Survey on Quantum Computer Architectures

Manoj Kumar Chamarthi
dept. of Computer Science
Texas A and M University-Corpus Christi
USA
mchamarthi@islander.tamucc.edu

I. Abstract

Quantum Computing is a branch of computer science that use quantum physics to compute mathematical operations.These are proven to perform better at complex calculations than the classical computers.Slowly, public interest in this field is increasing.Most modern companies like google,IBM,Intel are developing quantum computers to be usable for their applications which might benefit end user. Since Quantum computing is entering into our lives, it is essential to develop and model software that can utilize quantum computing architecture.We did a survey on various aspects like architectural processes, designs, support and challenges on quantum architectures.This survey results might help quantum computing engineers to develop the applications in an optimized and more suitable way.

II. Introduction

Quantum computer(QC) is a machine that uses quantum superposition and entanglement to perform computations. This works on quantum mechanics[1].With current development trend in quantum computing and programming, developers are able to extract the intuition of quantum mechanics to retrieve information and perform mathematical computation lot faster than classical computers[2].On contrast to classical computing, quantum computing can perform certain parallel computation tasks exponentially better.The fundamental unit in a quantum computer is qubit(Quantum bit).A Qubit can represent either 0 or 1 or both 0 and 1.This representation of 0 and 1 at same time is known as superposition.This superposition is the advantage over traditional computer which can have either 0 or 1.Quantum Programming languages [3] can make use of qubits and quantum algorithms to solve many impossible problems (breaking cryptography by brute force).They also provide faster results in fields like search response, machine learning, artificial intelligence etc.

The Inception of quantum computing began with Richard Feynman, famous American quantum physicist and Nobel Laureate.His proposal was based on limitations of classical computers for simulating quantum particles[4].

In order to understand quantum computers architectures, one must understand the laws that govern the quantum particles, this study of tiny particles is called as quantum mechanics(motion of quantum particles).Classic mechanics was not able to solve problems like black body radiation and photo electric effect.For black body radiation problem, Max Planck's formula worked and it created a new branch of science called Quantum Physics.Fig.1 depicts black body experiment that was limitation for classical physics.Other classical mechanics problems that Quantum physics solved was photo-electric effect.This problem was solved by Albert Einstein in the year 1905, this proved that when a light wave (electro-magnetic) hits a metal surface, a small amount of free electrons will be released.By this Einstein observed that light consists of small quantum particles called photons.Fig 2. depicts the emission of electrons when light hits a metal.

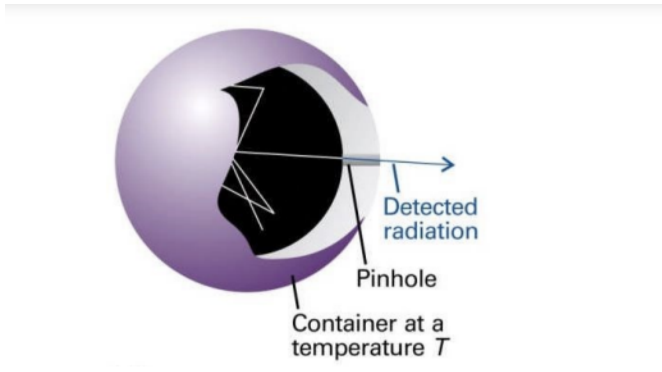


Fig. 1. Black body radiation experiment

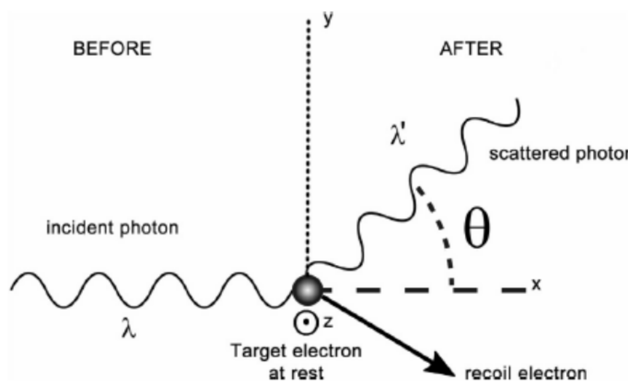


Fig. 2. Phenomenon of photoelectric effect

Quantum particles possesses wave nature, that means they have amplitudes, frequencies etc.So, they are represented using wave functions.Famous Schrodinger's wave function is an example of wave function.Erwin Schrodinger proposed this in the year 1925 and it is an equation that represents wave with respect to time.In any wave function, the exact position of a particle cannot be known at a given time(Heisenberg's Uncertainty principle), so we use probabilities to represent the position.

Quantum gates: The main functionality of a quantum gate is to get abstraction over single operations. Physically, quantum gate is a combination of quantum circuits. These processes quantum bits as fundamental units. Some examples of this are Pauli gates, phase shifter, hadamard gates etc. There are numerous ways to deploy these in applications, few examples of deployment techniques are quantum polynomial time circuits and shallow circuits.

Quantum memory: Similar to conventional architecture, all the states of quantum bits will be stored in a specific location, these allocations are called as quantum memories. In the last ten years, several implementations are put forward, that store states in an array like data structure.

Quantum processing units: It is similar to CPU, it has Quantum memory and uses quantum bus to communicate and operates on qubits. It stores quantum mechanical state of particles.

Quantum error correction is also an important aspect in dealing with quantum computers. Similar to traditional computers, quantum computers will also have specific codes to distinguish errors, but unlike traditional computing, quantum errors will be mostly due to coherence with free particles in environment. Quantum error correction will be done to undo the external particle coherence.

