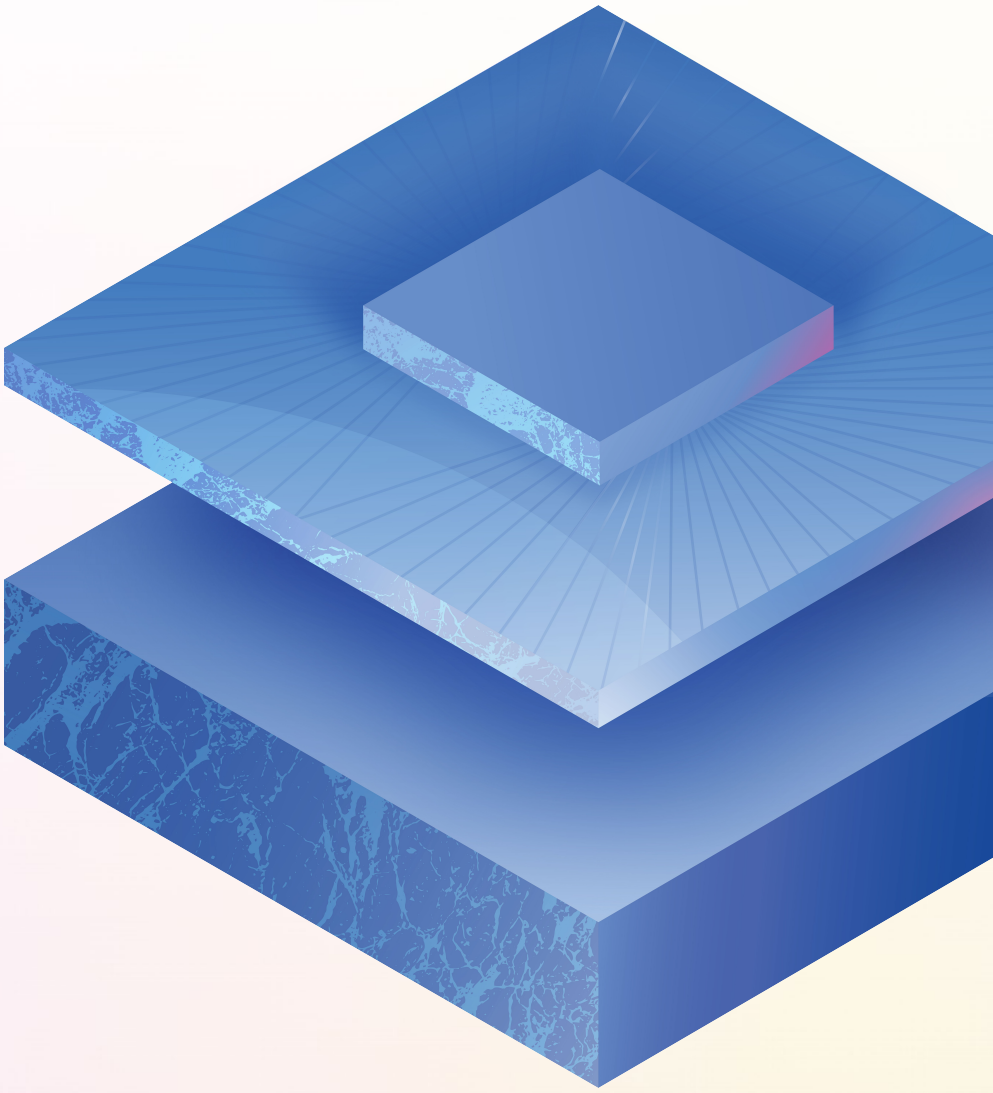
What is quantum computing?



