Quantum

Figures current as of October 2026

The physics one level deeper than the headlines, the ways to build a qubit, error correction and why it decides everything, and the algorithms that matter and the ones that do not. The threat to encryption and the migration under way, the sensors and networks already in service, the industry and the national programs, and an honest account of where the technology stands.

MODULE 1 — Foundations: The Quantum World

Goal: Give the phenomena everything else depends on a precise meaning.

Superposition, entanglement, measurement, and decoherence; what a qubit is and is not; interference worked on one and two qubits; and why 'exponential' is the right word and 'tries everything at once' the wrong one.

MODULE 2 — The Physics, One Level Deeper

Goal: Cover the quantum mechanics a serious reader needs.

The wavefunction and the Schrödinger equation in words, uncertainty, the double slit, Bell's theorem and the 2022 Nobel, no-cloning, tunneling, and the interpretations.

MODULE 3 — A Brief History: From Planck to Logical Qubits

Goal: Trace the century from a lecture in 1900 to error-corrected machines.

Planck, Einstein, Bohr, Heisenberg, Schrödinger, and Dirac; Feynman's proposal; Deutsch, Shor, and Grover; the first qubits and the inventions that built the industry.

MODULE 4 — Qubits and Hardware

Goal: Compare the ways to build a qubit on the metrics that matter.

Superconducting, trapped-ion, neutral-atom, photonic, spin, and topological qubits, and annealers, in a table of fidelity, coherence, speed, connectivity, temperature, and scale; the dispute over Microsoft's Majorana devices; and why qubit count is the wrong scoreboard.

MODULE 5 — Gates, Circuits, and Algorithms

Goal: Explain how quantum computers compute and where the speedups are.

Gates and circuits, Shor's algorithm, Grover's search worked, quantum simulation, the variational algorithms, the complexity classes, and what quantum computers cannot do.

MODULE 6 — Error Correction and the Road to Fault Tolerance

Goal: Explain the single problem that decides everything.

Physical against logical qubits, the surface code and its overhead worked, the better codes, the 2023-26 results on three platforms, and the companies' roadmaps to 2029-33.

MODULE 7 — The Industry

Goal: Map the companies and the money.

Big tech's programs, the pure plays public and private, the 2025-26 capital wave, and the consolidation and listings of 2025-26.

MODULE 8 — Applications: What Is Real

Goal: Assess each claimed application against the evidence.

The test any application must pass, a readiness table, chemistry and materials, and the advantage claims from Google's 2019 experiment to IBM's 2026 candidates, weighed.

MODULE 9 — Cryptography: The Threat and the Migration

Goal: Explain what a quantum computer would break, when, and what replaces it.

RSA and elliptic curves, the falling resource estimates and the argument over Q-Day, harvest now and decrypt later, the NIST standards and their deployment, the deadlines, an organization's migration worked, and quantum key distribution.

MODULE 10 — Sensing, Timing, and Communication

Goal: Cover the quantum technologies already in service.

Atomic clocks and the coming redefinition of the second, magnetometers and gravimeters, navigation without GPS, quantum key distribution from China's satellites to Europe's plans, and the quantum internet's real state.

MODULE 11 — Geopolitics and National Programs

Goal: Map the race and its rules.

National programs in a table, the US-China competition, export controls, DARPA's referee, and Washington's turn to owning stakes in quantum companies, argued.

MODULE 12 — Investing in Quantum

Goal: Assess quantum as an investment, with the numbers.

The public stocks and their round trip, Quantinuum's listing, revenue against market value worked, how to value a pre-revenue platform, the risk table, and the ways in.

MODULE 13 — Where Things Stand, and What to Watch

Goal: Close with the argument and the dates.

The argument in a page, the contradictions no single module states, a dated watch list, and the last word.

The State of the Art, as of October 2026

The Leading Machines, Standards, and Services, and Who Makes Them

This table is the course's reference point: the most advanced or most widely used product in each part of the field as of October 9, 2026, who makes it, its status, and the module that explains it. A few terms recur. A qubit is the quantum version of a bit (Module 1), and a logical qubit is one encoded across many physical qubits so that their errors can be corrected (Module 6). An annealer is a special-purpose machine that searches for low-energy solutions to optimization problems rather than running general programs. Post-quantum cryptography is ordinary encryption designed to resist a quantum computer, and quantum key distribution sends encryption keys as single photons.

Category	Leading product	Maker	Shipped or status	Module
Superconducting processors	Willow; Heron r3 and Nighthawk	Google Quantum AI; IBM	In service; Nighthawk from November 2025	4
Trapped-ion computers	Helios; Tempo	Quantinuum; IonQ	In service	4
Neutral-atom computers	QuEra's machines	QuEra, with Harvard and MIT	On Amazon Braket and at Japan's AIST	4
Photonic computing	The Omega chipset	PsiQuantum	Chipset published in 2025; first systems being built	4
Silicon spin qubits	Devices made on industrial wafers; Tunnel Falls	Diraq and imec; Intel	Research devices	4
Topological qubits	Majorana 1; Majorana 2	Microsoft	Announced February 2025 and June 2026; disputed	4
Quantum annealer	Advantage2	D-Wave	Generally available May 2025	4
Cloud access	IBM Quantum Platform; Amazon Braket; Azure Quantum	IBM; Amazon; Microsoft	In service	7
Hybrid software and interconnects	CUDA-Q; NVQLink	Nvidia	NVQLink announced October 2025	7
Post-quantum standards	ML-KEM, ML-DSA, and SLH-DSA (FIPS 203, 204, and 205)	NIST	Final August 2024	9
Post-quantum key exchange in use	Hybrid X25519 and ML-KEM	Google Chrome; Cloudflare; Apple; OpenSSH	Chrome's default since 2024; OpenSSH 10's default from April 2025; Apple's system-wide default from iOS 26, September 2025	9
Quantum key distribution by satellite	Jinan-1 microsatellite	University of Science and Technology of China (USTC)	Launched 2022	10
Quantum navigation	Ironstone Opal; AQNav	Q-CTRL; SandboxAQ	In flight trials	10
Optical clocks	Strontium and ytterbium lattice clocks	National metrology laboratories	Laboratory standards	10

Company announcements, standards bodies, and press reports. 'In service' means available to outside users or customers.

Who's Who

The Companies, Agencies, and Research Bodies This Course Names

Name	What it is	Based in
Algorithmiq and BlueQubit	Quantum software companies; partners in IBM's advantage tracker	Finland; US
Alice & Bob	Maker of superconducting cat qubits	France
Alphabet (Google)	Google's parent; Google Quantum AI builds the Willow chips and runs a neutral-atom program in Boulder	US
Amazon	Runs the Braket cloud service; maker of the Ocelot cat-qubit chip	US
Anyon Systems, Nord Quantique, and Photonic	Quantum-computer makers in the Canadian program	Canada
Apple	Maker of the iPhone, whose operating system turned on post-quantum key exchange	US
AQT and eleQtron	Trapped-ion makers	Austria; Germany
Atlantic Quantum	Superconducting start-up from MIT, absorbed by Google	US
Atom Computing	Neutral-atom maker; Microsoft's partner on Magne	US
BIPM and the General Conference on Weights and Measures	The bodies that maintain the international system of units, including the definition of the second	International
Bluefors	The leading maker of dilution refrigerators	Finland
Boehringer Ingelheim	Drug maker with a quantum-chemistry program	Germany
Caltech, Oratomic, and UC Berkeley	Authors of a neutral-atom resource estimate (Module 9); Caltech also built the largest array of atoms	US
Cerca Magnetics and QuSpin	Makers of optically pumped magnetometers for brain imaging	Britain; US
CISA (Cybersecurity and Infrastructure Security Agency)	US cybersecurity agency	US
Cleveland Clinic	Hospital system; partner with RIKEN and IBM on protein simulation	US
Cloudflare	Web infrastructure company carrying much of the internet's traffic	US
Coherent and Toptica	Laser makers	US; Germany
Commerce Department	US department that sets export controls and signed the CHIPS letters of intent	US
DARPA (Defense Advanced Research Projects Agency)	The Pentagon's research agency; runs the Quantum Benchmarking Initiative	US
Defense Innovation Unit (DIU)	Pentagon unit that funds prototypes, including quantum sensors	US
Department of Energy (DOE)	US department that runs national laboratories and quantum research centers	US
Diraq	Silicon spin-qubit maker	Australia
D-Wave	Maker of quantum annealers, now also building gate-model machines	US and Canada
EPFL and the Flatiron Institute	Research bodies whose classical simulations challenged D-Wave's claim (Module 8); Flatiron is also a partner in IBM's tracker	Switzerland; US
Fraunhofer	Applied-research society	Germany

Name	What it is	Based in
Fujitsu and RIKEN	IT company and national research institute; builders of Japan's superconducting machines	Japan
GlobalFoundries	Chip foundry; a recipient of a CHIPS letter of intent	US
Global Risk Institute	Research institute that surveys experts on the quantum threat to encryption	Canada
Harvard and MIT	Universities whose neutral-atom groups produced logical-qubit results with QuEra	US
Honeywell	Industrial group; Quantinuum's largest shareholder	US
Horizon Quantum	Quantum software company	Singapore
HPE (Hewlett Packard Enterprise)	Computer maker; a participant in DARPA's initiative that did not advance	US
IBM	Maker of the Heron and Nighthawk processors; the most detailed fault-tolerance roadmap	US
ID Quantique	Quantum key distribution maker, controlled by IonQ	Switzerland
imec	Semiconductor research center; partner of Diraq	Belgium
Infleqtion	Neutral-atom computers, clocks, and sensors	US
Intel	Chip maker; maker of the Tunnel Falls silicon spin chip	US
IonQ	Trapped-ion maker and the sector's most active acquirer	US
IQM	Superconducting quantum-computer maker	Finland
Keysight, Zurich Instruments, and Quantum Machines	Makers of control electronics for quantum computers	US; Switzerland; Israel
Lightsynq and Capella	Photonic-interconnect and satellite companies bought by IonQ	US
LIGO	Gravitational-wave observatory that uses squeezed light	US
McKinsey and PitchBook	Consultancy and data provider whose counts of quantum investment the course cites	US
Microsoft	Developer of the Majorana topological devices; runs Azure Quantum	US
National Cyber Security Centre (NCSC)	Britain's cybersecurity agency	Britain
NIST (National Institute of Standards and Technology)	US standards agency; published the post-quantum standards	US
NSA (National Security Agency)	US signals-intelligence agency; sets the CNSA 2.0 rules for national security systems	US
NSF (National Science Foundation)	US research funder	US
Nvidia	Chip maker; supplies CUDA-Q software, NVQLink, and GPUs for quantum systems	US
Office of Management and Budget (OMB)	White House office that directs federal agencies	US
OQC, Quantum Motion, and SEEQC	Quantum hardware companies	Britain; Britain; US
Origin Quantum and QuantumCTek	Quantum computing and key-distribution companies	China
Oxford Ionics	Trapped-ion chip maker bought by IonQ	Britain
Pasqal and planqc	Neutral-atom makers	France; Germany
PsiQuantum	Photonic quantum-computer maker; designer of the Omega chipset	US
Q-CTRL	Quantum control software and navigation company	Australia

Name	What it is	Based in
Quandela, QuiX, and Classiq	Photonic makers and a quantum software company	France; Netherlands; Israel
Quantinuum	Trapped-ion maker of Helios; the logical-qubit leader	US and Britain
Quantum Circuits	Superconducting start-up bought by D-Wave	US
QuEra	Neutral-atom maker; partner of Harvard and MIT	US
QuTech	Quantum research institute at Delft University of Technology	Netherlands
Rigetti	Superconducting quantum-computer maker	US
SandboxAQ	Quantum software and navigation company; maker of AQNav	US
Signal	Encrypted messaging service	US
Silicon Quantum Computing (SQC)	Silicon qubit maker	Australia
Singapore University of Technology and Design	University whose researchers, with Nvidia, simulated IBM's explicit advantage claim	Singapore
SkyWater	Chip foundry bought by IonQ	US
SoftBank	Technology investor; an investor in QuEra	Japan
Toshiba	Electronics group; quantum key distribution maker	Japan
Treasury Department	US department whose rule restricts investment in Chinese quantum companies	US
University of Birmingham	University that ran field trials of a quantum gravity gradiometer	Britain
University of Oxford and Yale University	Universities where trapped-ion and transmon qubits were developed	Britain; US
University of St Andrews	University of Henry Legg, whose critique of Microsoft's Majorana test appeared in *Nature*	Britain
USTC (University of Science and Technology of China)	China's leading quantum university; maker of the Zuchongzhi and Jiuzhang machines and the Micius and Jinan-1 satellite experiments	China
Xanadu	Photonic quantum-computer maker	Canada
Zapata	Quantum software company that has closed (Module 7)	US

Organizations grouped in one row share a role. Figures and dates are in the modules.

Module 1 — Foundations

The Quantum World

Recommended Reading / Reference

Book: Chris Bernhardt, *Quantum Computing for Everyone*, the best short mathematical introduction

Reference: Michael Nielsen and Isaac Chuang, *Quantum Computation and Quantum Information*, the textbook

1a. Superposition

A classical bit is definitely 0 or definitely 1. A quantum bit, or qubit, can be in a superposition: a state described by two numbers called amplitudes, one for 0 and one for 1, such that a measurement gives 0 with probability equal to the square of the first amplitude and 1 with probability equal to the square of the second. The amplitudes can be negative, and in general complex, and that sign is the whole point. Amplitudes add and cancel like waves, so two paths to the same outcome can reinforce or destroy each other. This is interference, and it is the resource quantum computers use. A qubit in superposition is not 'both 0 and 1', and it does not 'try every answer at once' (1e). It is a system whose measurement statistics are governed by amplitudes that can interfere, which is a different and stranger thing.

1b. Entanglement

Two qubits can be in a joint state that cannot be written as one state for the first and one for the second, which is called an entangled state. In the simplest, the pair is in a superposition of 'both 0' and 'both 1'. Measure one and you get a random answer, but the other will always give the same answer, instantly, however far away it is. Einstein called it spooky action at a distance and took it as a sign that quantum mechanics was incomplete, and the experiments of Module 2 showed that the correlations are real and cannot be explained by any pre-agreement between the particles. Entanglement carries no usable signal, because each answer is random until the two are compared, so it does not violate relativity. What it does is make the state of n qubits require 2^n amplitudes to describe. Three hundred entangled qubits have more amplitudes than there are atoms in the observable universe, which is the source of quantum computing's power and of the difficulty of simulating it on a classical computer.

1c. Measurement and Decoherence

Measurement destroys superposition: the qubit becomes definitely 0 or definitely 1, the amplitudes collapse to the outcome, and the information in the other amplitude is gone. That is why a quantum computer cannot simply read out 2^n answers (1e). Decoherence is unintended measurement. Any interaction with the environment, whether a stray photon, a vibration, a magnetic fluctuation, or heat, partly measures the qubit and destroys its superposition. It is the reason quantum computers isolate their qubits in vacuum chambers or refrigerators, many of them near absolute zero, the reason their qubits survive only microseconds to minutes, and the enemy that every later module is about.

