SREENIVASA INSTITUTE OF TECHNOLOGY AND MANAGEMENT STUDIES, CHITTOOR
(AUTONOMOUS)
Approved by AICTE, New Delhi | Permanently Affiliated to JNTUA, Ananthapuramu

LECTURE NOTES

Unit 1: Introduction to Quantum Theory and Technologies

Course: Quantum Computing / Emerging Technologies — Non-Engineering / Conceptual Track

1. Introduction Part

1.1 Key Terminologies

These foundational terms recur throughout the unit and should be understood before proceeding.

Term	Definition
Superposition	A quantum system's ability to exist in a combination of multiple states simultaneously, until measured.
Entanglement	A special correlation between quantum particles such that their states cannot be described independently, however far apart they are.
Uncertainty Principle	Heisenberg's principle that certain pairs of physical properties (e.g., position and momentum) cannot both be known with arbitrary precision at once.
Wave-particle duality	The observation that quantum entities such as electrons and photons exhibit both wave-like and particle-like behaviour depending on how they are observed.
Quantization	The restriction of certain physical quantities (such as energy) to a discrete set of allowed values rather than a continuous range.
Measurement / Observation	The physical process of extracting a definite classical outcome from a quantum system, which irreversibly alters the system's state.

1.2 The Transition from Classical to Quantum Physics

By the end of the 19th century, classical physics — Newtonian mechanics and Maxwell's electromagnetism — appeared to explain nearly all observed phenomena. However, a handful of unresolved experimental puzzles could not be reconciled with classical theory:

- Black-body radiation: classical theory predicted infinite energy at short wavelengths (the "ultraviolet catastrophe"); Planck resolved this in 1900 by proposing that energy is emitted in discrete packets, or quanta.
- The photoelectric effect: classical wave theory could not explain why light below a certain frequency, however intense, fails to eject electrons from a metal; Einstein explained this in 1905 by treating light itself as discrete photons.
- Atomic stability and spectral lines: classical physics predicted that electrons orbiting a nucleus should continuously radiate energy and spiral inward, yet atoms are stable and emit light only at specific, discrete wavelengths.

These anomalies forced physicists, over roughly three decades (1900–1930), to replace classical determinism with a fundamentally probabilistic and discrete framework — quantum mechanics — developed by Planck, Einstein, Bohr, Heisenberg, Schrödinger, and Dirac, among others.

1.3 Fundamental Principles Explained Conceptually

(a) Superposition

A quantum system can exist in a combination of multiple possible states at once, rather than being confined to just one. A useful (imperfect) analogy is a spinning coin: while spinning, it is not simply "heads" or "tails" but a blend of both possibilities, and only settles into one definite outcome when it is observed (stopped and looked at).

(b) Entanglement

Two or more particles can become linked in such a way that measuring one instantly tells you something about the other, no matter how far apart they are. This is not because a hidden signal passes between them, but because their combined state was never separable to begin with — Einstein referred to this correlation, sceptically, as "spooky action at a distance."

(c) Uncertainty Principle

Heisenberg's uncertainty principle states that some pairs of properties — most famously position and momentum — cannot both be measured to unlimited precision simultaneously. The more precisely you pin down a particle's position, the less precisely its momentum can be known, and vice versa. This is not a limitation of measuring instruments; it is a fundamental property of nature itself.

(d) Wave-Particle Duality

Quantum entities such as electrons and photons display wave-like behaviour (interference, diffraction) in some experiments and particle-like behaviour (discrete, localized impacts) in others. The double-slit experiment is the classic illustration: individual electrons fired one at a time still build up an interference pattern on a detection screen, as though each electron interferes with itself.

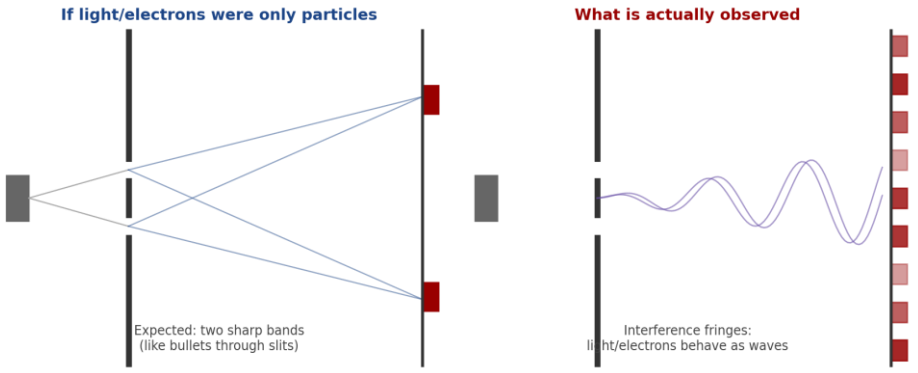

Fig 1.1 — The double-slit thought experiment: classical intuition predicts two bands, but quantum entities produce a wave-like interference pattern.

1.4 Classical vs Quantum Mechanics — Theoretical Comparison

Aspect	Classical Mechanics	Quantum Mechanics
Nature of state	Definite position and momentum at all times	Described by a probability wave function; definite values emerge only on measurement
Determinism	Fully deterministic — future states are exactly predictable from initial conditions	Fundamentally probabilistic — only the probability of outcomes can be predicted
Energy	Can take any continuous value	Restricted to discrete, quantized levels in bound systems
Measurement	Observation does not disturb the system	Measurement unavoidably and irreversibly disturbs the system

Aspect	Classical Mechanics	Quantum Mechanics
Correlations between particles	Explained fully by shared history / local interactions	Entanglement permits correlations with no classical local explanation
Domain of validity	Accurate for macroscopic, everyday-scale objects	Necessary for atomic, subatomic, and many nanoscale phenomena

1.5 Quantum States and Measurement: The Nature of Observation

In quantum mechanics, a system is described by a wave function (or state vector) that encodes the probabilities of all possible outcomes of a measurement — not a single definite value. This is fundamentally different from classical uncertainty, where an object always has a definite value that we simply may not yet know.

The act of measurement plays a uniquely active role: before measurement, a system can be in a superposition of many possible states; the instant a measurement is made, the system "collapses" onto one specific outcome, with a probability determined by the wave function (the Born rule). This raises the deep and still-debated measurement problem: what physically constitutes an "observation," and does collapse require a conscious observer, a macroscopic measuring device, or simply any irreversible interaction with the environment? Mainstream physics treats measurement as any interaction that entangles the quantum system with a much larger environment (decoherence), without requiring consciousness — but the interpretational debate is not fully settled.

1.6 Overview of Quantum Systems: Electrons, Photons, and Atoms

Electrons: Elementary particles carrying a fixed negative charge and an intrinsic "spin," which can serve as a natural two-level quantum system. Electrons bound in atoms occupy discrete energy levels, and their wave-like behaviour underlies phenomena from atomic structure to electron microscopy.

Photons: Quanta of the electromagnetic field — the particle-like units of light. Photons have no rest mass, always travel at the speed of light, and carry energy proportional to their frequency. Their polarization state is widely used to encode quantum information for communication.

Atoms: Composed of a nucleus and surrounding electrons, atoms exhibit quantized internal energy levels; transitions between these levels by absorbing or emitting photons are the basis of atomic spectra, lasers, and atomic clocks.

1.7 The Concept of Quantization: Discrete Energy Levels

A bound quantum system — such as an electron confined within an atom — cannot possess just any amount of energy; it can only occupy specific, discrete energy levels. Moving between levels requires absorbing or emitting a photon whose energy exactly matches the gap between two levels. This is why atoms absorb and emit light only at characteristic wavelengths, producing the sharp spectral lines used to identify elements in chemistry, astronomy, and spectroscopy.

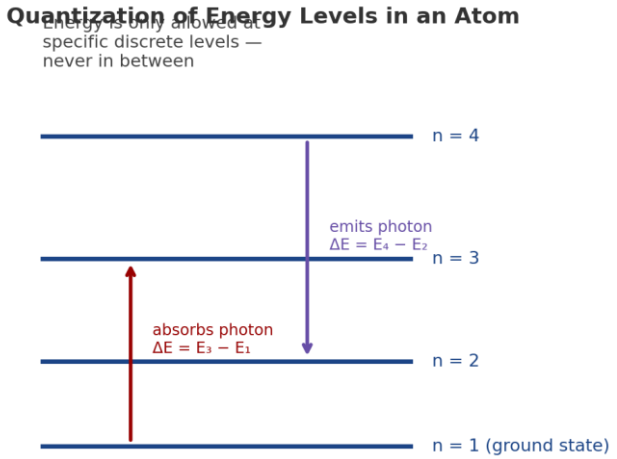

Fig 1.2 — Electrons in an atom occupy discrete, quantized energy levels; transitions between levels absorb or emit photons of specific energy.

1.8 Advantages and Disadvantages of the Quantum Framework

Advantages	Disadvantages / Challenges
Explains phenomena classical physics cannot (atomic stability, spectral lines, superconductivity)	Highly counter-intuitive; conflicts with everyday classical experience and intuition
Enables entirely new technologies: lasers, transistors, MRI, quantum computing and communication	Quantum states are fragile and easily disturbed by the environment (decoherence)
Provides extraordinarily precise predictions, verified to many decimal places experimentally	Interpretational questions (measurement problem, role of observer) remain philosophically unresolved
Enables fundamentally new information-processing paradigms via superposition and entanglement	Building and controlling large-scale quantum systems demands extreme, costly engineering conditions

1.9 Applications and Limitations

- Electronics: transistors and semiconductor devices rely on quantum band theory of solids.
- Medical imaging: MRI exploits quantized nuclear spin states; PET imaging relies on quantum processes in radioactive decay.
- Precision timekeeping and navigation: atomic clocks use quantized atomic transitions as a stable frequency reference.
- Emerging computing and communication: superposition and entanglement underpin quantum computing, quantum key distribution, and quantum sensing (detailed in Section 3).

Limitations: most large-scale quantum technologies remain in early stages ("NISQ" — Noisy Intermediate-Scale Quantum — era for computing); practical, fault-tolerant, large-scale quantum computers do not yet exist, and many quantum effects are only observable under carefully controlled laboratory conditions.

1.10 Real-World Example

The Global Positioning System (GPS) depends on quantum mechanics in two essential ways: the atomic clocks aboard GPS satellites rely on quantized atomic energy transitions for extreme timing precision, and Einstein's relativistic corrections (needed because satellite clocks run faster than ground clocks) must be applied for GPS to remain accurate to within meters — without accounting for these quantum and relativistic effects, GPS position errors would accumulate by several kilometres per day.

1.11 Safety & Standards Component

Quantum technologies raise emerging governance and standards considerations rather than conventional laboratory hazards for most students:

- Export-control and dual-use classification: many governments (including the U.S., EU, and India) are beginning to classify advanced quantum computing and communication hardware as sensitive dual-use technology, subject to export controls.
- Post-Quantum Cryptography (PQC) standards: NIST has standardised new cryptographic algorithms (e.g., CRYSTALS-Kyber, CRYSTALS-Dilithium) designed to remain secure even against future large-scale quantum computers, since such machines could eventually break widely used public-key encryption (RSA, ECC).

