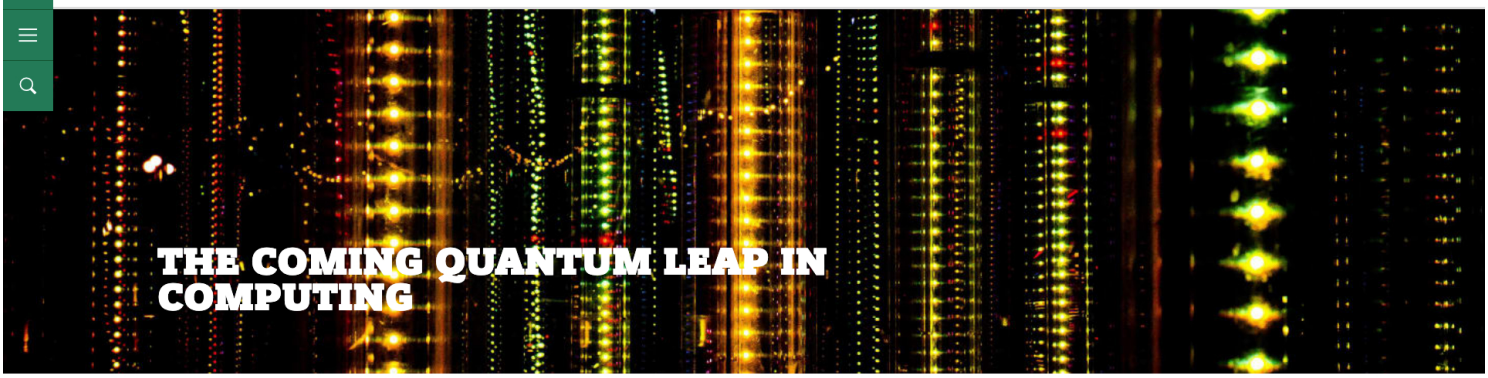


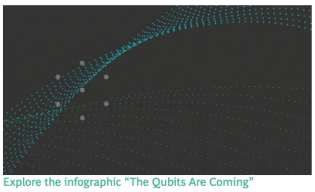
THE COMING QUANTUM LEAP IN COMPUTING

MAY 16, 2018

By Massimo Russo, Anant Thaker, and Suhare Adam

The buzz gets louder, the potential is huge, but the hurdles remain high. When will quantum computing make its mark on business? Our recent research says the answer may be sooner than many people think.

Quantum computing is not a replacement for the binary classical computing that has become a staple of modern life. But to paraphrase Nobel laureate Richard Feynman, because quantum computers use quantum physics to emulate the physical world, they can solve problems that today's computers will never have the power to tackle.



Explore the infographic "The Qubits Are Coming"

Not everybody needs this capability, but the use of quantum computers to model physical systems has immediate applications in industries such as pharmaceuticals, chemicals, and energy. Algorithms using quantum math can unlock value by vastly speeding up data-intensive applications in such fields as search, cryptography, and machine learning. In the future, hybrid systems consisting of classical computers that call on their quantum cousins for assistance will solve problems that are intractable today.

> **THE USE OF QUANTUM COMPUTERS TO MODEL PHYSICAL SYSTEMS HAS IMMEDIATE APPLICATIONS IN PHARMACEUTICALS, CHEMICALS, AND ENERGY.**

We expect quantum computing to develop toward maturity over three generations spanning the next 25 years. Companies could be using early-generation machines to address practical business and R&D needs much sooner. In fact, we see a potential addressable quantum computing market of more than $50 billion developing by 2030. Realizing the potential, however, will be possible only when the technology can produce the number of "logical" qubits—the basis for quantum calculations—that critical applications require.

There's a long way to go: a quantum simulation needs about 150 logical qubits, each of which consists of anywhere from ten to thousands of "physical" qubits, which are required for error correction and stability. As John Preskill of the California Institute of Technology pointed out earlier this year, today's quantum processors use noisy physical qubits with limited capability and a penchant for errors. They should be regarded as a stepping stone to more capable technologies; their primary near-term value is to provide a platform for the development of quantum algorithms

and applications that will be useful over the long term.[*] More comprehensive metrics to measure quantum processing's progress are also needed. One example is IBM's "quantum volume," which provides a good assessment of a quantum computer's processing capability until such systems grow to demonstrate multiple logical qubits.