1d. The Qubit, Concretely

	Classical bit	Qubit
States	0 or 1	$\alpha\|0\rangle + \beta\|1\rangle$, with $\|\alpha\|^2 + \|\beta\|^2 = 1$; α and β complex
Reading it	Returns the stored value, repeatably	Returns 0 with probability $\|\alpha\|^2$ and 1 with probability $\|\beta\|^2$; the state then becomes that outcome
Copying	Trivial	Impossible for an unknown state (Module 2)
n of them	2^n possible values, one at a time	2^n amplitudes describing one joint state
Operations	AND, OR, NOT; irreversible	Rotations and controlled rotations; reversible
Errors	Bit flips, corrected by copying	Bit flips, phase flips, and everything between, corrected only by clever encoding (Module 6)
Physical form	A transistor's voltage; a magnetic domain	Energy levels of a superconducting circuit, an ion, or an atom; a photon's path; an electron's spin

Worked example — Two Qubits and Interference

Put one qubit through a Hadamard gate, the basic operation that makes an equal superposition: it goes from $|0\rangle$ to $(|0\rangle + |1\rangle)/\sqrt{2}$, with both amplitudes 0.707, so a measurement gives 0 or 1 with probability 0.5 each. Apply a second Hadamard. The $|0\rangle$ component becomes $(|0\rangle + |1\rangle)/\sqrt{2}$ and the $|1\rangle$ component becomes $(|0\rangle - |1\rangle)/\sqrt{2}$. Adding them, the $|1\rangle$ amplitudes, +0.5 and −0.5, cancel, and the $|0\rangle$ amplitudes, +0.5 and +0.5, reinforce to 1. Measure, and you get 0 with certainty. Two random-looking operations combined into a certain result because the amplitudes interfered: the negative sign did the work, and probabilities, which cannot be negative, could never have produced it. Now take two qubits, apply a Hadamard to the first, and then a CNOT, the two-qubit gate that flips the second qubit when the first is 1. The state is $(|00\rangle + |11\rangle)/\sqrt{2}$, an entangled pair. Measure the first and you get 0 or 1 at random, and the second then agrees with certainty. Every quantum algorithm is an arrangement of such interferences across many qubits, designed so that the wrong answers cancel and the right one survives.

1e. Why 'Exponential' Is Right and 'Tries Everything' Is Wrong

The popular description, that a quantum computer tries all 2^n possibilities at once and picks the best, is false, and the falsehood matters because it produces wrong expectations. A quantum computer does hold a superposition over 2^n states, but a measurement returns one of them at random, so 'trying everything' would yield a random answer. What quantum algorithms do is exploit the structure of a specific problem so that interference concentrates the amplitude on the answer. That is possible for problems with the right mathematical structure, such as the periodicity behind factoring, the amplitude amplification behind search, and the quantum nature of chemistry, and, as far as anyone knows, not for most problems. The honest summary is that quantum computers are not faster computers but computers of a different kind: exponentially faster at a small set of problems, quadratically faster at a larger set, and no faster at most.

Module 1 Key Points

Foundations

• A qubit's two amplitudes give its measurement probabilities; because amplitudes can be negative, they interfere, and interference is the resource.

• Entanglement is a joint state that cannot be split into parts; it carries no signal, and n qubits need 2^n amplitudes.

• Measurement collapses a superposition to one outcome; decoherence is unintended measurement by the environment, the field's enemy.

• Two Hadamards return a qubit to 0 with certainty because the paths to 1 cancel; a Hadamard and a CNOT make an entangled pair.

• Quantum computers are exponentially faster at a few structured problems, quadratically faster at some, and no faster at most.

Module 1 Quiz

Check Your Understanding

1. What determines the probability of measuring a qubit as 0?

A) Its coherence time sets it.
B) The square of the amplitude for 0 sets the probability of reading 0.
C) The number of gates applied to it sets it.
D) Its temperature in the refrigerator sets it.

2. Why can entanglement not be used to send a message faster than light?

A) Each outcome is random until the two are compared
B) The state decays before any signal could be encoded in it, at every distance tried so far
C) Relativity forbids entanglement
D) It can, but only over short distances

3. In the worked example, why do two Hadamard gates return a qubit to 0 with certainty?

A) Decoherence resets the qubit to 0
B) The first gate measures the qubit, so the second always starts from a known state, which forces the outcome
C) The two paths to 1 cancel out
D) Hadamards do nothing

4. What is decoherence?

A) Collapse caused by a deliberate measurement at the end of a circuit
B) A two-qubit gate that entangles a pair
C) A programming error in a circuit
D) Measurement by the environment

5. Why is 'a quantum computer tries all answers at once' misleading?

A) Superposition is only a mathematical fiction, with no physical meaning in the machine
B) It tries no answers
C) A measurement returns one answer at random
D) Quantum computers are slower than classical ones at every task

Module 2 — The Physics, One Level Deeper

The Quantum Mechanics a Serious Reader Needs

Recommended Reading / Reference

Book: Leonard Susskind and Art Friedman, *Quantum Mechanics: The Theoretical Minimum*

Reference: The 2022 Nobel Prize in Physics scientific background (Aspect, Clauser, Zeilinger)

2a. The Wavefunction and the Schrödinger Equation

Quantum mechanics describes a system by a wavefunction, the complete list of amplitudes for every possible configuration, and the Schrödinger equation says how it changes in time: smoothly, deterministically, and linearly, like a wave. Nothing random happens while a system evolves. Randomness enters only at measurement, when the wavefunction is replaced by one of its possible outcomes with a probability given by the squared amplitude, a law called the Born rule. The equation's linearity is what makes superposition possible, since the sum of two solutions is a solution, and what makes quantum computing possible, since a gate acts on every component of a superposition at once. Its determinism makes quantum evolution reversible, so every gate can be undone, which is why quantum circuits are built from reversible operations and why measurement, the one irreversible step, is postponed to the end.

2b. Uncertainty and the Double Slit

Heisenberg's uncertainty principle is not a statement about clumsy measurement but about what exists. A particle does not have both a definite position and a definite momentum, and the product of the two uncertainties is bounded below by Planck's constant. For a qubit the analogous pairs are the different bases it can be measured in: a qubit that is definitely 0 in one basis is a 50-50 superposition in another. The double-slit experiment shows the phenomenon in its purest form. Send electrons one at a time through two slits, and over thousands of arrivals they build an interference pattern on the screen, as if each electron went through both slits and interfered with itself. Put a detector at the slits to see which one each electron takes, and the pattern vanishes, because the which-path information destroys the interference. That is measurement destroying superposition, in an experiment first done with electrons in 1961 and since repeated with molecules of 2,000 atoms.

2c. Bell's Theorem and the 2022 Nobel

Einstein, Podolsky, and Rosen argued in 1935 that entanglement's correlations must be explained by hidden variables, properties the particles carried from their creation, like a pair of gloves sent to different cities. In 1964 John Bell showed that any such local hidden-variable theory must satisfy an inequality on the correlations, and that quantum mechanics predicts violations of it. John Clauser (1972), Alain Aspect (1982), and Anton Zeilinger (1998 and after) measured the violations, closing successive loopholes until the 'loophole-free' tests of 2015, and they shared the 2022 Nobel Prize. The conclusion is not that information travels faster than light but that nature is not 'locally realistic': the particles did not carry pre-agreed answers. The practical consequence is that entanglement is a real physical resource, confirmed in experiments with every major loophole closed, on which quantum computing, quantum cryptography, and the quantum internet are built.

2d. No-Cloning, Tunneling, and the Interpretations

The no-cloning theorem of 1982 states that an unknown quantum state cannot be copied, a direct consequence of linearity. It is why classical error correction, which makes three copies and takes a majority vote, does not work for qubits, why quantum error correction needed a new idea (Module 6), and why quantum key distribution is secure, since an eavesdropper cannot copy the photons without disturbing them (Module 9). Quantum tunneling, a particle passing through a barrier it lacks the energy to climb because its wavefunction extends beyond it, is the mechanism of the Josephson junctions inside superconducting qubits, of flash memory, and of the search an annealer performs. The interpretations disagree about what the wavefunction is. In the Copenhagen view it is knowledge and collapse is real; in many-worlds every outcome happens in a branching universe and nothing collapses; in pilot-wave theory particles have definite positions guided by the wave. All of them agree about every experimental prediction, so the disagreement matters to philosophy and not, so far, to engineering.

Module 2 Key Points

The Physics, One Level Deeper

• The Schrödinger equation evolves the wavefunction smoothly and reversibly; randomness enters only at measurement, through the Born rule.

• Uncertainty is about what exists, not clumsy measurement; the double slit loses its pattern when which-path information is taken.

• Bell's theorem and the loophole-free tests honored by the 2022 Nobel show that entangled particles carry no pre-agreed answers.

• No-cloning forbids copying a qubit, which is why error correction needed a new idea and why quantum key distribution is secure.

• The interpretations disagree about what the wavefunction is and agree on every prediction.

Module 2 Quiz

Check Your Understanding

1. When does randomness enter quantum mechanics?

A) During every gate operation in a circuit

B) Only at measurement

C) Never, because the theory is fully deterministic from start to finish, measurement included, as the Schrödinger equation shows

D) During decoherence alone

2. What happens in the double-slit experiment when detectors record which slit each electron uses?

A) The pattern vanishes

B) It sharpens

C) It stays the same

D) The electrons stop at the slits

3. What did Bell's theorem and the experiments honored by the 2022 Nobel establish?

A) That quantum mechanics is incomplete

B) That information travels faster than light between entangled particles, at least over short distances

C) That entanglement is an illusion

D) That no pre-agreed values carried by the particles can explain the correlations they show when measured apart

4. Why does classical error correction, copying and voting, fail for qubits?

A) Qubits are too small to copy.

B) The no-cloning theorem forbids copying an unknown state.

C) It works, but too slowly to keep up with errors.

D) Copies would decohere faster than the original, so voting would always pick the wrong value.

5. What do the interpretations of quantum mechanics disagree and agree about?

A) They disagree on what the wavefunction is and agree on every prediction.

B) They agree about everything.

C) They disagree about the predictions of experiments and agree that the wavefunction is real, which is why they can be tested.

D) They disagree about distance and agree about the wavefunction's meaning in every case they cover.

Module 3 — A Brief History

From Planck to Logical Qubits

Recommended Reading / Reference

Book: Manjit Kumar, *Quantum: Einstein, Bohr, and the Great Debate About the Nature of Reality*

Reference: Richard Feynman, 'Simulating Physics with Computers' (1982), and Peter Shor's 1994 factoring paper, the two documents the field grew from

Year	Event	Why it mattered
1900	Max Planck explains the radiation of hot bodies by assuming energy comes in discrete quanta	The quantum is born, as a mathematical trick Planck disliked
1905	Albert Einstein explains the photoelectric effect with light quanta, later called photons	Light is particles too; the 1921 Nobel
1913	Niels Bohr's atom, with quantized orbits	Atoms have discrete energy levels
1925-28	Werner Heisenberg's matrix mechanics; Erwin Schrödinger's wave equation; Max Born's rule for probabilities; Paul Dirac's equation uniting quantum mechanics with relativity	The theory is complete
1935-2022	The argument over entanglement, from the Einstein-Podolsky-Rosen paper to the Nobel for Bell tests (Module 2)	Entanglement becomes a measurable resource
1947-60	The transistor and the laser, both quantum devices	Quantum physics becomes technology
1981	Richard Feynman proposes building quantum computers to simulate quantum physics	The idea of a quantum computer
1985	David Deutsch defines the universal quantum computer	The theoretical machine
1994	Peter Shor's factoring algorithm	A quantum computer could break RSA encryption, and the field's funding begins
1995-96	Shor's and Andrew Steane's error-correcting codes; Lov Grover's search algorithm	Error correction possible in principle; a second speedup
1998-2001	The first two-qubit demonstrations in nuclear magnetic resonance; Shor's algorithm factors 15	Proof of concept
2007-11	The transmon, a superconducting qubit designed at Yale; D-Wave sells the first commercial annealer	The dominant qubit design; the industry begins
2016	IBM puts a five-qubit computer on the cloud; China launches the Micius satellite	Public access; quantum communication in space
2019	Google's 53-qubit Sycamore claims 'quantum supremacy' on a sampling task (Module 8)	The first claim of a task beyond classical reach
2022	NIST selects its first post-quantum algorithms (Module 9)	The defense against Shor begins
2023-26	The error-correction era (Module 6)	Logical qubits better than their parts

3a. The Century of Theory

Quantum mechanics was built in a quarter century by a dozen people who mostly disliked what they found. Planck hoped his quantum would go away, and Einstein, who made it physical, spent the rest of his life resisting its consequences. The debates between Bohr and Einstein over whether the theory was complete produced the puzzle of entanglement, which took the rest of the century to settle (Module 2). Through all of it the theory never failed a test. It is the most precisely confirmed theory in science, its prediction of the electron's magnetism agreeing with experiment to about one part in a trillion. It also produced the transistor,

the laser, nuclear magnetic resonance, and the semiconductor industry, which is to say the modern world, without anyone building a machine that used its strangest features directly.

3b. The Idea of a Quantum Computer

That step began with Feynman's observation that simulating quantum systems on classical computers is exponentially hard, since a molecule of a few dozen atoms has more amplitudes than any conceivable classical memory could hold, and that a computer built from quantum parts might do it naturally. The field stayed a curiosity until Shor's algorithm. RSA encryption, which secures much of the internet, rests on factoring being hard, so a fast quantum factoring method turned an academic idea into a national-security question overnight. The error-correcting codes that followed showed that the no-cloning theorem was not fatal, which made the machine buildable in principle, and Grover's search gave a second, smaller speedup. The first experiments were demonstrations of principle on a handful of qubits.

3c. From Curiosity to Industry

The hardware era ran on three inventions: the transmon, which IBM and Google adopted; the trapped-ion qubit, refined at NIST and Oxford; and the neutral-atom array, which Harvard, Caltech, and their spinouts scaled in the 2020s. D-Wave's annealers made the first commercial market, IBM's cloud let anyone run a circuit, and Google's sampling experiment made the field a public contest over speed. The milestones that mattered most in the 2020s, however, were about errors rather than qubit counts: the first logical qubits that outperformed the physical qubits they were made of, and the first codes whose errors fell as they grew. Those results, the subject of Module 6, took the field from a reluctant mathematical trick to error-corrected machines.

Module 3 Key Points

A Brief History

• The theory was built in 1900-28 by people who disliked it, has never failed a test, and produced the transistor and laser.

• Feynman proposed quantum computers in 1981 to simulate quantum physics, which is exponentially hard for classical machines.

• Shor's 1994 factoring algorithm turned the idea into a national-security question, because RSA encryption rests on factoring being hard.

• Error-correcting codes in 1995-96 made the machine buildable in principle, despite the no-cloning theorem.

• Three inventions built the industry, the transmon, the trapped ion, and the atom array, and the decisive milestones concern errors.