Google

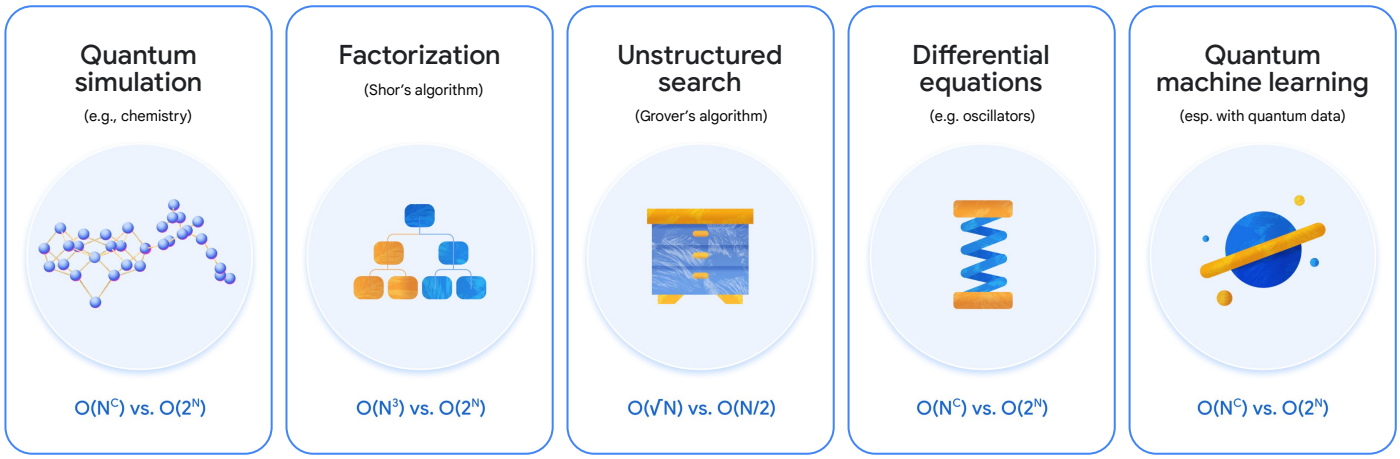
Why should policy makers care about quantum computing?

Quantum computers are not merely faster versions of classical computers; they represent an entirely different computing paradigm. By harnessing principles of quantum mechanics, **"qubits"** – quantum bits, the fundamental building blocks of quantum computers – can exist in multiple interconnected states simultaneously. This unique capability allows for **highly complex information processing,** opening up unprecedented possibilities in computation.

Quantum computing holds promise for addressing some of society's toughest challenges – problems beyond the reach of even today's supercomputers. Broadly speaking, quantum computers leverage the principles of quantum mechanics **to directly simulate the fundamental processes in nature.** This capability will allow future quantum computers to perform a wide array of calculations – including molecular simulations – on a scale that is far out of reach of classical computing technologies, leading to potential breakthroughs in energy, healthcare, climate, and more.

Quantum computers will be a powerful tool for computation

For example, consider global fertilizer production. The current industrial method, known as the Haber-Bosch process, consumes a staggering 2% of the world's energy. Scientists have long sought a more efficient way to produce fertilizer, but the underlying chemistry is far too complex for traditional computers to simulate. Future quantum computers, with their more powerful capabilities of molecular simulation, would allow us to model these chemical processes with unprecedented accuracy, potentially leading to the discovery of new, energy-saving methods of fertilizer production and a **significant reduction in global energy consumption.**



Above: *Common examples of difficult problems quantum computers have the potential to solve.*

As we all learned with AI, greater processing power does not just make present functionalities faster and cheaper. It can enable entirely new applications that weren't possible before. Technological progress is not linear, and slow progress can accelerate quickly due to the sudden parallel occurrence of innovations in converging areas.

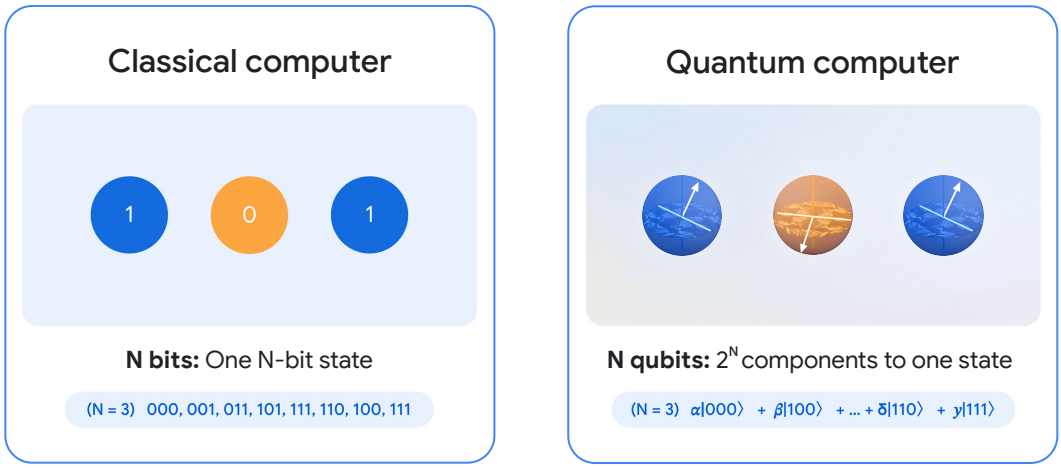
The following sections provide policymakers with an analysis of the current state of quantum computing, including recent advancements and the significant technical hurdles that remain. This information will equip decision-makers with the insights needed to shape policies that effectively support quantum technology's development for societal benefit, while proactively addressing data security and infrastructure challenges.

