International Journal of Engineering Research & Management Technology
(Peer-Reviewed, Open Access, Fully Refereed International Journal) ISSN: 2348-4039
Volume 11, Issue-5, September-October- 2024 Impact Factor: 7.09
Email: editor@ijermt.org www.ijermt.org

The Future of Quantum Computing Harnessing the Power of Quantum Mechanics

Dr. Om Pal Singh

Officiating Principal, Salawa Inter College, Salawa (Meerut)

Abstract

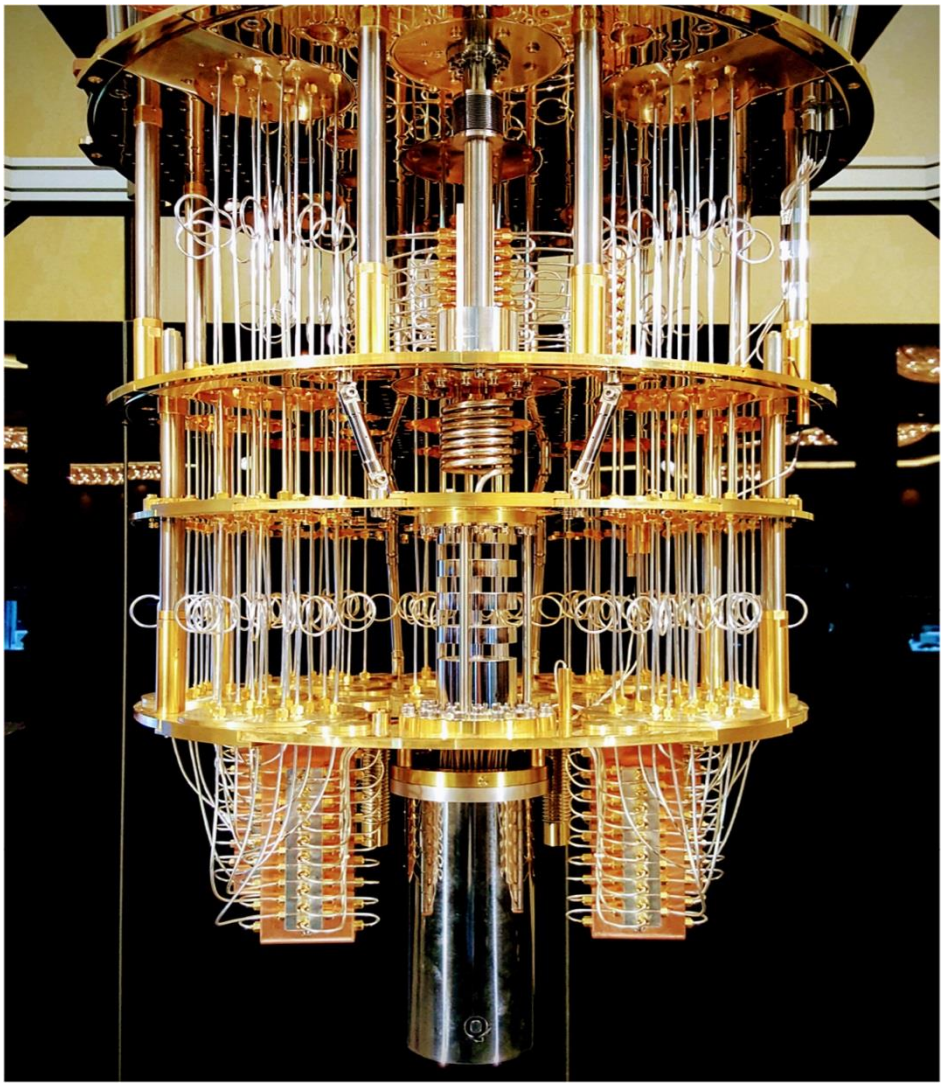
Quantum computing is currently a topic of interest that harnesses the phenomena of quantum mechanics. It can address several scientific challenges and generate new business opportunities. Recently, for the first time in the history of quantum computing, the authors are starting to see practical applications. Keeping this in mind, this article is designed to explore the field without any required prerequisites. The authors start with a brief overview of the fundamentals of quantum computing and also outline several applications. The timeline for widespread adoption cannot be predicted, but quite a few organisations have built the first generation of quantum computers using various hardware technologies. The authors have briefly covered the wide landscape of hardware technologies. The first generation of quantum computers can be programmed using available software development kits and accessed using online cloud services. Furthermore, the growing trend in investments and patents in the field of quantum computing is also presented. A major reason for this trend is the threat that quantum computers pose against cryptography.