In a computer, bit is a very fundamental concept.Classical computers only have 2 states i.e. 0 or 1 (off and on).Which we consider is a limitation to computation as there are 2 bits.As we have mentioned above, state of an electron in quantum realm has infinite number of possibilities as we use probability to determine the position.Qubit is a representation of state a quantum particle, which can benefit from it's wave nature[5].

A qubit's state can be —0¿ or —1¿, qubit can also have a state of superposition of two wave particles, since waves can combine to form a wave with different sets of amplitudes and frequencies.Because of this superposition phenomenon, a qubit can store 0 and 1 at the same time.Fig 3 represents super position of two waves in a Bloch.and probability of qubit is measured by Greek alphabet 'psi'.

This infinite states in a qubit brought a huge amount of power to quantum computing over classical computing. Algorithms that need lots parallel computing (example: Shor's algorithm) can utilize this power to compute quicker.

Similar to logic gates like AND,OR,XOR in classical computing, Quantum computing architecture will also make use of Quantum gates to perform operations, similar to logic gates using bits, Quantum computers make use of Qubits. Quantum gates make up the quantum circuits.Some examples of Quantum gates are Pauli-X,Pauli-Y,Hadamard and CNOT.There are several gates that operate on multiple qubits.

arbitrary states and described by the wave function shown in

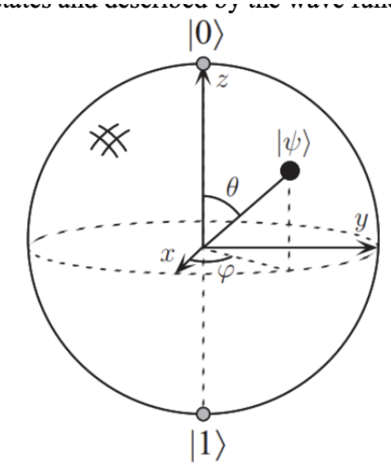


Fig. 3. Superposition of two waves

Quantum Architecture:- Quantum computers are complicated computers that needs isolation from outer environment because quantum particles like free electrons can escape and its coherence can be effected by other particles in environment.So entire system must be made closed box.Decoherence is an important issue in these systems.Decoherence is the phenomenon of losing coherence, Coherence is what enables electrons or waves to work like a computer.Without Coherence, quantum computers cannot function. Maintaining the phase of a particle is also crucial in quantum computing.

Some techniques for controlling and isolating the internal components from external environment are as follows:

Super conductors can conduct energy from one particle to other particle without much resistance.Super conductors are divided into three types prominently they are charge based super conductors,Flux-based super conductors and phase based super conductors.These systems should maintain very low temperatures, which is huge challenge because it is not economical.

Nuclear Resonance is a technique which uses liquid state to store and maintain the states of various quantum bits and quantum gates.

Photon based approaches also provide promising results in maintaining quantum state without any decoherence. Polarization of photons is a method for producing qubits but these polarized photons can infer with other photons that are free.

Trapped atoms are the best possible way when our main concern is decoherence and dephasing.

There are many other methods that we can follow to overcome the challenges.

Table.1 indicated decoherence time for various approaches that are available today.

III. Related Works

In this section, we will introduce few papers on quantum computing architectures and discuss their pros and cons in a structural manner. we will analyse several research papers

No.	Decoherence time (T_2) comparison for various qubits	
	Qubit type	T_2
1	Infrared photon	0.1 ms
2	Trapped ion	15 s
3	Trapped neural atom	3 s
4	Liquid moldecule nuclear spins	2 s
5	e^- spin in GaAs quantum dot	3 µs
6	e^- spin bound to ^{31}P:^{28}Si	0.6 s
7	^{29}Si nuclear spins in ^{28}Si	25 s
8	NV centre in diamond	2 ms
9	Superconducting circuit	4 µs

Fig. 4. Comparison of decoherence times

related to quantum computers, this survey also includes architectures, quantum algorithms, quantum machine learning and quantum cryptography techniques.

[6] Byung et.al.used a 2D architecture as an adder with sqaure root depth complexity and square root qubits for the first time.This paper proved that 2D quantum architecture performed better than 1D architecture.This performs better only when the length of input registers is more than 58.This architecture is more stable and will have more throughput.

[7] Ameen et.al. put forward an architecture that is hybrid in nature, this is a co-quantum computer that is a combination of classical architecture and quantum computer. In this architecture, computational tasks will be divided based on their nature, conventional operations will be handled by classical processors, problems that utilize parallel computation will make use of quantum computer architecture.

[8] Veldhorst in 2017 proposed an approach that utilise CMOS technology for storing qubit state.CMOS transistors will be programmed to work in parallel with qubits in 2 Dimensional quantum computing architecture.Qubit state will be defined by spin of an electron as usual.This is the type of architecture that can be extended to a million qubits.

[9] Kuntam et.al provided a report that compared several problems solved by classical computer with respect to quantum computer.The results showed that a quantum computer performed certain tasks hundreds of times faster than a computer with classical architecture,we will use this paper to understand what kind of tasks a quantum computer can perform better.

[10] This research paper provides an insight into implementing neural networks on to Quantum computers.A new quantum algorithm is implemented to check the neural network efficiency on a quantum computer.This can also be applied for numerous other deep learning and machine learning based approaches.

