Demystifying Quantum Computing: A Holistic Non-Technical Overview of the NISQ Paradigm and its Opportunities and Obstacles

Arnav Shah. *ORCID: 0009-0004-2283-6885 and* Tanay Pachisia. *tanaypachisia1@gmail.com*

***Abstract*—Quantum Computing is a field that is gaining recognition at a rapid rate around the world. This review shall address the unique elements of quantum computing with respect to classical computing, the current situation of quantum computing (i.e. Noisy Intermediate Scale Quantum or NISQ era computers) and the potential of such technology for the future. The review further seeks to discuss the problems that need to be overcome to attain quantum computing feasibility and the use of hybrid computing as an alternative that can derive from the benefits of the quantum world.**

***Index Terms*—Quantum communication, Quantum mechanics, Quantum system**

I. Introduction

Quantum computing is a process that leverages the laws of quantum physics to scale up classical computing processes to achieve exponentially larger computational ability. While the idea of quantum computing was fathered in the 1980s by physicist Richard Feynman [1], this method of computing has recently been gaining popularity among the masses. As such, this review seeks to depict and represent the progress made in the field and the potential of quantum computing, including its applications in cryptography, materials and pharmaceutical research, finance and Artificial Intelligence (AI), as well as giving a glimpse into the potential of quantum computing in the future.

A. Quantum and Classical Computing

To understand quantum computers, it is essential to understand classical computing and the difference between these methods of computing. Classical computers are those that are used on an everyday basis, such as laptops, phones, TVs, or even calculators. All these devices make use of 'bits' that represent two states 'on' and 'off' or '1' and '0'. Actions can be performed on the 'states' of single or multiple bits to return a different result that provides relevant information. These operations are known as logic gates.

To understand quantum computing, one must understand the phenomena leveraged by this computational model. This model was first proposed by Richard Feynman in 1981. Quantum Computing uses physical phenomena. It works on the principle that any quantum bit (or qubit), which can essentially be in the states 0 and 1 at the same time in varying proportions. The 0 and 1 in terms of a qubit can refer to any quantum properties of any particle such as the spin states of an electron (up and down) or the polarization states of a photon (H and V) [2]. This superposition state allows quantum computers to make use of other quantum phenomena such as quantum entanglement. Entanglement refers to the property of quantum objects in superposition to be somehow mathematically related to each other, where the state of one quantum particle informs about the states of all other particles. Therefore, when an operation is performed on one quantum particle in a group of entangled particles, the operation is effectively performed on all entangled particles. This phenomenon largely reduces processing time for non-deterministic algorithms, bringing often extremely lengthy calculations down to processes that take mere seconds. Note that this is not the case for every algorithm and that a quantum computer is largely impractical for deterministic algorithms such as a simple sum and that a classical computer would fare better in this scenario. A quantum computer's power lies in its ability to run multiple computations simultaneously allowing quantum computers to quickly process much larger data that would generally take much longer for classical computers. Although this may seem groundbreaking, the extent of experimental physics falls behind that of theoretical physics.

B. The Current State of Quantum Computing (NISQ)

While the field of quantum computing is brimming with potential, the technology existent today is subpar and infeasible as it is highly constrained by numerous limitations.

With the materialization and public availability of quantum processors, we can measure the extent to which they can currently operate. Although at present the functions of quantum computers are limited, they far surpass what we could have even imagined a few decades ago. At present, quantum computers can handle huge amounts of data. As a result of this, they are capable of conducting virtual experiments while considering innumerable random external factors, something that would not be viable on conventional computers. The sheer amount of data that quantum computers can hold also allows them to perform absurd calculations [3]. To put this into perspective, it is easy to model a hydrogen atom by hand, however, when dealing with atoms with over 70 electrons entangled with each other, to write down every conceivable result would take trillions of years. However, this function could take quantum computers mere seconds. It is possible for them to hold such vast amounts of data because of the ability of quantum bits to exist in multiple states simultaneously as compared to standard computers that use bits to exist in single

states (either 1 or 0) [4]. For example, Google's supercomputer uses a 53-qubit processor which can store more than 10 quadrillion combinations to perform infeasible calculations in a reasonable amount of time. To put this into perspective, in 2019, Google's supercomputer performed a calculation based on a simulation in about 200 seconds which would take the world's fastest supercomputer about 10,000 years to do.

