ARTHUR D LITTLE
2022

QUANTUM COMPUTING

The state of play and what it means for business

Quantum computing is among the most hyped technology topics at the moment. It can be hard for a nonspecialist to form a balanced view about when quantum computing solutions could become mature enough to disrupt their business. Looking at the status of development today, we believe that while huge technical challenges still remain, now is the time for businesses to start preparing to avoid being left behind if and when a breakthrough occurs.

AUTHORS

Albert Meige

Rick Eagar

Lucas Könnecke

With kind acknowledgment to Olivier Ezratty, consultant and author of *Understanding Quantum Technologies* (September 2021)

WHAT QUANTUM COMPUTING DOES, AND DOES NOT, PROMISE

Quantum computing is not an easy subject. An intelligent generalist can easily grapple with the idea of bits in a conventional computer, which can have a value of either 0 or 1, to perform mathematical calculations using logic gates. However, the quantum equivalent, "qubits," can be both 0 and 1 simultaneously, and the readout of their value is probabilistic rather than deterministic. The process by which qubits can be harnessed to perform calculations is nothing like that of a conventional computer, and the technical challenges to build a usable quantum computing device are immense. Without some in-depth knowledge in quantum physics and mathematics, it is pretty much impossible to really grasp "how it works."

This means that most businesspeople, however smart and technology-savvy they are, simply have to take on trust what they read about the technology. The last few years have seen a big acceleration of activity in quantum computing, with venture capital increasing 50% to over US $1 billion from 2020 to 2021, and estimates of total global investment now reaching $25 billion. Big players such as Google claim already to have achieved "quantum supremacy" (i.e., solving a particular problem with quantum computing that conventional computing could not solve in any feasible amount of time), yet this claim is not at all straightforward to validate. There are many new prototypes — with increasing numbers of qubits — promised by major players in the next decade, but there are still massive technical challenges to overcome.

First of all, a common misconception about quantum computing is that it will ultimately replace conventional computing because of its much greater processing power. This is absolutely not the case. In fact, quantum computing will only ever be superior to conventional computing for solving certain types of complex problems. These are problems involving systems with multiple elements, variables, and interactions, in which the solution complexity quickly scales up exponentially beyond the reach of conventional computing — so-called intractable problems. Quantum computers are suitable for intractable problems because they have a theoretical ability to perform exponentially increasing numbers of calculations simultaneously: a quantum processor with N qubits can theoretically perform 2^N simultaneous calculations, so each additional qubit doubles processing power. Conventional computing, even if Moore's law were to continue forever, could never achieve this. As far as we know, quantum computing is suitable for the following categories of applications:

- **Simulation.** Complex physical and molecular simulations, such as so-called in-silico simulations, which could enable digital development of new materials, chemical compounds, and drugs without the need for lab experimentation.

- **Optimization.** Optimization of complex systems, such as logistics planning, distribution operations, energy grid systems, financial systems, telecoms networks, and many others.

- **Machine learning (ML).** Artificial intelligence (AI) and ML applications require very high processing power, stretching the limits of conventional computing. The applicability is large but the "quantum advantage" for these types of applications is much less obvious in this field, particularly since ML usually involves training with a lot of data.

- **Cryptography.** A quantum algorithm has already been developed to conduct rapid integer factoring, which poses a disruptive threat to conventional cryptographic protection approaches for IT, finance, and so on. Quantum technologies will be critically important for future cryptographic solutions.

Quantum computers require very specific types of algorithms to tackle problems. So far, demonstrations of simulation and optimization quantum algorithms have fallen short of what conventional computers can achieve, largely due to hardware constraints. Data preparation and input can also be very significant in quantum computing, hence it is unlikely to be superior to conventional computing in fields such as, for example, big data management. What this means is that quantum computing will be a complement to conventional high-performance computers (HPCs) but won't replace them. Ultimately, it will be available as a cloud service, alongside other cloud services and not as a piece of kit that would be purchased by potential users.

HUGE CHALLENGES TO OVERCOME

The hype around quantum computing is such that a casual observer might conclude that it's only a matter of five to 10 years of further development before quantum computers start to become widely accessible to industry. This is possible, but on balance is still very unlikely. Without diving into the details, it's worth being aware of some of the huge technical challenges that still need to be overcome, mainly associated with hardware. There are seven different basic approaches to quantum computing currently under research and development, with differing relative degrees of maturity and activity, as shown in Figure 1.