How do quantum computers work?

Abacus | Classical computer | Quantum computer

Quantum computers are fundamentally different from classical computers and are expected to complement them rather than replace them. While classical computers handle everyday tasks like organizing information, quantum computers introduce a new computing paradigm suited for some complex problems that classical machines cannot solve.

Quantum computers use quantum bits, or **qubits,** as their fundamental units of computation. In classical computers, the basic building blocks are bits, which can be in one of two states: 0 or 1, much like a light bulb that is either on or off. Qubits, however, can exist in a state called **superposition,** where they are not just 0 or 1 but can exist in both simultaneously (like a light dimmer, or the light being on and off at the same time). We can imagine the state as a position on the surface of the Earth, with the north and south poles representing the states 0 and 1. Being in a superposition is like standing at the equator, where there's a 50% chance of measuring the state as 0 and a 50% chance of measuring it as 1. Unlike classical bits, whose state remains the same unless altered, qubits in superposition provide a **probabilistic outcome when measured.**

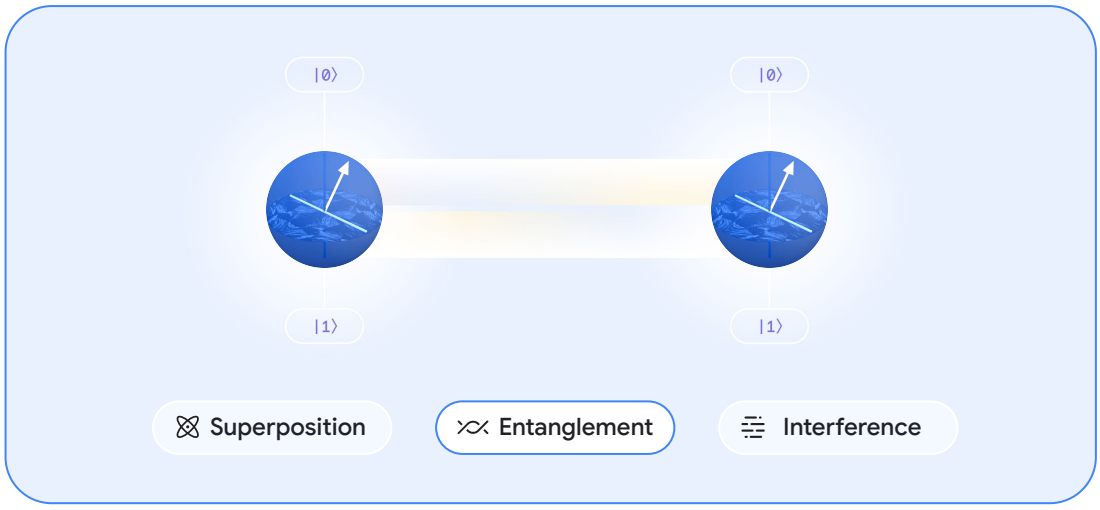


Quantum computing leverages **three key quantum mechanical properties:**

- **Superposition,** which as noted above allows qubits to represent multiple states at once, like a spinning coin that embodies both heads and tails. This enables quantum computers to explore many possibilities in parallel during computation. When qubits are measured, this superposition "collapses" – i.e. the qubit is measured in a 0 or 1 state, like the coin when it comes to rest on heads or tails.

- **Entanglement** links qubits so that the state of one instantly correlates with another, even at a distance, enhancing computational power; Albert Einstein called this "spooky action at a distance."

- **Interference** allows quantum algorithms to amplify correct solutions through constructive interference while canceling out incorrect ones via destructive interference. This can be thought of like waves on the ocean that can build on each other or cancel each other out.



Unlike classical computers, which process **one state at a time**, quantum computers **encode and manipulate probabilities across many states simultaneously** during computation. This parallel exploration enables them to solve complex problems much faster, handling **certain tasks** exponentially faster than classical computers.

