Quantum-Safe Cryptography: Mitigating Vulnerabilities in Post-Quantum era

Table of Contents

[Task 1: Research Post-Quantum Computational Ability 1](#_Toc173681620)

[Computational Ability and Efficiency 1](#_Toc173681621)

[Economic Feasibility 2](#_Toc173681622)

[Challenges and Constraints 3](#_Toc173681623)

[Cost Constraints 3](#_Toc173681624)

[Time Constraints 4](#_Toc173681625)

[Technological Constraints 4](#_Toc173681626)

[Task 2: Outline Post-Quantum computational Limit 5](#_Toc173681627)

[Errors and Reliability 5](#_Toc173681628)

[Benchmark Standards 5](#_Toc173681629)

[Threats and Vulnerabilities 5](#_Toc173681630)

[Usability and Calculation Powers 6](#_Toc173681631)

[General Risks 6](#_Toc173681632)

[References 6](#_Toc173681633)

# Task 1: Research Post-Quantum Computational Ability

There is no denying to the fact that quantum computing is able to revolutionize various sectors in the coming years by allowing them to solve complex problems beyond the reach of classical computers. In order to discuss it in detail, the segregation have been done into different sections like computational ability and efficiency, economic feasibility and production value, cost and other related constraints, calculation ability and other challenges that are primarily faced.

## Computational Ability and Efficiency

It is evident that quantum computers are likely to take part in the coming future owing to the increased data volume and cryptographic calculations to make sure business operations are carried out in an efficient manner. There is no denying to the fact that quantum computers mainly works on the basis of qubits which means it is able to exist in multiple states simultaneously. As a result of its existence in the multiple states, it helps in providing higher computational power (Desdentado et al., 2024). As per the current scenario, the development is emphasized on transitioning from physical qubits to the error-corrected logical qubits which means it is able to improve overall stability and reliability. This paradigm is of utmost importance as it will make sure practical quantum computations is able to supersede classical super computers, especially when it comes to simulations as well as optimization problems. Even for the computational scientists as well as other researchers also, the use of quantum computers can be done which will allow them in tacking large scale problems in an easy manner (IBM, 2024).

In terms of efficiency, it can be said that quantum computing is able to offer a powerful experience to organizations with its unparalleled computational process, making it easy for tacking a wide range of problems. For instance, in terms of financial modeling, it can be said that quantum computing is able to transform it based on two dissimilar elements like risk evaluation and portfolio optimization and real-time trading. In the context of risk assessment and portfolio optimization, this technology will aim to strike an optimal balance amongst a risk and a return by handling colossal data amounts concurrently. The use of algorithms like **Quantum Approximate Optimization Algorithm (QAOA)** could be done which is capable of traversing multi-faceted landscape of financial data in an efficient manner. Even though the financial organizations are able to identify optimal portfolios in a fraction of the time taken by traditional trading algorithms. In the figure given below, the use of Quantum computing for boosting Monte Carlo simulations have been shown that shows how it creates a distribution curve through an iterative process of previous simulations (Hock, 2024).

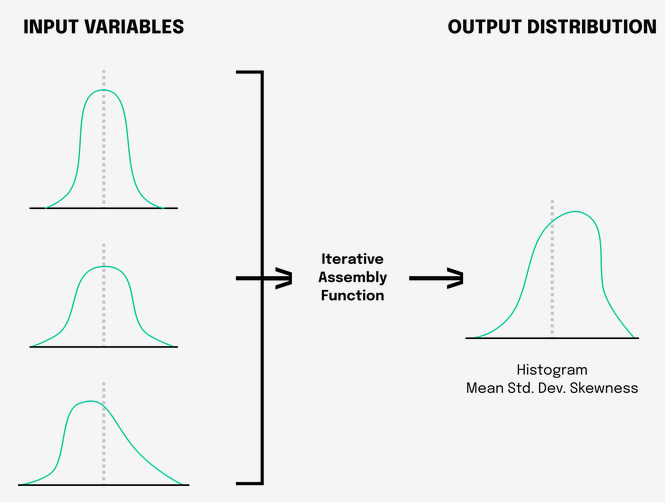


Figure 1: https://neosfer.de/en/quantum-computing-the-use-cases-for-the-future-of-computing/

On the other hand, in the case of trading and pricing of assets, traditional algorithms are not able to remain updated with real-time market data that results in delayed decision making and even lost opportunities. However, with quantum computing technology, it helps in analyzing the processes in real-time in a faster speed for taking informed trading decisions (Hock, 2024). Apart from financial use case, the use of quantum computing can also be done in the context of cryptography, cyber security, flight simulations, climate science, and other eco-friendly technologies for great opportunities. Therefore, it clearly shows how efficient the quantum computing technology is and with the passage of time, how efficient it will become in future (Golec et al., 2024).

