to be representative for the load that quantum computers will be subjected to in practice.

3. application-level benchmarking

   Due to the complexity of errors in quantum hardware, neither a quantum computer's component-level benchmark nor system-level benchmark nor any other single metric is likely to accurately predict its performance for all problem-solving quantum algorithms corresponding with real-world applications. There is thus a need for application-centric metrics and benchmarks that test the performance of quantum computers on practically relevant tasks. Application-level benchmark suites fulfil this need.

Appendix A - Qubit technologies and manufacturers

Important distinguishing characteristics (metrics) of qubit technologies are:

- qubit fidelity (aka qubit stability) refers to T_1 (qubit coherence time aka bit-flip error) and T_2/T_{2*} (qubit dephasing time aka phase-flip error); see Figure A.1.

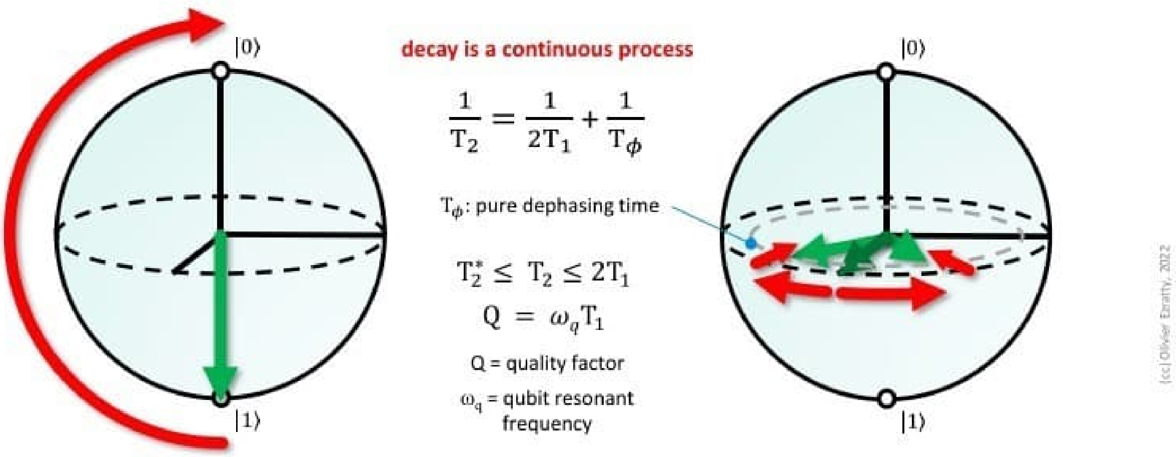


Figure A.1: Flip errors and phase errors (source: Olivier Ezratty 2022)

- quantum gate fidelity refers to the error rate that is associated with single-qubit and two-qubit quantum gate operations.

- trace distance refers to differences in phase which can be overlooked by the gate fidelity metric.

- qubit readout fidelity (aka qubit measurement fidelity) refers to the error rate associated with qubit readout operations.

- quantum gate execution time (aka quantum gate speed) refers to the time needed to perform quantum gate operations.

- qubit readout execution time (aka qubit readout speed) refers to the time needed to perform qubit readout operations.

- qubit reset execution time (aka qubit reset speed) refers to the time needed to set the qubit's quantum state to its ground state (|0⟩) or a chosen basis state.

- qubit connectivity refers to the way in which qubits can be linked together.

- qubit entanglement scope refers to entanglement not being limited to immediately neighbouring qubits.

- qubit connectivity (i.e. the way in which qubits can be linked together) and scope of qubit entanglement (i.e. not being limited to the immediately neighbouring qubits). These characteristics will condition many parameters such as the depth of the quantum algorithms that can be exploited and their run time.

- qubit density and qubit control electronics/photonics density, both of which impact scalability.

- operating temperature for the qubits and for the accompanying control electronics and/or photonics subsystems.

- manufacturing process characteristics, which depend on a wide range of parameters.

The scalability potential of a particular qubit technology depends on many system parameters, both at the fundamental level with the qubit stability and fidelities at large scale, but also with the various enabling and manufacturing technologies.

Note
When evaluating and comparing quantum computers, vendors and (social) media often put emphasis on the number of qubits. However, as should be clear from the list above, this is a rather deficient metric for such evaluation and comparison purposes.

Currently, qubits are based on a limited number of totally different types of quantum systems:

- natural two-state quantum systems, such as for example electron spins and photon polarisations;

- natural quantum systems with multiple discrete variable states, such as for example ions and atoms;

- natural quantum systems with continuous variable states, such as for example light waves consisting of multiple photons;

- engineered "atomic-scale" quantum systems, such as for example artificial defects (aka vacancies) created in crystalline structures;

- engineered "miniature" quantum systems, such as for example superconducting current loops and superconducting nanowires.

Multiple qubit technologies (each with several variants) are being developed and/or deployed for building quantum computers. These qubit technologies can be classified as follows:

- controlled atoms:
  - trapped ion;
  - neutral atom (aka cold atom);
  - Nuclear Magnetic Resonance (NMR);

- controlled electrons:
  - superconducting:
    - Josephson junction;
    - bosonic;
  - electron spin (aka quantum dot);
  - cavity spin;
  - topological;

- photonic (controlled photons).

Table A.1 provides an (incomplete) list of various qubit technologies. The choices for the basis $|0\rangle$ and $|1\rangle$ in the 4th and 5th column are those that are commonly used for the qubit technology as indicated in the 2nd column.

Physical support	Name	Information support	$\lvert 0\rangle$	$\lvert 1\rangle$
Photon	Polarization encoding	Polarization of light	Horizontal	Vertical
	Number of photons	Fock state	Vacuum	Single photon state
	Time-bin encoding	Time of arrival	Early	Late
Coherent state of light	Squeezed light	Quadrature	Amplitude-squeezed state	Phase-squeezed state
Electrons	Electronic spin	Spin	Up	Down
	Electron number	Charge	No electron	Two electron
Nucleus	Nuclear spin addressed through NMR	Spin	Up	Down
Neutral atom	Atomic energy level	Spin	Up	Down
Trapped ion	Atomic energy level	Spin	Up	Down
Josephson junction	Superconducting charge qubit	Charge	Uncharged superconducting island (Q=0)	Charged superconducting island (Q=2e, one extra Cooper pair)
	Superconducting flux qubit	Current	Clockwise current	Counterclockwise current
	Superconducting phase qubit	Energy	Ground state	First excited state
Singly charged quantum dot pair	Electron localization	Charge	Electron on left dot	Electron on right dot
Quantum dot	Dot spin	Spin	Down	Up
Gapped topological system	Non-abelian anyons	Braiding of Excitations	Depends on specific topological system	Depends on specific topological system
Vibrational [15]	Vibrational states	Phonon/vibron	$\lvert 01\rangle$ superposition	$\lvert 10\rangle$ superposition
van der Waals heterostr [16]	Electron localization	Charge	Electron on bottom sheet	Electron on top sheet

Table A.1: Comparison of qubit technologies (source: Wikipedia 2023)

The relative matureness of these qubit technologies is shown in Figure A.2 and Table A.3 below.

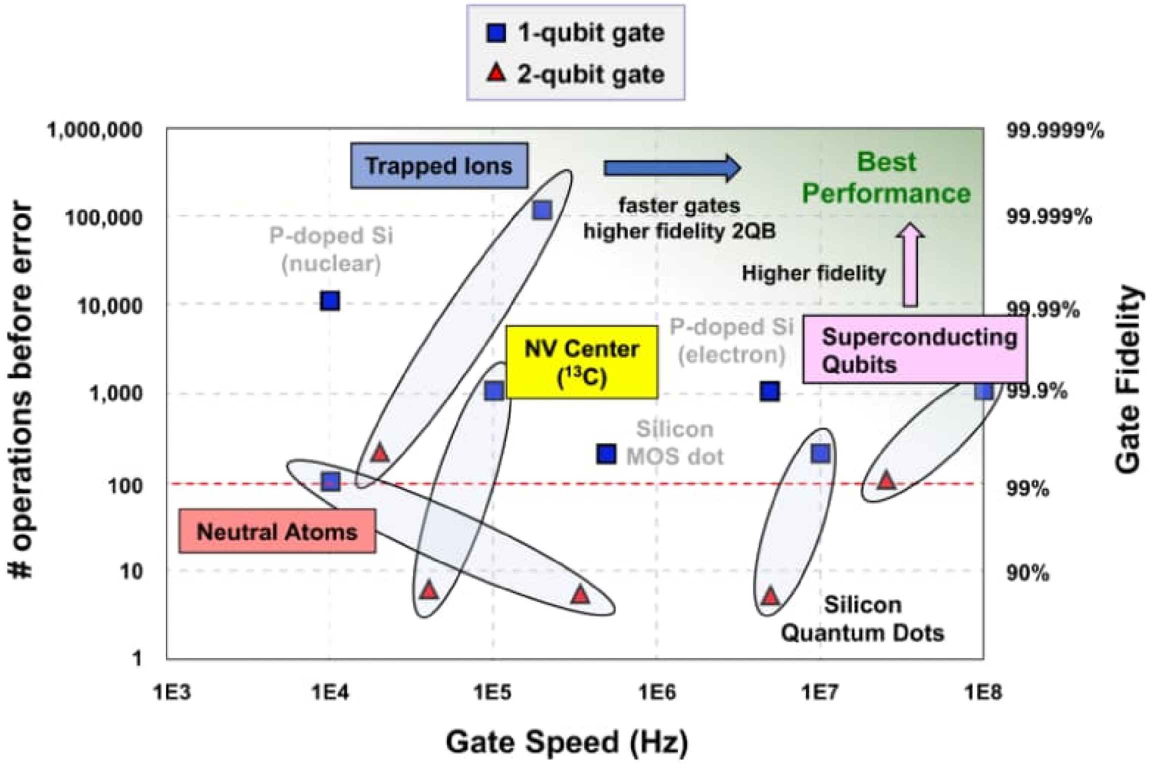


Figure A.2: Comparison of qubit technologies (source: Engineering Quantum Computers 2023)

