Unlocking Quantum Computing Early On

TCS Incubation
Abstract

Quantum Computing (QC) is an advanced computing paradigm that promises to deliver the power required to solve complex problems that are either intractable or cannot be practically handled by even the most powerful supercomputers of today. QC is believed to have the potential to enable better solutions and create new opportunities that could result in tremendous business value across verticals.

Unfortunately, this promised power of QC would also make it easy for malicious elements to break current cryptographic schemes, resulting in new threats. It is therefore important for businesses to not only look at opportunities, but to also ensure readiness against any new threats that may arise as a result of QC.

Here, we present, our point of view on QC, and its potential impact and evolution. We also share our perspectives on what businesses could do to keep up with the pace of developments in this area and be prepared for a quantum future.

An introduction to Quantum Computing

QC derives its theoretical foundations from quantum mechanics, which is based on fundamental properties of atomic and sub-atomic particles. While classical computers represent information using binary bits that can assume values of either 0 or 1, QC represents information using qubits that can assume an infinite number of values resulting from combinations of 0 and 1.

The immense power of QC emerges from three fundamental properties of qubits, viz. superposition, entanglement, and interference (while it is not the objective of this paper to get into technical details, the inset text attempts to explain these three properties at a very high-level).

Superposition, Entanglement, and Interference

Superposition: While in principle, qubits can assume an infinite number of values between 0 and 1, when measured, they either give a value of 0 or 1. This phenomenon is represented using the “basis state” of a qubit, which can either be $|0\rangle$ and $|1\rangle$. Superposition is the phenomenon of qubits existing in a linear combination of the states $|0\rangle$ and $|1\rangle$, unlike classical bits which can only be either 0 or 1 at a time. More specifically, the state of a qubit can be written as $a|0\rangle+b|1\rangle$, where a and b are complex numbers. Upon measurement, the qubit “collapses” to the state $|0\rangle$ with a probability of $|a|^2$, or to the state $|1\rangle$ with a probability of $|b|^2$. The process of collapse to $|0\rangle$ or $|1\rangle$ is truly stochastic—a property which finds use in the generation of truly random number through QC.
Due to physical limitations on the number of transistors that can be packed on a microchip, there are limits to scaling the performance of chips that power classical computers. QC promises a way to break through these limitations and provide the power needed to solve complex problems that current supercomputers struggle to handle. These problems, generally referred to as intractable or NP complete (nondeterministic polynomial), occur in a wide variety of use cases such as vehicle routing, portfolio optimization, and molecular simulation.

What lies beneath

At a high level, the QC hardware of today can be grouped under two classes:

**Quantum annealers**, which aim to solve a specific class of problems by trying to find the global minimum of an objective function. Optimization is a class of problems where quantum annealers are more effective in the present scenario. While annealers are easier to build and scale, they are not suitable for solving all types of problems.

**Universal quantum computers**, which are general purpose and aimed at solving complex computational problems of any type. These are more complex to build but offer a universal model of computation. At present universal quantum computers are limited by their number of qubits. However, as the technology evolves, such universal quantum computers will be able to solve a wide range of problems, solutions to which would be almost inconceivable on classical computers.

A variety of quantum properties and phenomena are leveraged to physically realize qubits and quantum processors, in the following ways:

**Physical Implementation**

- Superconducting
- Trapped Ions
- Photonics
- Superconducting annealing
- Quantum Dots
- Topological

**Entanglement**: Without getting into the how and why of entanglement, for the sake of our understanding, when two qubits are entangled, if one obtains a state of one of the qubits, the state of the other qubit can be predicted with certainty, without having to measure it at all, regardless of the distance between them. Similarly, any change made to the state of one of the entangled qubits has a ripple effect on the state of the other. This strong non-classical correlation extends to multiple qubits. Consequently entanglement, has huge implications in quantum technologies, including computing, communication, and sensing. In QC, every quantum algorithm which shows “exponential speed up” compared to classical algorithms, must exploit entanglement. A follow-up point of it is that the phenomenon of entanglement cannot be simulated classically at a large scale.

