gesda

GESDA Solutions

GESDA Impact Story

Quantum Computing

Geneva, April 2022

Executive Summary

Few emerging technologies have generated as much excitement as quantum computers in recent years. The reason is simple: these devices promise to solve problems that are currently unsolvable.

Despite rapid advances in computing capabilities over the past half century, there are still certain calculations that even today's most powerful supercomputers can't crack in any reasonable time frame. They include things like accurately modelling the smallest molecules, simulating the most complex materials or finding prime factors or large numbers.

Finding ways to solve these problems could impact large swathes of the economy and help solve some of the grand challenges facing humanity this century. By exploiting the unusual characteristics of quantum systems, quantum computers should be able to dramatically speed up these kinds of calculations and bring solutions within reach.

This could accelerate progress in some crucial areas, making it possible to develop better drugs, cheaper fertilizers, longer lasting batteries and more efficient solar panels. It could even turbocharge progress in artificial intelligence, which would have significant knock-on effects for a host of other sectors.

Quantum computing isn't a new idea. The potential of this technology has been known since the 1980s when legendary physicist Richard Feynman highlighted its ability to simulate physics beyond classical computers. But excitement has been building in recent years because the technology finally seems to be moving from theory to practice.

In 2019, researchers at Google achieved a crucial landmark known as quantum primacy: they showed, for the first time, that their quantum computer could solve a problem that would be essentially impossible for a classical computer to solve. Since then, funding for quantum computing has skyrocketed. Private investments in 2021 hit a record high of $1.7bn, compared to $187.5m in 2019 and just $93.5 in 2015. There have also been enormous public investments in quantum technology – the US has committed $1.3bn, the EU $7.2bn and China $15bn.

This is leading to rapid progress in the field. Some of the more optimistic predictions suggest we may have quantum computers that are able to tackle practical problems by the end of this decade. If those predictions come to fruition, it could have an enormous impact on society. Many of the problems that quantum computers will excel at are directly applicable to implement the Sustainable Development Goals (SDGs) outlined by the United Nations.

But making sure that this new technology benefits all of humanity will be a major challenge. Quantum computers are hugely expensive and hard to build so ensuring broad access to them will be difficult. Those developing the technology will also be incentivized to recoup their investment, which could lead to a focus on applications with the greatest potential for profit rather than impact for society.

Quantum computers are also increasingly seen by governments as a prestige technology that has critical geopolitical and security implications. Maintaining the spirit of open collaboration that has powered progress in the field so far will be an onerous task for both scientists and policy makers.

What kind of problems can quantum computers tackle?

Quantum computers are not general-purpose computers, and for many tasks they will provide no advantage over current technology. But for certain problems they will, in theory, be able to provide enormous speed-ups over classical machines. Some of the key areas where they could provide an advantage are:

- **Simulation** – many chemical and biological processes play out at the nanoscale of matter, where quantum effects are prominent. Classical computers struggle with the complexity of simulating these interactions and so have to rely on approximations that produce imprecise results in all but the smallest systems. Quantum computers, on the other hand, are a natural fit for simulating quantum behavior like this and should be able to produce accurate results for large systems.

- **Factorization** – factorization is the process of breaking numbers down into smaller ones that, multiplied together, give you the original number. It serves as the basis of today's leading encryption schemes. This task is extremely difficult for classical computers when dealing with large numbers. But quantum computers excel at it, and will therefore be able to break most modern encryption.

- **Quantum Machine Learning** – there are hopes that quantum computers may be able to improve the predictive ability of machine learning models. They are expected to be particularly useful for learning for applications where small datasets are hard to learn with current machine learning approaches.

- **Optimization** – one of quantum computers' "superpowers" is the ability to escape from being trapped in one state of calculation, this by using a property called "quantum tunneling": this is useful for optimization problems that involve finding the best solution to a problem that has a very large number of options. Surprisingly, quantum tunneling can be efficiently emulated on classical computers and quantum optimization using these quantum-inspired optimization algorithms is available today on classical hardware.

These capabilities could impact key sectors of the economy including pharmaceuticals, materials science, chemistry, energy, finance, security, and logistics. Given the potential, companies are already learning about and exploring quantum computing.