Module 3 Quiz

Check Your Understanding

1. Why did Planck introduce the quantum in 1900?

A) He wanted to explain the photoelectric effect, which classical light could not.
B) He meant to explain entanglement, which Einstein had just described.
C) He set out to challenge Einstein's relativity with a rival theory of light.
D) He needed it to fit the radiation of hot bodies.

2. What was Feynman's 1981 insight?

A) That RSA was breakable
B) That qubits could be cloned
C) That simulating quantum physics needs a quantum machine
D) That light is made of particles

3. Why did Shor's 1994 algorithm transform the field?

A) It showed a quantum computer could factor fast enough to break RSA encryption, which secures much of the internet.
B) It built the first working qubit in a laboratory at Bell Labs.
C) It proved that quantum error correction was impossible.
D) It made quantum hardware cheap enough for any university to buy.

4. Which three inventions built the quantum hardware industry?

A) The vacuum tube, the transistor, and the laser
B) Photons, electrons, and neutrons
C) The transmon, trapped ions, and atom arrays
D) The annealer, the mainframe, and the graphics chip

5. What kind of milestone mattered most in the 2020s, by the module's account?

A) Counts of physical qubits
B) Error milestones
C) Stock prices of the quantum companies after each announcement, which drew in the capital the field needed
D) Cloud access to machines

Module 4 — Qubits and Hardware

The Ways to Build a Qubit, on the Metrics That Matter

Recommended Reading / Reference

Reference: The companies' technical papers and roadmaps (IBM, Google, Quantinuum, IonQ, QuEra, PsiQuantum, Microsoft), and the *Nature* and *Physical Review* hardware results behind the tables

4a. The Modalities

Modality	What the qubit is	Best two-qubit fidelity (October 2026)	Coherence	Gate speed
Superconducting	Oscillation modes of a circuit of Josephson junctions on a chip	Median errors of about 0.15-0.4% on the leading chips (Google, IBM, USTC); IBM's best couplers below 0.1%	About 100 μs to 1 ms	10-100 ns, the fastest
Trapped ion	Energy levels of ions of ytterbium, barium, or calcium, held in electromagnetic traps and controlled by lasers or microwaves	99.99% on a two-qubit prototype (IonQ, company claim); 99.921% across all pairs of a working machine (Quantinuum)	Seconds to minutes	10-100 μs, slow
Neutral atom	Energy levels of rubidium, cesium, or strontium atoms held in optical tweezers and entangled through highly excited Rydberg states	About 99.5% (Harvard and QuEra, 2023)	Seconds	About 1 μs
Photonic	Photons' paths or time bins in silicon waveguides	99.22% for the 'fusion' that joins photons, counting only runs in which the photons arrived (PsiQuantum)	Immune to decoherence, but photons are lost	Light speed; gates succeed only with some probability
Spin (silicon)	The spin of an electron or nucleus in a silicon quantum dot or donor atom	Above 99% on every operation, on devices from a 300 mm industrial wafer (imec and Diraq, 2025)	About 1 ms for electrons; seconds for nuclei	About 100 ns
Topological (Majorana)	A hypothesized protected state in a superconductor-semiconductor nanowire	None shown	Protected, in theory	—
Annealer (not gate-based)	Superconducting flux qubits that settle into low-energy solutions	Not applicable	Short	—

Modality	Connectivity	Temperature	Largest systems (October 2026)	Who builds it
Superconducting	Nearest neighbors on a grid, through couplers	About 15 millikelvin, in a dilution refrigerator	IBM's Condor, 1,121 qubits on one chip (2023); IBM's Nighthawk, 120 qubits with denser couplings; Google's Willow, 105; USTC's Zuchongzhi 3.2, 107	IBM, Google, Rigetti, IQM, Alice & Bob, OQC, USTC
Trapped ion	Any qubit to any other within a trap; ions shuttled between zones	Trap at room temperature in vacuum; cooling optional	Quantinuum's Helios, 98 qubits; IonQ's Tempo	Quantinuum, IonQ (with Oxford Ionics), AQT, eleQtron

Modality	Connectivity	Temperature	Largest systems (October 2026)	Who builds it
Neutral atom	Reconfigurable, since atoms can be moved	Room temperature, in ultra-high vacuum	Caltech held 6,100 atoms with no gates run (2025); Harvard, MIT, and QuEra kept more than 3,000 qubits for over two hours by continuous reloading (2025); Atom Computing about 1,200; Pasqal more than 1,000	QuEra, Pasqal, Atom Computing, Infleqtion, planqc; Google, through its program in Boulder (Module 6)
Photonic	Through fusion; flexible	Room temperature, with cryogenic detectors	Xanadu's Aurora, 12 qubits (2025); PsiQuantum building toward a million-qubit machine (Module 6)	PsiQuantum, Xanadu, Quandela, QuiX, ORCA
Spin (silicon)	Nearest neighbors; crossbar designs	About 100 mK to 1 K, warmer than superconducting	Tens of qubits; Intel's Tunnel Falls, 12	Intel, SQC, Diraq, Quantum Motion, QuTech
Topological (Majorana)	—	Millikelvin	Single test devices (4b)	Microsoft
Annealer (not gate-based)	A fixed graph	Millikelvin	D-Wave's Advantage2, more than 4,400 qubits	D-Wave

Approximate values from company disclosures and publications. Fidelities are the best reported, not typical, and company figures are claims.

4b. The Tradeoffs

No modality wins on every metric, which is why five are funded at scale. Superconducting qubits are the fastest and the most manufacturable, since they are chips, but they have the shortest coherence, need dilution refrigerators, and connect only to their neighbors, which makes error correction expensive. Trapped ions hold the fidelity and coherence records and the freest connectivity, but their gates are about a thousand times slower, and scaling beyond a few hundred requires shuttling ions between zones or linking traps with photons. Neutral atoms scale to thousands cheaply and can be rearranged in the middle of a computation, the property behind the Harvard group's logical-qubit results (Module 6), but their gate fidelities trail the ions' and moving them is slow. Photons never decohere and run at room temperature, but they are lost in transit and their gates are probabilistic, so PsiQuantum's bet is on making millions of them. Silicon spins promise to use the semiconductor industry's factories at warmer temperatures, and the industrial-wafer results in the table are a step toward that, but their devices remain small.

Microsoft's topological qubit would be protected from errors by physics rather than by code, and its evidence is the most disputed in the field. Majorana 1's paper in *Nature* showed a single parity measurement, and the journal's editors noted that it was not evidence of the Majorana states the qubit depends on; a 2018 Majorana paper by Microsoft-backed researchers had been retracted in 2021. Majorana 2, a preprint, reported a parity lifetime of about 22 seconds, roughly a thousand times longer, on a single device, with no qubit operations, braiding, or logical qubit. A peer-reviewed critique of Microsoft's test protocol by Henry Legg of the University of St Andrews appeared in *Nature* alongside Microsoft's rebuttal, and Microsoft has reportedly brought its target for a scalable machine forward (Module 6). The lesson is to watch what is demonstrated rather than what is announced.

4c. Why Qubit Count Is the Wrong Scoreboard

The most-cited metric, the number of qubits, is the least useful, because a thousand noisy qubits cannot do what fifty good ones can. Four metrics decide usefulness. The first is the error rate per gate: a 99.9% gate fails once in a thousand operations, and useful algorithms need billions. The second is coherence relative to gate time, the number of operations that fit before the state decays, which is about a thousand for superconducting qubits and far more for ions. The third is connectivity, how far a qubit must be moved to interact, which sets the overhead of error correction. Above all, the fourth is the number and quality of logical qubits a machine can sustain. IonQ's 'algorithmic qubits', Quantinuum's logical-qubit counts, and Google's error-suppression ratio are the industry's attempts to report what matters, and DARPA's Quantum Benchmarking Initiative (Module 11) is the government's attempt to referee them.

Module 4 Key Points

Qubits and Hardware

• Six kinds of qubit and the annealer compete on fidelity, coherence, speed, connectivity, temperature, and scale, and none wins on all.

• Superconducting qubits are fastest and most manufacturable; trapped ions lead on fidelity and coherence; atoms scale to thousands and rearrange.

• Photons do not decohere but get lost; silicon spins promise industrial factories; topological qubits remain undemonstrated.

• Microsoft's Majorana devices show parity measurements on single devices, not working qubits, and a peer-reviewed critique disputes its test.

• Qubit count is the wrong scoreboard: error rate, coherence against gate time, connectivity, and logical qubits decide usefulness.

Module 4 Quiz

Check Your Understanding

1. What is the main weakness of superconducting qubits?

A) Slow gates

B) Their chips are too large to make in factories, so every one is built by hand at great cost to the laboratory

C) Poor fidelity

D) Short coherence and millikelvin operation

2. Which modality holds the records for two-qubit fidelity and coherence?

A) Superconducting circuits

B) Trapped ions

C) Neutral atoms held in optical tweezers, because they can be moved between zones and kept for seconds

D) Photonic chips

3. What did Majorana 2 show, according to the module?

A) A parity lifetime of about 22 seconds on a single device, with no qubit operations

B) The first logical qubit

C) A working eight-qubit chip running error-corrected circuits

D) Braiding of Majorana states

4. Why is qubit count the wrong scoreboard?

A) Every machine reports the same count

B) More qubits always mean more errors, so the largest machines are the least useful ones on any task

C) Counts are kept secret

D) Good qubits beat many noisy ones

5. What property of neutral atoms lies behind the Harvard group's logical-qubit results?

A) They run at millikelvin temperatures.

B) Their gates are the fastest.

C) They can be rearranged in the middle of a computation.

D) Their two-qubit fidelity is the highest of any modality, above the ions'.

Module 5 — Gates, Circuits, and Algorithms

How Quantum Computers Compute, and Where the Speedups Are

Recommended Reading / Reference

Reference: Nielsen and Chuang, chapters 4-6; the Quantum Algorithm Zoo (quantumalgorithmzoo.org); Scott Aaronson's blog, *Shtetl-Optimized*, on which speedups are real

5a. Gates and Circuits

A quantum program is a circuit: a sequence of gates applied to qubits, followed by measurement. Single-qubit gates rotate a qubit's state, and two-qubit gates create entanglement. Any quantum computation can be built from single-qubit rotations and CNOTs, just as any classical one can be built from NAND gates, so the set is called 'universal'. Every gate is reversible (Module 2). The circuit's depth, its number of sequential layers, is limited by coherence, and the output is read by measuring every qubit at the end, which gives one string of classical bits sampled from the final state's probabilities. Running the circuit many times, in repetitions called 'shots', estimates that distribution, and a well-designed algorithm makes the right answer its most likely outcome.

Gate	Acts on	What it does	Role
X (Pauli-X)	1 qubit	Flips $\|0\rangle \leftrightarrow \|1\rangle$	Quantum NOT
Z (Pauli-Z)	1 qubit	Flips the sign of $\|1\rangle$'s amplitude	Phase flip, the error type classical computers lack
H (Hadamard)	1 qubit	Makes an equal superposition (Module 1)	Creates superposition and interference
S, T (phase gates)	1 qubit	Rotate the phase by 90° or 45°	T is expensive to perform under error correction, so a circuit's 'T-count' is a measure of its cost
CNOT (CX)	2 qubits	Flips the target if the control is $\|1\rangle$ (Module 1)	Entanglement; the universal two-qubit gate
CZ	2 qubits	Flips the phase if both are $\|1\rangle$	The native gate on many superconducting chips
Toffoli (CCX)	3 qubits	Flips the target if both controls are $\|1\rangle$	Reversible AND, for arithmetic
Measurement	1 qubit	Collapses the qubit to 0 or 1	Reads out the answer, irreversibly

5b. Shor's Algorithm

Factoring a large number is hard for classical computers because the running time of the best known methods grows almost exponentially with the number's length, and by standard estimates factoring a 2,048-bit RSA key would take them longer than the age of the universe. Shor's insight was that factoring reduces to finding the period of a sequence, the remainders left when successive powers of a random number are divided by the number to be factored, and that a quantum computer can find a period exponentially fast. It prepares a superposition over all inputs and computes the sequence into a second register in one pass. It then applies the quantum Fourier transform, the quantum version of the operation that finds the frequencies in a signal, which makes the amplitudes interfere so that a measurement returns the period with high probability. Ordinary arithmetic turns the period into the factors. The quantum algorithm's cost grows only as roughly the cube of the number's length, so the gap between the two methods widens exponentially as keys get longer. Its price is the length of the computation, far more clean

operations than noisy qubits survive, which is why it needs error correction (Module 6) and why the estimates of its cost (Module 9) are the field's most consequential numbers.

5c. Grover's Search, Worked

Grover's algorithm searches an unstructured list of N items for one that satisfies a condition in about √N steps instead of N, a quadratic speedup. It works by amplitude amplification. Start in an equal superposition over all items, apply an 'oracle', a circuit that recognizes the answer and flips the sign of its amplitude, and then apply a reflection that boosts the marked amplitude and shrinks the rest. Each round rotates the state a little toward the answer, and after about $(\pi/4)\sqrt{N}$ rounds a measurement returns it with near certainty. It is the general-purpose quantum speedup, applicable to any problem whose answers can be checked, and because it is quadratic rather than exponential its practical value is limited.

Worked example — Grover Versus Brute Force

Search a space of 2^{64} possibilities, the keys of a 64-bit cipher. Classical brute force needs about 2^{63}, or 9×10^{18}, tries on average, and Grover about $(\pi/4) \times 2^{32}$, or 3.4×10^{9} rounds, which looks like a factor of nearly three billion until the cost of each round is counted. Assume each Grover round, one encryption under error correction, takes a millisecond on a machine of the 2030s. That makes 3.4 billion rounds about 40 days on one machine, and splitting the search across k machines shortens it only by a factor of √k. Classical brute force at 10^{12} tries a second on a large cluster takes about 100 days. The quantum advantage is real and modest. Against a 128-bit key it is useless, because $(\pi/4) \times 2^{64}$ rounds, about 1.4×10^{19}, at a millisecond each would take about 460 million years. That is why the answer to Grover is to double key lengths, as AES-256 does, and why the cryptographic threat comes from Shor's exponential speedup rather than Grover's quadratic one.

5d. Simulation, Variational Algorithms, and the Complexity Map

Quantum simulation, the use of a quantum computer to model molecules and materials, is the purpose Feynman proposed (Module 3), and it has the strongest theoretical case for an exponential speedup because the problem is itself quantum. The states available to a catalyst's electrons grow exponentially with the number of atoms, as a quantum computer's grow with its number of qubits, so one can represent the other. A routine called phase estimation, which reads out a system's energy levels, can compute a molecule's lowest energy to 'chemical accuracy', the precision needed to predict how a reaction goes, given enough clean qubits and a good starting guess. Whether that beats the best classical methods on molecules that matter is argued in Module 8. The variational algorithms, the variational quantum eigensolver (VQE) and the quantum approximate optimization algorithm (QAOA), dominated the 2018-24 era of what John Preskill named 'noisy intermediate-scale quantum' (NISQ) machines. They tried to do the job with a classical optimizer in the loop.