Each approach uses a different physical phenomenon to create a qubit, based on a variety of particles from superconducting electrons through to ions, photons, and atoms. **Superconducting** qubit technology is both the most mature and the most invested in currently, with key players including IBM, Google, Amazon, and Rigetti, among many others.

Figure 1. Core qubit technologies mapped by maturity, intensity, and disruption potential
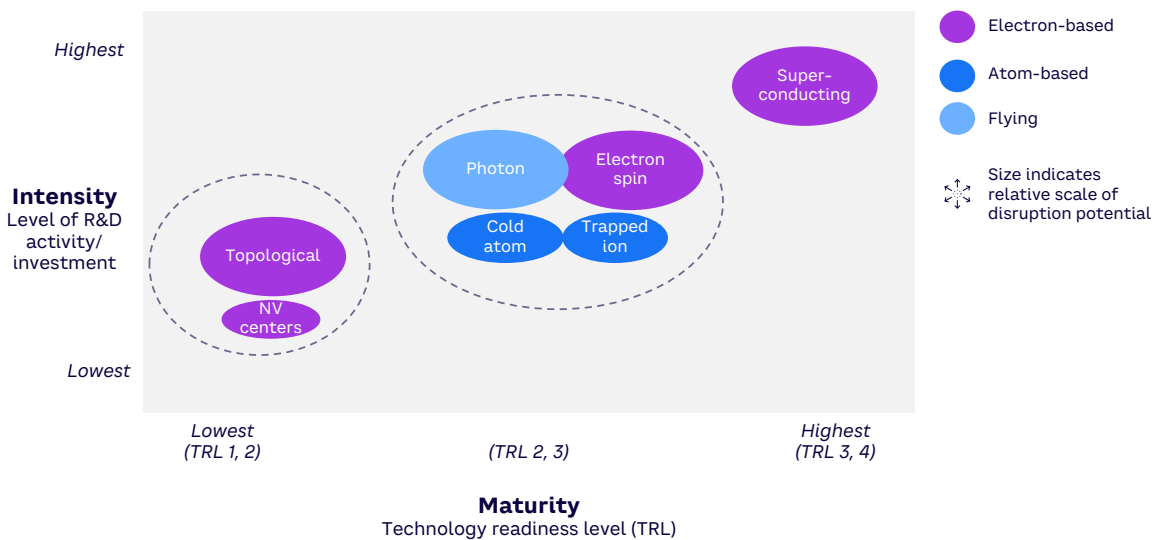
NV = nitrogen vacancy
Source: Arthur D. Little, Olivier Ezratty

At superconducting temperatures close to absolute zero, electrons behave like a single particle with an energy level that can be controlled accurately. **Electron spin** qubits are based on the spin orientation of an electron secured in a semiconductor structure. **Photons** can also be used as qubits, exploiting polarization or other physical characteristics. **Trapped ion** qubits are based on ionized atoms that are trapped in a limited space via magnets or electrodes and controlled by lasers or microwaves. **Cold atom** qubits are based on cold atoms held in position with lasers rather than electrodes. **Nitrogen vacancy (NV) centers** are based on the control of electron spins trapped in artificial defects of crystalline carbon structures. **Topological** qubits are based on using "anyon" particles and the "Majorana fermion" variant of anyons. This is the path being investigated by Microsoft.

The technical challenges for qubit computing come in a variety of forms:

- Qubits are inherently unstable and tend to "decohere," which destroys the properties of superposition and entanglement that are at the heart of their ability to provide computing power. This leads to high error rates, which require very large numbers of additional physical qubits for error correction, especially if the device is required to tackle complex algorithms. Currently this is a hugely limiting factor. The holy grail is to develop a fault-tolerant quantum computer with stable qubits, but this seems unlikely to be possible for at least a decade and possibly much longer. One reason is that implementing quantum error correction requires using qubits with much better fidelities than those available today.

- Due to the instability and the need to ensure low ambient thermal noise, very low operating temperatures (close to absolute zero) are required for most, but not all, of the technologies. Supporting infrastructure is usually complex and costly, including equipment such as cryogenic refrigeration units, superconducting cables with complex wiring, microwave generation and readout systems, low-temperature thermometers, and lasers.