1 Introduction

Quantum computing is an emerging field that uses the concepts of quantum mechanics to perform computations. It is an intersection of fields such as mathematics, physics and computer science. The starting point for quantum computers can be traced back to the 1980s when physicists asked whether a universal device can simulate quantum mechanical systems.

Quantum computers exist today but their practical use is close to zero. The field has shown enormous potential, but research is still ongoing, and it is impossible to predict the future. In the 1990s, could anyone have predicted the use of the internet in our daily lives? In the same manner, quantum computing is in its infant stage. Researchers call this era the noisy intermediate-scale quantum (NISQ) era because the current quantum circuits are susceptible to noise. There is hope that devices in the NISQ era will soon start showing practical applications such as optimisation problems, machine learning, cryptography, finance and simulation of quantum mechanical systems.

As of the year 2020, organisations have built quantum computers with up to 50 qubits and are increasing it up to 100 qubits. Large companies such as Google, IBM and Microsoft and startups such as Rigetti, D-Wave and Xanadu have built quantum computers. Fig. 1 shows a quantum computer developed by IBM. Organizations have also developed a software development kit (SDK) using which the general public can experiment with quantum computers. There also exist cloud services that allow people to run their code on a real quantum computer. IBM quantum experience and Rigetti forest are examples of such services. In the next section, we discuss some of the fundamentals of quantum computing.



2 Fundamentals

Analogous to bits in classical computers, quantum computers have quantum bits or qubits [4].

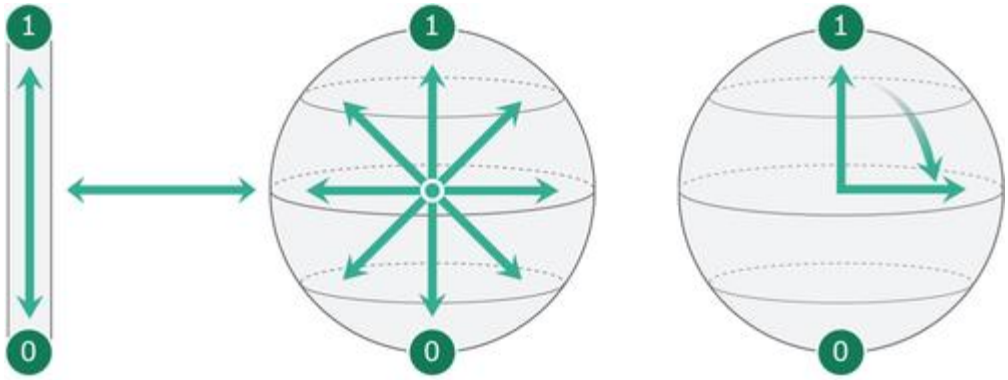
$$0 \rightarrow |0\rangle$$

$$1 \rightarrow |1\rangle$$

Unlike bits, qubits are two-dimensional vectors that exist in the Hilbert space. They can be physically represented as a single atom, electron, photon or a cold superconducting circuit with moving electrons.

2.1 Superposition

The qubits $|0\rangle$ and $|1\rangle$ are known as computational basis. The actual qubit can be a superposition of these computational bases. In other words, it can exist in between $|0\rangle$ and $|1\rangle$. Qubits can be represented graphically using a Bloch sphere. As seen in Fig. 2*a* thequbits $|0\rangle$ and $|1\rangle$ point up and down, respectively. A qubit in superposition can point in any direction of the sphere. Mathematically speaking, a superposition is a linear combination of the computational bases.



2.2 Measurement

Qubits exist in superposition of $|0\rangle$ and $|1\rangle$. It is very strange, but when a qubit is measured, it collapses to either $|0\rangle$ or $|1\rangle$. It cannot be predicted with certainty to which state the qubit will collapse. However, a probability of whether a qubit will collapse to a particular state can be determined.