The complexity map shows where speedups can be expected. BQP, the class of problems quantum computers solve efficiently, contains P, the class classical computers solve efficiently, and it contains factoring and simulation, which are believed to lie outside P. It is believed not to contain the NP-complete problems, the hardest problems whose answers can be checked quickly, such as the traveling-salesman problem and most scheduling and optimization. As far as is known, a quantum computer can help with those only quadratically, through Grover's search, which is why the optimization and machine-learning claims deserve the skepticism Module 8 applies.

Algorithm or task	Speedup over the best classical method	Example	Needs error correction?	Status (October 2026)
Shor (factoring, discrete logarithms)	Exponential	Breaking RSA and elliptic-curve keys	Yes: a thousand or more logical qubits and billions of operations	Not yet achievable; cost estimates in Module 9
Simulation by phase estimation	Exponential, for quantum systems	Catalyst and battery chemistry; nitrogenase	Yes; requirements in Module 8	None yet; expected timing in Module 8
Grover (unstructured search)	Quadratic	Searching keys; subroutines in optimization	Yes, at useful sizes	Marginal even when available
Quantum linear algebra (HHL, after Harrow, Hassidim, and Lloyd)	Exponential under narrow conditions	Solving linear systems	Yes, with heavy caveats on loading data in and out	Theoretical
Variational methods (VQE, QAOA)	Unproven	Small molecules; small optimization problems	No	No demonstrated advantage over classical methods
Sampling (random circuits, boson sampling)	Exponential for the sampling task itself	Google's 2019 experiment; China's Jiuzhang	No	Beyond-classical claims, narrowed by classical methods (Module 8); no practical use
Quantum machine learning	Mostly unproven; several speedups 'dequantized', matched by new classical algorithms	—	Varies	Skeptical consensus
Annealing	No proven speedup	Scheduling; magnetic materials	No	A commercial niche; speedup claims disputed (Module 8)

Module 5 Key Points

Gates, Circuits, and Algorithms

• A quantum circuit applies reversible gates and ends in measurement; single-qubit rotations plus CNOT are universal, and T gates are the costly ones.

• Shor's algorithm turns factoring into period-finding, which the quantum Fourier transform does exponentially faster, but it needs error-corrected machines.

• Grover's search gives a quadratic speedup: modestly useful against 64-bit keys, hopeless against 128-bit ones, so doubling key length is the defense.

• Simulation of molecules and materials has the strongest case for an exponential speedup; the noisy era's variational algorithms beat no classical method.

• BQP is believed to exclude NP-complete problems, so quantum help with optimization and machine learning is likely quadratic at best.

Module 5 Quiz

Check Your Understanding

1. Why is a quantum circuit run many times?

A) Each run's measurement samples one bit string from the final state's probabilities

B) Its gates fail too often to trust one run

C) Measurement is reversible, so each run must be undone and repeated before its result can be read out by the classical computer

D) The qubits must cool between runs

2. What does Shor's algorithm reduce factoring to?

A) Searching all factors

B) Annealing to a minimum

C) Finding a period

D) Solving a linear system

3. In the worked example, why is Grover's search useless against a 128-bit key?

A) Its oracle cannot be built for a 128-bit cipher

B) Its 1.4×10^{19} rounds, at a millisecond each, would take about 460 million years

C) Quadratic speedups stop at 64 bits

D) Error correction fails on long keys

4. Which application has the strongest theoretical case for an exponential speedup?

A) Scheduling deliveries

B) Training neural networks

C) Quantum annealing

D) Molecular simulation

5. What does the complexity map imply about NP-complete problems such as scheduling?

A) Quantum computers solve them exponentially faster

B) BQP contains them

C) Annealing solves them in polynomial time, as commercial scheduling results on D-Wave machines have shown

D) Quantum help is likely limited to Grover's quadratic speedup

Module 6 — Error Correction and the Road to Fault Tolerance

The Single Problem That Decides Everything

Recommended Reading / Reference

Reference: Google Quantum AI, 'Quantum error correction below the surface code threshold' (*Nature*, December 2024); Quantinuum's Helios technical papers; IBM's papers on qLDPC codes and the 'gross code'; the Harvard, MIT, and QuEra neutral-atom papers in *Nature* (2023 and 2025)

6a. Physical and Logical Qubits

Every qubit built so far makes errors far too often for useful algorithms (Module 4), so no physical qubit is good enough on its own. No-cloning rules out the classical remedy of copying and voting (Module 2). The quantum remedy, the codes of Shor and Steane (Module 3), spreads one logical qubit across many physical qubits and checks them by measuring parities. A parity measurement reveals whether neighboring qubits agree without revealing their values, so it detects an error without collapsing the encoded state, and a classical computer called a decoder works out from the pattern of failed checks which correction to apply. The threshold theorem, proved in 1996-98, shows that if physical error rates are below a threshold, about 1% for the most common code, then adding physical qubits per logical qubit drives the logical error rate down exponentially. A machine that can run arbitrarily long computations this way is called fault-tolerant. Every roadmap in the field rests on that theorem, and the results since 2024 are the first hardware demonstrations that it holds.

6b. The Surface Code, Worked

The surface code, that most common code, arranges physical qubits in a two-dimensional grid, with data qubits interleaved with measure qubits that repeatedly check the parities of their neighbors; each round of checks is called a cycle. A code of distance d uses about $2d^2$ physical qubits to encode one logical qubit and can correct up to $(d-1)/2$ errors per cycle. Its virtues are that it needs only nearest-neighbor gates, which suits superconducting chips, and that it tolerates the highest physical error rates of any practical code. Its cost is the overhead, and the measure of progress is the suppression factor Λ (lambda), the factor by which the logical error falls with each increase of two in distance.

Worked example — Distance, Overhead, and Logical Error

A distance-3 surface code uses 17 physical qubits, 9 data and 8 measure, and corrects one error per cycle; distance 5 uses 49 and corrects two; distance 7 uses 97, nearly all of Willow's 105, and corrects three. Google's December 2024 result was that the logical error fell by a factor Λ of 2.14 with each step, to 0.143% per cycle at distance 7. Now extrapolate, assuming the factor holds. Reaching one error in a trillion cycles, roughly what Shor's algorithm on a 2,048-bit key needs, takes about 28 more steps, a distance near 63, and about 8,000 physical qubits per logical qubit, so a thousand logical qubits would need about 8 million. Next assume physical errors about five times lower, which raises Λ to about 10, since Λ scales roughly as the threshold divided by the physical error rate. The same target then needs a distance near 21, about 900 physical qubits per logical qubit, and under a million for a thousand logical qubits. Resource estimates such as those in Module 9 typically assume a uniform 0.1% error on every operation, which in standard noise

models gives a Λ near 10. That is the strategy in one calculation: make the physical qubits a few times better, and the machine shrinks nearly tenfold.

6c. Better Codes

The overhead has driven a search for codes that encode more logical qubits per physical qubit, and quantum low-density parity-check (qLDPC) codes are the leading family. IBM's 'gross code' stores 12 logical qubits in 144 data qubits plus 144 check qubits, which IBM says cuts the overhead by about 90%, but it needs long-range connections that a flat grid of neighbors cannot provide. IBM's Loon test chip (2025) carries those connections, and Kookaburra (6d) is planned as the first module that both stores and processes encoded information. Google's color code (6d) packs a logical qubit into fewer physical ones than the surface code and makes some logical gates easier.

Machines with flexible connectivity can run codes a grid cannot. Quantinuum reports that Helios, whose ions can be moved so that any qubit meets any other, ran 48 error-corrected logical qubits on its physical qubits (Module 4), using a code of distance 4 spread across 80 of them. Two caveats apply. Runs in which the code found an error it could not correct were discarded, about 38% of them, and the larger counts of 50, 64, and 94 logical qubits used codes that only detect errors, the 94 at distance 2 with about a quarter of runs kept. Bosonic 'cat' qubits, used in Amazon's Ocelot chip (2025) and by the French company Alice & Bob, build protection against one type of error into the physical qubit, so that a simpler code can handle the rest; Amazon says this can cut the overhead by up to 90%. Microsoft's topological approach would protect the qubit by physics, if it works (Module 4). The field's hope is that the overhead of a thousand to one, assumed a decade ago, will fall to between ten and a hundred to one, the difference between a million-qubit machine and one of a hundred thousand.

6d. The Milestones and the Roadmaps

Date	Who	Result	Significance
Dec 2023	Harvard, MIT, and QuEra	48 logical qubits on 280 atoms, mostly in codes that detect errors rather than correct them	Logical circuits at scale, made possible by moving atoms
Sep 2024	Microsoft and Quantinuum	12 entangled logical qubits on the H2, with errors far below the physical ones (company claim)	Logical qubits better than their parts
Dec 2024	Google	Surface codes of distance 3, 5, and 7 on Willow, with Λ of 2.14	The threshold theorem confirmed in hardware
Jun 2025	Google	A color code below threshold, with Λ of 1.56; the states that supply T gates (Module 5) prepared at 99% fidelity	A second, more compact code works
Nov 2025	Quantinuum	Helios's logical qubits, with the caveats in 6c	Efficient codes on ions that can be moved
Nov 2025	Harvard, MIT, and QuEra	448 atoms; surface-code errors cut 2.14 times from distance 3 to 5; logical gates	Below threshold on neutral atoms
Dec 2025	USTC	Zuchongzhi 3.2: a distance-7 surface code with Λ of 1.40	Below threshold in China
Jul 2026	Google	Self-calibration by reinforcement learning; 0.077% error per cycle at distance 7	Machines that calibrate themselves

Company	Target	Logical qubits	Date	Approach
IBM	Starling	200, running 100 million operations	2029	qLDPC codes on linked superconducting modules: Kookaburra (2026) the first, Cockatoo (2027) joining two; Blue Jay, more than 2,000 logical qubits, from 2033
Google	A useful error-corrected machine	Not stated	By the end of the decade	Surface and color codes on superconducting chips; a neutral-atom program in Boulder, with QuEra, since March 2026
Quantinuum	Sol, then Apollo	Hundreds, for Apollo, with universal fault tolerance	2027; 2029	Trapped ions moved between zones; efficient codes
IonQ	2 million physical qubits	40,000-80,000	2030	Trapped ions on chips from Oxford Ionics, linked by photons
QuEra	Libra	More than 256, at errors of one in a million, on Amazon's cloud	2028	Neutral atoms
Microsoft and Atom Computing	Magne, for Denmark	About 50, on about 1,200 atoms	Start of 2027	Neutral atoms
PsiQuantum	A utility-scale photonic machine	Not stated; about a million physical qubits	No firm date	Photons; construction near Brisbane began in June 2026, after a missed 2025 target; Chicago's first phase is a test system for DARPA
Microsoft	A scalable topological machine	Not stated	2029 (reported)	Majorana devices (Module 4)
DARPA (QBI)	Verify a utility-scale machine	—	2033	A staged evaluation of companies' designs (Module 11)

Company targets as stated, all of them claims; the field's record of slippage suggests treating the dates as optimistic.

6e. When Will Fault Tolerance Arrive?

The roadmaps' advocates make a strong case. Error suppression below threshold has now been shown on superconducting chips by Google and USTC and on neutral atoms by Harvard, MIT, and QuEra, so the physics is no longer in doubt. Physical fidelities keep improving, which shrinks the overhead faster than in proportion, as the worked example shows, and the leading companies converge on useful fault-tolerant machines around 2029. The skeptics answer that every result so far is a memory or a few logical operations at low distance, often with runs discarded. Useful algorithms need thousands of logical qubits (Module 5), decoders fast enough to keep up in real time, and wiring, cooling, and control at a scale no one has built. They point to slippage at PsiQuantum's Brisbane site (6d) and at Rigetti, which delayed its 108-qubit system in January 2026 when its gates fell short of target. A minority, most prominently the mathematician Gil Kalai, argues that correlated noise will stop error correction from scaling at all.

The evidence so far favors the physics and leaves the schedule open. Suppression has been reproduced, but the best Λ in the table is far below the 10 that makes the overhead manageable, and the largest error-corrected logical-qubit counts depend on discarding runs. This course's reading is that fault tolerance will arrive, because the threshold theorem has passed every test hardware has given it, but that the 2029 dates are the optimistic case. The first fault-tolerant machines are likely to run physics and chemistry simulations of scientific interest on a few hundred logical qubits well before any machine runs Shor's algorithm at the scale Module 9 describes.

Module 6 Key Points

Error Correction and the Road to Fault Tolerance

• Error correction spreads a logical qubit across many physical ones and checks parities, detecting errors without collapsing the encoded state.

• Below a threshold of about 1% error, adding qubits suppresses logical errors exponentially; Google, USTC, and Harvard have shown this in hardware.

• At Willow's suppression factor of 2.14, a thousand logical qubits need about 8 million physical; five-times-better qubits cut that below a million.

• Better codes cut the overhead, but read each claim's code distance and whether errors were corrected or only detected.

• Roadmaps converge on useful fault-tolerant machines around 2029, a date best treated as the optimistic case.

Module 6 Quiz

Check Your Understanding

1. What does a parity measurement reveal in error correction?

A) Whether qubits agree
B) The value of each data qubit
C) The logical qubit's full state
D) Which qubit decohered first

2. What did Google's December 2024 result on Willow show?

A) Shor's algorithm factored a small RSA key on it.
B) Logical errors fell about 2.14 times with each distance step.
C) Its single logical qubit ran for a full day without making any error.
D) Its two-qubit gates became error-free once the chip was cooled further.

3. In the worked example, what happens if physical errors fall about fivefold?

A) The code distance must rise to about 63
B) The overhead doubles
C) Λ rises to about 10, and a thousand logical qubits fit in under a million physical ones
D) Error correction is no longer needed

4. What kind of code did Helios use for its 94 logical qubits?

A) A distance-7 surface code
B) Error detection only
C) Topological protection
D) IBM's long-range gross code

5. What is this course's reading of the 2029 fault-tolerance dates?

A) They have already been met by Helios and Willow
B) They are impossible, because correlated noise will stop error correction from ever scaling, as the mathematician Gil Kalai has proved
C) They are conservative
D) They are the optimistic case

Module 7 — The Industry

The Companies, Their Revenue, and the Capital Wave

Recommended Reading / Reference

Reference: McKinsey, *Quantum Technology Monitor 2026* (April 2026); PitchBook's quantum reports; company filings from IonQ, Rigetti, D-Wave, and Infleqtion, and Quantinuum's S-1 registration (May 2026)

7a. Big Tech

The deepest pockets belong to companies that make little or no revenue from quantum computing. IBM has the longest program, with the first cloud quantum computer (Module 3), what IBM describes as the largest fleet of machines, and the most detailed roadmap (Module 6), and it treats quantum as a decade-long research and cloud business. Google Quantum AI has produced the field's most cited results, from the 2019 sampling experiment (Module 8) to the below-threshold codes (Module 6), and its neutral-atom program in Boulder is a hedge on modality by the company best placed to judge. Microsoft bet on topological qubits (Module 4) while working with Quantinuum and Atom Computing on logical qubits it could show sooner, and it sells access to others' machines through Azure Quantum. Amazon runs Braket, a cloud marketplace for other companies' machines, and builds its own cat-qubit chip (Module 6). Nvidia sells the classical side, the CUDA-Q software, the NVQLink interconnect, and the GPUs that run decoders, and has become the field's indispensable supplier without building a qubit; its venture arm is among Quantinuum's investors. Intel pursues silicon spins. None of them discloses what it spends on quantum.