The current quantum hardware processors are NISQ (noisy intermediate scale quantum) devices. NISQ devices are first functional quantum computer prototypes, however, they are not yet capable of performing at a sufficient degree of efficiency [5]. They can be helpful for the development of future quantum computer prototypes and hold a lot of potential for the field of computing. By analysing and examining the behaviour of these devices, we can create bigger, operational quantum computers in the future.

Although at present, quantum computing is in a preliminary state, it is being researched around the world, as it has the potential to revolutionize computing.

II. Potential Utilities and Beneficiaries of Quantum Computing

A. Quantum Encryption (Quantum Key Distribution)

Quantum Key Distribution (or QKD), proposed by Charles H. Bennett Gilles Brassard in 1984 [6] through an algorithm we now know as 'BB84', works on three essential principles: the observer effect, the no-cloning theorem and quantum entanglement.

The observer effect refers to the fact that merely observing the state of a quantum particle in superposition causes it to collapse into one of its eigenstates thereby constituting interference.

The no-cloning theorem states that it is impossible to 'copy' an entangled qubit into an unentangled qubit.

Quantum entanglement as discussed above refers to the nature of a system of particles in superposition to all undergo an operation when any one of them does. Although entanglement was not included in the original proposal of BB84, it has come to become integral to quantum cryptography.

Quantum cryptography works on the transmission of photons through fibre optic cables and varying quantum bases in the form of photon polarization to create a theoretically 'unhackable' system of encryption.

To understand what this means, let us look at the conventional example of Alice, Bob, and Eve [7], where Alice is sending a message to Bob. First let us analyse this process on a single qubit scale, without considering entanglement. When Alice sends a bit to Bob, she uses one of two means of polarization (bases) of her photon: rectilinear (0 and 90 degrees) and diagonal (45 and 135 degrees). At Bob's end, he will choose one of the two bases to measure the photon in. Bob and Alice then compare the basis they used. If Bob and Alice used a different basis, Bob discards the bit.

Now, if Eve, an eavesdropper, uses a different basis from the one Alice and Bob used, it would cause interference, collapsing the photon to its states measuring either 0 or 1, making it possible that Bob detects a different value from that sent by Alice, signalling the presence of an eavesdropper. Now, in reality, the data transferred is likely going to be more than a single bit, increasing the likelihood that an eavesdropper uses the wrong basis (as the eavesdropper would not have access to the information about the correct bases) and results in Bob receiving a photon encoding a different qubit than that sent by Alice. Furthermore, the effect of entanglement causes even more photons in the system to measure differently for Bob, as the same interference effect will affect all entangled photons. This makes it almost certain that the presence of an eavesdropper or man in the middle would be detected when using QKD algorithms.

Classical algorithms on the other hand would need other perhaps more complicated ways of detecting man-in-the-middle attacks, and yet it is not certain that a man-in-the-middle would always be detected as eavesdroppers relay information as a bitwise process. Due to the absence of entanglement and interference in classical mechanics, there is no indicator that the bit has been read by an eavesdropper. Whereas, due to interference and entanglement that are leveraged in QKD, it is almost certain that a man-in-the-middle attack is detected by a Quantum Computer.

While theoretically un-hackable, QKD faces physical limitations due to the fact that interference can be caused by any interactions with the particle in superposition, even during interparticular collisions. This makes it quite difficult to transmit qubits over long distances through fibre optic cables as the cables themselves play a part in condensing the superposed qubits.

B. Medicine and Material Simulation

Quantum computing and simulation technology are becoming more commonly used and tested within the field of life sciences. Many models such as those of quantum chemistry and superconducting materials cannot be solved with sufficient accuracy on classical computers. Quantum computers play a key role in simulating such quantum systems as well as numerically simulating mathematical models of physical systems. Quantum computing has already aided the development of the healthcare system. For example in radiotherapy, to optimize the best results in radiation determination, multiple simulations must be performed until the optimal level is reached [8]. With the aid of quantum computers, each simulation can be closely monitored and evaluated in terms of its potential and can be operated as a much broader prospect. In the future, the prospects of quantum computing in this field will be very versatile. For instance, in terms of medicines for diseases, currently, some companies have developed software that can compare hundreds of millions of molecules on classical computers [9]. However, this is limited by the size of the molecules that can be computed. With the emergence of quantum computers, it will be possible to more easily compare larger molecules, which is important in the pharmaceutical industry for developing new drugs. Additionally, quantum computers can save significant cost and time in bringing a drug to market. The advent of quantum computers can also facilitate the creation of more personalized therapies by linking genomes

of particular individuals of desired outcomes [10]. Clinical trials could also be optimized to improve safety by increasing causality analyses for side effects. A future possibility of a quantum MRI machine could produce highly accurate images that can visualize individual molecules. Artificial intelligence and quantum computing can be used to analyze these images, which would result in improved image quality and increased precision in identifying abnormalities, which could be better than human interpretation [11].