Major players are on the case. IBM recently announced a 20-qubit quantum processor and a simulator that can emulate up to 49 qubits, only to be outdone by Google a few months later with its Bristlecone chip, a 72-qubit processor. Other big tech companies and research institutions, including Intel, Microsoft, MIT, Yale, and Oxford, are active in the field.

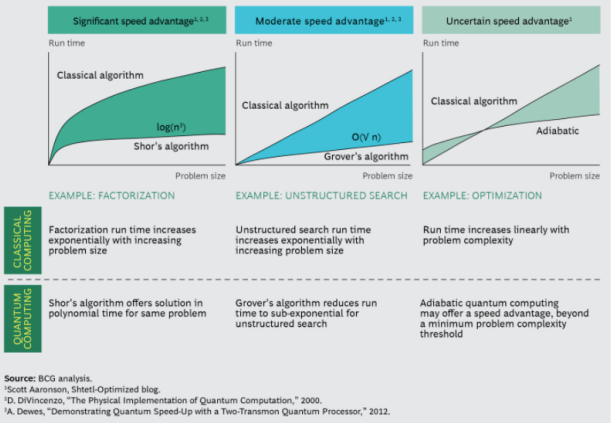
Here we offer a guide for how business executives can think about quantum computing and its applications. We explore a likely timetable for development, several high-potential early applications, the current state of the technology and potential models for adoption, and the steps companies can take now to prepare for the advent of quantum computing.

THE QUBITS ARE COMING

There are two primary prerequisites to practical business applications for quantum computing: processors with enough qubits to run quantum simulations and quantum algorithms that solve the mathematical problem underlying the application. Several such algorithms, in fields such as cryptography and machine learning, already exist. The processors are under active development, and announcements of increasingly capable processors come at an accelerating pace.

To size the market opportunity and assess the timing of quantum computing applications' availability, BCG researched various functions for which computing loads exceed classical computing capacity and for which quantum math solutions could apply. We identified three types of problems, based on the computing speeds required to solve them, that quantum computing can address with run-time speeds superior (or potentially superior) to those of classical computing. (See Exhibit 1.)

EXHIBIT 1 | Quantum Computing Offers a Big Speed Advantage for Solving Some Problems



Source: BCG analysis.
[1]Scott Aaronson, Shtetl-Optimized blog.
[2]D. DiVincenzo, "The Physical Implementation of Quantum Computation," 2000.
[3]A. Dewes, "Demonstrating Quantum Speed-Up with a Two-Transmon Quantum Processor," 2012.

Significant Speed Advantage. Because classical computers work sequentially, they are impractical for tackling very large or complex problems. For example, there is no known solution to factoring large numbers into their primes; computers simply have to guess through trial and error, and the number of tries grows exponentially with the number of digits. Quantum computers, in contrast, attack problems concurrently; in effect, they consider all possible solutions at once and discard the ones that don't work. For certain problems, the solution run time for a quantum processor grows linearly rather than exponentially with the number of dimensions, which creates an enormous speed advantage. Prime factorization of a large number is one exponential computational problem that can be solved in practical amounts of time using a quantum approach (and a specific math solution known as Shor's algorithm).

> **QUANTUM COMPUTERS CONSIDER ALL POSSIBLE SOLUTIONS TO A PROBLEM AT ONCE AND DISCARD THE ONES THAT DON'T WORK.**

One application for this significant speed advantage with substantial near-term market potential is in pharmaceutical and chemical R&D: simulating the interaction among molecules as they grow in size, since they exhibit exponential growth in solution complexity similar to prime factorization of large numbers. Consistent with Richard Feynman's vision, quantum processors can consider all possible interactions at once and arrive at a molecule's lowest energy state, which will represent how molecules interact. We estimate that quantum simulations could represent an addressable market in pharmaceuticals of up to $20 billion by 2030 with another $7 billion coming from chemicals, materials science, and other materials science–intensive industries.

Moderate Speed Advantage. The time it takes to solve problems involving unstructured search, including those critical to machine learning applications, also increases exponentially with problem size. Quantum math solutions, such as Grover's algorithm, promise a moderate speed advantage (in proportion to the square root of the problem size) for unstructured search. Today, large-scale search and machine learning problems are addressed through massive, parallel, specialized graphics processing units, or GPUs, produced by companies such as Nvidia. We expect a market of more than $20 billion in search and machine learning applications to develop as quantum computing methods displace GPU-based platforms. This potential is likely behind Google's and IBM's interest in search-optimizing quantum computing platforms.