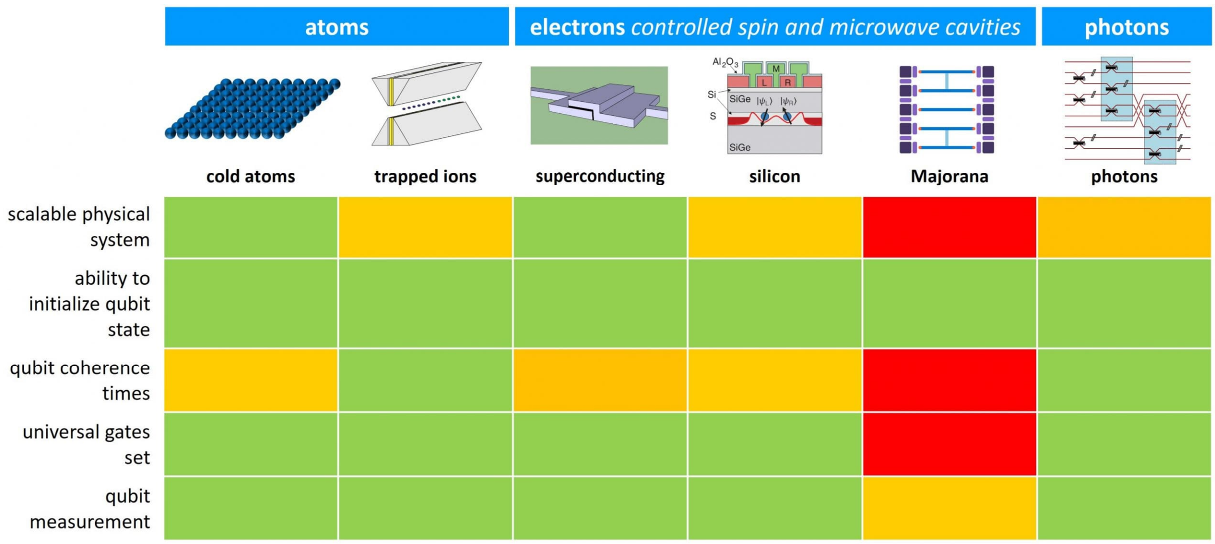


Table A.2: Comparison of qubit technologies (source: Olivier Ezratty 2024)

Sections A.1 through A.6 provide a brief description of prevalent qubit technologies and their manufacturers (according to the taxonomy described above).

Note that one could define alternate qubit technology taxonomies because there is some overlap between these technologies (Table A.3)

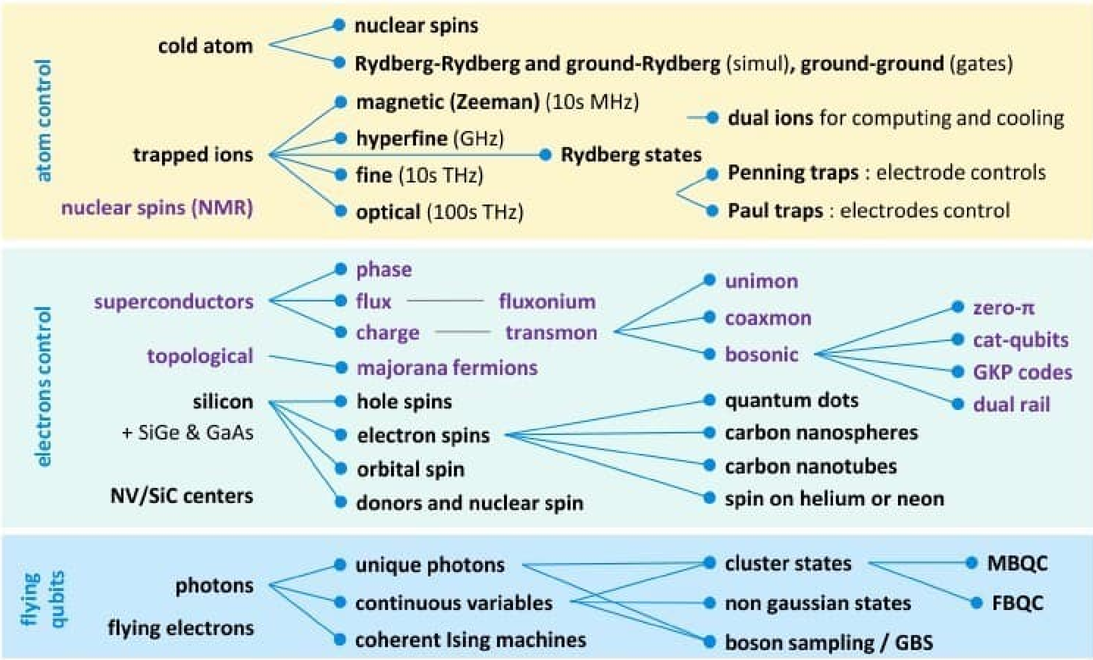


Table A.3: Alternate qubit technology taxonomy (source: Olivier Ezratty 2023)

A.1 Controlled atom qubits

Controlled atom qubits can be divided into three main types: trapped ion qubits, neutral atom qubits, and NMR qubits.

1. Trapped ion qubits use two internal states of an atom as their basis quantum states. The atoms are each stripped of an outer electron, leaving them as positively charged ions so that their positions can be controlled with electrical fields in devices called ion traps.

   Both the ions and the ion traps are contained in ultra-high vacuum chambers to minimise interaction with the environment. Lasers are used to cool the motion of the ions down to very low temperatures (0.1-1 mK). Although the ion traps typically operate at room temperature, they can also be cooled to cryogenic temperatures (4-10 K) to improve the vacuum environment and/or reduce the impact of intrinsic electrical noise on the ion's motion.

   The state of each ion can be changed by using precisely controlled laser or microwave pulses. These pulses can also be arranged to couple the states of two or more ions together to create entanglement between them.

   Manufacturers of trapped ion-based quantum computers (in alphabetical order):
   - Alpine Quantum Technologies/AQT (Austria): 24-qubit PINE system;
   - Aquabits (Canada);
   - Crystal Quantum Computing (France);

- eleQtron (Germany);
- Foxconn (Taiwan);
- IonQ (US): 11-qubit Harmony system, 25-qubit Aria system and 32-qubit software-configurable Forte and Forte Enterprise systems (with 64-qubit Tempo system planned in 2025);
- neQxt (Germany);
- NextGenQ (France)
- Oxford Ionics (UK);
- Quantum Art (Israel);
- Quantum Factory (Germany);
- Quantinuum (US/UK[4]): 6-qubit H0 system, 10-qubit H1 system, 12-qubit H1-2 system, 20-qubit H1-1 system and 32-bit H2 system;
- QUDORA Technologies (Germany);
- Rosatom (Russia): 20-qubit quantum computer (50..100 qubits expected in the near future);
- Universal Quantum (UK).

2. Neutral atom qubits (aka cold atom qubits) are an approach for qubits that is very similar to trapped ions, but instead of using ionised atoms and exploiting their charge to hold the qubits in place, neutral atoms and laser tweezers are used. Like for trapped ion qubits, microwave pulses are used for qubit manipulation, with lasers also being used to cool the atoms before computation.

   Manufacturers of neutral atom-based quantum computers (in alphabetical order):
   - Atom Computing (US): 1,125 physical-qubit system and 28 logical-qubit system (integrated into Microsoft's Azure Quantum cloud service);
   - ColdQuanta/Infleqtion[5] (US): 100-qubit Hilbert system;
   - GDQLABS (India);
   - M Squared Lasers (UK): 100-qubit Maxwell system;
   - NanoQT (Japan);
   - Pasqal (France): 324-qubit Fresnel system (10,000 physical qubits and hundreds of logical qubits planned in 2027);
   - planq (Germany): still under development;
   - QUANTier (China);
   - QuEra Computing (US): 256 physical qubit software-configurable Aquila system (100 logical qubits expected in 2026).

[4] Quantinuum is the result of a merger of the quantum computer hardware vendor Honeywell Quantum Systems/HQS (US) and the quantum computer software vendor Cambridge Quantum Computing/CQC (UK).

[5] In 2022, ColdQuanta created a new umbrella brand Infleqtion. ColdQuanta became the dedicated research branch of Infleqtion.

3. Nuclear Magnetic Resonance (NMR) qubits use the spin of atomic nuclei within large assemblies of up to 10^{15} molecules as their basis quantum states. Qubit readout is performed using nuclear magnetic resonance. At the moment, the Chinese company SpinQ Technology is the only manufacturer of NMR quantum computers. They sell a desktop version suitable for learning purposes (currently a 2-qubit system that will eventually be extended to 15 qubits).

A.2 Superconducting qubits

Superconducting qubits can be divided into two main types: Josephson junction-based qubits and bosonic qubits.

1. Josephson junction-based qubits are built using the unique properties of superconducting materials. Josephson junctions (named after the British physicist Brian David Josephson) are nanometric insulating barriers between two superconducting metallic layers (electrodes), creating a quantum tunnel junction.

