



GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

Aplicación del fenómeno Quantenverschränkungen en Ingeniería de Telecomunicación

Autor: Iván Sánchez Pérez

Director: Prof. Dr. Cristina Puente Águeda

Madrid

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título
“Aplicación del fenómeno Quantenverschränkungen en Ingeniería de Telecomunicación”
en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el
curso académico 2023/24 es de mi autoría, original e inédito y
no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido
tomada de otros documentos está debidamente referenciada.



Fdo.: Iván Sánchez Pérez

Fecha: 02/ 06/ 2024

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO



Fdo.: Prof. Dr. Cristina Puente Águeda

Fecha: 02/ 06/ 2024



GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

Aplicación del fenómeno Quantenverschränkungen en Ingeniería de Telecomunicación

Autor: Iván Sánchez Pérez

Director: Prof. Dr. Cristina Puente Águeda

Madrid

Agradecimientos

Quiero agradecerles a Carmen y Alfredo, mis padres, todo su sacrificio y entrega para que tuviera la mejor formación humana y académica; los valores que me han inculcado siempre para convertirme en quien hoy soy.

A Leticia y Carla, mis hermanas, por estar siempre a mi lado y confiar en mí.

A mis abuelos, por su cariño y amor incondicional. En especial Luis, mi abuelo materno, del que sé que hoy está orgulloso desde el cielo. Su ejemplo y legado están siempre conmigo.

Conchita, mi querida tutora de Primaria, gracias por tanta dedicación y disciplina.

Cristina, directora del presente TFG, por desarrollar y guiar mi potencial investigador. Paloma, Lucía y Alfonso, profesores, por su inestimable tiempo y consideración.

CL Duque, mi hermano, alias dictus Zatoichi, en la enseñanza de un espíritu: “Somos héroes incógnitos todos,...El correr de la vida forjó” —aquellos que nunca piden nada para sí mismos.

Epílogo, quiero dar las gracias a Dios y a la Virgen María por ayudarme siempre.

APLICACIÓN DEL FENÓMENO QUANTENVERSCHRÄNKUNGEN EN INGENIERÍA DE TELECOMUNICACIÓN

Autor: Sánchez Pérez, Iván.

Director: Puente Águeda, Cristina.

Entidad Colaboradora: ICAI – Universidad Pontificia Comillas.

RESUMEN DEL PROYECTO

Este proyecto de investigación explora la aplicación del entrelazamiento cuántico y la computación cuántica en la Ingeniería de Telecomunicaciones. Mediante una revisión de protocolos de comunicación basados en la Distribución Cuántica de Claves (QKD), como el BB84 y BBM92, se analizan los principios fundamentales y el uso de la Física Cuántica para garantizar la seguridad en las comunicaciones modernas. Asimismo, se desarrolla un modelo cuántico para la optimización de portafolios utilizando la herramienta de programación Qiskit de IBM. Los resultados obtenidos sugieren ventajas del modelo cuántico en comparación con enfoques clásicos, aunque con tiempos de ejecución más extensos a medida que aumenta el número de activos.

Palabras clave: Computación Cuántica, Quantum-as-a-Service, QKD, Qiskit, Optimización de Portafolios, Toma de Decisiones, Cambio de Paradigma, Inversiones de Capital, Economía Digital.

1. Introducción

Partiendo de los fundamentos que sustentan la Ingeniería de la Telecomunicación en su forma más convencional, incluyendo su método de investigación científica, que comparte sus fundamentos con la Física, comprendemos de repente cómo los bits, que son el objeto fundamental de información en la comunicación clásica, se transforman en qubits o bits cuánticos como el objeto fundamental de información en la comunicación cuántica [1].

Cambio de paradigma: Mientras que un bit puede tener el valor 0 o 1, un qubit puede tener un valor que es 0 o 1 o una superposición cuántica de 0 y 1 a la vez.

Un qubit, al igual que un simple bit, contiene toda la información necesaria para describir el estado de una variable binaria. La computación cuántica trata de dar respuesta a algunos de los desafíos más apremiantes en diversas áreas, que abarcan desde las comunicaciones, la energía y la salud, hasta la agricultura, las finanzas y la ciencia de materiales, entre otros [2]. Esto se debe a que a medida que los desafíos se vuelven más complejos y demandantes, la eficiencia de la informática convencional disminuye debido a sus límites en la capacidad de procesamiento. En este contexto, las aplicaciones cuánticas emergen como una solución prometedora.

2. Definición del proyecto

El objetivo principal de este proyecto es investigar la aplicación del fenómeno de entrelazamiento cuántico en la Ingeniería de Telecomunicación. Para lograrlo, se establecen tres objetivos específicos:

1. Explorar protocolos de comunicación basados en la Distribución Cuántica de Claves (QKD), e.g. BB84 y BBM92, analizando sus principios fundamentales y su uso en sistemas de telecomunicación modernos.
2. Desarrollar un modelo cuántico para la optimización de portafolios utilizando el lenguaje de programación Qiskit de IBM. Se comparan dos escenarios: uno con 5 acciones y otro con 20 acciones, evaluando la composición del portafolio, los rendimientos obtenidos y, los tiempos de ejecución entre el modelo clásico y cuántico.
3. Sentar las bases para futuras investigaciones entre el campo de la Ingeniería de Telecomunicación y la Computación Cuántica, estableciendo un punto de partida y referencia para proyectos posteriores.

3. Descripción del Sistema/Modelo

El protocolo BB84, desarrollado por Charles Bennett y Gilles Brassard en 1984, es uno de los protocolos QKD más importantes y conocidos. El esquema básico del protocolo BB84 se puede describir de la siguiente manera:

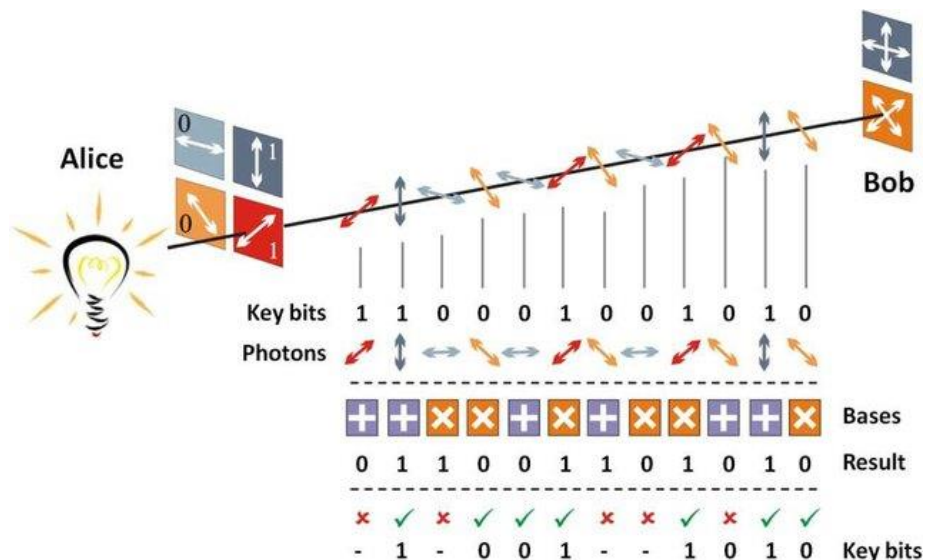


Ilustración 1 - Esquema básico del protocolo BB84 [3].

El protocolo BBM92, ideado por Charles Bennett, Gilles Brassard y N. David Mermin en 1992, es otro protocolo QKD de gran relevancia. A continuación, el esquema básico del protocolo BBM92:

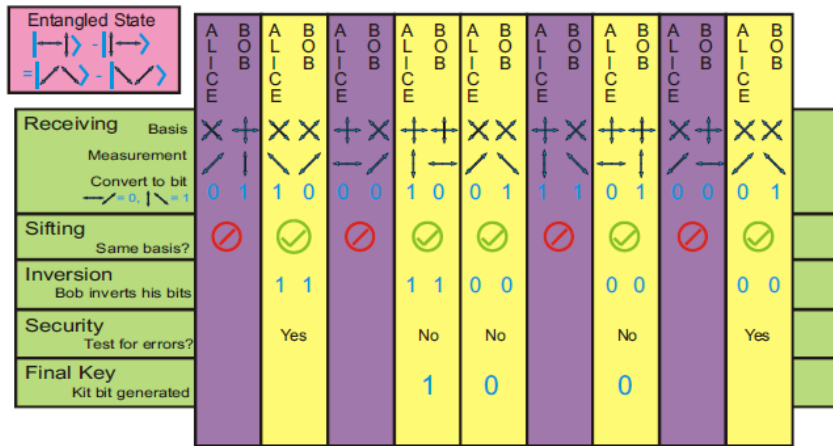


Ilustración 2 - Esquema básico del protocolo BB84 [4].

Los modelos de optimización utilizados en el presente proyecto se dividen en dos categorías: clásicos y cuánticos. El modelo clásico emplea técnicas tradicionales de programación matemática, utilizando específicamente el algoritmo de optimización CPLEX de IBM [5]. Método reconocido por ser efectivo a la par que eficiente con portafolios de tamaño moderado, ya que ha sido perfeccionado a lo largo de varios años.

El modelo cuántico, por otro lado, utiliza el algoritmo Variational Quantum Eigensolver (VQE), implementado a través de Qiskit [6]. VQE es un algoritmo híbrido que aprovecha la capacidad de los ordenadores cuánticos para explorar grandes espacios de soluciones mediante la superposición y el entrelazamiento [7]. Aunque los ordenadores cuánticos actuales son sensibles al ruido, VQE es adecuado para problemas de optimización debido a su capacidad para aproximar soluciones óptimas con menor tiempo de ejecución que los métodos clásicos en ciertos casos.

Para ambos modelos, se estableció un nivel de riesgo del 10%, y se realizaron simulaciones para carteras de 5 y 20 activos. Tanto en el modelo clásico como en el cuántico, los activos se seleccionaron basándose en criterios de minimización de riesgo y maximización de retorno. Las simulaciones fueron comparadas en términos de composición del portafolio, rendimientos a lo largo del tiempo y tiempos de ejecución, facilitando una evaluación comprensiva de cada enfoque. Los datos necesarios para la construcción del portafolio se obtuvieron de la biblioteca de Yahoo Finance [8], en el período comprendido entre el 1 de marzo de 2023 y el 1 de marzo de 2024.

A continuación, una ilustración del circuito cuántico parametrizado (ansatz) de 5 qubits para la optimización del portafolio con 5 activos.

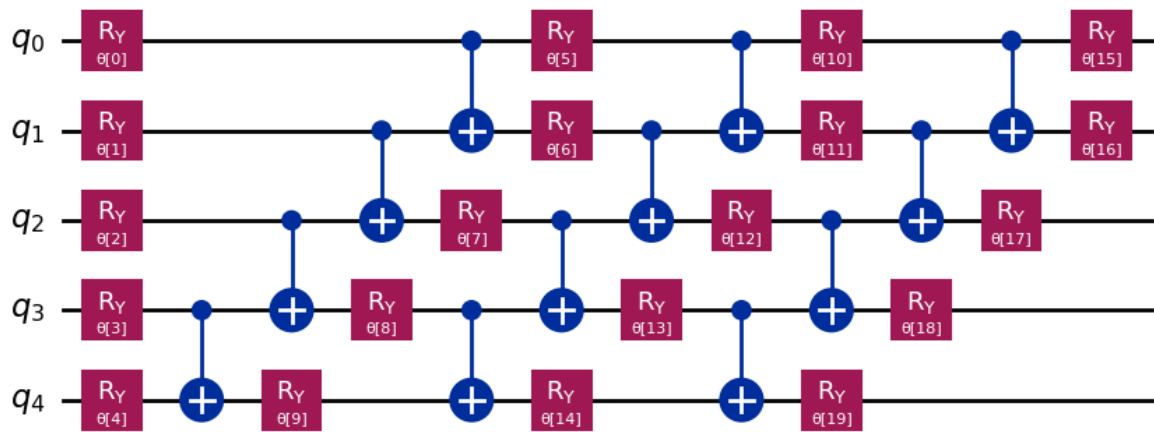


Ilustración 2 - Circuito cuántico parametrizado (ansatz) de 5 qubits.

4. Resultados

Los resultados obtenidos en el proyecto abarcan tanto el análisis de protocolos cuánticos para comunicaciones seguras como el desarrollo de un modelo cuántico para la optimización de portafolios.

En cuanto a los protocolos cuánticos, se ha realizado una revisión de los principales protocolos de QKD, como el BB84 y el BBM92. El protocolo BB84 [9], pionero en el área de QKD, utiliza dos bases de polarización para transmitir fotones y generar claves seguras. Su seguridad se basa en los principios de la mecánica cuántica, donde cualquier intento de interceptación altera los estados cuánticos y es detectable. Aunque el BB84 ha demostrado su viabilidad práctica, su principal limitación es la sensibilidad a errores y pérdidas en el canal de comunicación.

Por otro lado, el protocolo BBM92 emplea solo dos estados no ortogonales para la transmisión de claves [10], lo que lo hace conceptualmente más simple y menos exigente en términos de recursos cuánticos. Sin embargo, también tiene restricciones similares al BB84 en cuanto a errores y pérdidas, además de una menor tasa de generación de claves debido a la probabilidad de descarte de fotones.

Otros protocolos QKD, como el E91 basado en entrelazamiento cuántico [11], el SARG04 que mejora la seguridad contra algunos ataques [12], el DPS que codifica la clave en diferencias de fase [13], y el COW que utiliza pulsos coherentes [14], ofrecen ventajas y limitaciones específicas. La elección del protocolo adecuado depende de factores como la distancia de transmisión, la tasa de generación de claves, la resistencia a ataques y la compatibilidad con la infraestructura existente.

Respecto a los modelos de optimización, los resultados del proyecto muestran diferencias significativas entre el modelo clásico y el modelo cuántico. En la simulación con 5 activos, el modelo clásico seleccionó Amazon, Netflix y Google, mientras que el modelo cuántico eligió Apple, Netflix y Google. Ambos modelos coincidieron en que Netflix y Google eran inversiones atractivas, pero difirieron en la inclusión de Amazon y Apple, respectivamente. El rendimiento del portafolio clásico fue ligeramente superior al del cuántico, especialmente en los últimos meses del período analizado.

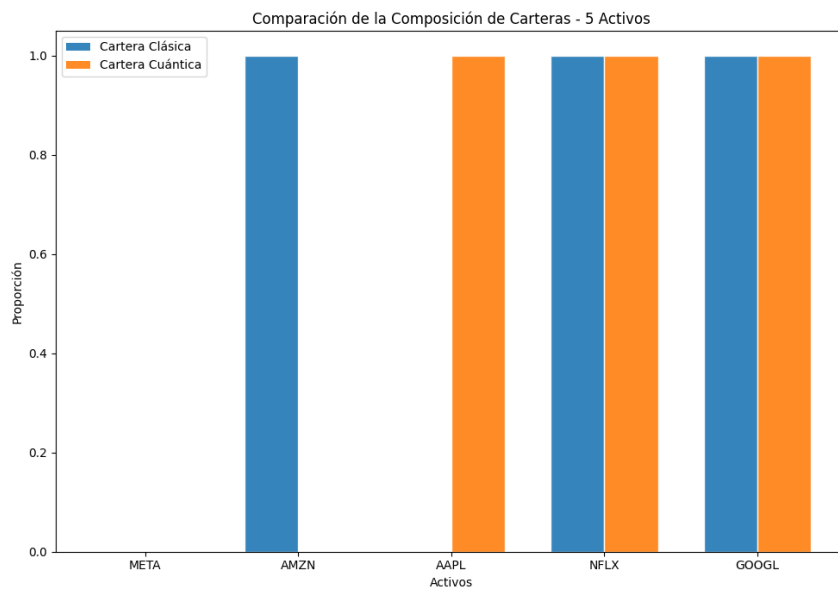


Ilustración 3 - Composición del Portafolio con 5 Activos.

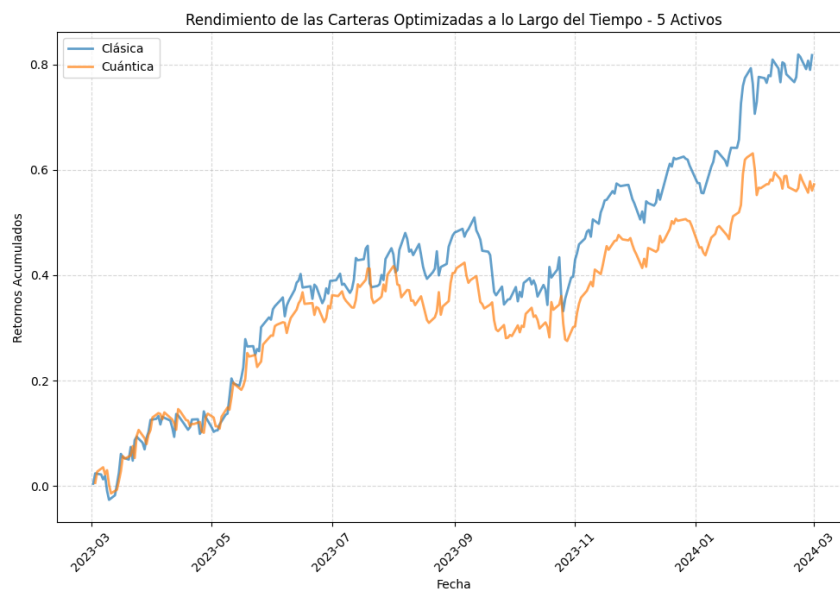


Ilustración 5 - Rendimiento del Portafolio con 5 Activos.

Para el caso de 20 activos, el modelo cuántico mostró un rendimiento superior y más consistente que el clásico. Seleccionó empresas como Facebook, Amazon, Apple, Berkshire Hathaway, ExxonMobil, Visa y Mastercard. En comparación, el modelo clásico incluyó Apple, Lockheed Martin, Berkshire Hathaway, ExxonMobil, JPMorgan Chase, Visa y Mastercard. Aunque ambos modelos coincidieron en seleccionar varias empresas, el modelo cuántico logró identificar y aprovechar oportunidades de inversión de manera más efectiva en un universo más amplio y diversificado de activos.

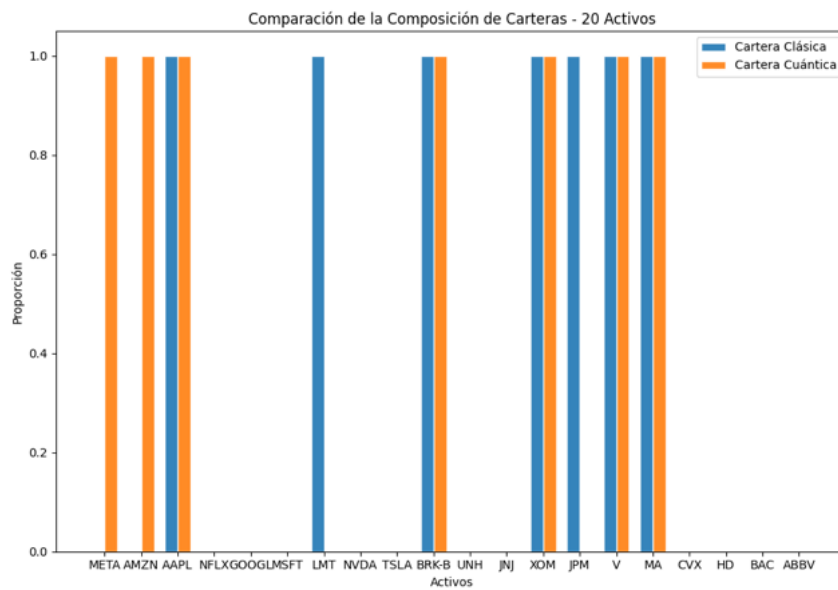


Ilustración 6 - Composición del Portafolio con 20 Activos.

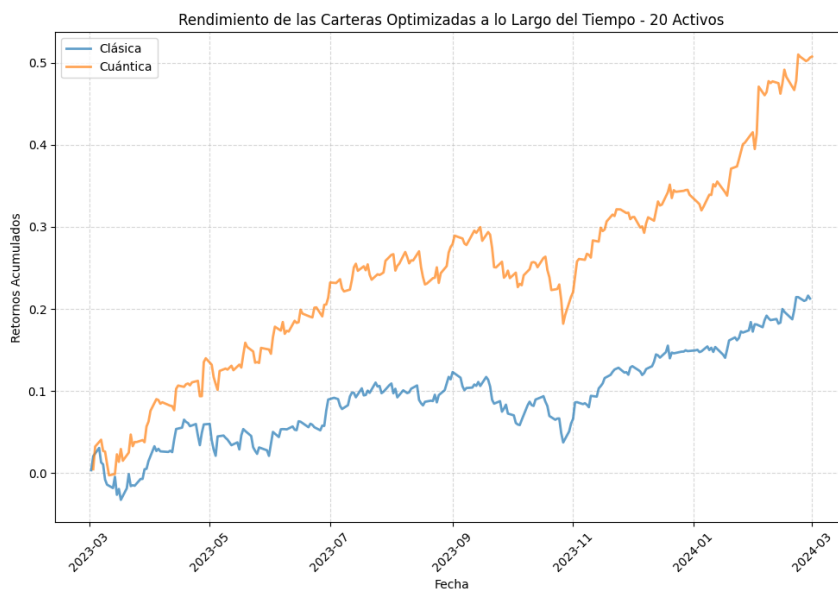


Ilustración 7 - Rendimiento del Portafolio con 20 Activos.

En términos de tiempo de ejecución, el modelo clásico fue más eficiente, con tiempos significativamente menores tanto para 5 activos como para 20 activos. El modelo cuántico, aunque más lento, mostró una capacidad prometedora para optimizar portafolios grandes, sugiriendo que la tecnología cuántica puede tener una ventaja en escenarios de mayor complejidad.

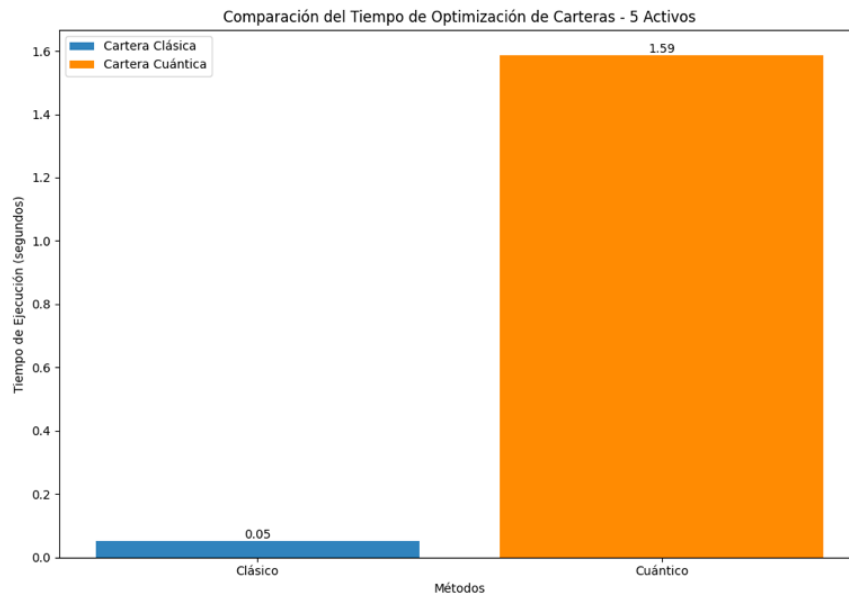


Ilustración 8 - Tiempo de Ejecución del Portafolio con 5 Activos.

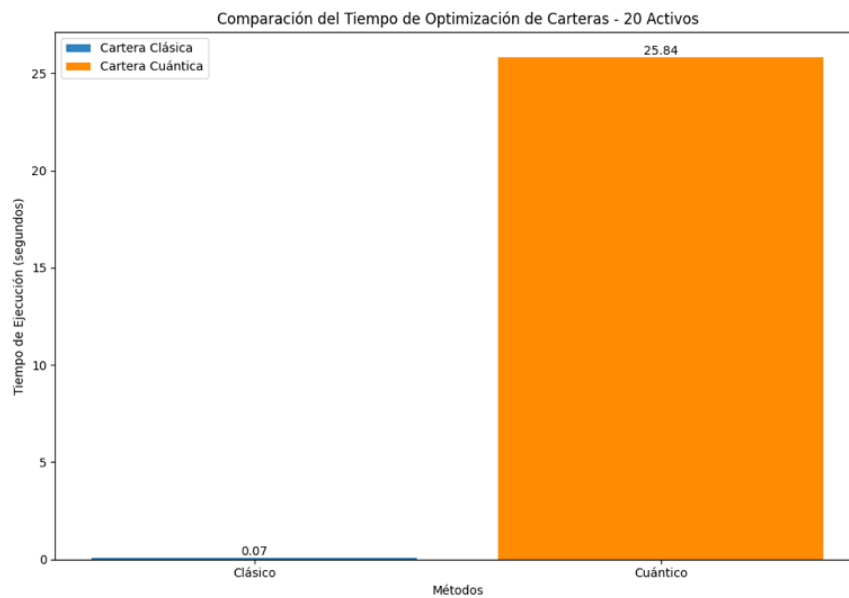


Ilustración 9 - Tiempo de Ejecución del Portafolio con 20 Activos.