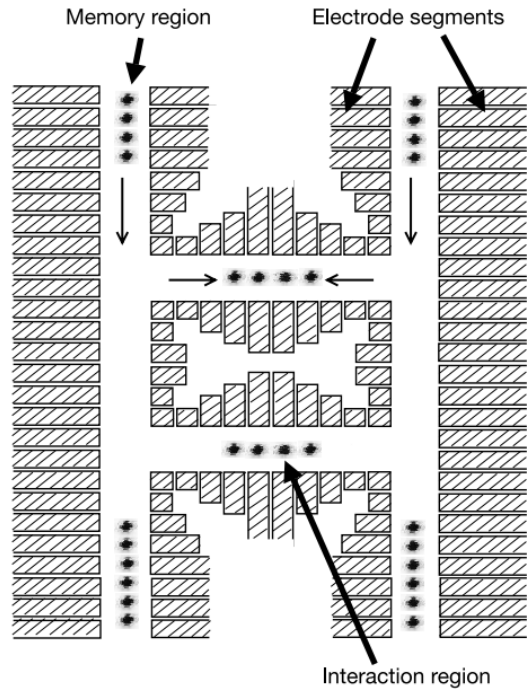


Fig. 5. QCCD Architecture

[22] Architecture for large scale ion trap QC Quantum computers offers a huge leap over classical computers while solving math problems such as finding prime numbers, Riemann zeta functions etc. In order to solve problems like this, a large-scale quantum computer is required. This QC must have architecture with millions of qubits and thousands of quantum gates.

Earlier approaches like [23] used to trap ions in a string like manner, ions in a string are used to transmit states using coulomb interactions between them. However, controlling a string of ions is not a simple task and this cannot be scaled up because of physical constraints.

Wineland [22] et al proposed this approach to solve above limitations, here they have designed an approach that uses number of ion trap registers, instead of using one. They have named this as Quantum charge coupled device (QCCD). This model will have large number of ion traps, and by modifying voltages, ions can be transferred from one trap to higher trap (to lower trap, if voltage is reduced). This ion transfer from one trap to other trap might consume some extra time, small fraction of a clock cycle.

Figure 5 is the basic structure of QCCD, trapped ions are indicated by black dots between various regions, voltage is applied at electrodes to move ions from memory region to interaction region. This ion displacement can perform logic gates in quantum computer, for obtaining entangled states coulomb coupling is to be done.

Like any other QC, decoherence is a major issue in this as well, trapped ions might get interacted with free particles from external environment. In order to avoid decoherence in

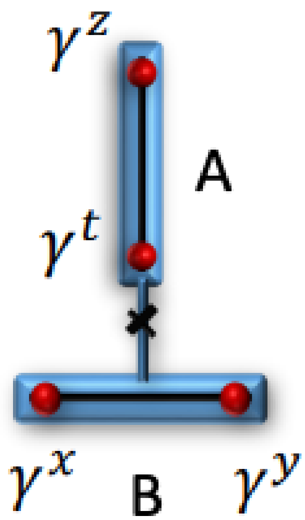


Fig. 6. MZM Architecture

this approach, each qubit is encoded to a decoherence free space of ions. This decoherence free encoding is implemented by Lidar et al in 1998 [24].

Because of encoding for decoherence, we might lose clock synchronization among logic gates, this paper efficiently solved this problem by keeping track of final phase accumulation. Quantum information on physical qubit is stored because of this.

This architecture can have more than ten million qubits, this technique can be scaled to any level of complexity. So, for solving huge mathematical problems, this approach can be used.

Topological Quantum Computation based on Majorana Nanowires:-

[26] Nayak proposed a QC approach that used topological qubits to manipulate the quantum memories and registers. But this approach has some downsides like non local Hilbert space because of no coupling between local operators. Jay et al [25] proposed an approach that overcomes this problem to a certain level for topological qubits.

In this paper, author's propose a universal method for topological QC, by using superconducting nanowires, that hosts Majorana Nanowires (MZM). MZMs can be used to realize a better type of non-abelian defect. It is a genon in Ising X Ising state. Combining these with fermion parities will include a desired topological quantum computer.

Above figure 6 is a simple circuit with nanowire A and B, blue region depicts super conductor. To summarise, this approach provides a better mechanism for protection against

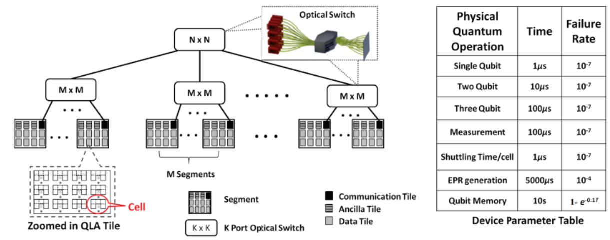


Fig. 7. MUSICQ Architecture

decoherence and helps for better resistance. This research is a significant improvement over previous models that implemented topological quantum computing.

Optimization using Resource Performance simulator:-

This paper mainly focuses on improving existing architectures by optimizing device parameters. Besides this paper also highlights the role played by device parameters, by measuring the performance of a fully error-corrected 1024-bit quantum carry adder based on trapped ions. A simulation tool measures the difference in performance in a Quantum architecture with different device parameters

Figure 7 indicates the architecture of modular scalable universal ion trap quantum computer also known as MUSICQ, tiles that are made of memory cells and BSC (Ballistic shuttling channels) regions are present at the bottom. Transporting qubits among multi quantum gates will be handled by BSC regions. Error correction will be performed regularly to maintain efficiency of a QC. At the next level hierarchy, there are segments, these segments perform complicated gate level operations.

Our simulation and assessment tools consists of two main components. 'Tile Designer and Performance Analyzer' and 'Architecture Designer and performance analyzer' . Both of these two tools work in coordination to measure the performance of a QC with varying DPs.