7b. The Pure Plays

Company	Modality	Status (October 2026)	Capital raised or last private valuation	Revenue (2025)	Notes
Quantinuum	Trapped ion	Public (Nasdaq) since June 2026 (Module 12)	$600M at a $10B pre-money valuation (September 2025), then the IPO	$30.9M; 2026 guidance $28-32M	Helios; the logical-qubit leader; Honeywell holds about 48% of the votes
IonQ	Trapped ion	Public (NYSE)	More than $2B of share sales in 2025	$130.0M, up about 200%; 2026 guidance $280-290M	Tempo; the sector's most active acquirer
PsiQuantum	Photonic	Private	About $2.3B; $1B at a $6B pre-money valuation (September 2025)	Not disclosed	Sites in Brisbane and Chicago (Module 6); Australian public funding (Module 11)
Rigetti	Superconducting	Public (Nasdaq)	About $350M of share sales in 2025	$7.1M, down 34%	108-qubit system at about 99.1%; out of DARPA's QBI (Module 11)

Company	Modality	Status (October 2026)	Capital raised or last private valuation	Revenue (2025)	Notes
D-Wave	Annealing, and gate-based machines in development	Public (NYSE)	Several hundred million dollars of share sales in 2025	$24.6M	Advantage2 (Module 4); a gate-model acquisition (7d)
Infleqtion	Neutral atom; sensing and clocks	Public (NYSE) since February 2026, through a SPAC	More than $550M raised, at a deal value of about $1.7B	$31.1M	12 logical qubits (company claim); clocks and navigation
Xanadu	Photonic	Public (Nasdaq and Toronto) since March 2026, through a SPAC	About $302M at listing	Not disclosed	Aurora (Module 4); in DARPA's QBI Stage B
QuEra	Neutral atom	Private	$230M round (early 2025; Google, SoftBank)	Not disclosed	Harvard and MIT's partner (Module 6)
Pasqal	Neutral atom	Private (France)	About $237M (February 2026)	Not disclosed	Neutral-atom arrays (Module 4)
Atom Computing	Neutral atom	Private	Not disclosed	Not disclosed	Neutral-atom machines (Module 4); Microsoft's partner on Magne (Module 6)
IQM	Superconducting	Private (Finland)	$320M round (2025)	Not disclosed	A leading European maker of superconducting machines
Alice & Bob	Superconducting cat qubits	Private (France)	€100M round (January 2025)	Not disclosed	Targets 100 logical qubits by 2030
Horizon Quantum	Software	Public (Nasdaq) since March 2026, through a SPAC	About $120M at listing	Not disclosed	Tools for writing quantum programs
OQC, Quandela, planqc, SEEQC, Q-CTRL, Classiq	Various	Private	Tens to hundreds of millions of dollars each	Small	The second tier of hardware, control, and software
China: Origin Quantum, QuantumCTek, USTC's spinouts	Superconducting; photonic	State-backed	State funding	Not disclosed	Zuchongzhi; Jiuzhang; key-distribution networks (Module 10)

Company filings, announcements, and press reports; company figures are claims, and revenue is as reported.

7c. The Money

Investment in quantum companies jumped in 2025. McKinsey counts $12.6 billion invested in quantum start-ups that year, about six times 2024's, a figure that includes public offerings and follow-on share sales, while PitchBook counts $3.9 billion of venture capital across 125 deals, itself a record. Governments' commitments, larger still, are set out in Module 11. The money in 2026 has come mainly from public markets, through the listings in 7d and share sales, and from Washington, through the CHIPS letters of intent and DARPA's contracts (Module 11). Revenue is far smaller. McKinsey estimates that

quantum-computing companies took in more than $1 billion in 2025, much of it from governments, national laboratories, and research customers, and forecasts $4.4 billion by 2028. How the stock market has priced that gap is the subject of Module 12.

7d. Consolidation and Listings

The industry is consolidating. IonQ has been the most aggressive buyer, paying $1.075 billion for Oxford Ionics in 2025 and about $1.8 billion for SkyWater, an American chip foundry, in a deal that closed on July 31, 2026. With smaller purchases in networking, sensing, and photonics, its spending on acquisitions has passed $3 billion, much of it paid in shares. D-Wave bought Quantum Circuits, a superconducting gate-model start-up, for about $550 million in January 2026, and Google absorbed Atlantic Quantum, an MIT spinout, in 2025. Failures have been few since Zapata closed in 2024. Three of the companies in the table came to market in 2026 through special-purpose acquisition companies (SPACs), listed shells that merge with private firms, the route IonQ, Rigetti, and D-Wave took in 2021-22. Quantinuum chose a conventional initial public offering instead, the largest in the field's history (Module 12).

Module 7 Key Points

The Industry

• Big tech funds quantum without quantum revenue: IBM, Google, Microsoft, and Amazon build machines, and Nvidia supplies the classical side.

• Listed pure plays include IonQ, Quantinuum, Rigetti, and D-Wave; PsiQuantum, QuEra, and Pasqal lead the private ones.

• IonQ's 2025 revenue of $130 million led the sector; Quantinuum took in $31 million, D-Wave $25 million, and Rigetti $7 million.

• Investment hit a record in 2025, $12.6 billion by McKinsey's count including public offerings, against revenue of just over $1 billion.

• Consolidation is under way: IonQ has spent more than $3 billion on acquisitions, and three companies listed through SPACs in 2026.

Module 7 Quiz

Check Your Understanding

1. What role does Nvidia play in quantum computing?

A) It builds superconducting qubits in its own fabs.
B) It owns a controlling stake in Quantinuum.
C) It supplies the software, interconnects, and GPUs for the classical side.
D) It runs the largest cloud marketplace for other companies' quantum machines.

2. Which pure play had the largest revenue in 2025?

A) IonQ, with about $130 million, roughly triple the year before
B) Quantinuum, controlled by Honeywell, with about $100 million
C) D-Wave
D) Rigetti

3. How did McKinsey's count of 2025 quantum investment differ from PitchBook's?

A) It was smaller
B) It included public offerings and follow-on sales
C) It excluded every company outside the United States and Europe, counting only North American and European venture rounds
D) It counted only government grants

4. What route did Infleqtion, Xanadu, and Horizon Quantum take to the stock market?

A) Mergers with special-purpose acquisition companies, listed shells that merge with private firms
B) Direct listings without new shares
C) Conventional initial public offerings, the route Quantinuum also took
D) Spin-offs from Honeywell

5. Which company did IonQ buy for about $1.8 billion?

A) Oxford Ionics
B) Quantum Circuits, the gate-model start-up
C) Atlantic Quantum, a superconducting start-up from MIT
D) SkyWater, a chip foundry

Module 8 — Applications

What Is Real

Recommended Reading / Reference

Reference: Hoefler, Häner, and Troyer, 'Disentangling Hype from Practicality: On Realistically Achieving Quantum Advantage' (*Communications of the ACM*, 2023); Lee and colleagues, 'Evaluating the evidence for exponential quantum advantage in ground-state quantum chemistry' (*Nature Communications*, 2023); Google's Quantum Echoes paper (*Nature*, October 2025); IBM's public quantum advantage tracker

8a. The Honest Framework

The test for any claimed quantum application comes from Torsten Hoefler, Thomas Häner, and Matthias Troyer (2023), and it has three parts. Does the problem have an exponential quantum speedup? Does the speedup apply to the computation that dominates the cost? And are the input and output small enough that loading data in and reading results out does not erase the gain? Most proposed applications fail the third part, because a quantum computer cannot read a database faster than a classical one, so 'big data' applications are out. Most optimization and machine-learning applications fail the first, because their speedups are quadratic at best (Module 5). By the authors' estimate a fault-tolerant quantum computer will be so much slower per operation than a classical chip that a quadratic speedup would pay off only on impractically long computations. What survives the test is a short list.

Application	Passes the input and output test?	Logical qubits needed	Expected timing	Verdict
Chemistry: molecular energies for catalysts, batteries, and enzymes	Yes: a molecule in, an energy out	Hundreds to a few thousand, at very low error (8b)	First useful cases around 2027-30; nitrogenase-class problems in the 2030s	The leading candidate, though its speedup is disputed (8b)
Materials: superconductors, magnets, and strongly interacting electrons	Yes	Hundreds to thousands	Late 2020s to 2030s	Real; follows chemistry
Physics simulation: lattice models and dynamics	Yes	Tens to hundreds	Beyond-classical demonstrations now (8c); useful results in the late 2020s	Real; the first candidates for advantage
Cryptanalysis (Shor)	Yes	Module 9	Module 9	Real, and the reason for post-quantum cryptography
Optimization: logistics, scheduling, portfolios	Often no	Large	Unclear	Skeptical: quadratic at best
Machine learning	Usually no, because of data loading	—	—	Skeptical
Finance: pricing by Monte Carlo simulation	Marginal	Thousands for a useful, quadratic speedup	2030s at best	Marginal
Drug discovery beyond the chemistry step	Partly	—	2030s	Real for the chemistry step; hype elsewhere
Random-number generation and sampling	Yes	Few	Now	Real, but a niche

Timings are the expectations of companies and researchers, not demonstrated results.

8b. Chemistry and Materials

The best-founded application is computing the properties of molecules and materials whose electrons interact too strongly for classical approximation. The canonical target is the iron-molybdenum cofactor, or FeMoco, of nitrogenase, the enzyme with which bacteria fix nitrogen at room temperature, while the Haber-Bosch process that makes the world's fertilizer needs about 450°C and 200 atmospheres. It is a cluster of a few dozen atoms whose electronic structure is beyond every classical method, and understanding it could reshape fertilizer production. Other targets include catalysts for carbon capture, the cathode chemistry of lithium-ion and solid-state batteries, high-temperature superconductors, and the enzyme mechanisms behind drugs. The estimated cost of simulating FeMoco has fallen by orders of magnitude as algorithms improved.

Year	Work	Estimate for FeMoco
2017	Markus Reiher, Matthias Troyer, and colleagues	About 111 logical qubits and 10^{14} T gates
2021	Joonho Lee and colleagues	2,142 logical qubits, 5.3×10^9 Toffoli gates, about 4 million physical qubits, and about four days
2024	Rocca and colleagues	Cost roughly halved
2025	Low, Berry, Rubin, and colleagues	Further speedups of 4 to 195 times, depending on the method
2025	PsiQuantum and Boehringer Ingelheim	278 times faster than earlier estimates (company claim)
2025	Alice & Bob	Physical qubits cut from 2.7 million to 99,000 with cat qubits (preliminary company claim)

T and Toffoli gates are the expensive operations under error correction (Module 5).

Whether chemistry offers an exponential speedup is itself disputed. Its advocates argue that strongly correlated molecules such as FeMoco defeat every classical approximation, so a fault-tolerant machine that computed their energies exactly would be exponentially faster. A 2023 study by Seunghoon Lee, Garnet Chan, and colleagues concluded that 'evidence for such an exponential advantage across chemical space has yet to be found', because classical methods scale well on most molecules and preparing a good starting state on a quantum computer is itself hard. The results so far fit that caution. In October 2025 IBM and RIKEN paired a Heron processor with the Fugaku supercomputer on an iron-sulfur molecule and beat a standard classical approximation called CCSD, but not the best classical method for such molecules, DMRG. A protein-ligand simulation by Cleveland Clinic, RIKEN, and IBM in May 2026 did not beat the best classical methods either. Pharmaceutical and chemical companies, Boehringer Ingelheim among them, run quantum programs, and none has yet produced a result a classical computer could not. This course's reading is that chemistry remains the strongest application but that its speedup may prove polynomial rather than exponential for most molecules, with the decisive gains on strongly correlated ones such as FeMoco.

8c. The Advantage Claims, 2019-26

'Quantum advantage' means a quantum computer doing something useful faster than any classical computer, while 'beyond-classical', or 'supremacy', means doing anything, useful or not, that classical computers cannot match. The record of claims is the best guide to reading the next one.

Claim	What was claimed	The classical response	Standing (October 2026)
Google's Sycamore (2019)	Random circuits sampled in 200 seconds, a task Google said would take a supercomputer 10,000 years	IBM argued, two days before Google's paper appeared, that its Summit supercomputer could do it in 2.5 days; by 2022 Chinese groups did it in hours on GPUs	A real feat of control on a task with no use; the 10,000 years is gone
D-Wave (March 2025, *Science*)	An annealer simulated the dynamics of magnetic materials beyond classical reach	Groups at the Flatiron Institute and EPFL matched key cases classically within days of publication; D-Wave disputes them	Contested and narrowed
Google's Quantum Echoes (October 2025, *Nature*)	Willow measured an out-of-time-order correlator, which tracks how a disturbance spreads, on 65 qubits, about 13,000 times faster than the Frontier supercomputer could (company claim)	None published; the result can be checked on another quantum computer or against experiment	Unrefuted; beyond-classical on a physics task, not yet useful
IBM and partners (July 2026)	Three preprints on Heron processors claimed 'trusted quantum advantage', one of them explicitly	A team from the Singapore University of Technology and Design and Nvidia simulated the explicit claim in 37 minutes on 256 GPUs (August 2026)	The explicit claim matched; none adjudicated
Quantinuum (August 2026)	Helios simulated magnetic materials beyond classical computers (company claim)	No independent test yet	Untested

IBM's public advantage tracker, launched in November 2025 with Algorithmiq, the Flatiron Institute, and BlueQubit, is the most honest framing the industry has adopted: a claim counts only if it survives the classical community's attempts to beat it. The advocates of the recent claims argue that the line has now been crossed. Quantum Echoes measures a physical quantity rather than random samples, its answer can be checked, and no classical method has matched it in a year, while IBM's candidates come with certified bounds on their accuracy and an open invitation to challenge them. The skeptics answer that speed claims have a poor record: Sycamore's, D-Wave's, and IBM's explicit claim each fell to the classical responses in the table, because classical algorithms improve as fast as the challenges appear. Even the unrefuted results are on tasks chosen to be hard for classical computers rather than useful to anyone. This course's reading is that beyond-classical computation has now been shown on narrow physics tasks, most credibly by Quantum Echoes, but that no useful advantage has survived classical challenge as of October 2026, and that the first will most likely come from simulating physics or chemistry rather than from optimization or machine learning.

Module 8 Key Points

Applications

• An application needs an exponential speedup, on the dominant computation, with input and output small enough not to erase it.

• Chemistry, materials, and physics simulation pass the test; optimization and machine learning mostly fail it, and finance is marginal.

• FeMoco cost estimates fell from 10^{14} T gates in 2017 to billions of Toffolis by 2021, with further cuts claimed since.

• Chemistry's exponential advantage is disputed, and no pharmaceutical or chemical program has yet beaten the best classical methods.

• Speed claims keep narrowing under classical challenge; Quantum Echoes stands unrefuted, but no useful advantage has survived as of October 2026.

