The Next Decade in Quantum Computing— and How to Play

Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not-for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with offices in more than 90 cities in 50 countries. For more information, please visit bcg.com.

THE NEXT DECADE IN QUANTUM COMPUTING—AND HOW TO PLAY

PHILIPP GERBERT

FRANK RUESS

CONTENTS

INTRODUCTION

THE EXPERTS ARE CONVINCED that in time they can build a high-performance quantum computer. Given the technical hurdles that quantum computing faces—manipulations at nanoscale, for instance, or operating either in a vacuum environment or at cryogenic temperatures—the progress in recent years is hard to overstate. In the long term, such machines will very likely shape new computing and business paradigms by solving computational problems that are currently out of reach. They could change the game in such fields as cryptography and chemistry (and thus material science, agriculture, and pharmaceuticals) not to mention artificial intelligence (AI) and machine learning (ML). We can expect additional applications in logistics, manufacturing, finance, and energy. Quantum computing has the potential to revolutionize information processing the way quantum science revolutionized physics a century ago.

The full impact of quantum computing is probably more than a decade away. But there is a much closer upheaval gathering force, one that has significance now for people in business and that promises big changes in the next five to ten years. Research underway at multiple major technology companies and startups, among them IBM, Google, Rigetti Computing, Alibaba, Microsoft, Intel, and Honeywell, has led to a series of technological breakthroughs in building quantum computer systems. These efforts, complemented by government-funded R&D, make it all but certain that the near to medium term will see the development of medium-sized, if still error-prone, quantum computers that can be used in business and have the power and capability to produce the first experimental discoveries. Already quite a few companies are moving to secure intellectual property (IP) rights and position themselves to be first to market with their particular parts of the quantum computing puzzle. Every company needs to understand how coming discoveries will affect business. Leaders will start to stake out their positions in this emerging technology in the next few years.

This report explores essential questions for executives and people with a thirst to be up-to-speed on quantum computing. We will look at where the technology itself currently stands, who is who in the emerging ecosystem, and the potentially interesting applications. We will analyze the leading indicators of investments, patents, and publications; which countries and entities are most active; and the status and prospects for the principal quantum hardware technologies. We will also provide a simple framework for understanding algorithms and assessing their applicability and potential. Finally, our short tour will paint a picture of what can be expected in the next five to ten years, and what companies should be doing—or getting ready for—in response.

HOW QUANTUM COMPUTERS ARE DIFFERENT, AND WHY IT MATTERS

THE FIRST CLASSICAL COMPUTERS were actually analog machines, but these proved to be too error-prone to compete with their digital cousins. Later generations used discrete digital bits, taking the values of zero and one, and some basic gates to perform logical operations. As Moore's law describes, digital computers got faster, smaller, and more powerful at an accelerating pace. Today a typical computer chip holds about 20×10^9 bits (or transistors) while the latest smartphone chip holds about 6×10^9 bits. Digital computers are known to be universal in the sense that they can in principle solve any computational problem (although they possibly require an impractically long time). Digital computers are also truly reliable at the bit level, with fewer than one error in 10^{24} operations; the far more common sources of error are software and mechanical malfunction.

Quantum computers, building on the pioneering ideas of physicists Richard Feynman and David Deutsch in the 1980s, leverage the unique properties of matter at nanoscale. They differ from classical computers in two fundamental ways. First, quantum computing is not built on bits that are either zero or one, but on qubits that can be overlays of zeros and ones (meaning part zero and part one at the same time). Second, qubits do not exist in isolation but instead become entangled and act as a group. These two properties enable qubits to achieve an exponentially higher information density than classical computers.

There is a catch, however: qubits are highly susceptible to disturbances by their environment, which makes both qubits and qubit operations (the so-called quantum gates) extremely prone to error. Correcting these errors is possible but it can require a huge overhead of auxiliary calculations, causing quantum computers to be very difficult to scale. In addition, when providing an output, quantum states lose all their richness and can only produce a restricted set of probabilistic answers. Narrowing these probabilities to the "right" answer has its own challenges, and building algorithms in a way that renders these answers useful is an entire engineering field in itself.

That said, scientists are now confident that quantum computers will not suffer the fate of analog computers—that is, being killed off by the challenges of error correction. But the requisite overhead, possibly on the order of 1,000 error-correcting qubits for each calculating qubit, does mean that the next five to ten years of development will probably take place without error correction (unless a major breakthrough on high-quality qubits surfaces). This era, when theory continues to advance and is joined by experiments based on these so-called NISQ (Noisy Intermediate-Scale Quantum) devices, is the focus of this report. (For more on the particular properties of quantum computers, see the sidebar, "The Critical Properties of Quantum Computers." For a

longer-term view of the market potential for, and development of, quantum computers, see "The Coming Quantum Leap in Computing," BCG article, May 2018. For additional context—and some fun—take the BCG Quantum Computing Test.)

THE CRITICAL PROPERTIES OF QUANTUM COMPUTERS

Here are six properties that distinguish quantum computers from their digital cousins.

Classical versus quantum bits

Configuration space of qubits

Arrows (→) are exemplary representations of a qubit state
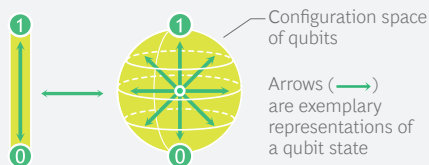
The basic constituents for quantum computing are not binary bits, with values 0 or 1, but qubits. **Qubits** take on arbitrary values between the state '0' and state '1' as described by their so-called **probability amplitude**; the latter also determines the probability of the states representing 0 or 1.

Superposition

Examples of single qubit superposition states
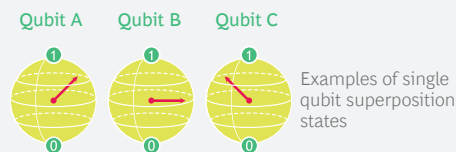
An overlay of the states '0' and '1' is called **superposition**. The images show examples of superposition with different probability amplitudes. Since amplitudes may generally be positive, negative, or even complex, qubit states are represented in a so-called '**Bloch**' sphere.

Entanglement
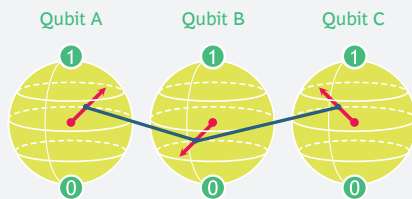
Contrary to bits, whose value we try to keep well-separated and which store their information in isolation, a collection of qubits occupies intertwined states, acting as a group. This so-called **entanglement** increases the information density by an exponential factor—the basic promise of quantum computers.
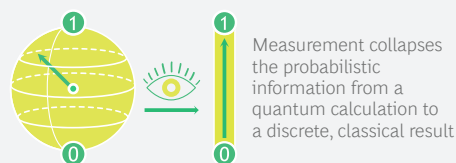
Quantum gates
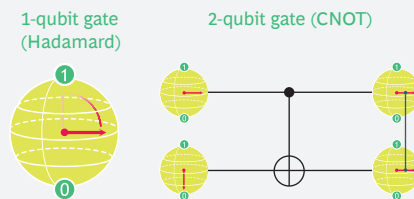
The most common so-called circuit-based quantum computers build their algorithms based on **q-gates** representing logical operations on the entangled quantum states. This is the most conventional feature. We can build any algorithm based on q-gates that act on only one or two qubits at a time.

Interference

Most gate-based algorithms exploit the fact that the probability amplitudes of quantum states can **interfere** with each other. This means that potential solutions can be amplified or weakened. Quantum algorithms have to be written in a way to amplify the correct answer toward near certainty.