**Interference**: This refers to the wave functions either reinforcing or diminishing each other. Leveraging the capability of interference, the probability of obtaining certain states is amplified at the cost of others, such that the amplified states occur with higher probabilities and correspond to the sought-after solutions to the problem being solved.
Even though superconducting implementations are the most common and seem to be the frontrunners, some of the other technologies such as trapped ions are gaining traction too. Each technology has its strengths and limitations in terms of their gate times, coherence times, cooling required, and versatility. While it is difficult to predict how the technologies will evolve, it is likely that the future will see at least a few of them coexisting, with specific technologies proving to be better for specific applications and contexts. Libraries and software development kits (SDKs) are likely to become available across technology implementations, which to a great extent, could make the underlying technology irrelevant to quantum software developers.

Where are we today?

Current quantum computers are severely constrained by their limited number of qubits, and are sensitive to environmental elements such as temperature, inter-qubit interdependence, and other ‘noise’ which make them prone to errors and decoherence. It is therefore accepted that we are today in what is known as the Noisy Intermediate Scale Quantum (NISQ) era. Noisy—because we do not have enough qubits to spare for error correction, and intermediate scale—because of the relatively small number of qubits. While these devices are not mature enough in terms of capacity or error-handling, they are still good enough to demonstrate the promise of QC.

NISQ era computers are evolving in capacity as well as in their resilience to errors. These continuous improvements will eventually result in the next frontier of Fault Tolerant QC (FTQC). Quantum fault tolerance refers to avoiding the uncontrolled cascade of errors caused by interaction of qubits. The goal is to achieve, through redundancy, a useful quantum computer given imperfect devices underneath. This redundancy is not cheap. Operating on and correcting the already encoded quantum data will require many more ‘physical qubits’.

The transition from NISQ to FTQC will be a continuous process with QC being able to provide practically implementable solutions to an increasingly wider set of problems. Till general purpose FTQCs become available, NISQ provides great value in advancing QC adoption by businesses. The key is to choose the right problem, scope it right, and solve it on contemporary hardware. Considering the high costs of quantum hardware, the practical approach is to first experiment with algorithms on simulators, which simulate quantum behavior on classical machines, and move them to quantum hardware after verification and validation.

Having mentioned the limited capabilities of current NISQ hardware, it is important to acknowledge that it is highly unlikely that quantum computers will ever fully replace classical computers. Instead, quantum computers will extend the capabilities of classical computers by working on problems, or parts of problems, that are hard or intractable for current classical computers. Typical business solutions will have large parts running on classical hardware with small chunks being executed on quantum processors.

The four classes of QC problems

Machine learning (ML), optimization, simulation, and security are seen to be the four broad areas that would be impacted most by the power promised by QC.

Quantum ML

Quantum ML explores the interplay of QC and machine learning. While end-to-end ML use cases on universal quantum machines may still be a few years away, a quantum enhanced ML pipeline
involving a combination of classical and quantum steps, is a clearly feasible option that can be explored with today's NISQ computers. Models built on quantum computers are expected to be more powerful for certain applications due to a combination of faster processing and requirement of lesser data for training.

**Optimization**

Optimization usually involves finding the best possible solution from a pool of options based on given conditions or constraints. These are generally formulated as minimization (or maximization) problems where one tries to minimize (or maximize) the ‘cost’ (or ‘gains’) as defined for the use case under consideration. Many optimization problems are computationally complex and become intractable as the number of parameters and constraints increase. QC opens up new possibilities for solving such problems with considerable speedup and/or better solutions as compared to classical solvers.

**Quantum security**

QC presents both opportunities and risks to the cybersecurity environment. While technologies such as Quantum Key Distribution and Quantum Random Number Generation will lead to more secure communication and systems, the power of quantum technologies also introduces new threats to current implementations. Most cryptographic algorithms today are computationally hard, thus making them difficult to be broken in practice in a reasonable amount of time by adversaries using classical computers. However, it has been theoretically established that certain current cryptographic algorithms can be broken by a sufficiently powerful quantum computer in a matter of minutes, thus posing a major threat to current cryptography.