The applications of the technology aren't just commercial though. Quantum computing promises to find solutions to some of the world's biggest challenges, which could have a transformative impact on large swathes of the world's population. In particular, quantum computers could help solve a variety of challenges at the heart of the SDGs.

SDG 2: Zero hunger

- Simulations of enzymes used by nitrogen fixing bacteria could lead to greener and cheaper sources of nitrogen-based fertilizers.
- Quantum computers could help design protein-based pesticides and herbicides that only target specific species, reducing use of toxic alternatives and making it harder for pests to develop immunity.

SDG 3: Good health and well-being

- One of the most promising applications for quantum computers is speeding up drug development by simulating new therapeutic molecules. However, it will be important to ensure that efforts are focused on the most in-need drugs rather than the most profitable.

SDG 6: Clean water and sanitation

- Quantum simulations could help develop efficient new membranes for water purification or catalysts that break down toxic contaminants.

SDG 7: Affordable and clean energy

- Future renewable energy systems are likely to be highly decentralized so quantum optimization could help to ensure they are as efficient and reliable as possible.
- Quantum simulations could help develop new materials for higher capacity batteries, more efficient solar panels and lighter wind turbine blades.
- They could even help discover room temperature superconductors, which could significantly improve the efficiency of all kinds of electronics, or develop better reactor designs that could make fusion power a reality.

SDG 13: Climate action

- Quantum-inspired optimization on classical computers could help us optimize everything from supply chains to transport networks, reducing CO2 emissions in the process.
- Quantum simulations on large-scale quantum computers could help develop greener cement production process or new catalysts for direct air capture of CO2.

The future of quantum computing isn't entirely rosy though. Access is likely to be uneven, which could lead to certain companies or countries having an unfair advantage over others. Given the transformative potential of quantum computers in critical sectors this could lead to significant disparities in economic competitiveness and development.

More concretely, the ability of quantum computers to carry out high-speed factorization could crack today's most widely-used encryption schemes. This is a problem that needs to be addressed today, because even though practical quantum computers are still a distant prospect, hackers can hoover up encrypted data now and wait until one is available to decrypt it. New quantum-resistant cryptography is also being developed.

A related issue is that quantum-vulnerable cryptography schemes are baked into many leading blockchain solutions. It will be a long time before a quantum computer is powerful and – equally important – fast enough to attack blockchains. But given the growing scale of the crypto economy, this could be destabilizing to the global financial system.

And it's important to remember that, as with any tool, quantum computers can be used for both good and evil. While the technology could be used to develop life-saving new drugs or more eco-friendly industrial chemicals, it could also be used to develop less benign materials and molecules – from new explosives to bioweapons.

What is the current state of technology?

Google's 2019 achievement of quantum primacy was a major milestone in quantum computing: scientists showed for the first time that their quantum computer could solve a problem that would be impossible for a conventional computer in any reasonable timeframe. This achievement has since been followed up with further demonstrations by Chinese researchers.

As impressive a feat as these experiments are though, the problems they solved are of little practical use. Now the goal that many are targeting is quantum advantage, which refers to the ability of quantum computers to solve real-world, practical problems much faster than classical computers. To achieve that, quantum computers will need to become a lot more powerful.

Technically, this will mean stringing together many more "qubits", the fundamental information processing units of all quantum computers. At the most basic level, all information in a classical computer is encoded as sequences of bits – 1s and 0s that represent the flicking on and off of tiny electrical switches known as 'transistors'. Qubits are the quantum equivalent of bits, but because they represent quantum systems rather than simple switches, they have unusual properties that classical bits don't. That allows them to store and process much more information simultaneously. **[See Box 1 – How do quantum computers work]**

Today, the biggest general purpose quantum computer is IBM's 127-qubit Eagle processor. But researchers expect we will need thousands, if not millions, of qubits to build practical quantum computers that can solve a wide variety of useful tasks. That's partly because you need lots of qubits to encode bigger problems into the machine, but also to deal with the fact that the fragility of quantum systems makes qubits error-prone.

To get round this quantum computers require error-correcting schemes to ensure that mistakes don't pile up too quickly and de-rail whatever computation the machine is trying to do. But to do this you need a lot more qubits to run the error-correction code – somewhere between 1,000 and 10,000 times as many.