   The supercurrent through the junction is driven by the phase difference between the electrodes. At temperatures well below the superconductivity critical temperature, Josephson junctions embedded in an electrical circuit[6] behave as an “artificial atom” (miniature quantum system), with about 10^{11} electrons forming Cooper pairs (Box A.1).

   > A Cooper pair, aka Bardeen–Cooper–Schrieffer (BCS) pair (named after the American physicist John Bardeen, the American theoretical physicist and neuroscientist Leon N. Cooper and the American physicist John Robert Schrieffer), is a pair of electrons bound together at low temperatures. The electrons in a Cooper pair are not necessarily close together; because the interaction is long range, paired electrons may still be many hundreds of nanometres apart. This distance is usually greater than the average interelectron distance so that many Cooper pairs can occupy the same space. Therefore, unlike “common” electrons, multiple Cooper pairs are allowed to be in the same quantum state, which is responsible for the phenomenon of superconductivity.

   Box A.1: Cooper pair

   Microwave pulses are used to manipulate the state of these artificial atoms and adjacent qubits can be electronically coupled together to create entangled states. Unfortunately, the energy levels in these circuits are still very small and furthermore, these circuits are always in contact with the material that they are built on. Isolating these circuits therefore requires cooling them to approximately 10 mK.

   Since the superconducting circuit can be defined lithographically in the same way as common IC components, it is possible to build arrays of these qubits using a process similar to that used for manufacturing ICs.

[6] Not be confused with a quantum circuit!

Josephson junction-based qubits can be further subdivided into phase qubits, charge qubits, flux qubits, coaxmon qubits, unimon qubits and ASQ qubits.

- Phase qubits use two levels of current energy of large Josephson junctions as the qubit basis quantum states. No vendor is developing this type of superconducting qubit.

- Charge qubits use electrical current flow thresholds in the Josephson junctions as the qubit basis quantum states. Small Josephson junctions delimit a superconducting island with a well-defined electrical charge. The quantum states of charge qubits are the states of these islands in Cooper pairs. The most common variant is the transmon qubit. Transmon qubits are either single-junction transmons (a single Josephson junction) or split transmons (two Josephson junctions connected in parallel).

  Manufacturers of transmon qubit-based quantum computers (in alphabetical order):
  - Google Quantum AI (US): the number of (split transmon) qubits increased steadily from 9 in 2016 to 53 in 2019; the latest version of their quantum computer (based on the Willow chip) has 72 or 105 qubits and Google plans to scale up to 1 million qubits in 10 years from now;
  - IBM Q (US): the number of (single-junction transmon) qubits increased steadily from 5 in 2016 to 1,121 in 2023; a 1,386-qubit system (Flamingo) is planned for 2025 and a 4,158-qubit system (Kookaburra) is planned for 2027, a system with 200 logical qubits (Starling) is planned for 2029 and system with 2,000 logical qubits (Blue Jay) is planned for 2033 or later;
  - QuantWare/QW (The Netherlands): Tenor-64 64-qubit quantum computer (100 qubits expected in 2028);
  - Toshiba (Japan): double-transmon coupler technology.

- Flux qubits are micron-sized superconducting loops where electrical current can flow clockwise or counter-clockwise, corresponding with the qubit's basis quantum states.

  Manufacturers of flux qubit-based quantum computers (in alphabetical order):
  - Alibaba (China): 11-qubit quantum computer;
  - Atlantic Quantum (US/Sweden);
  - Bleximo (US): Vortex 8 TQ 8-qubit quantum computer;
  - D-Wave Systems (Canada): already produced five generations of quantum annealers (128-qubit D-Wave One, 512-qubit D-Wave Two, 1,000-qubit D-Wave 2X, 2,048-qubit D-Wave 2000Q and 5,640-qubit Advantage); a 7,440-qubit Advantage 2 system has been announced for 2023-2024;
  - Qilimanjaro Quantum Tech (Spain): quantum annealer (under development);
  - Rigetti Computing (US): the number of qubits increased steadily from 8 in 2015 (Agave system) to 84 in 2023 (Ankaa-2 system). A 336-qubit system (Lyra) is expected in late 2024.

- Coaxmon qubits are composed of highly planar qubits, use a 3D structure connecting the quantum chipset with an interposer (a layer above the chipset for qubit control and another layer below the chipset for qubit readout). Oxford Quantum Circuits/OQC (UK) has built an 8-qubit coaxmon quantum computer.

- Unimon qubits use a single Josephson junction in a resonator. IQM (Finland) has delivered a 20-qubit unimon quantum computer to VTT and has announced the release of a 54-qubit quantum computer (Radiance) in 2024 and a 150-qubit variant in 2025.

- Andreev Spin Qubit (ASQ) qubits, named after the Russian physicist Alexander Fyodorovich Andreev, rely on the two levels of a localised microscopic excitation of a nanowire-based BCS condensate as the qubit's basis quantum states. ASQ quantum computers are still being researched, e.g. by QuTech (The Netherlands).

2. Bosonic qubits are a broad category of qubits that are more resilient to noise (i.e. fault-tolerant). This category contains cat qubits and GKP qubits:

   - Cat qubits (named after Schrödinger's Cat) use microwave cavities, using two coherent states of microwaves of same amplitude and opposite phase as the qubit's basis quantum states. The cavities are connected to a transmon qubit that is used only for their preparation, readout and/or correction. Cat qubits are more complex to design and operate but it would only take about 30 physical qubits to create a (perfect) logical qubit, which would enable a better scalable architecture than other superconducting qubits. Cat qubits have been implemented by Alice&Bob[7] (France) and are under development at Amazon (US), Nord Quantique (Canada) and Quantum Circuits Inc./QCI (US).

   - Gottesman-Kitaev-Preskill (GKP) qubits named after Daniel Gottesman, Alexei Kitaev and John Preskill, use oscillator states as the qubit's basis quantum states. The GKP codewords are coherent superpositions of periodically displaced squeezed vacuum states. The GKP code was for a long time considered to be impractical. However, developments in quantum technology during the last two decades have put GKP qubits back in the race to build bosonic qubits.

Other manufacturers of superconducting qubit-based quantum computers, of which the precise superconducting technology that is used has not been determined, are (in alphabetical order):

- Academia Sinica (Taiwan): 5-qubit quantum computer;
- Anyon Systems (Canada);
- Baidu (China): 10-qubit quantum computer;
- China Telecom Quantum Group (China): 504-qubit Tianyan-504 quantum computer,
- ConScience (Sweden): 4-qubit Qubit-in-a-Box 0 (QiB0) quantum computer;
- DY-SLQT and TFIR (India): 6-qubit quantum computer;

[7] In December 2023, Alice&Bob announced a 16-qubit QPU (Helium 1) that integrates cat qubits for QEC. A 100 logical qubit system is expected in 2030.

- Fujitsu/RIKEN (Japan): 64-qubit quantum computer (with 1,000 qubits planned in 2026);
- IAI and Yssum (Israel): 20-qubit quantum computer;
- NEC (Japan): 8-qubit quantum annealer;
- Origin Quantum Computing (China): 198-qubit Wukong quantum computer (72 computational qubits and 126 coupler qubits);
- RIKEN (Japan): 53-qubit quantum computer;
- SEEQC (US): 5-qubit quantum computer (System Red);
- SpinQ Technologies (China): 20-qubit quantum computer;
- USTC (China): 62-qubit Zuchongzhi system, 66-qubit Zuchongzhi 2.1 system and 255-qubit Jiuzhang 3 (prototype) system[8];
- VTT/IQM (Finland): 20-qubit quantum computer (50 qubits under development).

A.3 Electron spin qubits (aka quantum dot qubits)

The quantum state of electron spin qubits (aka quantum dot qubits) qubits is generally the spin orientation of an electron trapped in a potential well or of an electron hole's (missing electron) inverse impact on structural spin.

The Silicon Metal-Oxide Semiconductor (Si-MOS) variant is the most generic and easiest to manufacture. Si-MOS qubits are derived from planar MOS bulk or FDSOI technologies as well as with FinFET technology.

Si-MOS-based qubits are developed by Diraq (Australia), by Intel (US) in cooperation with QuTech (The Netherlands), by SemiQon (Finland, 4-qubit quantum dot array), by Qpi (India) and by Quantum Motion Technologies (UK).

FDSOI-based qubits are developed by equal1.labs (Ireland/US).

An alternative approach consists of placing individual phosphorous atoms in a pure silicon lattice structure. This approach is known as 'donor spin' and is in fact an hybrid scheme of quantum dots (electron spin) and NMR (nuclear spin). The main benefit is the long coherence time (up to several seconds) of the nuclear spins. *Donor spin qubits* are controlled by magnetic and electrical fields. The challenges are to precisely position the phosphorous atoms in the silicon lattice and implementing qubit entanglement and qubit readout.

[8] In October 2023, Chinese scientists claimed that this quantum computer has solved an ultra-complicated mathematical problem within a millionth of a second, a million times faster than its predecessor and more than 20 billion years quicker than the world's fastest supercomputer. The researchers also said that despite the advance, there is still a long way to go before the technology replaces classical computers.

Another hybrid approach is to use transmon qubits for quantum computing and donor spin qubits for quantum memory.

Donor spin qubits are developed by Quobly (France) and Silicon Quantum Computing/SQC (Australia).