Module 8 Quiz

Check Your Understanding

1. Why do most 'big data' applications fail the test for quantum advantage?

A) Quantum computers cannot store more than a few kilobytes of classical data in any form
B) Their speedups are exponential only for small inputs
C) Loading the data erases the gain
D) Classical cloud computing costs less per query

2. Which enzyme's cofactor is the canonical chemistry target?

A) Cytochrome P450
B) Photosystem II
C) Nitrogenase
D) ATP synthase

3. What did IBM and RIKEN's October 2025 chemistry result beat?

A) The CCSD method
B) Every classical method
C) DMRG
D) The Fugaku supercomputer alone

4. What happened to the explicit advantage claim in IBM's July 2026 preprints?

A) It was confirmed by IBM's advantage tracker.
B) A classical team simulated it in 37 minutes on 256 GPUs.
C) It was withdrawn before peer review.
D) Google reproduced it on Willow within a week of the preprints.

5. Which advantage claim stood unrefuted as of October 2026?

A) Sycamore's sampling
B) D-Wave's annealing
C) IBM's explicit claim
D) Google's Quantum Echoes

Module 9 — Cryptography

The Threat and the Migration

Recommended Reading / Reference

Reference: NIST's FIPS 203, 204, and 205 and its HQC selection (2025); Craig Gidney, 'How to factor 2048 bit RSA integers with less than a million noisy qubits' (2025); the NSA's CNSA 2.0; Executive Order 14412 (June 2026); the Global Risk Institute's *Quantum Threat Timeline Report* (March 2026)

9a. What Breaks

Modern public-key cryptography rests on two problems that classical computers cannot solve at scale. Factoring underlies RSA, which secures most web certificates, email, and software signing, and the discrete logarithm on elliptic curves underlies elliptic-curve cryptography (ECC), which secures most key exchange on the web, Bitcoin and other blockchains, Signal, and most modern protocols. Shor's algorithm solves both (Module 5). A cryptographically relevant quantum computer, one able to run it at full scale, would let its owner read any recorded communication protected by RSA or ECC, forge signatures, and spend any cryptocurrency whose public key has been exposed. Symmetric ciphers such as AES and hash functions such as SHA-256 face only Grover's quadratic speedup, which longer keys answer (Module 5), so the migration is about public keys.

9b. When: The Resource Estimates and the Argument over Q-Day

Estimate	Date	Target	Physical qubits	Time	Assumptions
Gidney and Ekerå	2019	RSA-2048	20 million	About 8 hours	Surface code at 0.1% physical error
Gidney (Google)	May 2025	RSA-2048	Under 1 million	Under a week	Yoked surface codes, 'magic-state cultivation', and approximate arithmetic; 0.1% error and 1 μs cycles
'Pinnacle' preprint	February 2026	RSA-2048	Under 100,000	About a month	qLDPC codes needing connectivity not yet built
Google Quantum AI, with Dan Boneh and others	March 2026	256-bit elliptic curve, as in Bitcoin	Under 500,000	About 18 minutes	1,200-1,450 logical qubits; circuits withheld and verified by a zero-knowledge proof
Oratomic, Caltech, and UC Berkeley	March 2026	256-bit elliptic curve	10,000-26,000 atoms	From about 3 years down to about 10 days	Neutral atoms with qLDPC codes and 1 ms cycles, not yet shown

Papers and preprints; every estimate assumes hardware that has not been built.

The estimates matter because they set the migration deadline. In 2019 the machine required was so far beyond the roadmaps that the threat felt theoretical, and the estimates have since fallen so far that the elliptic-curve attack that would threaten Bitcoin sits inside the range that IonQ's and PsiQuantum's roadmaps announce (Module 6). The Global Risk Institute's survey of 26 experts, published in March 2026, put the chance of a machine that can break RSA-2048 within 24 hours at 28-49% within ten years and 51-70% within fifteen, so its median falls around 2036-40. The ten-year figure is the highest in the survey's seven years.

When 'Q-Day', the arrival of such a machine, will come is the field's most consequential argument. Those who expect it early point to the falling estimates, the below-threshold results and roadmaps of Module 6, and Google and Cloudflare have set early internal deadlines for their own migrations (9e). Those who expect it late note that every estimate assumes hardware no one has built. The best machines run tens of logical qubits at error rates far above what these attacks need (Module 6), and the leanest designs depend on connectivity or cycle times not yet demonstrated. This course's reading is that a machine able to break RSA-2048 or elliptic-curve keys is unlikely before about 2030 but plausible within a decade, and that because migration takes most organizations five years or more, the exact date matters less than the fact that the work must start now.

9c. Harvest Now, Decrypt Later

The threat does not wait for the machine. Encrypted traffic recorded today, by any intelligence service with the storage, can be decrypted whenever a quantum computer arrives, so any secret that must stay secret into the mid-2030s is already at risk: diplomatic cables, weapons designs, health records, trade secrets, and the long-lived keys that sign software updates. Signatures face a later risk, because a forgery requires the machine to exist when the signature is checked, which is why the deadlines below move key exchange first. It is also why migration deadlines are set a decade before the expected machine, and why 'it is fifteen years away' is not an argument for waiting.

9d. The Replacement: Post-Quantum Cryptography

Standard	Algorithm	Type	Based on	Role	Status (October 2026)
FIPS 203	ML-KEM (Kyber)	Key encapsulation	Module lattices	Replaces RSA and elliptic-curve key exchange	Final; widely deployed in hybrid mode
FIPS 204	ML-DSA (Dilithium)	Digital signature	Module lattices	Replaces RSA and ECDSA signatures	Final; not yet in web certificates
FIPS 205	SLH-DSA (SPHINCS+)	Digital signature	Hash functions	A conservative backup	Final; not approved for national security systems
FIPS 206	FN-DSA (Falcon)	Digital signature	NTRU lattices	Compact signatures	Submitted for approval in August 2025; final expected late 2026 or 2027
HQC	HQC	Key encapsulation	Error-correcting codes	A backup to ML-KEM on different mathematics	Selected March 2025; draft standard pending
SP 800-227	Guidance	—	—	How to use key encapsulation safely	Final September 2025
Hybrid modes	X25519 plus ML-KEM	Key exchange	Both	Belt and braces during the transition	The default in major browsers and operating systems

NIST ran an eight-year competition (2016-24) and standardized lattice-based schemes, whose security rests on problems believed hard for both classical and quantum computers, along with a hash-based backup, and it selected a code-based alternative. Key exchange has moved fastest. More than half of the human traffic through Cloudflare now uses post-quantum key agreement (company claim), a share that jumped when Apple's iOS 26 turned it on, and in October 2025 Signal added post-quantum protection to the 'ratchet' that keeps updating its keys. Signatures have barely begun, because ML-DSA's keys and signatures are far

larger than the ones they replace and certificate systems change slowly. The hard part is everything else: embedded devices, industrial controls, satellites, cars, and long-lived certificates that cannot easily be updated, and the inventories most organizations lack of where they use which algorithm. In 2022 classical attacks broke two candidates, the finalist Rainbow and the later-round candidate SIKE, the latter in about an hour on one processor core, which is the lesson that post-quantum algorithms are young and that the transition should be hybrid and agile.

9e. The Deadlines

Authority	Requirement	Deadline
NSA's CNSA 2.0 (US national security systems)	Software and firmware signing	Preferred from 2025; exclusive by 2030
NSA's CNSA 2.0	Browsers, servers, and cloud services	Preferred from 2025; exclusive by 2033
NSA's CNSA 2.0	New acquisitions of national security systems	Must comply from January 1, 2027
NSA's CNSA 2.0	All national security systems	Quantum-resistant by 2035
NSM-10 and OMB (2022)	Federal inventories and migration plans	Inventories from 2023; migration through 2035
Executive Order 14306 (June 2025)	A federal list of product categories where post-quantum products are available (published January 2026); TLS 1.3 across government	TLS 1.3 by January 2, 2030
Executive Order 14412 (June 22, 2026)	High-value and high-impact federal systems, excluding national security systems, move key establishment, then signatures; contractors meet NIST's standards	Key establishment by December 31, 2030; signatures by December 31, 2031; contractors by December 31, 2030; agency plans due October 22, 2026 under OMB's guidance (reported)
NIST IR 8547 (draft)	Deprecate 112-bit RSA and ECC; then disallow all quantum-vulnerable public-key algorithms	After 2030; after 2035
EU coordinated roadmap (2025)	Strategies and inventories; then high-risk uses and critical infrastructure	End of 2026; end of 2030; as far as feasible by 2035
UK National Cyber Security Centre (NCSC)	Discovery and plans; priority migrations; completion	2028; 2031; 2035
Canada; Australia	High-priority systems migrated; no traditional public-key cryptography	2031 (Canada); after 2030 (Australia)
Google; Cloudflare	Their own systems, including authentication	2029 (company targets)

Blockchains have no authority that can order a migration, and they are the largest unmigrated target. About 2.3 million bitcoin sit in old or reused addresses whose public keys are already exposed, by Google's count, and Bitcoin's leading proposal, BIP-360, was merged as a draft in February 2026 but not activated. Ethereum's developers aim to have post-quantum infrastructure in place around 2029.

Worked example — What Q-Day Means for One Organization

Take a hypothetical bank that holds 40 million customer records behind RSA-protected connections, signs its software with ECDSA, and runs 3,000 servers, 200 embedded devices in branches, and a decade of archived encrypted backups. First it must inventory every use of public-key cryptography, a year of work that most organizations have never done. Switching its connections to hybrid ML-KEM is largely its vendors' job and takes months. Re-signing its software with ML-DSA means updating every device that checks

signatures, and the embedded devices may lack the memory, so replacing them takes years. Archived backups whose contents matter past 2035 must be re-encrypted, or their exposure accepted, and the bank must plan to switch algorithms quickly if ML-KEM is ever broken. Assume the cost is tens of millions of dollars over five years. Starting now, the bank finishes around 2031, close to the federal deadlines and ahead of the experts' median estimate for Q-Day; starting in 2030, it would finish inside the window in which the early estimates put the machine.

9f. Quantum Key Distribution as a Defense

The other defense uses physics. Quantum key distribution sends keys as single photons whose states cannot be copied or observed without disturbance (Module 2), so an eavesdropper is detected; its networks and satellites are the subject of Module 10. Its limits are that it needs dedicated fiber or line-of-sight links, cannot by itself confirm who is at the other end and so still needs classical cryptography, can be attacked through flaws in its hardware rather than its physics, and does not scale to the internet. That is why the NSA and the NCSC recommend post-quantum cryptography over quantum key distribution for almost all uses, and why the latter's real market is high-security links between fixed points.

Module 9 Key Points

Cryptography

• Shor's algorithm breaks RSA and elliptic-curve cryptography; symmetric ciphers and hashes survive with longer keys, so the migration is about public keys.

• Estimates fell from 20 million qubits for RSA-2048 in 2019 to under a million in 2025, and under 500,000 for elliptic curves in 2026.

• Experts give better-than-even odds of a cryptographically relevant machine within about 15 years, and recorded traffic is already at risk.

• Post-quantum key exchange is widely deployed; post-quantum signatures, embedded devices, and inventories are the hard part of the migration.

• US high-value federal systems must move key exchange by 2030 and signatures by 2031, and national security systems by 2035.

Module 9 Quiz

Check Your Understanding

1. Why does Grover's algorithm not drive the post-quantum migration?

A) Longer symmetric keys answer its quadratic speedup

B) It cannot run on error-corrected machines, because its oracle needs more qubits than any surface code can supply at useful distances

C) It only searches sorted lists

D) Its speedup is exponential

2. Which survey put 28-49% odds on a cryptographically relevant machine within ten years?

A) NIST's draft guidance on deprecation

B) McKinsey's quantum monitor

C) The NSA's CNSA 2.0 FAQ

D) Global Risk Institute

3. What does Executive Order 14412 require of high-value federal systems?

A) They must stop using RSA by 2027.

B) They must move key establishment by 2030 and signatures by 2031.

C) They must switch to quantum key distribution networks by the end of 2030.

D) They must replace every elliptic-curve certificate before the end of 2026.

4. Why have post-quantum signatures moved more slowly than key exchange?

A) NIST has not yet finalized ML-DSA.

B) Signatures are not threatened by Shor's algorithm.

C) Their keys and signatures are far larger, and certificate systems change slowly.

D) Harvest-now attacks apply to signatures more than to keys.

5. What do the NSA and NCSC recommend for almost all uses?

A) Quantum key distribution

B) Longer RSA keys

C) Post-quantum cryptography

D) Larger elliptic curves

Module 10 — Sensing, Timing, and Communication

The Quantum Technologies Already in Service

Recommended Reading / Reference

Reference: The BIPM's roadmap for redefining the second; Q-CTRL's and SandboxAQ's navigation trial reports (2025-26); the *Nature* paper on the Jinan-1 satellite link (March 2025); the US Department of Energy's quantum internet blueprint (2020)

10a. Clocks

The oldest quantum technology in service is the atomic clock, which defines the second by the frequency of a cesium transition and underlies GPS, telecommunications, and financial timestamps. Optical lattice clocks, which hold strontium or ytterbium atoms in a lattice of laser light, are about 100 times more accurate than the best cesium clocks and would lose less than a second over the age of the universe. The bodies that govern the international system of units plan to redefine the second on an optical standard. Their time committee is to choose among the options in 2028-29, and the General Conference on Weights and Measures is to decide in 2030, if eight criteria are met, with the change taking effect later. A clock precise enough to detect that time runs slower a centimeter lower in Earth's gravity is also a gravity sensor, which is where sensing begins.

10b. Sensors and Navigation

Sensor	Principle	Advantage	Application	Status (October 2026)
Optically pumped magnetometer (OPM)	The spins of alkali atoms in a vapor cell precess in a magnetic field	Works at room temperature; femtotesla sensitivity	Wearable brain imaging (MEG) replacing helium-cooled sensors; mineral exploration	Commercial research systems (Cerca Magnetics, QuSpin); clinical studies
NV-diamond magnetometer	Nitrogen-vacancy defects in diamond	Nanoscale resolution; robust	Battery inspection, chip diagnostics, current sensing	A commercial niche
Atom interferometer (gravimeter, accelerometer)	Interference of the matter waves of cold atoms	Inertial sensing without drift	Navigation without GPS; underground mapping; surveys	Ship and aircraft trials; one aboard the X-37B space plane since August 2025
Quantum navigation	Magnetometers or interferometers matched to maps	Positioning without satellites	Aircraft and ships under jamming	Flight and sea trials
Quantum gravity gradiometer	Two atom interferometers	Sees buried structures	Civil engineering, archaeology, defense	Field trials since 2022 (University of Birmingham)
Quantum radar and lidar	Entangled or squeezed photons	A theoretical sensitivity gain	Detecting stealth aircraft (claimed)	Not practical; Chinese claims unverified
Squeezed light	Light whose quantum noise is pushed below the usual limit	Beats the standard quantum limit	LIGO's gravitational-wave detectors	In operation since 2019

Sensing is where quantum technology already earns revenue, because a sensor exploits the sensitivity of a single quantum system rather than running a computation, so it needs no error correction. McKinsey expects the quantum sensing market to reach $7-10 billion a year by 2035. The application governments care most about is navigation without GPS, since jammed or spoofed satellite signals are now routine in the Baltic, the Black Sea, and the Middle East. In 2025 Q-CTRL reported flight trials in which magnetic-anomaly navigation, which matches readings of Earth's magnetic field to a map, held errors to about 0.03% of the distance flown, about 150 meters over 500 kilometers, and performed up to 50 times better than a high-end inertial system (company claims, not peer-reviewed). SandboxAQ says its AQNav has logged more than 450 hours of flight tests. The money so far is for prototypes and research, through DARPA's and the Defense Innovation Unit's programs, but the June 2026 order on quantum innovation requires the Pentagon to name at least three quantum-sensor projects for deployment by September 30, 2028. Wearable magnetoencephalography, which maps brain activity for epilepsy care and research, and gravity sensors that find tunnels and pipes from the surface are the civilian leads.