2.3 Quantum gates

The most common model of computation for quantum computers is the quantum circuit model. Other models such as adiabatic quantum computer and quantum Turing machine also exist. Analogous to a classical computer, this model has quantum gates that transform the input qubit. A sequence of gates can be used to perform complex computations. A quantum gate can be completely described by specifying how the computational basis, i.e. $\{|0\rangle, |1\rangle\}$ are transformed by the operation of a quantum gate. The NOT(X), Hadamard and CNOT(CX) are the most common gates. The NOT gate transforms $|0\rangle$ to $|1\rangle$ and vice versa. Fig. 2*b* shows a graphical representation for the application of a Hadamard gate. The Hadamard gate creates an equal superposition state, which means that the qubit's probability to collapse to either $|0\rangle$ or $|1\rangle$ is equal. The CNOT gate is special in the sense that unlike NOT and Hadamard, it takes two qubits as input. It acts like the 'if condition' in programming.

2.4 What makes quantum computers special?

Two concepts of quantum mechanics, namely *superposition* and *entanglement*, make quantum computers special. As discussed above, superposition means that a qubit can exist in between $|0\rangle$ and $|1\rangle$. In entanglement, two qubits are prepared in an entangled state in which they do not act individually but as a group. This will hold even if the qubits are light-years apart. Entanglement increases the information density of quantum computers.

As an example, imagine two qubits. One of the methods to entangle qubits is by applying the Hadamard and the CNOT gate in a particular configuration. After the gates application, we have two qubits, which, when measured, have an equal probability of collapsing to either $|0\rangle$ or $|1\rangle$ state. If the output of measurement for the first qubitis $|0\rangle$, then due to entanglement, we can be certain that the second qubit will also collapse to $|0\rangle$ when it is measured. Similarly, if the first is measured to be $|1\rangle$, then the second will undoubtedly collapse to be $|1\rangle$ when measured.

Classical computers can compute difficult problems. However, the time period can be infinitely large. This is the case when classical computers try to simulate quantum mechanics. To simulate a molecule containing *n* atoms, a classical computer needs to track and store k^n complex numbers, where $k \geq 2$. Molecules can contain >100 atoms. It will require an unimaginable amount of memory even to store the complex numbers. It is safe to assume that classical computers can never simulate a quantum mechanical system. Other than simulation, researchers have also identified quantum algorithms that provide an exponential speed-up [5].

3 Benefits of quantum computing

Quantum computing is a technology which can process data at an exponential rate, faster than any supercomputer. Realising this fact, many private sector companies have started investing in R&D. Many experts in this field believe that the development of quantum computing technologies may not follow the normal smooth curve of progression. In this early development phase, companies that have started investing and developing plans to incorporate their business structure with quantum supremacy have far better chances to capitalise on the future market.

3.1 Types of problems it can solve

There are four categories of problems where a quantum computer can be significantly advantageous over a classical computer. These four types of problems cover most of the applications developed by many industries to generate new business opportunities and have a competitive advantage. This is adapted from [6].

- (i) *Combinatorial optimisation*: It is the process of searching for maxima (or minima) of an objective function, for example, finding the shortest total distance among a given set of points. In many such problems, performed on a classical computer, brute-force search is not tractable. Applications based on finding the shortest path in a complex network fall under this category.
- (ii) *Problems based on linear algebra*: Linear algebra is a sub-field of mathematics which involves vectors, matrices, and linear transforms. It serves as a fundamental pillar to machine learning, which has a prominent significance in numerous applications across industries.
- (iii) *Problems involving differential equations*: A differential equation can be mathematically stated as an equation that relates one or more functions and their derivatives. It can be used to model the behaviour of complex systems involving fundamental laws of physics. Various applications based on simulation fall under this category.
- (iv) *Factorisation*: It is the process of decomposition of an expression into a product of its factors. In the present scenario, computer security and cryptography are heavily reliant on classical computers' infeasibility in factoring the product of two prime numbers.

3.2 Applications and use cases

The most valuable quality of a quantum computer is its ability to perform large-scale simulations. This property accounts for a large number of applications in various kinds of industries. Table 1 shows a list of possible use cases with its related industry [7].

Table 1. List of potential industrial applications

4 Threats to existing cryptography

Apart from the numerous benefits of quantum computing, it has a few negative consequences. Since quantum computers can process data at an exponential rate, it can raise serious threats to the existing cryptosystems. The ‘Shor's algorithm,’ developed by Peter Shor in 1994, has raised some serious concerns regarding the present cryptosystems which are reliant on algorithms like the Rivest-Shamir-Adleman (RSA). However, the present quantum computers do not meet the hardware requirements to implement this algorithm.