## Economic Feasibility

In terms of economic feasibility of quantum computing, it can be said that it is a multi-faceted topic which is mainly driven by significant investments made in it, its market size, and its anticipated value across multiple sectors. In terms of its market potential, it has been asserted that quantum computing is expected to accelerate by several folds in future which will be around $450 billion to $850 billion by the end of 2040. Although this growth will also provide a support to the market worth $90 billion to $170 billion when it comes to hardware and software related resources (Bobier et al., 2024). These projections have been made in relation to the quantum computing’s ability to perform very complex computational problems faster than existing computers with proper handling. These areas mainly include logistics optimization related problems, drug discoveries, and even other advanced simulation systems (O’Halloran, 2023). Particularly, for the year 2023, a lot of investments have been made in quantum computing technology by startup companies which had reached almost $1.70 billion despite a decline in tech related investments. This figure clearly shows that there is a strong investor confidence in the long term potential of quantum computing and other associated technologies. Along with such investments, the public funding have also been increased which holds almost $35.5 billion in global investments. Almost all big countries like the United States, China and European region are increasing their funding in order to establish technological leadership as well as foster a culture of innovation (Bogobowicz et al., 2024).

## Challenges and Constraints

This section is basically divided into two different sub-sections such as challenges and constraints of quantum computing technologies.

### Cost Constraints

As the quantum computing technology is emerging, the development and deployment costs for the same are significant because of its complex nature and a dire need for specialized materials and hardware. When it comes to development, it mainly requires higher initial cost because there would be a need for investing in research and development centers (R&D), purchasing specialized equipment, and other advanced materials for constructing qubits. For instance, if there is a need for setting up a quantum computer that is able to maintain the lower temperatures, there would be need for such qubits for maintaining cooling systems because they are expensive and even energy intensive. Despite the higher initial cost, it also requires substantial investment which means there would be need for people to invest in it and it is even increasing, but has not increased the baseline mark (Golec et al., 2024).

### Time Constraints

Basically, the timeline that have been prepared for mass producing quantum computers have been segregated into three different phases such as NISQ, Broad and even full scale. All these phases have been explained below in a detailed manner.

* NISQ Era, also known as **Noisy Intermediate Scale Quantum** is the first phase which will be completed by the end of 2030. The main focus of this phase is on improving qubits counts as well as fidelity.
* The next phase is **Broad Quantum Advantage** which is expected to be completed amongst 2030 and 2040 where quantum computers will be able to start outperforming all classical computers in different case scenarios.
* The last phase is **Full Scale Fault tolerance** post 2040 where it will solely emphasize on for being robust and error correct quantum systems that is able to handle a wide range of applications in an efficient manner (Gill & Buyya, 2024).

### Technological Constraints

In the context of technology, there are a lot of technological constraints that are likely to impact this technology. The first one is stability and coherence of qubits where the maintenance of such bits is a great challenge. These bits are extremely sensitive to the environment which means it can cause errors if disturbance is faced. Another major constraint is related to the error correction where qubits require complex error correction algorithms to make sure computations are carried out. If there is no such algorithms, it is likely to face higher complexity and even errors. Lastly, for scaling up also, there would be a need for integration of millions of qubits and to do so, the technology like diamond micro-chiplets is required (Rieffel et al., 2024).

# Task 2: Outline Post-Quantum computational Limit

Basically, there are two phases for a technology, the first one is emerging and the second one is matured. Subsequently, in the case of quantum computing also, it is at an early stage which means it is currently emerging and would take a lot of years to fully matured over pentane decades. Along with this, there are several computational limits with its early stage in the context of errors, threats, vulnerabilities, reliability and even benchmark standards.

## Errors and Reliability

In the context of errors and reliability, it can be said that these systems are highly susceptible to errors owing to de-coherence and quantum noise. Basically, de-coherence refers to the qubits which loses their quantum state when there is an interaction with an environment. There are a lot of error correction methods available but a majority of them are under development and even require physical qubits in order to make sure proper error control is made possible. In some cases, there may not be qubits available for computation that means qubits will not be available (Claudino et al., 2024).

## Benchmark Standards

When it comes to benchmark standards, currently, the emphasis is laid on quantum volume which means the measuring can be done based on largest random circuit of equal width and depth. When such metrics have been set, then the quantum computer can be implemented successfully. In the context of IBM quantum computer also, they have been able to achieve a quantum volume of 128 which clearly shows their improvements when it comes to error rates and gate fidelities (Mimona et al., 2024).