Beyond the complexity of building such large devices, running these error-correcting schemes results in significant computational overheads that could make some quantum applications impractical. While quantum algorithms for simulation and factorization are capable of exponential speed-ups compared to classical approaches, for other problems like optimization and machine learning the speed-ups are more modest. Those benefits could be cancelled out by the overheads required to ensure fault-tolerance.

It's also not simply a matter of how many qubits you have. Other considerations include:

- **Coherence times** – how long can your qubits maintain their quantum states
- **Speed** – how quickly can you carry out operations on qubits
- **Errors** – how often do one of those operations goes wrong
- **Connectivity** – how many qubits can make direct connections with each other
- **Scalability** – how well does the system operate as the number of qubits increases
- **Data loading** – how much classical data can you load into your quantum computer for problems like machine learning and optimization.

To achieve large-scale, practical quantum computers, there needs to be improvements on all of these fronts.

Predictions for how far we are from that point vary, but general consensus is that we are probably still at least a decade away, more likely considerably longer. IBM has suggested a 1 million qubit device, which would bring us close to the scale required for fault-tolerant quantum computing, will be feasible by 2030. But this only takes into account the challenge of getting the hardware up and running. We also need a host of new software tools that make it easy to give instructions to complex and unreliable quantum computers that can vary significantly in their underlying hardware and to help translate real-world problems into quantum algorithms that they can run.

Even once all of this is solved, only a few companies and countries are even capable of building quantum computers. That means that, at least in the medium term, only a handful of these devices will exist so capacity will be limited and most users will have to access them over the cloud. Despite all these challenges though, there is evidence that we're building up some steam. So far, five manufacturers have announced plans to have fault-tolerant quantum computing hardware by 2030. And the number of software start-ups is growing faster than any other segment of the quantum computing value chain.

And we may not have to wait for massive, fault-tolerant quantum computers to start tackling practical applications. Efforts are underway to find problems that we can solve with today's smaller, more error-prone devices. One approach is to use hybrid algorithms that rely on both quantum and classical approaches to get the best of both worlds. Other possibilities included developing algorithms that are able to filter out errors, or working on problems that are naturally tolerant of them like machine learning.

There are also ways to start work on quantum solutions to problems before the hardware gets up to speed. Quantum simulators are software programs running on classical computers that mimic the behavior of quantum hardware, making it possible to develop, test and debug realistic quantum programs today.

Getting to work now on quantum applications – the use of quantum computers to solve real-world problems – will be crucial. The process will highlight roadblocks or inefficiencies in the underlying technology that limit its application to specific challenges, as well as any issues in adapting conventional processes to a quantum mindset. These findings can be fed back into the technology development and adoption process so that when quantum computers reach maturity, they can tackle the challenges we need them to.

What is needed to direct quantum computing towards implementing the SDGs?

At present the field of quantum computing is being driven by the private players developing the underlying hardware. Given the enormous cost of developing quantum computers, they are understandably focused on the most profitable areas that could provide a return on their considerable investments. Fortunately, there is some overlap between applications that are of interest to big business and those that could help implement the SDGs. But there is also a need to ensure that this technology's transformative potential is also focused on other important challenges that may not be top priorities for industry.

Purely market-driven approaches are likely to be insufficient and so new governance models will be needed that ensure the benefits of quantum computing are directed at the world's most pressing problems and that its benefits are shared by all. Now is a good time to do this because quantum computing is advanced enough for us to understand its implications, but far enough away from having major impacts that there is still time to mitigate the risks and optimize its disruptive potential. This will be aided by the use of simulators to map out potential development paths.

Quantum computing is also still highly reliant on public research funding, which means governments still have plenty of sway to direct the course of the industry and the kind of applications it targets. There are already growing calls for research agendas to be assessed in terms of public benefit. And there are examples of how this can work in frameworks that underpin research funding from the European Commission and UK Research and Innovation (UKRI) council, as well as National Science Foundation funding for nanotechnology. These initiatives were informed by research that showed it is much harder to manage the social impact of technology after it has already emerged. The goal therefore should be to anticipate innovation pathways and reshape them while there is still time.

For quantum computing to contribute towards implementing the SDGs these are the key concerns that need to address:

Inclusive R&D:

- It will be important to make sure that there is transdisciplinary collaboration between quantum computing experts and experts from other domains who understand the solutions that can help implement the SDGs.
- Ensuring diversity of views will make it easier to find solutions to R&D roadblocks, bring more legitimacy to the development process, and make it easier for more people to adopt and implement the solution.

