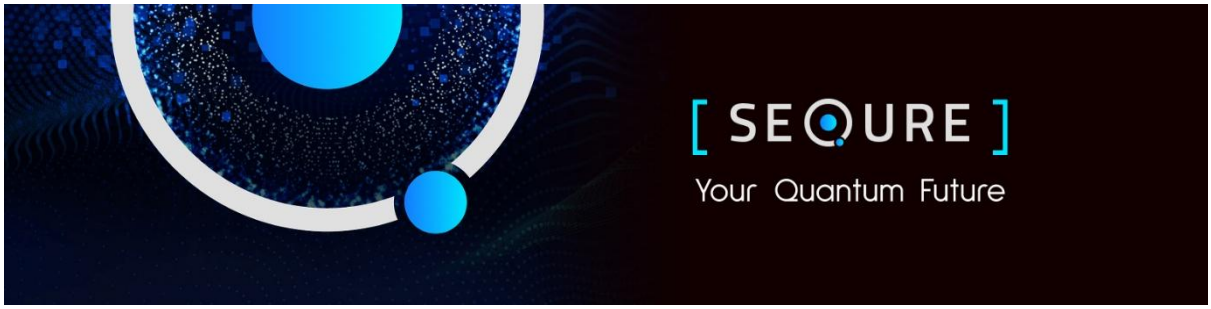


QUANTUM COMPUTING 101

Amit Agarwal

Nov 2025

Contents

Quantum computing is a type of computation that harnesses the collective properties of quantum states, such as superposition and entanglement perform operations.

Quantum computers, once finally realized, are not suited for all types of computational problems, but they are exceptionally well-suited for certain tasks, such as factoring large numbers, searching databases, and simulating quantum physical processes, which would be impractically slow on classical computers.

While quantum computing is still in its infancy, with many technical challenges to overcome, its development could revolutionize industries by making previously intractable problems solvable, potentially leading to breakthroughs in materials science, cryptography, drug discovery, and optimization problems in logistics and manufacturing.

1. What is Quantum?

Quantum is based on latin word “quantus” meaning quantity, amount, how much. Quantum (physics definition) is a discrete quantity of energy proportional in magnitude to the frequency of radiation it represents. It is the smallest discrete unit of a phenomenon- For example,

Quantum of light = photon; Quantum of electricity = charge of an electron

Planck’s distance = shortest meaningful distance; Planck’s time = shortest meaningful time. (Energy of 1 photon = Planck’s constant, h)

For anything smaller, Heisenberg’s uncertainty principle, makes measurements meaningless.

2. What is Quantum Mechanics?

Quantum Mechanics is the mathematical representation of Quantum Physics. Quantum Physics is the fundamental theory in physics that describes nature at the smallest scales of energy levels of atoms and subatomic particles. Aspects of quantum mechanics – specifically superposition and entanglement – offer the potential for incredible computational advantages.

3. What Is Quantum Computing?

Quantum computing is a type of computing that uses quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data. In classical computing, data is processed using binary bits (0s and 1s). In contrast, quantum computing uses quantum bits or qubits, which can probabilistically exist in multiple states simultaneously, allowing quantum computers to process a vast number of calculations at once.

4. Why build a Quantum Computer?

With the advancement of technology and science, the search for faster forms of computation capable of solving intractable problems has become a fundamental goal of science. Quantum computing represents an answer to this need, since its principles allow for exponentially faster calculations in certain classes of problems. This area is showing particular promise in fields such as cryptography, optimization of large volumes of data, modeling of quantum phenomena such as chemical reactions, and even in artificial intelligence. Its development has the potential to revolutionize science, technology, and the world.

5. How does a Quantum Computer work?

A quantum computer works by manipulating qubits through quantum gates in a quantum circuit. Unlike classical bits, qubits can be in a state of 0, 1, or any quantum superposition of these states. This allows quantum computers to perform complex calculations more efficiently than classical computers for certain problems. The operations of quantum computing are also influenced by entanglement, a property that allows qubits that are entangled to be in a correlated state.

6. What are Qubits?

A qubit (or quantum bit) is the fundamental unit of information in quantum computing, analogous to a bit in classical computing. While a classical bit is in a definite state of either 0 or 1, a qubit can exist in a superposition of these two states, being both 0 and 1 to some degree. This characteristic allows the qubit to represent information in a much richer way.

In essence, just as 2 voltage levels are used to encode binary information as 0 or 1 in classical computers, 2 quantum mechanical properties e.g., up or down spin of an electron is used to encode binary information in qubits in quantum computer. The difference is that in quantum mechanical world, as per Heizenberg's uncertaintly principle, you cannot know the precise spin, so the state is a combination of probability of occurance of both 0 and 1, at any point of time. This is the principle of superposition.

More mathematics and physics of quantum mechanics and qubits is provided in the appendix A of this document.

7. What is needed to generate Qubits?

Classic computers use transistors as the physical building blocks of logic. The key characteristics that make transistors viable for computing are that they are robust against failure, can accurately store, represent and process information, scale very well, can be reliably given inputs and outputs can be measured to get an answer and we know how to define and characterize the logic elements.

In quantum computing, Qubits are built using natural phenomenon or constructs like electron states of an ion, electron spin of phosphorous atoms, nuclear spin of a defect in diamond, photons, quantum dots, or electrical circuits constructred to behave as quantum mechnical 2-level system, meaning artificial atom.

For viable quantum computer, a Qubit should satisfy the DiVencenzo Criteria:

DIVINCENZO CRITERIA

REQUIREMENTS FOR THE PHYSICAL IMPLEMENTATION OF QUANTUM COMPUTATION	
D1: Scalable qubits	Scalable physical system of well-defined, characterized qubits
D2: Initialization	Prepare a simple, fiducial input state
D3: Measurement	Measure the qubit state
D4: Universal gate set	Perform a universal set of gate operations with high fidelity
D5: Coherence	Robustly represent quantum information (long coherence times)
REQUIREMENTS FOR ROUTING QUANTUM INFORMATION	
D6: Interconversion	Ability to interconvert stationary and flying qubits
D7: Communication	Ability to transmit flying qubits faithfully between two locations

8. What is Superposition?

In quantum mechanics, superposition allows a particle to exist in a combination of multiple states at the same time. This is unique and different to classical where a bit

can be only in one state at a time 0 or 1. In quantum computer, the principle of superposition means qubit states are a combination of 0 and 1, which introduces inherent parallelism, which in turn lets them be much fasted in computation.

Imagine a coin spinning in the air. Before it lands, it is not either “heads” or “tails”, it is, in a sense, in a state of both at the same time, a superposition of the two. Only when it lands and is observed does the coin assume one of the definitive states.

9. What is Entanglement?

Entanglement is a phenomenon that occurs when two quantum particles interact in such a way that their states become interdependent, even if they are separated by large distances. After entanglement, measuring the state of one particle automatically defines the state of the other. Einstein was so frightened by this phenomenon that he dubbed it “spooky action at a distance.”

A good analogy for understanding quantum entanglement is that of a pair of gloves. Imagine that you have a left glove and a right glove, and you put them in separate boxes and send one to a distant friend. When you open your box, if you find the left glove, you can instantly conclude that the glove your friend has is the right one, regardless of the distance between you. Just as you can know which glove your friend has without communication, in quantum entanglement, when we measure a property of one particle, we instantly know the corresponding property of the other particle, no matter how far apart they are. However, unlike gloves, entangled particles do not have definite states until they are measured, which makes quantum entanglement an intriguing and non-local feature of quantum mechanics, revealing correlations that defy our classical intuition.

This connection means that by just measuring the properties of one entangled qubit, you can instantly know the properties of its partners without having to look. As a result, the more entangled qubits you can have in your quantum computer, the more (and faster) calculations that computer can make. And because each qubit exists in multiple states it can make multiple calculations simultaneously — add more entangled qubits and the number of possible calculations the computer can perform increases exponentially.