10c. Quantum Communication

Quantum key distribution (Module 9) is the first quantum communication technology deployed at scale, and China leads it. The Micius satellite (Module 3) distributed keys between ground stations 1,200 kilometers apart, the Beijing-Shanghai backbone runs 2,000 kilometers of fiber through trusted relay nodes, and a 2021 paper described a 4,600-kilometer network joining satellite and fiber links. The Jinan-1 microsatellite, a sixth of Micius's mass and served by ground stations under 100 kilograms, set a record in March 2025 with a 12,900-kilometer link between China and South Africa, and China is considering a small constellation of such satellites. Europe's EuroQCI is building a continental network of fiber and satellites, though its first satellite, Eagle-1, has not launched and is not expected before 2027-28. Commercial hardware comes from Toshiba, from ID Quantique, now controlled by IonQ, and from Chinese firms.

The trusted-relay design, in which keys are decrypted and re-encrypted at every node, is the technology's weakness, because each node is a classical target. The fix is the quantum repeater, which would carry entanglement across nodes without measuring it. Links between quantum-memory nodes over tens of kilometers were shown in 2024 by Harvard and Amazon in Boston, by USTC in Hefei, and by QuTech between Delft and The Hague, and none is deployed.

10d. The Quantum Internet

A quantum internet would distribute entanglement between distant quantum devices, joining quantum computers into larger machines, linking sensors into arrays more sensitive than any single one, and allowing communication whose security needs no trusted relays. Its building blocks are quantum memories that store entanglement, repeaters that extend it, and transducers that convert between the microwave photons of superconducting qubits and the optical photons that travel in fiber. Each exists in laboratories, and none at scale. Delft's QuTech has run a three-node network, the US Department of Energy published a blueprint for a national quantum internet in 2020, and the June 2026 order asks agencies for five-year plans for networking. IonQ's purchases of Lightsynq and Capella in 2025 are a bet that photonic links between ion traps will be both how its computers scale (Module 6) and how a network forms. Beyond the metropolitan links of 10c, a continental quantum internet is a project for the 2030s.

Module 10 Key Points

Sensing, Timing, and Communication

• Optical lattice clocks are about 100 times more accurate than cesium, and a 2030 decision may redefine the second around them.

• Quantum sensors earn revenue now because they need no error correction; McKinsey expects $7-10 billion a year by 2035.

• Navigation without GPS leads government interest; company flight trials claim errors near 0.03% of distance flown.

• China leads quantum key distribution, from Micius to a 12,900-kilometer satellite link; trusted relays remain the networks' weakness.

• Quantum repeaters and memories work over tens of kilometers in laboratories; a continental quantum internet is a 2030s project.

Module 10 Quiz

Check Your Understanding

1. Why do quantum sensors earn revenue when quantum computers do not?

A) Governments buy every sensor made
B) Their market is protected by export controls that keep foreign competitors out of defense procurement
C) They are older
D) They need no error correction to be useful

2. Which atom's transition defines the second today?

A) Strontium
B) Cesium
C) Aluminum ions
D) Rubidium

3. What kind of support has quantum navigation received from the US military so far?

A) Prototype and research funding
B) Full-rate production contracts for every combat aircraft in the fleet, signed in 2025 after the first trials
C) A ban on foreign sensors
D) A single satellite program run by the Space Force alone

4. What did China's Jinan-1 microsatellite achieve in a March 2025 paper?

A) A 1,200-km link
B) The first quantum computer in orbit, linked to ground stations in Hefei and Beijing
C) A 12,900-km key-distribution link with South Africa
D) Entanglement between two satellites

5. Why are trusted relays the weakness of today's key-distribution networks?

A) They lose photons
B) Keys are decrypted and re-encrypted at each node, which makes every node a classical target
C) They need satellites
D) They cannot carry keys more than a few kilometers between cities

Module 11 — Geopolitics and National Programs

The Race and Its Rules

Recommended Reading / Reference

Reference: The National Quantum Initiative Act and the 2026 reauthorization bills; DARPA's Quantum Benchmarking Initiative announcements; the EU's Quantum Europe Strategy (July 2025); the Commerce Department's export-control rule (September 2024) and CHIPS letters of intent (May 2026); the two executive orders of June 22, 2026

11a. The Programs

Country or bloc	Program	Public commitment	Focus	Status (October 2026)
United States	National Quantum Initiative (2018), with reauthorization bills passed by Senate and House committees in April and May 2026; DOE and NSF centers; DARPA's QBI; Executive Orders 14412 and 14413 (June 22, 2026)	About $4-5B federal through 2025; CHIPS letters of intent (11e)	The full stack; benchmarking; post-quantum migration; defense sensing	The largest private sector; the innovation order aims to deliver a quantum computer to a Department of Energy facility for science
China	The national laboratory in Hefei; the Five-Year Plans; USTC	About $15B announced (McKinsey); real spending perhaps a quarter to a third of that, by the physicist Chao-Yang Lu's estimate	Superconducting and photonic computing; key distribution; talent	The 15th Five-Year Plan (March 2026) ranks quantum first among seven 'future industries' and calls for scalable quantum computers and a space-ground network
European Union	Quantum Flagship (€1B, 2018-28); Quantum Europe Strategy (July 2025); EuroHPC quantum machines	Several billion euros across EU and national budgets	EuroHPC quantum computers; EuroQCI; IQM, Pasqal, planqc	A Quantum Act was slated for the second quarter of 2026; its proposal is unconfirmed
Germany	National program (2023 plan)	€3B	IQM, planqc, Fraunhofer	A strong research base
United Kingdom	National Quantum Technologies Programme (since 2014); National Quantum Computing Centre; 2023 strategy	£2.5B (2024-34), plus £2B announced in March 2026 for procurement and scaling	Sensing; five national missions	The talent-drain debate over Oxford Ionics (Module 7)
Japan	Moonshot program; RIKEN; Fujitsu	¥1.05 trillion (about $7.4B) for chips and quantum together (2025), about $900M of it for quantum	Superconducting machines, among them RIKEN and Fujitsu's 256 qubits (April 2025); QuEra's machine at AIST	A government-industry consortium
South Korea	National strategy (2023)	KRW 3 trillion (about $2.3B) to 2035	Superconducting; key distribution	Growing
India	National Quantum Mission (2023)	INR 6,004 crore (about $730M) to 2031	Four hubs; key distribution; targets of 50 to 1,000 qubits	Early

Country or bloc	Program	Public commitment	Focus	Status (October 2026)
Canada	National Quantum Strategy (2023)	C$360M; C$334M more over five years for defense (Budget 2025); up to C$92M for the Quantum Champions program (December 2025)	Xanadu, D-Wave, Anyon, Nord Quantique, Photonic	Strong start-ups
Australia	National Quantum Strategy; the PsiQuantum investment	A$940M for PsiQuantum (2024) among other programs	A photonic site in Brisbane; Silicon Quantum Computing	The PsiQuantum bet (Module 6)
Others	The Netherlands, France, Denmark, Switzerland, Finland, Israel, Singapore	€100M to €1.8B each	QuTech (Delft); Pasqal and Alice & Bob (France); IQM (Finland); Denmark's Magne (Module 6)	Specialized strengths

Approximate public commitments; worldwide they exceed $60 billion by PitchBook's count. Private investment is concentrated in the United States.

11b. The US-China Race

Quantum is the one strategic technology in which China's position is credibly close to America's. China leads in quantum communication, with the largest key-distribution networks on the ground and in space (Module 10), and its superconducting and photonic computers have tracked Google's results within a year or two, as Zuchongzhi 3.2's below-threshold code showed (Module 6). The true size of its state funding is disputed (11a). The United States leads the industry, with every major pure play outside China, most of the private capital, the cloud platforms, and the error-correction milestones. It also leads the supply chain of dilution refrigerators, control electronics, and lasers, together with the allied network around it. The race is close enough that each side's policies, on export controls, on funding, and now on ownership, are made with the other in view.

11c. Export Controls and Chokepoints

In September 2024 the US Commerce Department imposed export controls on quantum computers above a threshold that starts at 34 qubits and depends on their error rates, on dilution refrigerators and cryogenic control electronics, and on related software and know-how, aimed chiefly at China, alongside similar controls that several allies adopted. A Treasury rule in force since January 2, 2025 also restricts American investment in Chinese quantum companies, and the June 2026 orders left the controls unchanged. The chokepoints are narrower than in semiconductors: dilution refrigerators come from a handful of companies led by Finland's Bluefors, the lasers for ion and atom systems from a few makers, and the high-purity materials from fewer still. China has pushed to make its own refrigerators and control chips. The controls slow China but do not stop it, and the field's expectation is that China will build its own stack a few years behind, as it has in other controlled technologies.

11d. DARPA's Referee and the Allied Strategy

The most consequential government program of the decade may be DARPA's Quantum Benchmarking Initiative, launched in 2024 to test whether any company can build a utility-scale quantum computer, one whose value exceeds its cost, by 2033. About eighteen companies entered its first stage in 2025. Eleven advanced to Stage B in November 2025, while Rigetti, Alice & Bob, and HPE did not. Stage C, the independent verification of a full design, now holds Microsoft and PsiQuantum, which entered through an earlier DARPA program, and IonQ and IBM, admitted on October 7 and 8, 2026, IonQ with up to $300 million. The initiative is the first independent referee of the industry's claims, and its judgments will shape which designs win the defense and intelligence contracts that are among the industry's largest sources of revenue. The allied strategy is to pool research, coordinate controls, and fund one another's companies, as with the Australian and Japanese deals in 11a, a network no rival can easily replicate.

11e. Washington's Stakes in Quantum Companies

In May 2026 the Commerce Department signed letters of intent to give $2.013 billion in CHIPS Act funds to nine quantum companies, each in exchange for a minority, non-controlling equity stake. IBM would receive $1 billion for a new quantum foundry subsidiary, GlobalFoundries $375 million, Atom Computing, D-Wave, Infleqtion, PsiQuantum, and Quantinuum $100 million each, Rigetti up to $100 million, and Diraq up to $38 million. IonQ was left out, and no final agreements had been reported by August. Advocates argue that quantum is a strategic technology in a race with a state-funded rival, that equity gives taxpayers a share of the upside where grants give it away, as the government's 2025 stake in Intel was meant to, and that federal money draws private capital into foundries and supply chains that markets underfund. Critics answer that Washington is picking winners among unproven technologies, that it becomes a shareholder in firms its own agencies license for export and referee through DARPA, that excluded firms such as IonQ must compete with government-backed rivals, and that stakes in small listed companies can move their share prices. The evidence is thin so far: the agreements are not final, the sums are small beside the companies' private capital, and the stakes have no record yet. This course's reading is that the stakes are too small to change who wins the technical race, so their real test is governance: whether companies in which Washington owns shares are judged by DARPA and the export licensers on the same terms as those in which it does not.

Module 11 Key Points

Geopolitics and National Programs

• Public commitments worldwide exceed $60 billion; the US, China, the EU, Britain, Japan, and others fund programs from research to procurement.

• China leads quantum communication and tracks Western computing results closely; the US leads the industry, private capital, and the supply chain.

• Export controls since September 2024 cover larger quantum computers, dilution refrigerators, and cryogenic electronics; they slow China rather than stop it.

• DARPA's benchmarking initiative referees the industry: eleven firms reached Stage B, and Microsoft, PsiQuantum, IonQ, and IBM are in Stage C.

• In May 2026 Commerce offered $2 billion to nine firms for minority equity stakes, an industrial-policy turn that remains disputed.

Module 11 Quiz

Check Your Understanding

1. Which company did the May 2026 CHIPS letters of intent leave out?

A) IBM, which received the largest award for a new quantum foundry
B) Quantinuum
C) D-Wave, whose award would be paid in shares
D) IonQ

2. What does China's 15th Five-Year Plan do for quantum?

A) Puts it first among seven 'future industries'
B) Bans foreign quantum hardware
C) Transfers the national laboratory in Hefei to the military and closes its civilian programs
D) Sets a target of a million-qubit machine by 2030

3. Besides quantum computers above a qubit threshold, what do the 2024 US export controls cover?

A) They cover dilution refrigerators and cryogenic electronics.
B) They cover every quantum paper published.
C) They cover the lasers sold to every university physics laboratory in the world.
D) They cover the post-quantum standards NIST published in 2024.

4. Which companies are in Stage C of DARPA's benchmarking initiative?

A) Rigetti, HPE, Atlantic Quantum, and Oxford Ionics
B) Microsoft, PsiQuantum, IonQ, and IBM
C) Google, Quantinuum, QuEra, and Atom Computing
D) All eleven Stage B companies, which advanced together after DARPA dropped its requirement for utility-scale designs

5. What is this course's reading of Washington's equity stakes?

A) They nationalize the industry
B) Their size, larger than all private funding combined, will decide which modality wins the technical race
C) They are illegal
D) Their real test is governance, not size

Module 12 — Investing in Quantum

Quantum as an Investment, With the Numbers

Recommended Reading / Reference

Reference: Company 10-K and 10-Q filings and investor presentations; Quantinuum's S-1 registration (May 2026) and first quarterly report (August 2026); McKinsey, *Quantum Technology Monitor 2026*

12a. The Public Stocks and Their Round Trip

Company (ticker)	Peak price	Price, early October 2026	Change from peak	Market value, early October 2026	Market value ÷ 2025 revenue	Business
IonQ (IONQ)	$84.64 (October 2025)	About $40	−53%	About $15-16B	About 120×	Trapped-ion computers; networking and sensing acquisitions
Rigetti (RGTI)	$58.15 (October 2025)	About $14.10	−76%	About $4.7B	About 660×	Superconducting chips; government contracts
D-Wave (QBTS)	$46.75 (October 2025)	About $14.60	−69%	About $5.5B	About 220×	Annealers; gate-model development
Quantinuum (QNT)	$86.79 (after its June 2026 listing)	About $41.30	−52%	About $10.7B	About 350×	Trapped-ion computers
Honeywell (HON)	—	—	—	—	—	Quantinuum's largest shareholder (Module 7)
IBM, Alphabet, Microsoft, Amazon, Nvidia	—	—	—	—	—	Quantum is a rounding error in each; Nvidia supplies the classical side (Module 7)

Delayed quotes from early October 2026; market values approximate; revenue from Module 7. The 2026 listings through SPACs (Module 7) are too new to judge.