Access:

- Facilitating access to quantum computers will be essential for ensuring that everyone has the ability to benefit from the technology and also that those closest to problems can make use of them.
- The cloud access model makes enabling access to a diverse set of users feasible but will also concentrate power in the hands of a few vendors. Efforts, like the EU's, to develop quantum hardware outside of private industry could broaden access.
- Making the technology accessible will also require significant progress on quantum software that hides the complexity of the quantum hardware and provide a simplified programming interface so the technology is still useable by people who aren't quantum experts.
- Quantum simulators could play a key role here, allowing people to start working on quantum applications even if access to real quantum hardware is limited.

Awareness:

- Many of those working on solutions to the SDGs will have little exposure to, or understanding of, quantum computing. Generating awareness of how the technology can help will be crucial.
- An informed public is more likely to increase pressure for quantum computing to be used for the common good.
- This will also be crucial for ensuring that a quantum-savvy workforce exists that is able to support increasing use of the technology.

***Measuring impact*:**

- It will be important to find ways to assess the extent to which different problems that can be solved by quantum computing contribute to implement the SDGs
- For instance, using a Quantum Computer to create expensive drugs for rare cancers is very different from using them to find cheap cures for malaria
- Finding ways to asses global *vs* local impacts or short *vs* long term impacts will also be important for influencing a responsible development path of the technology.

What challenges exist to getting the key actors to work together for the benefit of all?

So far, the development of quantum computing has been concentrated in a few rich nations and dominated by larger multinational corporations. This increases the risk that the most socially beneficial use cases will be deprioritized in favor of applications that confer commercial or geostrategic advantages. In the context of using quantum computers to implement the SDGs, this also means those developing the technology are not in touch with the realities of the countries in most need and facing the greatest societal challenges. Building real use cases requires input from these countries, which at present is limited due to lack of both awareness and access.

Much of the discourse around quantum computing at the national level is also framed as a "race", which can pose risks. The suggestion of urgency and competition could lead to less deliberation around the future impact of the technology and a failure to anticipate the governance mechanisms required to direct the technology in positive directions.

Concerns around the security implications of the technology could also see the field drift away from the open collaboration that has powered advances to date towards more siloed efforts, which could slow innovation. The US has a long history of using export controls to prevent the spread of advanced technology and already restricts the sale of several quantum technologies, in particular quantum sensors. But while effective in the short term, these approaches often backfire by inadvertently creating independent foreign technology ecosystems that are resistant to any controls over the long term. Europe's approach is more explicitly open, with the €1 billion European initiative to promote quantum technologies calling for "end-user-inspired applications". So far it is unclear what China's attitude to open quantum development will be. Most of its scientists' research is being published in top journals, but national competition with the US has already led the two countries to pursue policies designed to decouple their economies and supply chains in a broad range of areas.

The expertise, materials and enabling technologies required to build quantum computers could become a major bottleneck. Countries that control certain resources or core technologies, such as rare earth metals or the helium needed for refrigerating quantum computers, could gain significant economic and geopolitical advantage. International efforts to ensure healthy competition and cooperation could be crucial in this regard. And while many of the major early commercial developers of quantum computers have opened up access to their prototypes over the cloud, governments may need to consider policies to prevent monopolization of the technology and ensure broad participation in the industry.

All of this will need to be balanced against the danger of heavy-handed government action stifling innovation in what is still essentially a fledgling field. But working to ensure an open future for quantum technology will be crucial. Quantum computing is incredibly challenging and unless the collective intelligence of the world's best minds is leveraged, the chance will be lost to make rapid progress and achieve the transformative potential of quantum computing for all of humanity.

Box 1. How do quantum computers work?

Quantum computers exploit quantum mechanics – the laws of physics that govern the behavior of matter at the tiniest of scales. Quantum mechanics defies all our intuitions about how the physical world operates. It is a world of probabilities rather than clear cause and effect and upends our understanding of time and space. The unusual properties of quantum computers stem from three main quantum effects:

Superposition – In a classical computer bits exists as either a 0 and 1. The fundamental information processing units in a quantum computer, known as qubits, can exist as a complex combination of the two, in which each outcome has a certain probability of being true. This state, known as superposition, can be maintained until the qubit is measured, at which point it will settle on one of the two values. You can think of bits as being like a flipped coin that is either heads or tails, while a qubit in superposition is like a coin spinning on its side.