- Scalability is a problem for most of the technologies for a variety of reasons. For example, error rates multiply as scale increases, and creating large numbers of qubits that are stable enough for long enough is extremely challenging.

"In the collective imagination, the quantum computer is a machine coming from science fiction, with mysterious ways of working and extraordinary powers. The illustration is composed as a triptych. In the center, individuals dehumanized by quantum supremacy which appears like a dream — or a nightmare. On either side, the quantum chandeliers remind us that this is a machine. It is not a dream but an imminent technological reality. The quantum computer is no longer just a fad fed by fantasies from popular culture. This is a promising, heavily funded research project."
Samuel Babinet, artist

Most development effort today is directed toward so-called gate-based quantum computers, which use logic gates like conventional computers, although they operate in a different way. Gate-based computers have the most general application for the full range of problem-solving. However, other types also exist, such as analog quantum annealers (such as that offered by D-Wave), which have limited specific applications, and quantum simulators, which can solve quantum physics simulation problems as well as optimization problems.

In addition, there is extensive development work ongoing on quantum communications and quantum sensing. Quantum communications can use quantum entanglement to enable safe and secure communications between quantum computers. Quantum sensing is the most mature of the quantum technologies and is already being used to enable better precision measurement of parameters such as time, distance, temperature, movement, acceleration, chemical composition, and others.

Of the hardware technologies for gate-based quantum computers mentioned above and shown in Figure 1, none so far have progressed beyond proof of concept at lab scale. The most recent device is the 127-qubit Quantum Eagle processor launched by IBM in late 2021.

On the software side, work on algorithms has preceded hardware development, starting as early as the 1990s. Today there may be 450 known algorithms currently in existence. Yet most of the speed-ups achieved are theoretical rather than practical, due to the current limitations of the hardware. For example, the noisy intermediate-scale quantum (NISQ) computers that are emerging now and will dominate the landscape for the next decade cannot run "deep" algorithms due to high error rates, hence they can only use algorithms that chain a small number of quantum gates. And their superiority to classical computing has not yet been demonstrated.

## EXTENSIVE DEVELOPMENT PLANNED IN COMING YEARS

Investment in quantum computing has been increasing significantly over the last few years and is truly global. The US remains the leading country in quantum computing development, with its mix of high public investment in basic research, huge global tech players, and the most developed startup ecosystems. However, China is aiming to catch up, with some $10 billion of investment claimed in the period to 2030, although this number is open to doubt. Europe remains a strong force in quantum computing, especially Germany, as well as the UK, France, and the Netherlands. In Asia-Pacific, besides China, Japan is a leading player, with Singapore, South Korea, Taiwan, and Australia also notably active.

As well as big tech players such as IBM, Google, Amazon, Microsoft, Quantinuum (formerly Honeywell Quantum Systems), and Intel, there are more than 450 quantum computing startups worldwide. Notable startups and specialist vendors include D-Wave, creators of one of the first commercially accessible quantum simulators, as well as Rigetti, IonQ, and QCI.

The roadmap for completion of new protypes promised by the ecosystem is extensive, with at least 20 new devices trumpeted by the respective key players between now and 2030 (see Figure 2).

As shown in Figure 2, a 1,000+ qubit machine such as the IBM Quantum Condor could be available as early as 2023. Looking further ahead, a 1 million qubit machine could be available before 2030. However, given the remaining technical challenges and uncertainties, this should best be viewed as an optimistic projection. A more conservative assumption would be that the key milestone of achieving a fault-tolerant large-scale quantum computer might occur in the range 2030-2040.