What does this exponentiality mean in practice? Well, for a quantum computer containing 1,180 qubits (still fewer than Colossus’ 1,600 bits), the number of entangled states on its processor would exceed the number of individual atoms in the known Universe.

This all means that, rather than having to run a calculation many times as you would with a boring old silicon processor, you can, in theory, run every conceivable calculation at the same time.

Imagine you are a delivery company and you want to plot the best route from A to B in a city, but you also have to make 150 stops en-route to make deliveries.

A normal computer would have to look at each possible route individually and then compare the results to determine the most efficient outcome. Because the quantum computer exists in many states at once, it can look at many different routes at once and determine the most efficient route almost instantaneously. Thus making complex calculations with many complex variables thousands of times faster. This ability to perform almost unlimited calculations at the same time gives quantum computers extraordinary real-time optimisation and pattern-finding abilities.

So it is expected that quantum computers will be able to provide unimaginable insights into the sort complex natural systems that binary computers just can't crack — such as how weather systems develop; how long-term climate change will unfold; and, on a smaller scale, how drugs interact with cancers. The flip side of this would be that a quantum computer could break almost any current data encryption system, which would give the planet's spy agencies a bit of a headache and prompt an arms race of quantum-based cryptography verses the quantum hackers.

10. What is Quantum Advantage ?

Quantum Advantage is a point at which quantum devices offer unprecedented speed and efficiency for certain calculations, benefiting from parallelism and increased computational capacity. If this level of performance is achieved, quantum computers could be vastly better than classical computers at solving certain problems.

The following table provides the quantum advantage (speed up) over classical:

QUANTUM ALGORITHM SPEEDUPS

ALGORITHM	CLASSICAL RESOURCES	QUANTUM RESOURCES	QUANTUM ADVANTAGE	LIMITATION
Simulation (quantum chemistry)	2^N (for N atoms)	N^C	Exponential*	Mapping problem to qubits
Factoring (+ related number theoretic)	2^N (for N digits)	N^3	Exponential	Classical runtime limit unproven
Linear systems (Ax=b)	2^N (for N digits)	~N	Exponential	Strict conditions, e.g. sparse matrix
Optimization	2^N (for N items)	?	?	Empirical
Search (unsorted/unstructured data)	N (for N entries)	$\sqrt{N}$	Polynomial ($\sqrt{N}$)	Data loading

11. What is Quantum Supremacy ?

Quantum Supremacy will be reached once a Quantum Computer can solve an algorithm faster than the fastest supercomputer in existance. Theoritically, this can be reached by having a Quantum Computer with 80 error free qubits.

12. What are current challenges in Quantum computing?

Quantum Decoherence

Quantum decoherence occurs when qubits lose their quantum state due to environmental interference. This can cause errors in calculations and is a significant challenge in quantum computing development. Superposition and entanglement are very unstable states and the slightest interference — such as vibrations or radiation — can cause these states to be disturbed or collapse. This is called quantum decoherence and when this happens the 'broken' qubit must be replaced. In fact, there is a problem in "reading" a quantum state, meaning reading a value of a qubit itself can change the value of its state because when you read you use lasers or optics and this introduces an electro-magnetic interference.

Error Correction

Quantum error correction is an essential area of research. Since qubits are highly sensitive, maintaining coherence and reducing noise are crucial for reliable quantum computing.

Qubit Stability

Qubits are sensitive to environmental disturbances (decoherence), requiring rapid computations and often low temperatures (temperatures close to temperature in Space – 15 kelvin !!!) to maintain stability. The more qubits you have, the more unstable the system becomes in absence of quick noise detection and correction.

Scalability

Building a quantum computer with a large number of qubits is challenging as qubit-based processors need to be kept carefully isolated from the outside world by using vacuums, dampening vibrations and shielding from radiation.

It is this 'scalability' problem and the "decoherence" or "noise" problem that most companies are focussed on solving. The current progress is very promising. The future of computing is unlikely to be solely quantum and will probably be a combination of qubits and good old fashioned binary bits. Therefore, talking about quantum computer in isolation is erroneous for the foreseeable future and one must talk about hybrid solution where a Quantum computer and classical computer combine to solve complex real world problems very fast and efficiently.

13. What are physical and logical Qubits ?

Physical Qubit is implemented in one of the currently known methods. Since they are inherently noisy due to problem of decoherence, scientists have created the concept of logical qubits in which multiple physical qubits are entangled and then initiatilized to a state. Then operations are carried out on them but the value is read by an algorithm which tries to see the states of all qubits which are entangled and derive a

correct “logical” state. The qubit state resulting from these redundant physical qubits are called “logical qubits”.

14. What differentiates Classical vs. Quantum Computing?

The term *classical* in classical computing is borrowed from conventions in physics. In physics, pre-1900 physics is “classical” and post-1900 physics is “modern.”

Modern physics includes general relativity and quantum physics. General relativity is Einstein’s theory of curved space and time, which explains the force of gravity. This theory, while instrumental in enabling us to comprehend awe-inspiring images of galaxies, has its most direct technological application in GPS, the Global Positioning System crucial for satellite navigation. Yet, even this remarkable application is not standalone — it also requires quantum technology for accurate functioning.

In contrast to general relativity, quantum physics has a broader range of applications that span diverse fields. It is the backbone of lasers and light bulbs, the lifeblood of medical scanners and radiation therapy, and the cornerstone of semiconductors and electron microscopes. It governs the precision of atomic clocks and the power of atomic bombs, among many others. And it is the fuel for quantum computers

Classical computing, which is the basis of our current information technology, uses bits (the smallest unit of information) to process and store data. Each bit assumes a specific value, 0 or 1, also known as binary language, representing the on or off state. These bits are manipulated by logic gates and circuits to perform operations that solve problems and execute programs.

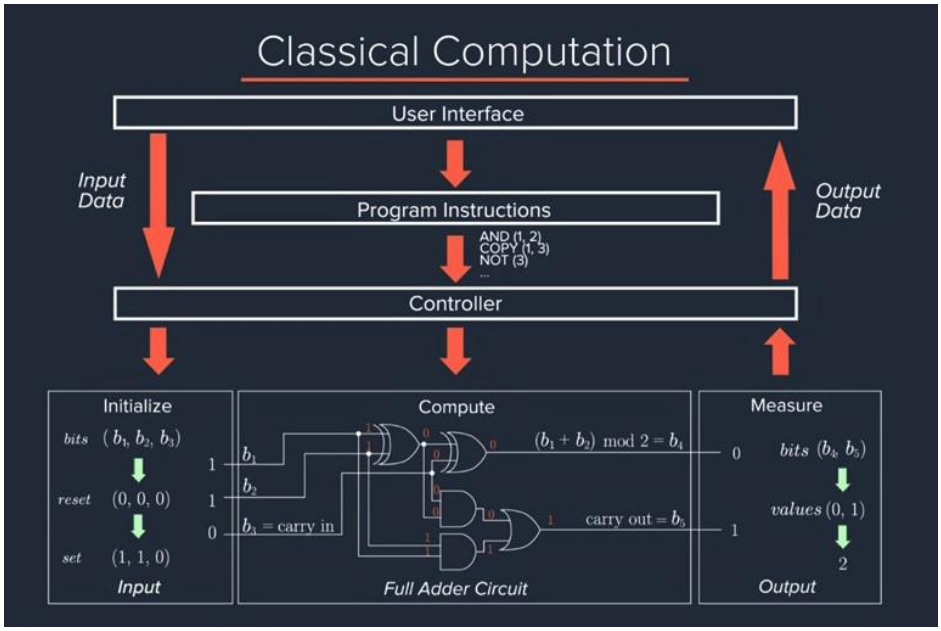
However, there are problems that classical computing cannot solve in a practical way, such as, for example, the accurate simulation of complex molecules and the efficient resolution of factorization problems. These types of problems require processing power that would grow exponentially on a classical machine, which makes it impossible to solve them in a feasible time. For example, to factor a number of 2048 bits (approximately 617 digits), a classical computer using the best current factorization algorithms would take trillions of years, possibly much longer than the age of the universe. A quantum computer that uses Shor’s algorithm, an algorithm specifically designed for factorization and exponentially faster, could solve this problem in a few seconds or minutes, depending on the capacity of the quantum processor (number of qubits and error rate).