The Si-MOS and donor spin approaches are the two mainstream avenues for implementing quantum dot qubits, but alternatives are actively being researched, including:

- Silicon/Silicon-Germanium (Si/SiGe) heterostructures: developed by ARQUE (Germany) and by TU Delft/QuTech (The Netherlands);
- Gallium-Arsenide: developed by a team of US and Brazil researchers;
- electrons trapped on solid (inert) neon: developed by Florida State university (US);
- electrons trapped on superfluid helium: developed by EeroQ (US);
- electrons trapped in carbon nanotubes: developed by C12 Quantum Electronics (France);
- electrons trapped in carbon nanospheres: developed by Archer Materials (Australia).

A.4 Cavity spin qubits

Nitrogen Vacancy (NV) centre qubits are based on the control of electron spins tapped in artificial defects of crystalline carbon structures (artificial diamonds), in which one carbon atom is replaced by a nitrogen atom and another carbon atom is replaced by a gap (aka cavity)[9].

Nitrogen-rich artificial diamonds are used to manufacture NV centres. The gaps are generated with irradiation, after which vacuum annealing[10] at 800-900 degrees Celsius moves the vacancies next to the nitrogen atoms in the crystalline carbon structure. Another technique to produce NV centres is to use vacuum deposition of hydrogen and methane to produce a perfect diamond structure, followed by ion implantation with nitrogen ion beams.

The gap creates a small bar of electrons that serve as a virtual magnet via their spin. The gap is put in its qubit quantum state by precise laser and microwave pulses. Qubit readout is performed by fluorescence brightness measurement.

Manufacturers of NV centre qubit-based quantum computers (in alphabetical order):

- Quantum Brilliance (Australia): 5-qubit prototype developed in 2021 (50-qubit system expected by 2026 and 100-qubit system expected by 2028);
- SaxonQ (Germany);
- Turing Inc. (US);
- XeedQ (Germany): 4-qubit prototype developed in 2021 (256-qubit system expected by 2026).

---

[9] It is however rather more complex than this simple description since the qubits themselves are stored in nuclear spins of the surrounding carbon and nitrogen atoms.

[10] Not to be confused with quantum annealing!

Besides NV centres, another similar technique is being researched, which uses vacancies in Silicon Carbide (SiC), aka carborundum. In this technology, vacancies can be either missing nearby couples of carbon and silicon atoms (called divacancies) or just a missing silicon atom.

Photonic (Canada) is developing cavity spin qubit computers, which are using a technique similar to NV centres and SiC. Quantum Transistor (Israel) is also developing *quantum* computers based on a technique similar to NV centres and SiC.

A.5 Topological qubits

Topological qubits use 2-dimensional quasiparticles called anyons. An anyon is a specific type of quasiparticle (i.e. a mathematical construct to study complex interactions in many-body systems) in a 1- or 2 dimensional space. Anyons are neither fermions nor bosons (both of which are particles in a 3 dimensional space): they have statistical properties intermediate between fermions and bosons. (Box A.2).

A fermion is a subatomic particle whose spin quantum number is an odd half-integer value (1⁄2 , 3⁄2 , 5⁄2 , etc.). Some fermions (e.g. the electron and the quarks) are elementary subatomic particles (with spin 1⁄2), other fermions (e.g. the proton and the neutron) are composite subatomic particles made up of smaller constituents. Elementary fermions are divided into two groups: those that must bind together (quarks) and those that can exist independently (leptons). According to the Pauli exclusion principle, fermions cannot occupy the same place at the same time; this leads to the common idea that "matter takes up space". The name fermion is in honour of the Italian-American physicist Enrico Fermi.

Box A.2: Anyon

Designing anyons based on a mix of conventional and superconducting electronics is currently an active area of research quantum in the field of computing technology. The most distinctive advantage of such “designed anyons” is their potential noise immunity. The worldlines of two particles (i.e. the path that these particles object trace in space-time) can wind around one another in a 3-dimensional spacetime consisting of one temporal dimension and two spatial dimensions. In the case of more than two particles, worldlines can become interwoven in elaborate patterns called braids. There are different topological classes of braids, distinguished among other things by the number of times different strands wind around one another.

The wave functions of these multiparticle quantum objects store memories of the braids formed by their worldlines and the transformation of the state of the quantum system depends only on the overall form (i.e. topological class) of these worldlines. The information which is stored in the state of such quantum systems is therefore impervious to small errors as the braids retain their overall form (topology) even if they are jostled a bit. This particular property could possibly enable the development of inherently reliable physical qubits and might reduce and possibly even eliminate the overhead of performing explicit QEC. While this would be a truly amazing advance, topological qubits are still the least developed qubit technology because designing and controlling topological qubits has remained a critically open problem, ultimately due to the difficulty of finding materials capable of hosting topological qubit quantum states.

A Majorana qubit (not to be confused with Majorana fermion[11]) is an "engineered" non-Abelian anyon in which bound states can appear at the interface between insulators and superconductors, called Majorana Zero Modes (MZMs). Majorana bound states can be used to create topological qubits.

In 1997, while he was a researcher at Microsoft, Alexei Kitaev had the idea to use anyons for quantum computing. Since then, Microsoft Research has been researching Majorana qubits for many years and made substantial investments in the quest for developing Majorana qubits.

In May 2018, Microsoft announced that they would release their first Majorana qubit-based quantum computer in 2023, but not until February 2025 they introduced the Majorana-1 chip (which is still not a complete working prototype of a topological quantum computer).

Microsoft Majorana qubits are made with four MZMs and are named "tetrons". They are made of two Majorana superconducting nanowires with an MZM at each end, the nanowires being connected in the middle by a regular superconducting nanowire. In the Majorana superconducting wire, all free electrons are assembled in Cooper's pairs with opposite spins, like in any superconducting material. When there is an unpaired electron in the nanowire, it exhibits a curious wave function splitting it in the two opposite edges of the nanowire. Each edge contains a supposedly "half-electron", but it is a probabilistic view of it.

Note

Majorana qubits are based on superconducting nanowires and could therefore also be classified as a superconducting qubit type.

Contrary to most other quantum computing platforms, Microsoft's future Majorana quantum computer will implement quantum gates with single-qubit measurements and two-qubit parity measurements, and by levering "braiding mechanisms". The measurements are probabilistic and errors are corrected by modification of subsequent non-Clifford operations and by classical means. This implies that Microsoft's quantum computer cannot work in "NISQ fashion", i.e. using physical qubits without QEC.

Braiding refers to moving MZMs around one another in a controlled way such that their positions exchange, which results in specific changes in the state of the quantum bit register (Figure A.3). The outcome depends only on the history of these exchanges rather than on the precise details of their motion. As a result, the information encoded in the braiding is inherently resistant to errors from local disturbances. Though an error rate will be obtained that is significantly higher

[11] In 1937, the Italian theoretical physicist Ettore Majorana predicted the existence of a new class of particles, called Majorana fermions, that are their own anti-particles (but they have never been discovered). Majorana was a member of the Italian National Fascist Party. He disappeared under mysterious circumstances after purchasing a ticket to travel by ship from Naples to Palermo on 25 March 1938.

than that of non-topological qubits, QEC will however still be needed to be compatible with most FTQC quantum algorithm computing times.

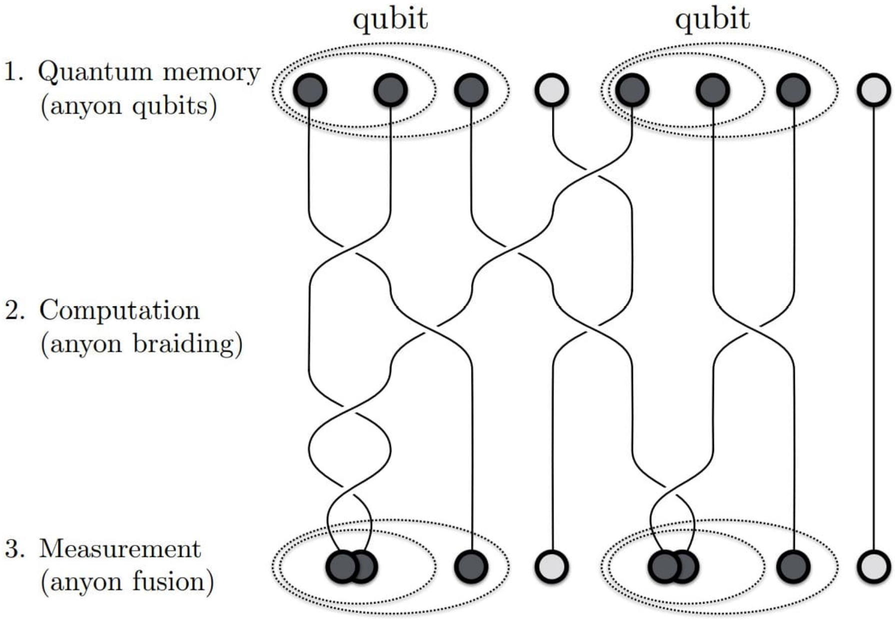


Figure A.3 :Braiding with Majorana qubits (source: Microsoft 2025)

In February 2025, Microsoft published their Majorana FTQC quantum computer roadmap (Figure A.4):

1. Majorana-1 singe-qubit chip (already announced in 2025).

2. Chip with 2 physical qubits that enables the creation of 2-qubit gates.

3. Chip with 8 physical qubits (4x2 tetron array) with QEC.

4. Chip with 371 physical qubits containing 2 logical qubits (each one consisting of an array of 13x13 physical qubits with distance-7 surface code.

5. Chip with a million physical qubits supporting about 1,000 logical qubits.

The debate over Microsoft's topological qubits escalated two weeks after the company's announcement when physicist Henry Legg of the University of St Andrews published a report casting doubt on Microsoft's verification methods, particularly the unreliability of the Topological Gap Protocol (TGP) in detecting Majorana quasiparticles. Microsoft defended its claim of creating topological qubits at the American Physical Society (APS) conference in March 2025 but scepticism remains over whether it has achieved a significant quantum computing milestone.