Uncertain Speed Advantage. Classical computing approaches today adequately address problems involving complex operations or networks—for example, route optimization in transportation and logistics. Quantum computing methods could offer a speed advantage beyond a certain threshold of problem size, but the companies we talked with in our research consider current computing methods to be sufficient. It is not clear today if quantum computing could unlock significant new value in the future.

WHEN WILL THE QUBITS ARRIVE?

The technological challenge, in a nutshell, is this: solving specific problems using quantum algorithms requires sufficient scale of quantum computational power. This is represented by the number of logical qubits (which are loosely equivalent to the number of bits and memory in a traditional processor) and the much higher number of physical qubits to handle error correction (more on this below).

We are now at a point equivalent to the stage in early binary computer development when mechanical computers, vacuum tubes, and semiconductors all vied to be the physical platforms for computing machines. Today's competing quantum computing technologies include superconductor, trapped ion, and semiconductor platforms. To project the rate of market development for each, we estimated when different sizes of quantum computers would likely become available using each platform. We did this by taking into account the starting point of each technology and applying the equivalent of Moore's law (the number of physical qubits doubles roughly every 24 months), which experts in all technology platforms indicated is a reasonable assumption, given the scalability of the underlying hardware. For each quantum technology, we identified both the number of physical qubits realized to date and the required error correction capability to create a logical qubit from multiple physical qubits.

On the basis of these assumptions and the current starting points, we expect the quantum computing market to evolve over three generations. During the first, which covers 2018 to 2028, engineers will develop nonuniversal quantum computers designed for applications such as low-complexity simulations. Much of the development of these computers will take place in the next few years, and they will be in use until the second generation arrives.

The second generation (2028–2039) will be the period in which quantum computers scale up to 50 logical qubits and achieve "quantum supremacy" over classical computing—meaning that they will be able to perform certain algorithms faster in specific applications. This second generation of quantum computing will focus on such problems as molecular simulation, R&D, and software development. During this period, usable applications will come to market, creating significant value. At the same time,

quantum information processing will develop further as a field, and companies will become more familiar with quantum simulation methods.

In the third generation (2031–2042), quantum computers will achieve the scale to perform advanced simulations for commercial use in simulation, search, and optimization with significant advantages over classical methods. Because of the scaling of Moore's law, and the thresholds at which quantum computing overtakes binary computing in certain applications, there is considerable overlap between the second and third generations. As a general trajectory, we expect a decade of steady progress in quantum computing followed by a significant acceleration after about 2030.

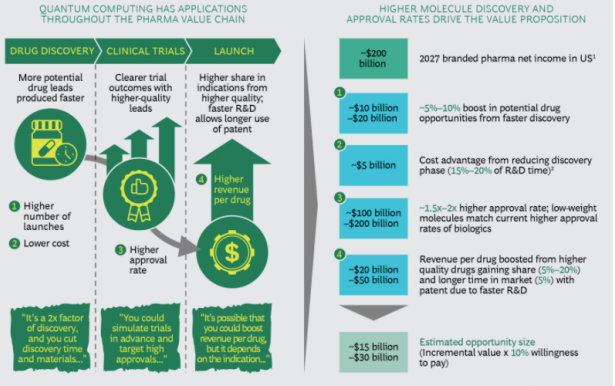
SOME APPLICATIONS MAY BE CLOSER THAN YOU THINK

While the biggest potential for quantum computing is more than a decade away, business leaders should monitor the first generation of development—particularly the next few years. During this time, we expect companies in industries such as chemicals to experiment with limited quantum computing applications in the modeling of relatively simple molecules and in specialized optimizations. These companies will familiarize themselves with quantum computing methods and tools through hands-on use. IBM and Microsoft are both developing quantum computing communities, quantum computing simulators, and easy-to-use tools that expose developers to quantum processing techniques. As quantum algorithms, programming languages, and quantum-processors-as-a-cloud services become available, developers will gradually incorporate them in software solutions. Hybrid computing systems combining classical and quantum approaches will emerge. This period of learning will be critical to increasing awareness and experience so that once quantum supremacy is achieved in certain fields, adoption can proceed quickly.