Quantum computing, unlike classical computing, is based on the principles of quantum mechanics, a branch of physics that studies subatomic particles and their unique behaviors. Instead of bits, it uses qubits, which can exist in a superposition of states (0 and 1 simultaneously) and become entangled with other qubits, creating an interdependence that allows for a form of parallel processing.

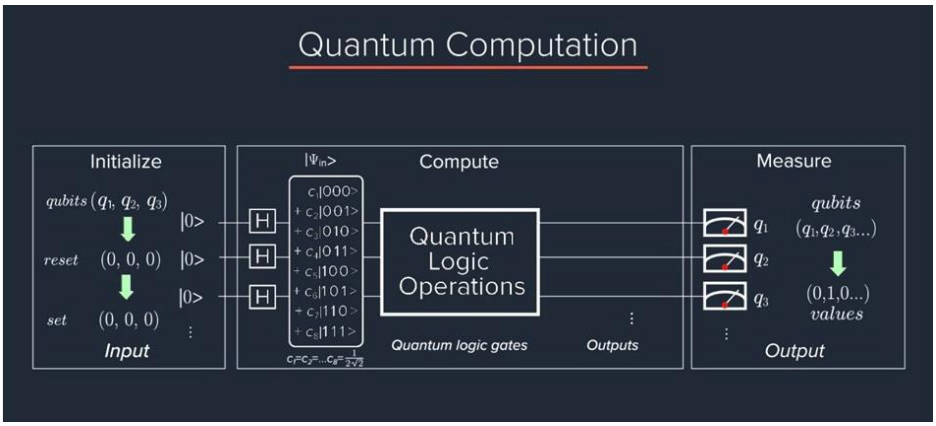
For example, to find solution to a maze with thousands of possible exits, where only one leads to the prize - a classical computer would need to test each route one by one linearly. A quantum computer, however, can exist on multiple paths at the same time, trying out multiple routes at once until it finds the correct exit. This “quantum parallelism” allows for a much more efficient search, making quantum computing capable of solving complex problems in a way that defies classical logic.

15. Difference between Quantum vs. Classical Circuits?

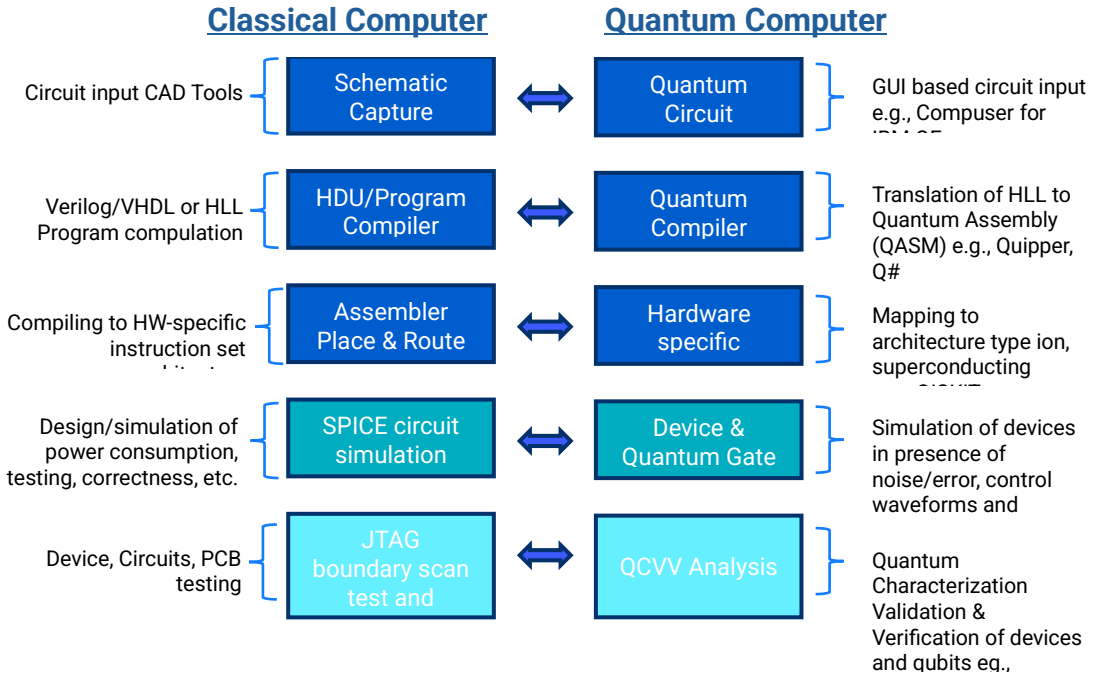
Classical Circuit: You manipulate signals using gates on inputs **sequentially**



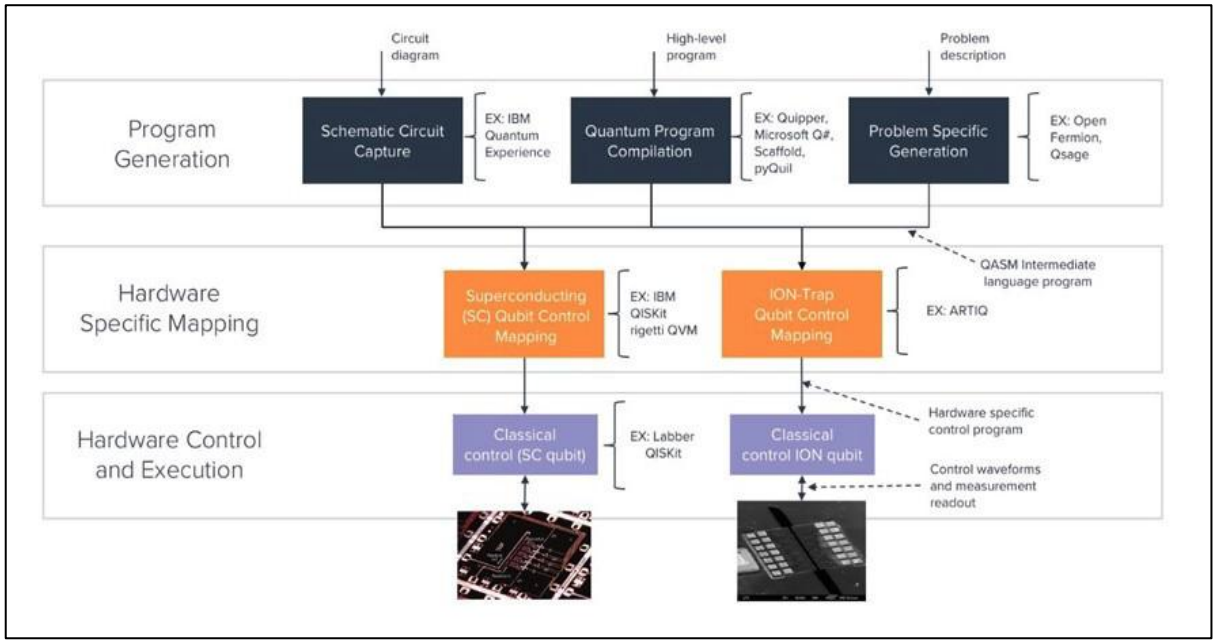
Quantum Circuit: You manipulate signals using gates on inputs **<u>in parallel</u>**



16. Difference Quantum vs. Classical HW/SW Stacks ?



Programming a Quantum Computer



17. What are the potential applications of Quantum Computing?

Quantum computing shows promise in areas like large-number factoring, database searching, and quantum physical process simulations. Quantum computing has potential applications in various fields including cryptography, drug discovery, optimization problems, financial modeling, machine learning, and materials science.

Cryptography and Cybersecurity: Quantum computers could both break current encryption methods and lead to more secure ones. This might reshape how we protect information, raising both challenges and opportunities for data security.

