HumanQ
Quantum Advanced Technologies

5 Quantum Computing myths you should stop believing

Table of contents

In meetings with business owners and technical leadership, the exact same scene plays out over and over. Someone mentions a news headline, someone else rolls their eyes, and within a few minutes the conversation shifts to a level that has very little to do with quantum computing. Myths about quantum computing are born right there, in the gap between an industrial announcement written for investors and a hasty read by someone who has to decide a budget.

So, we wanted to gather the five myths we hear most often: reasonable beliefs that, in certain contexts, could lead to wrong decisions, one way or the other. Some people get convinced they need to buy a machine (which they won't need), while others shelf the subject for another ten years right as their encrypted data is being copied somewhere else... well, both mistakes can prove quite costly.

What are the most common myths about quantum computing?

The five myths about quantum computing encountered most regularly concern the replacement of classical machines, the nature of quantum advantage, cryptography timelines, the need for dedicated hardware, and the right moment to take action. They are recurrent because each contains a kernel of truth, and that is precisely what makes them so enduring; debunking them does not mean downplaying the technology, given that quantum computing remains one of the few credible directions for problems that currently remain out of reach. Instead, it means understanding where the boundary actually lies between what works in a lab and what will soon enter a real business process.

Myth 1. Will the quantum computer replace the classical computer?

This is the most widespread belief and also the easiest to debunk. A quantum computer does not retire today's enterprise servers, for the simple reason that it cannot perform almost anything that those servers do all day long. Quantum cannot run an ERP system, does not draft spreadsheets, contracts, or quotes, does not archive invoices, nor is it used for database storage. On the contrary, it operates on a totally different class of mathematical problems, and consequently, it must be driven by a classical machine that prepares this data, sends it to the circuit, evaluates responses, collects results, and integrates them into the business process or research system.

The correct mental model is that of an accelerator. No one stopped using the CPU when GPUs arrived, because GPUs simply took over the specific computational workload they were best suited for. If you want to see a step-by-step comparison, it is detailed on the page about quantum vs classical computers. The practical takeaway is that no enterprise architecture will need to be rewritten from scratch; integration will look much more like adding a specialized service to enhance overall outcomes—two tools complementing each other.

Myth 2. Is a quantum computer simply faster?

The second quantum computing myth causes the most disappointment, because it leads people to expect a generalized speedup that will never arrive. A quantum processor operates on entirely different metrics; in fact, it has modest clock speeds and lengthy readout times. Thus, on ordinary tasks like running an operating system, it loses out to low-to-mid-range hardware without even a fight.

The gain does not come from the speed of an individual step; it comes from reducing the required number of steps. When a quantum algorithm can leverage superposition and entanglement to make incorrect computational paths interfere destructively with each other, the operation count drops by orders of magnitude. Outside of those specific cases, the count remains identical or gets worse—a distinction that might seem subtle on a presentation slide, but becomes decisive when selecting a use case for a pilot project.

Deep Dive: Why not all problems can be accelerated

> A measurement on a quantum register returns only a single outcome, with a probability equal to the squared magnitude of the associated amplitude. Having $2n$ amplitudes involved across n qubits is therefore not equivalent to having $2n$ readable results. A useful algorithm must build interference that concentrates amplitude on the correct solutions before measurement occurs, something that only succeeds if the problem possesses an exploitable structure—such as periodicity in the case of Shor's algorithm. For unstructured searches, Grover's algorithm stops at a quadratic speedup, from N to roughly $\sqrt{N}$ evaluations, which on real hardware is largely eroded by the overhead of quantum error correction. Hence the actual definition of quantum advantage, as discussed on the page about quantum supremacy and quantum advantage.

Myth 3. Will cryptography be broken tomorrow morning?

Here, the myth travels in two opposite and equally wrong directions. Unfortunately, on one side lies the alarmism that imagines the immediate collapse of banking systems, Bitcoin, and blockchains within a few months; on the other lies the shrug of those who consider the issue a problem for 2050. Reality is less dramatic than the former and far more urgent than the latter.

No existing machine comes close to the computational resources required to factor a 2048-bit RSA key, as it would take millions of physical qubits to sustain a few thousand stable logical qubits. Therefore, the issue lies elsewhere and does not depend on the exact date that machine arrives. The true danger is that encrypted traffic intercepted today can be stored for years and decrypted when the processing power to break the encryption becomes available—a practice known as "harvest now, decrypt later." Organizations handling medical records, multi-year contracts, or trade secrets face exposure starting right now, not twenty years from today.

NIST published its first post-quantum cryptography standards in 2024, including ML-KEM for key exchange and ML-DSA for digital signatures; guidelines are available on the NIST Post-Quantum Cryptography project. Replacing algorithms within a complex application landscape—where systems untouched for a decade coexist—requires years of structured effort. That is why the relevant question is not when the hypothetical machine will arrive, but how long organizations need to update their encryption without halting operations.

Myth 4. Do you need quantum hardware to get started?

This is the myth that stalls the most projects, and also the one debunked most willingly. The belief that doing **quantum computing** requires an in-house cryostat or an expensive cloud contract with a foreign vendor holds no weight. The hardest part of a quantum project is not executing on a physical processor, but knowing how to formulate the problem in quantum terms, prepare the data, and determine whether a real advantage exists.

All of this is performed on classical hardware. Quantum simulation and, above all, quantum emulation reproduce the behaviour of a qubit register with controlled precision. This allows you to design circuits, execute them, measure results, and benchmark them against the classical approaches already in place. **HumanQ** builds quantum emulation projects for this exact reason: it enables working today on the value-generating components without waiting for the maturity of an uncertain future hardware landscape, leveraging quantum emulation in this domain.