Figure 2. Quantum computing prototypes announced on vendor roadmaps
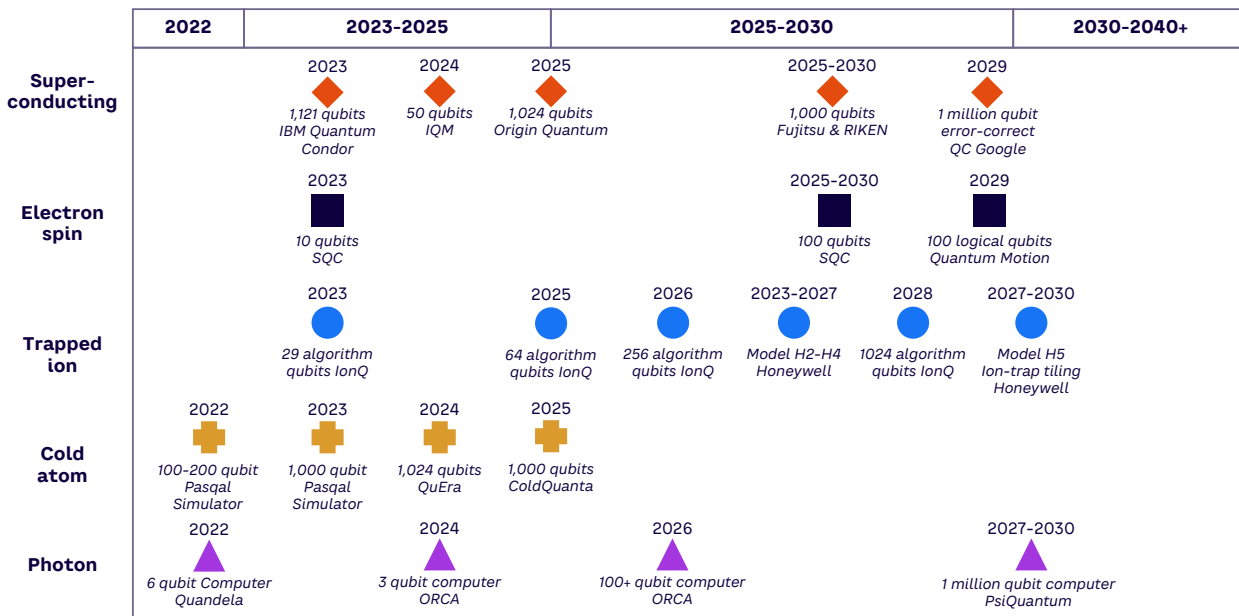
Source: Arthur D. Little, Olivier Ezratty

Currently, it might be reasonably concluded that the Superconducting technology is the most likely candidate to become commercially available for practical use in the next decade. But the technology development path at this limited level of maturity, and with this level of complexity, is rarely linear. If one of the other competing technologies achieves a breakthrough, it is possible that it could leapfrog the others. Vendors are strongly motivated to provide overly optimistic roadmaps to attract investment and build demand. It is quite possible that we may still face a "trough of disillusionment," as has happened with many other developing technologies, such as AI and autonomous vehicles.

One promising avenue in the shorter term is hybrid quantum computing, in which quantum computing is used as an accelerator for a conventional HPC to run specially designed hybrid algorithms. Although there are still challenges in design integration between the HPC and the quantum accelerator, hybrid machines promise to circumvent some of the scaling limitations of pure quantum devices for some applications.

SOME BUSINESS APPLICATIONS TO BECOME AVAILABLE SOONER

Looking ahead at applications for business and industry, predicting when these will become commercially available is very difficult. Not only will timing be affected by the technological challenges mentioned above, geopolitical and economic factors will also have a significant influence. For example, quantum computing may be viewed as key for national security, especially as it has extensive application in defense and telecommunications. It is possible that some of the global collaborations that already exist could be affected by increasing protectionism and nationalism in the current unstable geopolitical climate. These factors could act as a significant brake on commercialization. From an economic point of view, growth projections for the quantum computing market up to 2030 vary wildly from less than $5 billion to more than $60 billion, depending on which forecast you trust.