Drug Discovery, Energy and Material Science: Simulating molecules to discover new drugs or materials requires significant computing power and time. Quantum computers could make these simulations faster and more accurate allowing us to model molecular processes to discover new medicines, create resistant materials, and improve catalysts for industry.

Optimization Problems: Quantum computing excels at solving optimization challenges, like finding the most efficient route for delivery trucks or the best way to allocate resources as it can evaluate multiple alternatives in parallel. Quantum computing can optimize complex routines, improving efficiency in areas such as logistics, transport routing and process planning.

Artificial Intelligence (AI): With faster data processing and the ability to handle complex algorithms, quantum computers can accelerate machine learning processes and neural network optimization, opening up new horizons for AI applications, potentially making AI smarter and more adaptable.Quantum computers are inherently suited for vector-based operations.

Climate Science: Quantum computers could improve climate models, allowing scientists to make better predictions and develop more effective ways to tackle climate change. The computing power they offer could help us process complex data on weather, emissions, and environmental changes.

Healthcare: Quantum computing could personalize treatments based on a person's genetic profile, making healthcare more precise and tailored to individual needs.

Finance: Quantum computers could transform financial modeling, leading to more accurate assessments of risks and faster fraud detection.

Energy and Environment: By optimizing resource use, quantum computing could improve energy efficiency, help develop sustainable materials, and even aid in renewable energy research.

18. What are the types of Quantum Computers ?

Based on qubits, the need for processing power and commercial viability, quantum computers are of three types:

1. **Quantum Annealing** – It is a special time of Quantum computer that addresses classical optimization problems by mapping them to a set of interconnected qubits and then searches for a solution that mimimizes the total energy. You set a set of qubits and their coupling to a ground state, you slowly apply changes to get to end state or configuration, you have a solution when the end state returns to the ground state. The steps represent the solution to optimization problem. The smallest number of steps to do is the optimum solution.

   Analogy: Swordsmith heats up metal rod, beats it into shape, cools in water and repeats the process until perfect sword gets built. If this is repeated several times starting with rod and ending with sword, the fastest to build a sword is the optimum solution.

   These annealers are best suited for solving optimization problems like the flow of air over an aircraft wings, optimizing the traffic flows in the streets of Mumbai, optimum way for a space mission, best way to navigate an aircraft around an airport given any arbitrary current state, etc.

   Traditional computers would take a few thousand hours, weeks or years to compute the optimism solution for these problems, but quantum annealers may do it in a matter of seconds to minutes.

   Quantum Annealing is currently the least powerful and narrow application of quantum computing. The challenge currently is that does not matter how slowly you change the state, the qubits leave the ground state unintentionally. However, companies are building quantum annealers already for large scale commercial use. Dwave systems is a leader in the field having built annealers commercially with >5000 qubits.

2. **Simulation or Analog Machines** - These machines can solve problems that are beyond traditional supercomputers like modeling like simulating a chemical reaction, simulating a protein fold (one of the toughest biochemistry problems) to help advance designer drug testing, Material Science and more.

   These are implemented using digital simulations of single and two qubit logic gates.They can also be simulated using actual qubits in the way the qubits connect to each other and the strength of these connections, which helps one emulate system behaviours in an analog simulation. This is because “Nature” is inherently quantum mechanical. They can also be built as a hybrid of both, which is the most common form of quantum computing existing today – a hybrid of quantum and classical computers.

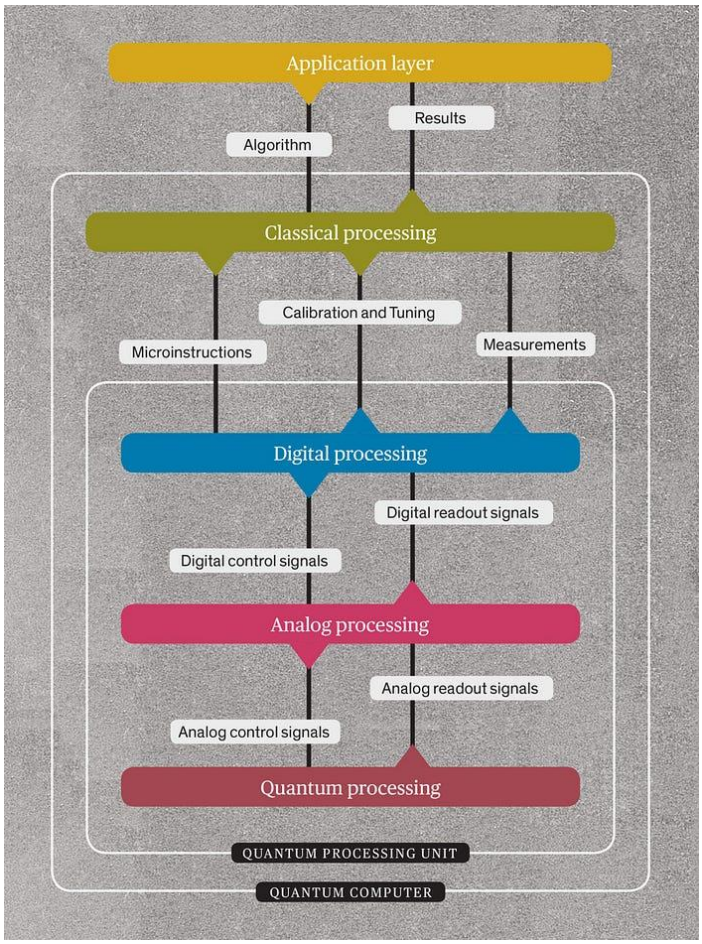
3. **General Purpose/Universal Fault Tolerant Quantum Computers** - Most powerful and the hardest to build. Ideal general-purpose quantum computers need about a million qubits, and right now we are trying to reach to 128-256 qubits. This type of quantum computers, when built, can compute any massively complex datasets and come up with a quick solution (including the annealing equations and simulations). The current 5 leading qubit-type approaches are:

Q-Types	Description	Key Companies
Superconducting	One of the most popular types of quantum computers is a superconducting qubit quantum computer. Usually made from superconducting materials, these quantum computers utilize tiny electrical circuits to produce and manipulate qubits. When using superconducting qubits, gate operations can be performed quickly. They need to be cooled to space temperatures for superconducting to work.	Google, IBM, IQM, Rigetti Computing, many more.
Photonic	These types of quantum computers use photons (particles of light) to carry and process quantum information. For large-scale quantum computers, photonic qubits are a promising alternative to trapped ions and neutral atoms that require cryogenic or laser cooling.	Xanadu, ORCA Computing, Quantum Computing Inc, PsiQuantum, Quantum Source, etc.
Neutral Atoms	Quantum computing based on neutral atoms involves atoms suspended in an ultrahigh vacuum by arrays of tightly focused laser beams called optical tweezers, though not all neutral atom companies use optical tweezers. Neutral atom quantum computers are less sensitive to stray electric fields, which makes them a good option for quantum processors.	Pasqal (merged with Qu&Co), Atom Computing, ColdQuanta, and QuEra.
Trapped Ions	A trapped ion quantum computer involves using atoms or molecules with a net electrical charge known as “ions” that are trapped and manipulated using electric and magnetic fields to store and process quantum information. As trapped ions can be isolated from their environment, they are useful for precision measurements and other applications requiring high levels of stability and control. Also, the qubits can remain in a superposition state for a long time before becoming decoherent.	Quantinuum (a company that came out of the merger between Cambridge Quantum Computing and Honeywell Quantum Solutions), IonQ, Quantum Factory, Alpine Quantum Technologies, eleQtron amongst others
Quantum Dots	A quantum dot quantum computer uses silicon qubits made up of pairs of quantum dots. In theory for quantum computers, such ‘coupled’ quantum dots could be used as robust quantum bits, or qubits.	Diraq, Siquance and Quantum Motion.
Other approaches	electrons on helium, NV diamond and the topological approach.	Several

Right now, researchers are designing algorithms that can work with these computers. Some well-known algorithms are Shor’s algorithm (for advanced code breaking) and Grover’s algorithm (for searching massive unstructured sets of data like internet searching and so on). Currently, there are 50+ unique algorithms developed for these general-purpose quantum computers. Some of these algorithms can be used as building blocks for quantum AI when the hardware catches up.