2. Mathematical Foundation (Conceptual Level)

As an introductory, non-computational unit, the mathematics here is kept to the minimum needed to make the conceptual principles above quantitatively precise.

2.1 Planck's Quantization of Energy

Planck proposed that electromagnetic energy is emitted or absorbed only in discrete packets (quanta), each of energy:

$$E = h \cdot f$$

Variable meanings:

- E — energy of one quantum (photon), in joules (J).
- h — Planck's constant, $h \approx 6.626 \times 10^{-34}$ J·s (a fixed constant of nature).
- f — frequency of the radiation, in hertz (Hz).

Assumption involved: this relation applies to a single quantum of radiation; total energy transferred is always an integer multiple of E = hf, never a fractional amount.

2.2 Heisenberg's Uncertainty Principle

The mathematical statement of the uncertainty principle for position and momentum is:

$$\Delta x \cdot \Delta p \geq \hbar / 2$$

- Δx — uncertainty (standard deviation) in position measurement, in metres.
- Δp — uncertainty in momentum measurement, in kg·m/s.
- $\hbar$ — reduced Planck's constant, $\hbar = h / 2\pi \approx 1.055 \times 10^{-34}$ J·s.

Assumption involved: this is a fundamental lower bound on the product of the two uncertainties — it does not depend on the quality of the measuring instrument and cannot be circumvented by better technology.

2.3 Fully Solved Numerical Problem

Problem: Calculate the energy of a single photon of red light with frequency 4.5×10^{14} Hz.

Solution

Given: $f = 4.5 \times 10^{14}$ Hz, $h = 6.626 \times 10^{-34}$ J·s.

$E = h \times f = (6.626 \times 10^{-34}) \times (4.5 \times 10^{14}) = 2.98 \times 10^{-19}$ J.

Interpretation (Academic Insight)

A single photon of visible light carries an extremely small but strictly fixed amount of energy. This is why the photoelectric effect shows a sharp frequency threshold: no matter how many low-frequency photons strike a metal surface, if each individual photon's energy (hf) is below the metal's work function, no electron will ever be ejected — intensity (more photons) cannot substitute for insufficient per-photon energy.

2.4 Design-Oriented Conceptual Problem

An electron is confined to a region of width $\Delta x = 1 \times 10^{-10}$ m (roughly one atomic diameter). Using $\Delta x \cdot \Delta p \geq \hbar/2$, the minimum uncertainty in momentum is $\Delta p \geq \hbar/(2\Delta x) \approx (1.055\times10^{-34})/(2\times10^{-10}) \approx 5.3 \times 10^{-25}$ kg·m/s. This shows that confining an electron tightly in space unavoidably forces a substantial uncertainty in its momentum — a direct, quantitative explanation of why electrons in atoms cannot be pictured as sitting still at a fixed point, and must instead be described by a spread-out probability distribution ("electron cloud").

3. Why Quantum? Strategic Significance and the Global Quantum Landscape

3.1 Why Quantum? Strategic, Scientific, and Technological Significance

- Scientific significance: quantum mechanics is the most thoroughly verified physical theory in history, underlying our understanding of atoms, molecules, materials, and fundamental particles.
- Technological significance: an estimated large share of modern GDP already rests on first-generation quantum technologies (transistors, lasers, MRI); second-generation technologies — quantum computing, communication, and sensing — promise similarly transformative impact.
- Strategic / national-security significance: quantum communication offers theoretically unbreakable encryption, while quantum computing threatens to break widely used classical encryption, making quantum capability a matter of national digital sovereignty and security, not merely commercial advantage.
- Economic significance: consulting and government estimates project the global quantum technology market could unlock on the order of one to several trillion dollars in economic value over the next decade, driving many nations to treat quantum leadership as a strategic priority comparable to AI or semiconductors.

3.2 A Snapshot of Quantum Technologies

Domain	What It Does / Why It Matters
Quantum Computing	Uses superposition and entanglement across many qubits to represent and process information in ways classical computers cannot efficiently replicate, targeting problems in chemistry, materials science, optimisation, and cryptanalysis.
Quantum Communication	Uses quantum states (typically photon polarization) to transmit information with security guaranteed by physical law rather than computational difficulty; includes quantum key distribution (QKD) and emerging quantum networks.
Quantum Sensing & Metrology	Exploits extreme quantum sensitivity to external fields to build ultra-precise magnetometers, gravity sensors, and atomic clocks, with applications in navigation, geology, medical imaging, and fundamental physics.

3.3 National and Global Quantum Missions

Recognising this strategic importance, major economies have launched dedicated, well-funded national quantum programmes over the last decade:

India — National Quantum Mission (NQM)

- Approved by the Union Cabinet on 19 April 2023 with an outlay of ₹6,003.65 crore (about US$730 million) for 2023-24 to 2030-31.
- Targets intermediate-scale quantum computers with 50–1,000 physical qubits within eight years, satellite-based quantum-secure communication over 2,000 km, and high-sensitivity quantum sensors and atomic clocks.
- Runs through four Thematic Hubs (T-Hubs) — Quantum Computing (IISc Bengaluru), Quantum Communication (IIT Madras & C-DOT), Quantum Sensing & Metrology (IIT Bombay), and Quantum Materials & Devices (IIT Delhi) — following a hub-and-spoke model with participating startups.
- India is recognised as the seventh country to launch a dedicated national quantum mission, and government assessments reported in mid-2026 that more than half of the Mission's eight-year targets had already been met within its first three years.

European Union — Quantum Flagship

- A long-term €1 billion initiative launched in 2018, running to 2028, coordinating quantum computing, communication, sensing, and simulation research across EU member states and industry partners.
- The European Commission has separately provided over €1.9 billion in cumulative quantum-related research funding over the preceding five years through Horizon Europe and related programmes, with a dedicated EU Quantum Act under preparation for 2026 to support commercialisation and strategic autonomy.

United States — National Quantum Initiative (NQI)

- Originally authorised in 2018 with about $1.2 billion over five years, the NQI has since been reauthorised with substantially increased funding for 2025–2029.
- The Department of Energy separately funds five National Quantum Information Science Research Centers, and cumulative U.S. public quantum funding is estimated in the range of several billion dollars, alongside very large private-sector investment from companies such as IBM and Google.

China — National Quantum Strategy

- China has made quantum technology a central pillar of its national technology strategy, coordinated through the National Laboratory for Quantum Information Sciences and the Chinese Academy of Sciences.
- Public estimates of China's cumulative quantum investment commonly cited in policy literature run into the tens of billions of dollars, spanning quantum communication satellites, computing, and a broader national technology fund covering multiple emerging technologies.

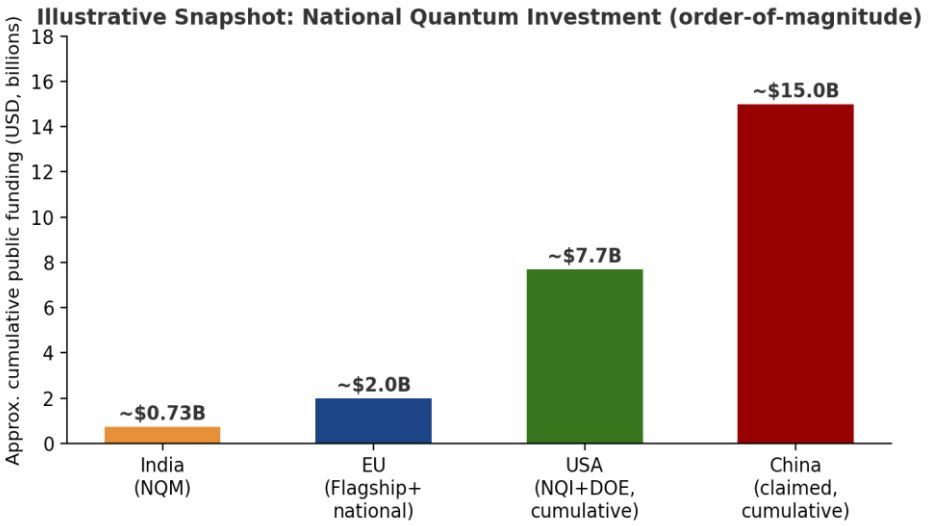

Fig 3.1 — Illustrative, order-of-magnitude comparison of cumulative public quantum-technology investment across major national programmes. Figures are approximate and drawn from multiple public policy sources; direct year-on-year comparison is difficult because programmes differ in scope, duration, and reporting methodology.

Note on figures: national quantum-investment figures are reported inconsistently across sources — some cover a single flagship programme, others aggregate multiple agencies or years, and some (particularly for China) are unofficial estimates rather than confirmed government figures. The comparison above should be read as indicative of relative scale and strategic priority, not as a precise or audited accounting.

4. Questions Section

4.1 Short Questions (2 Marks)

- Define quantum superposition in one or two sentences.
- State Heisenberg's uncertainty principle in words.
- What is meant by quantization of energy?
- Name any two physical quantities exhibiting wave-particle duality.
- What is the significance of the double-slit experiment?
- Name any two national or regional quantum missions and their approximate launch year.

4.2 Essay-Type Questions (10 Marks)

- Trace the historical transition from classical to quantum physics, explaining at least three experimental anomalies that classical physics could not resolve.
- Explain wave-particle duality with reference to the double-slit experiment, and discuss how the outcome differs from classical expectations.
- Compare classical and quantum mechanics with respect to determinism, measurement, and the nature of physical state, citing specific examples.
- Discuss the concept of quantization of energy levels in atoms, and explain how it accounts for atomic spectral lines.
- Discuss the strategic and technological significance of quantum technologies, and compare the goals of India's National Quantum Mission with one other national programme (EU, USA, or China).

4.3 Case-Study-Based Question

- Compare the objectives, funding scale, and thematic focus of India's National Quantum Mission with the EU Quantum Flagship or the U.S. National Quantum Initiative. Discuss what India's strategy suggests about its priorities within the global quantum race.

4.4 Design-Oriented / Higher-Order Thinking (HOTS) Questions

- If Planck's constant h were significantly larger than its actual value, discuss qualitatively how everyday macroscopic experience might change.
- Critically evaluate why intensity (photon count) cannot compensate for insufficient photon energy in the photoelectric effect, linking your answer to the quantization principle.
- Given that quantum computing could eventually break widely used classical encryption, evaluate the urgency and adequacy of current post-quantum cryptography standardisation efforts.

5. References

5.1 Standard Reference Books

- Griffiths, D. J., and Schroeter, D. F., "Introduction to Quantum Mechanics," 3rd Edition, Cambridge University Press, 2018.
- Eisberg, R., and Resnick, R., "Quantum Physics of Atoms, Molecules, Solids, Nuclei, and Particles," 2nd Edition, Wiley, 1985.
- Nielsen, M. A., and Chuang, I. L., "Quantum Computation and Quantum Information," 10th Anniversary Edition, Cambridge University Press, 2010.
- Rieffel, E. G., and Polak, W. H., "Quantum Computing: A Gentle Introduction," MIT Press, 2011.