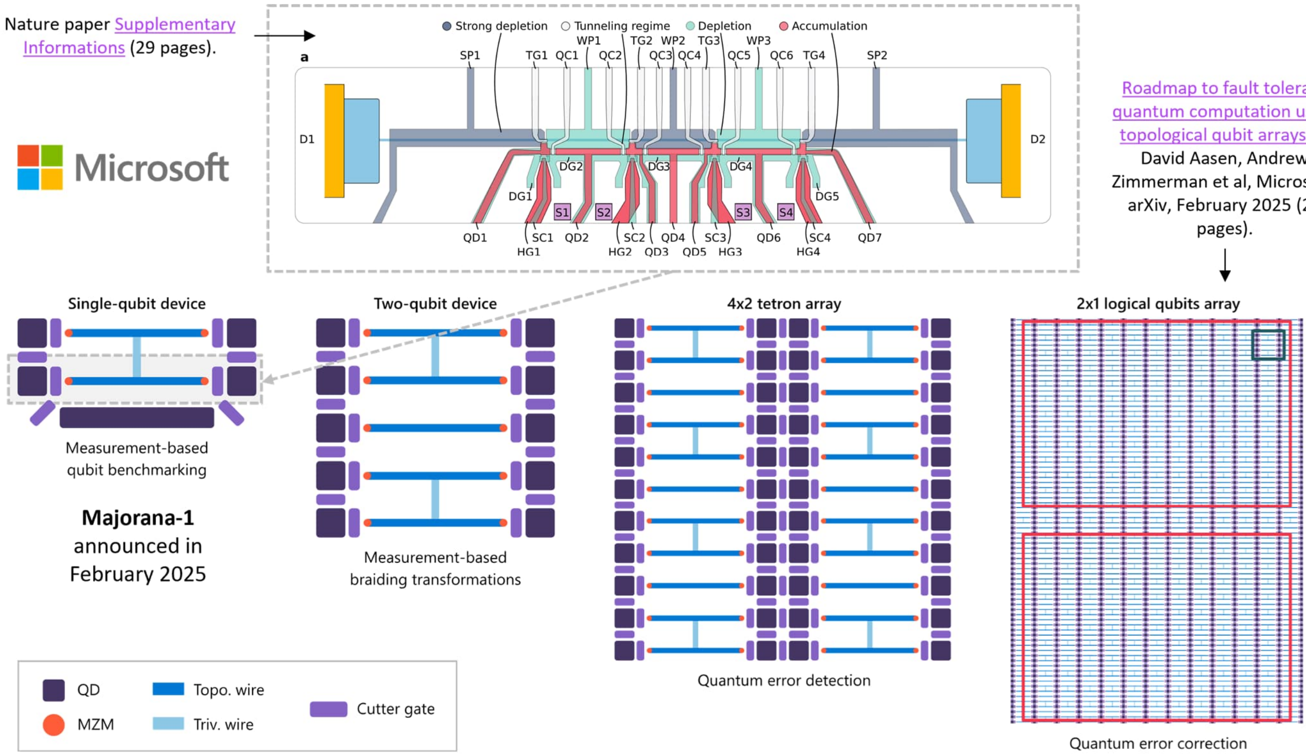


Figure A.4: Microsoft's 2025 Majorana-based FTQC roadmap (source: Microsoft 2025)

Legend
DG*n* Depletion Gate *n*
HP*n* Helper gate *n*
QC*n* QD Cutter gate *n*
QD*n* Quantum Dot *n*
SC*n* Source Cutter gate *n*
SP*n* Side Plunger *n*
TG*n* Tunnel Gate *n*
WP*n* Wire Plunger *n*

Even if everything would work as predicted by Microsoft, the practical benefits of their Majorana qubits seem to be a little oversold, particularly when compared with high-fidelity non-topological qubits. Some time ago, non-topological qubits modalities did not feature good fidelities but things have changed since then and many of these qubit modalities have significantly improved their fidelities. For example, even though they are relatively slow, trapped-ion qubits showcase very high fidelities and high qubit connectivity and could therefore compete very well with topological qubits.

Furthermore, topological qubits are not the only one with autonomous error correction. For example, autonomous error correction is featured by cat qubits from Alice&Bob, AWS and Nord Quantique, which are just starting to be demonstrated (the first cat qubit of Alice&Bob is already testable on Google's cloud).

Besides Microsoft Research, several universities (including TU Delft in the Netherlands) and research laboratories (including Google Quantum AI, IBM Research and Nokia's Bell Labs) are researching topological qubit technologies but it is uncertain whether or when these efforts will be successful.

A.6 Photonic qubits

Photons are often used for qubit control and qubit readout (using microwaves or laser beams), but they can also be used to construct *photonic qubits*.

Photons have a number of properties that make them an attractive technology for qubits: they are quantum particles that interact weakly with their environment and with each other, which results in less decoherence of photonic qubits compared to most other qubit technologies. Photonic qubits can also operate at room temperature and can be produced using nanophotonic CMOS manufacturing processes.

Their main disadvantage is that, being flying qubits, they can't be stopped or be stored, they can just be slightly delayed. This implies that a limited amount time is available for performing quantum gate operations on these qubits, which severely constrains the size of the quantum circuits needed to perform quantum computations.

Photonic qubits can be divided into two main types: Discrete Variable (DV) qubits and Continuous Variable (CV) qubits.

1. Discrete Variable (DV) qubits use single photons arranged in a two-dimensional space, like orthogonal polarisations or the absence and presence of single photons (exploiting the particle nature of photons). DV qubits rely on highly efficient, deterministic and indistinguishable single photon sources (their indistinguishability must be at least 95 %). DV qubit readout is performed by photon detectors/counters.

2. Continuous Variable (CV) qubits encode quantum information in the fluctuations of the magnetic field, in their quadrature component (exploiting the wave nature of photons). These "qubits" are often called *qumodes* because they encode more than two basis quantum states as qubits do. CV qubit readout is performed by a Gaussian measurement, supplemented by a non-Gaussian measurement implementing photon counting (returning an integer).

Hybrid atom-photon qubits are a novel hybrid quantum qubit technology approach using a single atom that modifies photon states via quantum teleportation (Box A.3) and implements quantum gates and quantum qubit readout.

Quantum (state) teleportation is a communication method that involves transmitting quantum information by exploiting the properties of quantum entanglement. It works by first creating pairs of entangled photons and then sending one photon of each pair to the sender and the other one to the receiver. The sender measures the quantum state of the photons that hold the quantum information and the state of the entangled photons at the same time. These interactions change the state of its photons, and because they are entangled with the receiver's photons, the interactions instantaneously change the state of the receiver's photons too. In effect, this "teleports" the quantum state in the

sender's photons to the receiver's photons. However, the receiver cannot reconstruct the quantum information until the sender sends the result of its measurements in the form of classical bits (via optical fibre cables or other means).

Box A.3: Quantum teleportation

Quantum walks-based simulation is a photonic computing technique. A distinction is made between discrete-time quantum walks (with discrete steps evolution) and continuous-time quantum walks (with a continuous evolution of a Hamiltonian coupling different sites). See Box A.4.

In mathematics, a random walk (aka drunkard's walk) is a random process that describes a path that consists of a succession of random steps in some mathematical space. An example is a random walk on a regular lattice, where at each step the location jumps to another site according to some probability distribution. In a simple random walk, the location can only jump to neighbouring sites of the lattice, forming a lattice path. In a simple symmetric random walk on a locally finite lattice, the probabilities of the location jumping to each one of its immediate neighbours are the same.

Quantum walks are quantum analogues of classical random walks. In contrast to the classical random walk, where the walker occupies definite states and the randomness arises due to stochastic transitions between states, in quantum walks randomness arises through either:

- quantum superposition of states;
- non-random, reversible unitary evolution;
- collapse of the wave function due to state measurements.

Box A.4: Quantum walk

Coherent Ising Machine (CIM) is another photonic computing technique. CIM is based on using optical neural networks that can solve combinatorial optimisation problems by mapping them onto NP-hard Ising problems.

The general principles for building photonic qubit-based quantum computers are the following:

- *photon sources*

  Photon sources are lasers, which are often coupled with photon generators that produce single photons. They are critical to generate simultaneously a large number of photons that will feed in parallel several qubits thanks to delay lines. These photons are time-isolated, unique and indistinguishable photons that are generated in well-spaced in time series. The photons are individually detectable at the end of processing with single photon detectors. There are two main types of Single-Photon Sources (SPSs): quantum dot single-photon sources (the best-in-class devices) and parametric photon-pair sources (laser pumping nonlinear optical waveguides or cavities).

- *qubit quantum state*

Qubit quantum state is based on a single or several properties of the photons. The most common property used is their polarisation. Other properties of photons are also used to create qubits, such as for example their phase, amplitude, frequency, path, etc. This potentially allows the creation of qudits with more than two basis quantum states.

- *single-qubit quantum gates*

  Single-qubit quantum gates use simple optical circuitry, including beam splitters, waveplates, (semi-reflective) mirrors and phase shifters.

- *two-qubit quantum gates*

  Two-qubit quantum gates are difficult to realise because it is not easy to have photons interact with each other, particularly when they are not perfectly indistinguishable. These quantum gates use optical circuits based on beam splitters or Mach-Zehnder interferometers (Box A.5) with two inputs integrating phase changes on the optical paths.