While it will take a few years for quantum computers to be able to break current cryptographic codes, it will also take approximately a similar amount of time to develop defenses against such threats. There is also a very real threat of people with malicious intents storing classically encrypted data today for decoding in future, when the quantum landscape is amenable. The magnitude of threat and the persistence of encrypted information has spurred efforts to develop quantum resistant algorithms. The goal should be to get ‘quantum-safe’ as soon as possible.

**Simulation and modeling**

The efficacy of quantum computers in predicting the behavior, properties, evolution, and configuration of chemical and biological elements such as molecules and proteins, has been established. This is expected to have huge implications for, say, pharmaceutical organizations where drug development life cycles may get significantly enhanced, or the energy sector where calorific values and reaction rates of compounds could be estimated to explore greener fuel alternatives.

The quantum phenomenon of superposition also allows multiple possible scenarios of a situation to be modeled and explored simultaneously. This finds immense applications in finance, which typically depend on Markov Chain Monte-Carlo-like methods to sample and explore possible pathways.

**Quantum use cases: An industry view**

While financial services, pharma, and manufacturing sectors seem to be among the early adopters, QC can be used across verticals:
The Quantum Ecosystem

The QC ecosystem comprises capabilities offered by providers, at various technology layers (hardware, systems software, cloud, tools, accelerators, solutions, and more).

We believe that a strong ecosystem of technology vendors, startups, and academic partners is crucial for agility and success in the QC space. It is therefore important to ensure regular reviews of the ecosystem to identify the right partners, in order for the best set of participants and capabilities coming together to provide an ideal solution in every situation.

Quantum Value Discovery

QC has been witnessing a steady increase in investments, startups, venture capitalist (VC) funding and patent filings. Not only are industries, along with technology partners, investing in exploring QC and building scaled down proofs of concepts (PoC) with the technology available, they are also forming consortia with academia and government bodies.

Such trends strongly indicate that QC is fast evolving and on its way toward a mainstream route.

The quantum computers of today are still limited by their capacity, coherence, and ability to handle noise. However, the rate at which the technology is evolving, makes us believe that now is the right time for businesses to start investing in experimenting with QC to understand potential opportunities for and threats to their businesses.

Depicted below is our recommendation of how organizations could get started with their journey of quantum value discovery.

<table>
<thead>
<tr>
<th>Industry vertical</th>
<th>Typical use cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking, Financial Services, and Insurance</td>
<td>Portfolio optimization, options/derivatives pricing, algorithmic trading, fraud detection, insurance and reinsurance risk, loans and credit scoring</td>
</tr>
<tr>
<td>Energy and Resources</td>
<td>Energy supply planning, operations scheduling, facility location planning, utilization forecasting, workforce scheduling, battery materials and design, windfarm design, alternative fuels, asset inspection</td>
</tr>
<tr>
<td>Life Sciences</td>
<td>Molecular simulation, chemical reaction simulation, protein folding, drug discovery, gene sequencing and annotation, organ exchange</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>Automated quality inspection, workforce scheduling, job scheduling, supply chain optimization, inventory optimization, demand forecasting, materials simulation</td>
</tr>
<tr>
<td>Retail and Consumer Packaged Goods</td>
<td>Route optimization, vehicle loading and dispatch, supply chain optimization, inventory optimization, demand forecasting, molecular simulation</td>
</tr>
<tr>
<td>Telecom</td>
<td>Cell site planning, radio access networks (RAN) development, anomaly detection, job and workforce scheduling, quantum security and communication</td>
</tr>
<tr>
<td>Travel and Transportation</td>
<td>Logistics and route optimization, vehicle loading and dispatch, traffic management</td>
</tr>
</tbody>
</table>
The role of a QC partner

As QC is still evolving, we believe that most of the work in this area today is likely to be of an exploratory and experimental nature. Hence the prudent approach for most organizations would be to postpone decisions related to big investments in specific technology stacks, and instead focus on identifying the right use cases to invest in. This is where we believe, having a QC partner in the quantum value discovery journey could make an immense difference.