5. Conclusiones

Este proyecto de investigación ha logrado contribuir a la comprensión y aplicación del fenómeno de Quantenverschränkungen en el campo de la Ingeniería de Telecomunicación. Se han explorado protocolos cuánticos de comunicación seguros, se ha desarrollado un modelo cuántico para la optimización de recursos y se ha ofreciendo una base sólida para futuras investigaciones. Los resultados obtenidos destacan el potencial transformador de las tecnologías cuánticas en la industria de las telecomunicaciones y abren nuevas perspectivas para la innovación y el desarrollo en este ámbito.

Como trabajo futuro, sería de interés extender la aplicación del modelo cuántico a otros problemas de optimización en el ámbito de las telecomunicaciones. Por ejemplo, se podrían abordar desafíos como la asignación óptima de recursos en redes, la planificación eficiente de rutas en sistemas de comunicación o la optimización de la calidad de servicio en redes inalámbricas. La adaptación del modelo cuántico a estos escenarios permitiría evaluar su versatilidad y potencial para resolver una variedad de problemas en la industria.

6. Referencias

- [1] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge university press, 2010.
- [2] Z. C. Seskir, R. Korkmaz, and A. U. Aydinoglu, “The landscape of the quantum start-up ecosystem,” *EPJ Quantum Technol*, vol. 9, no. 1, p. 27, 2022.
- [3] A. Carrasco-Casado, V. Fernández, and N. Denisenko, “Free-space quantum key distribution,” *Optical Wireless Communications: An Emerging Technology*, pp. 589–607, 2016.
- [4] C. Erven, “On Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source,” 2007. [Online]. Available: <https://api.semanticscholar.org/CorpusID:7953345>
- [5] “Qiskit – CPLEX Optimizer Documentation.” Accessed: Jun. 01, 2024. [Online]. Available: https://qiskit-community.github.io/qiskit-optimization/stubs/qiskit_optimization.algorithms.CplexOptimizer.html
- [6] “Qiskit – VQE Documentation.” Accessed: Jun. 01, 2024. [Online]. Available: https://qiskit-community.github.io/qiskit-algorithms/stubs/qiskit_algorithms.VQE.html
- [7] H. L. Tang *et al.*, “qubit-adapt-vqe: An adaptive algorithm for constructing hardware-efficient ansätze on a quantum processor,” *PRX Quantum*, vol. 2, no. 2, p. 020310, 2021.
- [8] “Yahoo Finance Library.” Accessed: Jun. 01, 2024. [Online]. Available: <https://pypi.org/project/yfinance/>

- [9] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor Comput Sci*, vol. 560, pp. 7–11, 2014.
- [10] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys Rev Lett*, vol. 68, no. 5, p. 557, 1992.
- [12] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys Rev Lett*, vol. 67, no. 6, p. 661, 1991.
- [12] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations," *arXiv preprint quant-ph/0211131*, 2002.
- [13] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Phys Rev Lett*, vol. 89, no. 3, p. 037902, 2002.
- [14] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Appl Phys Lett*, vol. 87, no. 19, 2005.

APPLICATION OF THE PHENOMENON OF QUANTENVERSCHRÄNKUNGEN IN TELECOMMUNICATION ENGINEERING

Author: Sánchez Pérez, Iván.

Director: Puente Águeda, Cristina.

Collaborating Entity: ICAI – Universidad Pontificia Comillas.

ABSTRACT

This research project explores the application of quantum entanglement and quantum computing in Telecommunications Engineering. By reviewing communication protocols based on Quantum Key Distribution (QKD), such as BB84 and BBM92, the fundamental principles of Quantum Physics to ensure security in modern communications are analysed. Additionally, a quantum model for portfolio optimisation is developed using IBM's Qiskit programming platform. The results obtained suggest advantages of the quantum model compared to classical approaches, although with longer execution times as the number of assets increases.

Keywords: Quantum Computing, Quantum-as-a-Service, QKD, Qiskit, Portfolio Optimisation, Decision Making, Paradigm Shift, Capital Investment, Digital Economy.

1. Introduction

The fundamental principles of classical Telecommunication Technologies engineering, including its scientific research methodology, which shares a foundation with physics, have paved the way for a profound understanding of the shift from bits—the basic unit of information in classical computing—to qubits, or quantum bits, which serve as the building blocks of information in the emerging field of quantum technology. [1]. This transition marks a significant leap forwards, opening up new possibilities and challenges in the realm of information processing and communication.

Paradigm Shift: While a bit or binary digit, can have the value 0 or 1, a qubit can have a value that is either 0 or 1 or a quantum superposition of 0 and 1.

A qubit, like a simple bit, contains all the information necessary to describe the state of a binary variable. Quantum computing aims to address some of the most pressing challenges in various areas, ranging from communications, energy, and health to agriculture, finance, and materials science, among others [2]. For some of these problems, classical computing becomes increasingly difficult as the size of the system increases. In this context, quantum applications emerge as a promising solution for the author.

2. Project Definition

The primary objective of this project is to explore the application of the phenomenon of quantum entanglement in Telecommunication Engineering. To achieve this, three specific objectives are established:

1. To explore communication protocols based on Quantum Key Distribution (QKD), such as BB84 and BBM92, analysing their fundamental principles and applicability in modern telecommunication systems;
2. To develop a quantum model for portfolio optimisation using IBM's Qiskit programming language. Two scenarios are compared: one with 5 assets and another with 20 assets, evaluating the portfolio composition, returns obtained, and execution times between the classical and quantum models; and
3. To lay the groundwork for future research between the field of Telecommunication Engineering and Quantum Computing, providing a starting point and reference for subsequent projects.

3. Description of the System/Model

The BB84 protocol, developed by Charles Bennett and Gilles Brassard in 1984, is one of the most important and well-known QKD protocols. The basic scheme of the BB84 protocol can be described as follows:

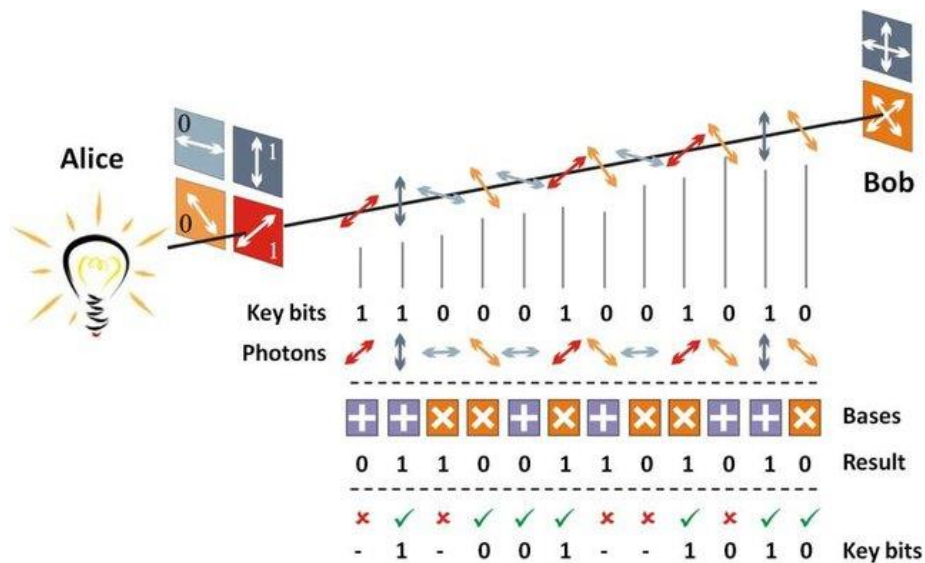


Figure 1 - Basic Scheme of the BB84 Protocol [3].

The BBM92 protocol, developed by Charles Bennett, Gilles Brassard, and N. David Mermin in 1992, is another important QKD protocol that uses entangled states. The basic scheme of the BBM92 protocol can be illustrated as follows:

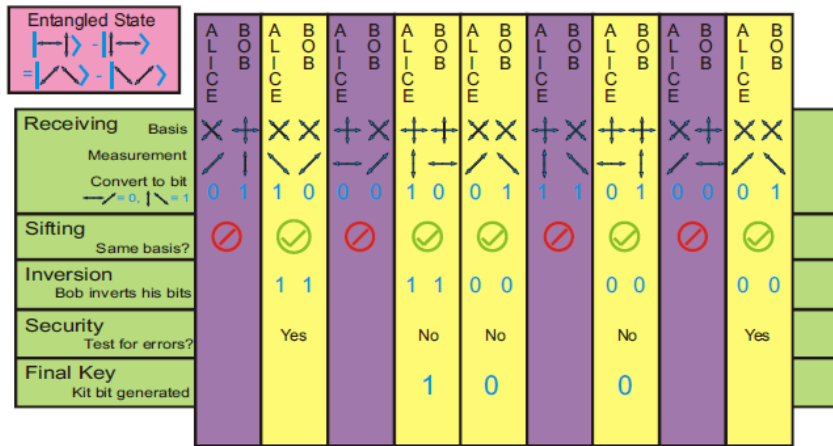


Figure 2 - Basic Scheme of the BBM92 Protocol [4].

The optimisation models used in this project are divided into two categories: classical and quantum. The classical model employs traditional mathematical programming techniques, specifically using IBM’s CPLEX optimisation algorithm [5]. This approach has been refined over decades and is known for its efficiency and ability to handle moderate-sized optimisation problems effectively.

The quantum model, on the other hand, uses the Variational Quantum Eigensolver (VQE) algorithm, implemented through Qiskit [6]. VQE is a hybrid quantum-classical algorithm that leverages the ability of quantum computers to explore large solution spaces through superposition and entanglement [7]. Although current quantum computers are noisy and limited in size, VQE is suitable for optimisation problems due to its ability to approximate optimal solutions with shorter execution times than classical methods in certain cases.

For both models, a risk appetite of 10% was established, and simulations were performed for portfolios of 5 and 20 assets. In both the classical and quantum models, assets were selected based on risk minimisation and return maximisation criteria. The simulations were compared in terms of portfolio composition, returns over time, and execution times to provide a comprehensive evaluation of each approach. The actual data required for the portfolio construction was sourced from Yahoo Finance library [8] for the period spanning March 1, 2023, to March 1, 2024.

Below is an illustration of the parametrised quantum circuit (ansatz) of 5 qubits for portfolio optimisation with 5 assets.

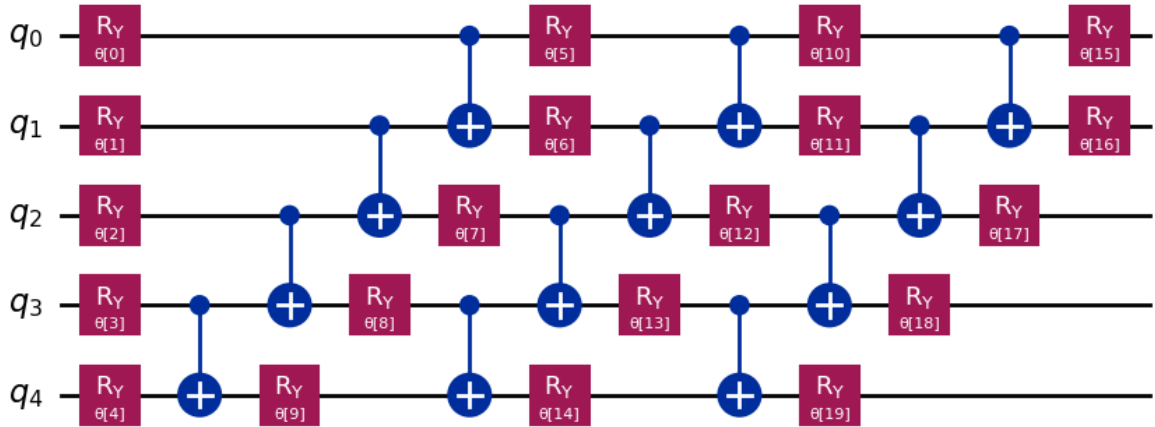


Figure 4 - Parametrised Quantum Circuit (ansatz) of 5 Qubits.

4. Results

The results obtained in this project encompass both the analysis of quantum protocols for secure communications and the development of a quantum model for portfolio optimisation.

Regarding quantum protocols, a comprehensive review of the main QKD protocols, such as BB84 and BBM92, has been conducted. The BB84 protocol [9], a pioneer in the QKD field, uses two polarisation bases to transmit photons and generate secure keys. Its security is based on the principles of quantum mechanics, where any interception attempt alters the quantum states and is detectable. Although BB84 has demonstrated its practical feasibility, its main limitation is its sensitivity to errors and losses in the communication channel.

On the other hand, the BBM92 protocol employs only two non-orthogonal states for key transmission [10], making it conceptually simpler and less demanding in terms of quantum resources. However, it also faces similar challenges to BB84 regarding errors and losses, in addition to a lower key generation rate due to the probability of photon discard.

Other QKD protocols, such as the E91 based on quantum entanglement [11], the SARG04 which improves security against certain attacks [12], the DPS which encodes the key in phase differences [13], and the COW which uses coherent pulses [14], offer specific advantages and limitations.

Regarding the optimisation models, the project results show significant differences between the classical and quantum models. In the 5-asset simulation, the classical model selected Amazon, Netflix, and Google, while the quantum model chose Apple, Netflix, and Google. Both models agreed that Netflix and Google were attractive investments but differed in the inclusion of Amazon and Apple, respectively. The classical portfolio's performance was slightly superior to the quantum one in this case, especially in the last months of the analysed period.

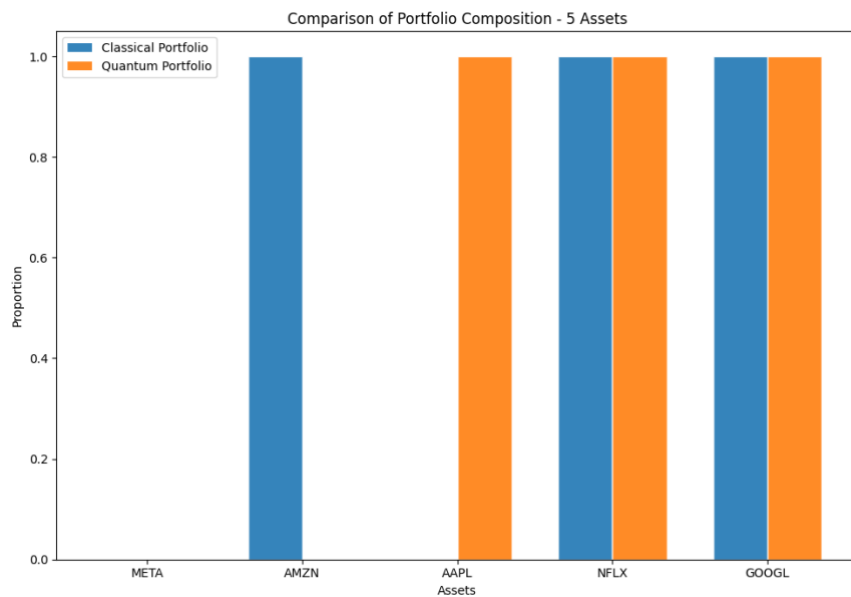


Figure 5 - Portfolio Composition with 5 Assets.

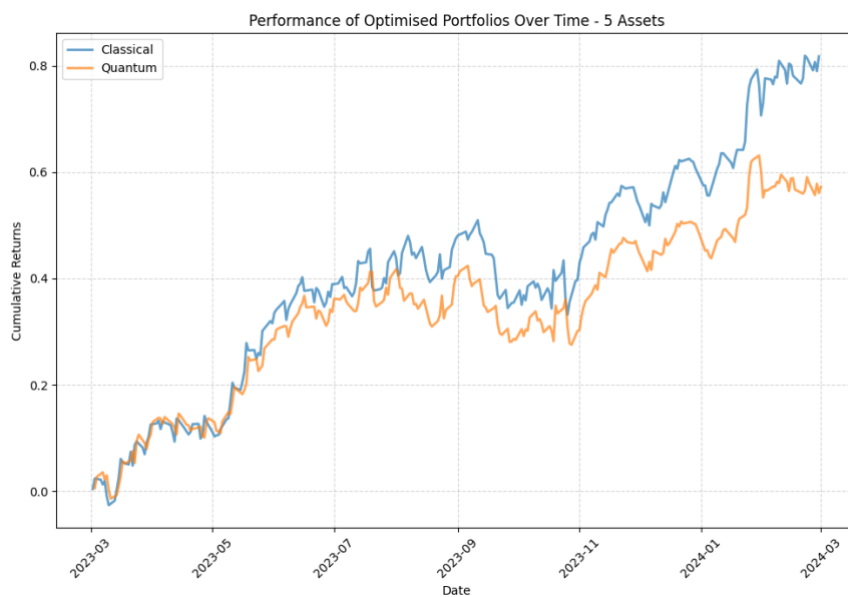


Figure 5 - Portfolio Performance with 5 Assets.

For the case of 20 assets, the quantum model showed superior and more consistent performance than the classical model. It selected companies such as Facebook, Amazon, Apple, Berkshire Hathaway, ExxonMobil, Visa, and Mastercard. In comparison, the classical model included Apple, Lockheed Martin, Berkshire Hathaway, ExxonMobil, JPMorgan Chase, Visa, and Mastercard. Although both models agreed on selecting several companies, the quantum model managed to identify and exploit investment opportunities more effectively in a broader and more diversified universe of assets.

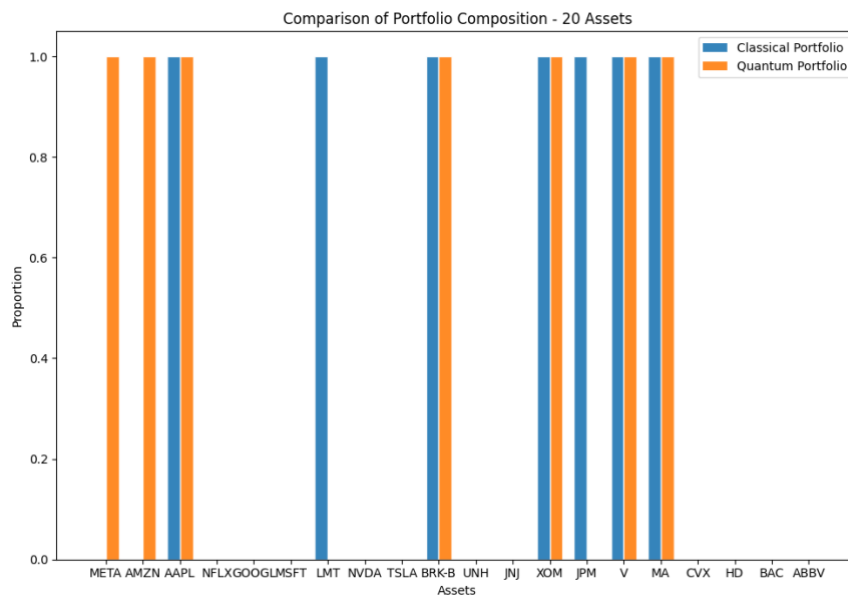


Figure 6 - Portfolio Composition with 20 Assets.

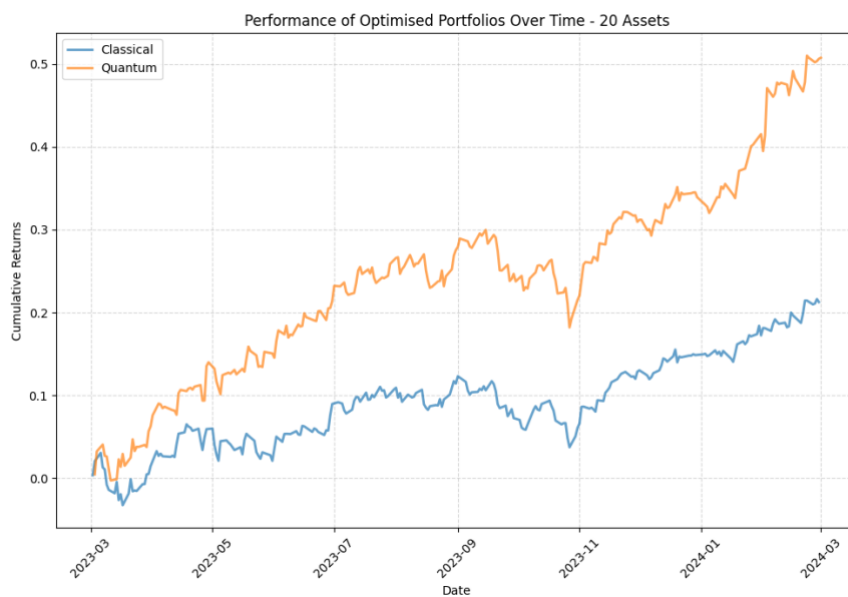


Figure 7 - Portfolio Performance with 20 Assets.

In terms of execution time, the classical model was more efficient, with significantly shorter times for both 5 and 20 assets. The quantum model, although slower, showed a promising capacity to optimise large portfolios, suggesting that quantum technology may have an advantage in more complex scenarios.

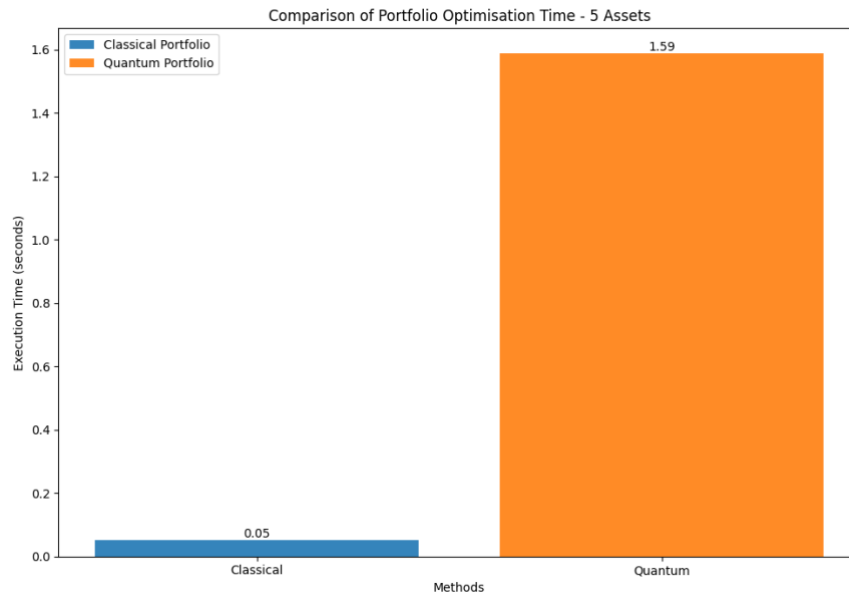


Figure 8 - Execution Time for the Portfolio with 5 Assets.

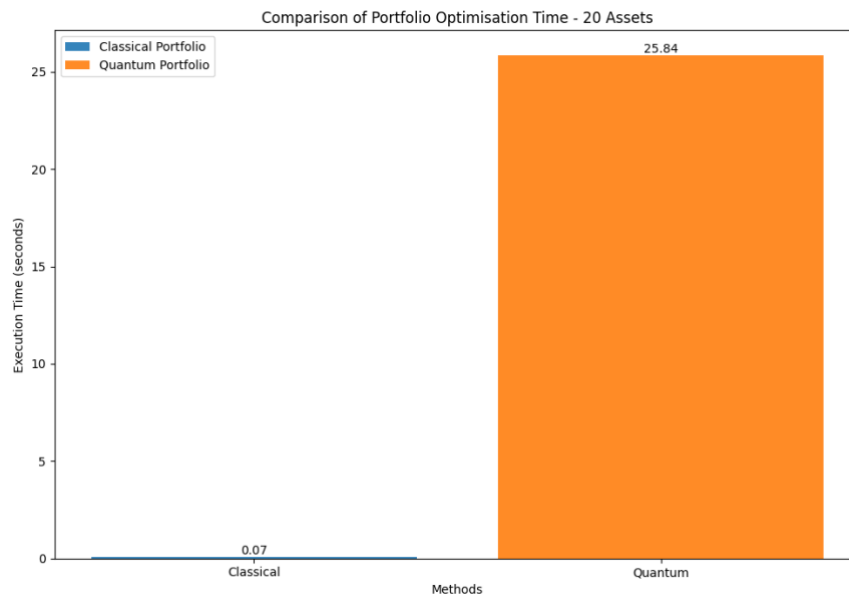


Figure 9 - Execution Time for the Portfolio with 20 Assets.

5. Conclusions

This research project has contributed to the understanding and application of the phenomenon of quantum entanglement in the field of Telecommunication Engineering. Secure quantum communication protocols have been explored, a quantum model for resource optimisation has been developed, and a solid foundation has been provided for future research. The results obtained highlight the transformative potential of quantum technologies in the telecommunications industry, opening new perspectives for innovation and development in this field.

For future work, it would be of interest to extend the application of the quantum model to other optimisation problems within the telecommunications domain. For example, challenges such as optimal resource allocation in networks, efficient route planning in communication systems, and quality of service optimisation in wireless networks could be addressed. Adapting the quantum model to these scenarios would allow for the evaluation of its versatility and potential to solve a variety of problems in the industry.