Measurement

Measurement collapses the probabilistic information from a quantum calculation to a discrete, classical result

A tricky aspect of quantum computing is that the rich information of a computational state cannot be directly read. When trying to extract an answer, the information **collapses** to a discrete state with some probability, ideally the critically amplified answer we are seeking.

THE EMERGING QUANTUM COMPUTING ECOSYSTEM

Q̲UANTUM COMPUTING TECHNOLOGY IS well-enough developed, and practical uses are in sufficiently close sight, for an ecosystem of hardware and software architects and developers, contributors, investors, potential users, and collateral players to take shape. Here's a look at the principal participants.

Tech Companies

Universities and research institutions, often funded by governments, have been active in quantum computing for decades. More recently, as has occurred with other technologies (big data for example), an increasingly well-defined technology stack is emerging, throughout which a variety of private tech players have positioned themselves.

At the base of the stack is quantum hardware, where the arrays of qubits that perform the calculations are built. The next layer is sophisticated control systems, whose core role is to regulate the status of the entire apparatus and to enable the calculations. Control systems are responsible in particular for gate operations, classical and quantum computing integration, and error correction. These two layers continue to be the most technologically challenging. (We provide an overview of the status and prospects of different technologies on page 13.) Next comes a software layer to implement algorithms (and in the future, error codes) and to execute applications.

This layer includes a quantum-classical interface that compiles source code into executable programs. At the top of the stack are a wider variety of services dedicated to enabling companies to use quantum computing. In particular they help assess and translate real-life problems into a problem format that quantum computers can address.

The tech stack is increasingly well-defined, and players are positioning themselves in it.

The actual players fall into four broad categories. (See Exhibit 1.)

End-to-End Providers. These tend to be big tech companies and well-funded startups. Among the former, IBM has been the pioneer in quantum computing and continues at the forefront of the field. The company has now been joined by several other leading-edge organizations that play across the entire stack. Google and more recently Alibaba have drawn a lot of attention. Microsoft is active but has yet to unveil achievements toward actual hardware. Honeywell has just emerged as a new player, adding to the heft of the group. Rigetti is the most advanced among the startups. (See "Chad Rigetti on the Race

EXHIBIT 1 | Companies Assume Four Roles Across Layers of the Stack in the Quantum Computing Ecosystem

	End-to-end providers[1]	Hardware & systems players	Software & services players	Specialists
SERVICES	IBM	Potential expansion	Zapata Computing / Cambridge Quantum Computing / QC Ware	Tellus Matrix Group / Quantika Entanglement Partners / h-bar Quantum Consultants
APPLICATIONS LAYER	Google / Rigetti Computing		1Qbit	Quantum Benchmark / Strangeworks / Q-CTRL
SYSTEM SOFTWARE LAYER	Microsoft[2]		Riverlane / QxBranch	Qindom / ProteinQure / QbitLogic
SYSTEMS	Alibaba Group / D-Wave Systems	IonQ[4,8] / QuTech[5] / Intel		SeeQC[7]
QUANTUM COMPUTER HARDWARE	Emerging: Honeywell / Xanadu / Qilimanjaro[3]	Quantum Circuits[6] / BraneCell / TundraSystems Global		Silicon Quantum Computing[8] / PsiQ[8] / Alpine Quantum Technologies[9]

Sources: Quantum Computing Report (quantumcomputingreport.com); BCG analysis.
[1]Based on player's ambition with varying levels of maturity and service activities.
[2]Multiple technologies in the labs with focus on topological qubits.
[3]Qilimanjaro is a spinoff from the University of Barcelona.
[4]AWS is invested in IonQ.
[5]QuTech was founded by TU Delft and TNO, and has collaborations with Intel and Microsoft.
[6]Quantum Circuits (qci) is a spinoff from Yale University.
[7]SeeQC is a subsidiary of Hypres.
[8]Vision to become end-to-end provider.
[9]Alpine Quantum Technologies (AQT) is a spinoff from University of Innsbruck.

for Quantum Advantage: An Interview with the Founder and CEO of Rigetti Computing," BCG interview, November 2018.)

Each company offers its own cloud-based open-source software platform and varying levels of access to hardware, simulators, and partnerships. In 2016 IBM launched Q Experience, arguably still the most extensive platform to date, followed in 2018 by Rigetti's Forest, Google's Cirq, and Alibaba's Aliyun, which has launched a quantum cloud computing service in cooperation with the Chinese Academy of Sciences. Microsoft provides access to a quantum simulator on Azure using its Quantum Development Kit. Finally, D-Wave Systems, the first company ever to sell quantum computers (albeit for a special purpose), launched Leap, its own real-time cloud access to its quantum annealer hardware, in October 2018.

Hardware and Systems Players. Other entities are focused on developing hardware only,

since this is the core bottleneck today. Again, these include both technology giants, such as Intel, and startups, such as IonQ, Quantum Circuits, and QuTech. Quantum Circuits, a spinoff from Yale University, intends to build a robust quantum computer based on a unique, modular architecture, while QuTech—a joint effort between Delft University of Technology and TNO, the applied scientific research organization, in the Netherlands—offers a variety of partnering options for companies. An example of hardware and systems players extending into software and services, QuTech launched Quantum Inspire, the first European quantum computing platform, with supercomputing access to a quantum simulator. Quantum hardware access is planned to be available in the first half of 2019.

The ecosystem is dynamic, and the lines between tech layers are easily blurred.

Software and Services Players. Another group of companies is working on enabling applications and translating real-world problems into the quantum world. They include Zapata Computing, QC Ware, QxBranch, and Cambridge Quantum Computing, among others, which provide software and services to users. Such companies see themselves as an important interface between emerging users of quantum computing and the hardware stack. All are partners of one or more of the end-to-end or hardware players within their mini-ecosystems. They have, however, widely varying commitments and approaches to advancing original quantum algorithms.

Specialists. These are mainly startups, often spun off from research institutions, that provide focused solutions to other quantum computing players or to enterprise users. For example, Q-CTRL works on solutions to provide better system control and gate operations, and Quantum Benchmark assesses and predicts errors of hardware and specific algorithms. Both serve hardware companies and users.

The ecosystem is dynamic and the lines between layers easily blurred or crossed, in particular by maturing hardware players extending into the higher-level application, or even service layers. The end-to-end integrated companies continue to reside at the center of the technology ecosystem for now; vertical integration provides a performance advantage at the current maturity level of the industry. The biggest investments thus far have flowed into the stack's lower layers, but we have not yet seen a convergence on a single winning architecture. Several architectures may coexist over a longer period and even work hand-in-hand in a hybrid fashion to leverage the advantages of each technology.

Applications and Users

For many years, the biggest potential end users for quantum computing capability were national governments. One of the earliest algorithms to demonstrate potential quantum advantage was developed in 1994 by mathematician Peter Shor, now at the Massachusetts Institute of Technology. Shor's algorithm has famously demonstrated how a quantum computer could crack current cryptography. Such a breach could endanger communications security, possibly undermining the internet and national defense systems, among other things. Significant government funds flowed fast into quantum computing research thereafter. Widespread consensus eventually formed that algorithms such as Shor's would remain beyond the realm of quantum computers for some years to come and even if current cryptographic methods are threatened, other solutions exist and are being assessed by standard-setting institutions. This has allowed the private sector to develop and pursue other applications of quantum computing. (The covert activity of governments continues in the field, but is outside the scope of this report.)