This paper successfully proved that by improving DP by certain range, we can improve the error performance. This was experimented with shor's algorithm

A Heterogeneous Quantum Computer Architecture:-

[28] is a hybrid quantum computer architecture that has certain classical computing parts. Here classical computing is mostly used for error correction. This paper provides a detailed overview of hybrid architecture.

Through this paper, Fu et al have proved that a hybrid architecture can reduce code overload by improving ESM instructions. Improving control logic has improved number of qubits that parallelly pass through quantum gates.

Network architecture for a topological quantum computer

In this paper, a large-scale surface code quantum processor is designed with respect to network. Here a network is introduced for a semiconductor qubits and minimal node is expected to have seven quantum dots. Dots are defined as particles that has specific electronic properties. Minimal nodes are separated to create space for conventional transistor circuits. Entanglement will be spread among nodes that are neighbors. Every node essentially consists of one qubit of data, and extra dots to accommodate shuttling of electrons.

At the end, Brandon et al proposed a novel quantum computing approach , that used surface code for quantum qubits in a silicon. Here the arrangement of nodes paved way for better processing and performance of a quantum architectures.

Quantum Machine Learning

Data science is one of the crucial and vastly developing fields in current day. There are numerous applications of data science like weather forecast, cancer detection, stock market analysis and other sciences like astronomy, geo spatial are relying on this to a greater extent. Data science mostly use techniques like machine learning, deep learning to solve complex problems. These techniques are nothing but mathematical and statistical analysis of a problem and finding best suitable and probable solutions.

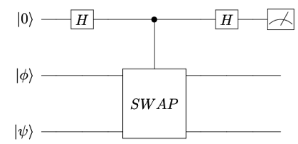
Machine learning techniques are further classified into three types, supervised learning, unsupervised learning and semi supervised learning. Supervised learning is defined as the process of learning with a dataset which has labels and features for certain data points. Most modern algorithms like linear regression etc. are examples of supervised learning. Contrary to supervised learning, unsupervised learning will not have access to any kinds of pre-defined labels or features. Clustering is one of old technique that is an example of unsupervised learning. Semi supervised learning is a process that is in between supervised and unsupervised learnings.

One of the main challenges faced by machine learning applications is runtime and high intensity computing. Most modern machine learning domains like natural language processing and computer vision will have lots of parameters to train on. This consumes plenty of time and memory. In order accommodate these huge requirements, most heavy applications are using Graphics Processing Units (GPU).

Here in this section, we will see how latest advancements in quantum computing has helped data analytics to boost up the performance and time consumption of machine learning approaches. Most machine learning algorithms are an extension to basic linear algebra. Quantum computers are proven to solve linear algebra equations exponentially faster than classical computers. Few examples are Quantum gradient descent and Quantum optimization algorithms.

Quantum Boltzmann architectures makes use of quantum optimization algorithms to solve linear algebra problems efficiently. Other machine learning algorithms like support vector machines (SVM), Principal component analysis can also be implemented in quantum architectures. Besides these few advanced machine learning approaches like Generative adversarial Networks are also implemented in quantum machines, these are named as Quantum Generative adversarial networks, Quantum Auto-encoders and quantum convolutional neural networks etc

Concepts



$$|0\rangle|\phi\rangle|\psi\rangle \to |0\rangle \otimes \frac{1}{2}(|\phi\rangle|\psi\rangle + |\psi\rangle|\phi\rangle) + |1\rangle \otimes \frac{1}{2}(|\phi\rangle|\psi\rangle - |\psi\rangle|\phi\rangle)$$

Fig. 8. SWAP test

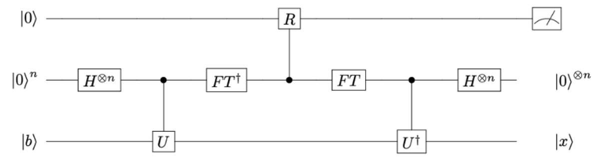


Fig. 9. Quantum Linear equations

Like RAM, quantum computers use QRAM, here each data point is stored as a vector with both magnitude and state representing the data. Hamiltonian simulation is an important technique in quantum machine learning, in this an initial wave function and Hamiltonian constant H are combined to form a quantum circuit.

Amplitude amplification is an important part of Grover's algorithm, this algorithm amplifies the state that is important. This basically converges all states into two categories. Phase estimation is an approach that is used to find the eigen values of a matrix, it is used to solve equations in Quantum computers. Swap test is a method used to find the commonness between two different states, following figure 8 is a framework diagram of swap test,

If qubit value becomes zero, then two states are considered to be equivalent. Other important phenomenon in quantum machine learning is controlled rotation. It is used to bring the eigen values out from their original states. Let's see few machine learning algorithms, that can be implemented in quantum computers.

Machine learning algorithms

One of the most used and basic algorithms, that was solved by quantum approaches is Linear equation (y=mx+b), this algorithm finds x for any given mx=b, the following figure 8 is the quantum representation of system of linear equations

Support Vector Machines

In this algorithm, the data is divided by using a n-1 dimensional hyper plane, prediction will be based on this divided hyper plane. There is a quantum version of this algorithm. Venkataraman et la proved mathematically that, quantum support vector machine algorithm is a huge leap over classical support vector machine.