19. Blueprint for a practical Quantum Computer

One possible way to build a universal quantum computer:



20. What are the challenges facing Quantum Computing?

Quantum computing faces several challenges, including error rates and qubit coherence. Quantum systems are extremely sensitive to their environment, which can lead to errors and loss of coherence. Maintaining qubits in a stable state (quantum decoherence) and error correction are significant challenges. Additionally, developing scalable quantum systems and creating useful algorithms are ongoing challenges in the field.

21. What is the Quantum Computing Market Landscape ?

Overview

The global quantum computing market could add a total of more than $1 trillion to the global economy between 2025 and 2035, according to a new analysis from The Quantum Insider, the leading source of market intelligence on the quantum technology landscape. Vendors are expected to capture $50 billion of revenue over this period.

This forecast points to the significant economic potential unlocked by quantum computing and reflects the growing confidence in quantum technologies as they edge ever closer to mainstream adoption. The key areas of impact is forecast to be:

- **Economic Impact:** A new report from The Quantum Insider forecasts that quantum computing will contribute $1 trillion in value creation by 2035.
- **Vendor Revenue:** Quantum computing vendors expected to generate $50 billion in revenue by 2035.
- **Job Creation**: Quantum computing will create an estimated 840,000 new jobs by 2035, with 250,000 by 2030.

As per Fortune Business Insights, the global quantum computing market size was valued at USD 885.4 million in 2023 and is projected to grow from USD 1,160.1 million in 2024 to USD 12,620.7 million by 2032, exhibiting a CAGR of 34.8% during the forecast period. The North America region dominated the market with a share of 43.86% in 2023. The quantum computing market growth is driven by advanced problem-solving, AI advancements, and global investments.
(Source: https://www.fortunebusinessinsights.com/quantum-computing-market-104855)

There are hundred of companies active in this industry, all dealing with various aspects. The key aspects are: building a fault tolerant quantum computer, solving the problem of decoherence or performing noise/error correction, quantum sensors, optics and photonics, solving the problem of scaling and most importantly implementing known and finding new applications with quantum advantage. Some companies were able to raise 100’s of millions in industry and VC funding.

Europe is estimated to grow with the third highest CAGR as the region has an increasing number of startups operating in the field of quantum technology. For instance, in January 2023, Paris–based quantum computer startup, PASQAL raised EUR 100 million (USD 109 million) to deliver commercial advantages over classical computers in Europe. Further, a growing number of digital government regulatory environments and initiatives to bring development across European industries using cloud and quantum technology are anticipated to drive market growth and technological advancements in the region during the forecast period. Owing to these

reasons, the regional market is projected to exhibit healthy growth in the next few years.

Healthcare, chemicals, and banking and finance are major industries in Asia Pacific. South Korea, China, and Japan are the regions' producers of electronic goods such as gaming consoles, mobile phones, and laptops. Simulation, machine learning, and optimization applications must be addressed across these industries. The rapid expansion of Asia Pacific's expanding economies and the increased use of new technologies in the industrial sector are providing opportunities for the region's medium-sized and large businesses.

Quantum services and systems are in high demand in Asia Pacific, which has a positive impact on the market's expansion. Hence, it is anticipated to grow with the highest CAGR during the forecast period i.e. from 2024 to 2032.

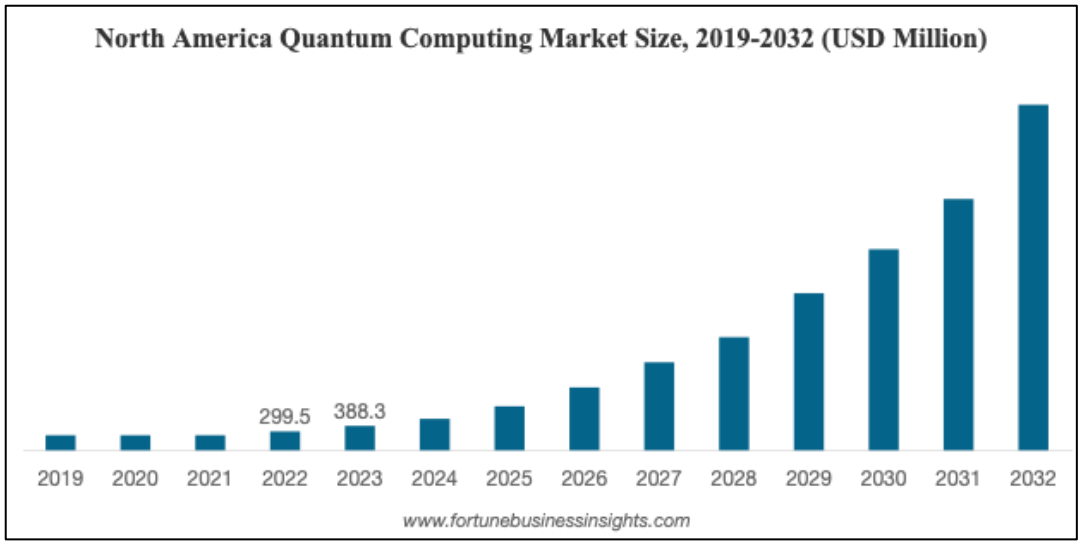
Growing investments in quantum computing technology to bring development across different sectors such as energy, life sciences, and finance across the Middle East & Africa and South America regions helps to drive the product demand during the forecast period. For instance, In February 2022, Saudi Arabia committed USD 6.4 billion investment in advanced technology to boost the demand of quantum computing to emphasize the R&D and technological advancements.