Quite a few industries outside the tech sector have taken notice of the developments in, and the potential of, quantum computing, and companies are joining forces with tech players to explore potential uses. The most common categories of use are for simulation, optimization, machine learning, and AI. Not surprisingly, there are plenty of potential applications. (See Exhibit 2.)

Despite many announcements, though, we have yet to see an application where *quantum advantage*—that is, performance by a quantum computer that is superior in terms of time, cost, or quality—has been achieved.[1]

However, such a demonstration is deemed imminent, and Rigetti recently offered a $1 million prize to the first group that proves quantum advantage. (We provide a framework for prioritizing applications, where a sufficiently powerful quantum computer, as it becomes available, holds the promise of superior performance on page 22 in Exhibit 9.)

NOTE
1. This has occasionally been called "quantum supremacy," but the community has moved away from this term because it can be misleading. Identifying a single problem for which a quantum computer performs better does not imply a general superiority, which the term "supremacy" suggests.

EXHIBIT 2 | Multiple Potential Use Cases for Quantum Computing Exist Across Sectors

INDUSTRIES	SELECTION OF USE-CASES	ENTERPRISES (EXAMPLES)	
High-tech	• Machine learning and artificial intelligence, such as neural networks • Search • Bidding strategies for advertisements • Cybersecurity • Online and product marketing • Software verification and validation	IBM Alibaba Google Microsoft	Telstra Baidu Samsung
Industrial goods	• Logistics: scheduling, planning, product distribution, routing • Automotive: traffic simulation, e-charging station and parking search, autonomous driving • Semiconductors: manufacturing, such as chip layout optimization • Aerospace: R&D and manufacturing, such as fault-analysis, stronger polymers for airplanes • Material science: effective catalytic converters for cars, battery cell research, more-efficient materials for solar cells, and property engineering uses such as OLEDS	Airbus NASA Northrop Grumman Daimler Raytheon	BMW Volkswagen Lockheed Martin Honeywell Bosch
Chemistry and Pharma	• Catalyst and enzyme design, such as nitrogenase • Pharmaceuticals R&D, such as faster drug discovery • Bioinformatics, such as genomics • Patient diagnostics for health care, such as improved diagnostic capability for MRI	BASF Biogen Dow Chemical	JSR DuPont Amgen
Finance	• Trading strategies • Portfolio optimization • Asset pricing • Risk analysis • Fraud detection • Market simulation	J.P. Morgan Commonwealth Bank	Barclays Goldman Sachs
Energy	• Network design • Energy distribution • Oil well optimization	Dubai Electricity & Water Authority	BP

Source: BCG analysis.

INVESTMENTS, PUBLICATIONS, AND INTELLECTUAL PROPERTY

THE ACTIVITY AROUND QUANTUM computing has sparked a high degree of interest.[1] People have plenty of questions. How much money is behind quantum computing? Who is providing it? Where does the technology stand compared with AI or blockchain? What regions and entities are leading in publications and IP?

A regional public funding race is emerging, with China leading the pack.

With more than 60 separate investments totaling more than $700 million since 2012, quantum computing has come to the attention of venture investors, even if is still dwarfed by more mature and market-ready technologies such as blockchain (1,500 deals, $12 billion, not including cryptocurrencies) and AI (9,800 deals, $110 billion).

The bulk of the private quantum computing deals over the last several years took place in the US, Canada, the UK, and Australia. Among startups, D-Wave ($205 million, started before 2012), Rigetti ($119 million), PsiQ ($65 million), Silicon Quantum Computing ($60 million), Cambridge Quantum Computing ($50 million), 1Qbit ($35 million), IonQ

($22 million), and Quantum Circuits ($18 million) have led the way. (See Exhibit 3.)

A regional race is also developing, involving large publicly funded programs that are devoted to quantum technologies more broadly, including quantum communication and sensing as well as computing. China leads the pack with a $10 billion quantum program spanning the next five years, of which $3 billion is reserved for quantum computing. Europe is in the game ($1.1 billion of funding from the European Commission and European member states), as are individual countries in the region, most prominently the UK ($381 million in the UK National Quantum Technologies Programme). The US House of Representatives passed the National Quantum Initiative Act ($1.275 billion, complementing ongoing Department of Energy, Army Research Office, and National Science Foundation initiatives). Many other countries, notably Australia, Canada, and Israel are also very active.

The money has been accompanied by a flurry of patents and publishing. (See Exhibit 4.) North America and East Asia are clearly in the lead; these are also the regions with the most active commercial technology activity. Europe is a distant third, an alarming sign, especially in light of a number of leading European quantum experts joining US-based companies in recent years. Australia, a hotspot for quantum technologies for many years, is
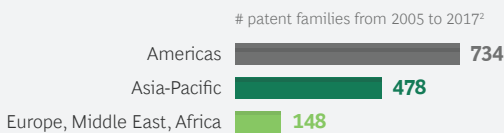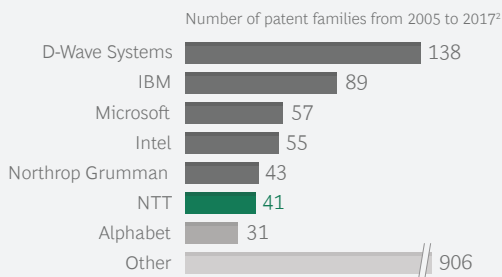
EXHIBIT 3 | Funding for Startups Has Increased in Recent Years

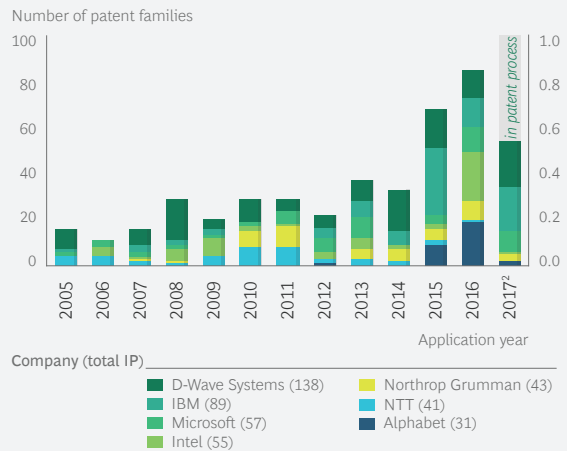| Startup	Total [US$ millions]	Most recent funding	
D-Wave Systems	205	June 1, 2018	US$10 million of grant funding in a deal led by the Canadian Government
Rigetti Computing	119	March 28, 2017	Announced further US$40 million in its series B round of funding
PsiQ	65	Undisclosed	Undisclosed
Silicon Quantum Computing	60	August 2017	AU$83 million venture funded by: New South Wales Government (AU$9 million), University of New South Wales (AU$25 million), Commonwealth Bank of Australia (AU$14 million), Telstra (AU$10 million over two years), and the Australian Government (AU$25 million over five years)
Cambridge Quantum Computing	50	August 26, 2015	US$50 million of development capital
1QBit	35	November 28, 2017	CA$45 million of development capital in Series B funding
IonQ	22	February 24, 2017	US$20 million of Series B venture funding
Quantum Circuits	18	November 13, 2017	US$18 million of Series A venture funding
Alpine Quantum Computing	12	February 8, 2018	€10 million of grant funding
QC Ware	8	July 5, 2018	US$7 million of Series A venture funding
Optalysys	8	September 21, 2017	£3 million of seed funding from undisclosed investors
Nextremer	5	August 8, 2017	JP¥500 million of venture funding
Oxford Quantum Circuits	3	September 8, 2017	£2 million of venture funding

Sources: Crunchbase; Pitchbook; BCG analysis.