Principal component analysis

It is one of the machine learning techniques, that is mostly used in reducing dimensions of the data. PCA eliminates the dimensions that do not provide any weight while prediction. Earlier Quantum PCA approaches used Hamiltonian simulation and phase estimation. As we have explained earlier, phase

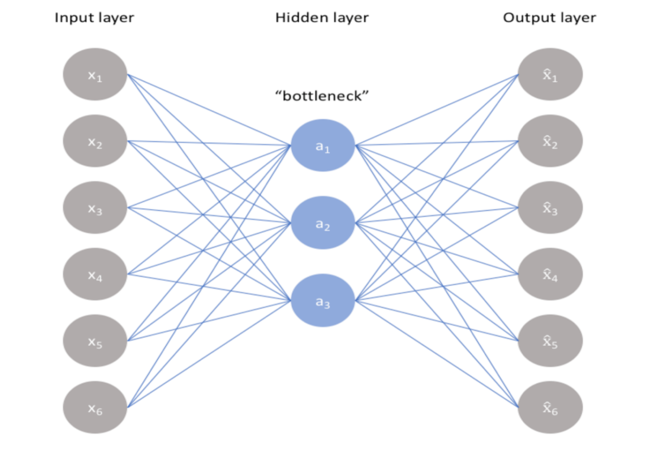


Fig. 10. Auto encoder architecture

estimation can disintegrate the matrix into eigen vectors. Here matrix represents the data points from the data set.

Gradient descent

This is one of the machine learning approaches, that use learning step by step to solve loss function values. Here cost function is also calculated, and it must be more in order for the model to be accurate. It takes polynomial time to execute in classical manner. Since this algorithm has many real-world applications, making a quantum computing version of this algorithm could help us to save a lot of time. Prakash et al proposed a quantized version of this in the year 2017, which has brought down its running time factor by at least hundred.

Generative adversarial networks

Due to increase in dimenstions and database sizes, neural networks are created. Among neural network architectures, GANs are innovative and reliable to find a pattern in data. GANs will have two components. One is generator and other is discriminator. Generator helps in generating the data randomly, discriminator helps in learning process. Discriminator tells generator whether the data it generated is inline or not. These two components work against each other and make a better prediction system.

Since it is heavy to compute, it consumes a lot of time. In order to solve, quantized version of GAN was implemented by Lloyd et al in the year 2015.. This approach saved a huge amount of computation time compared to classical approach

Quantum Auto-encoders

Auto encoders are neural networks that is used in unsupervised scenarios, these essentially will have a bottle neck layer in between input and output layers. This bottle neck layer gets the bare minimum from a input data, from this bare minimum, encoders will try to amplify this to original input level, this entire encoding and decoding helps a model to predict better for datasets with no labels.

Since this is iterating over each data column again and again, it's running time complexity will be in the order of exponential level, so quantum approaches are proposed to reduce the time complexity. So, [32] was proposed in 2018, like other quantized ML approaches, this also performed better in quantum state. Several other sources proved that this worked better a factor of thousand in cases with large sets of data.

Reinforcement Learning

It is a process in which an agent or object tries multiple times to fit in a specified environment, reinforcement learning setting will be mostly based on Markov chains, since a Markov chain is a continuous chain with n number of data points, quantification helps in processing results faster and better.

Initially it was proposed in the year 2008, in this approach has two Hilbert spaces are Hs and Ha, because of these two Hilbert spaces, eigen values can be extracted easily by using these Hilbert spaces, quantum computing is a technology that takes advantage of using Hilbert spaces.

This also uses the approach that makes use of probability functions, this probability can be used in deciding the tradeoff between exploration of dataset and exploitation of data in a reinforcement learning environment.

This tradeoff can be settled in classical computing by using the probabilistic functions, but probabilities cannot be used in quantum computing architectures. In order to settle tradeoffs, we need to make use of eigen values in data set matrix, as we have already put forward, we have to consider as a vector with some magnitude and direction in a Hilbert space. Eigen values are figured out using super position phenomenon in a quantum computing architecture.

The above approach is called as action collapse and here super position state forms a eigen value of the vector. In further steps, probability is amplified by using amplitude amplification technique that we have discussed in above section. It is mostly like Glover's algorithm, the probability of a single action should in directly proportional to action value, whereas in Glover's algorithm, it is proportional to 1. So, high probabilities mean higher chance of predicting that label.

Open problems in Quantum machine learning

Even with rapid improvements in quantum computing, there are several problems which quantum computers cannot solve, Gaussian kernels can be implemented for nonlinear systems, since kernels are polynomials. Besides this, there are several other problems that are NP hard, L0 normalization is an example of this. Similar to this L1 norm cannot be solved by using quantum architectures, this L1 norm is extensively used in few classical ML algorithms like SVM, linear regression because these are dependent on least squares.

Noise is an important issue in optimization techniques, since noise might get given priority instead of giving priority, noise is still a major issue in quantum computing as well. There are few machine learning algorithms that works better with very less rows of data, these might not work better in case of quantum computing.