## Threats and Vulnerabilities

Cyber security is considered as one the foremost requirements for all technologies and for quantum computing also, quantum computers are likely to pose both direct and indirect security threats. In the case of direct threats, the security attacks are faced on quantum hardware, for example, noise injection and even qubit tampering. On the other hand, for indirect security threats, it stem from the computational capabilities of such computers so as to break cryptographic algorithms. As a result of this, it compromise cyber security infrastructure, leading to downtime. Some widely accepted vulnerabilities have been found that have the ability to break encryption like RSA and ECC which clearly threatens secure communications and data protection. For hardware also, the hardware can be exploited by cyber attackers based on inducing errors and control qubits states that could further affect reliability of computations (Yu et al., 2024).

## Usability and Calculation Powers

There is a limited usability for quantum computers in today’s world based on their complexity level and there would be a need for a specialized knowledge in order to operate such computers easily. There would be a need for having a proper knowledge regarding technologies and environment so as to make sure quantum computers could be used in an easy manner. Also, for the calculation powers, it has an ability to solve the specific problems from classical computers. On the other hand, for practical implementation, there is still no solutions available for it (Sood & Chauhan, 2024).

## General Risks

The list of all general risks that could be faced with quantum computing technology mainly include:

* In the case of technological maturity, it is still immature and there is a major need for advancements to make sure it can be adopted by the organizations (Yu et al., 2024).
* For the economic viability also, there is a higher cost of developing and maintaining quantum computers owing to their economic risks due to the limited access.
* Even there is a shortage of professionals who have expertise with quantum computing which means it lacks professionals for working (Claudino et al., 2024).

# References

Bobier, J.-F., Langione, M., Naudet-Baulieu, C., Cui, Z., & Watanabe, E. (2024, July 18). *The Long-Term forecast for quantum computing still looks bright*. www.bcg.com. https://www.bcg.com/publications/2024/long-term-forecast-for-quantum-computing-still-looks-bright

Bogobowicz, M., Dutta, K., Gschwendtner, M., Heid, A., & Issler, M. (2024). Steady progress in approaching the quantum advantage. In *McKinsey & Company*. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage

Desdentado, E., Calero, C., Moraga, M. Á., Serrano, M., & García, F. (2024). Exploring the trade-off between computational power and energy efficiency: An analysis of the evolution of quantum computing and its relation to classical computing. *Journal of Systems and Software*, 112165. https://doi.org/10.1016/j.jss.2024.112165

Gill, S. S., & Buyya, R. (2024). Transforming Research with Quantum Computing. *Journal of Economy and Technology*. https://doi.org/10.1016/j.ject.2024.07.001

Golec, M., Hatay, E. S., Golec, M., Uyar, M., Golec, M., & Gill, S. S. (2024). Quantum Cloud Computing: trends and challenges. *Journal of Economy and Technology*, *2*, 190–199. https://doi.org/10.1016/j.ject.2024.05.001

Hock, R. R. U. J. (2024, March 7). *Quantum Computing: The use cases for the future of computing*. Neosfer. https://neosfer.de/en/quantum-computing-the-use-cases-for-the-future-of-computing/

IBM. (2024). *What is quantum utility? | IBM Quantum Computing Blog*. https://www.ibm.com/quantum/blog/what-is-quantum-utlity

O’Halloran, D. (2023, November 7). *State of Quantum Computing: Building a quantum economy*. World Economic Forum. https://www.weforum.org/publications/state-of-quantum-computing-building-a-quantum-economy/

Rieffel, E. G., Asanjan, A. A., Alam, M. S., Anand, N., Neira, D. E. B., Block, S., Brady, L. T., Cotton, S., Izquierdo, Z. G., Grabbe, S., Gustafson, E., Hadfield, S., Lott, P. A., Maciejewski, F. B., Mandrà, S., Marshall, J., Mossi, G., Bauza, H. M., Saied, J., . . . Biswas, R. (2024). Assessing and advancing the potential of quantum computing: A NASA case study. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2024.06.012

Claudino, D., Lyakh, D. I., & McCaskey, A. J. (2024). Parallel quantum computing simulations via quantum accelerator platform virtualization. *Future Generation Computer Systems*, *160*, 264–273. https://doi.org/10.1016/j.future.2024.06.007

Mimona, M. A., Mobarak, M. H., Ahmed, E., Kamal, F., & Hasan, M. (2024). Nanowires: Exponential speedup in quantum computing. *Heliyon*, *10*(11), e31940. https://doi.org/10.1016/j.heliyon.2024.e31940

Sood, V., & Chauhan, R. P. (2024). Quantum computing: Impact on energy efficiency and sustainability. *Expert Systems With Applications*, *255*, 124401. https://doi.org/10.1016/j.eswa.2024.124401

Yu, J. Y., Sim, W. S., Jung, J. Y., Park, S. H., Kim, H. S., & Park, Y. R. (2024). Evaluation of conventional and quantum computing for predicting mortality based on small Early-Onset Colorectal Cancer data. *Applied Soft Computing*, 111781. https://doi.org/10.1016/j.asoc.2024.111781