6. References

- [1] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge university press, 2010.
- [2] Z. C. Seskir, R. Korkmaz, and A. U. Aydinoglu, "The landscape of the quantum start-up ecosystem," *EPJ Quantum Technol*, vol. 9, no. 1, p. 27, 2022.
- [3] A. Carrasco-Casado, V. Fernández, and N. Denisenko, "Free-space quantum key distribution," *Optical Wireless Communications: An Emerging Technology*, pp. 589–607, 2016.
- [4] C. Erven, "On Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source," 2007. [Online]. Available: <https://api.semanticscholar.org/CorpusID:7953345>
- [5] "Qiskit – CPLEX Optimizer Documentation." Accessed: Jun. 01, 2024. [Online]. Available: https://qiskit-community.github.io/qiskit-optimization/stubs/qiskit_optimization.algorithms.CplexOptimizer.html
- [6] "Qiskit – VQE Documentation." Accessed: Jun. 01, 2024. [Online]. Available: https://qiskit-community.github.io/qiskit-algorithms/stubs/qiskit_algorithms.VQE.html
- [7] H. L. Tang *et al.*, "qubit-adapt-vqe: An adaptive algorithm for constructing hardware-efficient ansätze on a quantum processor," *PRX Quantum*, vol. 2, no. 2, p. 020310, 2021.
- [8] "Yahoo Finance Library." Accessed: Jun. 01, 2024. [Online]. Available: <https://pypi.org/project/yfinance/>
- [9] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor Comput Sci*, vol. 560, pp. 7–11, 2014.

- [10] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys Rev Lett*, vol. 68, no. 5, p. 557, 1992.
- [12] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys Rev Lett*, vol. 67, no. 6, p. 661, 1991.
- [12] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations," *arXiv preprint quant-ph/0211131*, 2002.
- [13] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Phys Rev Lett*, vol. 89, no. 3, p. 037902, 2002.
- [14] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Appl Phys Lett*, vol. 87, no. 19, 2005.

Índice de la memoria

Capítulo 1. Introducción	7
Capítulo 2. Descripción de las Tecnologías	9
2.1 Plataforma de Programación Cuántica: Qiskit.....	9
2.2 Plataforma de Computación Cuántica: IBM Quantum Platform	10
2.3 Lenguaje de Programación: Python	12
2.4 Entorno de Desarrollo: Anaconda.....	13
2.5 Control de Versiones: Git y GitHub.....	14
2.6 IDE: Visual Studio Code.....	15
2.7 Herramientas de Visualización: Matplotlib y Seaborn	15
Capítulo 3. Definición del Trabajo	18
3.1 Motivación	18
3.2 Objetivos	19
3.2.1 <i>Objetivo General</i>	19
3.2.2 <i>Objetivos específicos</i>	19
3.3 Metodología	20
3.3.1 <i>Análisis Exploratorio de Protocolos Cuánticos y Recursos</i>	20
3.3.2 <i>Desarrollo de Modelos Cuánticos</i>	20
3.3.3 <i>Revisión de Objetivos</i>	21
3.3.4 <i>Contribución a Futuras Investigaciones</i>	21
3.4 Planificación.....	21
3.5 Estimación económica	25
Capítulo 4. Estado del Arte.....	28
4.1 Introducción	28
4.2 Revisión de la Literatura Científica	28
4.2.1 <i>Fundamentos del Entrelazamiento Cuántico</i>	28
4.2.2 <i>Evolución Histórica y Avances Recientes</i>	29
4.2.3 <i>Aplicaciones del Entrelazamiento Cuántico en las Telecomunicaciones</i>	30
4.3 Protocolos Cuánticos.....	32
4.3.1 <i>Protocolo BB84</i>	33

4.3.2	Protocolo BBM92.....	34
4.3.3	Otros Protocolos de Distribución Cuántica de Claves (QKD).....	35
4.4	Comparación entre Sistemas de Comunicación Clásicos y Cuánticos	37
4.4.1	Limitaciones de los Sistemas de Comunicación Clásicos.....	37
4.4.2	Ventajas de los Sistemas de Comunicación Cuánticos	38
4.5	Optimización de Portafolios con Computación Cuántica	39
4.5.1	Introducción a la Optimización de Portafolios.....	40
4.5.2	Métodos Clásicos de Optimización de Portafolios	41
4.5.3	Algoritmos Cuánticos en la Optimización de Portafolios.....	42
4.5.4	Ventajas y Desafíos de la Optimización Cuántica de Portafolios	43
Capítulo 5. Modelo Desarrollado		46
5.1	Introducción	46
5.1.1	El concepto de modelo	46
5.1.2	Enfoque tentativo.....	47
5.2	Definición del Problema	47
5.3	Modelo de Optimización Clásico.....	54
5.4	Modelo de Optimización Cuántico	55
Capítulo 6. Análisis de Resultados.....		61
6.1	Comparación de la Composición del Portafolio	61
6.1.1	Composición del Portafolio con 5 Activos.....	61
6.1.2	Composición del Portafolio con 20 Activos.....	63
6.1.3	Diferencias en la Selección de Activos	65
6.2	Comparación de los Rendimientos del Portafolio.....	66
6.2.1	Rendimiento del Portafolio con 5 Activos.....	67
6.2.2	Rendimiento del Portafolio con 20 Activos.....	68
6.2.3	Análisis Comparativo de Rendimientos	69
6.3	Comparación del Tiempo de Ejecución del Modelo.....	70
6.3.1	Tiempo de Ejecución del Modelo con 5 Activos	70
6.3.2	Tiempo de Ejecución del Modelo con 20 Activos	71
6.3.3	Análisis Comparativo de Tiempos.....	72
Capítulo 7. Conclusiones y Trabajos Futuros.....		75
7.1	Conclusiones	75

7.2 Trabajos Futuros.....	76
<i>Capítulo 8. Bibliografía.....</i>	<i>78</i>
<i>Anexo I: Alineación Del Proyecto Con Los ODS.....</i>	<i>88</i>

Índice de figuras

Fig. 1 Logo de Qiskit.....	9
Fig. 2 Página principal de IBM Quantum Platform.....	11
Fig. 3 Ordenadores Cuánticos disponibles en IBM Quantum Platform.	12
Fig. 4 Logo de Anaconda.	13
Fig. 5 Logo de Git.....	14
Fig. 6 Logo de Github.....	14
Fig. 7 Logo de Visual Studio Code.	15
Fig. 8 Página principal de Matplotlib.	16
Fig. 9 Página principal de Seaborn.	16
Fig. 10 Cambio de paradigma: Bit vs Qubit [27].	19
Fig. 11 Planificación del proyecto.....	21
Fig. 12 Precios de Qiskit.....	26
Fig. 13 Esquema básico del protocolo BB84 [49].....	34
Fig. 14 Esquema básico del protocolo BBM92 [51].	35
Fig. 15 Matriz de Covarianza - 5 Activos.	50
Fig. 16 Matriz de Correlación - 5 Activos.....	51
Fig. 17 Matriz de Covarianza - 20 Activos.	52
Fig. 18 Matriz de Correlación - 20 Activos.....	53
Fig. 19 Ansatz de 5 qubits.	57
Fig. 20 Ansatz de 10 qubits.	58
Fig. 21 Composición del Portafolio con 5 Activos.	63
Fig. 22 Composición del Portafolio con 20 Activos.	65
Fig. 23 Rendimiento del Portafolio con 5 Activos.	68
Fig. 24 Rendimiento del Portafolio con 20 Activos.	69
Fig. 25 Tiempo de Ejecución del Portafolio con 5 Activos.....	71
Fig. 26 Tiempo de Ejecución del Portafolio con 20 Activos.....	72

Fig. 27 Objetivos de Desarrollo Disponible de la Agenda 2030. 88

Índice de tablas

Tabla 1 Estimación económica del proyecto. 25

Capítulo 1. INTRODUCCIÓN

La aplicación del fenómeno de Quantenverschränkungen, o entrelazamiento cuántico, en el campo de la Ingeniería de Telecomunicación representa un avance de gran relevancia en la intersección entre la física cuántica y la ingeniería de las comunicaciones. El entrelazamiento cuántico, un fenómeno que desafía las intuiciones de la física clásica, ha emergido como un componente esencial de la revolución tecnológica que está configurando el futuro de las telecomunicaciones.

Retrocediendo en el tiempo, el fenómeno de Quantenverschränkungen se origina en el artículo de Albert Einstein, Boris Podolsky y Nathan Rosen, publicado en 1935 [1]. Posteriormente, Erwin Schrödinger contribuyó con varios artículos [2] [3], que describieron lo que más tarde se conocería como la paradoja EPR.

El entrelazamiento cuántico se refiere, en su esencia, a la conexión instantánea entre partículas subatómicas, lo cual permite que sus propiedades estén correlacionadas sin importar la distancia que las separe [4]. Este fenómeno ha dado origen a conceptos paradójicos, como la teleportación cuántica [5] o la criptografía cuántica [6], que tienen una gran relevancia en las telecomunicaciones.

En este contexto, la investigación y desarrollo de dispositivos y tecnologías cuánticas se destacan como un área de estudio fundamental. Empresas e instituciones académicas a nivel global compiten por desarrollar hardware y software cuántico más avanzado. La colaboración interdisciplinar entre físicos cuánticos y expertos en telecomunicaciones está experimentando un crecimiento constante; potenciando una sinergia única entre ambas disciplinas.

Conforme avanzamos en la aplicación del entrelazamiento cuántico en el campo de la Ingeniería de Telecomunicación, iniciamos una nueva era de comunicaciones en la que la

seguridad, la conectividad global y la capacidad de procesamiento experimentan un cambio de paradigma.

A lo largo de este documento, se examinará el estado actual de las tecnologías cuánticas, considerando los protocolos de comunicación basados en la Distribución Cuántica de Claves, destacando su relevancia y potencial para revolucionar las comunicaciones. Asimismo, se describirá la metodología de investigación empleada, así como el proceso de desarrollo de un modelo cuántico para la optimización de carteras de inversión. Los resultados obtenidos serán analizados con detenimiento, se extraerán las conclusiones y se propondrán futuras líneas de investigación.

Por último, se explicará la alineación de este proyecto con los Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030, resaltando su capacidad para impulsar un avance tecnológico sostenible y transformador en el ámbito de las telecomunicaciones.

Capítulo 2. DESCRIPCIÓN DE LAS TECNOLOGÍAS

En este capítulo se describirán en detalle las tecnologías, protocolos y herramientas específicas que se utilizarán a lo largo de este proyecto. Estas tecnologías serán fundamentales para alcanzar los objetivos establecidos.

2.1 PLATAFORMA DE PROGRAMACIÓN CUÁNTICA: QISKIT

Qiskit es una plataforma de programación cuántica de código abierto desarrollada por IBM [7]. Se utilizará como la herramienta principal para el desarrollo y la implementación de los algoritmos cuánticos programados. Qiskit nos permitirá la simulación y ejecución de circuitos cuánticos, junto con la optimización y análisis de resultados.



Fig. 1 Logo de Qiskit.

Qiskit se compone de varios elementos clave:

- **Qiskit Terra** [8]: Es el núcleo de Qiskit y otorga las herramientas necesarias para construir y manipular circuitos cuánticos a nivel de pulsos y puertas. Permite la creación, optimización y transformación de circuitos cuánticos, así como la integración con otros componentes de Qiskit.
- **Qiskit Aer** [9]: Es un simulador que permite la ejecución de circuitos cuánticos en entornos de simulación clásicos, lo que facilita la prueba y depuración de algoritmos

cuánticos. Qiskit Aer introduce simuladores de estado, de matriz de densidad y de evento, para emular diferentes tipos de ruido y condiciones experimentales.

- **Qiskit Finance** [10]: Esta biblioteca forma parte de Qiskit Applications la cual se especializa en el desarrollo de algoritmos cuánticos para aplicaciones financieras. Incluye herramientas y modelos para la optimización de portafolios, simulación de mercados y análisis de riesgos.
- **Qiskit Optimization** [11]: Para formular y resolver problemas de optimización utilizando técnicas cuánticas y clásicas. Con interfaces para diferentes algoritmos de optimización, como el optimizador de mínimos valores propios (Minimum Eigen Optimizer) o el algoritmo VQE, que veremos más adelante.
- **Qiskit Machine Learning** [12]: Ofrece herramientas y algoritmos para el desarrollo de modelos de aprendizaje automático cuántico. Esta biblioteca proporciona algoritmos de clasificación, regresión y clustering.
- **Qiskit Experiments** [13]: Reemplaza a Qiskit Ignis y ofrece un conjunto de herramientas para la caracterización, calibración y mitigación de errores en ordenadores cuánticos reales.

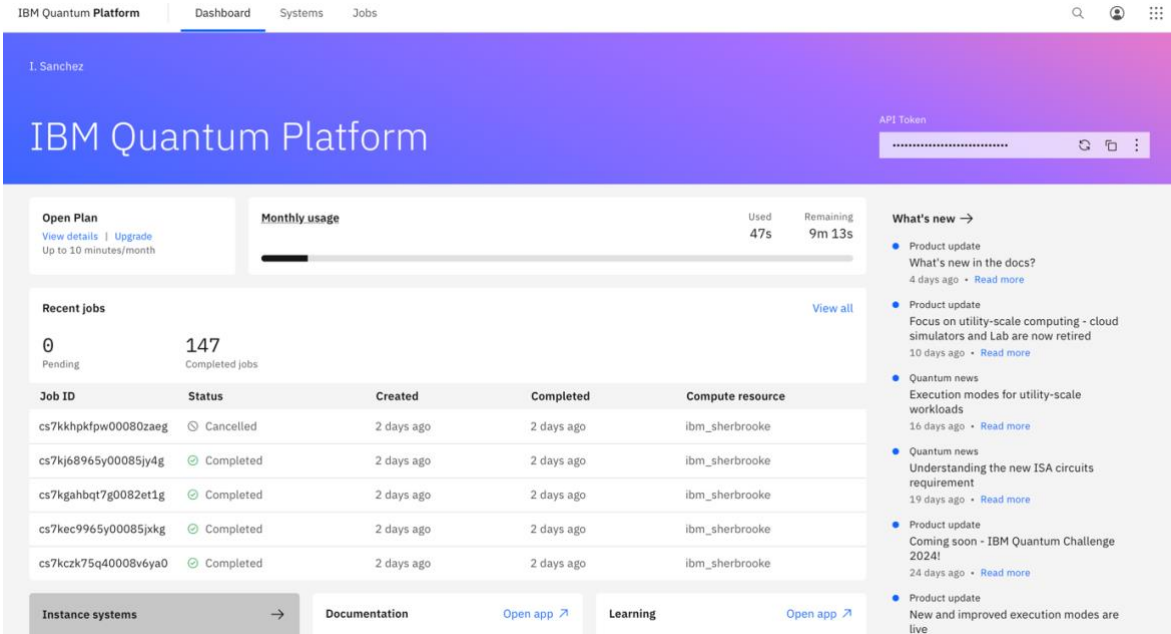
Qiskit también se integra con Qiskit Runtime [14], un entorno de ejecución basado en la nube que permite la ejecución eficiente y escalable de algoritmos cuánticos en hardware cuántico de IBM. Esto optimiza la latencia y el rendimiento, facilitando experimentos más complejos en tiempos de ejecución más cortos.

2.2 PLATAFORMA DE COMPUTACIÓN CUÁNTICA: IBM QUANTUM PLATFORM

IBM Quantum Platform es una plataforma en la nube que permite el acceso a ordenadores cuánticos reales y simuladores [15].

La plataforma ofrece el servicio Quantum-as-a-Service (QaaS) [16], que permite a los usuarios aprovechar las ventajas de la computación cuántica sin la necesidad de tener un ordenador cuántico físico. Esto es especialmente útil para la investigación, ya que reduce los costos y la complejidad asociados con la implementación y al mantenimiento de hardware especializado.

IBM Quantum Platform también facilite el desarrollo y la ejecución de algoritmos cuánticos, con herramientas como el Qiskit Notebook, empleado para la creación de cuadernos Jupyter con código Qiskit.



The screenshot shows the IBM Quantum Platform dashboard for user I. Sanchez. The dashboard includes a navigation bar with 'Dashboard', 'Systems', and 'Jobs'. The main content area features a 'Monthly usage' section with a progress bar showing 47s used and 9m 13s remaining. Below this is a 'Recent jobs' table with columns for Job ID, Status, Created, Completed, and Compute resource. The table lists several jobs, all of which are 'Completed' and were created '2 days ago'. A 'What's new' section on the right provides updates on product changes and documentation. At the bottom, there are links for 'Instance systems', 'Documentation', and 'Learning'.

Job ID	Status	Created	Completed	Compute resource
cs7kkhpkfpw00080zaeg	Cancelled	2 days ago	2 days ago	ibm_sherbrooke
cs7kj68965y00085jy4g	Completed	2 days ago	2 days ago	ibm_sherbrooke
cs7kgahbqt7g0082et1g	Completed	2 days ago	2 days ago	ibm_sherbrooke
cs7kec9965y00085jxkg	Completed	2 days ago	2 days ago	ibm_sherbrooke
cs7kczk75q40008v6ya0	Completed	2 days ago	2 days ago	ibm_sherbrooke

Fig. 2 Página principal de IBM Quantum Platform.

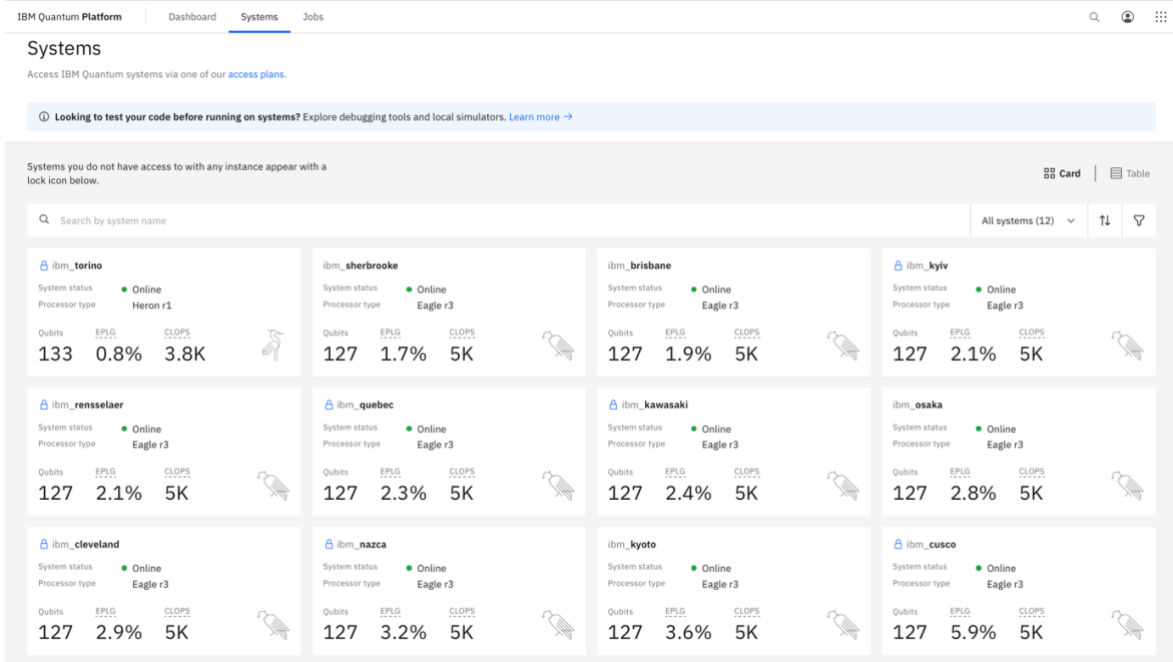


Fig. 3 Ordenadores Cuánticos disponibles en IBM Quantum Platform.

2.3 LENGUAJE DE PROGRAMACIÓN: PYTHON

Python es un lenguaje de programación de alto nivel, interpretado y de propósito general. Se utilizará como el lenguaje principal para el desarrollo de los algoritmos cuánticos y el análisis de datos.

Python se destaca por su sintaxis clara y legible, su amplia adopción en la comunidad científica y su extenso ecosistema de bibliotecas y frameworks. Algunas de las bibliotecas de Python más relevantes para este proyecto incluyen:

- **NumPy** [17]: Da soporte para arrays multidimensionales y funciones matemáticas de alto nivel, para el procesamiento de datos y cálculos numéricos.
- **SciPy** [18]: Se basa en NumPy y ofrece funcionalidades adicionales para optimización, álgebra lineal, integración, interpolación y más. Será utilizado para tareas de optimización clásica y comparación con los resultados obtenidos por el modelo cuántico.

- **Pandas** [19]: Es una biblioteca para la manipulación y análisis de datos que proporciona estructuras y herramientas para trabajar con conjuntos de datos tabulares. Se utilizará para el preprocesamiento y el análisis de los datos financieros utilizados en los modelos de optimización de portafolios.
- **Yahoo Finance** [20]: Es una biblioteca de Python que permite obtener datos bursátiles en tiempo real. Se usará para importar los tickers de las acciones, así como para calcular el rendimiento esperado (μ) y la volatilidad (σ) de los activos financieros, parámetros fundamentales para la creación del portafolio de inversión.

La integración de Python con Qiskit y la plataforma IBM Quantum Platform permite un flujo de trabajo *seamless* para el desarrollo, simulación y ejecución de los algoritmos cuánticos.

2.4 ENTORNO DE DESARROLLO: ANACONDA

Anaconda es una distribución de Python y R de código abierto que simplifica la gestión de paquetes y entornos [21]. Se utilizará para crear y gestionar los entornos de desarrollo utilizados.



Fig. 4 Logo de Anaconda.

Conda, permite instalar, actualizar y gestionar fácilmente las bibliotecas y dependencias necesarias para el proyecto; garantiza la reproducibilidad en distintos equipos y evita conflictos entre diferentes versiones de paquetes.

2.5 CONTROL DE VERSIONES: GIT Y GITHUB

Git es un sistema de control de versiones distribuido que permite el seguimiento de cambios en el código fuente a lo largo del desarrollo del proyecto [22]. Se utilizará para gestionar y controlar las diferentes versiones del código desarrollado.



Fig. 5 Logo de Git.

GitHub es una plataforma web usada mundialmente para el alojamiento de repositorios Git. Asimismo, ofrece funcionalidades para la colaboración y la gestión de proyectos [23]. Se utilizará principalmente para alojar el código del proyecto.



Fig. 6 Logo de Github.

2.6 IDE: VISUAL STUDIO CODE

Visual Studio Code (VS Code) es un editor de código fuente desarrollado por Microsoft [24]. Actúa como entorno de desarrollo integrado (IDE) para la escritura, depuración y prueba del código desarrollado.

VS Code se destaca por su amplio soporte para diferentes lenguajes de programación, e.g. Python, Java, C++... Su integración con Git y su amplio ecosistema de extensiones, lo ha llevado a ser uno de los IDEs más reconocidos.

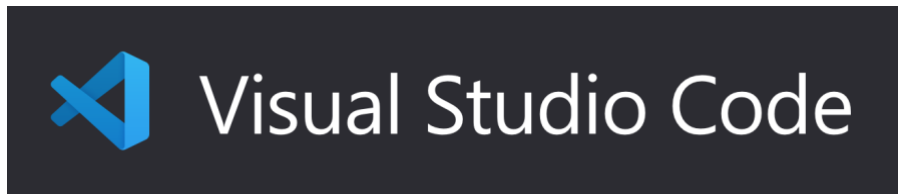


Fig. 7 Logo de Visual Studio Code.

2.7 HERRAMIENTAS DE VISUALIZACIÓN: MATPLOTLIB Y SEABORN

Para la presentación gráfica de los resultados y el análisis de datos, se utilizarán las bibliotecas Matplotlib y Seaborn de Python.

Matplotlib es una biblioteca de visualización que permite crear una gran variedad de gráficos, e.g. gráficos de líneas, gráficos de barras y gráficos de dispersión [25]. Permite un control detallado sobre los elementos del gráfico, como los ejes, las etiquetas, los títulos y las leyendas.

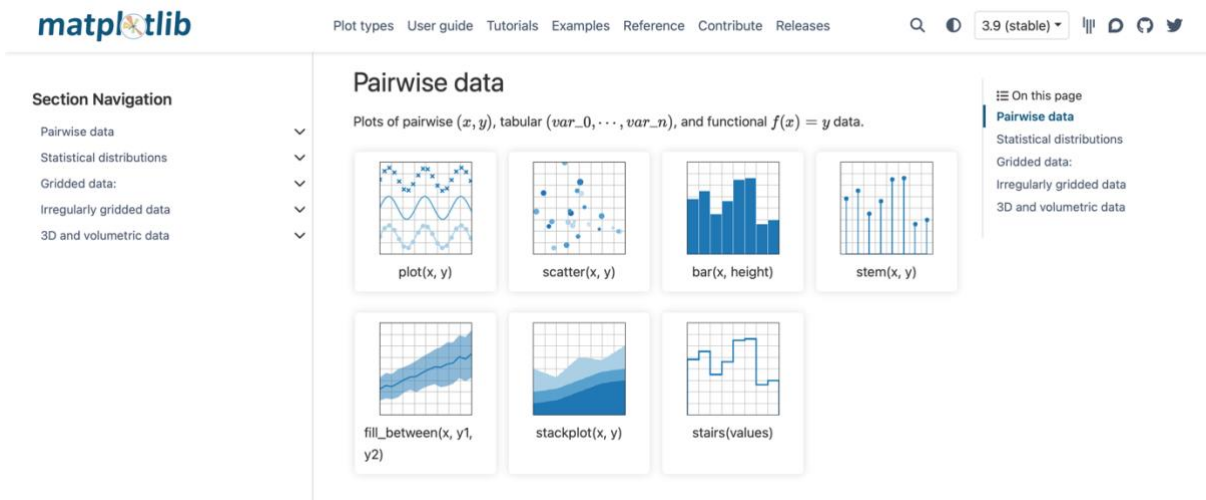


Fig. 8 Página principal de Matplotlib.