Entanglement – when two quantum systems are entangled, changing the state of one instantaneously changes the state of the other no matter the distance between them. This is what Einstein called "spooky action at a distance". Entanglement makes it possible to connect multiple qubits together so that all of their fates are intertwined. The result is a single superposition of all the possible outcomes encoded in each individual qubit. Reading one of these qubits tells you about the states of all of the others, which means a quantum computer can process information exponentially faster than a classical one.

Interference – how you link up the qubits matters though. The probabilities that govern the outcome of each qubit can interfere with those of its neighbors, amplifying or cancelling each other out. To go from all possible outcomes to the one that is the solution to your problem, you need a quantum algorithm that carefully choreographs a pattern of interference that leads to the correct solution.

There are several options for how to arrange your qubits, but the most popular model involves organizing them into circuits, much like in classical computers. These circuits are built up of a sequence of operations on smaller subsets of qubits, which together help to solve whatever problem the quantum computer has been set.

While this approach is common to most quantum computers under development today, the physical systems used to implement qubits can vary considerably. The leading modalities are:

- Superconductors – qubits encoded in electrical properties of a loop of superconducting wire
- Ion traps – qubits encoded in quantum states of an ion trapped by lasers
- Cold atoms – qubits encoded in quantum states of an atom trapped by lasers
- Silicon – qubits encoded in quantum states of electrons in a silicon chip
- Photonics – qubits encoded in quantum states of photons moving along circuits in silicon chips

Sources used to develop the explanations in this box:
> Explainer: What is a quantum computer? (MIT Technology Review)
> How does a quantum computer work? (Scientific American)
> What makes quantum computing so hard to explain? (Quanta Magazine)
> Quantum computing and quantum supremacy, explained (WIRED)
> Understanding quantum computing (Cosmos Magazine)
> Quantum computing for the qubit curious (Cosmos Magazine)
> Quantum computing in a nutshell (Qiskit)

Box 2. Who are the major quantum computing players?

Major technology companies like IBM, Google, Microsoft and Intel are still setting the pace for the industry, but the number of companies has expanded from just a handful in 2013 to 213 today.

Most players are in component manufacturing, followed by application software, but younger companies like Rigetti Computing, IonQ Universal Quantum and Xanadu are providing serious competition on the hardware front too. Honeywell's decision to spin off its quantum computing division and merge it with start-up Cambridge Quantum last year has also created a major new player in the field.

Despite the expansion in the industry, quantum hardware has a high costs barrier to entry which benefits the larger technology companies. That is likely why application software is the fastest growing segment, although most solutions are only prototypes and will need significant development to support full-scale quantum computers.

The USA still dominates the quantum computing market with 9 established companies entering the space, 59 start-ups, 18 public organizations and 63 academic groups working on the technology. But Canada and the UK have burgeoning quantum industries with 23 and 19 start-ups respectively. And China, whose quantum research is primarily government driven, has 12 public organizations actively working on quantum computing applications.

China's quantum capabilities are developing rapidly. Reports of total funding are conflicting, but some estimates put the figure as high as $15bn. The country is the world leader in terms of quantum communications technology, but is also making strides in quantum computing, most notably with the unveiling of two large quantum computers last year.

China is not the only country trying to shape the development of the quantum technology industry. As of January 2021, 17 countries have some form of national initiative or strategy to support quantum technology R&D. Most of these initiatives have a heavy focus on bringing stakeholders together with emphasis on innovation hubs to help academic researchers work in collaboration with government and industry.

Another key policy goal is to facilitate the translation of research into commercial applications through the establishment of technology testbeds, support for startups, and the creation of market opportunities for quantum applications.

Several governments, including those of China, South Korea, and Germany, have explicit goals to achieve "technological sovereignty" through local development and control of core quantum technologies. Others, including the UK, Sweden, and Japan, have announced plans to build their own quantum computer locally by 2030 or earlier.

@Geneva Science and Diplomacy Anticipator, April 2022
Document written by Edd Gent, Catherine Lefebvre and Olivier Dessibourg.