Data augmentation is the process of creating new data that fits in a certain manner, that obeys the original pattern. This task is easier for classical computing whereas for quantum computing, this is a very challenging task. Quantum com-

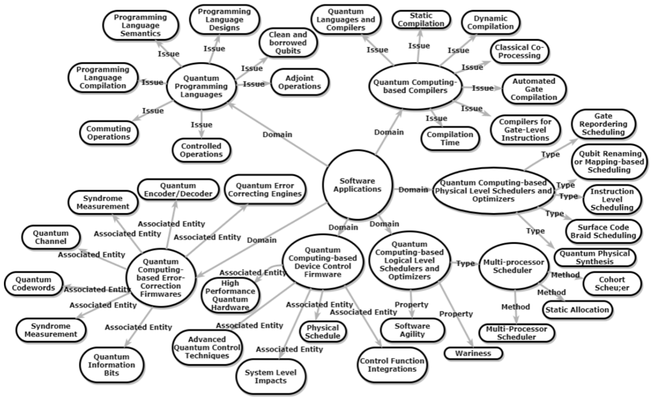


Fig. 11. Quantum Applications

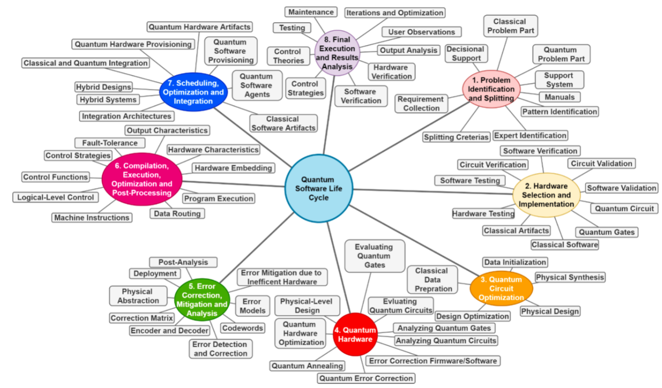


Fig. 12. Quantum Software Lifecycle

putations can simulate simple rotations, but for simulating complicated pools QC cannot be relied upon.

Zero shot learning is an important aspect in machine learning, that learns frequent pattern in a reasonable time frame. This kind of approaches are easier in a classical computing, whereas in a quantum computer, they are much slower. Another challenge is for reinforcement learning, quantum computing architecture cannot set in a reinforcement environment. We conclude this section by stating , Quantum computing can be reliable and makes an application faster in certain cases, but there are other corner cases where classical computing is better that quantum computing.

Quantum Computing and its applications

Above is a mapping figure of quantum computing used in modern real-world applications, in this section we will see how quantum computers are performing and improving efficiency of several domains

Quantum based Compilers: In this domain several research papers are published in recent years, Compilers for gate logic, dynamic compilation, Automated gate compilation are some of the attributes of quantum compilers, in these aspects' quantum compilers perform better than classical compilers. There are few challenges for designing quantum compilers, they include hybrid models that can interact with classical computers in order to follow the instructions of an algorithm step by step. Another challenge is to design compilers that can perform well in terms of latency, computation cost etc. Economic reasons are also concern for these kinds of compilers.

Quantum Schedulers and Optimizers:

Few research papers were published in this domain, that make use of quantum architectures to improve several CPU tasks like scheduling, optimizing the performance of a computer. [33] proposed a novel architecture for implementing quantum schedulers and optimizers that perform better that several classical scheduling techniques. [33] discussed the importance of quantum scheduler and optimizers in fault tolerant quantum architectures like topological QCs. The processors will consume logical operations besides qubits and quantum gates. This paper concluded by proving authentic quantum nodes perform better than regular quantum nodes.

Quantum Software Engineering

There are several papers proposed on this domain, which include various steps in life cycles like quantum requirements, quantum logic gates design, quantum hardware building, quantum programming, quantum software quality attributes. Besides these, this domain also works out the syntax, semantics of a quantum programming languages and develops architecture that perform better and computationally economical.

Below is a figure that depicts the branches and sub branches in a quantum software development life cycle. Unlike any software life cycle, this has 8 important nodes.

1.Problem Identification

2. Hardware Selection

3. Circuit Optimization

4. Hardware development

5. Error Correction

6. Execution/Compilation

7. Scheduling

8. Final Execution and Result Analysis

Quantum Cryptography

The most important application of Quantum computing is Cryptographic tools development. With everyday quantum computers are getting closer to our lives, with easy access to these complex machines, there will be a risk of misuse.

Most encryption algorithms like AES etc., can be broken by using modern quantum computers using brute force attacks. In order to save user privacy from quantum computers, itself is used against it to prevent data losses and breaches.

In this section, we will see several cryptographic approaches where quantum computing will have advantage

Quantum key distribution:

QKD is an approach used to protect key from going into attackers, it works a regular key distribution algorithm, where two parties will mutually agree for key exchange. But this entire happens in quantum environment, in a quantum computer, there is no chance any two systems to have a similar quantum particle alignment, Quantum key distribution mainly depends on this effect. This is called as No-Cloning theorem.

Below is a table that depicts different QKD approaches and their corresponding pros and cons.

Type of CV-QKD	Pros	Cons
Gaussian-modulated CV-QKD	• Security analysis is much more advanced compared to discrete-modulated CV-QKD.	• Distance limitation for secure QKD is a major concern. • The use of high-performance error-correcting code can improve security but reduces the distance coverage [148].
Discrete-modulated CV-QKD	• More suitable for long-distance secure key transmission. • Simple experimentation setup. • Great potential for large-scale deployment in secure quantum networks. • The integration of post-selection strategies with reverse reconciliation can significantly improve the key rates.	• Security analysis in this system is more challenging compared to Gaussian-modulated CV QKD because analysis relies on the linearity of the channels which is not an easy condition for verification.
Coherent On-Way (COW) Quantum Key Distribution	• Simple in experimentation • Reduce interference visibility • Avoid photon number splitting attack to a large extent • Falls in distributed-phase-reference QKD category	• Empty pulses contain a light that can introduce noise. This can increase error rates. • Performance decreases with an increase in disturbances. Small disturbances do not affect performance.
Differential Phase-Shift (DPS) Quantum Key Distribution	• Falls in distributed-phase-reference QKD category. • Integration with randomness or improved transmitter can reduce the disturbances and improve the performance [151] [152].	• Chances of side-channel attacks are higher. Thus, techniques (e.g. attenuation) are required to be integrated for removing it. • Performance decreases with an increase in disturbances. Small disturbances do not affect performance.