Por último, Seaborn es una biblioteca de visualización basada en Matplotlib con una interfaz de alto nivel para crear gráficos estadísticos visualmente atractivos [26]. Ofrece una variedad de temas y paletas de colores predefinidos, así como funciones específicas para visualizar distribuciones, relaciones y datos categóricos.

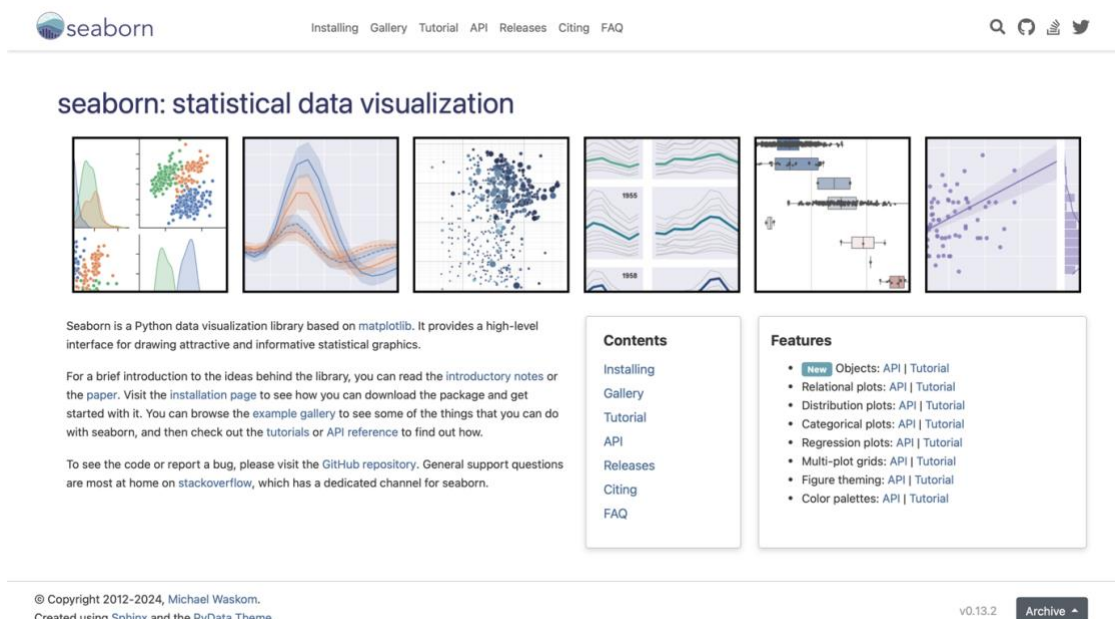


Fig. 9 Página principal de Seaborn.

Estas herramientas de visualización se emplearán para presentar los resultados de la optimización de portafolios, comparar el rendimiento de los enfoques cuánticos y clásicos, y comunicar de manera efectiva los hallazgos de la investigación.

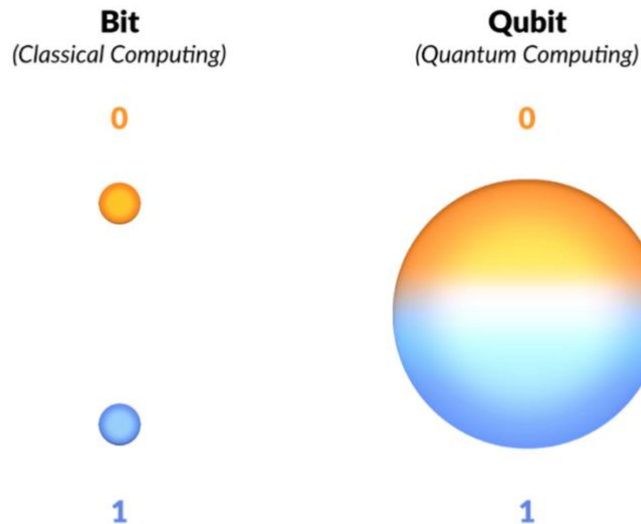
Capítulo 3. DEFINICIÓN DEL TRABAJO

3.1 *MOTIVACIÓN*

Partiendo de los fundamentos que sustentan la Ingeniería de la Telecomunicación en su forma más convencional, incluyendo su método de investigación científica, que comparte sus fundamentos con la Física, comprendemos de repente cómo los bits, que son el objeto fundamental de información en la comunicación clásica, se transforman en qubits o bits cuánticos como el objeto fundamental de información en la comunicación cuántica [1].

Cambio de paradigma: Mientras que un bit o dígito binario puede tener el valor 0 o 1, un qubit puede tener un valor que es 0 o 1 o una superposición cuántica de 0 y 1.

Un qubit, al igual que un simple bit, contiene toda la información necesaria para describir el estado de una variable binaria. La computación cuántica trata de dar respuesta a algunos de los desafíos más apremiantes en diversas áreas, que abarcan desde las comunicaciones, la energía y la salud, hasta la agricultura, las finanzas y la ciencia de materiales, entre otros. Esto se debe a que a medida que los desafíos se vuelven más complejos y demandantes, la eficiencia de la informática convencional disminuye debido a sus límites en la capacidad de procesamiento. En este contexto, las aplicaciones cuánticas emergen como una solución prometedora.



Source: Dumon, K (2019). The computational power of Quantum Computers: an intuitive guide. *Medium*.

Fig. 10 Cambio de paradigma: Bit vs Qubit [27].

3.2 OBJETIVOS

3.2.1 OBJETIVO GENERAL

El objetivo principal de este estudio es investigar y analizar la aplicación del fenómeno de Quantenverschränkungen (entrelazamiento cuántico) en el campo de la Ingeniería de Telecomunicación.

3.2.2 OBJETIVOS ESPECÍFICOS

Para alcanzar el objetivo general, se plantean los siguientes objetivos específicos:

1. Explorar protocolos de comunicación basados en la Distribución Cuántica de Claves (QKD - Quantum Key Distribution). Se llevará a cabo una revisión de los protocolos existentes que aprovechen las propiedades de la física cuántica para garantizar la seguridad en las comunicaciones, e.g. BB84 Protocol and BBM92 Protocol. Se analizarán los principios fundamentales de QKD y se evaluará su aplicación en sistemas de telecomunicación modernos.

2. Desarrollar un modelo cuántico que permita la optimización de recursos. Se buscará diseñar y analizar un modelo matemático basado en la teoría cuántica que pueda utilizarse para mejorar la gestión de recursos y la asignación de activos. Se utilizará la plataforma Qiskit (IBM) y el lenguaje de programación Python.
3. Ayudar a futuros estudios en el área de las telecomunicaciones. Este trabajo no solo busca generar conocimiento en el ámbito de las comunicaciones cuánticas, sino también establecer una base sólida para futuras investigaciones en el campo de Ingeniería de Telecomunicación. Se espera que los hallazgos y conclusiones de esta investigación sirvan como punto de partida y referencia para proyectos de investigación posteriores, estimulando así el avance en este sector en constante evolución.

3.3 METODOLOGÍA

El estudio se divide en varias etapas, que se detallan a continuación:

3.3.1 ANÁLISIS EXPLORATORIO DE PROTOCOLOS CUÁNTICOS Y RECURSOS

Se examinarán los protocolos QKD existentes, como el BB84 Protocol y el BM92 Protocol, para comprender sus fundamentos y evaluar su uso en sistemas de telecomunicación modernos.

3.3.2 DESARROLLO DE MODELOS CUÁNTICOS

En esta sección, se desarrollará un modelo matemático basado en la teoría cuántica utilizando la plataforma Qiskit y el lenguaje de programación Python. Este modelo se centrará en la optimización de portafolios en el contexto de las finanzas y la ingeniería de las telecomunicaciones. Se explorará cómo la computación cuántica puede mejorar la gestión de recursos y la asignación de activos en sistemas de telecomunicación y finanzas.

3.3.3 REVISIÓN DE OBJETIVOS

En esta etapa, se revisarán los objetivos y se analizará cómo se alinean con los objetivos detallados anteriormente. Asimismo, se identificarán áreas en las que la investigación podría contribuir a metas relacionadas con la sostenibilidad y la innovación tecnológica.

3.3.4 CONTRIBUCIÓN A FUTURAS INVESTIGACIONES

El objetivo final de este estudio es contribuir al avance en el campo de la Ingeniería de Telecomunicación. Se espera que los hallazgos y conclusiones sirvan como punto de partida y referencia para proyectos de investigación posteriores.

3.4 PLANIFICACIÓN

El plan de trabajo se ejecutará siguiendo de forma estructurada y organizada, dividido en varias etapas con objetivos específicos y plazos definidos. Para visualizar de manera clara la distribución temporal de las diferentes fases del proyecto, se ha elaborado un cronograma que se presenta en la siguiente figura:

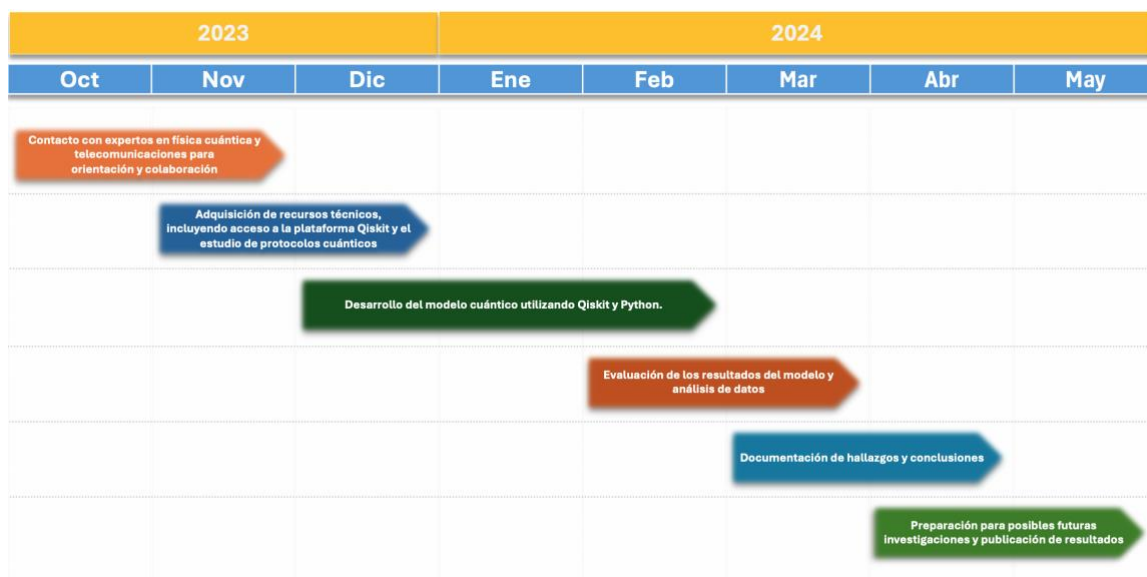


Fig. 11 Planificación del proyecto.

A continuación, la planificación detallada del proyecto:

1. **Octubre 2023 – Noviembre 2023:** Contacto con expertos en física cuántica y telecomunicaciones para orientación y colaboración.
 - Se identificarán expertos relevantes en el campo de la física cuántica y las telecomunicaciones, tanto en el ámbito académico como en la industria.
 - Se establecerán contactos y se programarán reuniones virtuales o presenciales para discutir el proyecto, obtener orientación y explorar oportunidades de colaboración.
 - Se definirán las bases del plan de trabajo junto con la directora del TFG, Cristina Puente Águeda.

2. **Noviembre 2023 – Diciembre 2023:** Adquisición de recursos técnicos, acceso a la plataforma Qiskit y el estudio de protocolos cuánticos.
 - Se gestionará el acceso a la plataforma Qiskit de IBM, la obtención de licencias, suscripciones o créditos de computación cuántica necesarios.
 - Se instalarán todas las librerías de Python y Qiskit requeridas para el desarrollo del proyecto, además de configurar el entorno de trabajo basado en Anaconda.
 - Se recopilará y estudiará la documentación y recursos relacionados con los protocolos cuánticos, como el BB84 Protocol y el BM92 Protocol, para comprender sus fundamentos y sus aplicaciones.

3. **Diciembre 2023 – Febrero 2024:** Desarrollo del modelo cuántico utilizando Qiskit y Python.

- Se diseñarán y desarrollarán los circuitos cuánticos necesarios para implementar el modelo de optimización de portafolios utilizando la plataforma Qiskit.
- Se programarán las funciones objetivo y restricciones del problema de optimización utilizando tanto Python (Computación Clásica) como Qiskit (Computación Cuántica).
- Se realizarán pruebas y depuración del modelo cuántico para garantizar su correcto funcionamiento y eficiencia.
- Se documentará el proceso de desarrollo, el código fuente, las decisiones de diseño y las lecciones aprendidas.

4. **Febrero 2024 – Marzo 2024:** Evaluación de los resultados del modelo y análisis de datos.

- Se ejecutarán simulaciones y experimentos utilizando el modelo cuántico desarrollado para evaluar su eficacia en la optimización de portafolios.
- Se recopilarán y analizarán los resultados obtenidos, comparándolos con enfoques clásicos de optimización para determinar las ventajas y limitaciones de la computación cuántica.
- Se analizarán los datos y se extraerán conclusiones sobre el rendimiento y la escalabilidad del modelo cuántico.

5. **Marzo 2024 – Abril 2024:** Documentación de hallazgos y conclusiones.

- Se elaborará una documentación completa del proyecto, incluyendo la introducción, el estado del arte, la metodología, los resultados y las conclusiones.
- Se redactarán informes técnicos detallados sobre el desarrollo del modelo cuántico, los protocolos de comunicación basados en QKD y los hallazgos obtenidos.
- Se prepararán presentaciones y materiales visuales para comunicar los resultados del proyecto de manera efectiva a diferentes audiencias.

6. **Abril 2024 – Mayo 2024:** Preparación para futuras investigaciones y publicación de resultados.

- Se identificarán oportunidades para futuras investigaciones basadas en los hallazgos y conclusiones del proyecto.
- Se prepararán artículos para la publicación de los resultados en revistas científicas especializadas.
- Se explorarán oportunidades de financiamiento y se presentarán solicitudes de subvenciones o becas para dar continuidad al proyecto.

Para facilitar la gestión y seguimiento del proyecto, se utilizará la herramienta Trello [28]. Trello es una plataforma visual y colaborativa que permite organizar y supervisar el progreso de las tareas de manera eficiente; se utilizarán etiquetas y listas para categorizar las tareas según su prioridad y estado de completitud.

3.5 ESTIMACIÓN ECONÓMICA

La estimación económica presentada a continuación es una aproximación preliminar de los costes que irían asociados al desarrollo de este estudio. Es importante tener en cuenta que, dado el estado actual de la tecnología, con los ordenadores cuánticos aún en fase experimental, resulta complejo estimar con precisión los costes de lanzamiento de un modelo cuántico al mercado. Por lo tanto, esta estimación se centra principalmente en los gastos relacionados con la investigación, el desarrollo y la difusión de los resultados, sentando las bases para futuras aplicaciones comerciales a medida que la tecnología cuántica madure y se vuelva más accesible.

Seguidamente, una tabla con la estimación económica del proyecto:

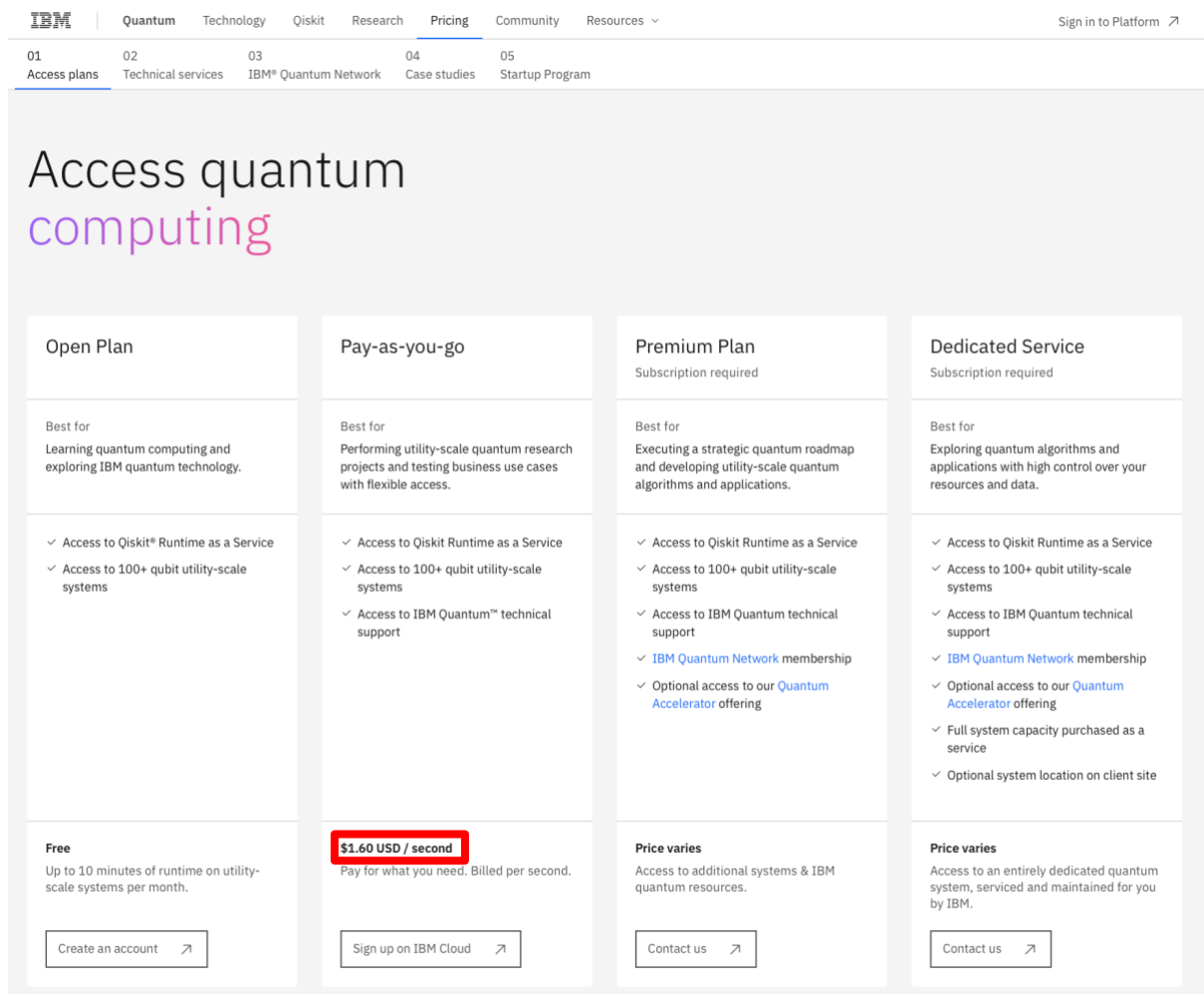
Concepto	Cantidad	Coste unitario	Coste total
Recursos humanos			
Investigador principal	1000 h	20 €/h	20000 €
Colaboradores externos	200 h	50 €/h	10000 €
Recursos técnicos			
Acceso a la plataforma Qiskit	1 hora	1.60€/seg	5760 €
Equipos informáticos	2	2500 €/u	5000 €
Publicaciones y difusión			
Costes de publicación en revistas científicas	1	2000 €/u	2000 €
Inscripción y asistencia a conferencias	1	1500 €/u	1500 €
Total			44260 €

Tabla 1 Estimación económica del proyecto.

Esta estimación económica incluye los principales costes que irían asociados al desarrollo del proyecto, divididos en tres categorías principales:

1. Recursos humanos: Incluye los costes del tiempo dedicado por el investigador principal y los colaboradores externos al proyecto. Se ha estimado una dedicación de 1000 horas por parte del investigador principal, a un coste de 20 €/hora, y una contribución de 200 horas por parte de colaboradores externos, a un coste de 50 €/hora.

2. Recursos técnicos: Incluye los costes relacionados con el acceso a la plataforma Qiskit y la adquisición de equipos informáticos. Para estimar el coste de uso de Qiskit, se ha tomado como referencia el precio oficial de 1,60 € por segundo, vigente a fecha de 24-05-2024. Teniendo en cuenta la duración estimada del proyecto y la necesidad de realizar simulaciones y experimentos, se ha calculado un total de 1 hora de uso de la plataforma, lo que supone un coste de 5760 €. Además, se ha presupuestado la adquisición de 2 equipos informáticos de altas prestaciones, a un coste unitario de 2500 €.



Open Plan	Pay-as-you-go	Premium Plan	Dedicated Service
Subscription required	Subscription required	Subscription required	Subscription required
Best for Learning quantum computing and exploring IBM quantum technology.	Best for Performing utility-scale quantum research projects and testing business use cases with flexible access.	Best for Executing a strategic quantum roadmap and developing utility-scale quantum algorithms and applications.	Best for Exploring quantum algorithms and applications with high control over your resources and data.
<ul style="list-style-type: none"> ✓ Access to Qiskit® Runtime as a Service ✓ Access to 100+ qubit utility-scale systems 	<ul style="list-style-type: none"> ✓ Access to Qiskit Runtime as a Service ✓ Access to 100+ qubit utility-scale systems ✓ Access to IBM Quantum™ technical support 	<ul style="list-style-type: none"> ✓ Access to Qiskit Runtime as a Service ✓ Access to 100+ qubit utility-scale systems ✓ Access to IBM Quantum technical support ✓ IBM Quantum Network membership ✓ Optional access to our Quantum Accelerator offering 	<ul style="list-style-type: none"> ✓ Access to Qiskit Runtime as a Service ✓ Access to 100+ qubit utility-scale systems ✓ Access to IBM Quantum technical support ✓ IBM Quantum Network membership ✓ Optional access to our Quantum Accelerator offering ✓ Full system capacity purchased as a service ✓ Optional system location on client site
Free Up to 10 minutes of runtime on utility-scale systems per month.	\$1.60 USD / second Pay for what you need. Billed per second.	Price varies Access to additional systems & IBM quantum resources.	Price varies Access to an entirely dedicated quantum system, serviced and maintained for you by IBM.
Create an account	Sign up on IBM Cloud	Contact us	Contact us

Fig. 12 Precios de Qiskit.

3. Publicaciones y difusión: Contempla los costes asociados a la publicación de resultados en revistas científicas y la participación en conferencias relevantes. Se ha estimado un

coste de 2000 € para la publicación en una revista científica de prestigio y 1500 € para la inscripción y asistencia a una conferencia internacional.

El coste total estimado del proyecto asciende a 44260 €. Es importante señalar que esta cifra es aproximada y podría variar según el precio/segundo de Qiskit y los posibles ajustes necesarios a lo largo del desarrollo.

Capítulo 4. ESTADO DEL ARTE

4.1 INTRODUCCIÓN

En este capítulo, revisaremos los fundamentos teóricos del entrelazamiento cuántico, su evolución histórica y los avances más recientes. Asimismo, se analizarán las aplicaciones potenciales del entrelazamiento cuántico en la industria de las telecomunicaciones, así como los protocolos cuánticos más relevantes y la comparación entre los sistemas de comunicación clásicos y cuánticos. Por último, se abordará la optimización de portafolios utilizando la computación cuántica, destacando sus ventajas e inconvenientes.

4.2 REVISIÓN DE LA LITERATURA CIENTÍFICA

4.2.1 FUNDAMENTOS DEL ENTRELAZAMIENTO CUÁNTICO

El entrelazamiento cuántico es uno de los fenómenos más fascinantes de la mecánica cuántica. Este fenómeno fue identificado por primera vez por Albert Einstein, Boris Podolsky y Nathan Rosen en 1935 [1]. Posteriormente, Erwin Schrödinger contribuyó con varios artículos [2], [3], que describieron lo que más tarde se conocería como la paradoja EPR (Einstein-Podolsky-Rosen).

La paradoja EPR fue propuesta para cuestionar la interpretación de la mecánica cuántica, sugiriendo que la teoría cuántica estaba incompleta. Según la mecánica cuántica, cuando dos partículas están entrelazadas, el medir el estado de una de ellas instantáneamente determina el estado de la otra, sin importar la distancia entre ellas [4]. Esta predicción parecía violar la teoría de la relatividad de Einstein, que establece que ninguna señal puede viajar más rápido que la luz. Esta aparente contradicción llevó a Einstein a describir el entrelazamiento cuántico como una "*acción espeluznante a distancia*" ("*spooky action at a distance*", expresión mas comúnmente conocida en inglés)

A pesar de las dudas iniciales, el entrelazamiento cuántico ha sido demostrado por numerosos experimentos. Una característica crucial del entrelazamiento es que las correlaciones entre las partículas entrelazadas no pueden explicarse mediante ninguna teoría clásica local. Esto fue demostrado por John Bell en 1964 con su famoso teorema de Bell [29], que definen una forma de distinguir entre predicciones cuánticas y las de cualquier teoría local realista.