> **THE BIGGEST POTENTIAL IS MORE THAN A DECADE AWAY, BUT BUSINESS LEADERS SHOULD MONITOR DEVELOPMENTS OVER THE NEXT FEW YEARS.**

As noted above, one class of problems in which quantum computers have a significant speed advantage is the modeling of large molecules to understand specific interactions and chemical processes. The idea is to use quantum processors to create a quantum (as opposed to a digital) twin, or simulation, and model the quantum processes involved at the subatomic level. Pharmaceutical and chemical companies are already experimenting with the potential of quantum simulation to accelerate drug discovery and design molecules with fewer unintended side effects. Executives in these industries estimate that identifying new targets in this way could increase the rate of drug discovery by 5% to 10% and accelerate development times by 15% to 20%. They also believe that better molecule design could increase drug approval rates by a factor of 1.5 to 2. (See Exhibit 2.) As the vice president of R&D at a major pharma company put it, "At the atomic level, current high-performance computing can't handle most simulations. Quantum can exponentially increase drug discovery."

EXHIBIT 2 | Complex Molecule Discovery in Pharma R&D Could Be a $15 Billion to $30 Billion Market Opportunity



Sources: Statistica reports; Wired; Lawrence Livermore National Laboratory; Motherboard; Fierce Biotech; expert interviews; BCG analysis.
¹Assumes 7% CAGR in line with historical trends, 30% net margin, and 75% of total pharma market branded. ²Reduces ~25% of drug discovery, itself 15% to 20% of R&D, which represents ~17% of revenue.

In the US pharmaceutical sector alone, if quantum simulations of complex atomic processes were available today, and 10% of companies were willing to pay for the capability, quantum computing would represent a $15 billion to $30 billion addressable market opportunity. Currently, the market for all high-performance computing globally is $10 billion.

There are other practical applications. Quantum computing can be applied to accelerate search and machine learning algorithms used with exponentially growing datasets. This will become increasingly important to unlocking the value of data, as the tens of billions of devices in the Internet of Things, for example, drive the volume of available data into the stratosphere.

For some classes of problems, the search for a solution requires trial and error and the simultaneous testing of potential solutions. Imagine an archipelago of thousands of islands connected by bridges and the need to find a path that crosses each island only once. The number of possible solutions rises exponentially with the number of islands, but checking that a given path satisfies the constraint of sole island visits is straightforward. If our hypothetical island puzzle had 1 million possible solutions, a binary computer would require an average of 500,000 tries to find the right one. A quantum processor running Grover's algorithm would solve the problem in only 1,000 attempts—500 times faster.

WHERE A BINARY COMPUTER WOULD NEED 500,000 TRIES TO FIND THE RIGHT SOLUTION, A QUANTUM PROCESSOR WOULD NEED ONLY 1,000.

This is equivalent to the type of problem faced by search algorithms and the large, multilayer neural networks that underlie machine learning. For neural networks to handle such tasks as object detection and identification—determining whether the object that suddenly appears in front of an autonomous car is a wind-blown plastic bag or a baby carriage, for example—they need to be trained on large data sets and a large number of outcomes through trial and error and supervised learning. While machine learning and artificial intelligence have become a reality through the combination of large data sets and parallel, low-cost GPUs, quantum computers can accelerate the training of neural networks and increase the amount of data they can handle. This application is an active field of research as scientists and engineers try to identify quantum algorithms that can be harnessed for machine learning. As more algorithms are discovered, the fundamental advantages of quantum over classical computers could lead to the displacement of the $20 billion market for high-performance machine-learning computing by 2030.

THE TECHNOLOGY TODAY...

Quantum computing's power comes from the fact that it is a fundamentally distinct technology from the binary, Boolean logic–based computing we are all used to. There are three essential differences. The first has to do with the bits. Binary computers use binary bits: everything is based on 1s and 0s or, as some like to think about it, on or off. Picture a light switch, which has only two positions. Qubits, on the other hand, can inhabit states of 1 and 0, or on and off, at the same time. The light switch is instead a dimmer with a theoretically infinite number of settings. Qubits are about probabilities rather than black-or-white certainties, and this is simultaneously a big enabler and a substantial problem (more on this below).