Thus, in the long run quantum computing can help healthcare providers improve diagnosis and reduce the need for repeated invasive testing. It can also be used to continuously monitor and assess an individual's health. This technology can not only benefit patients but also healthcare providers and health plans by reducing treatment costs through early diagnosis. It can also support more detailed diagnostic procedures to make data-driven decisions for individuals and healthcare providers.

C. Artificial Intelligence

Currently, while some research is being done to integrate quantum computing and AI, there does not exist an implementation that is more efficient than conventional means. However, through 'parallelism', the nature of quantum computers to simulate/process multiple outcomes simultaneously due to the power of entanglement that causes operations on one qubit to reflect in other qubits too (thus reducing the computation required for situations wherein a user desires for the same operation to occur on multiple bits), the training of AI can possibly be sped up. Experts believe that the quantum search algorithm [12] hints at the beginning of Quantum AI Development, but they have had little success in bridging quantum computing and AI.

The quantum search algorithm or Grover's algorithm [12] aims to identify a unique input to a black box function (or one wherein the function and its mechanics are unknown) that produces a particular output (cite Grover's algorithm). Grover's algorithm has a time complexity of $O(\sqrt{n})$ while classical algorithms have a time complexity of O(n). This means that, on average, Grover's algorithm needs a square root of the number of computations required by a classical approach to do the same task. This is but a rudimentary representation of the potential of quantum computing in applications in the field of AI. Algorithms including a Quantum adaptation of the Convolutional Neural Network [13] have been designed, but no modern computer possesses the ability to run such intensive algorithms.

However, instead of looking at quantum computing as a tool to scale the impacts of artificial intelligence, artificial intelligence can also support quantum computing, too, especially when it comes to the optimization of quantum circuits to utilize minimum resources and thus maximise feasibility.

D. Finance

Considering the potency of quantum computers with numbers, it is a given that they can play a great role in the field of finance. In fact, it is a major breakthrough that can decrease risk and increase profits by analyzing market conditions more quickly and with greater precision.

For stock traders, an advanced algorithm could provide successful strategies in High Frequency Trading which allows a large number of transactions to take place in split seconds. This can significantly increase transaction speed and reduce processing costs, resulting in many advantages such as optimization in portfolio management for assets with interdependencies [14].

Moreover, it replaces the task of hiring skilled mathematicians to perform such calculations and create algorithms on inefficient traditional computers.

Additionally, with such large amounts of data, the learning rate of artificial neural networks can be exponentially increased, allowing us to recognize previously undetectable and inconceivable patterns of the market.

Another potential benefit would be that the downtime on infrastructure using quantum computing would be negligible, this would result in savings in terms of time, money, resources and would fasten the progression of the market and firms.

Lastly, it can play an unimaginable role in synthetic data generation, which could allow for the testing of several models, without the need for collecting real world data.

III. Issues Surrounding Modern Quantum Computing

A. Decoherence

Due to the fact that quantum computers are never completely isolated from their surroundings, qubits tend to interact with the environment and are subject to environmental entanglements that can affect the qubit's future measurements. This means that decoherence is a natural process that will always occur, resulting in noisy and unreliable results. Finding a way to nullify or account for the effects of decoherence would facilitate increased reliance on the results of processes on quantum computers such as quantum simulations. This is one of the areas of study gaining a lot of academic attention recently. One popular method to account for decoherence is quantum error correction [15], which relies on the use of error correction codes that encode redundancies into the quantum computing processes. This essentially involves the leveraging of entanglement throughout the system in such a way that errors introduced into the system can be located and appropriately accounted for. However, the effects of decoherence will be felt at a greater scale with the increasing of qubits in a quantum computer as increased qubits mean increased susceptibilities to decoherence. Thus, it is a crucial challenge to overcome to allow for the growth of quantum computing.

B. Crosstalk

Crosstalk refers to the phenomenon where one qubit undesirably influences another qubit. This could be due to unintentional coupling between qubits, pulse spillover (wherein operations performed on a target qubit have an unintended effect on an independent non-target qubit), or shared environments. This phenomenon is a major source of noise in Noisy Intermediate Scale Quantum (NISQ, the current era of

quantum computing) computers [16]. Crosstalk also causes operations conducted in parallel to corrupt each other. This is a major problem in high qubit quantum computers [17] and can lead to errors spilling from one qubit onto others due to the fact that errors on different qubits can become correlated to each other due to crosstalk. This negatively affects error correction and makes such computers unreliable. Thus, mitigating or minimizing crosstalk would starkly improve quantum computer performance.