4.2.2 EVOLUCIÓN HISTÓRICA Y AVANCES RECIENTES

La evolución del entrelazamiento cuántico ha pasado por varias etapas significativas desde sus inicios hasta los avances más recientes. Tras la formulación de la paradoja EPR y el teorema de Bell, la comunidad científica se embarcó en una serie de experimentos para verificar las predicciones de la mecánica cuántica.

En la década de 1980, los experimentos de Alain Aspect y sus colaboradores demostraron las primeras pruebas sólidas del entrelazamiento cuántico [30]. Estos experimentos no solo demostraron el entrelazamiento, sino que también descartaron las teorías de variables ocultas locales, que intentaban explicar las correlaciones cuánticas mediante factores no observables.

En las décadas siguientes, el desarrollo de tecnologías avanzadas permitió la manipulación precisa de partículas cuánticas, llevando a una explosión de investigación en el sector. Los avances en la tecnología láser y la óptica cuántica permitieron la creación de estados entrelazados de fotones con alta fidelidad [31]. Esto abrió la puerta a aplicaciones prácticas como la criptografía cuántica, con el primer protocolo QKD denominado BB84 [32].

La década de 1990 y principios de los 2000 vieron el desarrollo de la computación cuántica, con propuestas teóricas como el algoritmo de Shor [33] para la factorización de números enteros y el algoritmo de Grover [34] para la búsqueda en bases de datos no estructuradas, ambos dependientes del entrelazamiento cuántico. Estos avances teóricos fueron acompañados por experimentos que demostraron la viabilidad de puertas lógicas cuánticas y circuitos cuánticos simples [35].

En una época en la que las amenazas de ciberseguridad son cada vez más sofisticadas, la aplicación del cifrado cuántico en las comunicaciones por satélite se vuelve imperativa. Las comunicaciones por satélite exigen medidas de seguridad sólidas para proteger los datos transmitidos a través del espacio. QKD establece canales de comunicación seguros entre la Tierra y los satélites, salvaguardando información sensible y previniendo la interceptación [36]. Como ejemplo, investigadores en China demostraron que su satélite, llamado Micius, creó una clave segura que podría usarse para cifrar y descifrar mensajes a lo largo de una distancia de 1.000 kilómetros [37].

El desarrollo de repetidores cuánticos, que permiten extender el alcance de la comunicación cuántica superando los problemas de decoherencia, y los avances en la fabricación de dispositivos cuánticos escalables, como los qubits superconductores y los qubits de trampa de iones, han llevado a una aceleración en la investigación y desarrollo de las tecnologías cuánticas.

4.2.3 APLICACIONES DEL ENTRELAZAMIENTO CUÁNTICO EN LAS TELECOMUNICACIONES

Cada vez más empresas y proyectos de investigación se están centrando en avanzar en la aplicación del entrelazamiento cuántico en las telecomunicaciones [38]. Las compañías están explorando formas de comercializar tecnologías de comunicación cuántica, desarrollar soluciones prácticas de cifrado cuántico y mejorar la confiabilidad de las redes cuánticas.

El mercado global de tecnología cuántica se estima que va a alcanzar una cifra de 53.2 mil millones de dólares para 2028 [39]. Varias economías importantes, entre ellas Estados Unidos, Suiza, Reino Unido, Alemania, India y China, ya han iniciado programas nacionales destinados a respaldar el desarrollo de tecnologías cuánticas [40]. La iniciativa Quantum Flagship, respaldada por la Unión Europea, lidera la investigación cuántica. Con un presupuesto que supera los mil millones de euros y abarca una década [41]. Su objetivo es situar a Europa a la vanguardia, resaltando el reconocimiento global de las tecnologías cuánticas como un catalizador para el futuro de varias industrias.

Todo parece indicar que los sistemas cuánticos tendrán capacidades que superarán a las de los super-ordenadores más poderosos de hoy. A medida que la comunidad global de investigadores, científicos, ingenieros y líderes empresariales cuánticos colaboran para avanzar en el ecosistema, se espera ver un aumento en el impacto cuántico en todos los sectores [42].

¿Cómo podrían afectar las tecnologías cuánticas a la industria de las telecomunicaciones?

- **Distribución Cuántica de Claves (QKD):** Utiliza los principios cuánticos de superposición y entrelazamiento para establecer claves de cifrado inquebrantables [43]. Dado que el acto de medir un estado cuántico entrelazado lo perturba, cualquier intento de espionaje sería detectable [44]. Esta tecnología puede mejorar significativamente la seguridad de la transmisión de datos, especialmente para comunicaciones sensibles como las industrias críticas o transacciones financieras.
- **Teletransportación Cuántica:** La teletransportación, que se basa en el entrelazamiento, permite la transmisión de información cuántica de un lugar a otro, incluso a largas distancias, sin la transferencia física de partículas [5]. Esto también podría utilizarse para las comunicaciones cuánticas seguras y de alta fidelidad a larga distancia.
- **Redes de Comunicación Cuántica:** Basándose en los principios de la mecánica cuántica, se pueden establecer redes de comunicación cuántica. Estas redes permitirían la distribución de información cuántica entre múltiples nodos, lo que posibilitaría la comunicación cuántica segura y potencialmente nuevas aplicaciones, i.e. Internet Cuántico [45].
- **Criptografía Cuántica:** Los protocolos criptográficos basados en la Física Cuántica pueden mejorar la seguridad de las telecomunicaciones. Por ejemplo, algoritmos de criptografía resistentes a la computación cuántica pueden proteger contra ataques cuánticos a los métodos de cifrado clásicos [46], e.g. RSA.

- **Repetidores Cuánticos:** A lo largo de largas distancias, el entrelazamiento tiende a degradarse debido a factores ambientales, denominados Decoherencia [47]. Se están desarrollando repetidores cuánticos, que utilizan técnicas de intercambio y purificación de entrelazamiento, para ampliar el alcance de la comunicación.
- **Comunicaciones Satelitales Cuánticas:** Las comunicaciones por satélite sirven como la columna vertebral de la conectividad global, facilitando la comunicación en regiones remotas y habilitando servicios críticos como la navegación y la predicción meteorológica. La integración de las comunicaciones por satélite en el ecosistema cuántico introduce una nueva era de intercambio de datos seguros e íntegros.
- **Computación Cuántica:** Con la capacidad para resolver problemas muy complejos en fracciones de tiempo comparadas con los ordenadores clásicos, tiene el potencial de transformar muchas industrias; aunque aún está en sus primeras etapas de desarrollo.

Los avances en las tecnologías de telecomunicación han allanado el camino para el desarrollo de algoritmos de próxima generación que pueden abordar la creciente complejidad y los requisitos de procesamiento de datos de las redes modernas. Las industrias se enfrentan ahora a conjuntos de datos más grandes y complejos, lo que presenta desafíos computacionales que el aprendizaje automático convencional lucha por gestionar de manera eficiente. La Inteligencia Artificial Cuántica (QAI) emerge como una solución prometedora, ofreciendo el potencial de resolver problemas complejos que actualmente están más allá del alcance de los métodos algorítmicos clásicos [48].

4.3 PROTOCOLOS CUÁNTICOS

En este apartado se describirán en detalle los fundamentos y el funcionamiento de protocolos como el BB84 y el BBM92, así como otros protocolos QKD. Se discutirán las ventajas y limitaciones de cada protocolo y, su implementación práctica los sistemas de comunicación.

4.3.1 PROTOCOLO BB84

El protocolo BB84, ideado por Charles Bennett y Gilles Brassard en 1984 [32], es el primer y más conocido protocolo QKD. Fundamentado en los principios de la mecánica cuántica para garantizar la seguridad de la transmisión de claves criptográficas, la idea principal del BB84 es utilizar las propiedades de los fotones, que pueden existir en múltiples estados cuánticos, para codificar la información.

En el BB84, las claves se transmiten utilizando dos bases de polarización: rectilínea (0° y 90°) y diagonal (45° y 135°). Alice, la transmisora, envía fotones polarizados al azar en una de estas dos bases. Bob, el receptor, mide cada fotón en una de las dos bases seleccionadas aleatoriamente. Debido a la naturaleza cuántica de los fotones, si Bob mide en la misma base que Alice usó para enviar el fotón, obtendrá el mismo resultado. Si utiliza la base incorrecta, obtendrá un resultado aleatorio.

Una vez que todos los fotones han sido enviados y medidos, Alice y Bob comparan públicamente las bases que usaron para cada fotón, sin revelar los resultados de las mediciones. Solo los fotones medidos en las mismas bases son utilizados para generar la clave compartida. La seguridad del protocolo BB84 proviene del hecho de que cualquier intento de interceptar y medir los fotones alterará sus estados cuánticos, lo que será detectable por Alice y Bob.

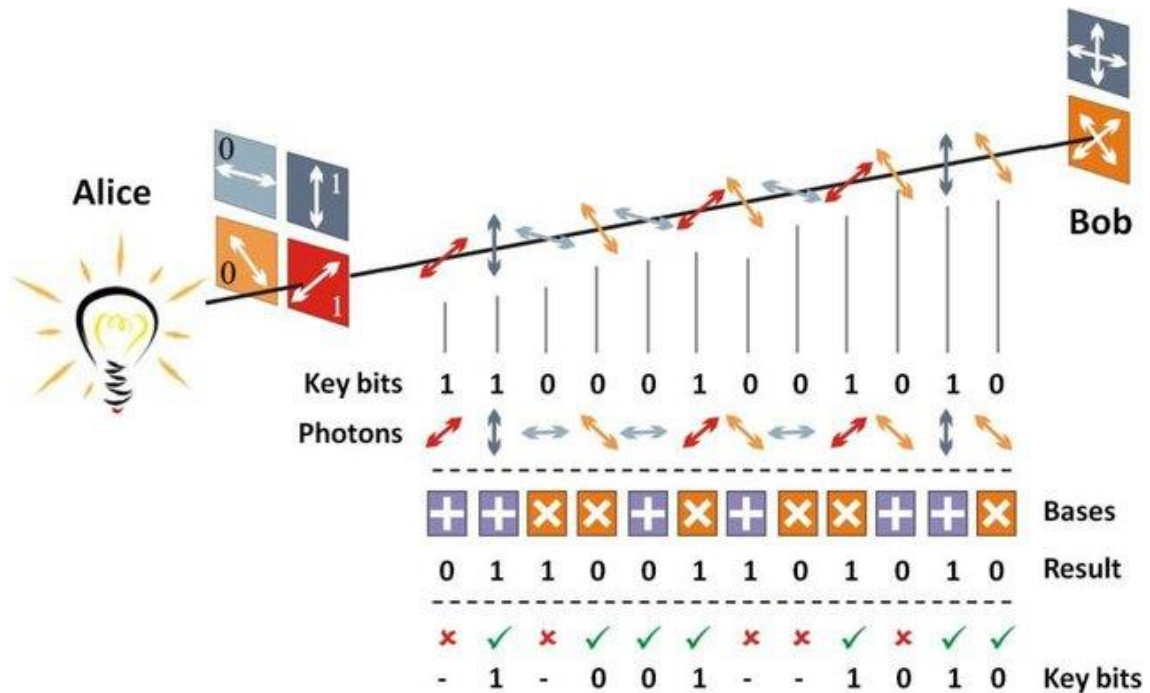


Fig. 13 Esquema básico del protocolo BB84 [49].

El BB84 ha sido implementado en numerosos experimentos y sistemas comerciales, demostrando su viabilidad práctica. Las principales ventajas del BB84 son su simplicidad y su robustez contra ataques de interceptación. Sin embargo, su principal limitación es la tasa de error, que puede aumentar en presencia de ruidos y pérdidas en el canal de comunicación [6].

4.3.2 PROTOCOLO BBM92

El protocolo BBM92, propuesto por Bennett y Brassard en 1992 [50], fue otra aportación importante en el sector de la comunicaciones. A diferencia del BB84, que utiliza cuatro estados cuánticos, el BBM92 emplea solo dos estados no ortogonales para transmitir la clave.

En el BBM92, Alice selecciona uno de los dos estados cuánticos no ortogonales para codificar cada bit de la clave. Bob, al recibir el fotón, utiliza un detector que discrimina entre los dos estados con cierta probabilidad de éxito. Si Bob detecta el fotón correctamente, puede determinar el bit correspondiente; si no, simplemente descarta el fotón.

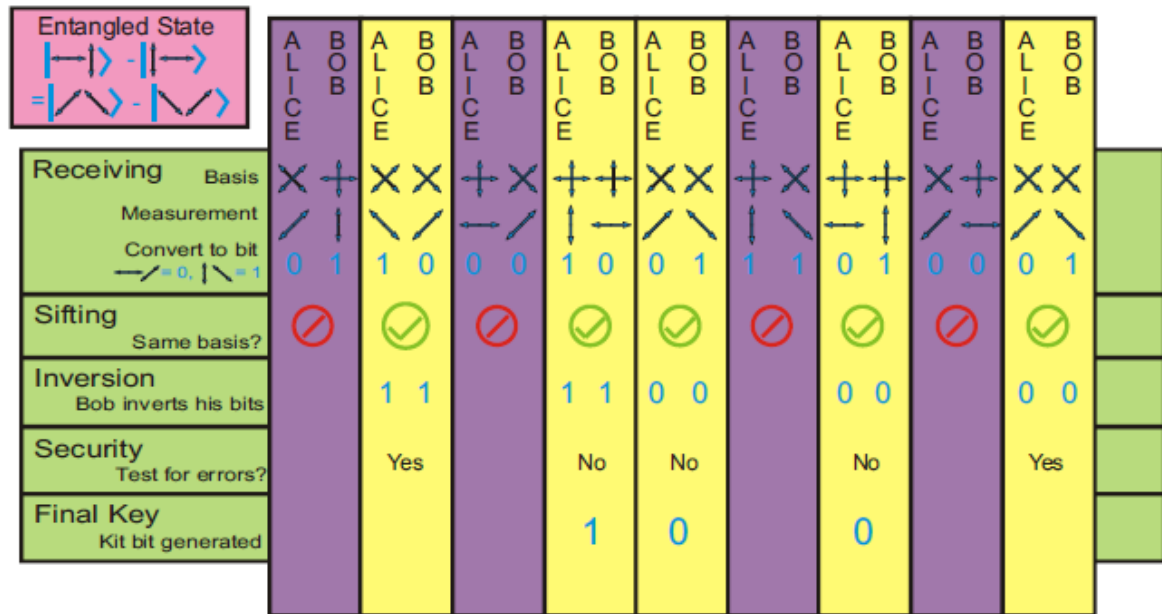


Fig. 14 Esquema básico del protocolo BBM92 [51].

La seguridad del BBM92 se basa en el hecho de que los estados no ortogonales no pueden ser distinguidos con certeza sin introducir errores. Cualquier intento de interceptar y medir los fotones por un espía será detectado por la introducción de errores adicionales en la clave. El BBM92 tiene la ventaja de ser conceptualmente más simple y utilizar menos recursos en términos de estados cuánticos, lo que puede ser beneficioso en algunos entornos prácticos.

Sin embargo, el BBM92 también tiene restricciones similares al BB84 en términos de sensibilidad a los errores y las pérdidas en el canal de comunicación. Su tasa de generación de claves puede ser menor debido a la probabilidad de descarte de fotones.

4.3.3 OTROS PROTOCOLOS DE DISTRIBUCIÓN CUÁNTICA DE CLAVES (QKD)

Además de los protocolos BB84 y BBM92, existen varios otros protocolos QKD que han sido desarrollados para mejorar la seguridad, la eficiencia y la practicidad de las comunicaciones cuánticas. Algunos de estos protocolos incluyen:

- **Protocolo E91:** Propuesto por Artur Ekert en 1991 [52], el protocolo E91 también se basa en el entrelazamiento cuántico y utiliza pares de partículas entrelazadas para

distribuir claves seguras. En este protocolo, Alice y Bob comparten pares de partículas entrelazadas y realizan mediciones en bases elegidas al azar. Las correlaciones cuánticas entre las partículas garantizan la seguridad de la clave, y cualquier intento de interceptación será detectable a través de la violación de las desigualdades de Bell.

- **Protocolo SARG04:** Desarrollado por Scarani, Acín, Ribordy y Gisin en 2002 [53], el protocolo SARG04 es una variante del BB84 que mejora la seguridad contra determinados tipos de ataques, como el ataque de interceptación y reenvío. En el SARG04, los estados cuánticos son codificados de manera que la información sobre la base utilizada se distribuye de manera más uniforme, aumentando la dificultad para un atacante de obtener información sin ser detectado.
- **Protocolo DPS (Differential Phase Shift):** La clave se codifica en las diferencias de fase entre pulsos sucesivos de luz. Bob mide las diferencias de fase para reconstruir la clave; particularmente robusto contra algunos tipos de ataques porque la información está distribuida en múltiples pulsos en lugar de estar contenida en un solo fotón [54].
- **Protocolo COW (Coherent One-Way):** Propuesto para simplificar la implementación de QKD en redes ópticas existentes, el protocolo COW utiliza pulsos coherentes enviados en una única dirección [55]. La información de la clave se codifica en la presencia o ausencia de pulsos de luz en intervalos de tiempo específicos. Destaca por su simplicidad y compatibilidad con la infraestructura óptica estándar, aunque puede requerir técnicas avanzadas para garantizar la seguridad contra ciertos ataques.

Cada uno de estos protocolos ofrece un conjunto único de ventajas y limitaciones, dependiendo de las necesidades específicas del sistema de comunicación cuántica en cuestión. La elección correcta depende de factores como la distancia de transmisión, la tasa de generación de claves, la resistencia a ataques y la compatibilidad con la infraestructura existente.

En términos de implementación práctica, los protocolos QKD han avanzado considerablemente en los últimos años. Empresas y laboratorios de investigación han desarrollado sistemas comerciales QKD que están siendo probados y utilizados en aplicaciones del mundo real. Por ejemplo, IDQuantique y Toshiba han desarrollado productos QKD que se utilizan para asegurar la transmisión de datos en redes financieras y gubernamentales [56].

Un desafío importante en la implementación de QKD es la necesidad de infraestructuras avanzadas para manejar y procesar estados cuánticos. Esto incluye fuentes de fotones individuales, detectores de alta eficiencia y redes de fibra óptica de baja pérdida. A medida que la tecnología avanza, se espera que estos componentes se vuelvan más accesibles y económicos, facilitando la adopción más amplia de QKD en diversas industrias.

En definitiva, cada protocolo tiene sus propias fortalezas y debilidades, y su implementación exitosa depende de los requisitos del sistema y las condiciones del entorno de comunicación. Con los continuos avances en la tecnología cuántica y la creciente necesidad de seguridad en las comunicaciones, es probable que veamos una mayor acogida de estos protocolos en el futuro cercano.

4.4 COMPARACIÓN ENTRE SISTEMAS DE COMUNICACIÓN CLÁSICOS Y CUÁNTICOS

En esta sección se realizará una comparación entre los sistemas de comunicación clásicos y cuánticos, destacando las ventajas y desventajas de cada uno. Se analizarán las diferencias fundamentales en términos de seguridad, capacidad de transmisión y eficiencia, y se discutirán las perspectivas futuras de los sistemas de comunicación cuántica.

4.4.1 LIMITACIONES DE LOS SISTEMAS DE COMUNICACIÓN CLÁSICOS

Los sistemas de comunicación clásicos, basados en la teoría de la información de Shannon [57], han sido el fundamento principal de la transmisión de datos durante décadas. Sin embargo, estos sistemas presentan varias limitaciones.

La seguridad en los sistemas de comunicación clásicos se basa en la criptografía algorítmica, donde la fortaleza de la encriptación depende de la complejidad matemática de los algoritmos y de la longitud de las claves utilizadas. Métodos criptográficos comunes como RSA [58] y AES [59] son actualmente seguros, pero con el avance de la computación cuántica, estas técnicas podrían volverse vulnerables. Un ordenador cuántico suficientemente potente podría resolver problemas matemáticos complejos en tiempos prácticos, amenazando la seguridad de estos sistemas clásicos.

La capacidad de transmisión en los sistemas clásicos también tiene impedimentos. La tasa de transmisión de datos está sujeta a restricciones físicas, como el ancho de banda disponible y la interferencia en los canales de comunicación. Aunque las tecnologías avanzadas, como la fibra óptica y las comunicaciones por satélite, han aumentado significativamente las capacidades de transmisión, aún existen límites inherentes a estas tecnologías. La Ley de Shannon-Hartley establece que la capacidad de un canal de comunicación es limitada por su ancho de banda y la relación señal-ruido, lo que impone un techo teórico a la cantidad de información que puede ser transmitida de manera confiable [60].

La latencia, o el retraso en la transmisión de datos, puede ser relevante en largas distancias, especialmente en sistemas basados en satélites [61]. Por otro lado, la eficiencia energética de los sistemas clásicos, aunque ha mejorado con tecnologías más avanzadas, sigue siendo un desafío en aplicaciones de gran escala y alta demanda de datos.

4.4.2 VENTAJAS DE LOS SISTEMAS DE COMUNICACIÓN CUÁNTICOS

Los sistemas de comunicación cuánticos, basados en principios de la mecánica cuántica como el entrelazamiento [4] y la superposición [62], prometen superar muchas de las limitaciones de los sistemas clásicos.

Una de las mayores ventajas de estos sistemas es su seguridad intrínseca. Con los protocolos QKD, cualquier intento de interceptar las claves de encriptación altera los estados cuánticos de las partículas, lo que puede ser detectado por los participantes legítimos de la comunicación, como se explicó anteriormente. Este principio permite una seguridad basada

en las leyes de la Física, en lugar de en la complejidad matemática, haciendo que las comunicaciones cuánticas sean resistentes incluso a los ataques de ordenadores cuánticos.

Aunque los sistemas de comunicación cuánticos están en una etapa de desarrollo temprana, tienen el potencial de ofrecer capacidades de transmisión mejoradas. Las tecnologías como la teletransportación cuántica [5] y las redes de comunicación cuántica [63] podrían permitir la transmisión de información cuántica a través de largas distancias sin degradación de la señal, superando algunas de las limitaciones físicas impuestas a los sistemas clásicos. Además, la codificación cuántica de la información podría aumentar la densidad de datos transmitidos por unidad de tiempo [64].

Estos sistemas prometen mejoras en la eficiencia y la latencia. La capacidad de realizar comunicaciones instantáneas a través de entrelazamiento cuántico, aunque teóricamente todavía en exploración, podría reducir drásticamente la latencia en las comunicaciones. Aparte, los avances en tecnologías de fotones individuales [65] están mejorando la eficiencia energética de estos sistemas.

La compatibilidad con las redes de fibra óptica y las plataformas de comunicación por satélite es esencial para una transición fluida hacia tecnologías cuánticas, i.e. Quantum Internet. Se están desarrollando soluciones híbridas que combinan elementos de la comunicación clásica y cuántica para facilitar esta integración, aprovechando las fortalezas de ambos enfoques [66].

4.5 OPTIMIZACIÓN DE PORTAFOLIOS CON COMPUTACIÓN CUÁNTICA

La optimización de portafolios es un campo esencial dentro de las finanzas que busca maximizar el retorno esperado de una inversión mientras se minimiza el riesgo asociado. Este apartado se centra en cómo la computación cuántica puede revolucionar este proceso, ofreciendo nuevas herramientas y métodos para gestionar de manera más efectiva los portafolios financieros.

4.5.1 INTRODUCCIÓN A LA OPTIMIZACIÓN DE PORTAFOLIOS

La optimización de portafolios se basa en la teoría moderna de carteras desarrollada por Harry Markowitz en la década de 1950 [67]. Su modelo de media-varianza introduce el concepto de diversificación para reducir el riesgo de inversión. Según Markowitz, un portafolio óptimo es aquel que maximiza el retorno esperado para un nivel dado de riesgo o minimiza el riesgo para un retorno esperado específico.

En términos matemáticos, la optimización de portafolios involucra la selección de un conjunto de activos financieros que cumplan ciertos criterios de rendimiento y riesgo. Esto se representa comúnmente mediante la función de media-varianza, donde se calcula el retorno esperado como la media ponderada de los retornos esperados de los activos individuales, y el riesgo se mide mediante la varianza o desviación estándar de estos retornos.

$$E(R_p) = \sum_i w_i E(R_i)$$

$$\sigma_p^2 = \sum_i \sum_j w_i w_j \sigma_{ij}$$

Donde:

- $E(R_p)$ es el retorno esperado del portafolio.
- w_i es el peso de la inversión en el activo i .
- $E(R_i)$ es el retorno esperado del activo i .
- σ_p^2 es la varianza del portafolio.
- σ_{ij} es la covarianza entre los retornos de los activos i y j .

La optimización implica resolver este problema para determinar los pesos w_i que minimicen el riesgo para un nivel dado de retorno esperado, o viceversa.