The public quantum stocks are among the most volatile in the market. Rigetti and D-Wave traded below a dollar in 2023 and again in the autumn of 2024, and in the late-2024 run alone Rigetti rose about 1,450% and D-Wave about 850%, on Willow's announcement, retail enthusiasm, and a story of quantum as the next AI. On January 7, 2025, Nvidia's chief executive, Jensen Huang, said useful quantum computers were 15 to 30 years away, and the next day Rigetti fell about 40%, IonQ 37%, and D-Wave more than 30%. He recanted at Nvidia's Quantum Day on March 20, the stocks recovered and then peaked, Rigetti at about 2,700 times its 2025 sales and D-Wave at roughly 650-700 times. Since then they have fallen to the prices in the table, while revenue, though growing fast, remains tiny beside their market values. None is profitable, all sell shares to fund their losses, and IonQ's use of its shares as currency for acquisitions (Module 7) is the sector's most consequential allocation of capital.

12b. Quantinuum's Listing

Quantinuum's listing was the sector's test. It priced on June 3, 2026 at $60 a share, above its range, selling 28 million shares to raise about $1.68 billion at a valuation of about $15.6 billion, and began trading on Nasdaq the next day. The shares rose after the listing (12a) and have since fallen below the offering price.

Its first public quarter, reported on August 11, showed revenue of $8.0 million, up 279%, and a GAAP loss of $596.5 million, most of it a one-time charge for stock awarded at the listing, against $2.11 billion of cash. The market's verdict was cool: it priced the logical-qubit leader (Module 7) well below IonQ, which then traded at about $27 billion, and it has since marked both down.

Worked example — Revenue Against Market Value

Take IonQ at about $15.5 billion, and assume that a mature, fast-growing technology company trades at 8-10 times its sales, a rough benchmark for profitable firms. Today's value then requires annual revenue of about $1.6-1.9 billion, 12-15 times IonQ's 2025 revenue and 5-7 times its 2026 guidance (Module 7). An investor who wants a 10% annual return needs the value to reach about $25 billion by 2031, which at the same multiples means revenue of about $2.5-3.1 billion that year. That is growth of roughly 54-61% a year for five years from the midpoint of the 2026 guidance, fast but not unheard of, and acquisitions supply part of it. Rigetti is the harder case: its $4.7 billion requires revenue of about $470-590 million, 66-83 times its 2025 sales. Either way the valuations are a bet that fault-tolerant machines arrive on the roadmaps' schedule (Module 6), and that these companies, rather than the hyperscalers, capture the revenue.

12c. How to Value a Pre-Revenue Platform

A conventional valuation fails, so the market uses three substitutes. Scenario value assigns a probability to fault-tolerant machines arriving by 2030-33, estimates the market they would open, and discounts the result. McKinsey's 2026 monitor puts the whole quantum-technology market at $60-100 billion a year by 2035, and the economic value quantum could create for its users at $1.3-2.7 trillion, a different and much larger number that is often misquoted as the market. Option value treats the stock as a call option on a technology transition, priced on volatility and narrative rather than cash flow, the frame in which a multiple of hundreds of times sales is not absurd, merely a lottery ticket. Relative value compares one company with another, as the market did in pricing Quantinuum against IonQ.

The argument over price follows from those frames. The bulls point to revenue that is more than doubling at IonQ, to error-correction results arriving faster than expected (Module 6), to government money and stakes that underwrite the leaders (Module 11), and to a transition that, if it comes, will make today's prices look small. The bears point to the multiples in 12a and to the dilution, slippage, and big-tech risks in 12d. The evidence of the past year favors caution: the stocks have fallen from their peaks (12a) while the technology advanced, which shows how far the prices had run ahead of it. This course's reading is that the stocks price a fault-tolerance schedule that the evidence treats as the optimistic case (Module 6).

12d. The Risk Table

Risk	Mechanism	Likelihood (this course's judgment)	Consequence
Roadmap slippage	Targets for 2029 slip into the 2030s, as earlier targets have (Module 6)	High	Revenue delayed; more shares sold to fund the gap
Modality loss	One or two of the five modalities win; pure plays on the others become suppliers or fail	High for at least two modalities	Total loss for the losers
Classical catch-up	Advantage claims keep being matched classically (Module 8)	Medium-high	'Advantage' keeps receding

Risk	Mechanism	Likelihood (this course's judgment)	Consequence
Big-tech capture	IBM, Google, Microsoft, and Amazon own the fault-tolerant machines and the clouds; pure plays become features	Medium	Margins go to the hyperscalers
Dilution	Loss-making companies sell shares in every rally	Certain	Per-share value erodes even if the company succeeds
Mania reversal	Multiples compress toward conventional levels	Medium in any two-year window	Falls like those already seen (12a)
Policy and geopolitics	Export controls; government stakes (Module 11); decoupling from China	Medium	Winners chosen by policy; a split market
Success	Fault tolerance on schedule; useful chemistry by about 2030; revenue from post-quantum migration	Low-medium	The leaders become very large companies

12e. The Ways In

For an investor who wants exposure, the choices are these. The pure plays offer the most leverage to the story and the most exposure to the risks above. Quantinuum can be owned directly, or through Honeywell. The hyperscalers and Nvidia offer quantum as an option attached to businesses that already exist, and the sensing companies have revenue now (Module 10). Venture funds reach the private market. The picks and shovels, makers of cryogenics (Bluefors, private), lasers (Coherent, Toptica), control electronics (Keysight, Zurich Instruments, Quantum Machines), and photonics, sell to every modality whichever wins. The last category is the one a value investor recognizes; the first is the one the market has priced. This module describes the choices and is not investment advice.

Module 12 Key Points

Investing in Quantum

• Quantum stocks soared in 2024-25 and fell 53-76% from their October 2025 peaks; none is profitable, and all sell shares to fund losses.

• Quantinuum listed at $60 in June 2026, valued near $15.6 billion, and now trades below its offering price.

• At 8-10 times sales, IonQ's value requires revenue of about $1.6-1.9 billion, several times its 2026 guidance.

• McKinsey's trillions are economic value to users; the market it forecasts is $60-100 billion a year by 2035.

• The valuations bet on fault tolerance arriving on schedule; dilution is certain, and modality loss likely for some companies.

Module 12 Quiz

Check Your Understanding

1. What did Jensen Huang's January 2025 remark do to quantum stocks?

A) Doubled them
B) Halted trading on Nasdaq
C) Cut Rigetti by about 40% and IonQ by 37% in a day, until he recanted in March
D) Sent them to their all-time peaks

2. Where did Quantinuum's shares trade in early October 2026, relative to its IPO?

A) Above $86
B) Exactly at the $60 offering price, held there by its underwriters' stabilization
C) Double the IPO price
D) About $41, below the $60 offering price

3. In the worked example, what revenue would justify IonQ's value at 8-10 times sales?

A) About $130 million, its 2025 revenue
B) About $1.6-1.9 billion a year, several times its 2026 guidance of $280-290 million
C) About $15.5 billion, as a fair multiple of sales is exactly one
D) About $500 million

4. What does McKinsey's $1.3-2.7 trillion figure measure?

A) Economic value to users by 2035
B) The market for quantum computers in 2030
C) Annual revenue of quantum-computing companies today, after the 2025 surge in government and cloud contracts
D) Total VC raised

5. Which risk does the table rate as certain?

A) Modality loss, as one or two of the five modalities win
B) Roadmap slippage
C) Dilution
D) Big-tech capture by the hyperscalers

Module 13 — Where Things Stand, and What to Watch

The Argument, the Contradictions, and the Dates

Recommended Reading / Reference

> **Reference:** IBM's public quantum advantage tracker; DARPA's Quantum Benchmarking Initiative announcements; the Global Risk Institute's annual quantum threat survey; Scott Aaronson's blog, *Shtetl-Optimized*, for the field's running conscience

13a. The Argument

The argument of this course fits in a page. The physics is settled: quantum mechanics has never failed a test (Module 3), and the only question was whether its strangest features could be engineered. The answer to the first engineering question is now yes. Error correction works as the threshold theorem predicted, on three platforms (Module 6), and that was the one result that had to hold for anything else to follow. The answer to the second question, how soon a machine will be large enough to matter, is not yet known, because the gap between today's tens of logical qubits and the thousands that useful algorithms need is engineering of a scale no one has attempted (Module 6).

The applications that survive scrutiny are the ones Feynman proposed, simulating physics and chemistry, and not the optimization and machine learning that dominate the marketing (Module 8). The threat to encryption does not wait for the machine, because recorded traffic can be read later, so the migration is the one quantum decision with a deadline today (Module 9). Meanwhile the clocks, sensors, and key-distribution links of Module 10 are already in service, and the money has run ahead of all of it (Module 12).

13b. The Contradictions

Four contradictions run across the modules, and no single module states them.

The quieter claims held. Claims of speed have narrowed or fallen under classical challenge, from Sycamore to IBM's July candidates (Module 8), while claims about the machines' own errors, Willow's and the others below threshold, have been reproduced (Module 6). The field's most credible progress is on the problem that makes the fewest headlines, and its most publicized results have been its least durable.

The machine that does not exist has already changed the internet. No quantum computer can yet break a real key, but most of Cloudflare's human traffic already uses post-quantum key agreement (company claim), and governments have set deadlines running to 2035 (Module 9). The largest economic effect of quantum computing so far is the cost of defending against it.

The revenue and the valuations are in different places. The technologies earning money need no error correction (Module 10), while the market values sit on computing companies whose revenue is small beside them (Module 12). Infleqtion, which sells clocks and sensors as well as building computers, took in about as much in 2025 as Quantinuum (Module 7), but its merger valued it at about a tenth of Quantinuum's value at listing (Module 12).

China's clearest lead is in what the West's agencies advise against. China's lead in quantum communication is the clearest in the race (Module 11), yet the NSA and the NCSC prefer post-quantum

software, which runs on ordinary networks, in nearly every case (Module 9). Either China is buying a capability the West has misjudged, or its clearest lead is in the technology that matters least.

13c. What to Watch

When	What	Why it matters
October 13-15, 2026	The General Conference on Weights and Measures meets in Versailles and reviews progress toward an optical second	Whether the 2030 decision (Module 10) stays on track
October 20, 2026	A report on the five-year federal plans for quantum sensing and networking, due within 120 days of the innovation order (Module 10)	Whether Washington funds deployment or only research
November 11-13, 2026	IBM's Quantum Developer Conference, in Chicago	The likeliest venue for news of Kookaburra (Module 6) and of the July advantage candidates (Module 8)
November 2026 (expected)	Third-quarter results from IonQ and Quantinuum	A test of IonQ's raised guidance (Module 7)
By the end of 2026	IonQ's 256-qubit system, which the company says is in full-system testing with a first unit sold (company claims)	The largest trapped-ion machine yet, if it arrives with data
December 2026	The proposed procurement rule under Executive Order 14412, due within 180 days of the order	The rule that will carry post-quantum requirements to every federal contractor (Module 9)
March 2027	CISA's guidance on a 'cryptographic bill of materials', an inventory of the cryptography in a product, due within 270 days	The inventories on which every migration depends (Module 9)
By December 31, 2027	NIST's post-quantum migration pilot under the order	The first federal test of a complete migration
Pending	Final CHIPS agreements and their equity stakes (Module 11); floor votes on reauthorizing the National Quantum Initiative; the EU's Quantum Act	Whether the policy turn of 2026 becomes binding
Pending	Activation of Bitcoin's BIP-360 or another migration path	Whether the largest unmigrated target (Module 9) moves before the machine
Ongoing	Classical attempts on Quantum Echoes; the tracker's verdicts on IBM's candidates (Module 8)	Whether the first beyond-classical result to survive a year survives for good
Ongoing	Microsoft's Majorana program (Module 4): a qubit operation or braiding, or a quiet retreat	Whether topological qubits exist
Ongoing	The next Global Risk Institute survey and the next resource estimates (Module 9)	Whether Q-Day keeps moving earlier

13d. The Last Word

Every technology in this course depends on how a quantum state responds to the world around it. The clocks, sensors, and key-distribution links already in service use that sensitivity: a magnetometer works because the field disturbs its atoms, and key distribution works because an eavesdropper disturbs the photons (Module 2). The quantum computer must defeat the same sensitivity, which is why it needs error correction and why it is the last of these technologies to arrive. That adds one question to the test of Module 8. Of any quantum claim, ask whether the technology uses the fragility of quantum states or must overcome it. Claims of the first kind can be checked against products in service today; claims of the second kind depend on error correction, and their dates should be read against the roadmaps and their record.

Module 13 Key Points

Where Things Stand, and What to Watch

• The physics is settled and error correction works; how soon machines grow large enough to matter remains the open engineering question.

• Speed claims narrowed under classical challenge while error-correction claims were reproduced, so the quieter results proved the more durable.

• Quantum computing's largest economic effect so far is the cost of migrating encryption against a machine that does not yet exist.

• Revenue sits in sensing and clocks, which need no error correction, while market values sit on computing companies.

• Ask whether a technology uses quantum fragility or must overcome it; only the second depends on error correction's timeline.

Module 13 Quiz

Check Your Understanding

1. Which kind of claim has proved the most durable?

A) Speed claims
B) Error-correction claims
C) Qubit-count records
D) Market forecasts from consultants

2. What is quantum computing's largest economic effect so far, according to the closing module?

A) Revenue from cloud access to quantum machines, which passed a billion dollars in 2025
B) Savings from faster logistics planning
C) The encryption migration
D) New drugs designed with quantum chemistry

3. What is the contradiction in China's lead in quantum communication?

A) China's networks use no trusted relays.
B) China leads only in quantum computing.
C) Its satellites cannot reach other continents.
D) Western security agencies advise against the technology China leads in.

4. In the last word's test, which claims depend on error correction's timeline?

A) Claims about clocks and magnetometers, which use the sensitivity of quantum states to their surroundings
B) Claims about key distribution
C) Claims about any quantum technology at all
D) Those overcoming fragility

5. What did the closing module call the one result that had to hold?

A) Working error correction
B) Shor's algorithm
C) Room-temperature qubits
D) Topological qubits

Answer Sheet

Answers to every module's Check Your Understanding quiz.

Module	Answers
Module 1 Quiz	1. B 2. A 3. C 4. D 5. C
Module 2 Quiz	1. B 2. A 3. D 4. B 5. A
Module 3 Quiz	1. D 2. C 3. A 4. C 5. B
Module 4 Quiz	1. D 2. B 3. A 4. D 5. C
Module 5 Quiz	1. A 2. C 3. B 4. D 5. D
Module 6 Quiz	1. A 2. B 3. C 4. B 5. D
Module 7 Quiz	1. C 2. A 3. B 4. A 5. D
Module 8 Quiz	1. C 2. C 3. A 4. B 5. D
Module 9 Quiz	1. A 2. D 3. B 4. C 5. C
Module 10 Quiz	1. D 2. B 3. A 4. C 5. B
Module 11 Quiz	1. D 2. A 3. A 4. B 5. D
Module 12 Quiz	1. C 2. D 3. B 4. A 5. C
Module 13 Quiz	1. B 2. C 3. D 4. D 5. A