The second difference is that binary computers keep all those 1s and 0s separate; they have to in order to run their calculations. Quantum computing works on the purposeful entanglement of qubits; by manipulating one, you simultaneously manipulate all of its entangled mates. Adjusting one light dimmer affects all the others in the room—and all the others in the house. This is what gives quantum computing its calculating prowess.

The third difference lies in the way that quantum computers do their work. While binary computers conduct massive numbers of arithmetic calculations sequentially, a quantum computer calculates all possible outcomes concurrently and settles on a potentially correct answer through constructive interference; it "cancels out" all the wrong answers. In the example of the bridges

connecting the islands, a quantum computer would simultaneously consider all potential routes and settle on one that is probabilistically "correct."

From a practical engineering standpoint, quantum computers have real constraints. Quantum circuits work best at very low temperatures—near absolute zero. Quantum states are highly unstable; any outside influence increases the chance of error, which is why they need to be super-cooled and isolated. Qubit stability, or coherence, and error correction are major issues—indeed, as machines get big enough to do useful simulations, the ratio of physical qubits (required for control and correction) to the qubits doing the actual work can be as high as three thousand to one. For these reasons, quantum computers require significant surrounding infrastructure and resemble old-style mainframes in large, climate-controlled data centers (just a lot colder!) much more than they do today's laptops or smartphones.

...AND TOMORROW

Today's quantum computers are in the very early stages of invention, not unlike classical computing in the early 1950s, when William Shockley of Bell Labs invented the silicon-based solid-state transistor that replaced the vacuum tubes powering the earliest computers and set the tech industry off on the pursuit of ever-more minute and powerful processors that continues to this day.

FOR TWO QUANTUM TECHNOLOGIES, TRAPPED ION AND SUPERCONDUCTOR, COMMERCIAL APPLICATIONS ARE IN SIGHT.

Several quantum technologies are racing to reach useful qubit thresholds. Two have made sufficient progress for commercial application to be in sight: trapped ion and superconductor. Trapped ion is widely viewed to produce the highest-quality qubits (those having the lowest inherent error rate) and therefore currently has an advantage over superconductor, both in time to market for key applications and capital cost. At the end of 2017, researchers working on trapped-ion machines successfully entangled 14 qubits to perform a designated operation with a logical success rate of 99.9%. The comparable numbers for superconductor are 9 qubits and 99.4%. If each technology followed a development scenario (without improvement to error correction) according to Moore's law, trapped ion would reach the threshold of 150 logical qubits necessary for major quantum simulation applications first, but not until around 2040.

That said, the need for error correction is the biggest driver of resource requirements and has an outsized impact on scale and cost. Significant reduction in error correction could accelerate trapped ion toward key thresholds in scale and cost reduction much sooner, perhaps as early as 2028 to 2030. Microsoft is pursuing a quantum computing technology with a potential one-to-one ratio of physical to logical qubits, but no working prototype has yet been produced. In the short term, we believe trapped ion is well positioned to be first to market, but it still has many of the risks inherent in early-stage technologies.

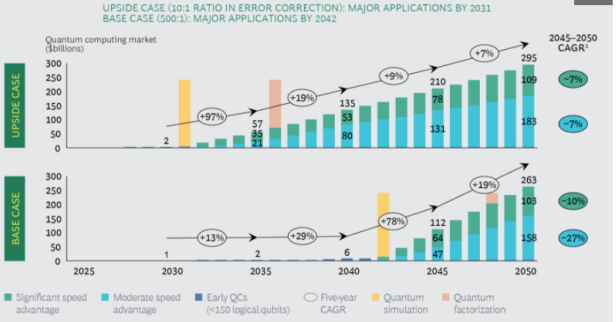
Once technical feasibility is established, we expect to see S-curve adoption patterns, similar to those of other advanced technologies. Adoption for each application will depend on the degree of the advantage conferred by quantum processing and the maturity of the algorithms directing the problem solving. More specifically, given that quantum computing can operate in the mode of platform-as-a-service, applications in which there is a significant speed advantage could see rapid adoption, on the order of 70% penetration within five years, similar to the adoption rate of GPUs in machine learning applications. Applications that offer a moderate speed advantage could take up to 15 years to reach 50% penetration (the development of software as a service is a useful analogy), while applications with unknown algorithms and potential will almost surely follow slower adoption curves, with quantum computing augmenting binary processing in 25% or fewer cases even after 15 years.