4.5.2 MÉTODOS CLÁSICOS DE OPTIMIZACIÓN DE PORTAFOLIOS

Los métodos clásicos de optimización de portafolios incluyen una variedad de técnicas matemáticas y heurísticas que han sido desarrolladas y perfeccionadas a lo largo de los años. Entre las más utilizadas se encuentran:

1. **Programación Cuadrática (QP):** Utilizada para resolver problemas de optimización de media-varianza, donde el objetivo es minimizar una función cuadrática (varianza) sujeta a restricciones lineales (retornos esperados y pesos de activos) [68].
2. **Optimización por Restricciones (Constrained Optimization):** Este método aplica restricciones adicionales, como límites en los pesos de los activos o requisitos de liquidez, para generar soluciones más prácticas y realistas [69].
3. **Optimización con Restricciones de Tracking Error:** Este planteamiento minimiza el tracking error, que es la diferencia entre el rendimiento del portafolio y el de un índice de referencia, sujeto a una restricción de riesgo [70].
4. **Técnicas Heurísticas:** Con métodos como algoritmos genéticos, búsqueda tabú y optimización de enjambre de partículas, útiles para problemas complejos y no lineales donde los métodos exactos pueden no ser factibles [71].
5. **Optimización de Valor en Riesgo (VaR) y Valor en Riesgo Condicional (CVaR):** Técnicas centradas en minimizar el riesgo de pérdidas extremas, utilizando medidas de riesgo más sofisticadas que la varianza [72].

A pesar de su eficacia, estos métodos sufren limitaciones, especialmente cuando se trata de problemas de gran escala con muchas variables y restricciones. Los cálculos pueden volverse computacionalmente intensivos y lentos, lo que limita su función en entornos de mercado dinámicos y de alta frecuencia.

4.5.3 ALGORITMOS CUÁNTICOS EN LA OPTIMIZACIÓN DE PORTAFOLIOS

La computación cuántica ofrece una nueva perspectiva para abordar los desafíos de la optimización de portafolios. Los algoritmos cuánticos prometen mejoras en la velocidad y la eficiencia de los cálculos, permitiendo resolver problemas que son computacionalmente muy complicados para los ordenadores clásicos.

Uno de los algoritmos cuánticos más populares es el Algoritmo Variacional Cuántico (VQE) [73]. VQE utiliza un circuito cuántico parametrizado para representar el portafolio, donde los pesos de los activos se codifican en los parámetros del circuito. El algoritmo optimiza iterativamente estos parámetros para minimizar una función objetivo, como la varianza del portafolio, usando una combinación de computación cuántica y clásica. La naturaleza híbrida de VQE lo hace adecuado para su implementación en hardware cuántico sensible al ruido térmico y de escala moderada.

Otra técnica interesante es el Algoritmo de Optimización Cuántica Aproximada (QAOA), que es especialmente adecuado para problemas de optimización combinatoria [74]. QAOA construye un estado cuántico que codifica la solución al problema de optimización mediante la aplicación de una secuencia de puertas cuánticas parametrizadas. Los parámetros se optimizan utilizando un optimizador clásico para maximizar la probabilidad de medir el estado correspondiente a la solución óptima. En el contexto de la optimización de portafolios, QAOA puede utilizarse para identificar la asignación óptima de activos teniendo en cuenta restricciones como el presupuesto y los límites de inversión.

El Annealing Cuántico es otra técnica que ha atraído un interés considerable para la optimización de portafolios [75]. En contraste con la computación cuántica basada en puertas, el Annealing Cuántico utiliza la evolución adiabática de un sistema cuántico para encontrar el estado fundamental de una función objetivo. Este proceso puede verse como una forma de túnel cuántico, que permite al sistema escapar de mínimos locales y converger hacia la solución óptima global. Las plataformas de Annealing Cuántico, como las desarrolladas por D-Wave Systems, han demostrado un potencial significativo para resolver problemas de optimización a gran escala, como la optimización de portafolios [76].

Aparte de los algoritmos puramente cuánticos, se están desarrollando algoritmos híbridos que combinan la computación cuántica y clásica para aprovechar las fortalezas de ambas. Estos algoritmos dividen el problema en partes que se resuelven mejor en un ordenador clásico y en un ordenador cuántico. En la optimización de portafolios, estos métodos híbridos pueden acelerar el proceso de identificación de la frontera eficiente, permitiendo a los gestores de portafolios tomar decisiones más informadas en tiempo real.

4.5.4 VENTAJAS Y DESAFÍOS DE LA OPTIMIZACIÓN CUÁNTICA DE PORTAFOLIOS

En esta sección final se discutirán las ventajas y desafíos de la computación cuántica en la optimización de portafolios. Se destacarán las oportunidades que ofrece esta aproximación, y se analizarán los desafíos técnicos y prácticos que se deben superar para hacer realidad estas ventajas.

Uno de los principales beneficios de la optimización cuántica de portafolios es la mejora en la eficiencia y velocidad de los cálculos. Los algoritmos cuánticos, como VQE y QAOA, prometen resolver problemas de optimización complejos en una fracción del tiempo que requieren los métodos clásicos [77]. Esto es especialmente relevante en el contexto de la gestión de portafolios, donde la capacidad de tomar decisiones rápidas y precisas puede tener un impacto en los resultados financieros. La naturaleza paralela de la computación cuántica permite explorar un amplio espacio de soluciones simultáneamente, lo que puede conducir a la identificación de oportunidades de inversión óptimas que podrían pasar desapercibidas utilizando enfoques tradicionales [78].

Además de la eficiencia computacional, la optimización cuántica de portafolios también ofrece la posibilidad de abordar problemas más complejos y realistas. Los algoritmos cuánticos pueden manejar de manera más efectiva las no linealidades, las interdependencias y las restricciones que caracterizan a los mercados financieros del mundo real [79]. Admitiendo la incorporación de una gama más amplia de factores de riesgo y objetivos de inversión en el proceso de optimización, lo que lleva a la construcción de portafolios más robustos y adaptados a las necesidades específicas de los inversores.

A pesar de estas ventajas prometedoras, la optimización cuántica de portafolios también enfrenta varios desafíos que deben ser superados para su implementación exitosa en la práctica. Uno de los principales desafíos es la escalabilidad de los sistemas cuánticos actuales. Aunque se han logrado avances relevantes en los últimos años, la mayoría de los dispositivos cuánticos disponibles todavía están limitados en términos de número de qubits y niveles de ruido [80]. Para abordar problemas de optimización de portafolios a gran escala que involucren cientos o miles de activos, se requerirán procesadores cuánticos más potentes y tolerantes al ruido. La corrección de errores cuánticos y las técnicas de mitigación de ruido serán cruciales para garantizar la precisión y la estabilidad de los cálculos cuánticos a medida que se escala a sistemas más grandes [81].

Otro desafío importante es la integración de los algoritmos cuánticos con los sistemas de trabajo financieros existentes. La optimización de portafolios no es un proceso aislado, sino que está estrechamente interconectado con una variedad de otras tareas, como el análisis de riesgo, la ejecución de operaciones y la generación de informes. Para aprovechar al máximo las capacidades de la computación cuántica, será necesario desarrollar interfaces y protocolos estandarizados que permitan una comunicación fluida entre los componentes cuánticos y clásicos del sistema [82].

La adopción generalizada de la optimización cuántica de portafolios también requerirá superar barreras organizativas y educativas. Los profesionales de las finanzas deberán adquirir nuevos conocimientos y habilidades para comprender y utilizar eficazmente estas herramientas cuánticas emergentes. Las empresas financieras tendrán que invertir en la capacitación de su personal, así como en la adquisición y el mantenimiento de la infraestructura necesaria para respaldar la computación cuántica. La creación de equipos multidisciplinarios que combinen experiencia en finanzas, matemáticas, informática y física será esencial para impulsar la innovación y la aplicación exitosa de estas tecnologías.

En conclusión, la optimización cuántica de portafolios presenta un enorme potencial para transformar la gestión de inversiones al ofrecer cálculos más rápidos, precisos y complejos. Sin embargo, para hacer realidad estas ventajas, será necesario superar desafíos relacionados

con la escalabilidad, la integración y la adopción. A medida que la tecnología cuántica continúa evolucionando y madurando, se espera que desempeñe un papel cada vez más importante en el futuro de las finanzas, permitiendo a los administradores de portafolios tomar decisiones más informadas y optimizadas en un mercado global en constante cambio.

Capítulo 5. MODELO DESARROLLADO

En este capítulo se presentan los modelos desarrollados para la optimización de portafolios, Se abordarán los conceptos fundamentales y se definirá el problema a resolver. Posteriormente, se explicarán en detalle el modelo de optimización clásico y cuántico, destacando las herramientas y algoritmos específicos empleados en cada uno.

5.1 INTRODUCCIÓN

La optimización de portafolios es habitual en las finanzas, tratando de busca la mejor combinación de activos para maximizar el retorno y minimizar el riesgo. Tradicionalmente, se han utilizado métodos clásicos basados en las matemáticas y algoritmos determinísticos para resolver este problema. Sin embargo, con el avance de la computación cuántica, han surgido nuevas oportunidades para abordar este desafío de manera más eficiente y efectiva.

5.1.1 EL CONCEPTO DE MODELO

El concepto de modelo actúa como un puente crucial entre los dominios de la Física y la Ingeniería, facilitando la traducción de principios teóricos en aplicaciones prácticas. Un modelo es una representación simplificada de un sistema o fenómeno del mundo real, diseñado para capturar los elementos esenciales mientras abstrae las complejidades. Al crear marcos matemáticos o conceptuales que capturan la esencia de un fenómeno físico, los modelos permiten un entendimiento compartido que trasciende las fronteras disciplinarias. Adoptando un enfoque centrado en la industria, los ingenieros utilizan este modelo para diseñar soluciones innovadoras, optimizar procesos y avanzar en la excelencia operativa.

La interacción entre la Física y la Ingeniería no es una relación unidireccional; es perfectamente recíproca. Por un lado, la Física establece los principios y leyes fundamentales que gobiernan el comportamiento del mundo físico. Estos principios, como las leyes de Newton del movimiento o las ecuaciones de Maxwell del electromagnetismo, sirven como

bloques de construcción para la ingeniería. Los ingenieros dependen de estos principios para diseñar y analizar sistemas, asegurando que sus creaciones operen dentro de las restricciones de las leyes físicas. Por otro lado, la Ingeniería también contribuye a la Física proporcionando aplicaciones en el mundo real y desafíos que impulsan la investigación científica. Por ejemplo, el logro ingenieril del Gran Colisionador de Hadrones en el CERN ha resultado en avances significativos en el campo de la física de partículas, como el descubrimiento del bosón de Higgs [83].

5.1.2 ENFOQUE TENTATIVO

En la ciencia aplicada, el término "*tentativo*" se utiliza para describir algo que aún no es definitivo o cierto, pero que está sujeto a cambios o validación adicional. Cuando una idea, hipótesis, resultado o conclusión se describe como tentativa, indica que se basa en la evidencia y comprensión disponibles en un momento particular, pero permanece abierta a revisión a medida que más datos, experimentación o análisis estén disponibles.

Dentro del ecosistema de la investigación y experimentación científica cuántica, a menudo se extraen conclusiones *tentativas* cuando la evidencia disponible es sugerente pero no concluyente.

5.2 DEFINICIÓN DEL PROBLEMA

El problema de optimización de portafolios se define como la selección de un subconjunto de activos de un conjunto más grande, con el objetivo de minimizar el riesgo y maximizar el retorno esperado. En este estudio, se realizaron dos análisis distintos: uno con un portafolio de 5 acciones, conocidas como *FAANG* (Facebook, Amazon, Apple, Netflix y Google), y otro con un portafolio de 20 acciones. La selección del tamaño de estos portafolios se basa en las capacidades actuales de los simuladores cuánticos, como el de IBM, que pueden manejar hasta 30 variables, pero con una precisión y velocidad que disminuyen significativamente a partir de 20 variables debido a la complejidad computacional.

Para el portafolio de 5 acciones, el objetivo es seleccionar 3 acciones que ofrezcan el mayor beneficio, minimizando al mismo tiempo el riesgo al nivel determinado. En el caso del portafolio de 20 acciones, se decidió seleccionar 7 acciones. En ambos casos, se definió un nivel de riesgo del 10% sobre un total del 100%. Los datos necesarios para la construcción del portafolio se obtuvieron de la biblioteca de Yahoo Finance, introducida en el Capítulo 2, en el período comprendido entre el 1 de marzo de 2023 y el 1 de marzo de 2024.

En este proceso, se obtuvieron los valores de μ (retornos esperados), σ (desviación estándar de los retornos) y la matriz de correlación. Valores son fundamentales para la optimización del portafolio por varias razones:

- **Retornos Esperados (μ):** Representan la ganancia promedio que se espera obtener de cada activo. Son cruciales para identificar qué activos ofrecen las mejores oportunidades de retorno.
- **Desviación Estándar (σ):** Mide la volatilidad o el riesgo de los retornos de cada activo. Una desviación estándar más alta indica un mayor riesgo asociado con el activo.
- **Matriz de Correlación:** Muestra cómo los retornos de los distintos activos se mueven en relación unos con otros. Una baja correlación entre activos es deseable para diversificar el riesgo, ya que permite que las fluctuaciones negativas en algunos activos sean compensadas por las positivas en otros.

Estos componentes son los que nos permiten construir un portafolio que optimice el equilibrio entre riesgo y retorno, siguiendo los principios de la teoría moderna de portafolios.

La función objetivo se formula de la siguiente manera [84]:

$$\min_{x \in \{0,1\}^n} (qx^T \Sigma x - \mu^T x)$$

Sujeto a: $1^T x = B$

Donde:

- $x \in \{0,1\}^n$ es el vector de variables de decisión binarias que indica qué activos elegir ($x[i] = 1$) y cuáles no ($x[i] = 0$).
- $\mu \in R^n$ define los rendimientos esperados de los activos.
- $\Sigma \in R^{n \times n}$ especifica las covarianzas entre los activos.
- $q > 0$ controla el nivel de riesgo de quien toma las decisiones.
- B denota el presupuesto, es decir, el número de activos a ser seleccionados de n .

El primer término de la función objetivo, $qx^T\Sigma x$, representa el riesgo del portafolio. Al minimizar este término, se busca reducir el riesgo. El segundo término, $-\mu^T x$, representa el rendimiento esperado negativo del portafolio. Minimizar este término es equivalente a maximizar $\mu^T x$, lo que implica maximizar el rendimiento esperado.

La restricción $1^T x = B$ asegura que se seleccionen exactamente B activos en el portafolio.

Este problema de optimización combinatoria se formula como un QUBO (Quadratic Unconstrained Binary Optimization), que puede ser resuelto eficientemente utilizando algoritmos especializados, con enfoques cuánticos y clásicos [85].

La elección de minimizar en lugar de maximizar la función objetivo se debe a las convenciones en la optimización matemática. Al incluir el signo negativo en el término del rendimiento esperado ($-\mu^T x$), se convierte en un término que, al minimizarlo, maximiza el rendimiento esperado. Además, es común formular los problemas como problemas de minimización, ya que muchos algoritmos de optimización están diseñados para encontrar mínimos.

Las figuras Fig. 15 y Fig. 16 muestran, respectivamente, la matriz de covarianza y la matriz de correlación entre las acciones del portafolio de las FAANG (5 Activos). En la matriz de correlación, se destaca que Netflix (NFLX) y Amazon (AMZN) tienen la correlación más

alta, con un valor de 0.6173, mientras que Google (GOOGL) y Netflix (NFLX) presentan la correlación más baja, con un valor de 0.3045.



Fig. 15 Matriz de Covarianza - 5 Activos.

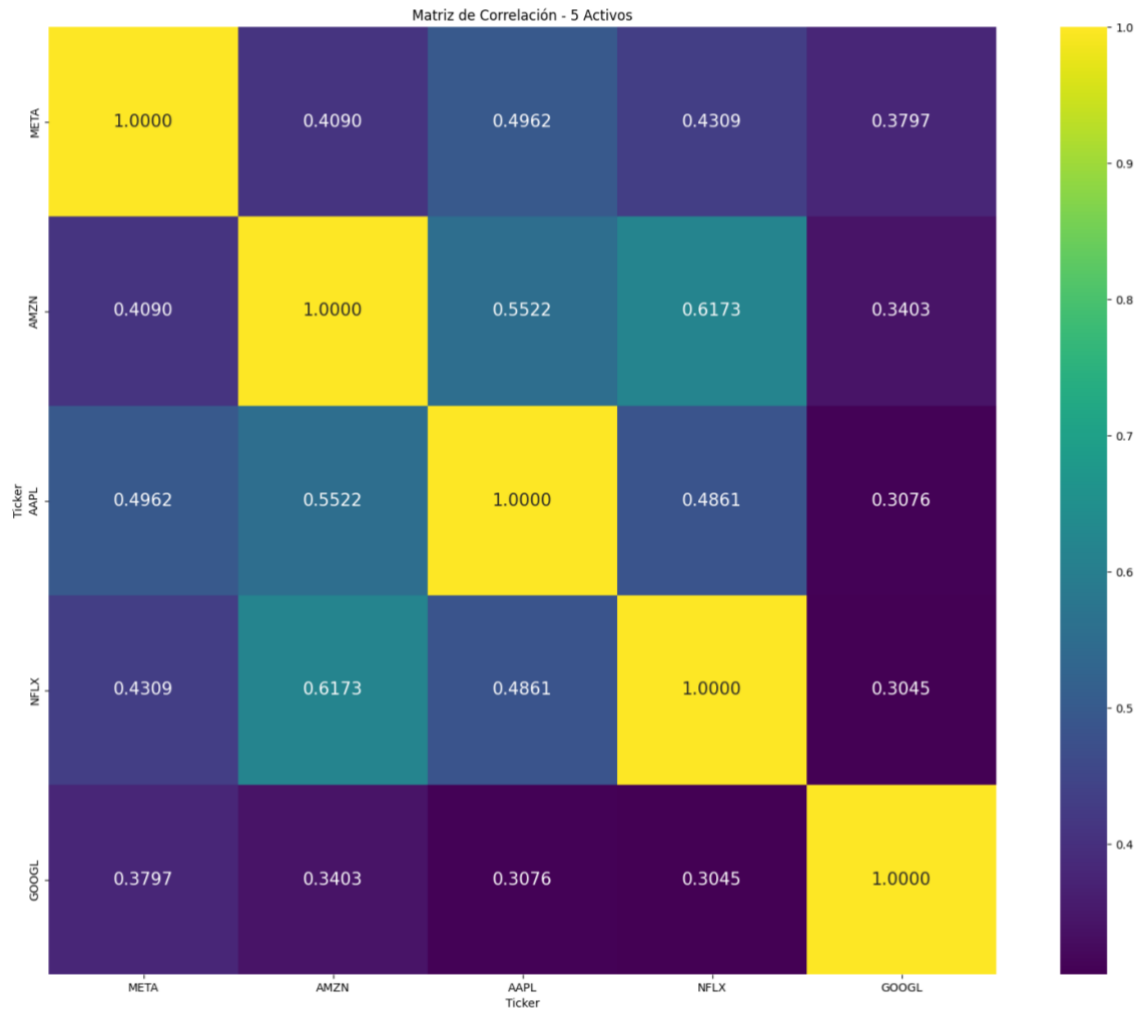


Fig. 16 Matriz de Correlación - 5 Activos.

Las figuras Fig. 17 y Fig. 18 muestran, respectivamente, la matriz de covarianza y la matriz de correlación entre las acciones del portafolio de 20 activos. En la matriz de correlación, vemos como Microsoft (MSFT) y AbbVie (ABBV) tienen la correlación más alta, con un valor de 0.8412, mientras que JPMorgan Chase (JPM) y AbbVie (ABBV) presentan la correlación más baja, con un valor de -0.1591. Es importante destacar el valor negativo, ya que esto implica una relación inversa entre los rendimientos de estos activos. Como consecuencia del gran número de activos, se recomienda hacer zoom para visualizar bien las figuras.

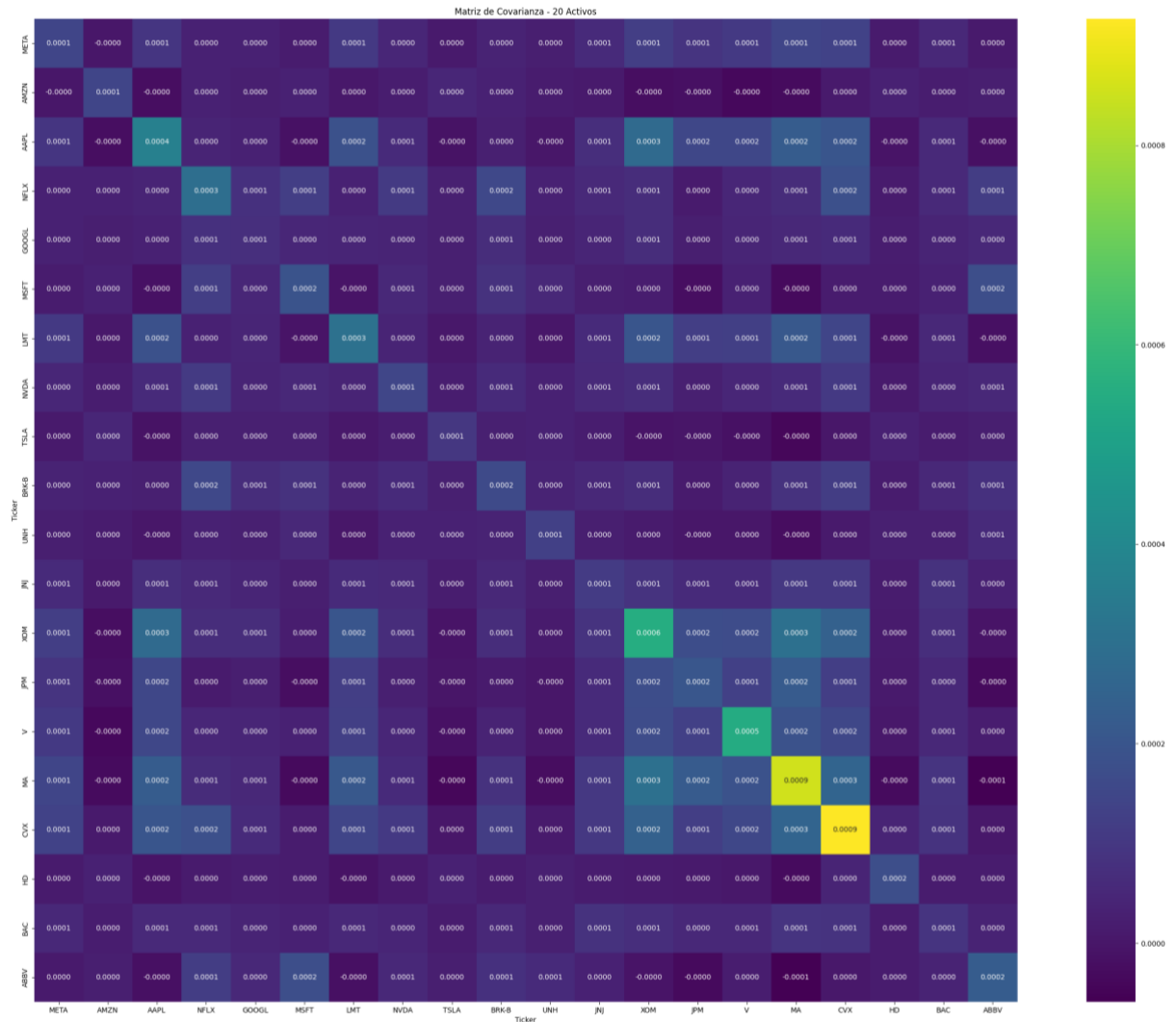


Fig. 17 Matriz de Covarianza - 20 Activos.