C. Temperature

For superconducting materials used in cutting-edge supercomputers, temperature regulation is a crucial need. At extremely low temperatures, superconductors are substances that show zero electrical resistance. The superconducting materials must be cooled using liquid helium or other cryogenic cooling systems to extremely low temperatures in order to maintain these superconducting capabilities. The material's superconducting properties improve with decreasing temperature, enabling quicker and more effective processing of data [18].

Advanced supercomputers also demand superconductivity in addition to temperature regulation. In comparison to ordinary electronic components, superconducting materials flow electrical current with no resistance, resulting in much lower power consumption and heat dissipation. For usage in computing systems that demand great processing power and energy efficiency, this makes superconducting materials appealing. Superconducting materials, however, may be challenging to create and are typically fragile, making it difficult to use them in real-world computing systems [19].

By enabling quicker and more effective processing, the use of superconducting materials is a crucial requirement to mitigate the error in quantum computers. However, the day that room temperature superconductors are achieved does not seem very far. In 2019, it was proved theoretically in India, that superconductors could exist at temperatures up to 70 degrees Celsius [20]. Additionally, in 2023 itself, a material LK-99 has shown promising results with near zero electrical resistance at 30 degrees Celsius [21]. This suggests a rapid growth in research and development of superconductors, suggesting the possibility of a room-temperature superconductor in the near future.

D. Drift

Drift is a time dependency which is non-trivial in the output probability of a circuit at a quantum level. To put it simply, when dealing with large amounts of data, which would be the case in the future, there would be an accumulation of errors which deviate from the ideal behaviour of the quantum circuit. These deviations, when stacked upon each other are known as drift. This could be caused due to interactions with the surroundings, unwanted interferences, decoherence, etc. and could result in inaccuracies in quantum circuits dealing with large amounts of data along with a significant waste of experimental effort [22], thus making it a very important issue to overcome, in order to achieve large scale quantum computing, performing tasks with big data and maintaining the accuracy of results produced by quantum computers [23].

IV. Hybrid Computing

Given the current limitations of quantum computing, innovative hybrid methods of computing may provide a more realistic alternative today. Hybrid computing or hybrid quantum-classical computing refers to algorithms that are made up of elements of quantum computing and elements of classical computing. Such algorithms include limited use of quantum computation at critical points when necessary so as to reduce the number of qubits needed. For example, Junhua Liu, Kwan Hui Lim, Kristin L. Wood, Wei Huang, Chu Guo & He-Liang Huang, in their paper, Hybrid quantum-classical convolutional neural networks [24], propose QCCNN (Quantum-Classical Convolutional Neural Network), that is the quantum version of the popular CNN (Convolutional Neural Network) based on classical algorithms. It further builds on an entirely quantum approach that would require as many qubits as the size of the input to the CNN, which can be impossibly large for current quantum machines to handle. This hybrid approach, however, uses a custom-designed parametric quantum circuit [24] on classically prepared feature maps (elements of a CNN that are essentially a function of CNN filters along the data) in the convolutional layer. Thus, the number of Qubits required depends solely on the window-size for the feature maps. Such synergistic uses of quantum and classical approaches would allow productive and effective use of current technology, even with its limitations.

V. Conclusions

Thus, traditional computers and quantum computers are technological advancements that are revolutionary in their respective temporal settings. Classical computing manipulates bits through logic gates, while quantum computing, uses qubits that can exist in several states simultaneously. Applying quantum computing could revolutionise industries including AI, banking, health, and cryptography, by allowing the use of big data and large scale simulations. However, issues like crosstalk, decoherence and temperature restrictions for superconductors must be overcome in order to advance to such a level. As such, it is imperative for increased research to be conducted and awareness to be generated with regard to the development and potential of quantum computing as a field.

Acknowledgments

We would like to thank Mr. Tejas Shyam for their inputs and guidance, which proved to be invaluable in shaping this paper.

References

[1] R. P. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, pp. 467–488, 06 1982.

[2] E. Rieffel and W. Polak, "An introduction to quantum computing for non-physicists," *ACM Computing Surveys*, vol. 32, pp. 300–335, 09 2000.