EXHIBIT 4 | Quantum Computing Patents Are Increasing Quickly

US companies lead intellectual property growth[1]

Number of patent families from 2005 to 2017[2]

D-Wave Systems 138
IBM 89
Microsoft 57
Intel 55
Northrop Grumman 43
NTT 41
Alphabet 31
Other 906

patent families from 2005 to 2017[2]

Americas 734
Asia-Pacific 478
Europe, Middle East, Africa 148

Intellectual property generation jumped in recent years

Number of patent families

Application year

Company (total IP)

D-Wave Systems (138)
IBM (89)
Microsoft (57)
Intel (55)
Northrop Grumman (43)
NTT (41)
Alphabet (31)

Sources: Derwent Innovation; BCG Center for Innovation Analytics.
Note: Analysis based on approximately 250,000 patent families related to quantum technology filed since 2005; total IP=cumulative IP patent families; patent activity does not reflect companies that pursue a "trade secrets" approach to protecting their IP.
[1]Only showing the top patent owners.
[2]Patent data for 2017 is incomplete due to publication delays.

striking given its much smaller population. The country is determined to play in the quantum race; in fact, one of its leading quantum computing researchers, Michelle Simmons, was named Australian of the Year 2018.

Two things are noteworthy about the volume of scientific publishing regarding quantum computing since 2013. (See Exhibit 5.) The first is the rise of China, which has surpassed the US to become the leader in quantity of scientific articles published.[2] The second is the high degree of international collaboration (in which the US remains the primary hub). The cooperation shows that quantum computing is not dominated by national security interests yet, owing in large part to consensus around the view that cryptographic applications are still further in the future and that effective remedies for such applications are in the making. The collaboration activity also reflects the need in the scientific community for active exchange of information and ideas to overcome quantum computing's technological and engineering challenges.

NOTES
1. "The race is on to dominate quantum computing," *The Economist*, August 18, 2018.
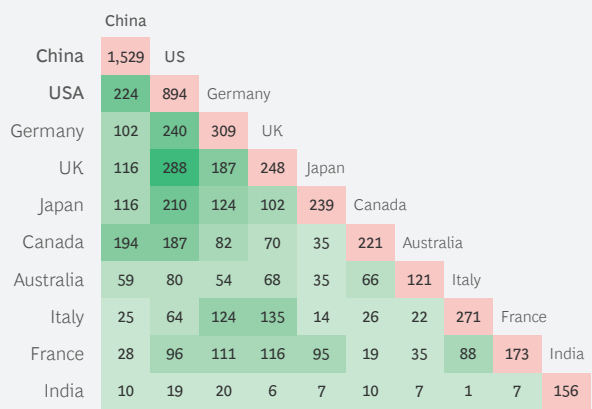2. A similar development has taken place in the field of AI.

EXHIBIT 5 | China Leads in Publications on Quantum Computing, but the US Is More Integrated Internationally

China leads by country
EMEA leads by region

US has strongest institutional collaborations[1]

Number of scientific publications since 2013

Country	Value
China	2,986
USA	2,494
Germany	1,086
UK	947
Japan	635
Canada	589
Australia	487
Italy	464
France	453
India	406
Other countries	4,011

Number of scientific publications since 2013

Region	Value
EMEA	6,013
Asia-Pacific	5,891
Americas	3,600

	China	US	Germany	UK	Japan	Canada	Australia	Italy	France	India
China	1,529									
USA	224	894								
Germany	102	240	309							
UK	116	288	187	248						
Japan	116	210	124	102	239					
Canada	194	187	82	70	35	221				
Australia	59	80	54	68	35	66	121			
Italy	25	64	124	135	14	26	22	271		
France	28	96	111	116	95	19	35	88	173	
India	10	19	20	6	7	10	7	1	7	156

Sources: Web of Science; BCG Center for Innovation Analytics.
Note: Analysis based on approximately 10,000 scientific publications related to quantum computing submitted from 2013 to mid-2018; EMEA=Europe, Middle East, Africa
[1]Where two or more universities from the same country were affiliated with the same publication, they were counted as one internal collaboration.

A BRIEF TOUR OF QUANTUM COMPUTING TECHNOLOGIES

THE TWO BIGGEST QUESTIONS facing the emerging quantum computing industry are, When will we have a large, reliable quantum computer, and What will be its architecture?

Hardware companies are pursuing a range of technologies with very different characteristics and properties. As of now, it is unclear which will ultimately form the underlying architecture for quantum computers, but the field has narrowed to a handful of potential candidates.

Criteria for Assessment

We use three sets of criteria to assess the current status of the leaders pursuing the mainstream circuit-based approaches and the challenges they still need to overcome.

Size of the Quantum System. Size refers to the number of qubits a system uses and is the most common standard for quantum technologies because it is the initial determinant for both the scale and the complexity of potential operations. The number of physical qubits currently ranges from 2 to 20 in machines that have been built and are known to be well-calibrated and performing satisfactorily. Scientists believe that computers with a few hundred physical qubits are within technological reach. (For a discussion of annealers, which have many more, albeit very short-lived qubits, see page 17.) A better

standard for size and capability in the future would be the number of fully error-corrected "logical qubits," but no one has yet developed a machine with logical qubits, so their number across all technologies is still zero (and will likely remain so for a while).

> It's unclear yet what the underlying architecture of quantum computing will be.

Complexity of Accurate Calculations. The factors that determine a computer's calculating capability include a number of factors. (See Exhibit 6.) They are:

- Qubit lifetime, currently 50 microseconds to 50 seconds

- Operation accuracy, in particular the most sensitive two-qubit gate fidelity (currently 90% to 99.9%, with 99.9% minimally required for reasonably effective scaling with error correction)

- Gate operation time, currently one nanosecond to 50 microseconds

- Connectivity, currently from the worst (one-to-one) to the best (all-to-all)—this is

EXHIBIT 6 | Assessment Criteria for Gate-Based Quantum Computers

CRITERIA	CURRENT RANGE	WHAT DOES IT MEAN?	WHY IS IT IMPORTANT?
Number of physical qubits	2–20	Number of physical quantum bits on a chip	Relevant for scaling and achievable operation complexity
Number of logical qubits	0	Number of error-corrected qubits used for fault-tolerant quantum computing	Determines scaling of sophisticated algorithms
Qubit lifetime	50 μs–50 s	Period of time information can be stored in a qubit	Determines how long qubits can store and process information
Gate fidelity	90–99.9 %	Accuracy for a two-qubit operation	Critical determinant for quality and overhead of quantum error correction
Gate operation time	1 ns–50 μs	Time for a two-qubit operation	Determines the clock speed for manipulating physical qubits
Connectivity	1:1–n:n	Connections between qubits	Determines how much information can be encoded in qubit group states
Scalability	low–high	Potential of the system to scale	Determines the ability to build a large-scale quantum computer
Maturity	TRL 1–5	Technology readiness level	Determines technological maturity on a scale from 1–9

Sources: BCG analysis; expert interviews.

important, because entanglement is a distinguishing factor of quantum computing and requires qubits to be connected to one another so they can interact

Technical Maturity and Scalability. The third set of criteria includes general technology readiness level or maturity (on a scale of 1 to 9), and, equally important, the degree of the challenges for scaling the system.

Unfortunately, the comparative performance of algorithms on different hardware technologies cannot be directly determined from these characteristics. Heuristic measures typically involve some notion of volume, such as the number of qubits times the number of gate operations that can be reliably performed until an error occurs, but the devil is in the details of such concepts.[1] The most common approach for performance assessments is a benchmarking on randomized algorithms by independent companies. End-to-end software and specialist players are offering services at different levels of sophistication both to assess the performance of

specific algorithms on the available hardware and to help with developing the best quantum algorithm based on these assessments.