The present cryptography is divided into symmetric and asymmetric encryption. Symmetric encryption involves the use of the same cryptographic key for both encryption and decryption of messages. It is fast and efficient to process a large amount of data, but protecting and transferring the secret key is a big challenge. advanced encryption standard (AES), data encryption standard (DES), one-time password (OTP) and secure hash algorithm (SHA) are few well-known algorithms under this scheme. To address the challenge of transferring the secret key in a public channel, asymmetric encryption schemes were developed. It required for the receiving person to generate two distinct but mathematically related cryptographic keys. One key is made public and can be used by the sender to encrypt his secret message. The other key is kept private and is used to decrypt the received encrypted message. RSA, Diffie–Hellman and elliptic-curve cryptography (ECC) are a few well-known algorithms under this scheme. Asymmetric encryption schemes are combined with the symmetric encryption schemes to provide robust security in present cryptosystems.

Numerous applications, like browsing webpages, making online payments, digital signatures and emails, are reliant heavily on the asymmetric encryption schemes such as the RSA algorithm. RSA algorithm hinges on the classical computers' inability to find factors of the product of two big prime numbers. However, this can be compromised if ‘Shor's algorithm’ is implemented. It is estimated that a quantum computer with 4000 qubits and 100 million gates is required to break a 2048 bit long RSA key [8]. Similarly, other public-key encryption schemes such as Diffie–Hellman and ECC become useless against a quantum computer [9]. On the other hand, the Grover algorithm can provide an efficient quantum search in an unstructured database, posing a threat to the symmetric encryption schemes [9]. Just to compare, the AES algorithm with 128-bit long key requires 2^{128} operations on a classical, whereas a quantum computer can recover the key with just 2^{64} operations [8].

Due to these security threats, R&D to establish quantum computer resistant cryptosystems is on prime focus. The National Institute of Standards and Technology has started the process of evaluation and standardisation of post-quantum cryptographic algorithms. The future of cryptography can be divided into two categories. The first is ‘post-quantum cryptography’, which provides alternative cryptosystems based on mathematical problems, which is proved to be hard even for quantum computers to solve. Various encryption schemes such as lattice-based cryptography, code-based cryptography, hash-based cryptography, multivariate cryptography and isogeny cryptography, fall under this category.

The second is quantum-based cryptography, which makes use of quantum phenomenon to develop quantum-resistant cryptosystems. Quantum mechanics posses a few fundamental properties, such as the ‘no-cloning theorem’, that can be exploited to establish robust cryptosystems. Researchers are working primarily on quantum key distribution, which utilises quantum principles such as Heisenberg Uncertainty Principle and quantum entanglement to enable secure key distribution in a public channel. Protocols such as BB84, SARG04, DPS and E91 fall under this category. At the present moment, many cryptography schemes rely on the ‘pseudo-random numbers’ generated on a classical computer. This can be further improved as quantum random number generation (QRNG), which can generate truly random numbers. Many private companies are working on QRNG to counter the risk posed by the present cryptosystems.

5 Quantum computing hardware landscape

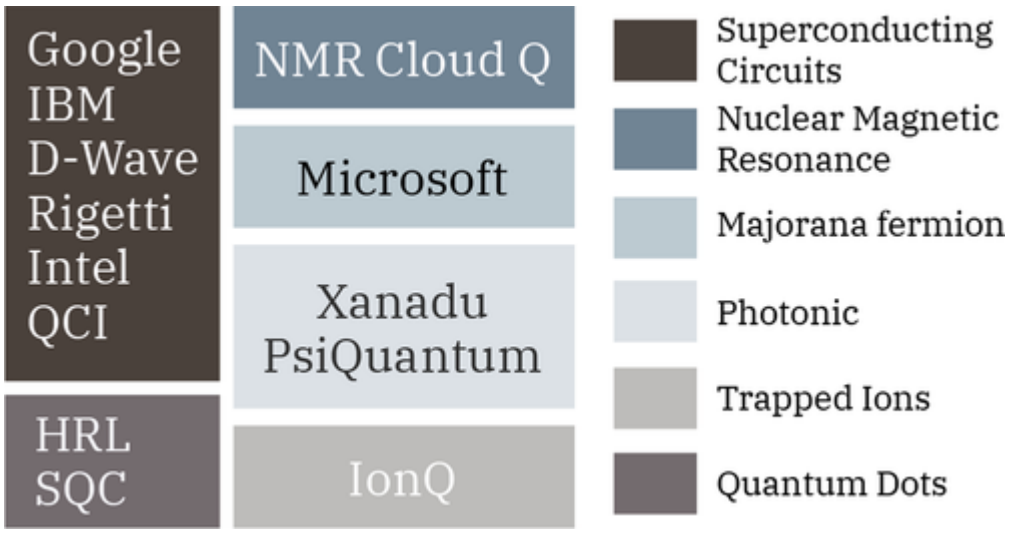
A question that is on everyone's mind is that when will we be able to see the practical benefits of quantum computing? It is hard to predict correctly, but progress has been happening at a tremendously fast rate. Companies such as Google, IBM, Rigetti have already developed quantum computers with qubits>50. Such computers may able to surpass today's classical computers.