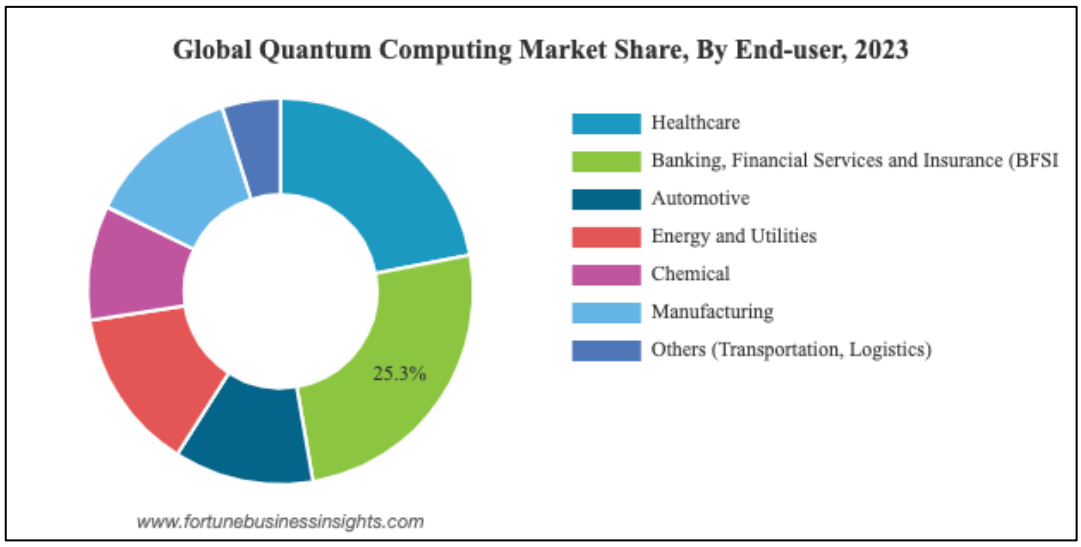
QUANTUM COMPUTING MARKET TRENDS

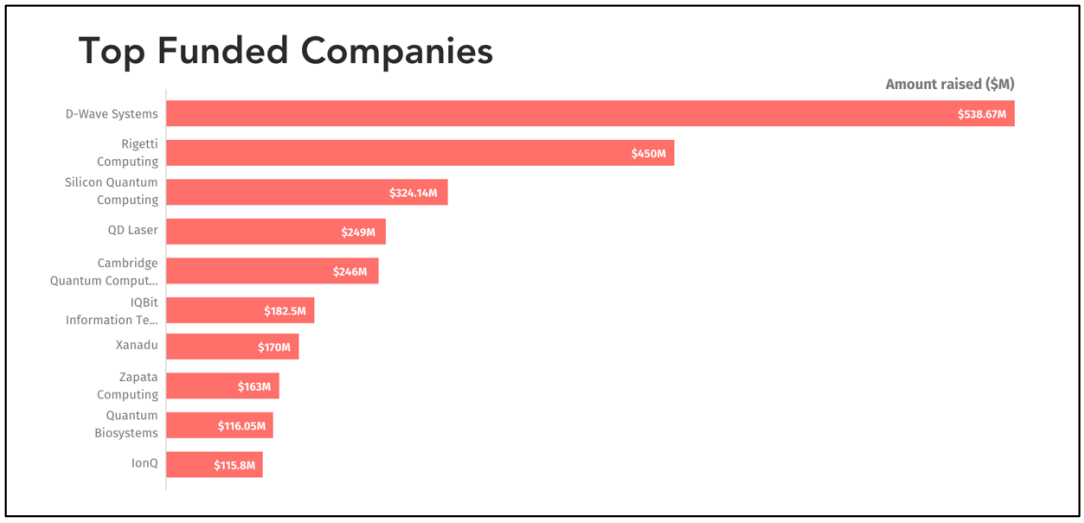
Quantum computing is an evolving high-tech technology. Patent filings for quantum technologies have been increasing rapidly in recent years. The increasing expansion of patenting activities along with computing technology across various technical and non-technical areas such as IT architectures, material engineering and drug development boosts the performance of the quantum ecosystem with a rising number of patent applications. For instance,

In October 2023, Amazon filed a patent for quantum computing across multiple quantum technologies through edge computing devices to utilize computing services without the need for direct access to quantum hardware.

Patents and investments are shaping the future by developing enhanced technologies. For instance, AMD submitted a patent for teleportation in September 2021, to power quantum computing. By reducing the number of qubits needed for precise calculations, the patent's model aims to address the issues of stability and scalability.







Quantum Computing Market Segments

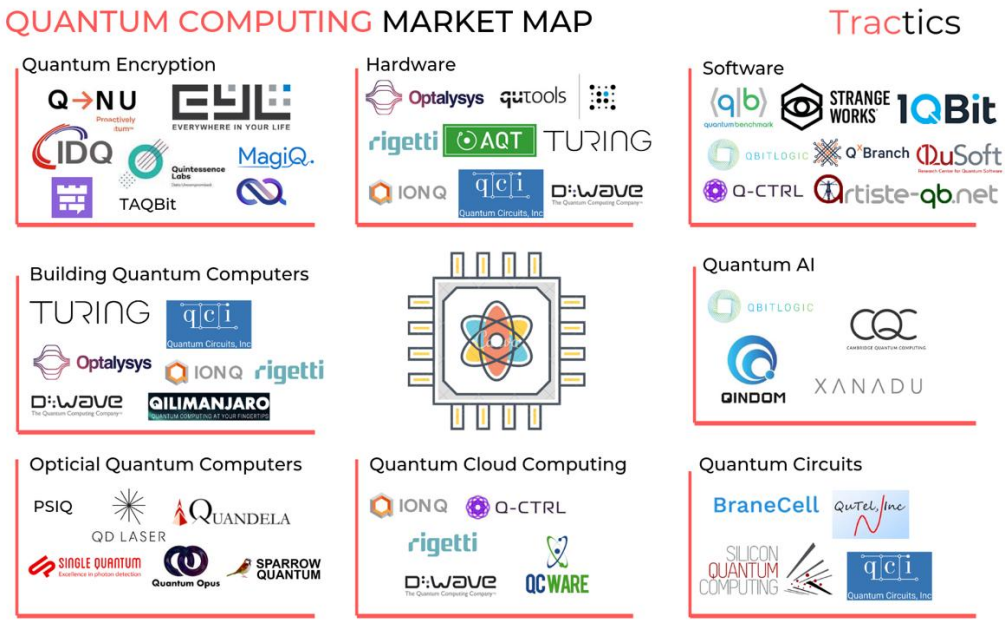
The market is segmented typically as follows:

- **Components** : Hardware, Software, Sensors
- **Deployment**: Cloud, On-premise
- **Application**: biomedical simulations, optimization, machine learning, electronic material discovery, financial services, and others (traffic optimization, weather forecasting, and others).
- **End user**: healthcare, automotive, BFSI (Banking, Financial Services and Insurance), chemical, manufacturing, energy and utilities, and others (transportation, logistics, and others)

Details of companies active in various segments:

- **Quantum Encryption** — Startups like ISARA, Crypta Labs, and Cyph offer encryption based on the science underlying quantum mechanics. There are 16 companies in this bucket.
- **Hardware** — These are startups that are building hardware components for quantum machines. Startups like IonQ, Optalysys, Photon Spot, ColdQuanta, and Qubitekk are developing and manufacturing hardware that is needed to build and maintain a quantum computing.
- **Software** — From developing tools for software engineers to build Quantum applications. Firmware framework, Quantum simulation software to the quantum algorithm that can help interface with the advanced computers. Horizon Quantum, Strangeworks, Quantum Benchmark, QuantumWise, QuSoft, Artiste QB Net, and 1QBit are some of the most interesting companies in this segment.
- **Building Quantum Computers** — These are hardware manufacturers who are building full-stack quantum computers. Companies like Oxford Quantum, IonQ, Optalysys, Rigetti Computing, D-Wave Systems, Turing Quantum, Alpine Quantum Technologies are working towards either Quantum Simulation machines or Full-stack general-purpose quantum computers.
- **Quantum AI** — Qindom, Zapata Computing, and Xanadu are some of the key players in this segment who are building quantum algorithms and hardware to create sustainable Infrastructure for Quantum ML/AI.
- **Optical Quantum Computing** — These are companies which develop high-speed photon detectors that will enable next-generation experiments in quantum optics, optical quantum computation, single-photon communication, low-flux biophotonics, and remote sensing. Sparrow Quantum, Fathom Computing, Single Quantum, and Quantum Opus are few key players in this segment.
- **Cloud** — Companies like QC Ware and Qilimanjaro are developing cloud-based platforms for quantum computing machines.
- **Circuits** — Circuits one of the key components in Quantum Computers and companies like BraneCell develops near ambient-temperature quantum computing architecture that make Quantum computers commercially viable. Other companies like QuTel, Oxford Quantum Circuits, Silicon Quantum Computing, and Quantum Circuits, Inc. are working on similar technology.