Current Technologies

Exhibit 7 reflects our assessment of the most important current technologies, ordered by an outside-in view of technical maturity, providing the performance along the criteria above. Two technologies are currently in the short-term lead:

- **Superconducting Qubits** (IBM, Google, Rigetti, Alibaba, Intel, and Quantum Circuits). The basic element is a two-level energy system of a superconducting circuit which forms a somewhat noise-resistant qubit (a so-called transmon, first developed at Yale University, the alma mater of many key people in superconducting qubits R&D).

- **Ion Traps** (IonQ, Alpine Quantum Technologies, Honeywell, and others). The core elements are single ions (charged atoms)

EXHIBIT 7 | Overview of Leading Quantum Computing Technologies During the NISQ Era

	Leading technologies in NISQ era[1]		Candidate technologies beyond NISQ		
	Superconducting[2]	**Trapped ion**	**Photonic**	**Silicon-based[3]**	**Topological[8]**
Qubit type or technology					
Description of qubit encoding	Two-level system of a superconducting circuit	Electron spin direction of ionized atoms in vacuum	Occupation of a waveguide pair of single photons	Nuclear or electron spin or charge of doped P atoms in Si	Majorana particles in a nanowire
Physical qubits[4,5]	IBM: 20, Rigetti: 19, Alibaba: 11, Google: 9	Lab environment: AQT[6]: 20, IonQ: 14	6×3[9]	2	target: 1 in 2018
Qubit lifetime	**~50–100 μs**	**~50 s**	**~150 μs**	**~1–10 s**	target ~100 s
Gate fidelity[7]	**~99.4%**	**~99.9%**	**~98%**	**~90%**	target ~99.9999%
Gate operation time	**~10–50 ns**	**~3-50 μs**	**~1 ns**	**~1–10 ns**	–
Connectivity	Nearest neighbors	All-to-all	To be demonstrated	Nearest neighbor	–
Scalability	No major roadblocks near-term	Scaling beyond one trap (>50 qb)	Single photon sources and detection	Novel technology potentially high scalability	?
Maturity or technology readiness level	TRL[10] 5	TRL 4	TRL 3	TRL 3	TRL 1
Key properties	Cryogenic operation Fast gating Silicon technology	Improves with cryogenic temperatures Long qubit lifetime Vacuum operation	Room temperature Fast gating Modular design	Cryogenic operation Fast gating Atomic-scale size	Estimated: Long lifetime High fidelities

Sources: BCG analysis; expert interviews.
[1]Noisy Intermediate-Scale Quantum devices era.
[2]Currently only technology with external cloud access; several forms (charge, flux, phase) of qubits exist but most pursue a less noise-sensitive charge-based qubit (transmon).
[3]Additional approaches include Si and SiGe quantum dots.
[4]Demonstrated ability to perform single and two-qubit gates.
[5]Announcements of next-generation qubit architecture: Intel: 49, IBM: 50, Google: 72, Rigetti: 128 (all superconducting qubits), IonQ: 50 (trapped ion), Hefei University: 50 (photonic).
[6]Alpine Quantum Technologies.
[7]Two-qubit fidelity.
[8]Microsoft roadmap to build first quantum computer in 2023.
[9]18 qubits were encoded with six photons using three degrees of freedom.
[10]Technology readiness level.

trapped in magnetic fields and the energy levels of their intrinsic spin form the qubit.

Both technologies (we discuss a third, annealers, separately) have produced promising results, but most leading large tech companies seem to be betting on superconducting qubits for now. We see two reasons for this. One is that superconducting circuits are based on known complementary metal-oxide semiconductor technology, or CMOS, which is somewhat more standardized and easier to handle than ion traps or other approaches. Second, the near-term path to medium scale might be more predictable. Ion traps face a significant hurdle when they reach about 50 qubits,

generally considered the limit of a single trap. Connecting a second trap introduces new challenges and proposed solutions are still under scientific investigation.

Superconducting qubits have mastered the short-term architectural challenges by inserting the operational micropulses from the third dimension onto the planar chip and moving toward regular autocalibration of the easily disturbed qubits. In fact, their most immediate scaling challenge may seem somewhat mundane—electric cabling and control electronics. The current way of addressing a qubit with two to four cables, while also maintaining cryogenic temperatures, triggers severe engineering challenges when the number of qubits runs into the hundreds.

All leading players in the superconducting camp have made their smaller chips accessible externally to software and service companies and preferred partners. Some have opened lower-performing versions and simulators to the community at large. This sign of commercial readiness has further strengthened the general expectation that superconducting qubits could lead over other technologies over the next three to four years.

When the fog settles, a global ecosystem will form around the dominant technology.

That being said, even superconducting qubit architectures have achieved only about 20 reliable qubits so far, compared with 10^{10} bits on a chip for classical computing, so there is still some ways to go. For IBM (50 qubits) and Google (72 qubits) the next-generation hardware is expected to become publicly accessible shortly, and Rigetti (128 qubits) has also announced it will offer access to its next generation by August 2019. The roadmaps of all these players extend to about 1 million qubits. They have a strong grip on what needs to be resolved consecutively along the journey, even if they do not yet have workable solutions for them.

Other Promising Technologies

Beyond the near-term time frame, the research landscape is more open, with a few promising candidate technologies in the race, all of which are still immature. They face several science questions and quite a few challenging engineering problems, which are particular to each technology. Only when the fog settles can a global ecosystem form around the dominant technology and scale up, similar to Moore's law for digital computing.

Each approach has its attractive aspects and its challenges. Photons, for example, could have an advantage in terms of handling because they operate at room temperature and chip design can leverage known silicon technology. For instance, PsiQ, a Silicon Valley startup, wants to leapfrog the NISQ period with an ambition to develop a large-scale linear optical quantum computer, or LOQC, based on photons as qubits, with 1 million qubits as its first go-to-market product within about five years. This would be a major breakthrough if and when it becomes available. The challenges for photons lie in developing single photon sources and detectors as well as controlling multiphoton interactions, which are critical for two-qubit gates.

Another approach, silicon-based qubit technologies, has to further master nanoengineering, but research at Australia's Centre for Quantum Computation & Communication Technology has made tremendous progress. In the longer run, it could prove easier, and thus faster, to scale these atomic-size qubits and draw from global silicon manufacturing experience to realize a many-qubit architecture.

The core ambition of the final—still very early-stage—topological approach is an unprecedented low error rate of 1 part per million (and not excluding even 1 part per billion). This would constitute a game changer. The underlying physical mechanism (the exotic Majorana quasiparticle) is now largely accepted, and the first topological qubit is still expected by Microsoft to become reality in 2018. Two-qubit gates, however, are an entirely different ballgame, and even a truly ambitious roadmap would not produce a workable quantum computer for at least five years.

One could think that the number of calculation cycles (simply dividing qubit lifetime by gate operation time) is a good measure to compare different technologies. However, this could provide a somewhat skewed view: in the short term, the actual calculation cycles are capped by the infidelities of the gate operations, so their number ranges between 10 and 100 for now and the near future. Improving the fidelity of qubit operations is therefore key for being able to increase the number of gates and the usefulness of algorithms, as well as for implementing error correction schemes with reasonable qubit overhead.

The near-term focus is on what can be achieved with the current technology.