EXPERIENCE SHOWS THAT GROWTH OFTEN FOLLOWS AN EXPONENTIAL CURVE, ACCELERATING VERY RAPIDLY

At this early stage of technology maturity, it is difficult to predict the economics of quantum computers that will ultimately be produced for commercial application. The only quantum computer currently on the market is the D-Wave analog quantum annealing device that costs around $15 million. It is understood that most customers access the device via D-Wave itself or Amazon, with some paying in excess of $200,000 per year. In comparison, access to Google's cloud-based supercomputer is priced at around $32 per hour, or $176,600 for a one-year commitment (2021). In any case, it seems unlikely that quantum computers will ever be produced in large quantities and costs can reasonably be expected to be many millions of dollars. Most users will access quantum computing capacity and capability from vendors via the cloud,
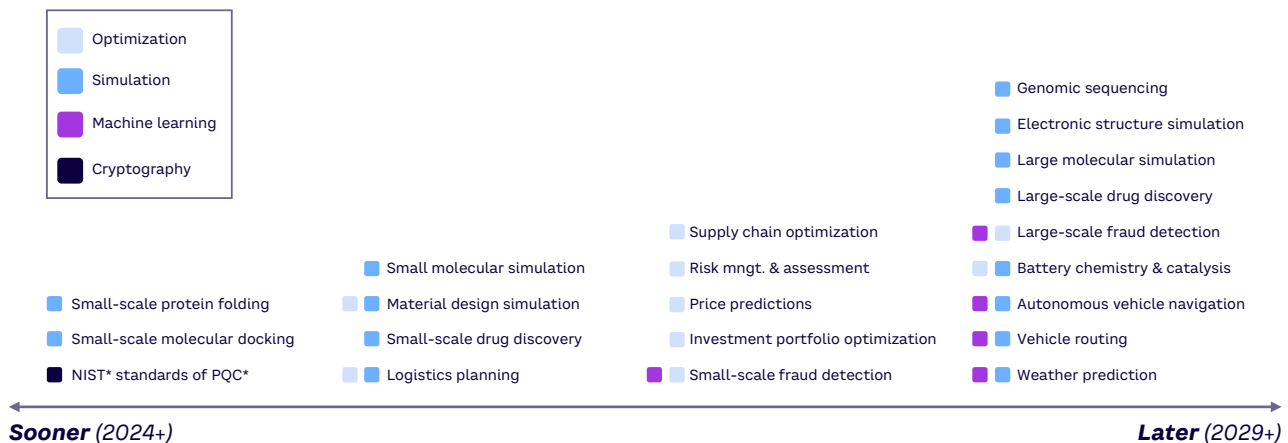
alongside conventional supercomputer access, with pricing set by the market. Indeed, quantum computing access is already being offered by IBM, Rigetti, D-Wave, Microsoft, and Amazon.

What can be expected is that applications involving simpler algorithms, such as material design or small-scale protein folding, will be available well ahead of applications such as large-scale drug discovery and molecular simulation, as shown in Figure 3.

WHAT BUSINESSES SHOULD DO NOW

What does all this mean for businesses? It is certainly possible that a breakthrough will happen in the medium term, say within five to 15 years. At this point, experience shows that growth often follows an exponential curve, accelerating very rapidly. The complex nature of quantum computing is such that companies with no knowledge or capability will struggle to catch up with those that are already up to speed and could be significantly disadvantaged. Therefore, it makes good business sense to take some action now to avoid being left behind. We recommend four steps for businesses to take (see Figure 4).

Figure 3. Illustrative relative timescales of business and industrial applications for quantum computing

Legend:
- Optimization
- Simulation
- Machine learning
- Cryptography

- Genomic sequencing
- Electronic structure simulation
- Large molecular simulation
- Large-scale drug discovery
- Large-scale fraud detection
- Battery chemistry & catalysis
- Autonomous vehicle navigation
- Vehicle routing
- Weather prediction

- Supply chain optimization
- Small molecular simulation
- Risk mngt. & assessment
- Small-scale protein folding
- Material design simulation
- Price predictions
- Small-scale molecular docking
- Small-scale drug discovery
- Investment portfolio optimization
- NIST* standards of PQC*
- Logistics planning
- Small-scale fraud detection

Sooner (2024+)   *Later* (2029+)