5.2 Web Resources

- NPTEL — "Quantum Mechanics I," IIT Bombay/Madras: https://nptel.ac.in/courses/115106065
- NPTEL — "Introduction to Quantum Information and Computing," IIT Madras: https://nptel.ac.in/courses/106106232
- SWAYAM — "Quantum Mechanics and Applications": https://swayam.gov.in
- Department of Science & Technology, Government of India — National Quantum Mission: https://dst.gov.in/national-quantum-mission-nqm
- European Commission — Quantum Technologies Flagship: https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship

6. Additional Enrichment Components

6.1 Neat Diagrams

Included above: (i) Double-slit wave-particle duality schematic (Fig. 1.1), (ii) Quantized atomic energy-level diagram (Fig. 1.2), (iii) Global quantum-investment snapshot chart (Fig. 3.1).

6.2 Industry Case Insights

- IBM, Google, and IonQ operate cloud-accessible quantum processors, allowing students and researchers worldwide to run real quantum circuits without owning specialised hardware.
- India's Quantum Valley project in Amaravati, Andhra Pradesh, involves a public–private partnership (government, IBM, TCS, L&T) aiming to install one of India's most powerful early quantum

computers, illustrating the industry–academia–government collaboration model used by national missions.

6.3 Emerging Trends and Recent Advancements

- Growing national "quantum acts" and strategies (e.g., the EU's planned Quantum Act, UK's expanded quantum procurement programme) signal a shift from pure research funding toward commercialisation and procurement.
- Post-quantum cryptography standardisation is accelerating globally as organisations begin "crypto-agility" planning ahead of future quantum-capable adversaries.
- Rising private investment and public listings of quantum-computing companies indicate the field's transition from a purely academic pursuit toward a maturing commercial industry.

7. Expected Outcome

On completing this unit, students should be able to:

- Explain why classical physics failed to account for key experimental observations, and describe how quantum theory resolved them.
- Describe superposition, entanglement, the uncertainty principle, and wave-particle duality in clear conceptual terms.
- Differentiate classical and quantum mechanics across determinism, measurement, and state description.
- Perform basic quantitative reasoning using Planck's relation and the uncertainty principle.
- Appreciate the strategic, scientific, and economic significance of quantum technologies, and compare major national quantum missions.

This aligns with Bloom's Taxonomy across Understand (historical transition, definitions), Apply (solved numerical problems), Analyse (classical vs quantum comparison), and Evaluate (HOTS and strategic-significance questions), and directly supports semester-end examination preparation through the graded question bank in Section 4.

8. Standard Quote

"If you think you understand quantum mechanics, you don't understand quantum mechanics."

— Richard P. Feynman

Unit 2: Theoretical Structure of Quantum Information Systems

Course: Quantum Computing / Emerging Technologies — Non-Engineering / Conceptual Track

1. Introduction Part

1.1 Key Terminologies

Before entering the theoretical structure of quantum information, the following terms must be clearly understood, since the entire unit builds on them.

Term	Definition
Qubit	The basic unit of quantum information; a two-level quantum system that can exist in a superposition of the states $\|0\rangle$ and $\|1\rangle$.
Superposition	The principle that a quantum system can exist simultaneously in a combination of multiple basis states until measured.
Entanglement	A correlation between two or more qubits such that the state of one cannot be described independently of the others, regardless of distance.
Decoherence	Loss of quantum behaviour (superposition/entanglement) due to unwanted interaction with the surrounding environment.
Hilbert Space	The abstract vector space in which quantum states are represented as vectors.
Measurement	The act of extracting classical information from a quantum state, which collapses the superposition into a single outcome.

1.2 What is a Qubit? Conceptual Understanding Using Spin and Polarization

A classical bit is always in a definite state — either 0 or 1 — like a light switch that is only ever fully OFF or fully ON. A qubit, by contrast, behaves like a spinning coin: while it is in the air, it is not simply heads or tails, but a combination of both possibilities, described mathematically as a superposition. Only when it is observed (measured) does it settle into one definite outcome.

Two physical analogies make this concrete:

- Electron spin: An electron's intrinsic angular momentum, or spin, can point "up" or "down" along a chosen axis. These two spin orientations are naturally mapped to $|0\rangle$ and $|1\rangle$. Before measurement, the spin can be oriented in a superposition of both directions.
- Photon polarization: A photon's electric field can oscillate in different orientations. Horizontal polarization can represent $|0\rangle$ and vertical polarization $|1\rangle$. A photon can also be polarised at 45°, which is a genuine superposition of horizontal and vertical — not a classical mixture.

In both analogies, the key conceptual point is the same: the intermediate state is not "uncertainty about which value it already has" (as in classical probability) but a real physical combination of both values that only resolves upon measurement.

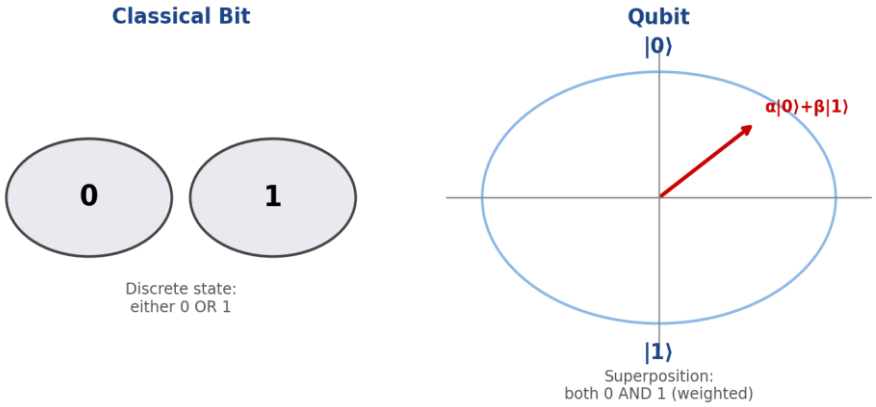

Fig 1.1 — A classical bit occupies exactly one of two discrete states, whereas a qubit occupies a continuum of weighted combinations of |0⟩ and |1⟩.

1.3 Standard Symbols and Representation (Bloch Sphere)

The standard graphical convention for a single qubit's state is the Bloch sphere — a unit sphere on which the north pole represents |0⟩, the south pole represents |1⟩, and every other point on the surface represents a valid superposition. This is the quantum-information equivalent of a circuit symbol: any qubit state used later in gates or circuits is drawn or referenced this way.

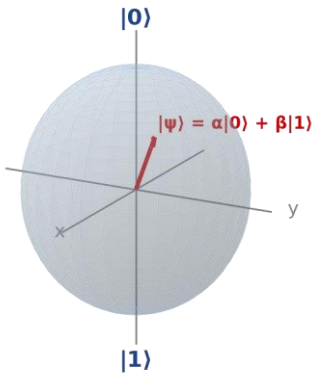

Fig 1.2 — Bloch sphere representation of a general qubit state |ψ⟩ = α|0⟩ + β|1⟩.

1.4 Why This Content Is Important

This theoretical foundation matters for three reasons:

- Without a firm grasp of qubits, superposition, and entanglement, none of the later units on quantum gates, circuits, or algorithms (Shor's, Grover's) can be understood meaningfully.
- Quantum information theory is reshaping entire industries — cryptography, secure communication, materials simulation, and optimisation — making conceptual literacy in this area increasingly essential even for non-specialists.
- The unit builds the abstract mathematical vocabulary (Hilbert space, operators, states) that is a prerequisite for reading any research paper or industry white paper in this field.

1.5 Comparison: Classical Bits vs Quantum Bits

Property	Classical Bit	Qubit
Possible states	Exactly one of 0 or 1	Superposition of $\|0\rangle$ and $\|1\rangle$
Representation	Single deterministic value	Complex vector in a 2-D Hilbert space
Combining n units	n bits → n possible values at a time	n qubits → 2^n-dimensional state space
Correlation between units	Independent unless explicitly linked by logic	Can be entangled — intrinsically correlated
Effect of observation	Reading a bit does not change it	Measurement collapses superposition irreversibly
Physical realisation	Voltage levels in transistors	Spin, polarisation, energy levels of quantum systems

1.6 Physical Realisations of Quantum Systems (Non-Engineering View)

A qubit is a mathematical abstraction; it must be physically instantiated. Three leading platforms illustrate the range of approaches, described here at a conceptual level rather than an engineering one.

Trapped ions: Individual charged atoms are suspended in free space using electromagnetic fields. Two internal energy levels of the ion serve as $|0\rangle$ and $|1\rangle$. Their isolation from the environment gives them long coherence times, though manipulating many ions together is slow.

Superconducting circuits: Tiny circuits made of superconducting material, cooled to near absolute zero, behave like artificial atoms with quantised energy levels. This is the platform used by most large commercial quantum-computing efforts because it is compatible with chip-fabrication techniques, though it is more sensitive to environmental noise.

Photons: Individual particles of light are used as qubits, typically encoded in polarisation or path. Photons interact very weakly with their environment, making them attractive for communication (quantum key distribution) and difficult to store for computation.

1.7 Advantages and Disadvantages

Advantages	Disadvantages / Limitations
Exponential state space growth with number of qubits enables massive parallel representation of information	Quantum states are extremely fragile; decoherence destroys information within microseconds to milliseconds
Entanglement enables correlations with no classical counterpart, useful for cryptography and communication	Measurement is destructive — a quantum state cannot be copied or read repeatedly without collapsing it (no-cloning theorem)
Potential for exponential speed-up on specific problem classes (factoring, search, simulation)	Requires extreme physical conditions (near absolute-zero cooling, vacuum, vibration isolation) for most platforms
Naturally models quantum-mechanical systems (chemistry, materials) that classical computers cannot simulate efficiently	Error rates remain high; large-scale fault-tolerant computation still requires substantial error-correction overhead

1.8 Applications and Limitations

- Cryptography: Quantum key distribution (e.g., BB84 protocol) uses qubit properties to detect eavesdropping.

- Chemistry & materials science: Simulating molecular structure, which grows exponentially hard for classical computers.
- Optimisation: Solving certain combinatorial problems faster using quantum annealing or variational algorithms.
- Communication: Quantum teleportation and entanglement-based secure channels.

Current limitations: no large-scale, fully fault-tolerant quantum computer exists yet; today's devices (called NISQ — Noisy Intermediate-Scale Quantum devices) have limited qubit counts and high error rates, restricting practical advantage to a narrow set of problems.

1.9 Real-World Example

In 2019, Google's Sycamore processor (53 superconducting qubits) was reported to complete a specific sampling task in about 200 seconds — a task the team estimated would take a classical supercomputer thousands of years — an event widely referred to as a claim of "quantum supremacy." The claim was later contested by classical-computing researchers who developed faster classical algorithms for the same task, illustrating how quantum advantage claims must be understood in the context of a specific, narrowly defined problem rather than as computation in general.