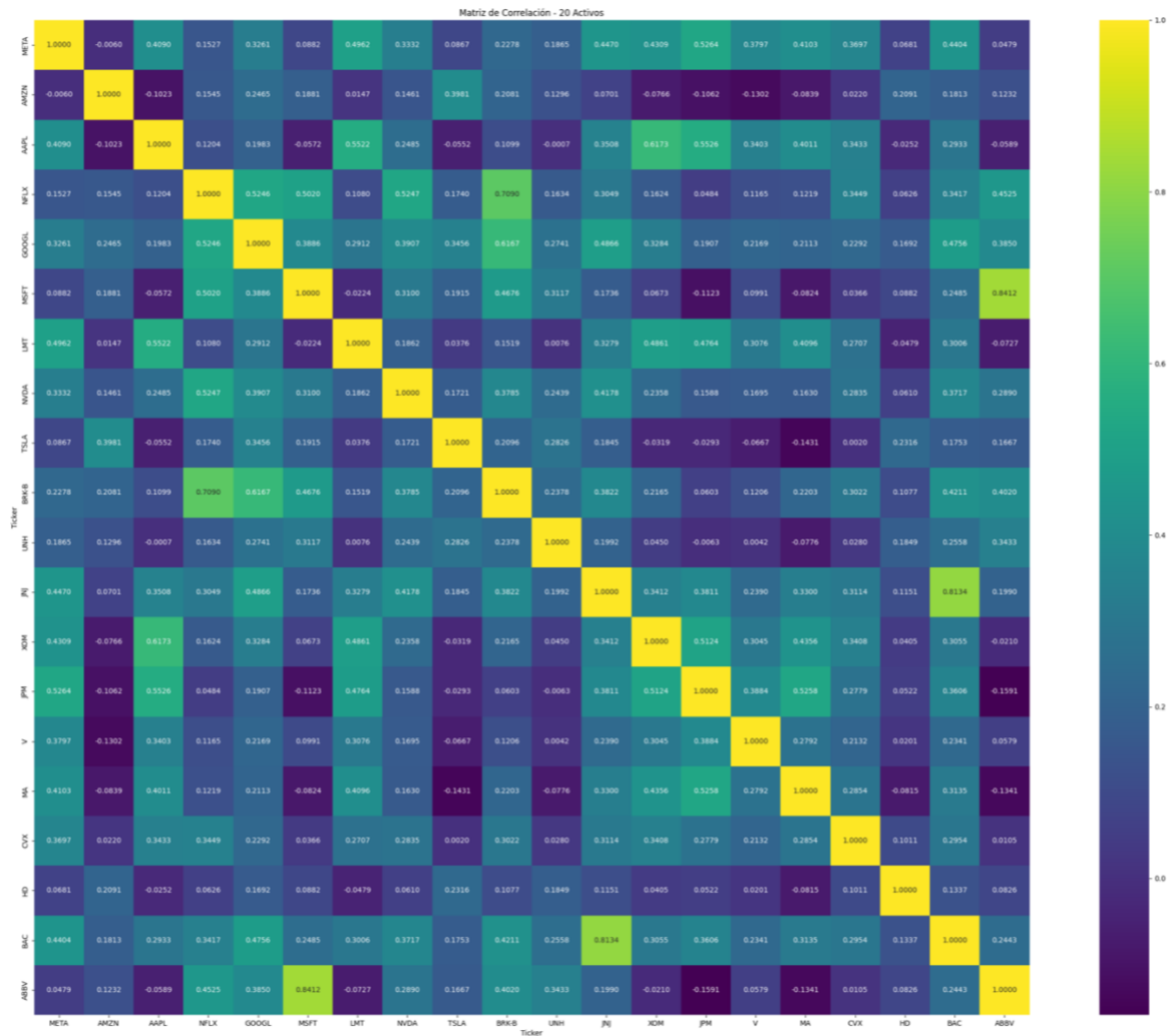


Fig. 18 Matriz de Correlación - 20 Activos.

5.3 *MODELO DE OPTIMIZACIÓN CLÁSICO*

El modelo de optimización clásico para la selección de portafolios se basa en técnicas tradicionales de programación matemática. Uno de los enfoques más utilizados es el modelo de media-varianza de Markowitz, que busca encontrar la asignación óptima de activos que minimice el riesgo del portafolio mientras se maximiza el retorno esperado, tal como vimos en el apartado 4.5.1 del presente documento.

Para este estudio, se empleó el optimizador CPLEX de Qiskit [86]. CPLEX es una herramienta de software de IBM ampliamente utilizada para resolver problemas de programación lineal y cuadrática de gran escala. Incorpora algoritmos eficientes y robustos para encontrar soluciones óptimas.

El primer paso en el modelo de optimización clásico es formular el problema como un programa cuadrático (QP). El QP captura la función objetivo y las restricciones del problema. La función objetivo, como se describió anteriormente, busca minimizar el riesgo del portafolio mientras se maximiza el retorno esperado. Las restricciones incluyen la limitación del presupuesto; i.e. la selección de un número específico de activos.

Una vez formulado el QP, se utiliza el optimizador CPLEX para resolverlo. CPLEX emplea algoritmos de programación matemática, como el método simplex y el método de punto interior, para encontrar la solución óptima [87]. Estos algoritmos exploran eficientemente el espacio de soluciones factibles y convergen hacia la solución que minimiza la función objetivo mientras satisface las restricciones.

El optimizador CPLEX destaca por su eficiencia y escalabilidad. Puede manejar problemas de optimización de gran tamaño con miles de variables y restricciones. Asimismo, CPLEX utiliza técnicas avanzadas de pre-procesamiento y estrategias de ramificación y acotamiento para acelerar la búsqueda de la solución óptima.

Una vez que CPLEX encuentra la solución óptima, establece la asignación de activos que minimiza el riesgo y maximiza el retorno esperado del portafolio. Esta solución indica qué activos deben ser incluidos en el portafolio.

Es importante destacar que el modelo de optimización clásico basado en CPLEX es determinista, lo que significa que siempre encontrará la misma solución óptima para un problema dado [88]. Esto es una ventaja en términos de reproducibilidad y consistencia de los resultados.

Sin embargo, a medida que el número de activos y restricciones aumenta, el tiempo de cálculo requerido por CPLEX puede crecer exponencialmente. Esto se debe a la complejidad inherente de los problemas de optimización combinatoria. En casos de problemas muy complejos, puede ser necesario recurrir a técnicas de aproximación o heurísticas [89], para obtener soluciones subóptimas pero aceptables en un tiempo razonable.

5.4 *MODELO DE OPTIMIZACIÓN CUÁNTICO*

El modelo de optimización cuántico para la selección de portafolios se basa en el algoritmo VQE (descrito en el punto 4.5.3) y utiliza un ansatz de Real Amplitudes para encontrar la solución óptima. El proceso comienza con la representación del problema como un Hamiltoniano mediante la formulación QUBO descrita anteriormente. Esta formulación permite mapear la función objetivo y las restricciones del problema en un Hamiltoniano que puede ser optimizado utilizando un algoritmo cuántico.

En física cuántica, un Hamiltoniano es un operador que corresponde a la energía total del sistema [90]. Representa la suma de la energía cinética y potencial del sistema. En el contexto de la optimización cuántica, se usa para codificar el problema de optimización de manera que las soluciones óptimas del problema correspondan a los estados de menor energía del Hamiltoniano.

Matemáticamente, se puede expresar como una matriz o un operador que actúa sobre el espacio de estados cuánticos. Para nuestro planteamiento, se construye de manera que sus

estados de menor energía representan la combinación de activos que minimiza el riesgo y maximiza el retorno esperado [91].

Una vez que el problema de optimización está representado como un Hamiltoniano mediante la formulación QUBO, el siguiente paso es construir el circuito cuántico que se utilizará en el algoritmo VQE.

En este caso, se utiliza el ansatz de Real Amplitudes, que es una forma particular de construir el circuito cuántico. Un ansatz se puede entender como una función parametrizada que genera un estado cuántico a partir de un conjunto de parámetros [92]. Estos parámetros son variables que se ajustarán durante el proceso de optimización para encontrar el estado cuántico que minimiza la energía del Hamiltoniano.

El ansatz de Real Amplitudes se caracteriza por utilizar únicamente puertas cuánticas de rotación con ángulos reales [93]. Esto significa que las amplitudes de probabilidad asociadas a los estados base del sistema cuántico serán números reales en lugar de números complejos; simplificando la implementación del circuito cuántico y reduciendo la complejidad computacional, en comparación con otros ansatzs que utilizan puertas cuánticas más generales.

La elección del ansatz adecuado impacte en el rendimiento del algoritmo VQE y la calidad de las soluciones obtenidas. El ansatz de Real Amplitudes ha demostrado ser efectivo en una variedad de problemas de optimización, ya que permite representar una amplia gama de estados cuánticos con una estructura relativamente simple y eficiente en términos de recursos cuánticos.

Una de las ventajas del ansatz de Real Amplitudes es que reduce la cantidad de parámetros necesarios para describir el estado cuántico en comparación con ansatzes más generales. Esto se traduce en una mayor eficiencia computacional y una convergencia más rápida del algoritmo VQE. Además, la restricción a ángulos reales simplifica la optimización de los parámetros, ya que se evita la necesidad de trabajar con números complejos.

Sin embargo, es importante tener en cuenta que la elección del ansatz adecuado depende del problema específico y de las características del sistema cuántico utilizado. En algunos casos, puede ser necesario utilizar ansatzes más complejos o específicos del problema para obtener resultados óptimos. La investigación en el diseño de ansatzes eficientes y adaptados a problemas particulares es un área activa en el campo de la computación cuántica.

A continuación, las figuras Fig. 19 y Fig. 20 muestran visualmente los ansatzes construidos para 5 y 20 activos, respectivamente.

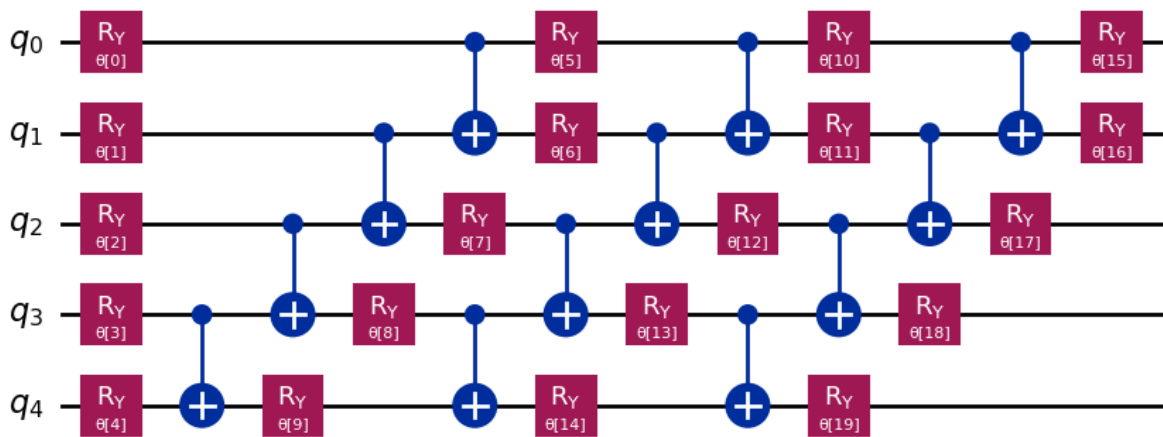


Fig. 19 Ansatz de 5 qubits.

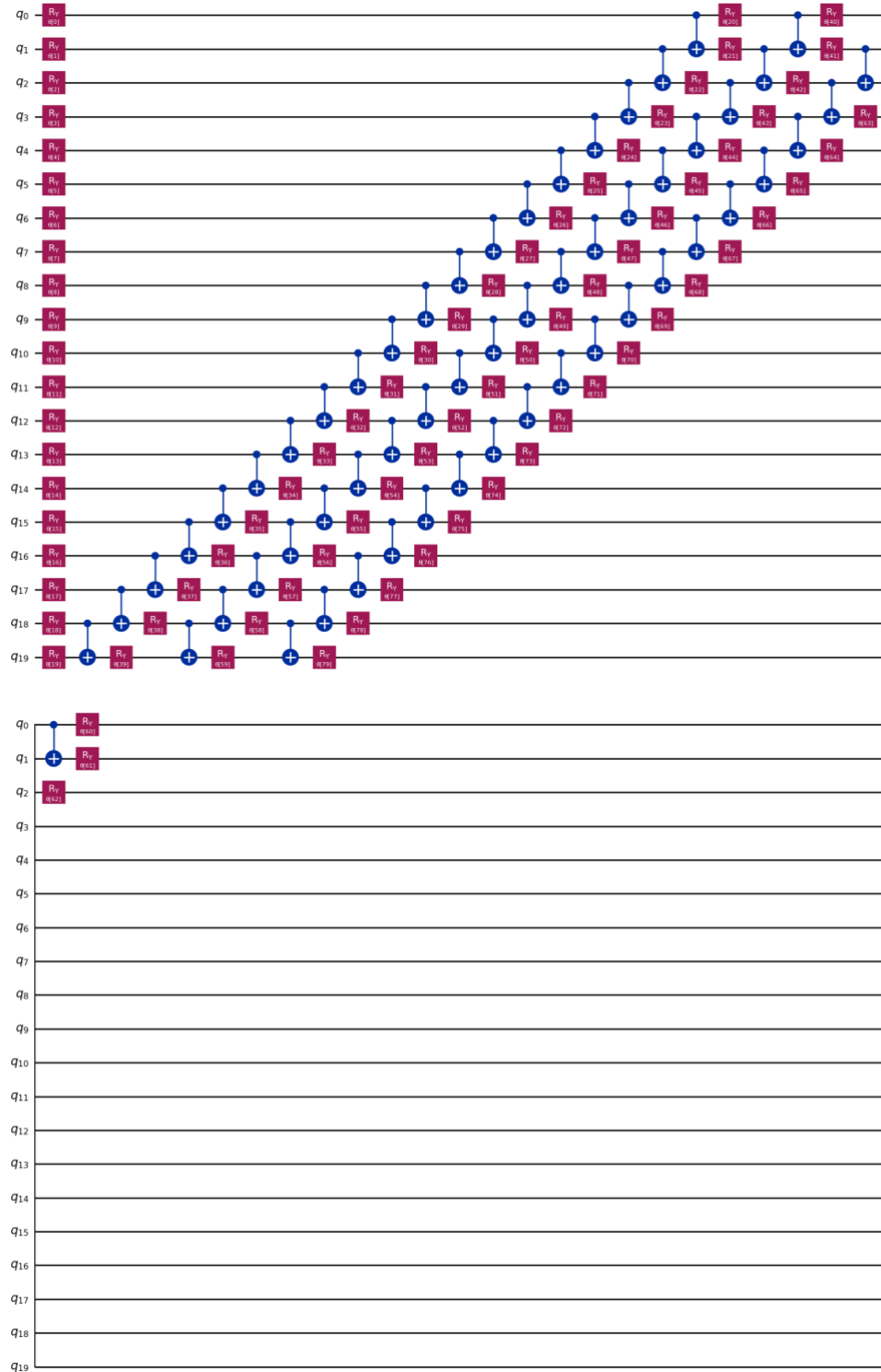


Fig. 20 Ansatz de 10 qubits.

Una vez que se ha construido el circuito cuántico, el siguiente paso es ejecutarlo para obtener los resultados de la optimización. Existen dos opciones principales para la ejecución del circuito cuántico: utilizando un ordenador cuántico real a través de Qiskit Runtime [14] o empleando un simulador cuántico, como el simulador Aer de Qiskit [9].

Este último simula el comportamiento de un sistema cuántico sin necesidad de acceso a hardware cuántico real. Esto es especialmente útil en la fase de desarrollo y prueba de algoritmos cuánticos, ya que permite evaluar su desempeño y corregir posibles errores antes de ejecutarlos en dispositivos cuánticos reales, que pueden ser más costosos y menos accesibles. Por esta razón, optaremos por esta segunda opción para ejecutar nuestro modelo de optimización.

Durante la ejecución del algoritmo VQE, se lleva a cabo una optimización híbrida que combina la ejecución del circuito cuántico con un optimizador clásico. En cada iteración, el circuito cuántico se ejecuta con diferentes valores de los parámetros del ansatz, y se mide la energía resultante del Hamiltoniano. Luego, el optimizador clásico, en este caso, el algoritmo SLSQP (Sequential Least Squares Programming) [94], [95], utiliza esta información para ajustar los parámetros del ansatz con el objetivo de minimizar la energía en la siguiente iteración.

Este proceso de optimización híbrida se repite iterativamente hasta que se alcanza un criterio de convergencia predefinido o se llega a un número máximo de iteraciones. El criterio de convergencia puede ser, por ejemplo, que la diferencia entre las energías obtenidas en iteraciones consecutivas sea menor que un umbral establecido, lo que indica que se ha alcanzado una solución estable. Alternativamente, se puede definir un número máximo de iteraciones para limitar el tiempo de ejecución del algoritmo. Optamos por esta última opción, ya que estos circuitos pueden requerir un tiempo considerable.

Finalmente, una vez que el algoritmo VQE ha convergido o alcanzado el número máximo de iteraciones, los parámetros óptimos del ansatz obtenidos representan la solución

aproximada del problema de optimización. Estos parámetros definen el estado cuántico final del sistema, que contiene información sobre la asignación óptima de activos en el portafolio.

Capítulo 6. ANÁLISIS DE RESULTADOS

En este capítulo se presentan los resultados obtenidos al aplicar los modelos de optimización clásico y cuántico para la selección de portafolios, utilizando los datos y metodologías descritos en los capítulos anteriores. Se realizará un análisis comparativo de la composición de los portafolios resultantes, los rendimientos obtenidos y los tiempos de ejecución de cada modelo. El objetivo es evaluar el desempeño y la eficiencia de ambos enfoques en la tarea de optimización de portafolios.

6.1 COMPARACIÓN DE LA COMPOSICIÓN DEL PORTAFOLIO

En esta sección se analizará y comparará la composición de los portafolios obtenidos mediante los modelos de optimización. Se examinarán las diferencias en la selección de activos, con el objetivo de comprender cómo cada solución aborda el problema de optimización y qué activos considera más relevantes para maximizar el rendimiento y minimizar el riesgo.

La comparación de la composición de los portafolios permitirá evaluar si los modelos clásico y cuántico convergen hacia soluciones similares o si presentan divergencias en la asignación de activos. Esto proporcionará información valiosa sobre la robustez y estabilidad de cada modelo, así como sobre su capacidad para adaptarse a diferentes condiciones de mercado y objetivos de inversión.

6.1.1 COMPOSICIÓN DEL PORTAFOLIO CON 5 ACTIVOS

La Fig. 21 muestra la composición del portafolio obtenido mediante los modelos de optimización clásico y cuántico para el caso de 5 activos conocidos como FAANG (Facebook, Amazon, Apple, Netflix y Google). Recordemos que nuestro presupuesto nos permitía seleccionar 3 acciones y que establecimos un nivel de riesgo del 10%.

En el modelo clásico, los activos seleccionados fueron Amazon (AMZN), Netflix (NFLX) y Google (GOOGL). Esta combinación sugiere que el modelo clásico priorizó empresas con un historial de crecimiento sólido y una fuerte posición en sus respectivos sectores. Amazon es líder en el comercio electrónico, mientras que Netflix ha revolucionado la industria del entretenimiento con su plataforma de streaming. Google, por su parte, domina el mercado de la publicidad en línea y ofrece una amplia gama de servicios tecnológicos.

Por otro lado, el modelo cuántico seleccionó Apple (AAPL), Netflix (NFLX) y Google (GOOGL). Indicándonos que el modelo cuántico identificó un equilibrio ligeramente diferente entre rentabilidad potencial y riesgo. Apple, siendo una de las empresas más valiosas del mundo, ha demostrado una capacidad constante para innovar y generar ganancias sólidas. Al igual que en el modelo clásico, Netflix y Google fueron seleccionados, destacando su atractivo como inversiones en el sector tecnológico.

Las diferencias en la selección de activos entre los modelos clásico y cuántico sugieren que ambos enfoques tienen perspectivas distintas sobre la optimización del portafolio. Mientras que el modelo clásico se ha centrado en empresas con un historial comprobado de crecimiento, el modelo cuántico parece considerar una combinación más diversa de factores.

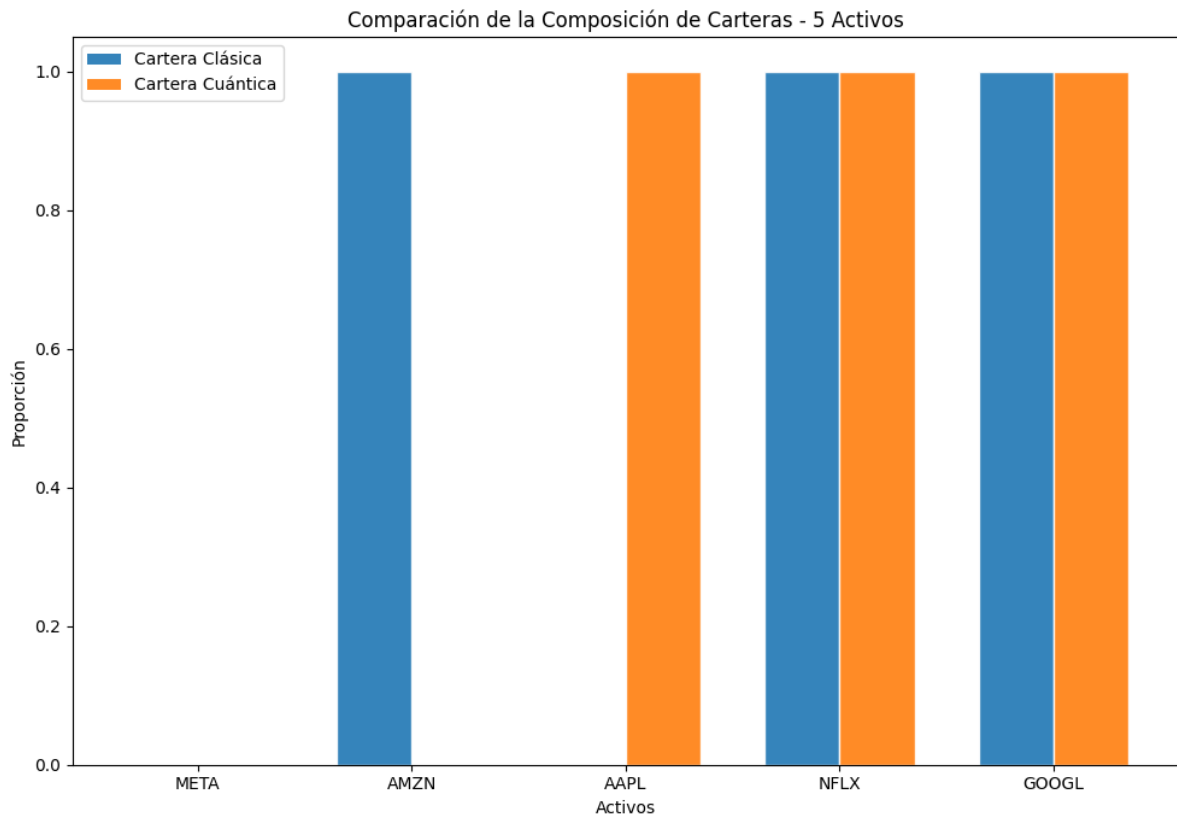


Fig. 21 Composición del Portafolio con 5 Activos.

6.1.2 COMPOSICIÓN DEL PORTAFOLIO CON 20 ACTIVOS

La Fig. 22 representa la composición del portafolio resultante de los modelos de optimización clásico y cuántico para el caso de 20 activos, que incluyen empresas de diversos sectores como tecnología, defensa, servicios financieros y energía. En este escenario, se observan diferencias más notables entre ambos enfoques. Cabe destacar que el nivel de riesgo se mantiene en un 10%, pero el presupuesto del número de acciones a seleccionar asciende a 7.

En el modelo clásico, los activos seleccionados son Apple (AAPL), Lockheed Martin (LMT), Berkshire Hathaway (BRK-B), ExxonMobil (XOM), JPMorgan Chase (JPM), Visa (V) y Mastercard (MA). Apple y Berkshire Hathaway son conocidas por su solidez financiera y su capacidad para generar ganancias consistentes. Lockheed Martin es un líder en la industria de defensa, mientras que ExxonMobil es una de las principales compañías

energéticas a nivel mundial. JPMorgan Chase, Visa y Mastercard son gigantes en el sector financiero, con una amplia presencia global y una gran base de clientes.

Por otro lado, el modelo cuántico ha seleccionado Facebook (META), Amazon (AMZN), Apple (AAPL), Berkshire Hathaway (BRK-B), ExxonMobil (XOM), Visa (V) y Mastercard (MA). Reflejando que el modelo cuántico ha considerado una combinación de empresas tecnológicas, financieras y energéticas. La inclusión de Facebook y Amazon sugiere que el modelo cuántico ha identificado un retorno mayor en estas. Al igual que en el modelo clásico, Apple, Berkshire Hathaway, ExxonMobil, Visa y Mastercard han sido seleccionadas, lo que destaca su atractivo como inversiones sólidas y estables.

Si bien ambos modelos han seleccionado algunas empresas en común, como Apple, Berkshire Hathaway, ExxonMobil, Visa y Mastercard, existen diferencias en la elección de otras compañías. El modelo clásico ha optado por incluir Lockheed Martin y JPMorgan Chase, mientras que el modelo cuántico ha preferido Facebook y Amazon. Estas diferencias pueden atribuirse a los distintos algoritmos utilizados por cada modelo para evaluar y optimizar el portafolio.

Es importante destacar que ambos modelos han buscado diversificar el portafolio con empresas de diferentes sectores, permitiendo mitigar el riesgo y aprovechar oportunidades en distintas áreas de la economía. La presencia de empresas tecnológicas, financieras y energéticas en ambos portafolios sugiere que estos sectores son considerados atractivos y resilientes por ambos modelos.