Source: Arthur D. Little, various

Figure 4. Four steps to avoid being left behind when quantum computing takes off
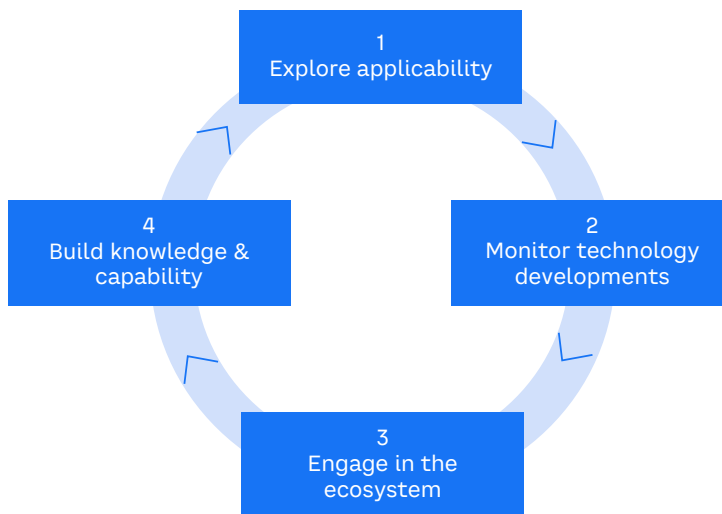
Source: Arthur D. Little

1. Explore likely applications for quantum computing in your business

Exploring where and how quantum computing could apply to your business is probably the most important thing to focus on initially. This means specifically identifying intractable problems that cannot be solved by conventional computing, and that could provide significant, disruptive advantage if they were solved. Looking at the operating model and understanding where simulation, optimization, AI/ML, and cryptography could be applicable is a good starting point. Understanding where HPCs are used today is one aspect of this, but perhaps more important is to think creatively around what-if scenarios for how your business model or your industry could be disrupted if these new intractable problems were solved. Long lists of potential opportunities can then be screened and ranked in terms of, for example, scale of business impact, maturity, and likely timescale ranges.

2. Put in place a technology-monitoring process

As with any emerging technology, if quantum computing could be key for your business, it makes sense to put in place a fit-for-purpose monitoring process. This process needs to be of a scale appropriate for your business — for many businesses, a light-touch approach may be sufficient. This means developing or acquiring the capability to understand the technology, setting up the channels to stay abreast of relevant developments, and rapidly evaluating their potential and limitations. Screening of ongoing work on quantum algorithm development targeted at your industry verticals is an important aspect of this.

3. Participate in the ecosystem

Forming partnering and collaborative relationships within the quantum computing ecosystem is a valuable way to stay in touch. Indeed, ecosystem thinking and orientation are a fundamental priority for effective innovation, not just for quantum computing. Businesses should begin by understanding the roles, activities, and level of involvement of different ecosystem players, including government, academia, research institutes, vendors, startups, and investors. Identify those players that are focusing on your sector, and establish how your business could become involved in some way — for example, through offering to participate in pilots, co-funding initiatives, secondments or temporary exchanges of staff, sponsoring of PhD projects, and so on. Testing of algorithms is already possible, and opportunities will increase over the coming years. For example, today algorithms can already be tested via the cloud with available universal quantum computers (such as those from IBM, Amazon, Microsoft, and Xanadu) or a quantum annealer (D-Wave) or an emulator (such as Atos, IBM, Microsoft, Amazon, or Google).

4. Build knowledge and capability

Most large companies are still involved in digital transformation of their businesses to a greater or lesser extent, and many have acquired certain hardware, software, and programming skills in-house that may not have existed previously. It is worth investing in education and training of at least a small number of such skilled individuals in quantum technologies, quantum programming, or even just a basic grounding to understand the language. This education is important to be able to engage effectively in the ecosystem and to monitor and evaluate developments. This is especially important for quantum technologies due to their complexity, reliance on specialist expertise, and the level of hype in published media. Creating a motivated and enthused community internally is one of the best ways to ensure that you stay abreast of developments in a natural, rather than wholly process-driven, manner. Naturally, the extent to which a business invests in education and training should be appropriate for the significance and impact of quantum computing for the business concerned.