1.10 Safety & Standards Component

While quantum information systems do not carry conventional electrical or mechanical safety hazards for end users, two standards-related concerns are emerging:

- Post-Quantum Cryptography (PQC) standards: NIST has been standardising cryptographic algorithms (e.g., CRYSTALS-Kyber, CRYSTALS-Dilithium) that remain secure even against future quantum computers, since large quantum computers could break widely used classical encryption (RSA, ECC).
- Data governance: Organisations are advised to begin "crypto-agility" planning — the ability to switch cryptographic algorithms — in anticipation of quantum-capable adversaries.

2. Theoretical & Mathematical Foundation (Abstract Interpretation Only)

This unit is conceptual rather than computational; the mathematics below is presented only to build interpretive understanding — not for engineering-level derivation or circuit design.

2.1 Hilbert Space and Quantum State Vectors

A Hilbert space is the abstract, complex vector space in which every possible state of a quantum system lives. For a single qubit, this space is two-dimensional, spanned by the orthonormal basis vectors $|0\rangle$ and $|1\rangle$ (read as "ket zero" and "ket one"), analogous to the x- and y-axes of ordinary 2-D space, except the "coordinates" here are complex numbers.

A general single-qubit state is written as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where α and β are complex numbers called probability amplitudes, subject to the normalisation condition:

$$|\alpha|^2 + |\beta|^2 = 1$$

Variable meanings:

- $|\psi\rangle$ — the quantum state of the qubit (a vector in Hilbert space).

- α, β — complex probability amplitudes associated with outcomes 0 and 1.
- $|\alpha|^2$ — the probability of measuring the qubit in state $|0\rangle$.
- $|\beta|^2$ — the probability of measuring the qubit in state $|1\rangle$.

Assumption involved: the state vector is assumed to be normalised (total probability = 1) and defined up to an overall, physically unobservable global phase.

2.2 Quantum States as Points on the Bloch Sphere

Because a global phase has no observable effect, the two complex amplitudes can be re-parametrised using just two real angles, θ and φ:

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi} \sin(\theta/2)|1\rangle$$

- θ (theta) — the polar angle from the $|0\rangle$ axis, $0 \leq \theta \leq \pi$.
- φ (phi) — the azimuthal angle around the sphere, $0 \leq \varphi < 2\pi$.

This confirms, in abstract algebraic form, exactly what Fig. 1.2 shows geometrically: every valid single-qubit state corresponds to a unique point on the surface of the Bloch sphere.

2.3 Operators (Interpreted Abstractly)

An operator is a mathematical object that acts on a quantum state vector and transforms it into another state vector — the quantum analogue of a logic gate acting on a classical bit. For interpretive purposes only (without circuit-level detail), two categories matter:

- Unitary operators: represent reversible evolution of a closed quantum system (e.g., a quantum gate acting on a qubit before measurement). They preserve the normalisation condition $|\alpha|^2 + |\beta|^2 = 1$.
- Measurement operators: represent the act of observation, which is fundamentally different — irreversible and probabilistic — collapsing $|\psi\rangle$ onto one basis state with a probability given by the amplitude's squared magnitude (the Born rule).

2.4 Fully Solved Illustrative Problem

Problem: A qubit is prepared in the state $|\psi\rangle = (\sqrt{3}/2)|0\rangle + (1/2)|1\rangle$. (a) Verify this is a valid quantum state. (b) Find the probability of measuring $|0\rangle$ and $|1\rangle$.

Solution

(a) Check normalisation: $|\alpha|^2 + |\beta|^2 = (\sqrt{3}/2)^2 + (1/2)^2 = 3/4 + 1/4 = 1$. ✓ The state is valid.

(b) Probability of measuring $|0\rangle = |\alpha|^2 = 3/4 = 0.75$ (75%). Probability of measuring $|1\rangle = |\beta|^2 = 1/4 = 0.25$ (25%).

Interpretation (Academic Insight)

Before measurement, the qubit is genuinely in both states at once, weighted 75:25. After a single measurement, this probabilistic description collapses irreversibly into one classical outcome — either 0 or 1 — and the original superposition information is lost. This illustrates why a single qubit cannot be "read out" repeatedly to learn α and β directly; only statistics gathered over many identically prepared qubits reveal the underlying amplitudes.

2.5 Design-Oriented Conceptual Problem

A research team wants a qubit that, upon measurement, yields $|0\rangle$ and $|1\rangle$ with equal probability (an unbiased quantum coin). Using the normalisation condition $|\alpha|^2 + |\beta|^2 = 1$ with $|\alpha|^2 = |\beta|^2$, a student can show that $|\alpha| = |\beta|$

= 1/√2, so |ψ⟩ = (1/√2)|0⟩ + (1/√2)|1⟩ satisfies the requirement — this is the state produced by applying a Hadamard operation to |0⟩, and forms the theoretical basis of quantum random-number generation.

3. Entanglement, Non-Locality, and Information-Theoretic Comparison

3.1 The Role of Entanglement and Non-Locality

Entanglement arises when two or more qubits are prepared such that their combined state cannot be factored into separate, independent single-qubit states. A canonical example is the Bell state:

$$|\psi\rangle = (|00\rangle + |11\rangle) / \sqrt{2}$$

Here, measuring the first qubit and getting |0⟩ instantly implies the second qubit will also read |0⟩ if measured — and likewise for |1⟩ — no matter how far apart the two qubits are physically separated. This correlation, stronger than anything achievable classically, is what Einstein famously and skeptically called "spooky action at a distance."

Crucially, non-locality here does not permit faster-than-light communication: the outcome of each individual measurement is random, and only when the two observers later compare results (via an ordinary classical channel) does the correlation become evident. This distinction — correlation without communication — is one of the most conceptually subtle and important ideas in quantum theory.

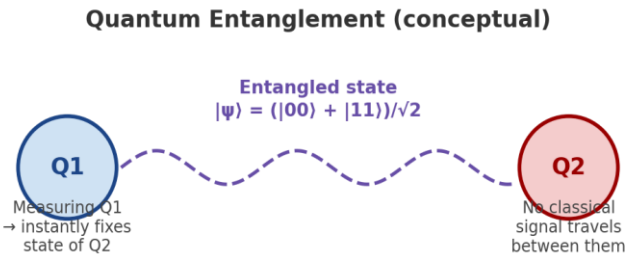

Fig 3.1 — Two entangled qubits Q1 and Q2: measuring one instantaneously determines the outcome for the other, without any signal passing between them.

3.2 Quantum Information vs Classical Information: Principles and Differences

Principle	Classical Information	Quantum Information
Basic unit	Bit (0 or 1)	Qubit (superposition of 0 and 1)
Copying	Freely copyable	Cannot be copied exactly (no-cloning theorem)
Correlation	Correlations explainable by shared prior information	Entanglement allows correlations with no classical explanation
Reading information	Reading does not disturb the value	Measurement irreversibly disturbs/collapses the state
Information density	n bits encode 1 of 2^n values at a time	n qubits carry amplitude information over 2^n dimensions simultaneously

3.3 Quantum Coherence and Decoherence — Intuitive Explanation

Coherence refers to a qubit maintaining a well-defined phase relationship between its $|0\rangle$ and $|1\rangle$ components — the property that makes superposition and interference possible, much like two water waves that stay in step so their crests and troughs reliably add or cancel.

Decoherence is the gradual loss of this phase relationship due to unavoidable interaction with the surrounding environment (stray electromagnetic fields, vibrations, thermal photons). Once decoherence occurs, the qubit behaves statistically like a classical, noisy bit rather than a genuine quantum superposition — the "waves" fall out of step and the interference effects disappear.

This is why quantum computers require extreme isolation (cryogenic cooling, vacuum, electromagnetic shielding): every engineering effort in building a quantum processor is, at its core, a fight against decoherence.

3.4 Case Study: Quantum Key Distribution (BB84)

The BB84 protocol, proposed by Bennett and Brassard, uses the fact that measuring a qubit in the wrong basis unavoidably disturbs it. Two parties exchange photons polarised in randomly chosen bases; any eavesdropper attempting to intercept and measure the photons introduces detectable errors, alerting the legitimate parties. This is a direct, practical application of superposition and measurement-disturbance principles covered in this unit, and is already deployed commercially in several metropolitan fibre-optic networks.

3.5 Philosophical Implications: Randomness, Determinism, and the Observer

Quantum theory raises questions that go beyond physics into philosophy of science:

- Genuine randomness vs hidden determinism: Quantum measurement outcomes appear to be fundamentally random, not merely unpredictable due to missing information. Bell's theorem and subsequent experiments (violating Bell inequalities) have ruled out broad classes of "hidden variable" theories that would restore determinism, though interpretational debate continues.
- The role of the observer: The measurement problem asks what physically constitutes an "observation" that collapses a superposition. Interpretations differ sharply — the Copenhagen interpretation treats collapse as a real physical process tied to measurement; the Many-Worlds interpretation denies collapse altogether, proposing that all outcomes occur in branching realities; and decoherence-based views treat collapse as an emergent, practical consequence of environmental interaction rather than a fundamental postulate.
- Locality and realism: Entanglement challenges the classical assumption that physical properties exist independently of measurement (realism) and that influences cannot act instantaneously across distance (locality). Experimental confirmation of Bell-inequality violations means at least one of these classical assumptions must be given up.

These questions remain open in the philosophy of physics and are introduced here only conceptually, to show students that the mathematics of this unit sits atop genuinely unresolved interpretational debates.

4. Questions Section

4.1 Short Questions (2 Marks)

- Define a qubit and state how it differs from a classical bit.
- What is meant by superposition in the context of a quantum state?
- Write the normalisation condition for a single-qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
- Name any two physical systems used to realise a qubit.

- Define quantum entanglement in one or two sentences.
- What is decoherence, and why is it undesirable in quantum computing?

4.2 Essay-Type Questions (10 Marks)

- Explain the concept of a qubit using the spin and polarisation analogies. Compare and contrast qubits with classical bits with respect to state space, measurement, and information capacity.
- Describe the Hilbert-space representation of a single-qubit state. Derive the Bloch-sphere parametrisation from the general state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and explain the physical meaning of θ and φ.
- Discuss quantum entanglement and non-locality. Using the Bell state as an example, explain why entanglement does not permit faster-than-light communication.
- Compare classical information theory with quantum information theory under the principles of copying, correlation, and measurement disturbance.
- Explain quantum coherence and decoherence with suitable examples, and discuss why decoherence is considered the primary engineering challenge in building practical quantum computers.

4.3 Case-Study-Based Question

- Study the BB84 quantum key distribution protocol. Explain how the principles of superposition and measurement-disturbance covered in this unit make eavesdropping detectable, and discuss one real-world deployment of quantum key distribution.