5.1 NISQ era

As mentioned in Section 2, qubits collapse to a classical state when measured. Practically, a slight disturbance to the qubit can cause the qubit to collapse. This makes developing hardware difficult. On the other hand, the qubits have to interact with each other strongly. Eventually, it may be possible to scale quantum computers using the principle of quantum error correction. Preskill in [10] coined the term NISQ to describe the era at hand. In this era, we will not have full control over qubits, but it is a significant milestone, as classical computers cannot simulate quantum computers having >50 qubits.

5.2 Promising technologies

This section provides an overview of the technologies that organisations are currently using to build their quantum computers. Fig. 3 divides the organisations based on the hardware technology they are using.



5.2.1 Superconducting circuits

Superconducting circuits are the leading technology in the NISQ era [11]. This is evident from the fact that organisations such as IBM, Google, Rigetti, Alibaba and Intel are all betting on this technology. A superconducting material has zero resistance. It can be created by cooling down materials to a very low temperature (around 1°K). The property of zero resistance allows the qubit to remain error-free. Each qubit is an LC oscillator comprising of an inductor and a capacitor. It looks similar to a classical electronic microwave circuit. The most important concept is of Josephson junction, which is used to provide an ordinary circuit with the qubit's properties. The tech companies have high hopes for this technology. One of the reasons is that it is based upon the CMOS technology with which the industry is already familiar. The cloud-based platform, known as IBM quantum experience [12] allows the general scientific community to run their programs on a real quantum computer based on superconducting circuits.

5.2.2 Trapped ions

Trapped ion is one of the primary contenders among various technologies for the development of the practical quantum computer. Ions are charged atoms formed by stripping electrons away from the atom. The ions are then trapped inside an electromagnetic field, hence their name. The qubit is represented by the energy level of their intrinsic spin. A laser beam is used to manipulate the qubits. Trapped ions can help in the study of condensed-matter physics, and can also be extended to perform high-level simulations such as cosmology and high-energy physics. A major advantage in the use of this technology is that individual ions can easily be measured and manipulated [13].

5.2.3 Other technologies

The scope for research to find alternative technologies for building a quantum computer is huge. An approach that is similar to trapped ions is using *neutral atoms* trapped inside an optical lattice. *Defect centres* in diamonds are also used to realisequbits. The idea is to remove a carbon atom from a diamond. This vacancy is then filled by a nitrogen atom. It creates an effective spin that is used to define a qubit. This technology is currently facing scalability issues.

The current mechanisms to represent a qubit are fragile and are susceptible to noise which makes them prone to errors. An approach known as *topological quantum computing,* hopes to have a meager error rate relative to other hardware technologies [14]. The technology is still in its early stages but can be a game-changer for the field. In such an approach, the information is encoded in the topology of a particle. An object's topology is defined by properties that are preserved under continuous deformations such as twisting and stretching. Since we are interested not in the particle but its topology, it makes this approach more noise and error resistant. The tech giant Microsoft is actively pursuing this approach.

There is also an approach based on *photons*. Since photons operate at room temperature and are based on silicon chips they can be a fascinating and alternative route. Other approaches include *nuclear magnetic resonance* and electrically controlled quantum dots. Nuclear magnetic resonance was the initial approach to building quantum computers, but it has since been majorly discarded. It is very hard to scale using this approach. Electrically controlled *quantum dot* is an approach that, unlike superconducting circuits, is semiconductor-based. Qubits are represented as electronic spins trapped in a semiconductor nanostructure.