TABLE I
QUANTUM KEY DISTRIBUTION TECHNIQUES

Type of CV-QKD	Pros	Cons
Gaussian-modulated CV-QKD	• Security analysis is much more advanced compared to discrete-modulated CV-QKD.	• Distance limitation for secure QKD is a major concern. • The use of high-performance error-correcting code can improve security but reduces the distance coverage [148].
Discrete-modulated CV-QKD	• More suitable for long-distance secure key transmission. • Simple experimentation setup. • Great potential for large-scale deployment in secure quantum networks. • The integration of post-selection strategies with reverse reconciliation can significantly improve the key rates.	• Security analysis in this system is more challenging compared to Gaussian-modulated CV QKD because analysis relies on the linearity of the channels which is not an easy condition for verification.
Coherent On-Way (COW) Quantum Key Distribution	• Simple in experimentation • Reduce interference visibility • Avoid photon number splitting attack to a large extent • Falls in distributed-phase-reference QKD category	• Empty pulses contain a light that can introduce noise. This can increase error rates. • Performance decreases with an increase in disturbances. Small disturbances do not affect performance.
Differential Phase-Shift (DPS) Quantum Key Distribution	• Falls in distributed-phase-reference QKD category. • Integration with randomness or improved transmitter can reduce the disturbances and improve the performance [151] [152].	• Chances of side-channel attacks are higher. Thus, techniques (e.g. attenuation) are required to be integrated for removing it. • Performance decreases with an increase in disturbances. Small disturbances do not affect performance.

TABLE II
MULTI VARIATE CRYPTOSYSTEM TECHNIQUES

Multi variate cryptosystem

In this system, NP hard and NP complete problems are evaluated. The efficiency of a multi variate system depends on ease with which it can solve quadratic equations over a certain order. One-way functions comprise of multiple map functions that could end up in a invert function without much awareness single sub functions. Multi variate crypto systems existed even before post quantum cryptosystems. This has better performance than post quantum cryptosystems and these put lesser load on computations.

Below is a table that compares various multi variate cryptosystems and provide their strengths

IV. FUTURE WORKS

With all the developments in quantum computing, it is constantly improving and reaching all the new domains and changing the future of it rapidly, In this section we will see few fields that are getting developed because of inception of quantum computing methodologies. Few authors have researched and observed the curve that indicates the hype for quantum computing.

Since it has certain futuristic and advanced aura to it, most people are developing techniques for these, even when there is no actual use for quantum computing. These types of unnecessary applications do not help anyone in any way. In fact they would pull back the technology.

Below is the hype graph depicted for quantum computing

Everything starts with a trigger; in this case it is innovation. This develops interest rapidly, where everyone thinks quantum

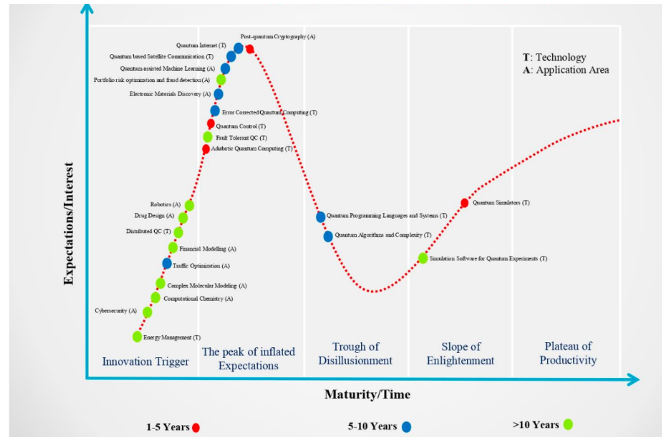


Fig. 13. Hype curve

computing is the solution for every problem. After exponential increase in hype, it reaches peak, after reaching the hype gradually falls due to disillusionment. Once it reaches all time low, then the actual progress of a technology raises, later it reaches to a new state called Plateau of productivity. Most stable applications of Quantum computing.

Coming to its endeavors, list is long, in this report, we have reviewed and analyzed various domains in which quantum computing played a major role in solving problems, that were once thought as impossible. It has done a lot to fields like Machine learning, Network security, algorithmic computations, finding prime numbers to trillion and various mathematical conjectures.

V. CONCLUSION

Through this survey, we have gone through several quantum computing journals, articles, research papers and other surveys and we have conclusively proved the importance of Quantum computing for future works.

Several fields like Quantum Cryptography, Quantum Internet, Robotics, Numerical weather prediction, Quantum Cloud computing and cryptography are currently in developing phase. Through advancements in Quantum realm, all of these have achieved progress in greater level than expected.

This paper presents a systematic review of quantum computing architectures, its important applications in Data science field, Cryptography. The main intention of this paper is to guide people with no knowledge in quantum computing to understand the working of it and how modern applications are harnessing its power to build a better computing future.

Modern tech giants like google, IBM and Microsoft are investing billions of dollars every year, for building, designing quantum computers, that are destined to serve common people some day in the future. Quantum computers are energy efficient than complex super computers. As the world is progressing towards carbon neutrality, quantum computers must be huge asset in the future.

VI. References

1.David Deutsch. Quantum theory, the church–turing principle and the universal quantum computer. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 400(1818):97–117, 1985.