4.4 Design-Oriented / Higher-Order Thinking (HOTS) Questions

- A qubit must be designed so that measurement yields $|0\rangle$ with 3 times the probability of $|1\rangle$. Determine suitable values of α and β satisfying the normalisation condition.
- Critically evaluate the claim that quantum randomness is "truly random" rather than a reflection of incomplete classical information. Use Bell's theorem in your argument.
- If quantum measurement is fundamentally probabilistic, discuss what this implies for the philosophical debate between determinism and free will, and evaluate at least two competing interpretations (Copenhagen vs Many-Worlds).

5. References

5.1 Standard Reference Books

- Nielsen, M. A., and Chuang, I. L., "Quantum Computation and Quantum Information," 10th Anniversary Edition, Cambridge University Press, 2010.
- Griffiths, D. J., and Schroeter, D. F., "Introduction to Quantum Mechanics," 3rd Edition, Cambridge University Press, 2018.
- Rieffel, E. G., and Polak, W. H., "Quantum Computing: A Gentle Introduction," MIT Press, 2011.
- Kaye, P., Laflamme, R., and Mosca, M., "An Introduction to Quantum Computing," Oxford University Press, 2007.

5.2 Web Resources

- NPTEL — "Introduction to Quantum Information and Computing," IIT Madras: https://nptel.ac.in/courses/106106232

- NPTEL — "Foundations of Quantum Mechanics," IIT Bombay: https://nptel.ac.in/courses/115106065
- SWAYAM — "Quantum Information and Computing": https://swayam.gov.in
- IBM Quantum Learning — conceptual modules on qubits and entanglement: https://learning.quantum.ibm.com

6. Additional Enrichment Components

6.1 Neat Diagrams

Included above: (i) Classical bit vs qubit state diagram (Fig. 1.1), (ii) Bloch sphere representation (Fig. 1.2), (iii) Entanglement schematic (Fig. 3.1).

6.2 Industry Case Insights

- IBM, Google, and IonQ are pursuing different physical platforms (superconducting circuits, superconducting circuits, and trapped ions respectively), reflecting the trade-offs discussed in Section 1.6.
- Financial institutions (e.g., JPMorgan Chase, Goldman Sachs research groups) are exploring quantum algorithms for portfolio optimisation and risk analysis, an early industry application of superposition-based computation.

6.3 Emerging Trends and Recent Advancements

- Error-corrected "logical qubits": recent demonstrations combine many noisy physical qubits into fewer, more reliable logical qubits using quantum error-correcting codes (e.g., surface codes).
- Post-quantum cryptography standardisation by NIST, motivated directly by the theoretical threat that large-scale quantum computers pose to current public-key cryptography.
- Growth of cloud-accessible quantum computing platforms, allowing conceptual and educational experimentation without owning specialised hardware.

7. Expected Outcome

On completing this unit, students should be able to:

- Explain the qubit as a superposition of basis states and interpret it geometrically using the Bloch sphere.
- Differentiate clearly between classical and quantum information at the level of principles, not just terminology.
- Interpret Hilbert-space notation, state vectors, and operators at an abstract, conceptual level.
- Reason critically about entanglement, non-locality, and their philosophical implications for determinism and observation.
- Connect theoretical principles to real applications such as quantum cryptography and emerging industry practice.

This aligns with Bloom's Taxonomy across Understand (definitions, comparisons), Apply (solved and design problems), Analyse (entanglement vs classical correlation), and Evaluate (philosophical HOTS questions), and directly supports semester-end examination preparation through the graded question bank in Section 4.

8. Standard Quote

“Anyone who is not shocked by quantum theory has not understood it.”

— Niels Bohr

UNIT III — BUILDING A QUANTUM COMPUTER: THEORETICAL CHALLENGES AND REQUIREMENTS

Topics Covered: What is Required to Build a Quantum Computer (Conceptual Overview), Fragility of Quantum Systems — Decoherence, Noise and Control, Conditions for a Functional Quantum System — Isolation, Error Management, Scalability, Stability, Theoretical Barriers — Why Maintaining Entanglement is Difficult, Error Correction as a Theoretical Necessity, Quantum Hardware Platforms — Superconducting Circuits, Trapped Ions, Photonics, Vision vs Reality, The Role of Quantum Software in Managing Theoretical Complexities.

1. Introduction Part

3.1 What is Required to Build a Quantum Computer (Conceptual Overview)

A quantum computer is a computing device that stores and processes information using quantum bits (qubits), which — unlike classical bits restricted to 0 or 1 — can exist in a superposition of both states simultaneously and can be entangled with one another to represent correlated multi-qubit states. Building a working quantum computer requires far more than simply creating qubits: it requires a complete engineering stack capable of initialising qubits into a known state, manipulating them precisely via quantum gates, preserving their delicate quantum properties long enough to compute, and finally measuring the result reliably.

At a conceptual level, four ingredients are essential: (i) a physical system capable of representing a well-defined two-level quantum state, (ii) a mechanism to control that state with high precision (quantum gates), (iii) sufficient isolation from the environment to preserve quantum coherence, and (iv) a readout mechanism to measure the final state without destroying the computation prematurely.

- Key Terminology: Qubit — the basic unit of quantum information, a two-level quantum system.
- Superposition — the ability of a qubit to exist in a linear combination of $|0\rangle$ and $|1\rangle$ simultaneously.
- Entanglement — a quantum correlation between two or more qubits such that their combined state cannot be described independently.
- Decoherence — the loss of quantum behaviour (superposition/entanglement) due to unwanted interaction with the environment.
- Quantum gate — a controlled operation (analogous to a classical logic gate) that transforms qubit states.

3.2 Why This Topic is Important

Understanding the practical requirements and obstacles to building quantum hardware is essential context for appreciating both the promise and the current limitations of quantum computing; without this grounding, claims of quantum advantage can be easily overstated or misunderstood.

- Explains why quantum computers today are noisy, small-scale (NISQ-era) devices rather than the large fault-tolerant machines quantum algorithms formally assume.
- Provides the engineering context needed to evaluate competing hardware platforms and national/industrial investment strategies.

3.3 Fragility of Quantum Systems: Decoherence, Noise and Control

Quantum states are extraordinarily fragile. Any unwanted interaction between a qubit and its environment — stray electromagnetic fields, thermal vibrations, imperfect control pulses — causes the qubit's superposition to gradually collapse towards classical, well-defined behaviour, a process called decoherence. The characteristic

time over which a qubit retains useful quantum coherence is called the coherence time (commonly denoted T_1 for energy relaxation and T_2 for phase (dephasing) coherence).

In addition to decoherence, quantum systems suffer from gate noise (imperfect application of the intended operation) and measurement noise (imperfect readout), both of which introduce errors into every step of a computation.

- Real-world example: superconducting qubits typically must be cooled to near absolute zero (around 10–15 millikelvin) inside a dilution refrigerator to suppress thermal noise sufficiently for usable coherence times.
- Advantage of understanding this fragility: it directly motivates the entire discipline of quantum error correction and fault-tolerant design.

3.4 Conditions for a Functional Quantum System

David DiVincenzo's widely cited criteria summarise the practical conditions a physical platform must satisfy to serve as a viable quantum computer. These can be grouped conceptually under four themes emphasised in this unit:

- Isolation — the qubits must be sufficiently shielded from environmental noise to preserve coherence for the duration of a computation, while still allowing controlled external manipulation.
- Error Management — since some noise is unavoidable, the system must support active error detection and correction (see Section 3.6) to prevent errors from accumulating and corrupting the computation.
- Scalability — the architecture must allow the number of qubits to be increased (ideally to thousands or millions) without a proportional loss of fidelity or an intractable increase in control complexity.
- Stability — gate operations, qubit frequencies, and coupling strengths must remain consistent and well-calibrated over the operational lifetime of the device.

3.5 Theoretical Barriers: Why Maintaining Entanglement is Difficult

Entanglement is a uniquely fragile and 'non-local' resource: entangling more qubits increases the size of the combined quantum state exponentially, but simultaneously increases the number of ways the system can leak information to (and become correlated with) its environment. Any single qubit in an entangled register decohering effectively destroys the useful entanglement of the entire register, not just that one qubit — making large-scale entanglement preservation dramatically harder than preserving a single isolated qubit.

- This effect scales unfavourably: as the number of entangled qubits N grows, the probability that at least one qubit decoheres within a given time window increases, placing a practical ceiling on how large a 'useful' entangled state can be maintained with current coherence times.

3.6 Error Correction as a Theoretical Necessity

Because quantum states cannot be simply copied (a consequence of the no-cloning theorem) or observed directly without collapsing them, classical error-correction techniques such as majority-vote replication cannot be applied directly to quantum information. Quantum Error Correction (QEC) instead encodes one 'logical' qubit redundantly across several physical qubits in a way that allows errors to be detected and corrected via indirect (syndrome) measurements that do not reveal — and hence do not collapse — the encoded quantum information itself.

- The surface code is the most widely pursued QEC scheme in current hardware roadmaps, owing to its relatively high error threshold and compatibility with 2-D qubit layouts.
- The Threshold Theorem states that if the physical error rate per gate can be brought below a certain threshold, arbitrarily long fault-tolerant quantum computation becomes possible by increasing the

amount of redundancy — this theorem is the theoretical foundation justifying continued investment in improving physical qubit fidelity.

3.7 Quantum Hardware Platforms: Brief Conceptual Comparison

Several distinct physical technologies are being pursued in parallel to realise qubits, each with different trade-offs in coherence time, gate speed, connectivity, and manufacturability.

Platform	Qubit Representation	Key Advantage	Key Challenge
Superconducting Circuits	Josephson-junction based artificial atom	Fast gates; leverages mature chip fabrication	Short coherence times; requires dilution-refrigerator cooling
Trapped Ions	Internal energy states of laser-trapped ions	Very long coherence times; high-fidelity gates	Slower gate speeds; complex laser control for scaling
Photonics	Polarisation/path state of single photons	Operates at room temperature; naturally suited to communication	Difficult to make photons interact for two-qubit gates

3.8 Vision vs Reality: What's Working and What Remains Elusive

The long-term vision of quantum computing is a large-scale, fault-tolerant machine running millions of error-corrected logical qubits to solve currently intractable problems. The present reality is the Noisy Intermediate-Scale Quantum (NISQ) era: devices with tens to a few thousand physical qubits, limited coherence times, and no full fault tolerance, capable of demonstrating narrow 'quantum advantage' on specially chosen benchmark tasks but not yet of outperforming classical computers on broadly useful problems.

- Working today: small-scale demonstrations of quantum supremacy/advantage on contrived sampling tasks; basic quantum error-correcting codes implemented experimentally with break-even or modest improvement over uncorrected qubits.
- Still elusive: large numbers (thousands+) of high-fidelity logical (error-corrected) qubits; qubit counts and fidelities sufficient to run practically useful algorithms such as large-scale Shor's algorithm for cryptographically relevant integers.