Once error correction has been implemented, calculation cycles will be a dominant measure of performance. However, there is a price on clock speed that all gate-based technologies will have to pay for fault-tolerant quantum computing. Measurement times, required in known error-correction schemes, are in the range of microseconds. Thus, an upper limit on clock speed of about one megahertz emerges for future fault-tolerant quantum computers. This in turn will be a hurdle for the execution speed-up potential of quantum algorithms.

Odd Man Out

There is an additional important player in the industry: D-Wave, the first company to ever build any kind of (still special-purpose) quantum computer. It has accumulated the largest IP portfolio in the field, which was in fact the company's original purpose. Later, D-Wave embarked on building what is called a "quantum annealer." This is different from all previously discussed technologies in that it does not execute quantum gates but is rather a special-purpose machine that is focused on solving optimization problems (by finding a minimum in a high-dimensional energy landscape). D-Wave's current hardware genera-

tion consists of 2,000 of a special type of very short-lived superconducting qubits.

D-Wave has sparked near-endless debates on whether its annealing truly performs quantum computing (it is now largely accepted that D-Wave uses quantum-mechanical properties to run algorithms) and how universal its specific type of problem solver can become. Being the only kind of quantum computer available for actual sale (assuming you have $10 million to $15 million to spare) has made D-Wave unique for several years, although the mainstream attention has now shifted away from its approach. Enabling more general operations is the biggest hurdle for quantum annealers going forward.

That being said, D-Wave's recently launched real-time cloud platform, called Leap, opens up widespread access to its quantum application environment and has the potential to be quickly embraced by the user community. The company also plans a new quantum chip by early 2020 with more than 4,000 (still short-lived) qubits and improved connectivity. Both could put D-Wave back into the game for real-time applications or inspire new classical algorithms during the NISQ period, when medium-sized gate-based quantum computers will still lack error correction.

In summary, the near-term focus in quantum computing will be on what can be achieved over the next five years by the applications based on superconducting and ion trap circuit systems with a few hundred qubits each, as well as annealing. In parallel, the technology players will keep fighting it out for the next generation of scalable quantum computers.

NOTES
1. For more detail, see IBM's definition of Quantum Volume: Nikolaj Moll et al, "Quantum optimization using variational algorithms on near-term quantum devices," arXiv, October 2017.

SIMPLIFYING THE QUANTUM ALGORITHM ZOO

THE US NATIONAL INSTITUTE for Standards and Technology (NIST) maintains a webpage entitled Quantum Algorithm Zoo that contains descriptions of more than 60 types of quantum algorithms. It's an admirable effort to catalog the current state of the art, but it will make nonexperts' heads spin, as well as those of some experts.

Quantum algorithms are the tools that tell quantum computers what to do.

Quantum algorithms are the tools that tell quantum computers what to do. Two of their attributes are especially important in the near term:

- **Speed-Up.** How much faster can a quantum computer running the algorithm solve a particular class of problem than the best-known classical computing counterpart?

- **Robustness.** How resilient is the algorithm to the random "noise," or other errors, in quantum computing?
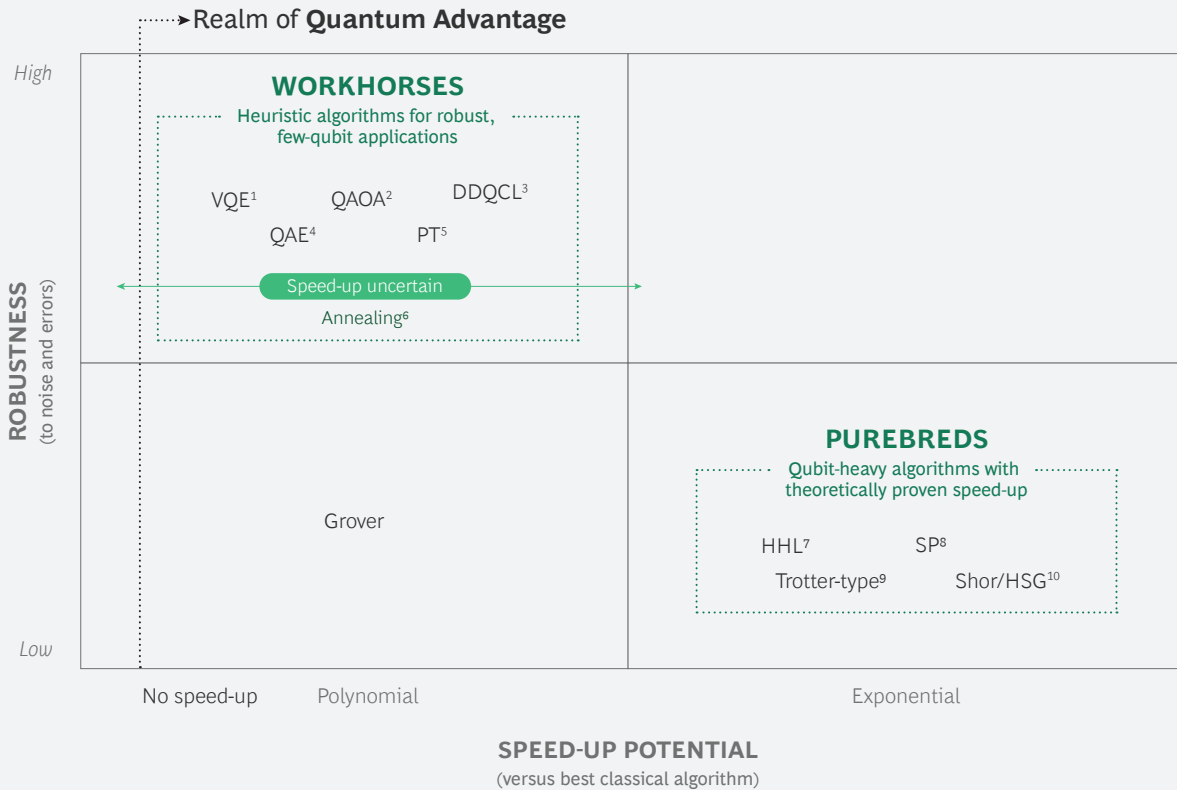
There are two classes of algorithm today. (See Exhibit 8.) We call the first purebreds—they are built for speed in noiseless or error-corrected environments. The ones shown in the exhibit have theoretically proven exponential speed-up over conventional computers for specific problems, but require a long sequence of flawless execution, which in turn necessitate very low noise operations and error correction. This class includes Peter Shor's factorization algorithm for cracking cryptography and Trotter-type algorithms used for molecular simulation. Unfortunately, their susceptibility to noise puts them out of the realm of practical application for the next ten years and perhaps longer.

The other class, which we call workhorses, are very sturdy algorithms, but they have a somewhat uncertain speed-up over classical algorithms. The members of this group, which include many more-recent algorithms, are designed to be robust in the face of noise and errors. They might have built-in error mitigation, but the most important feature is their shallow depth—that is, the number of gate operations is kept low. Most of them are then integrated with classical algorithms to enable longer, more productive loops (although these still have to be wary of accumulating errors).