There is an additional advantage that often surprises technical teams. On physical machines, noise—namely decoherence and disturbances that degrade qubit states—is a spontaneous, hard-to-isolate phenomenon. In emulation, there is no physical hardware, meaning noise does not occur naturally; it is added deliberately using parameters you control. In this way, you can measure exactly how much noise tolerance your algorithm requires to stay effective—an insight that is impossible to isolate on a physical machine.

Myth 5. Is it too early for a business to care?

The answer depends on what "caring" means. If it means buying quantum hardware, then yes, for almost all companies it is too early and likely will remain so for quite a few years. However, if it means establishing the foundation to leverage quantum computing when needed, then time is already tight. Training initiatives and engineering for quantum software development have long adoption cycles and cannot be bought on demand.

Organizing process data, training internal personnel to read quantum circuits, auditing where cryptographic keys reside in production systems, and identifying the two or three optimization problems currently solved through rough approximations—these are all tasks that take months. They remain immensely valuable even if quantum hardware timelines slip by years, because they improve operational efficiency today for the future. The complete journey and its milestones are detailed on our page about quantum readiness for enterprise.

Why do quantum computing myths arise, and who feeds them?

Part of the responsibility lies with popular science communication, which relies on metaphors like Schrödinger's cat or infinite parallel processing to make superposition accessible. These analogies work fine as metaphors, but become misleading when taken literally to estimate a return on investment.

Another portion comes from market dynamics. Companies developing hardware compete for capital and attention, often presenting today's results in the best possible light, far ahead of actual maturity. Headline qubit counts are frequently communicated without the context needed to evaluate them. A press release touting a few hundred physical qubits says very little if gate fidelity and the resulting logical qubit count after error correction are omitted. Public programs like the European Quantum Flagship publish more measured roadmaps and serve as a more reliable reference than commercial announcements.

Finally, a third component is regulatory, which indirectly amplifies the hype. Ever since quantum technologies entered the scope of critical technologies—along with the state-level scrutiny mechanisms covered on the page about critical quantum technologies and Golden Power—the topic has taken on geopolitical weight that tends to inflate short-term expectations.

How do you spot an unrealistic quantum promise?

When evaluating a proposal, the first thing to check is whether a comparison with classical methods exists. If a vendor presents the output of a quantum algorithm without tangible metrics on how long a state-of-the-art classical solver would take on the same problem, the baseline required to interpret the numbers is missing. Many claimed quantum advantages have dissolved precisely this way—when classical alternatives were rewritten with greater care and scientific rigour in data collection.

The second red flag involves instance size. A demonstration performed on twenty variables reveals almost nothing about performance on a thousand variables, and bridging that gap is precisely the unsolved

challenge. The third sign is the absence of pre-conditions. Quantum algorithms rely on specific applicability assumptions regarding problem structure and input data encoding; vendor promises that omit these constraints are selling a generic illusion. This holds true for quantum machine learning as well, where the data loading bottleneck is often more computationally expensive than the core processing itself.

What can a business do today without buying hardware?

We recommend four concrete steps, none of which require physical quantum hardware. First, conduct a cryptographic inventory to identify which algorithms protect which data assets and how long that data must remain confidential; without this mapping, planning a post-quantum migration is virtually impossible.

Second, provide targeted training for a small internal team—three or four key members who can interpret quantum circuits and engage knowledgeably with vendors. Third, select candidate application areas, which in our experience almost always stem from the same problem families: highly constrained optimization, materials and chemistry simulation, or risk modelling. We have compiled an overview on our page covering quantum computing applications, featuring specialized deep dives for finance and healthcare.

Fourth, execute a Proof of Concept (POC) in emulation using a real, scoped problem. Formulate it for quantum execution and benchmark it scientifically against existing classical methods. The output will conclusively show whether an advantage exists today or may emerge in the future—an invaluable result, because reaching that determination in a few weeks of work is far better than discovering it after a massive hardware investment. To understand the underlying mechanics being emulated, step-by-step operations are explained on the page detailing how a quantum computer works.

Which questions should you ask before launching a quantum project?

The questions needed in an initial meeting are few and intentionally challenging: Which problem are you currently solving using rough approximations because exact solutions take too much compute time? What is a ten percent improvement on that problem worth in actual monetary or operational value? How many years must your data remain secure and confidential? Who within your organization can dedicate time to oversee a three-month pilot project?

Answering these four questions accomplishes the hardest part of the journey: transforming a complex technology topic into a concrete business objective with numerical metrics. From there, it becomes standard engineering work with measurable targets and clear timelines. Myths surrounding quantum computing disappear when you stop asking what will be possible someday and start measuring what can be validated within the next quarter.

Want to evaluate which of these myths are influencing your decisions?

HumanQ guides enterprises and institutions from initial exploration to measurable execution. Our core services include:

- Quantum emulation of algorithms for real-world business use cases
- Quantum readiness assessments and strategic roadmap development
- Training and educational workshops for technical teams and executive leadership
- Industrial pilot projects with empirical benchmarking against classical methods
- Custom quantum algorithm development for domain-specific problems

Related topics: qubit, quantum superposition, quantum entanglement, quantum computer, quantum vs classical, how a quantum computer works, quantum algorithms, Shor's algorithm, quantum simulation, quantum emulation, error correction, quantum supremacy and advantage, quantum machine learning, quantum applications, post-quantum cryptography, quantum computing in healthcare, quantum computing in finance, Golden Power, quantum readiness.