6 Tools for quantum computers

Analogous to a classical computer, a stack of technologies is required to control a quantum computer. However, the classical stack does not have the necessary features to manipulate quantum data. Therefore, numerous instruction sets, compilers, languages and interfaces have been developed to run on a quantum computer or simulate a quantum computer on a classical computer since the late 1990s.

A quantum computer is a hybrid machine comprised of both a quantum device and a classical computer. Classical computing is required at a higher level where a user can write a program and send instructions to the quantum hardware. The lowest layer of abstraction is the physical quantum computer on which instructions are executed. The instructions are part of an instruction set which are directly understandable by a quantum computer. Example of instruction sets include OpenQASM [15], Quil [16]. The actual code that is written by humans are then later compiled to directly executable instructions. Humans write algorithms

in quantum programming languages that can then be applied to solve various problems. All the above-mentioned layers are bundled into SDKs. Fig. 4 shows levels of abstraction of a quantum computer.

6.1 Tools of significant interest

6.1.1 IBM quantum experience (qiskit)

IBM quantum experience [12] is a cloud-based platform that allows the general scientific community to access real quantum computers with 5 or 16 qubits. It also contains a cloud-based simulator of 32 qubits. *Qiskit* is an open-source SDK developed by IBM, which can be used alongside IBM quantum experience. Qiskit is built on top of python and can run locally or in online Jupyter notebooks. Qiskit contains four fundamental elements Terra, Aer, Ignis and Aqua, which provide different levels of abstraction. Terra provides the lowest level of abstraction and can be used to create quantum circuits. On the other hand Aqua provides the highest level of abstraction and can be used to create quantum algorithms. Other than Qiskit, IBM quantum experience also includes a GUI-based interface to create quantum circuits.

6.1.2 Rigetti forest (pyQuil)

Rigetti computing is a startup that provides the Forest SDK. It includes *pyQuil*, the Rigettiquil compiler (*quilc*) and the quantum virtual machine (qvm) [16]. The pyQuil is an open-source python library to write programs. *Quil* is an instruction set architecture for quantum computers. The quilc is a compiler that compiles Quil for different architectures. The qvm can be used to simulate quantum computers on classical machines and execute Quil instructions.

Rigetti computing offers quantum cloud services to access their quantum computers through an access point. It is currently not publicly available. The quantum cloud services provide a virtual machine preconfigured with Forest SDK and is called quantum machine image.

6.1.3 Azure quantum (Q#)

Azure quantum is a full-stack, cloud ecosystem for quantum computers by the giant Microsoft [18]. For software development, it includes Microsoft's quantum development kit (QDK). Q# is an open-source programming language part of the QDK. Q# has integrations with visual studio and visual studio code. Programs written in Q# can be combined with Python or NET framework. The QDK includes a rich source of libraries and code samples.

The written programs can run on a simulator locally, on classical computers hosted on Azure, or a quantum computer. Due to the collaboration of Azure quantum with other industry leaders, it has the advantage of providing the user different types of quantum hardware to choose from.

6.1.4 Project Q

Project Q is an open-source python framework that was started in ETH Zurich [19]. It provides a powerful and intuitive syntax. The main feature is that it has support for different backends such as IBM's quantum computer, a classical quantum simulator or CircuitDrawer (it generates TikZ code for drawing quantum circuits). It can be expected that other backend will be supported

in the future. The compiler for Project Q is modular and customisable. A library called FermiLib is also included, which can be used to analysefermionic quantum simulation problems.

6.1.5 Cirq

Cirq is also an open-source Python library for programming quantum computers [20]. With the increasing availability of NISQ computers (50–100 qubits), the development of algorithms to understand the power of these machines is of increasing importance. However, a common problem when designing a quantum algorithm on a NISQ processor is how to take full advantage of these limited quantum devices. Cirq attempts to solve these problems by exposing the details of the hardware rather than abstracting it. They believe that the details are important in the current NISQ era to determine whether a circuit is executable. The library is currently in the alpha stage and is promoted by the Google AI quantum team.