3.9 The Role of Quantum Software in Managing Theoretical Complexities

Quantum software — compilers, error-mitigation libraries, pulse-level control software, and hybrid classical-quantum orchestration frameworks — plays a critical role in extracting useful performance from imperfect NISQ hardware. Software-level error mitigation techniques (such as zero-noise extrapolation and probabilistic error cancellation) statistically compensate for some hardware noise without the full overhead of hardware-level error correction, serving as an interim bridge until fault-tolerant hardware matures.

- Quantum compilers translate high-level algorithm descriptions into hardware-specific native gate sequences, optimising for the specific connectivity and noise characteristics of a given device.
- Application: frameworks such as Qiskit, Cirq, and PennyLane allow researchers to design and simulate algorithms independent of the underlying hardware platform.

2. Mathematical Foundation

2.1 Assumptions

- A qubit is modelled as a two-level quantum system whose state is a unit vector in a 2-D complex Hilbert space.
- Noise processes are modelled as acting independently on each qubit unless explicitly coupled by an entangling error channel.
- The Threshold Theorem's guarantees assume errors are sufficiently uncorrelated (local) and below the fault-tolerance threshold.

2.2 Qubit State Representation

A general single-qubit pure state is written as a normalised linear combination (superposition) of the computational basis states $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{where } \alpha, \beta \in \mathbb{C} \text{ and } |\alpha|^2 + |\beta|^2 = 1$$

- $|\alpha|^2$ gives the probability of measuring the qubit in state $|0\rangle$, and $|\beta|^2$ gives the probability of measuring $|1\rangle$ — this normalisation constraint is why the coefficients cannot be chosen freely.

2.3 Coherence Time Decay Model

The loss of a qubit's excited-state population due to energy relaxation is commonly modelled as an exponential decay with characteristic time T_1:

$$P(t) = P(0) \cdot e^{(-t / T_1)}$$

2.4 Fully Solved Numerical Problem — Coherence Decay

Problem: A superconducting qubit has a measured T_1 of 100 microseconds. If a quantum circuit requires 250 microseconds to execute, what fraction of the initial excited-state population survives to the end of the computation?

$$P(250) / P(0) = e^{(-250/100)} = e^{(-2.5)} \approx 0.082$$

- Interpretation: only about 8.2% of the original population survives — illustrating quantitatively why circuits must be kept short (few gates, low circuit depth) relative to the hardware's coherence time, and why improving T_1 is a primary hardware research goal.

2.5 Fully Solved Numerical Problem — Entangled-Register Survival Probability

Problem: If each of 5 entangled qubits independently has a 95% probability of remaining coherent over a given time window, what is the probability that the entire 5-qubit entangled register remains fully coherent (i.e., no qubit decoheres) over that window?

$$P(\text{all coherent}) = (0.95)^5 \approx 0.774$$

- Academic insight: even with a respectable 95% per-qubit survival probability, the probability of the whole register surviving drops to ≈77.4% — this quantitatively demonstrates Section 3.5's claim that entanglement preservation becomes exponentially harder as more qubits are involved.

2.6 Design-Oriented Numerical Problem

A hardware team wants a 20-qubit entangled register to remain coherent with at least 90% overall probability over the runtime of an algorithm. Using the independent-qubit survival model of Section 2.5, determine the minimum required per-qubit coherence-survival probability p, and comment on the practical implication for T_1 requirements.

$$p^{20} \geq 0.90 \implies p \geq 0.90^{(1/20)} \approx 0.9947 \text{ (i.e., } \geq 99.47\% \text{ per-qubit survival)}$$

4. Questions Section

(a) Short Answer Questions (2 Marks Level)

1. Define decoherence.
2. List the four DiVincenzo-style conditions emphasised for a functional quantum system.
3. What is the no-cloning theorem, and why is it relevant to quantum error correction?
4. Define coherence time (T_1).
5. Name the three quantum hardware platforms discussed in this unit.
6. What is meant by the 'NISQ era'?
7. What is a logical qubit?
8. State the Threshold Theorem in one sentence.

(b) Essay Type Questions (10 Marks Level)

9. Explain why maintaining large-scale entanglement is fundamentally harder than preserving a single isolated qubit's coherence.
10. Describe the four conditions (isolation, error management, scalability, stability) required for a functional quantum system, with a brief justification for each.
11. Compare superconducting circuits, trapped ions, and photonic qubits in terms of coherence time, gate speed and scalability challenges.
12. Explain why quantum error correction is a theoretical necessity rather than an optional engineering add-on, referencing the no-cloning theorem and the Threshold Theorem.
13. Discuss the gap between the long-term vision of fault-tolerant quantum computing and the current NISQ-era reality.

(c) Design-Oriented / Higher Order Thinking (HOTS) Questions

14. Given the coherence-decay model of Section 2.3, propose a design strategy (algorithmic and/or hardware) to run a 500-gate circuit on hardware with $T_1 = 50$ microseconds and a gate time of 0.1 microseconds, and justify whether this is currently feasible.
15. A quantum start-up claims 'quantum advantage' using 50 noisy qubits with no error correction. Critically evaluate this claim using the concepts of decoherence, error accumulation and the Threshold Theorem.
16. Design a hybrid classical-quantum workflow (identify which parts run classically vs quantum) for a NISQ-era application, explaining how software-level error mitigation compensates for the lack of full error correction.

5. References

(a) Standard Reference Books

- Nielsen, M. A. and Chuang, I. L., "Quantum Computation and Quantum Information", 10th Anniversary Edition, Cambridge University Press, 2010.
- DiVincenzo, D. P., "The Physical Implementation of Quantum Computation", Fortschritte der Physik, 2000.
- Preskill, J., "Quantum Computing in the NISQ era and beyond", Quantum, 2018.

(b) Web Resources

- NPTEL — "Introduction to Quantum Computing" by Prof. Rajat Mittal, IIT Kanpur: https://nptel.ac.in/courses/106106232
- IBM Quantum Learning platform: https://learning.quantum.ibm.com
- SWAYAM — "Quantum Information and Computing": https://swayam.gov.in

6. Additional Enrichment Components

- Neat labelled diagrams of a dilution refrigerator stage layout used for superconducting qubits.
- Comparison table of superconducting, trapped-ion and photonic platforms (given above).
- Graph illustrating exponential T_1 decay of qubit population over time.
- Industry case insight: IBM's roadmap towards modular, networked quantum processors to address scalability limits.
- Emerging trend: neutral-atom qubit arrays and topological qubits as candidate platforms for improved scalability and error resilience.

7. Expected Outcome

On successful completion of this unit, the student will be able to:

- Explain the essential physical and engineering requirements for a functional quantum computer.
- Describe the sources of noise and decoherence, and quantify coherence-time effects using the exponential decay model.
- Compare major quantum hardware platforms and their respective trade-offs.
- Explain why quantum error correction is theoretically essential and outline the role of the Threshold Theorem.
- Critically assess claims of quantum advantage against the current NISQ-era reality.

8. Standard Quote

"Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical."

— Richard P. Feynman

UNIT IV — QUANTUM COMMUNICATION AND COMPUTING: THEORETICAL PERSPECTIVE

Topics Covered: Quantum vs Classical Information, Basics of Quantum Communication, Quantum Key Distribution (QKD), Role of Entanglement in Communication, The Idea of the Quantum Internet — Secure Global Networking, Introduction to Quantum Computing, Quantum Parallelism (Many States at Once), Classical vs Quantum Gates, Challenges — Decoherence and Error Correction, Real-World Importance and Future Potential.

1. Introduction Part

4.1 Quantum vs Classical Information

Classical information is encoded in bits that take one definite value (0 or 1) at any time and can be freely copied. Quantum information is encoded in qubits that can exist in superposition, can become entangled with other qubits (correlations with no classical analogue), and — by the no-cloning theorem — cannot be copied exactly without disturbing the original. These differences are not merely technological but fundamental, rooted in the postulates of quantum mechanics, and they underlie both the extra computational power and the unique communication security properties of quantum systems.

- Key Terminology: Classical bit — a value in {0,1}.
- Qubit — a normalised vector in a 2-D complex Hilbert space (Section 2.2 above).
- No-cloning theorem — it is impossible to create an identical, independent copy of an arbitrary unknown quantum state.
- Measurement collapse — observing a qubit forces it probabilistically into one basis state, irreversibly destroying superposition information.

4.2 Basics of Quantum Communication

Quantum communication uses qubits — typically encoded in the polarisation or phase of single photons, well suited to travel through optical fibre or free space — as carriers of information between parties. Because measurement disturbs a quantum state, and because the no-cloning theorem prevents undetected copying, any eavesdropper attempting to intercept a quantum-encoded message inevitably introduces detectable disturbances, forming the theoretical basis for provably secure quantum communication protocols.

4.3 Quantum Key Distribution (QKD)

QKD protocols allow two parties (conventionally Alice and Bob) to establish a shared secret cryptographic key with security guaranteed by the laws of physics rather than by computational hardness assumptions (unlike classical public-key cryptography). The BB84 protocol, the first and most widely known QKD scheme, has Alice send photons randomly encoded in one of two conjugate polarisation bases; Bob measures each photon in a randomly chosen basis, and the two parties publicly compare (but do not reveal the values of) their basis choices, discarding measurements where bases mismatched.

- Security guarantee: any eavesdropper (Eve) attempting to intercept and measure photons in transit necessarily disturbs a detectable fraction of them (since she cannot know the correct basis in advance), revealing her presence through an elevated error rate in the sifted key.
- Advantage: security is based on fundamental physics (no-cloning, measurement disturbance), not on the presumed computational difficulty of a mathematical problem.

- Disadvantage: practical range is currently limited by photon loss in fibre and the difficulty of amplifying quantum signals (no quantum repeater equivalent to classical signal boosting without quantum memory/repeater technology).

4.4 Role of Entanglement in Communication

Entangled photon pairs enable additional communication protocols beyond simple key distribution. In entanglement-based QKD (e.g., the Ekert protocol), correlations between measurements on entangled pairs — which violate classical Bell inequalities — are used both to generate a shared key and to certify, via the strength of the observed correlation, that no eavesdropper has tampered with the channel.

- Quantum teleportation uses a shared entangled pair plus a classical communication channel to transmit an unknown qubit's state from one location to another, without physically transporting the qubit itself (and without violating the no-cloning theorem, since the original state is destroyed in the process).
- Application: entanglement distribution is the foundational primitive underlying proposals for a future quantum internet.

4.5 The Idea of the Quantum Internet: Secure Global Networking

A quantum internet envisions a global network capable of distributing entanglement and quantum information between distant nodes, enabling applications such as unconditionally secure communication (via QKD), distributed quantum computing (linking smaller quantum processors into a larger effective one), and enhanced-precision networked sensing. Realising this vision requires quantum repeaters — devices that extend entanglement over long distances using quantum memory and entanglement swapping, since simple optical amplification (used in classical fibre networks) cannot be applied to quantum signals without destroying their quantum information.