Unlike classical computers, which primarily use silicon, today's quantum computers employ various materials and modalities to construct qubits, including superconducting circuits, cold atoms, silicon dots, and trapped ions. We are still in an **exploratory phase,** where different device platforms are being tested to store and manipulate quantum states. Each approach has unique advantages, but **none have yet reached the scale needed to solve significant real-world problems.** The future of quantum hardware remains a very active area of research.

Where are we today?

The ultimate goal of quantum computing is to develop a **large-scale fault-tolerant quantum computer** - a device with millions of **reliable** qubits that can perform **error-free** computation (via quantum error correction, which is described below). A large-scale fault-tolerant quantum computer would unlock immense computational power, but achieving this goal remains a distant prospect due to the technical challenges involved in connecting thousands of fault-tolerant qubits without disturbing their delicate quantum states.

Currently, we are in the **NISQ (Noisy Intermediate-Scale Quantum) era,** where machines with on the order of 100 qubits can conduct groundbreaking research in physics. For instance, such devices have been used to realize the curious behavior of a long-sought particle, study exotic matter, and resolve a long-standing debate about magnets – important scientific discoveries that inform progress in many fields of science. In addition to their scientific interest, physics breakthroughs may also unlock new technologies such as loss-free power grids. After all, while general relativity and quantum mechanics seemed esoteric at first, they seeded now-ubiquitous technologies like GPS, silicon computer chips, and MRI machines.

Despite these advances, **error rates** present a significant challenge. While classical bits also experience occasional errors - about one error in a trillion operations - the range of possible errors is limited: a 0 can flip to a 1 and vice versa. Qubits, however, are far more susceptible to a wide variety of errors due to their quantum properties. **Correcting these errors as quantum hardware scales is one of the field's biggest technical challenges.**

Challenges and opportunities

While quantum computing has gained great interest, and we are already doing breakthrough science on the current NISQ devices, significant challenges exist in bringing the technology to full potential. These challenges could be grouped into three main cohorts: technological, economic and ecosystem challenges.

Technological challenges

1. Error correction: Current NISQ devices are very error prone - qubits are delicate systems, and their state can be disrupted by many factors - temperature, vibration, and even stray particles of light can introduce errors. As quantum circuits become larger, the number of errors, if not corrected, also increases. Without error correction, quantum information encoded in qubits will be lost to the environment very quickly, rendering computation infeasible. **For meaningful computation, these errors must be corrected.**

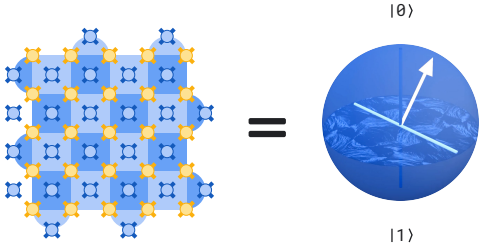
Some leading modalities of quantum computers (e.g. superconducting qubits) require advanced cryogenics systems to cool down chips to about 10 millikelvin - temperature colder than outer space. This leads to chips exhibiting quantum mechanical properties and isolating them from environmental noise. Cooling addresses some errors, but not all of them. Other factors impacting error rates are **chip architectures** (i.e. how qubits are layered out on the chip to eliminate crosstalk and loss of information), and **Quantum Error Correction** - a set of techniques to correct errors.

Quantum error correction is a **software-based** approach to increasing the reliability of quantum computers by encoding the information of a single qubit into multiple physical qubits, creating a **"logical qubit."** It is believed to be the only way to produce a large-scale quantum computer with error rates low enough for useful calculations. Instead of computing on the individual qubits themselves, we will then compute on logical qubits. By encoding larger numbers of physical qubits on our quantum processor into one logical qubit, we hope to reduce the error rates to enable useful quantum algorithms.

Transitioning from NISQ to fault tolerance requires reducing quantum error rates dramatically: from approximately one error in every 10,000 operations (in the best cases today) to about one error in a trillion operations. **Bridging this gap represents one of the most substantial obstacles to building practical, large-scale quantum computers.**

Quantum error correction:

Enhance robustness to errors by encoding a single logical qubit in many physical qubits. Our team achieved the first demonstration in 2023.