2.Frederic T Chong, Diana Franklin, and Margaret Martonosi. Programming languages and compiler design for realistic quantum hardware. Nature, 549(7671):180–187, 2017.

3.Donald A Sofge. A survey of quantum programming languages: History, methods, and tools. In Second IEEE International Conference on Quantum, Nano and Micro Technologies (ICQNM 2008), pages 66–71, 2008.

4.Richard P. Feynman, "Simulating physics with computers," International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982.

5.Charles H. Benett, and David P. DiVincenzo, "Quantum Information and computation," NATURE, Vo. 404, 16 March 2000.

6.Byung-Soo Cho, and Rodney Van Meter, "An depth quantum order on the 2d ntc quantum computer architecture," Quantum Information and Computation, Vol. 0, No. 0, 2010.

7.E. M. Ameen, H. A. Ali, and A. Osman, "Proposed architecture for conventional computer with co-quantum processor," International Journal of Scientific Engineering, Research, Vol. 5, Issue 8, ISSN 2229-5518, Aug 2014.

8.M. Veldhorst, H. G. J. Eenink, C. H. Yang and A. S. Dzurak, "Silicon CMOS architecture for a spin-based quantum computer," NATURE COMMUNICATIONS, 8, 1766, 2017

9. Kuntam Babu Rao, "Computer systems architecture vs quantum computer," IEEE, International Conference on Intelligent Computing and Control Systems, ICICCS 2017.

10. Adenilton J. da Silva, and Rodolfo Luan F. de Oliveira, "Neural networks architecture evaluation in a quantum computer," IEEE, Brazilian Conference on Intelligent Systems, Oct 2017.

11.D. Kielpinski, C. Monroe, and D. J. Wineland, "Architecure for a large-scale ion-trap quantum computer," NATURE, Vol. 417, June 2002.

12.Peter W. Atkins, and Ronald S. Friedman, "Molecular quantum mechanics," OUP Oxford, 2011.

13.Julio Guemez, and Manuel Fiolhais, "Relativistic description of the photoelectric effect," American Journal of Physics, 86(11):825-830, November 2018.

14.Ziya Saglam, Gokhan Sahin, and Bahadir Boyacioglu, "Compton effect in terms of spintronic," Results in Physics 6, 726-727, 2016.

15.David J. Griffiths, and Darrel F. Schroeter, "Introduction to quantum mechanics," Cambridge University Press, 2017.

16.T. D. Ladd, et al. , "Quantum computers," NATURE, Vol. 464, 4 March 2010.

17.P. Michler, et al. "A quantum dot single-photon turnstile device," SCIENCE, Vol. 290, 22 Dec 2000.

18.C. Monroe, et al. "Large scale modular quantum computer architecture with atomic memory and photonic interconnects," Physical Review A 89, 022317, 13 Feb 2014.

19.Maissam Barkeshli, and Jay D. Sau, "Physical architecture for a universal topological quantum computer based on a network of majorana nanowires," arXiv, 1509.07135, 2015.

20.Eyob A.Sete, et al. "A Functional Architecture for Scalable Quantum Computing", IEEE, International Conference on Rebooting Computing, 2016

21. Norbert M. Linke, et al. "Experimental comparison of two quantum computing architectures,",Proceedings of National Academy of Sciences,2017

22. D. Kielpinski, C. Monroe, and D. J. Wineland, "Architecure for a large-scale ion-trap quantum computer," NATURE, Vol. 417, June 2002.

23. Cirac, J. I. Zoller, P. Quantum computations with cold trapped ions. Phys. Rev. Lett. 74, 4091–4094 (1995).

24. Lidar, D. A., Chuang, I. L. Whaley, K. B. Decoherence-free subspaces for quantum computation. Phys. Rev. Lett. 81, 2594–2597 (1998).

25. Maissam Barkeshli, and Jay D. Sau, "Physical architecture for a universal topological quantum computer based on a network of majorana nanowires," arXiv, 1509.07135, 2015.

26. C. Nayak, S. H. Simon, A. Stern, M. Freedman, and S. D. Sarma, Rev. Mod. Phys. 80, 1083 (2008).

27. Muhammad Ahsan, and Jungsang Kim, "Optimization of quantum computer architecture using a resource-performance simulator," Design, IEEE Automation Test in Europe Conference and Exhibition (DATE), 23 Apr 2015.

28. X. Fu, et al. "A hetrogenous quantum computer architecture," CF '16 Proceedings of the ACM Internatiuonl Conference on Computing Frontiers, Pages 323-330, 16 May 2016.

29. Brandon Buonacorsi, et al. "Network architecture for a topological quantum computer in silicon," Quantum Science and Technology, 2018

30. Kerenidis, I., and Prakash, A. Quantum gradient descent for linear systems and least squares.

31. Lloyd, S., and Weedbrook, C. Quantum generative adversarial learning. Physical review letters (2018),040502

32. Khoshaman, A., Vinci, W., Denis, B., Andriyash, E., and Amin, M. H. Quantum variational autoencoder. arXiv:1802.05779v1 [quant-ph] (2018).

33. Oskin, M., Chong, F.T. and Chuang, I.L., 2002. A practical architecture for reliable quantum computers. Computer, 35(1), pp.79-87.

34. Ekert, A.K., 1991. Quantum cryptography based on Bell's theorem. Physical review letters, 67(6), p.661.

35. Ghalaii, M., Ottaviani, C., Kumar, R., Pirandola, S. and Razavi, M., 2020. Discrete-modulation continuous-variable quantum key distribution enhanced by quantum scissors. IEEE Journal on Selected Areas in Communications, 38(3), pp.506-516.