The workhorses should be able to run on anticipated machines in the 100-qubit range (the annealing approaches, although somewhat different, also fall into this category). The dilemma is that very little can be proven

EXHIBIT 8 | Workhorse Algorithms Will Dominate During the NISQ Era

⋯▸Realm of **Quantum Advantage**

High

WORKHORSES
⋯ Heuristic algorithms for robust, ⋯
few-qubit applications

VQE[1]   QAOA[2]   DDQCL[3]
QAE[4]   PT[5]

Speed-up uncertain

Annealing[6]

ROBUSTNESS
(to noise and errors)

Grover

PUREBREDS
⋯ Qubit-heavy algorithms with ⋯
theoretically proven speed-up

HHL[7]   SP[8]
Trotter-type[9]   Shor/HSG[10]

Low

No speed-up   Polynomial   Exponential

SPEED-UP POTENTIAL
(versus best classical algorithm)

Sources: BCG analysis; expert interviews.
[1]Variational quantum eigensolver.
[2]Quantum approximate optimization algorithm.
[3]Data-driven quantum circuit learning for generative modeling in machine learning tasks.
[4]Quantum auto encoder, a compression algorithm for quantum data.
[5]Population transfer between computational states with similar energies for search and reverse annealing optimization.
[6]Optimization by quantum annealing as an alternative to circuit-based algorithms.
[7]Linear-system-solving algorithm devised by Harrow, Hassidim, and Lloyd.
[8]Semidefinite programming.
[9]Trotter-based algorithms for molecular simulation and adiabatic state preparation.
[10]Algorithms exploiting hidden-subgroup symmetries such as Shor's algorithm.

about their speed-up performance with respect to classical algorithms until they are put to experimental testing. Challenging any quantum advantage has become a favorite pastime of theorists and classical algorithm developers alike, with the most productive approaches actually improving upon the performance of the classical algorithms with which they are compared by creating new, quantum-inspired algorithms.

The lack of proof for speed-up might frustrate the purist, but not the practical computer scientist. Remember that deep learning, which today dominates the fast-growing field of AI, was also once a purely experimental success. Indeed, almost nothing had been proven theoretically about the performance

of deep neural networks by 2012 when they started to win every AI and ML competition. The real experiments in quantum computing of the coming years will be truly interesting.

Of less certain immediate impact are the universal and well-known Grover algorithm and its cousins. They share the noise-susceptibility with purebreds, but at a much lower, although proven, speed-up.[1] Their strong performance on some other dimensions might someday make up for these weaknesses.

Quantum computing companies are currently betting on the workhorses, which are likely to be the useful algorithms during the error-prone NISQ period of the next decade. The individual performance of any single

algorithm on a specific hardware does remain an uncertain bet, but taken as a group the gamble is reasonable. If none of the algorithms were to perform well for any of the problems under investigation would be a true surprise (and one that could point toward a new, more fundamental phenomenon that would need to be understood).

From a practical point of view, the value of the potential ease of cloud access (compared with supercomputer queues) and quantum experiments inspiring new classical approaches should not be underestimated—both are tangible and immediate benefits of this new, complementary technique.

NOTE
1. Grover-type algorithms have quadratic or more general polynomial speed-up, compared to the much more powerful exponential speed-up of the purebreds.

HOW TO PLAY THE NEXT FIVE YEARS AND BEYOND

I**T CAN BE REASONABLY** expected that over the next five years universal quantum computers with a few hundred physical qubits will become available, accompanied by quantum annealers. They will continue to be somewhat noisy, error-prone, and thus constrained to running workhorse algorithms for which experiments will be required to determine the quantum speed-up. That said, in science, the interplay of theory and experiment has always led to major advances.

But what of more practical applications? What problems might be solved? How should companies engage? What can they expect to achieve in the field and what effort is required?

Determining Timing and Engagement

Industries and potential applications can be clustered on the basis of two factors—the expected timing of quantum advantage and the value of this advantage to business. They can then be grouped into four categories of engagement: racing team members, riders, followers, and observers. (See Exhibit 9.)

Racing team members are at the forefront of immediate business benefits. Their expected time frame to quantum advantage is shortest and the potential business benefit is high. These are the industries and applications driving current investment and development.
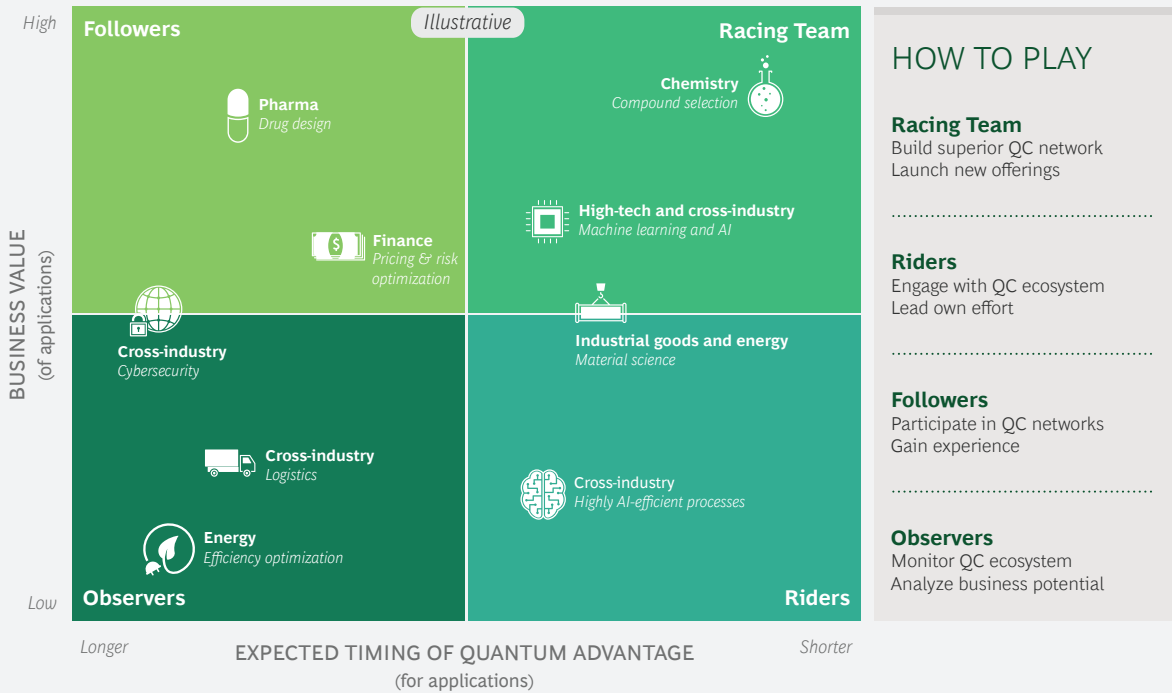
Riders will profit from similar developments, but for less critical value drivers, and are therefore less likely to fund core investments.

Followers see high potential but long development time frames to quantum advantage. For observers, both a clear path to benefits and the development time are still unclear.

Among racing team members, those with the highest tangible promise of applications are companies experimenting with quantum chemistry, followed by AI, ML, or both. They are most likely working with end-to-end providers and a few may even start to build a quantum computer for their own use and as an offering to other companies.

Quantum chemistry is particularly interesting because many important compounds, in particular the active centers of catalysts and inhibitors, can be described by a few hundred quantum states. A number of these compounds are important factors in the speed and cost of production of fertilizers, in the stability and other properties of materials, and potentially in the discovery of new drugs. For these companies and applications, quantum computing provides a highly valuable complementary lens and even outright quantum advantage could be within reach of the next generation of quantum computers. The latter can come in the form of higher precision, speed-up, or simply easier cloud access to run

EXHIBIT 9 | The Determinants of a Quantum Play for Business

High

Followers

Illustrative

Racing Team

Chemistry
Compound selection

Pharma
Drug design

High-tech and cross-industry
Machine learning and AI

BUSINESS VALUE (of applications)

Finance
Pricing & risk optimization

Industrial goods and energy
Material science

Cross-industry
Cybersecurity

Cross-industry
Logistics

Cross-industry
Highly AI-efficient processes

Energy
Efficiency optimization

Low

Observers

Riders

Longer

EXPECTED TIMING OF QUANTUM ADVANTAGE (for applications)

Shorter

HOW TO PLAY

Racing Team
Build superior QC network
Launch new offerings
....