2. Scalability: Scaling quantum computers from a few qubits to the large numbers needed for practical applications presents a massive challenge due to **error rates, hardware limitations, and system complexity. It's not just about increasing qubit count; the quality of each qubit and the scalability of the overall system are equally critical.**

One major obstacle is **decoherence,** where quantum information in a qubit is lost to its environment, making **Quantum Error Correction** essential to sustain computation. However, scaling up to fault-tolerant systems with millions of qubits will require far more than just advanced QEC techniques. We will need innovative chip architectures and improvements in supporting components.

For instance, superconducting quantum computers require expensive dilution refrigerators to cool systems down to near absolute zero, stabilizing qubit behavior. Each qubit on Google's superconducting quantum computers is currently controlled by an individual wire sending microwave pulses, but scaling this approach to millions of qubits - each with its own wire - is infeasible due to heat generation, physical limitations, system complexity and cost. As a result, innovation is crucial, not only in chip architecture but also in redesigning control systems and ancillary components, which number around 10,000 for a device with under 100 qubits today.

3. Applications: We have identified ~60 algorithms for which a quantum computer will offer advantage – i.e. it will be possible to run these algorithms on a future quantum computer, and it is impossible or intractable to run them on a classical supercomputer. **Examples include:**

- **The CYP450 mechanism** – *"Reliably assessing the electronic structure of cytochrome P450 on today's classical computers and tomorrow's quantum computers"*
- **Lithium-ion batteries** – *"Fault tolerant quantum simulation of materials using Bloch orbitals"*
- **Fusion reactor dynamics** – *"Quantum computation of stopping power for inertial fusion target design"*

But there is a need to identify more real-world applications for future quantum computers. The challenge here is to **take a long-term view and encourage algorithms researchers to focus on practical, impactful uses.** It is difficult to discover new quantum applications, and three key things need to be present for a commercially-viable quantum computing application: it needs to be a (1) useful problem to which (2) there exists no fast classical algorithm, and there is a (3) fast quantum algorithm.

Economic challenges

1. Supply chain: Quantum computing requires specialized infrastructure and scarce components, but demand has not yet scaled to create reliable supply chains. Different qubit architectures also have varied infrastructure needs.

2. Practical concerns: Finding useful quantum algorithms that offer exponential speedup without classical equivalents is challenging. Significant investment in research and development is needed from both public and private sectors.

3. Workforce development: There is a shortage of qualified personnel with expertise in quantum computing, materials science, and programming. As the industry matures, there is a growing need for specialized engineers and technicians, not just PhD scientists, which presents recruitment challenges.

Ecosystem challenges

1. Security: Despite their potential, quantum computers are often spotlighted for their ability to challenge current encryption systems. Since the publication of Shor's algorithm in 1994, which theorized that a large, reliable quantum computer could break today's public-key encryption, the risks to cybersecurity have gained attention. Current encryption, like RSA, depends on the difficulty of factoring large numbers, but Shor's algorithm indicates that a **large enough fault-tolerant quantum computer** could do factorization efficiently, rendering existing encryption vulnerable.

However, realizing this level of quantum capability is still a long-term endeavor. **It's estimated that building a quantum computer capable of breaking public-key encryption would require approximately 4 million physical qubits - a significant leap from where we are today, with our current NISQ devices of on the order of a hundred qubits.**

That said, **organizations should take steps and protect their infrastructures from such potential attacks now.** In August 2024, The National Institute of Standards and Technology (NIST) released a final set of post-quantum cryptography (PQC) algorithms designed to withstand the attack of a quantum computer. While quantum computers will not break encryption soon, proactive migration to PQC is necessary in order to:

- Prevent "store-now-decrypt-later" attacks, where encrypted data is stored until a quantum computer can decrypt it;
- Address firmware in some hardware that needs to be operational for over a decade; and
- Allow time for a gradual transition and necessary investments.

2. Investment and funding in quantum research: Considerable and continued funding is needed for research and development in quantum computing, both from public and private sectors.

3. Industrial adoption and readiness: Enterprise stakeholders need to be prepared for adopting quantum technologies. This includes skills (workforce development), a clear understanding of what problems quantum computing can realistically solve, and a plan for integrating quantum technology when it is sufficiently mature to apply in that industry.

Addressing these challenges will require coordinated efforts across research, industry, and policy to pave the way for meaningful quantum computing advancement.

Focus areas for policymakers

In this promising yet challenging field, policymakers can play a critical role in accelerating quantum computing's potential. Here are some key areas for engagement:

Supply chain

- **Support key component production:** Provide support for companies manufacturing essential components like cryogenics and specialized wiring. Since only a few companies supply these critical parts, the industry is vulnerable if one goes out of business. This is challenging given the heterogeneity of the supply chain, but there are still likely to be some commonly needed components for which governments could provide support.