CONCLUSION

THE KEY IS PREPARATION

BUSINESSES CANNOT AFFORD TO IGNORE THE TECHNOLOGY

It is certainly true that there is a lot of hype around quantum computing, and it is sensible to maintain a healthy degree of skepticism about the many claims and predictions that are regularly publicized. But at the same time, businesses cannot afford to ignore the technology altogether. Instead, they need to make sure that if and when quantum computing applications start to take off exponentially, they are adequately prepared to take advantage of its disruptive impact and avoid being left behind.
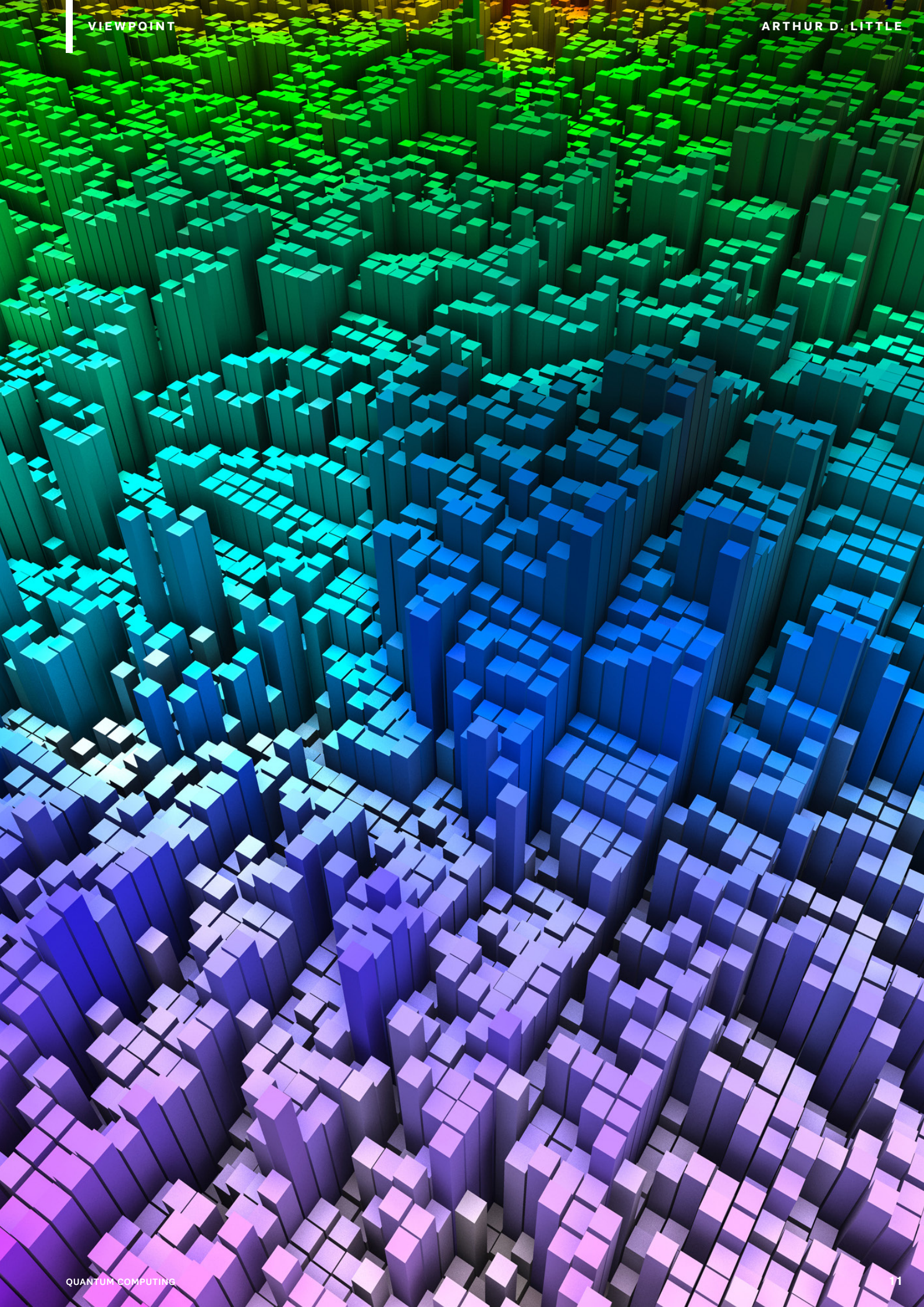
ARTHUR D LITTLE

Arthur D. Little has been at the forefront of innovation since 1886. We are an acknowledged thought leader in linking strategy, innovation and transformation in technology-intensive and converging industries. We navigate our clients through changing business ecosystems to uncover new growth opportunities. We enable our clients to build innovation capabilities and transform their organizations.

Our consultants have strong practical industry experience combined with excellent knowledge of key trends and dynamics. ADL is present in the most important business centers around the world. We are proud to serve most of the Fortune 1000 companies, in addition to other leading firms and public sector organizations.

For further information, please visit www.adlittle.com.