Riders
Engage with QC ecosystem
Lead own effort
....

Followers
Participate in QC networks
Gain experience
....

Observers
Monitor QC ecosystem
Analyze business potential

Source: BCG analysis.

quantum algorithms and thus lower the cost of experimentation. New advances and discoveries could have an incredible impact in agriculture, batteries, and energy systems (all critical in fighting climate change), and on new materials across a wider range of industries, as well as in health care and other areas.

Next, speeding up AI and ML is one of the most active fields of research for quantum computing, and combined classical-quantum algorithms are arguably the most promising avenue in the short term. At the same time, AI-based learning models (assuming sufficient volumes of data) can address many of the same business needs as quantum computing, which leads to a certain level of competition between the approaches. We can expect an interesting period of co-opetition.

Overall, quantum computing can help solve simulation and optimization problems across all industries, albeit with varying business values and time frames. In many instances, quantum computers do not focus on replacing current high-performance computing methods, but rather on offering a new and complementary perspective, which in turn

may open the door to novel solutions. Risk mitigation or investment strategies in finance are two such examples. Many more areas are under active exploration, and we are bound to see some unexpected innovations.

Here's how race team members, riders, and some followers, can approach quantum computing during the NISQ era.
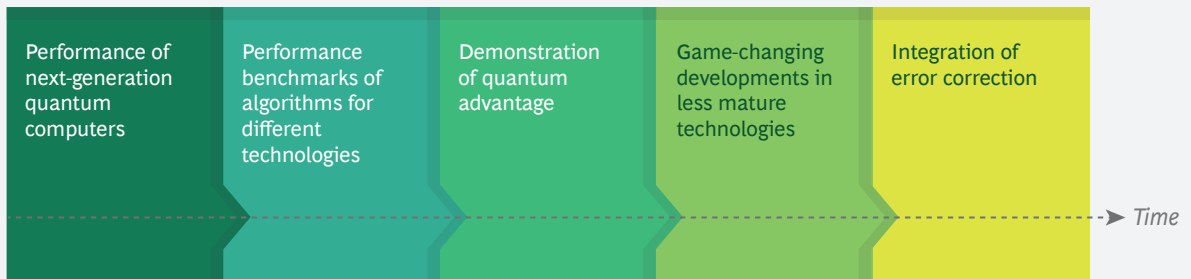
Analyze the potential. Companies need to quantify the potential of quantum computing for their businesses. (See Exhibit 10 for some key performance indicators to watch closely during the NISQ phase.) They should also monitor the progress of the ecosystem, systematically assessing where to develop or secure promising future IP that is relevant for a particular industry.

Gain experience. Companies can experiment with and assess quantum algorithms and their performance on current and upcoming quantum hardware using cloud-based access. This requires only a minimal investment in a small, possibly virtual, quantum group or lab. Building capabilities by collaborating with key software and service players can be complemented with

What to watch out for

Performance of next-generation quantum computers	Performance benchmarks of algorithms for different technologies	Demonstration of quantum advantage	Game-changing developments in less mature technologies	Integration of error correction

Time

Source: BCG analysis.

partnerships and potential investments in, or acquisitions of, small players.

Lead your own effort. Companies can build their own quantum unit with dedicated resources to lead quantum pilots in collaboration with outside providers, which guarantees direct access to hardware and the latest technology developments. Direct collaboration with an end-to-end tech player allows partners to leverage technology-specific speed-ups and take early advantage of rising technology maturity. However, at this stage companies should avoid locking in to a particular technology or approach—pioneers confirm the importance of testing the performance on several technologies.

Launch new offerings. This scenario requires an even larger investment in a cross-functional group of domain and quantum computing experts. It will likely be based on either a preferential collaboration with leading technology players to assure frontline access to top-notch hardware or, for a select few companies, building their own quantum computer. Either way, the ambition is to realize the first-mover advantage of a new discovery or application more than to demonstrate quantum advantage. Such players become active drivers of the ecosystem.

The Current State of Play

Businesses are already active at all levels of engagement. A few companies with deep pockets and a significant interest in the underlying technology—such as Northrop

Grumman and Lockheed Martin in the aerospace and defense sectors, or Honeywell, with considerable strength in optical and cryogenic components and in control systems—already own or are building their own quantum computing systems.

We are seeing a number of partnerships of various types take shape. JP Morgan, Barclays, and Samsung are working with IBM, and Volkswagen Group and Daimler with Google. Airbus, Goldman Sachs, and BMW seem to prefer to work with software and services intermediaries at this stage. Commonwealth Bank and Telstra have co-invested in Sydney's Silicon Quantum Computing startup, which is a University of New South Wales spinoff, while Intel and Microsoft have set up strong collaborations with QuTech.

A number of startups, such as OTI Lumionics, which specializes in customized OLEDs, have started integrating quantum algorithms to discover new materials, and have seen encouraging results collaborating with D-Wave, Rigetti, and others. A more common—and often complementary—approach is to partner with active hardware players or tech-agnostic software and services firms.

The level of engagement clearly depends on each company's strategy, and its specific business value potential, financial means, and risk appetite. But over time, any company using high-performance computing today will need to get involved. And as all of our economy becomes more data-driven, the circle of affected businesses expands quickly.

A POTENTIAL QUANTUM WINTER, AND THE OPPORTUNITY THEREIN

LIKE MANY THEORETICAL TECHNOLOGIES that promise ultimate practical application someday, quantum computing has already been through cycles of excitement and disappointment. The run of progress over past years is tangible, however, and has led to an increasingly high level of interest and investment activity. But the ultimate pace and roadmap are still uncertain because significant hurdles remain. While the NISQ period undoubtedly has a few surprises and breakthroughs in store, the pathway toward a fault-tolerant quantum computer may well turn out to be the key to unearthing the full potential of quantum computing applications.

Some experts thus warn of a potential "quantum winter," in which some exaggerated excitement cools and the buzz moves to other things. Even if such a chill settles in, for those with a strong vison of their future in both the medium and longer terms, it may pay to remember the banker Baron Rothschild's admonition during the panic after the Battle of Waterloo: "The time to buy is when there's blood in the streets." During periods of disillusionment, companies build the basis of true competitive advantage. Whoever stakes out the most important business beachheads in the emerging quantum computing technologies will very likely do so over the next few years. The question is not whether or when, but how, companies should get involved.

FOR FURTHER READING

BCG publishes frequently on subjects related to advanced technologies and their impact on business. For more on quantum computing, please see the following.

The Coming Quantum Leap in Computing, BCG article, May 2018

The BCG Quantum Computing Test

NOTE TO THE READER

About the Authors

Philipp Gerbert is a senior partner and the global head of digital strategy at Boston Consulting Group. He is also a Fellow studying artificial intelligence in business at BCG Henderson Institute. Philipp holds a PhD in physics from the Massachusetts Institute of Technology.

Frank Ruess is a project leader at BCG. He is an expert in quantum computing and in the industrial Internet of Things. He holds a PhD in quantum physics from the Centre for Quantum Computation and Communication Technology at the University of New South Wales in Sydney, Australia.

For Further Contact

For more information on the report, please contact one of the authors.

Philipp Gerbert
Senior Partner and Managing Director
BCG Munich
+49 89 231 740
gerbert.philipp@bcg.com
LinkedIn

Frank Ruess
Project Leader
BCG Munich
+49 89 231 740
ruess.frank@bcg.com
LinkedIn

11/18

BCG