- **Monitor standardization efforts:** While setting standards is premature at this stage due to varying modalities and supply chains, keeping track of developments can help guide future standardization.

Search for applications

- **Invest in fault-tolerant quantum computing:** Increase funding for research into fault-tolerant quantum applications, which will be critical for practical use and to realize the potential economic benefits of quantum computing, which we expect to mostly emerge with fault tolerant computers.

- **Focus on real world use cases:** Existing investments should be directed toward solving real-world problems and supporting cross-disciplinary research to uncover valuable applications (versus only identifying algorithms for quantum computers). Related to the above point, most of these valuable applications are expected to be possible only on a fault tolerant quantum computer.

Workforce development

- **Expand educational opportunities:** Promote quantum computing education to build a skilled workforce, including existing programs and new programs such as quantum computing masters degrees, retraining programs, and technician training programs.

- **Encourage immigration and exchange programs:** Facilitate the movement of talent to meet the growing demand for experts in quantum computing and related fields.

Transition to post-quantum cryptography

- **Begin the transition now:** Conduct crypto inventories and prioritize risks based on exposure to quantum threats.
- **Follow NIST standards:** Implement the latest standards and plan for a phased migration to post-quantum cryptography.

Effective security policies

- **Address real security risks:** Work with companies on best practices to protect national security while fostering quantum technology growth.
- **Avoid conflicting policies:** Ensure new regulations do not inadvertently undermine other policy goals, such as innovation and international collaboration.

International collaboration

- **Building a fault-tolerant quantum computer and discovering its applications is so complex that any single country or private company will not be able to achieve it alone.** International collaboration on fundamental research with like-minded nations is essential to drive breakthroughs in this field. Policymakers must carefully balance promoting active collaboration with safeguarding national security and maintaining competitiveness.

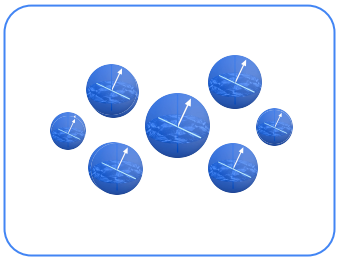
Policymakers can accelerate progress by targeting these areas, balancing immediate needs with long-term strategic goals for quantum computing.

ANNEX:
Evaluating quantum computing claims

There's a lot of hype and fear around quantum computing, making it crucial for policy leaders to critically assess claims.

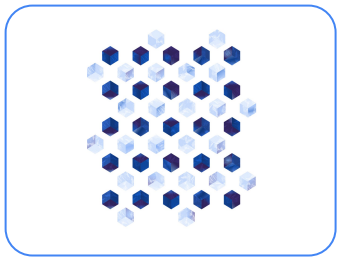
When evaluating quantum computing claims for hardware, consider the following:

- Check the **number of qubits and their quality** (coherence, gate time, gate fidelity).
- Assess how many **operations** can be performed **before the first error.**
- Determine if the system can **scale** to over a million physical qubits (or thousands of logical qubits) needed for practical applications.
- Ensure the claim has been **independently validated or peer-reviewed.**



Number of qubits

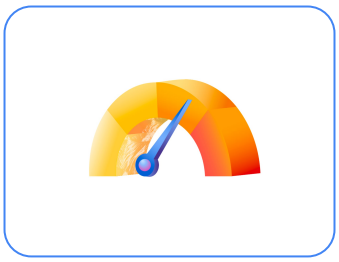
Qubit quality



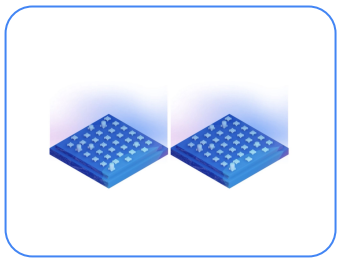
Overall error rate, and error correction

For quantum application claims:

- Evaluate if the quantum application **outperforms classical algorithms.**
- Consider whether the problem being addressed is **relevant in the real world.**
- Identify if the application is suited for current NISQ-era machines or future fault-tolerant computers.
- Look for **independent validation and peer review** to confirm the claim's reliability.



Speed
(operations per unit of time)



Scalability

Independent validation / peer review