Overall, we project a substantial market for quantum computing, but the timing could vary widely depending on when the critical technical milestones are reached that unlock actual business-

applicable computing capacity. In a "base-case" scenario (assuming a Moore's law speed of qubit development with no improvement on error correction), the market for quantum applications would reach about $2 billion in 2035, then soar to more than $260 billion by 2050 as adoption picks up. An "upside" case, in which there is significant reduction in the need for error correction, would see a substantial market develop much sooner: about $60 billion in 2035, growing to $295 billion by 2050 (compared with an $800 billion global commercial and consumer computing market today). (See "The Quantum Stack and Its Business Models" and Exhibit 3.)

THE QUANTUM STACK AND ITS BUSINESS MODELS +

EXHIBIT 3 | The Speed of Market Growth Depends on Technical Milestones



Source: BCG analysis.
Note: Assumes machine learning grows at current projected rate of ~18% CAGR until 2037 and then levels off at 2% CAGR per year until reaching a steady-state growth rate of ~7% applied to majority of other applications. Because of rounding, numbers may not add up to the totals shown.
²CAGR based on 2045–2050 to compensate for downward bias of higher initial adoption rates of solutions that offer significant and moderate speed advantages.

HOW SHOULD COMPANIES PREPARE FOR A QUANTUM LEAP?

Quantum computing won't be for everybody. But if your company is in a data-intensive field or an industry in which the ability to run simulations of complex real-world functions and interactions in a practical amount of time advances R&D, you'll want to start engaging with this advanced technology. Already, BASF, VW, Airbus, and other companies are investing in building quantum computing capabilities. A good first step is to launch an initiative to build an understanding of quantum algorithms and gain experience using quantum computing platforms and tools provided by IBM, Microsoft, and others. Emerging software development and consulting companies such as QxBranch, QC Ware, and 1Qbit are working in multiple industries to develop quantum applications. Companies may also want to consider sponsoring academic research in quantum applications. IBM, for example, is working with MIT on an initiative on AI and quantum computing.

Pharmaceutical companies and others dependent on materials science innovation should begin to explore molecule simulation using quantum processors. (IBM has accurately modeled the largest molecule to date, Beryllium hydride, or BeH2, using a scalable method on a quantum computer.) They should also challenge their R&D organizations to follow quantum computing breakthroughs, especially as they accelerate. Companies leveraging search, neural networks, and optimization algorithms should encourage their data scientists to learn quantum algorithms and approaches and to study how quantum processors could significantly accelerate their capabilities. As with other advanced technologies, such as AI and machine learning, the companies that position themselves to take advantage of quantum computing early will establish a significant advantage.

> **PHARMA COMPANIES SHOULD BEGIN TO EXPLORE MOLECULE SIMULATION USING QUANTUM PROCESSORS.**

One note of caution: quantum computing has potentially significant implications for cryptography and encryption. Because current encryption methods often rely on the prime factorization of large numbers, quantum computing's ability to factor these numbers within practical time frames is a potential (if long-term) threat to keeping messages secure. While the number of logical qubits required (more than 1,000) suggests that quantum encryption-cracking computers will not be practical before about 2040, companies should watch emerging quantum-proof

encryption methods and be ready to shift away from a dependence on prime factorization methods, especially for critical applications. Already countries such as China and the US are investing heavily in quantum research for secure communication, with China launching the first satellite dedicated to implementing a quantum communication channel.

Quantum computing is moving quickly from research labs to real-world applications. It has the potential to unlock significant value for companies in the next decade. Executives need to start watching now for key milestones indicating that quantum computers are approaching supremacy, and companies that want to capitalize need to start building internal capabilities to take full advantage of the strange but awesome computing powers quantum processors can provide.

BCG **HENDERSON INSTITUTE**

The BCG Henderson Institute is Boston Consulting Group's strategy think tank, dedicated to exploring and developing valuable new insights from business, technology, and science by embracing the powerful technology of ideas. The Institute engages leaders in provocative discussion and experimentation to expand the boundaries of business theory and practice and to translate innovative ideas from within and beyond business. For more ideas and inspiration from the Institute, please visit Featured Insights.

AUTHORS

MASSIMO RUSSO
Managing Director & Senior Partner
Boston

ANANT THAKER
Principal
Boston

SUHARE ADAM
Consultant
Boston