Interferometers work by merging two or more sources of light to create an interference pattern, which can be measured and analysed; hence "Interfere-o-meter", or interferometer.

Box A.5: Interferometer

- *qubit readout*

  Qubit readout uses single-photon detectors that also capture their quantum state. This detection technique is currently still imperfect and several single-photons detection technologies are competing.

One of the perspectives of photonic qubits is to overcome their shortcomings (in particular the limited time available for performing quantum computations with flying qubits) by implementing Measurement-Based Quantum Computing (MBQC).

MBQC is a method of quantum computing that prepares an entangled resource state (usually a photonic cluster state) and then performs single-qubit measurements on it. Photonic cluster states can be generated in many ways, including Spontaneous Parametric Down-Conversion (SPDC) using a powerful laser for single-photon generation and 2D spin-photon cluster states.

The entanglement of the cluster state resource is created independently ("off-line") from the rest of the quantum computation (Figure A.5).

The blue qubits are in a cluster state, where the bonds between them represent entanglement. The grey qubits have been measured, destroying the entanglement and removing them from the cluster. At the same time, the green qubits are being added to the cluster by entangling them with it. This feature makes it particularly attractive for photonic quantum computers: we can use expendable qubits that can't stick around for the full quantum calculation. If one can find a reliable way to produce qubits and stitch them together through entanglement, it can be used to produce the cluster state resource. Essentially, all that is needed is some kind of qubit factory and a stitching mechanism that puts it all together. The stitching mechanism depends on the qubit's technology platform, it can for example be implemented with an Ising interaction or by interfering two optical modes with a beam splitter.

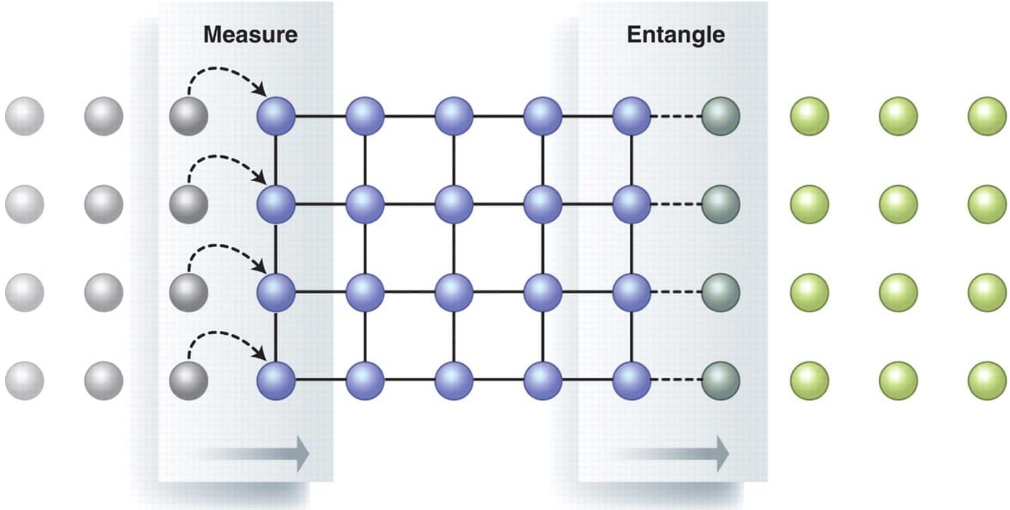


Figure A.5: Off-line resource state entanglement (source: Xanadu 2023)

The outcome of each individual measurement is random, but the measurements are related in such a way that the computation always succeeds (the measurements ***are*** the computation). In general the choices of basis for later measurements need to depend on the results of earlier measurements hence the measurements cannot all be performed at the same time.

MBQC is also called "one-way quantum computing" because qubit states are destroyed by the measurements. It has been shown that this form of quantum computing constitutes a Quantum Turing Machine (QTM) and is therefore universal and equivalent to gate-based quantum computing.

Manufacturers of photonic qubit-based quantum computers (in alphabetical order):

- Bose Quantum (China);
- BraneCell (US);
- Duality Quantum Photonics (UK): photonic quantum simulator system;
- It's Q (Germany);
- LightOn (France);
- ORCA Computing (UK): MBQC system;
- photonicsQ (Israel);
- PsiQuantum (US/Europe): development 1 million physical qubits (100 logical qubits) Fusion-Based Quantum Computing (FBQC) system (a variant of MBQC);
- Q.ANT (Germany);
- QBoson (China);
- QCDESIGN (Germany): MBQC system;

- Quandela (France): 12-qumode MBQC system;
- Quanfluence (India);
- Quantum Computing Inc./QCi (US): Quantum Photonic System (QPS) and 200 discrete modes (qudits) Dirac-3 Entropy Quantum Computer (EQC);
- Quantum Source Labs (Israel);
- QuiX Quantum (The Netherlands): 20-qumode quantum photonic processor;
- RIKEN (Finland): MBQC system);
- Rotonium (Italy);
- TundraSystems (UK);
- TuringQ (China);
- Xanadu (Canada): 8/10/24-qubit X-Series MBQC systems and 256-qumode Borealis system.

Appendix B - Dutch quantum R&D ecosystem

Note: Organisations are described in alphabetical order.

Delft Circuits

Delft Circuits has an in-house fabrication and pilot-production facility of 150 m^2 located at the Delft Quantum Campus. Its lab contains a fully-fledged production process, capable of fabricating multi-layer (super)conducting circuits on flexible substrates. These processes require expertise and equipment including metal deposition, lithography, chemical processing, high-resolution inspection and much more.

Eindhoven Hendrik Casimir Institute

TU/e has established the Eindhoven Hendrik Casimir Institute (EHCI) to create a unique and optimal environment to enable photonics and quantum technologies to grow synergistically. The institute will “entangle” two major technology fields: the superfast light-driven communication technology of photonics and the powerful calculation capabilities of quantum technology.

These technology fields hold great promise in overcoming the limits that current computation and communication technologies. Both technologies are world-class in Eindhoven, illustrated by multimillion funds from PhotonDelta/National Growth Fund. The work at EHCI is done at various hierarchical levels, from groundbreaking science in materials, via novel devices and innovative circuits, to disruptive systems that will shape our future world. This approach, already applied at TU/e to bring integrated photonics technology from the lab to real-world applications, will also be used for quantum technology and other emerging information technologies.

FermionIQ

FermionIQ, a spin-off of University of Amsterdam (UvA), Centrum Wiskunde & Informatica (CWI) and QuSoft, is a quantum company fully focused on the development of quantum software applications.

Current quantum hardware is limited in quality and availability and therefore FermionIQ delivers quantum circuit emulators as a SaaS platform to design and test quantum algorithms at scale, in collaboration with actual quantum devices.

IMPAQT

In December 2020, the Dutch quantum industry created the IMPAQT consortium. The first members are Orange QS, Qblox, Delft Circuits and QuantWare. Its goal is to improve the coordination of how they are creating quantum computer enabling technologies.

Leiden Cryogenics

With a flexible and dedicated team of cryogenic experts, Leiden Cryogenics provides various cryogenic solutions for cryogenic applications. Its current systems have the lowest vibration levels and highest cooling power available on the market today.

MolKet

MolKet offers consulting and AI services for modelling solutions for quantum molecular dynamics and cryptography with cloud-based software on hybrid HPC and quantum computing platforms.

Onnes Technologies

Founded in 2018, Onnes Technologies is headquartered in Leiden. Onnes Technologies is a leading provider of advanced cryogenic nanopositioners for low temperatures scientific research and industrial applications. With a focus on precision engineering and cutting-edge Cryo-Walking technology, Onnes Technologies is redefining cryogenic nanopositioning technology.

Onnes is dedicated to developing innovative products that enable scientists and researchers to explore the frontiers of low temperature physics including quantum computing, nano-electronics, and materials science.

Orange Quantum Systems

Orange Quantum Systems (Orange QS) aims to share their know-how in building complex quantum computing systems with research groups worldwide and help them develop quantum computing technology. Part of the team of Orange QS was involved in the development of QuTech's Quantum Inspire (QI), Europe's first quantum computing system in the cloud.

Orange QS currently depends in part on the development of quantum technology within QuTech, with Microsoft and Intel as partners of TNO and TU Delft, but within a few years it aims to be an entirely independent company. The quantum computers that it will then be making will not be rolling off a production line for use in the cloud, but will be entirely customised machines, i.e. they will be tailored in order to suit the client's specific application. The client might be a pharmaceutical company, a financial organisation, the Ministry of Defence – whoever wants to be able to carry out superfast complex calculations, but because of IP or regulatory obstacles cannot use, or does not wish to use, quantum computer cloud services.

PhotonDelta

PhotonDelta aims to create energy-efficient, faster, and more accurate microchips using the foundational units of light photons. The work conducted at the company could potentially position the Netherlands at the pinnacle of a field of study called "photonics."

In April 2022, PhotonDelta received a € 1.1 billion investment from the National Growth Fund and private investments. There is a major overlap between photonics and quantum technology so this investment could provide a major boost to the development of technology such as quantum photonic processors.

Q*Bird

Q*Bird is a start-up in the Delft Quantum Ecosystem that provides technology for quantum secure networking. The Q*Bird team has operated inside QuTech for 3 years as an engineering group, and within that time has designed and built next-generation QKD prototype systems that have been delivered to projects of industrial and commercial partners, and tested in relevant field environments. Q*Bird's mission is to provide quantum networking equipment for the current and future European quantum internet.

Q1t BV

Q1t BV specialises in the development of new quantum algorithms. Its fields of focus are quantum chemistry, quantum optics and financial analysis.