Quantum Computing Market Map of key companies per segment:

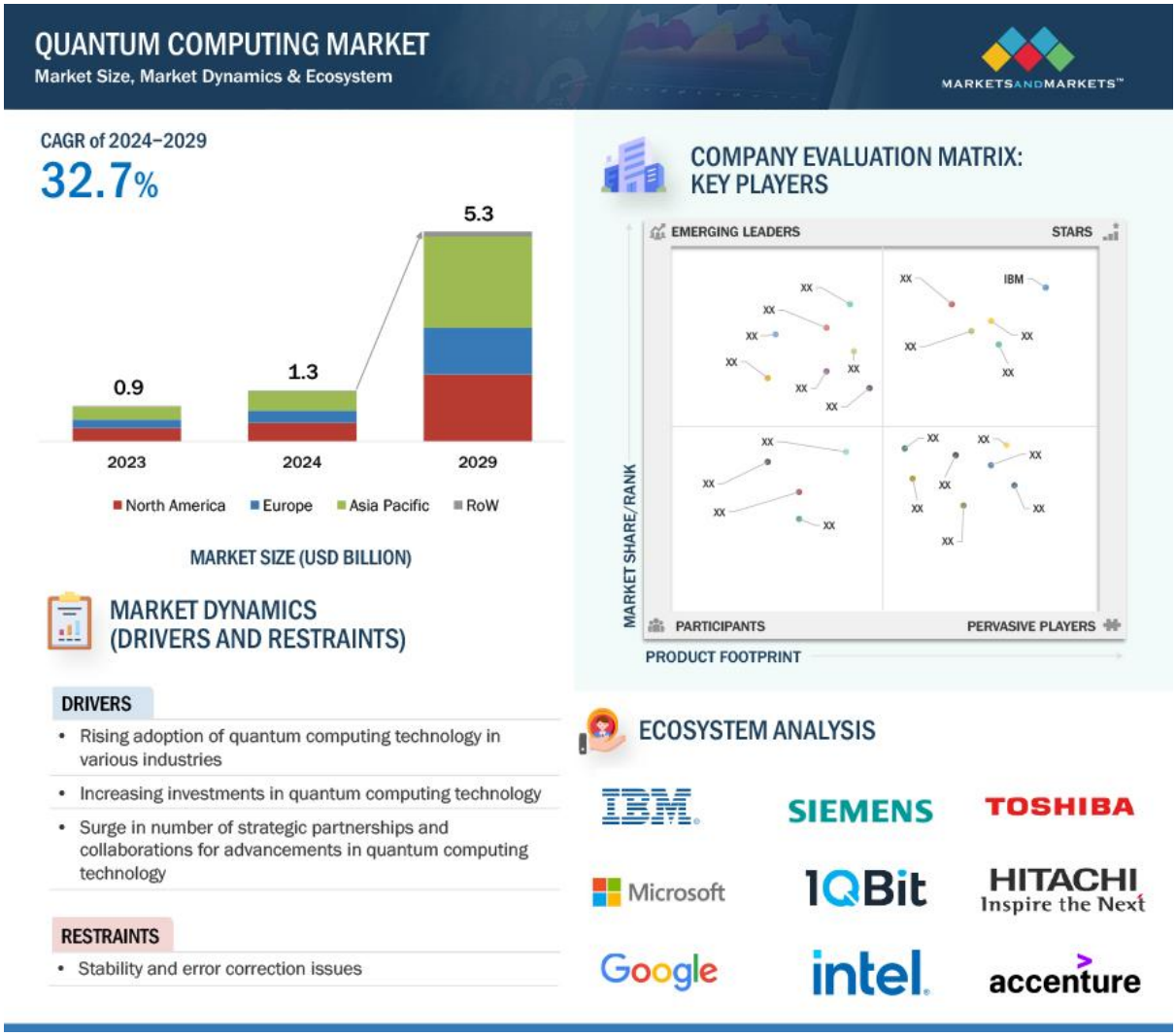


COMPETITIVE LANDSCAPE

The leading players in the market are focusing on collaborations, partnerships, product innovation, and expansion of the market presence globally. The key players in the market include IBM Corporation, Microsoft Corporation, Intel Corporation, D-Wave Systems, IonQ, Rigetti, Quantinuum, QC Ware, Google LLC, and others developing innovative quantum solutions.

LIST OF TOP QUANTUM COMPUTING COMPANIES:

- IBM Corporation (U.S.)
- D-Wave Systems Inc. (Canada)
- Microsoft Corporation (U.S.)
- Intel Corporation (U.S.)
- Rigetti & Co, Inc. (U.S.)
- Google LLC (U.S.)
- QC Ware (U.S.)
- Quantinuum Ltd. (U.S.)
- Riverlane (U.K.)
- IonQ (U.S.)
- TerraQuantum (Switzerland)
- Alpine Quantum Technologies (Switzerland)
- IDQuantique (Switzerland)



KEY DEVELOPMENTS IN THE QUANTUM COMPUTING MARKET:

November 2024: Google DeepMind develops an AI-based decoder that identifies quantum computing errors. Researchers from the RIKEN Center for Quantum Computing and Toshiba have succeeded in building a quantum computer gate based on a double-transmon coupler (DTC), which had been proposed theoretically as a device that could significantly enhance the fidelity of quantum gates.

February 2024: D-Wave has made their 1,200+ qubit Advantage prototype available via their Leap real-time quantum cloud service. This allows existing Leap subscribers to gain immediate access to the new hardware, and new users can sign up for Leap and receive up to one minute of complimentary use of the Advantage2 prototype alongside other quantum processing units (QPUs) and solvers offered by the platform

November 2023: Rigetti Computing has secured Phase 2 funding from DARPA (Defense Advanced Research Projects Agency). These USD 1.5 million (potential) grants will support Rigetti in developing benchmarks to measure the performance of large-scale quantum computers for real-world applications.

November 2023: Terra Quantum, a quantum service provider, collaborated with NVIDIA to develop quantum-accelerated applications. The deal would help bridge the gap between classical and quantum computing, leveraging hybrid algorithms.

October 2023: Fujitsu partnered with RIKEN and developed AI drug discovery technology. This launch of AI drug discovery technology combines the computing power of the newly developed 64 qubit superconducting quantum computer to deliver a new platform to businesses and research institutions.

September 2023: Xanadu, partnered with Electronics and Telecommunications Research Institute (ETRI) to bring advancement in computing technologies using machine learning and artificial intelligence (AI) technologies.

November 2022: IBM entered a collaboration with Vodafone on quantum-safe cybersecurity by joining the IBM Quantum Network. This collaboration would help validate and progress potential quantum use cases in telecommunications.

March 2022: Quix Quantum unveiled new quantum photonic processor. It was developed at QuiX' facility, in the Netherlands. It performs nearly two times better than current processors. This processor has a record number of qumodes (20) and the highest operating specification

22. What is Quantum Computing threat to cybersecurity ?

Quantum computing, once robust enough, could potentially break many of the current cryptographic algorithms, such as RSA and ECC, which secure digital communications. This is because quantum computers, once they reach sufficient maturity, could perform calculations, like factoring large numbers, much faster than classical computers. However, this threat has led to the development of quantum-resistant cryptography, which aims to develop new algorithms that could be secure against quantum attacks.

Asymmetric Encryption:

RSA is the standard for digital firms and some TLS 1.2 protocols that are found in the network. This algorithm was created (or at least proposed) in 1978. RSA stands for ***Rivest–Shamir–Adleman***, the surnames of its creators. It allows an entity to cypher and decypher a message without sharing the same secret key.

Whereas symmetric mechanisms such as AES are based on computational problems such as working with Galois Bodies, matrix shifting and transposition and operating with polynomials (which our computers are good at doing, they are purely mathematical operations), asymmetric cyphers are… different.

They are based on harder mathematical problems such as factorising big prime numbers, discrete logarithms and elliptic curves. And of course, discrete mathematics. The security of RSA is based, especially, on working with factorising numbers. In classical computers, this is a computationally complex problem to solve (NP Hard, complexity and time needed to solve grows exponentially with size of input).

However, with quantum computers, this statement changes. Because of the nature of the qubits (they can be either 0 or 1 at the same time due to some physics procedures), Peter Shor invented Shor's Algorithm which is capable of factorising prime numbers in an impressive polynomial time (O(log N)).

There are several variations of this algorithm, each one specialised in solving a different problem (factorising, discrete logarithm and the period-finding problem). Once there is a fault tolerant quantum computer with sufficient qubits (currently estimated to about 1000 logical qubits to break 2048 bit ciper), RSA can be cracked in seconds or minutes. Same logic applies to Diffie Hellman algorithm based on elliptic curves (ECC – Elliptical Curve Cryptography), also popular in cyber security.

Symmetric Encryption

AES-128: Due to the nature of commonly used algorithms, in order to break with classical computers, it we will need brute force, especially 2^{128} operations (O(n)).