An ideal partner would be one who can tick off most of the following boxes:

• Does the partner have investments and capabilities in research?

• Does the partner have capabilities in the QC area?

• Does the partner bring in capabilities in allied technologies such as AI, ML, Optimization? Considering that most problems would require hybrid solutions using a mix of classical and quantum, strong capabilities in classical technologies would be equally critical to success.

• Does the partner have expertise in the industry domain and contextual knowledge of your business?

• Does the partner have a strong ecosystem of partners across established technology providers, startups, academia, and research institutes?

• Does the partner’s approach reflect a collaborative mindset and a focus on minimizing costs and mitigating risks?

• Does the partner have a proven capabilities of delivering across technologies, industries, and geographies?

• Does the partner have a track record of enduring relationships with customers?
References:


About the authors

Vidyut Navelkar: Head, Quantum Computing – Strategy & Consulting

Vidyut heads Quantum Computing – Strategy and Consulting at TCS and is responsible for incubating quantum computing as a potential big-bet business for TCS. In his career spanning over 30 years, Vidyut has played multiple roles in the intrapreneurship, innovation, learning and development, and software development areas, where he has been responsible for leading a variety of functions, programs, and projects. He has also been an active participant in various industry and academic forums. A senior member of IEEE and a life member of the Computer Society of India, Vidyut holds M.S. degrees in Computer Science, and Industrial and Management Systems Engineering.

Sridhar CV: Head, Alliances & Ecosystem partnerships, Incubation

Sridhar CV heads alliances and ecosystem partnerships for the incubation team for QC. He has over 21 years of experience in the areas of financial services and payments, governments solutions, transportation and telecom networks, and delivering multi-million-dollar technology transformation initiatives. Sridhar brings a blend of business and technology skills in the areas of QC, AI, ML, drones, robotics, and embedded systems to accelerate innovation with the help of technology leaders, startups, and other ecosystem partners. He represents TCS on BIS LITD 27 sub-committee for Internet of Things (IoT) standards. Sridhar has a bachelor’s in electronics and communication engineering from JNTU Hyderabad and holds an ExPGP in strategic management from IIM Indore.

Godfrey Mathais: Consultant, Quantum Computing

Godfrey Mathais is a Technical Consultant for the Incubation team for QC and is responsible for identifying big bet opportunities in the area. He has over 15 years of experience in the areas of cognitive solutions like data extraction, chatbots, and IoT solutions. He started out as a multiple stack mobile developer with an extensive experience in designing and developing Android SDKs. Godfrey holds a bachelor’s in computer science engineering from Mumbai University.

Sayantan Pramanik: Technical Architect, Quantum Computing

Sayantan Pramanik completed his graduation in electronics engineering in 2019 and has been working at TCS Incubation in the field QC for ML and optimization since. He has authored and co-authored multiple research papers that have been accepted at various international, peer-reviewed conferences, and has two patents filed. He is a Qiskit Advocate, and has hands-on experience in Qiskit, Amazon Braket SDK, and Pennylane.
Awards and accolades

About Tata Consultancy Services Ltd (TCS)
Tata Consultancy Services is a purpose-led transformation partner to many of the world’s largest businesses. For more than 50 years, it has been collaborating with clients and communities to build a greater future through innovation and collective knowledge. TCS offers an integrated portfolio of cognitive powered business, technology, and engineering services and solutions. The company’s 500,000 consultants in 46 countries help empower individuals, enterprises, and societies to build on belief.

Visit www.tcs.com and follow TCS news @TCS.

Contact
For more information on TCS Incubation visit https://www.tcs.com
Email: tcs.incubation@tcs.com

All content/information present here is the exclusive property of Tata Consultancy Services Limited (TCS). The content/information contained here is correct at the time of publishing. No material from here may be copied, modified, reproduced, republished, uploaded, transmitted, posted or distributed in any form without prior written permission from TCS. Unauthorized use of the content/information appearing here may violate copyright, trademark and other applicable laws and could result in criminal or civil penalties.

Copyright © 2022 Tata Consultancy Services Limited