Qblox

Qblox is a spin-out from Delft-based QuTech. Qblox is a manufacturer of integrated quantum control stacks. Qblox's control stacks can control up to 20 qubits from a single compact, cost-effective and ultra-low latency device. The company's goal is to develop the Supercluster, a modular 1,600-qubit quantum control stack with error correction capabilities, which will allow their customers in the quantum hardware sector to focus on core product development and accelerate their path towards quantum advantage.

Qblox technology is currently being integrated and tested by world leaders in quantum technology like Intel, the Peng Cheng Laboratory in Shenzhen and the University of Technology Sydney.

Qphox

Qphox is developing the Quantum Modem Transducer, the world's first quantum modem connecting quantum computers across a quantum network. This technology will form the backbone of the future quantum internet.

Quantum Application Lab

QAL consists of six partners: University of Amsterdam (UvA), the Netherlands organisation for applied scientific research (TNO), the national research institute for mathematics and computer science (CWI), the Dutch collaborative ICT organisation for Dutch higher education and research (SURF), TU Delft (on behalf of QuTech and Quantum Inspire) and the Netherlands eScience Center.

QAL fulfils the much-needed connection between scientific developments of quantum hardware and software and demand-driven solutions for optimisation, simulation and machine learning. Embedded in the Quantum Delta NL ecosystem, QAL will accelerate the construction of a social and economic innovation infrastructure for quantum computing and the knowledge, capabilities and competencies required for this. QAL will do this by identifying promising domains for quantum computing applications and executing projects together with scientific, industrial and/or private sector partners.

The QAL partners are developing a public-private partnership that will bridge the gap between academic research and industrial applications of quantum computing to solve some of our most pressing societal challenges in the area of health care, energy, technology and security. They will set up collaborative projects to explore and develop quantum applications with added value for other research and industrial partners.

Quantum Delta NL

Quantum Delta NL consists of five major quantum hubs and several universities and research centres, which are all connected. The hubs are collaborating on innovation by bringing together top-quality scientists, engineers, students and entrepreneurs, working together on the frontier of quantum technology. The five hubs are:

- Eindhoven hub (post-quantum cryptography, quantum simulation and materials, with ASML, ThermoFisher, NanoLabNL and others);

- Leiden hub (applied quantum algorithms, with aQa, Google, Shell, Volkswagen, Total and others);
- Quantum Delft (quantum computing, internet and network, with QuTech, Kavli Institute, Microsoft, Intel and others);
- Quantum.Amsterdam (applied quantum algorithms, quantum sensing and simulation, with QuSoft, CWI, UvA, VU, SURFsara and others);
- Twente hub (quantum electronics and quantum photonics, with MESA+, Lockheed Martin, QuiX, IMEC and others).

Quantum Delta NL's mission is as follows:

- forging strong bonds between the five major quantum research hubs and affiliated universities and research centres;
- accelerating developments in network creation, in simulation and in applications in three catalyst programmes;
- strengthening large-scale facilities across the country in five locations for nanotechnological research in a National Cleanroom Infrastructure programme;
- kicking off four action programmes to facilitate research and cooperation and to boost social readiness levels.

Quantum Quants

Quantum Quants is a consultancy firm focused on the intersection of quantum physics and business, operating within the quantum computing industry. The company provides business intelligence and software solutions to optimise business operations, leveraging the power of quantum technologies. Quantum Quants primarily serves sectors such as finance, energy and logistics. It was founded in 2020 and is based in Rotterdam, Netherlands.

Quantum.Amsterdam

Quantum.Amsterdam, founded by QuSoft, CWI and UvA, is the gateway to the quantum world for companies to explore and develop quantum software, technology and new applications. As one of the five innovation hubs of Quantum Delta NL, it acts as liaison to the national quantum activities as described in the national agenda on quantum technology and beyond. The hub's mission is to connect academia, industry and society in a quantum ecosystem in the Amsterdam region by facilitating knowledge exchanges and innovation. It prepares companies for the quantum age by providing in-depth knowledge about this new technology and by helping to identify and validate high-impact use cases.

The Amsterdam University of Applied Sciences (AUAS), CWI and Capgemini have launched an applied quantum computing research group for applied quantum computing research, to investigate whether quantum computing can be used in various practical applications, and if so how. The research will focus on potential implementations of theoretical algorithms and protocols developed by CWI and QuSoft, or other knowledge partners.

Researchers at the UvA are working on quantum devices, especially quantum sensors and computers based on ultracold Sr atoms. An example are optical clocks, which are so precise that they would only lose one second over the lifetime of the universe.

Researchers at the NWO institute AMOLF are studying materials and devices for quantum sensing and metrology, communication, and simulation.

QuantWare

Delft-based QuantWare (QW) develops high-quality quantum processors with unusually short delivery times. By enabling quantum researchers and start-ups to accelerate their research, the company is helping this rapidly growing technological field to advance.

QuantWare originated at QuTech. Possessing extensive experience in quantum research, the QuantWare team has specialised in the development of quantum hardware that is scalable and rapidly deliverable while meeting customers' (often researchers) needs. The company's primary focus is to deliver standardised quantum processors so that research can be reproduced by multiple parties, thereby accelerating progress in the field as a whole.

Quix Quantum

QuiX Quantum is a UT spinoff. Its mission is to develop a plug-and-play integrated and reconfigurable light-based quantum processor. QuiX' Photonic Integrated Circuits (PICs) are based on the TriPleX technology, i.e. silicon-nitride based waveguides. The TriPleX technology includes a tapering method that converts low contrast modes for optimal fibre coupling, to high contrast modes for small bending radii.

QuSoft

QuSoft, the Dutch research centre for quantum software, was founded by CWI, UvA and TNO. Its mission is to develop new protocols, algorithms and applications that can be run on small and medium-sized prototypes of a quantum computer. The main focus of QuSoft is on the development of quantum software, which requires fundamentally different techniques and approaches from conventional software. The work is organised into four research groups:

1. few-qubit applications;
2. quantum testing and debugging;
3. quantum cryptography;
4. quantum architectures.

QuTech

QuTech was founded as a collaboration between TU Delft and TNO. It is positioned as a separate research institute within the TU Delft organisation. The governance structure is divided into three divisions:

1. quantum computing;
2. quantum internet and networked quantum computing;
3. qubit research.

QuTech is involved in quantum computing research in association with Intel and Microsoft.

Single Quantum

Single Quantum was among the first to manufacture and commercialise superconducting nanowire single photon detectors. Since then, its multi-channel Single Quantum Eos photon detection system has been chosen by more than 100 academic and industrial labs all over the world to perform complex optical measurements.

TU Delft

The department of Quantum and Computer Engineering (QCE) is one of the six departments in the faculty of Electrical Engineering, Mathematics and Computer Science (EEMCS) at TU Delft. QCE's research focuses on computer and network architectures, with the ambition to keep its role as one of the top European research groups and to become one of the top research groups worldwide.

The research on computer architectures targets the invention, design, prototyping and demonstration of disruptive computing accelerators/engines by making use of unique features of emerging devices (quantum bits, memristors, spintronics, graphene, etc.), while mainly targeting energy-constrained low-granularity computing for a wide range of edge applications (including AI) such as personalised healthcare, smart environments and drones. QCE research adapts a holistic approach in which it addresses the whole computing engine design stack (i.e. technology, circuit design, architectures, compilers, algorithms and applications) in order to maximize the computing efficiency. The main focus is on the middle layers (circuit design, architectures and compilers). This research goes hand in hand with the research on the dependability aspects of such designs such as testability and design-for-testability, reliability, security, etc. QCE has two research sections performing research on computer architectures:

1. Computer Engineering (CE) focusing on architectures related to neuromorphic computing, approximate computing, computation-in-memory, spin-wave computing, new hardware architectures for AI, big data architectures and hardware dependability.

2. Quantum Circuits, Architectures and Technology (QCAT) focusing on quantum computing, including the development of materials and integration techniques for quantum and classical components, the design of the electrical interfaces for quantum bits using Cryo-CMOS circuits/systems and quantum architectures. QCAT operates in close collaboration with QuTech.

The research on network architectures targets the design, the management and the control of resilient and secure complex interdependent critical Infrastructures (such as telecom, 5G, power grid, transportation, water, gas, banking, etc.), by exploiting network science and AI. In QCE, the Network Architectures and Services (NAS) group conducts research in the broad area of complex networks, ranging from man-made infrastructures such as data communications and energy networks, to biological, brain, social and financial networks.

TUD is involved in many quantum technology research projects, such as for example the IARPA LogiQ project.

Universiteit van Maastricht

UM participates in IBM Q Network quantum computing for next-generation advanced physics detectors. The goal of the IBM Q-UM academic collaboration is to develop the high-performance computational power required for two next-generation advanced physics detectors: the Einstein Telescope (ET) gravitational wave detector and the upgraded LHCb particle detector at the High-Luminosity Large Hadron Collider (HL-LHC) at CERN.

Two departments of UM’s Faculty of Science and Engineering will join forces with IBM Research Europe: the Department of Data Science and Knowledge Engineering (DKE) and the Department of Gravitational Waves & Fundamental Physics (GWFP), the latter as a member of the national Nikhef collaboration. These UM departments will bring their expertise in gravitational wave physics, elementary particle physics, signal analysis and artificial intelligence.

In the first step of this collaboration, IBM Research will sponsor two postdocs with a dual appointment at IBM Research's Lab in Zurich and at UM's Faculty of Science and Engineering. IBM will support the projects with access to its quantum computing expertise and resources.