With the quantum Grover's algorithm, which is considered to be a quantum search algorithm, we can reduce this complexity to an O(n^(1/2)). That makes a total of 2^{64} operations to calculate. However, research is being made to further optimize this and once a strong enough quantum computer is built, the inherent parallelism could lead to also breaking these ciphers within seconds or minutes.

Modern Communication and The Quantum Threat

The Cyber Security industry finds itself in a never-ending arms race against ever more sophisticated and ingenious attackers, hacking groups and malicious actors. Companies today face myriad threats that exploit all kinds of vulnerabilities in their enterprises. The surface area of potential compromise is expanding, stretching from an organization's employees — who are frequently the target of phishing and social engineering attacks — to the supporting technological infrastructure that is all too often the subject of devastating evolving attacks and zero-day threats. This constantly changing threat landscape, organizations must be increasingly vigilant and proactive in preventing catastrophic damages to their business.

However, amidst all this chaos, one threat that is currently largely unaddressed looms large on the horizon. As will be explained in the section on the "store now — decrypt later" risk, for some data and some companies, it is already too late to prevent against it. This vulnerability exists in just about every network and internet

service used across the globe.

Quantum computers have the potential to help humankind overcome various technological limitations and solve our greatest challenges in both business and society.Their development is a double-edged sword because they will be able to run an algorithm capable of decrypting much of the world's confidential data. any information encrypted using certain encryption methods (e.g., the RSA method) could be decrypted by a quantum computer. Currently, the enormous amount of information that is transferred using this kind of quantum-vulnerable encryption includes — but is not limited to — email, direct messages, file transfers, financial information, internet browsing and so on.

The "Harvest Now – Decrypt Later" Risk

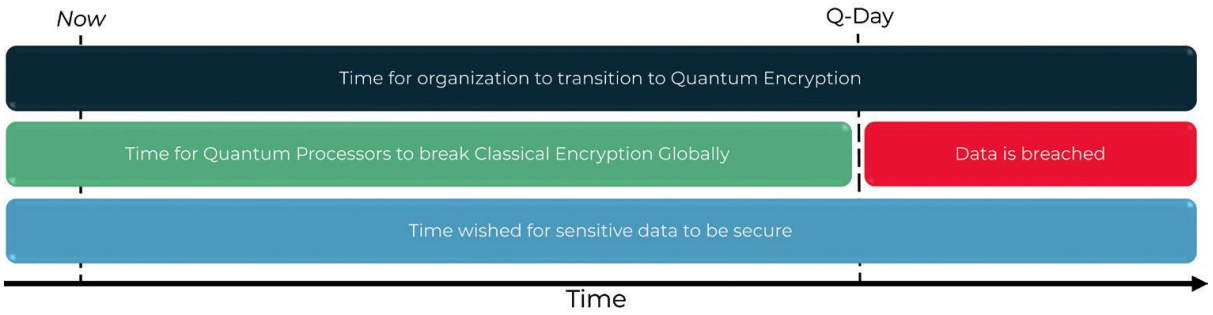
Y2Q (also known as Q-Day) is the date when quantum computers will have advanced to the point where they can easily crack some of the public-key cryptography schemes that are used in communications everywhere from internet browsing to email messaging. Past this date, any individuals or organizations in possession of a quantum computer will be able to decrypt the information they have acquired that was secured with the quantum-vulnerable methods (e.g., RSA encryption).

Notably, this includes sensitive information that could be acquired today and might still be sensitive in the future. This is known as the "store now — decrypt later" threat. Because malicious actors can obtain copies of recently encrypted data and then wait until sufficient quantum computing resources have become available to decrypt and access the sensitive information, one could say that some encrypted data that exist today are effectively already stolen. This is best described by Mosca's theorem (See Figure 1. Mosca's Theorem).

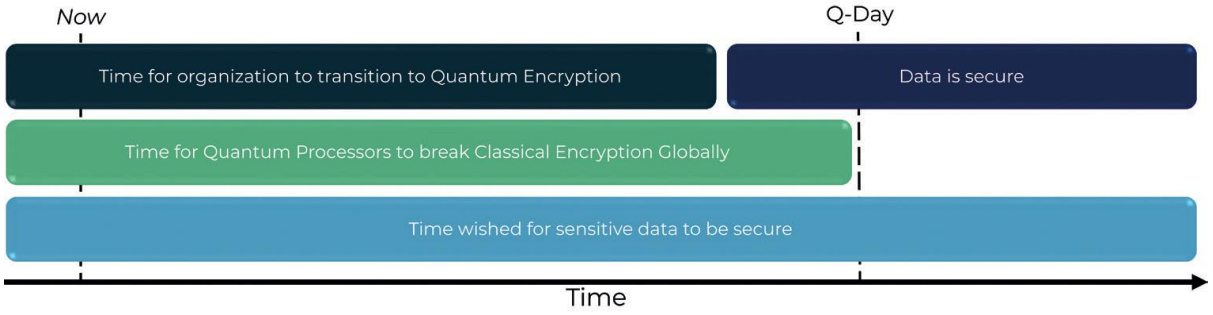
Even though a portion of the encrypted data that exist today will become less sensitive and important with time, this is certainly not true of all data. Much of the most sensitive and private data types have very long shelf lives and though estimates of when Y2Q will arrive vary, some groups state that any sensitive data stored today with a shelf life longer than five to ten years is already at risk. From medical records within healthcare to bank details and transfer information, this threat is widespread across multiple industries.

NATO, the U.S. Government and a wide array of global organizations have already begun preparation for Y2Q, as it is understood that if swift action is not taken, the security of a vast proportion of global data will be compromised. As each day passes, organizations that do not address the incoming threat are increasing the risk of having their sensitive data stolen in the future.

Mosca's Inequality Outcomes



Scenario 1: Organisation does not quantum-secure their data in time for Q-Day, leading to data breaches in the future



Scenario 2: Organisation does quantum-secure their data in time for Q-Day, mitigating future data breaches

Technical Deep Dive on Quantum Decryption

The basis for all classical public-key encryption methods in use is the computational difficulty of solving certain mathematical problems. An example of this is RSA encryption, which is predicated on the problem of factorizing large integers into constituent primes — for which currently there exists no efficient algorithmic solution.

These problems are called 'intractable' — there is no efficient algorithm to solve them. Therefore, these methods of encryption are secure simply due to the staggering amount of time it would take any classical computer — however large — to decrypt them.

However, this is not true of quantum computers. Quantum computers, and the algorithms that can be run on them, turn certain classically intractable problems into tractable ones. Which is to say, they become solvable in much smaller amounts of time and do not require exponentially more time for larger problem instances. For instance, one such algorithm which enables this is Shor's algorithm, which allows quantum computers to tractably factorize large prime numbers, as well as to efficiently solve the so-called discrete logarithm problem. The algorithm shrinks

the computational time to solve these problems exponentially. This means all the widely popular encryption key protocols based off these problems — such as RSA, Diffie-Hellman and Elliptic Curve schemes — will soon no longer be secure.
When quantum computers and resources become more widely available past Y2Q, malicious actors or organizations will be able to utilize them with algorithms such as Shor's to decrypt commonly used public key encryption protocols with relative ease. They will then have full access to sensitive data that should have been kept confidential.

23. How to Quantum-Secure Your Organization

1. Organizations are advised to conduct a thorough inventory to determine what systems and processes use public-key cryptography. Clarity should be obtained on how the cryptography is used to protect the confidentiality and integrity of data at rest, data in use and data in motion. This applies to numerous types of data, including financial, legal and industry specific.

2. Organizations are advised to assess what quantum-secure technology upgrades are appropriate, while seeking to discover any technical constraints that their systems may have with regards to implementing security upgrades.

3. Organizations should also work with service providers, partners and customers to coordinate their adoption of any quantum-secure technologies, such as to preserve the interoperability of their existing infrastructure and to ensure there are no service disruptions in the process of securing data.

4. Organizations can contact service providers to execute the decided implementations of quantum-secure technologies.

5. Overall, as we approach Q-day and beyond, organizations should seek to adopt a long-term, quantum-agile strategy when it comes to their security upgrades.