4.6 Introduction to Quantum Computing

Quantum computing exploits superposition and entanglement to represent and manipulate information in ways that have no classical counterpart. Whereas a classical n-bit register can represent exactly one of 2^n possible values at a time, an n-qubit register can, in superposition, represent a weighted combination of all 2^n basis states simultaneously — the resource that underlies quantum parallelism (Section 4.7).

4.7 Quantum Parallelism (Many States at Once)

Quantum parallelism refers to the ability of a quantum computer to evaluate a function on a superposition of many inputs in a single application of a quantum circuit, since applying a unitary operation to a superposition state simultaneously transforms every basis state in that superposition according to linearity.

- Important caveat: quantum parallelism alone does not directly yield speed-up, because a measurement of the resulting superposition collapses it to a single random outcome; useful quantum algorithms must cleverly use interference to amplify the probability of measuring a useful answer (as in Grover's and Shor's algorithms).

$$|\psi\rangle = (1/\sqrt{N}) \Sigma_{x=0}^{N-1} |x\rangle \quad \text{applied through } U_f: \quad U_f|\psi\rangle = (1/\sqrt{N}) \Sigma_x |x\rangle|f(x)\rangle$$

4.8 Classical vs Quantum Gates

Classical logic gates (AND, OR, NOT) are generally irreversible (multiple inputs can map to the same output, so information is lost) and operate on definite bit values. Quantum gates are represented by unitary matrices acting on qubit state vectors, and are inherently reversible (a unitary matrix always has an inverse), operating coherently on superposed and entangled states.

Gate	Type	Effect
NOT / Pauli-X	Single-qubit	Flips $\|0\rangle \leftrightarrow \|1\rangle$ (quantum analogue of classical NOT)
Hadamard (H)	Single-qubit	Creates an equal superposition of $\|0\rangle$ and $\|1\rangle$ from a basis state
CNOT	Two-qubit	Flips the target qubit if the control qubit is $\|1\rangle$; used to generate entanglement

4.9 Challenges: Decoherence and Error Correction

As introduced in Unit III, decoherence and gate/measurement noise remain the central practical obstacles to scaling both quantum computation and quantum communication. In the communication context, photon loss in optical fibre (roughly exponential with distance) plays a role analogous to decoherence, motivating the development of quantum repeaters and quantum memories to extend usable range.

4.10 Real-World Importance and Future Potential

Quantum communication offers a path to communication security that remains provably secure even against a future adversary with a large-scale quantum computer (relevant because such a machine could break widely used classical public-key cryptography via Shor's algorithm). Quantum computing more broadly promises transformative speed-ups for specific classes of problems in cryptanalysis, optimisation, and simulation of quantum systems themselves — with far-reaching implications explored further in Unit V.

2. Mathematical Foundation

2.1 Assumptions

- Quantum channels are assumed to introduce a measurable, non-zero disturbance whenever an eavesdropper attempts to gain information about a transmitted quantum state (used in QKD security proofs).
- Photon loss in optical fibre is modelled as an exponential attenuation process with distance.
- Quantum gates are assumed ideal (perfectly unitary) unless a noise model is explicitly introduced.

2.2 Hadamard Gate Derivation

The Hadamard gate is defined by the following unitary matrix, which, applied to the basis state $|0\rangle = [1,0]^T$, produces an equal superposition:

$$H = (1/\sqrt{2}) \cdot [[1, 1], [1, -1]]$$

$$H|0\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$$

- Verification of unitarity: $H \cdot H^T = I$, confirming H is a valid (reversible) quantum gate, and that applying H twice returns the original state ($H^2 = I$).

2.3 Fully Solved Numerical Problem — QKD Sifted Key Rate

Problem: In the BB84 protocol, Alice sends 10,000 photons. Bob's basis choice matches Alice's basis for approximately 50% of photons (random independent choices from 2 bases). Of the matching-basis photons, an eavesdropper's interference introduces a 20% error rate (well above the ~11% security threshold typically used). Compute: (a) the expected sifted key length, and (b) the number of erroneous bits expected in the sifted key.

$$\text{Sifted key length} = 10{,}000 \times 0.50 = 5{,}000 \text{ bits}$$

$$\text{Expected errors} = 5{,}000 \times 0.20 = 1{,}000 \text{ bits (20\% error rate)}$$

- Interpretation: since the observed error rate (20%) far exceeds the standard ~11% security threshold for BB84, Alice and Bob would detect the eavesdropper's presence and abort the key, refusing to use this compromised key for encryption — this is the core security mechanism of QKD in action.

2.4 Fully Solved Numerical Problem — Fibre Photon Loss

Problem: An optical fibre attenuates photons at 0.2 dB/km. What fraction of photons survives transmission over a 100 km link?

$$\text{Total loss} = 0.2 \text{ dB/km} \times 100 \text{ km} = 20 \text{ dB}$$

$$\text{Fraction surviving} = 10^{\wedge}(-20/10) = 10^{-2} = 0.01 \text{ (i.e., 1\%)}$$

- Academic insight: only ~1% of photons survive over 100 km, illustrating quantitatively why quantum repeaters (Section 4.5) are essential for a practical, long-distance quantum internet — direct transmission loss makes naive point-to-point QKD impractical beyond a few hundred kilometres.

2.5 Design-Oriented Numerical Problem

A telecom provider wants to guarantee at least 100 surviving photons per second arrive at a receiver 150 km away, using fibre with 0.2 dB/km attenuation. Given a required minimum surviving fraction, calculate the minimum transmission rate (photons/second) Alice's source must produce, and discuss whether a quantum repeater would be advisable at this distance.

4. Questions Section

(a) Short Answer Questions (2 Marks Level)

17. State the no-cloning theorem.
18. What is Quantum Key Distribution (QKD)?
19. Name the protocol described as the first QKD scheme.
20. Define quantum parallelism.
21. What is the key difference between classical and quantum logic gates in terms of reversibility?
22. What is a quantum repeater used for?
23. Define quantum teleportation.
24. Why is Shor's algorithm relevant to the motivation for quantum-safe communication?

(b) Essay Type Questions (10 Marks Level)

25. Explain how the no-cloning theorem and measurement disturbance together provide the theoretical security guarantee of QKD protocols such as BB84.
26. Describe the role of entanglement in quantum communication, covering both entanglement-based QKD and quantum teleportation.
27. Explain quantum parallelism, deriving how a quantum register in superposition allows simultaneous evaluation of a function on multiple inputs, and clarify why this does not trivially yield a computational speed-up.
28. Compare classical and quantum logic gates, including a discussion of reversibility and the role of the Hadamard and CNOT gates in creating superposition and entanglement.
29. Discuss the vision of a global quantum internet, the role of quantum repeaters, and the practical challenges of photon loss over long distances.

(c) Design-Oriented / Higher Order Thinking (HOTS) Questions

30. Design a hybrid classical-quantum secure communication architecture for a bank needing quantum-safe key exchange between two cities 300 km apart, addressing the photon-loss challenge quantitatively.
31. Critically evaluate the claim that 'quantum communication makes all communication unconditionally secure', identifying the specific assumptions and limitations of this claim.
32. Using the Hadamard and CNOT gates, describe (conceptually, step by step) how to prepare a two-qubit entangled Bell state starting from $|00\rangle$, and explain how this state could be used in an entanglement-based QKD protocol.

5. References

(a) Standard Reference Books

- Nielsen, M. A. and Chuang, I. L., "Quantum Computation and Quantum Information", 10th Anniversary Edition, Cambridge University Press, 2010.
- Bennett, C. H. and Brassard, G., "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984.
- Kimble, H. J., "The Quantum Internet", Nature, 2008.

(b) Web Resources

- NPTEL — "Introduction to Quantum Computing" by Prof. Rajat Mittal, IIT Kanpur: https://nptel.ac.in/courses/106106232
- NPTEL — "Quantum Information and Computing": https://nptel.ac.in

- SWAYAM — "Quantum Cryptography and Communication": https://swayam.gov.in

6. Additional Enrichment Components

- Neat labelled diagrams of the BB84 protocol steps (encoding, transmission, basis reconciliation).
- Comparison table of classical vs quantum gates (given above).
- Graph of exponential photon-loss with fibre distance.
- Industry case insight: national and commercial QKD network deployments (e.g., metropolitan quantum-secure links).
- Emerging trend: satellite-based QKD for intercontinental secure key distribution, overcoming terrestrial fibre-loss limitations.

7. Expected Outcome

On successful completion of this unit, the student will be able to:

- Explain the fundamental differences between classical and quantum information.
- Describe the working principle and security basis of QKD protocols such as BB84.
- Explain the role of entanglement in secure communication and teleportation.
- Describe quantum parallelism and the reversible nature of quantum gates.
- Quantitatively assess photon-loss and sifted-key-rate trade-offs in quantum communication links.

8. Standard Quote

"Information is physical."

— Rolf Landauer

UNIT V — APPLICATIONS, USE CASES, AND THE QUANTUM FUTURE

Topics Covered: Real-World Application Domains — Healthcare (Drug Discovery), Material Science, Logistics and Optimization, Quantum Sensing and Precision Timing, Industrial Case Studies — IBM, Google, Microsoft, PsiQuantum, Ethical, Societal, and Policy Considerations, Challenges to Adoption — Cost, Skills, Standardization, Emerging Careers in Quantum — Roles, Skillsets, and Preparation Pathways, Educational and Research Landscape — India's Opportunity in the Global Quantum Race.

1. Introduction Part

5.1 Real-World Application Domains: Healthcare (Drug Discovery)

Simulating molecular structures and chemical reactions accurately requires modelling quantum-mechanical interactions between electrons — a task that grows exponentially expensive for classical computers as molecule size increases, but which quantum computers, being themselves quantum systems, are natively suited to simulate. Quantum algorithms for quantum chemistry (e.g., the Variational Quantum Eigensolver, VQE) aim to compute molecular ground-state energies more efficiently, potentially accelerating the discovery of new drug candidates and catalysts.

- Application: simulating protein–ligand binding energies to screen candidate drug molecules faster and more accurately than classical approximation methods.
- Current limitation: today's NISQ hardware can only simulate very small molecules; clinically useful drug-discovery simulations require far larger, fault-tolerant quantum computers.

5.2 Material Science

Quantum computers are well suited to modelling novel materials — such as high-temperature superconductors, battery electrolytes, and catalysts — whose properties are governed by strongly correlated quantum-mechanical electron behaviour that is notoriously difficult for classical approximation methods to capture accurately.

- Application: accelerating the search for room-temperature superconductors or more efficient battery materials for electric vehicles and grid storage.

5.3 Logistics and Optimization

Many logistics and scheduling problems (vehicle routing, supply-chain optimisation, portfolio optimisation) are combinatorial optimisation problems with a search space that grows exponentially with problem size. Quantum optimisation approaches, such as the Quantum Approximate Optimization Algorithm (QAOA) and quantum annealing, aim to find good (though not always provably optimal) solutions faster than classical heuristics for certain problem structures.