[3] T. Proctor, K. Rudinger, K. Young, E. Nielsen, and R. Blume-Kohout, "Measuring the capabilities of quantum computers," *Nature Physics*, vol. 18, pp. 75–79, 12 2021.

[4] A. Pandhare, "Quantum computer : An overview," *www.academia.edu*. [Online]. Available: https://www.academia.edu/34973026/Quantum_Computer_An_Overview

[5] J. Preskill, "Quantum computing in the nisq era and beyond," *Quantum*, vol. 2, p. 79, 08 2018. [Online]. Available: https://quantum-journal.org/papers/q-2018-08-06-79/

[6] *Quantum Cryptography: Public-Key Distribution and Coin Tossing*. Proceedings of the International Conference on Computers, Systems and Signal Processing, 1984. [Online]. Available: https://doi.org/10.48550/arXiv.2003.06557

[7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, pp. 145–195, 03 2002.

[8] K. L. Brown, W. J. Munro, and V. M. Kendon, "Using quantum computers for quantum simulation," *Entropy*, vol. 12, pp. 2268–2307, 11 2010.

[9] R. Corporation, *Using Quantum Computers and Simulators in the Life Sciences: Current Trends and Future Prospects*, 01 2022.

[10] D. Solenov, J. Brieler, and J. F. Scherrer, "The potential of quantum computing and machine learning to advance clinical research and change the practice of medicine," *Missouri medicine*, vol. 115, pp. 463–467, 2018. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6205278/

[11] S. Sahai, R. Jones, and N. Sahai, "Benefits of quantum computing in predictive healthcare system," *International Journal of Computer Trends and Technology*, vol. 69, pp. 16–21, 02 2021.

[12] *A fast quantum mechanical algorithm for database search*. Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96, 1996. [Online]. Available: doi.org/10.1145/237814.237866

[13] I. Kerenidis, J. Landman, and A. Prakash, "Quantum algorithms for deep convolutional neural networks," arXiv.org, 11 2019. [Online]. Available: https://arxiv.org/abs/1911.01117

[14] V. Muddu, "Quantum computing in banking how far are we from day zero?" [Online]. Available: https://sbi.co.in/documents/2182813/4777159/Quantum+Computing+in+Banking_Indian.pdf

[15] S. J. Devitt, W. J. Munro, and K. Nemoto, "Quantum error correction for beginners," *Reports on Progress in Physics*, vol. 76, p. 076001, 06 2013.

[16] J. Preskill, "Quantum computing in the nisq era and beyond," *Quantum*, vol. 2, p. 79, 08 2018. [Online]. Available: https://quantum-journal.org/papers/q-2018-08-06-79/

[17] P. Murali, D. McKay, M. Martonosi, and A. Javadi-Abhari, "Software mitigation of crosstalk on noisy intermediate-scale quantum computers," *arXiv (Cornell University)*, 03 2020.

[18] Y.-P. Shim and C. Tahan, "Semiconductor-inspired design principles for superconducting quantum computing," *Nature Communications*, vol. 7, 03 2016.

[19] K. Berggren, "Quantum computing with superconductors," *Proceedings of the IEEE*, vol. 92, p. 1630–1638, 10 2004. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/1335553

[20] S. Hingorani, V. Pillai, P. S. Kumar, M. Multani, and D. O. Shah, "Microemulsion mediated synthesis of zinc-oxide nanoparticles for varistor studies," *Materials Research Bulletin*, vol. 28, pp. 1303–1310, 12 1993.

[21] S. Lee, J.-H. Kim, and Y.-W. Kwon, "The first room-temperature ambient-pressure superconductor," arXiv.org, 07 2023. [Online]. Available: https://arxiv.org/abs/2307.12008

[22] T. Proctor, M. Revelle, E. Nielsen, K. Rudinger, D. Lobser, P. Maunz, R. Blume-Kohout, and K. Young, "Detecting and tracking drift in quantum information processors," *Nature Communications*, vol. 11, 10 2020.

[23] C. Arenz, B. Russell, D. Burgarth, and H. Rabitz, "The roles of drift and control field constraints upon quantum control speed limits," *New Journal of Physics*, vol. 19, pp. 103 015–103 015, 10 2017.

[24] J. Liu, K. H. Lim, K. L. Wood, W. Huang, C. Guo, and H.-L. Huang, "Hybrid quantum-classical convolutional neural networks," *Science China Physics, Mechanics & Astronomy*, vol. 64, 08 2021.