Appendix C - References

[Bernhardt 2019] Quantum Computing for Everyone 2019

[Ezratty 2024] Understanding Quantum Technologies Seventh edition 2024

[Hidary 2021] Quantum Computing: An Applied Approach Second edition 2021

[NOREA 2024] Quantum Annealing Explained

[NOREA 2025] Quantum Algorithms

[Russ Fein 2025] The Quantum Leap blog

[Sutor 2019] Dancing with Qubits 2019

[Wikipedia 2025]

[Wong 2022] Introduction to Classical and Quantum Computing Third edition 2022

Appendix D - Acronyms and abbreviations

2D	2-Dimensional
2Q	two-Qubit quantum gate
2QB	two-Qu*b*it quantum gate
3D	3-Dimensional
5G	5th Generation
µs	microsecond
µW	microWatt
ω	frequency
π	pi
π/8	π/8 gate (T gate)
√	square root
ADC	Analogue-to-Digital Converter
AG	Aktien*g*esellschaft
AI	Artificial Intelligence
aka	also known as
Al_2O_3	Aluminium Oxide
AMOLF	← *Atoom- en Molecuulfysica*
amp	amplifier
ANF	Aramid Nano*f*iber
AOD	Acousto-Optical Deflector
APS	American Physical Society
aQa	*A*pplied Quantum *A*lgorithms
AQC	Adiabatic Quantum Computer
AQT	Alpine Quantum Technologies
ASIC	Application-Specific Integrated Circuit
ASML	← *Advanced Semiconductor Materials Lithography*

ASQ	Andreev Spin Qubit
AUAS	Amsterdam University of Applied Sciences
Avg.	Average
AWG	Arbitrary Wave Generator
AWS	Amazon Web Services
BCS	Bardeen–Cooper–Schrieffer
bit	binary digit
blog	web log
BV	Besloten Vennootschap
byte	← bite
c	celeritas
C	C gate (Feynman gate) Carbon Celsius
C2NOT	Controlled CNOT gate (Toffoli gate)
CC	Creative Commons
CCD	Charge-Coupled Device
CCNOT	Controlled CNOT gate (Toffoli gate)
CCX	Controlled CX gate (Toffoli gate)
CE	Computer Engineering
CERN	Conseil Européen pour la Recherche Nucléaire
CIM	Coherent Ising Machine
Circ	Circuit
CMOS	Complementary Metal-Oxide Semiconductor
CNOT	Controlled NOT gate
CPU	Central Processing Unit
CQC	Cambridge Quantum Computing
CR	Controlled R gate
Cryo-CMOS	Cryogenic Complementary Metal-Oxide Semiconductor

cryostat	from cryo meaning cold and stat meaning stable
CS	Controlled S gate
CSS	Calderbank, Shor and Steane
CSWAP	Controlled SWAP gate (Fredkin gate)
CUDA	Compute Unified Device Architecture
CV	Continuous Variable
CWI	Centrum Wiskunde & Informatica
CX	Controlled CNOT gate
CZ	Controlled Z gate
d	depth
DA	Digital Annealer
DAC	Digital-to-Analogue Converter
dB	deciBel
DC	Direct Current
DG	Depletion Gate
DKE	Data Science and Knowledge Engineering
dlog	discrete logarithm
DM	Density Matrix
DQS	Direct Quantum Simulator
DV	Discrete Variable
DYSL-QT	DRDO Young Scientists Laboratory for Quantum Technologies
e	electron charge
E	Exponent
e.g.	exempli gratia
EEMCS	Electrical Engineering, Mathematics and Computer Science
EHCI	Eindhoven Hendrik Casimir Institute
EQC	Entropy Quantum Computer
ET	Einstein Telescope
et al.	et alia

etc.	et cetera
F	Fahrenheit Fredkin gate
FBQC	Fusion-Based Quantum Computing
FDSOI	Fully Depleted Silicon-On-Insulator
FinFET	Fin Field-Effect Transistor
FPGA	Field-Programmable Gate Array
FTQC	Fault-Tolerant Quantum Computer
GaAs	Gallium-Arsenide
GB	Giga*b*yte
Gbit/s	Gigabit per second
GBS	Gaussian Boson Sampler Gaussian Boson Sampling
GHz	GigaHerz
GKP	Gottesman-Kitaev-Preskill
GQI	Global Quantum Intelligence
GUI	Graphical User Interface
GWFP	Gravitational Waves & Fundamental Physics
H	Hadamard gate
HEMT	High Electron Mobility Transistor
HL-LHC	High-Luminosity Large Hadron Collider
HP	Hel*p*er gate
HPC	High-Performance Computing
HQS	Honeywell Quantum Systems
Hz	Herz
i	imaginary number

I	Identity gate In-phase
i.e.	id est
I/Q	In-phase and Quadrature
IAI	Israel Aerospace Industries
IARPA	Intelligence Advanced Research Projects Activity
IBM	International Business Machines
IC	Integrated Circuit
ICT	Information and Communication Technology
id	identifier
IMEC	Interuniversity Microelectronics Centre
Inc.	Incorporated
Intel	*Integrated* E*lectronics*
ion	ionised atom
IP	Intellectual Property
JPA	Josephson Parametric Amplifier
K	Kelvin
lab	laboratory
Lab	Laboratory
laser	light amplification by stimulated emission of radiation
LHCb	Large Hadron Collider beauty
Li	Lithium
LO	Local Oscillator
m	metre
MBQC	Measurement-Based Quantum Computing
memresistor	memory resistor
MHz	MegaHerz

MESA	MicroElectronics, Sensors and Actuators
mK	milliKelvin
MOS	Metal-Oxide Semiconductor
ms	millisecond
MZM	Majorana Zero Mode
N	Negative
NanoQT	Nanofiber Quantum Technologies
NAS	Network Architectures and Services
NEC	Nippon Electric Company
Nikhef	*Nationaal Instituut voor Kernfysica en Hoge-Energiefysica* (← Nationaal Instituut voor Kernfysica en Hoge-Energiefysica)
NISQ	Noisy Intermediate-Scale Quantum
NL	Netherlands
NMR	Nuclear Magnetic Resonance
np	nanoscale porosity
NP	Nondeterministic-Polynomial
ns	nanosecond
NV	Nitrogen-Vacancy
NWO	Nederlandse Organisatie voor Wetenschappelijk Onderzoek
OQC	Oxford Quantum Circuits
P	Phase gate Polynomial Positive
Para. Amp.	Parametric Amplifier
paramp	parametric amplifier
PEC	Probabilistic Error Cancellation
PIC	Photonic Integrated Circuit

Q	Electrical charge Quadrature Quantum Qubit
QA	Quantum Annealer Quantum Annealing
QAL	Quantum Application Lab
QC	QD Cutter gate
QCAT	Quantum Circuits, Architectures and Technology
QCBM	Quantum Circuit Born Machine
QCE	Quantum and Computer Engineering
QCi	Quantum Computing Inc.
QCI	Quantum Circuits Inc.
QCNN	Quantum Convolutional Neural Network
QD	Quantum Dot
QEC	Quantum Error Correction
QEM	Quantum Eror Mitigation
QFT	Quantum Fourier Transform
QI	Quantum Inspire
QiB0	Qubit-in-a-Box 0
QKD	Quantum Key Distribution
QPS	Quantum Photonic System
QPU	Quantum Processing Unit
QS	Quantum Systems
QTM	Quantum Turing Machine
QuAS	Quantum Application Score
qubit	quantum bit
qudit	quantum digit
QV-n	Quantum Volumetric class n
QW	QuantWare
R	R gate

R/O	Readout
R&D	Research & Development
RAM	Random-Access Memory
Res.	Resistor
RF	Radio Frequency
RFSoC	Radio Frequency System-on-Chip
RT	Real-Time
s	second
S	Phase gate Sulphur
SaaS	Software-as-a-Service
SC	Source Cutter gate
Si	Silicon
Si-MOS	Silicon Metal-Oxide Semiconductor
SiC	Silicon Carbide
SiGe	Silicon-Germanium
SLM	Spatial Light Modulator
SP	Side Plunger
SPDC	Spontaneous Parametric Down-Conversion
SPS	Single-Photon Source
SQC	Silicon Quantum Computing
Sr	Strontium
SU	Special Unitary
SURF	Samenwerkende Universitaire Rekenfaciliteiten
SURFsara	SURF - Stichting Academisch Rekencentrum Amsterdam
SV	State Vector
t	time
T	T gate Time

telecoms	telecommunications
TG	Tunnel Gate
TGP	Topological Gap Protocol
THz	TeraHerz
TIFR	Tata Institute of Fundamental Research
TN	Tensor Network
TNO	*N*ederlandse *O*rganisatie voor Toegepast Natuurwetenschappelijk Onderzoek
TOFF	T*off*oli gate
transmon	transmission line shortened plasma oscillation
TU	Technische Universiteit
TU/e	Technische Universiteit *E*indhoven
TUD	Technische Universiteit Delft
TWPA	Traveling-Wave Parametric Amplifier
U	Unitary
UK	United Kingdom
UM	Universiteit van Maastricht
URB	Universal Randomized Benchmarking
US	United States
USA	United States of America
USTC	University of Science and Technology of China
UT	Universiteit Twente
UvA	Universiteit van Amsterdam
V	Voltage
VQA	Variational Quantum Algorithm
vs	versus
VU	Vrije Universiteit
VTT	Valtion Teknillinen Tutkimuskeskus
w	width

W	Watt
WP	Wire Plunger
X	Pauli X gate
Y	Pauli Y gate
Z	Pauli Z gate
ZNE	Zero-Noise Extrapolation