- Application: airline crew scheduling, delivery route optimisation, and financial portfolio rebalancing.
- Current status: quantum optimisation has shown promise on small benchmark instances but has not yet demonstrated a clear, unambiguous advantage over the best classical optimisation heuristics on large real-world instances.

5.4 Quantum Sensing and Precision Timing

Quantum sensing exploits the extreme sensitivity of quantum states (e.g., superposition and entanglement) to external fields to measure physical quantities — magnetic fields, gravity, time — with precision beyond classical sensor limits. Atomic clocks, which use the highly stable quantum energy transitions of atoms as a frequency reference, are the most mature and widely deployed quantum sensing technology.

- Application: GPS satellite timing relies on atomic clocks; next-generation optical atomic clocks promise even greater precision for applications such as gravitational wave detection and geodesy.
- Application: quantum magnetometers for mineral exploration and medical imaging (e.g., magnetoencephalography).

5.5 Industrial Case Studies: IBM, Google, Microsoft, PsiQuantum

Major technology companies are pursuing distinct hardware and software strategies towards scalable quantum computing, illustrating the diversity of approaches discussed in Unit III.

Organisation	Primary Platform Focus	Notable Contribution
IBM	Superconducting circuits	Large public superconducting qubit roadmaps and the Qiskit open-source software ecosystem
Google	Superconducting circuits	Demonstrated an early 'quantum supremacy' benchmark result on a specialised sampling task
Microsoft	Topological qubits (research) + Azure Quantum cloud	Pursuing intrinsically error-resistant topological qubits; provides multi-hardware cloud access
PsiQuantum	Photonics	Pursuing a fault-tolerant photonic architecture manufactured using conventional semiconductor fabrication processes

5.6 Ethical, Societal, and Policy Considerations

The advent of large-scale quantum computing raises significant ethical and policy questions, most urgently the threat posed to widely deployed classical public-key cryptography by Shor's algorithm, which could in principle break encryption schemes (such as RSA) that currently protect financial transactions, government communications, and personal data.

- 'Harvest now, decrypt later' concern: adversaries may be recording encrypted data today with the intention of decrypting it once sufficiently powerful quantum computers become available, motivating urgent migration to post-quantum cryptography.
- Broader societal concerns include equitable access to quantum computing resources, potential concentration of quantum advantage among a small number of well-resourced nations/companies, and dual-use risks (e.g., quantum-accelerated cryptanalysis for offensive purposes).
- National policy responses include government-funded post-quantum cryptography standardisation efforts (e.g., by the U.S. National Institute of Standards and Technology) and national quantum technology strategies/missions.

5.7 Challenges to Adoption: Cost, Skills, Standardization

Despite rapid research progress, several practical barriers slow the broader industrial adoption of quantum computing.

- Cost: quantum hardware (e.g., dilution refrigerators, ultra-high-vacuum ion traps) is extremely expensive to build and operate, and cloud-access pricing for quantum processing time remains a barrier for smaller organisations.
- Skills: there is a global shortage of professionals with combined expertise in quantum physics, computer science, and specific application domains (e.g., chemistry, finance).
- Standardization: the lack of mature, universally agreed hardware interfaces, benchmarking metrics, and software standards makes it difficult for enterprises to plan long-term quantum adoption strategies with confidence.

5.8 Emerging Careers in Quantum: Roles, Skillsets, and Preparation Pathways

The growing quantum industry is creating a range of new career paths spanning hardware engineering, software/algorithm development, and application-domain specialisation.

- Quantum Hardware Engineer — designs and fabricates physical qubit devices; requires strong background in condensed-matter/AMO physics and electrical engineering.
- Quantum Software/Algorithm Developer — designs quantum circuits and algorithms; requires linear algebra, quantum mechanics fundamentals, and programming (e.g., Qiskit, Cirq).
- Quantum Application Specialist — applies quantum algorithms to a specific domain (chemistry, finance, logistics); requires strong domain expertise plus working quantum literacy.
- Preparation pathway: a foundation in linear algebra, probability, and classical computer science, followed by dedicated coursework/certifications in quantum information science and hands-on practice with quantum SDKs on real or simulated hardware.

5.9 Educational and Research Landscape: India's Opportunity in the Global Quantum Race

India has launched the National Quantum Mission, a multi-year government initiative aimed at fostering quantum technology research and development across computing, communication, and sensing, with dedicated Thematic Hubs (T-Hubs) hosted at premier research institutions. This positions India to build indigenous quantum hardware and software capability, train a domestic quantum-skilled workforce, and participate competitively in the global quantum technology landscape.

- Opportunity: India's strong existing base in classical software engineering and IT services provides a natural pipeline of talent that can be up-skilled into quantum software and application development roles.
- Challenge: building the specialised hardware fabrication and cryogenic engineering infrastructure needed for indigenous quantum hardware development requires sustained, long-term investment.

2. Mathematical Foundation

2.1 Assumptions

- Quantum chemistry simulation problems are assumed to scale exponentially in resource requirements for exact classical simulation, motivating quantum approaches.
- Optimisation problem instances are assumed to have combinatorial (exponential) classical search complexity in the general case.
- Post-quantum cryptographic risk assessments assume a sufficiently large fault-tolerant quantum computer will eventually become available.

2.2 Classical Simulation Cost of Quantum Systems

Representing the full quantum state of an n-electron (or n-qubit) system classically requires storing complex amplitudes for every one of the 2^n basis states, giving exponential memory scaling — the central motivation for quantum-native simulation approaches such as VQE:

$$\textit{Classical memory required} \approx 2^n \times \textit{(bytes per complex amplitude)}$$

2.3 Fully Solved Numerical Problem — Classical Simulation Infeasibility

Problem: Estimate the memory required to classically store the full state vector of a 50-qubit quantum system, assuming 16 bytes per complex amplitude (double-precision real + imaginary parts).

$$\textit{Number of amplitudes} = 2\text{^}50 \approx 1.126 \times 10\text{^}15$$

$$\textit{Memory required} = 1.126 \times 10\text{^}15 \times 16 \textit{ bytes} \approx 1.8 \times 10\text{^}16 \textit{ bytes} \approx 18 \textit{ petabytes}$$

- Interpretation: 18 petabytes vastly exceeds the memory capacity of even the largest classical supercomputers, quantitatively demonstrating why exact classical simulation of even modest-sized quantum systems (relevant to drug discovery and materials science) becomes rapidly infeasible — precisely the gap quantum computers aim to fill.

2.4 Fully Solved Numerical Problem — Atomic Clock Precision

Problem: A quantum atomic clock has a fractional frequency uncertainty of 1×10^{-18}. Over one year (≈3.15×10^7 seconds), estimate the resulting timing error.

$$\textit{Timing error} = \textit{fractional uncertainty} \times \textit{elapsed time} = (1\times10^{-18}) \times (3.15\times10^{7}\,s) \approx 3.15\times10^{-11}\,s$$

- Academic insight: an error of only ≈31.5 picoseconds per year illustrates the extraordinary precision achievable with quantum sensing technology, directly relevant to applications such as GPS timing and fundamental physics tests.

2.5 Design-Oriented Numerical Problem

A logistics company wants to evaluate whether QAOA-based quantum optimisation is worth piloting for a vehicle-routing problem with 30 delivery stops. Given that the classical brute-force search space for such a routing problem grows factorially (~n!), estimate the brute-force search space size for n=30, and discuss why practical classical solvers instead rely on heuristics rather than brute force — and where a quantum approach might realistically add value at current NISQ scale.

4. Questions Section

(a) Short Answer Questions (2 Marks Level)

33. Name two application domains for quantum computing discussed in this unit.

34. What is the Variational Quantum Eigensolver (VQE) used for?
35. Define quantum sensing and give one example application.
36. Name the four industrial organisations discussed as case studies.
37. What does 'harvest now, decrypt later' refer to?
38. List two barriers to industrial adoption of quantum computing.
39. Name two emerging quantum career roles.
40. What is India's National Quantum Mission?

(b) Essay Type Questions (10 Marks Level)

41. Explain why quantum computers are naturally suited to simulating molecular and material systems, and discuss the current limitations of NISQ-era chemistry simulation.
42. Discuss quantum optimisation approaches (e.g., QAOA) for logistics problems, including their current demonstrated advantages and limitations versus classical heuristics.
43. Compare the quantum hardware strategies of IBM, Google, Microsoft, and PsiQuantum, and discuss the implications of platform diversity for the field's overall progress.
44. Discuss the ethical, societal, and policy implications of large-scale quantum computing, with particular reference to post-quantum cryptography.
45. Describe the skillsets and preparation pathways for emerging quantum-industry careers, and discuss India's opportunity in the global quantum technology landscape.

(c) Design-Oriented / Higher Order Thinking (HOTS) Questions

46. Design a national strategy brief (bullet-point action plan) for a country seeking to build indigenous quantum computing capability, addressing hardware, software, workforce, and policy dimensions discussed in this unit.
47. A pharmaceutical company is deciding whether to invest in quantum computing for drug discovery today. Using the classical-simulation-cost argument (Section 2.3) and the current NISQ-era limitations (Unit III, Section 3.8), construct a reasoned recommendation.
48. Propose a post-quantum cryptography migration plan for a bank's IT infrastructure, justifying the urgency using the 'harvest now, decrypt later' threat model.

5. References

(a) Standard Reference Books

- Nielsen, M. A. and Chuang, I. L., "Quantum Computation and Quantum Information", 10th Anniversary Edition, Cambridge University Press, 2010.
- Cao, Y. et al., "Quantum Chemistry in the Age of Quantum Computing", Chemical Reviews, 2019.
- National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Standardization", U.S. Department of Commerce, ongoing.

(b) Web Resources

- NPTEL — "Introduction to Quantum Computing" by Prof. Rajat Mittal, IIT Kanpur: https://nptel.ac.in/courses/106106232
- Government of India, National Quantum Mission: https://dst.gov.in
- IBM Quantum Learning platform: https://learning.quantum.ibm.com

6. Additional Enrichment Components

- Neat labelled diagram of a VQE hybrid classical-quantum optimisation loop.
- Comparison table of IBM, Google, Microsoft, and PsiQuantum strategies (given above).
- Graph illustrating exponential classical memory scaling vs qubit count.
- Industry case insight: national quantum missions and their thematic hub structures (India, USA, EU, China).
- Emerging trend: growth of quantum-as-a-service (QaaS) cloud platforms lowering the barrier to entry for enterprise experimentation.

7. Expected Outcome

On successful completion of this unit, the student will be able to:

- Identify and explain key real-world application domains for quantum computing and sensing.
- Compare the strategic approaches of major industrial quantum computing organisations.
- Discuss the ethical, societal, and policy implications of quantum technology, including post-quantum cryptography.
- Explain the practical barriers (cost, skills, standardisation) to quantum technology adoption.
- Describe emerging quantum career pathways and evaluate India's position in the global quantum technology race.

8. Standard Quote

"The future belongs to those who understand that classical and quantum thinking must coexist — not compete."

— Attributed sentiment in contemporary quantum-technology policy discourse