6.1.6 Strawberry fields and pennly lane

Xanadu is a startup working on quantum computers based on photonic technology. Penny Lane is a cross-platform Python library developed by Xanadu that provides quantum machine learning tools, automatic differentiation and optimisation of hybrid quantum-classical computations. Penny Lane can combine quantum hardware and existing libraries such as NumPy, TensorFlow and PyTorch. The library is device independent and has supported various quantum hardware and simulators, including IBM quantum experience, Rigetti forest, Microsoft QDK, Cirq and their own hardware.

Strawberry Fields is another open-source full stack python library that can be used to design, simulate and optimise the continuous-variable quantum optical circuits [21]. Programs can run on their own photonic quantum computing chips via the Xanadu Quantum Cloud.

6.1.7 D-Wave ocean

D-Wave is a company that develops a quantum computer based on quantum annealing. These quantum computers are not universal, unlike the ones discussed in Section 5. They are suitable for solving optimisation problems such as finding the minimum of a system. The *Ocean* is a set of open-source tools developed by D-Wave. Programs can also be submitted to D-Wave for execution on their quantum processing unit.

7 Growth in the field of quantum computing

Keeping in mind the high impact that the quantum computers can have in the future, many governmental institutes and private agencies have funded R&D in quantum computing technologies. Despite having many market-ready and mature technologies such as artificial intelligence and blockchain, quantum computing has caught the attention of many venture capitalists. This is evident from the rise in investments among various startups. Fig. 6 shows investments in USD Million, in various startups working on quantum computing technologies, as of the year 2020.

References

- 1Feynman R.P.: ‘Simulating physics with computers’, *Int. J. Theor. Phys.*, 1999, **21**, (6/7), pp. 467–488

- 2Srivastava R., Choi I., Cook T. *et al.*: 'The commercial prospects for quantum computing', *Networked Quantum Inf. Technol.*, 2016, **1**, (1), pp. 1–48
- 3Ploughman L.: ' IBM's Q quantum computer. CC-BY-SA 2.0 via flickr'. Available at:
- 4Nielsen M.A., Chuang I.: ' *Quantum computation and quantum information*' (American Association of Physics Teachers, Maryland, United States, 2002)
- 5Montanaro A.: 'Quantum algorithms: an overview', *Npj Quantum Inf.*, 2016, **2**, (1), pp. 1–8
- 6Langione M., Kumar A., Tillemann-Dick C. *et al.*: ' Where will quantum computers create value–and when?', Boston Consulting Group, November 2019,
- 7Gerbert P., Rueß F.: ' The next decade in quantum computing and how to play', Boston Consulting Group, November 2018
- 8Moses T.: ' *Quantum computing and cryptography*' (Entrust Inc, Dallas, Texas, United States, January, 2009)
- 9Mavroeidis V., Vishi K., Zych M.D. *et al.*: ' The impact of quantum computing on present cryptography', arXiv preprint arXiv:180400200, 2018
- 10Preskill J.: 'Quantum computing in the NISQ era and beyond', *Quantum*, 2018, **2**, p. 79
- 11Kjaergaard M., Schwartz M.E., Braumüller J. *et al.*: 'Superconducting qubits: current state of play', *Annu. Rev. Condens. Matter Phys.*, 2020, **11**, pp. 369–395
- 12Aleksandrowicz G., Alexander T., Barkoutsos P. *et al.*: ' Qiskit: an open-source framework for quantum computing', Accessed on: Mar, 2019, vol. 16
- 13Buluta I., Nori F.: 'Quantum simulators', *Science*, 2009, **326**, (5949), pp. 108–111
- 14Lahtinen V., Pachos J.K.: 'A short introduction to topological quantum computation', *SciPost Physics*, 2017, **3**, (3), pp. 1–43
- 15Cross A.W., Bishop L.S., Smolin J.A. *et al.*: ' Open quantum assembly language', arXiv preprint arXiv:170703429, 2017
- 16Smith R.S., Curtis M.J., Zeng W.J.: ' A practical quantum instruction set architecture', 2016
- 17Purkeypile M.: ' Cove: A practical quantum computer programming framework', arXiv preprint arXiv:09112423, 2009
- 18'Experience quantum impact with azure quantum', 2019.
- 19Steiger D.S., Häner T., Troyer M.: 'Projectq: an open source software framework for quantum computing', *Quantum*, 2018, **2**, p. 49
- 20'Announcingcirq: An open source framework for NISQ algorithms', 2018.