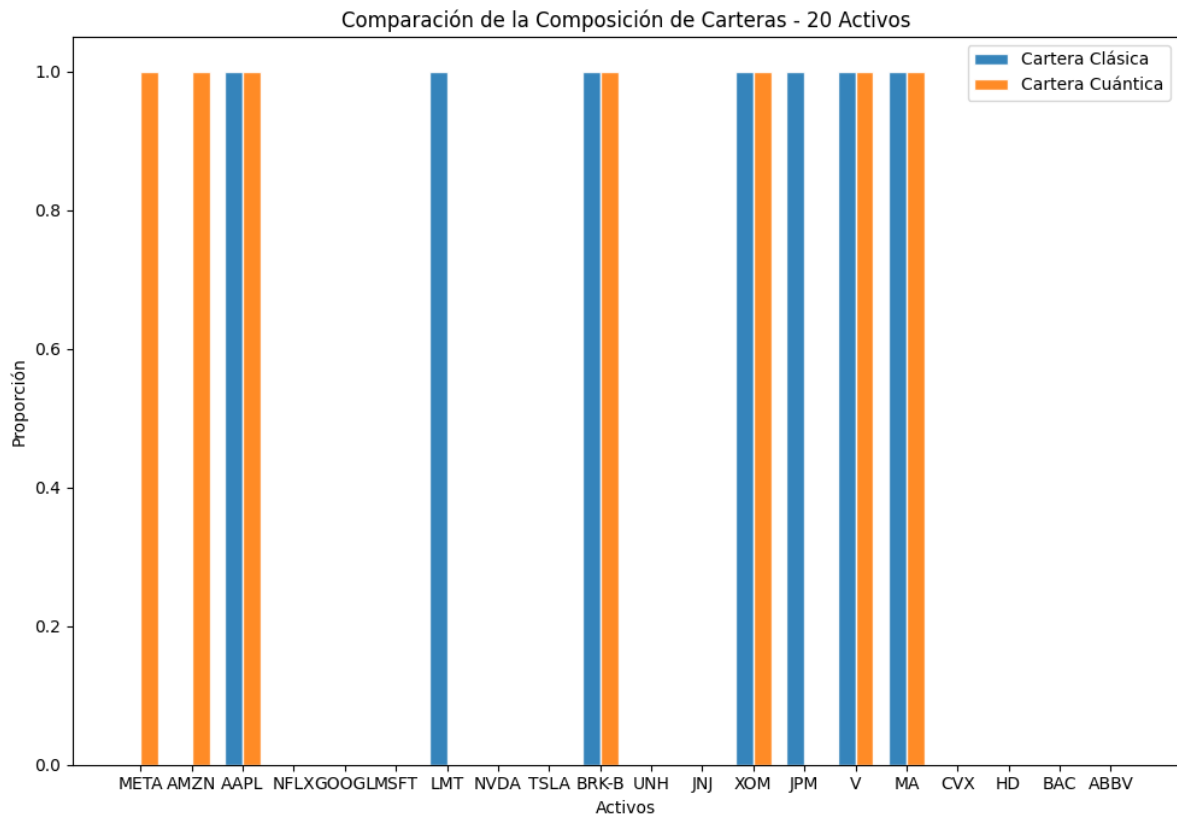


Fig. 22 Composición del Portafolio con 20 Activos.

6.1.3 DIFERENCIAS EN LA SELECCIÓN DE ACTIVOS

Al comparar la composición de los portafolios obtenidos mediante los dos modelos, tanto para el caso de 5 activos como de 20 activos, se pueden observar diferencias interesantes en la selección de activos.

En el portafolio de 5 activos, ambos modelos coincidieron en la selección de Netflix (NFLX) y Google (GOOGL), lo que denota que estas empresas presentan características atractivas desde ambas perspectivas. Sin embargo, el modelo clásico optó por incluir Amazon (AMZN), mientras que el modelo cuántico seleccionó Apple (AAPL). La discrepancia puede atribuirse a los distintos enfoques utilizados por cada modelo para evaluar la rentabilidad y el riesgo.

En el portafolio de 20 activos, las diferencias en la selección son más notables. Aunque ambos modelos coincidieron en la inclusión de varias empresas, como Apple (AAPL), Berkshire Hathaway (BRK-B), ExxonMobil (XOM), Visa (V) y Mastercard (MA).

Las diferencias en la selección de activos pueden atribuirse a varios factores. En primer lugar, los algoritmos y técnicas utilizados por cada modelo pueden tener diferentes enfoques para evaluar y optimizar el portafolio. El modelo clásico se basa en técnicas tradicionales de programación matemática, en concreto utiliza el algoritmo de optimización CPLEX como vimos en el Capítulo 5. ; mientras que el modelo cuántico utiliza el algoritmo VQE, que pueden explorar el espacio de soluciones de manera diferente y considerar otros factores.

Además, las diferencias en la selección de activos pueden reflejar las distintas formas en que cada modelo pondera los criterios de rentabilidad, riesgo y diversificación. El modelo clásico puede dar mayor importancia a la minimización del riesgo y la selección de empresas con un historial sólido, mientras que el modelo cuántico puede estar más orientado a maximizar el rendimiento potencial y considerar empresas con un mayor potencial de crecimiento.

Es importante destacar que, a pesar de las diferencias en la selección de activos, ambos modelos buscan construir portafolios diversificados que maximicen el rendimiento y minimicen el riesgo. La inclusión de empresas de diferentes sectores y con perfiles de riesgo variados es una estrategia común para mitigar el riesgo y aprovechar oportunidades en distintas áreas de la economía.

6.2 COMPARACIÓN DE LOS RENDIMIENTOS DEL PORTAFOLIO

En esta sección se compararán los rendimientos obtenidos por los portafolios. El análisis comparativo de los rendimientos permitirá evaluar cuál de las dos soluciones logra un mejor desempeño en términos de generación de retornos y gestión del riesgo.

6.2.1 RENDIMIENTO DEL PORTAFOLIO CON 5 ACTIVOS

La Fig. 23 muestra cómo cambiaron los rendimientos del portfolio de cinco activos utilizando ambos modelos.

El portafolio clásico muestra un rendimiento ligeramente superior al portafolio cuántico durante la mayor parte del período analizado. Sin embargo, es importante destacar que la diferencia entre ambos se acentúa en los últimos meses, lo que sugiere que el modelo clásico ha sido capaz de adaptarse mejor a las condiciones cambiantes del mercado en este tramo final.

Ambos portafolios exhiben una tendencia de crecimiento similar, con algunos períodos de volatilidad y correcciones. No obstante, en general, logran mantener una trayectoria ascendente y generar rendimientos positivos a lo largo del tiempo.

A pesar de que el portafolio clásico presenta un rendimiento levemente superior en este caso particular, es fundamental destacar que ambos enfoques demuestran ser efectivos en la selección de activos y la optimización del portafolio. Sin embargo, la diferencia observada no es suficiente como para descartar la validez del modelo cuántico.

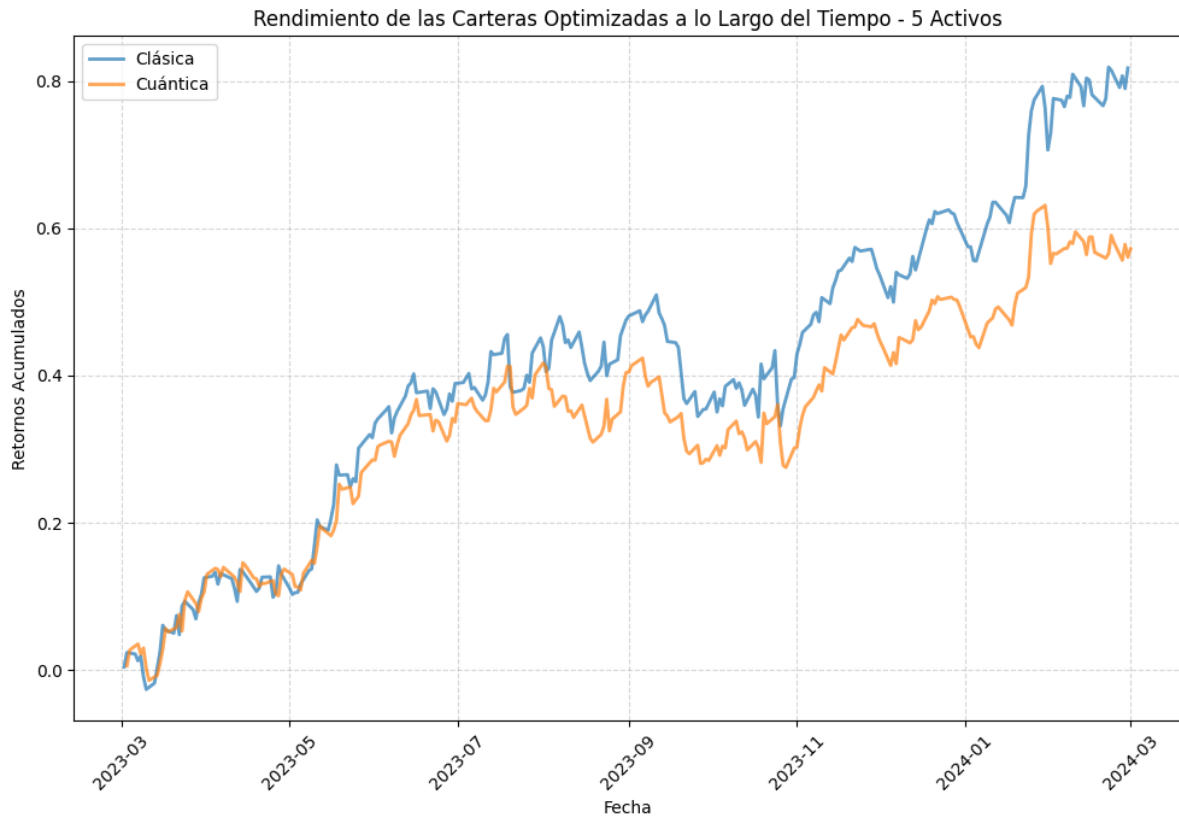


Fig. 23 Rendimiento del Portafolio con 5 Activos.

6.2.2 RENDIMIENTO DEL PORTAFOLIO CON 20 ACTIVOS

La Fig. 24 presenta la evolución de los rendimientos de los portafolios optimizados mediante los modelos clásico y cuántico para el caso de 20 activos.

En este escenario, se observa una dinámica diferente en comparación con el caso de 5 activos. El portafolio cuántico muestra un rendimiento superior al portafolio clásico de manera consistente a lo largo del tiempo. Exhibiendo una tendencia de crecimiento más pronunciada, con menos períodos de volatilidad y correcciones en comparación con el portafolio clásico. Sugiriendo que el modelo cuántico ha sido capaz de identificar y aprovechar de manera más efectiva las oportunidades de inversión en un universo más amplio y diversificado de activos.

Como consecuencia, en el caso de un universo de inversión más grande y complejo, el modelo cuántico podría tener una ventaja aparente en la selección de activos y la optimización del portafolio, logrando un mejor desempeño en términos de rendimientos y gestión del riesgo.

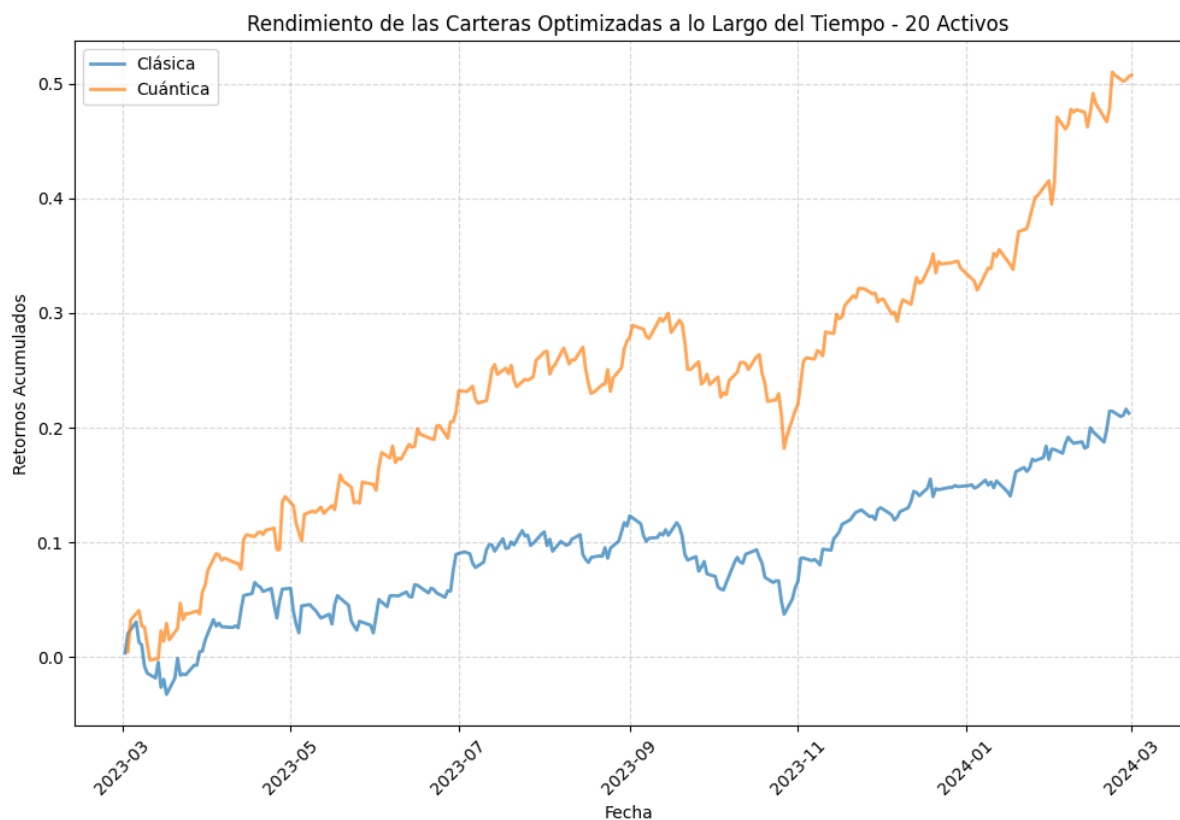


Fig. 24 Rendimiento del Portafolio con 20 Activos.

6.2.3 ANÁLISIS COMPARATIVO DE RENDIMIENTOS

De manera *tentativa*, parece que con menos activos el modelo clásico obtiene un mejor rendimiento, pero con más activos el modelo cuántico indica ser superior. Sin embargo, para poder afirmarlo rotundamente haría falta hacer pruebas con diferentes algoritmos de optimización tanto clásicos como cuánticos y probar con un rango mayor de acciones.

Cabe resaltar que estos resultados se basan en un conjunto limitado de datos y en la comparación de dos modelos específicos. Para poder llegar a conclusiones más sólidas y

generalizables, sería necesario realizar pruebas adicionales con diferentes algoritmos de optimización, tanto clásicos como cuánticos, y considerar un rango más amplio de acciones y escenarios de mercado.

6.3 COMPARACIÓN DEL TIEMPO DE EJECUCIÓN DEL MODELO

En esta sección se analizarán y compararán los tiempos de ejecución de los modelos, considerando tanto la fase de construcción del modelo como el proceso de optimización en sí. Se evaluará la eficiencia computacional de cada enfoque y se discutirán las implicaciones en términos de escalabilidad y función en situaciones reales.

Se presentarán gráficos que muestren los tiempos de ejecución para diferentes tamaños de portafolio y niveles de complejidad, comparando el rendimiento de los modelos clásico y cuántico en cada caso.

6.3.1 TIEMPO DE EJECUCIÓN DEL MODELO CON 5 ACTIVOS

La Fig. 25 ilustra los tiempos de ejecución para el caso de 5 activos, considerando tanto la fase de construcción del modelo como el proceso de optimización.

Se puede observar que el modelo clásico tiene un tiempo de ejecución notoriamente menor en comparación con el modelo cuántico (50 milisegundos vs 1.59 segundos). Esto se debe a que los algoritmos clásicos, son computacionalmente eficientes y pueden resolver problemas de optimización de portafolios de tamaño moderado en un tiempo relativamente corto.

Por otro lado, el modelo cuántico ha requerido más tiempo de ejecución debido a la complejidad adicional introducida por los algoritmos cuánticos, como el VQE, y la necesidad de realizar múltiples iteraciones para encontrar la solución óptima.

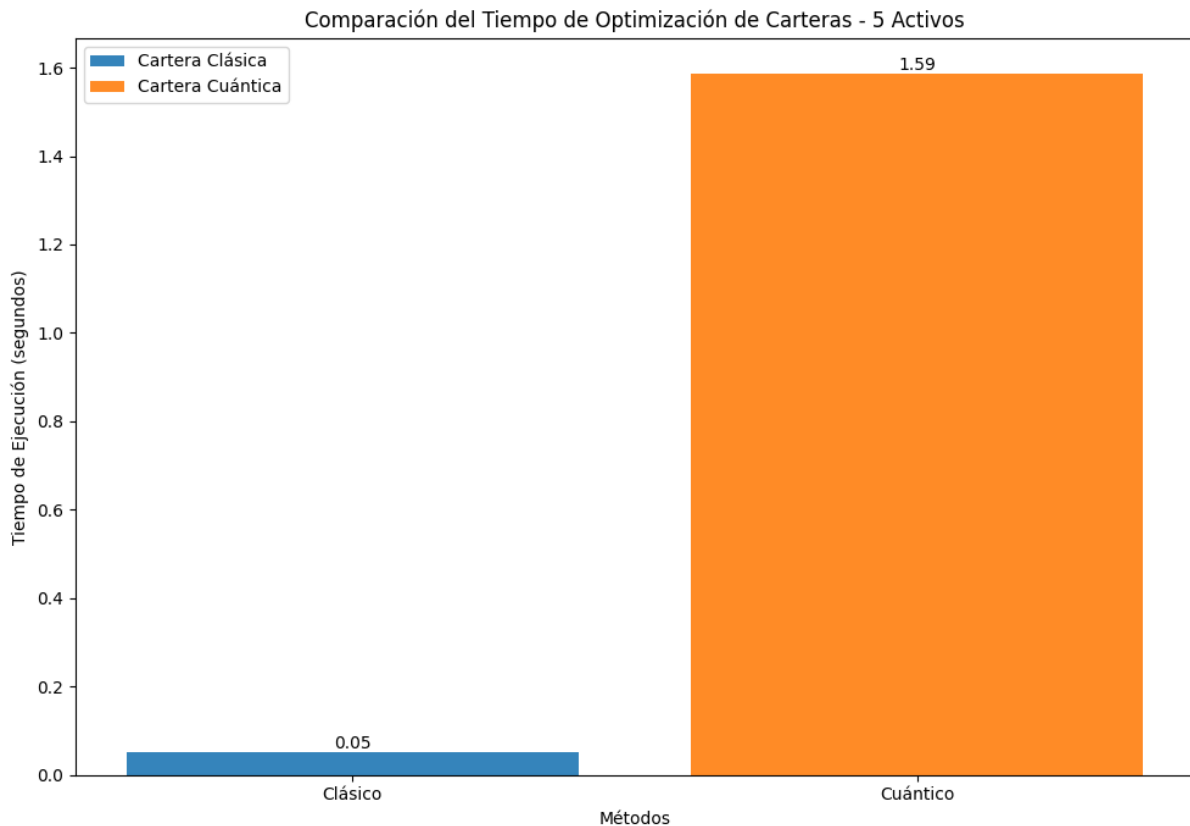


Fig. 25 Tiempo de Ejecución del Portafolio con 5 Activos.

6.3.2 TIEMPO DE EJECUCIÓN DEL MODELO CON 20 ACTIVOS

Para el caso del portafolio de 20 activos, la Fig. 26 presenta los tiempos de ejecución de los modelos.

En este escenario, se observa una diferencia significativamente más notable entre los tiempos de ejecución de ambos modelos. El modelo clásico muestra un aumento casi insignificante en el tiempo de ejecución en comparación con el caso de 5 activos (50 milisegundos vs 70 milisegundos), señalando que puede manejar problemas de optimización de portafolios de mayor tamaño de manera eficiente.

No obstante, el modelo cuántico experimenta un incremento elevado en el tiempo de ejecución al aumentar el número de activos (25.84 segundos). Es por ello que la implementación de algoritmos cuánticos todavía se encuentra en una etapa temprana de

desarrollo, y la calidad y escala de los dispositivos cuánticos disponibles pueden limitar su capacidad para resolver problemas de gran tamaño de manera eficiente.

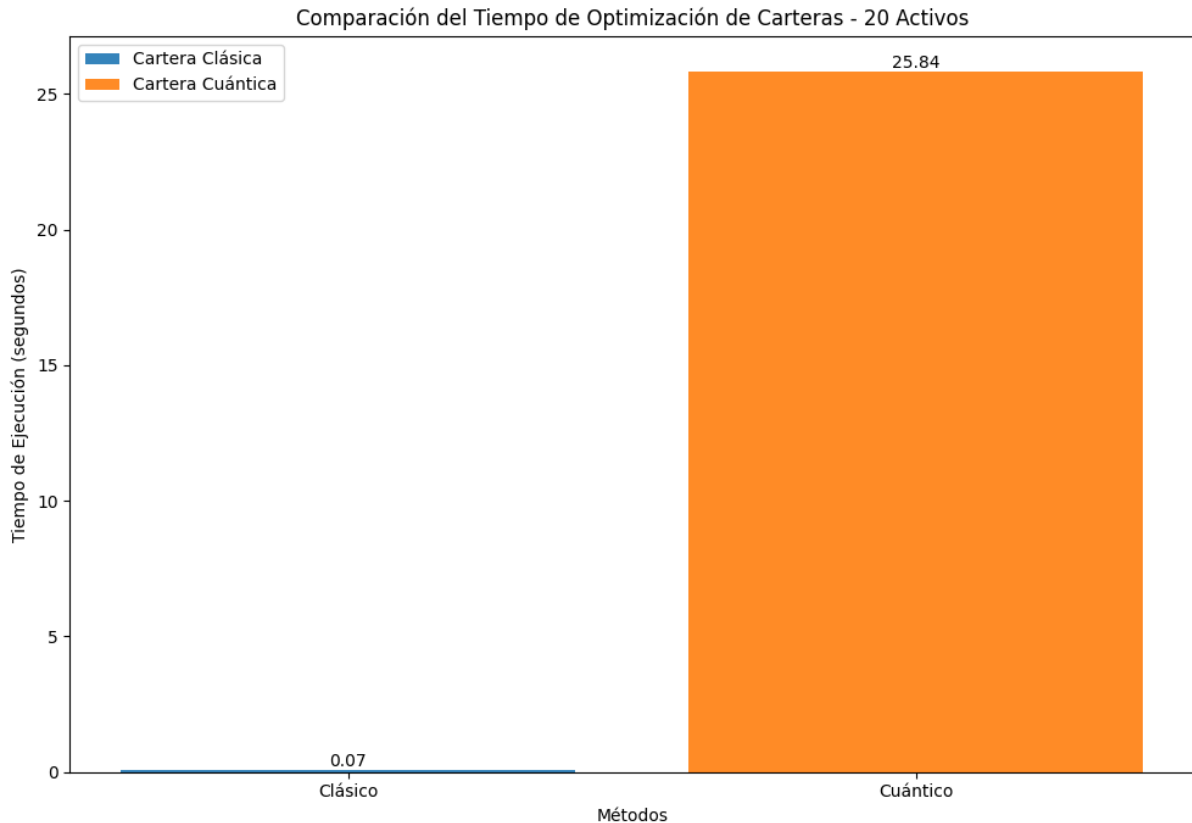


Fig. 26 Tiempo de Ejecución del Portafolio con 20 Activos.

6.3.3 ANÁLISIS COMPARATIVO DE TIEMPOS

Los resultados correspondientes a los tiempos de ejecución de los modelos, presentan algunas consideraciones que merecen ser mencionadas.

Es evidente que el modelo clásico tiene una ventaja significativa en términos de eficiencia computacional cuando se trata de problemas de optimización de portafolios de tamaño pequeño y moderado. Los algoritmos clásicos han sido objeto de extensas investigaciones y mejoras a lo largo de décadas, lo que les ha permitido alcanzar un alto nivel de optimización

y eficiencia. Estos algoritmos son capaces de abordar problemas de este tamaño de manera rápida y efectiva, aprovechando al máximo los recursos computacionales disponibles.

En contraste, el modelo cuántico muestra tiempos de ejecución más prolongados en comparación con el modelo clásico, y esta diferencia se vuelve más notable a medida que aumenta el número de activos incluidos en el portafolio. Este comportamiento se puede atribuir a varios factores. Los algoritmos cuánticos son inherentemente más complejos que sus contrapartes clásicas, ya que operan en un espacio de estados mucho más grande y aprovechan principios cuánticos como la superposición y el entrelazamiento. Además, el software y hardware cuántico actuales aún se encuentran en una etapa temprana de desarrollo, lo que limita su capacidad para procesar problemas de gran escala de manera eficiente.

Es importante destacar que en este experimento se utilizó un simulador cuántico en lugar de un ordenador cuántico real. Los simuladores cuánticos son programas que emulan el comportamiento de un sistema cuántico en un ordenador clásico. Aunque son herramientas valiosas para el desarrollo y prueba de algoritmos cuánticos, tienen limitaciones en términos de escalabilidad y rendimiento en comparación con un ordenador cuántico real. Por lo tanto, es probable que los tiempos de ejecución observados en este estudio sean mayores que los que se obtendrían en un hardware cuántico dedicado.

A pesar de las diferencias en los tiempos de ejecución, es fundamental evaluar el equilibrio entre la eficiencia computacional y la calidad de las soluciones obtenidas al comparar los modelos clásico y cuántico. En algunas situaciones, puede ser aceptable tolerar tiempos de ejecución más prolongados si a cambio se obtienen resultados superiores en términos de rendimiento y gestión del riesgo del portafolio. La elección entre velocidad y calidad dependerá de las necesidades y prioridades específicas de cada caso de uso.

Mirando hacia el futuro, se espera que los avances en la computación cuántica conduzcan a mejoras significativas en los tiempos de ejecución del modelo cuántico. A medida que se desarrollen ordenadores cuánticos más potentes y se optimicen los algoritmos cuánticos, es probable que la brecha de rendimiento entre los modelos clásico y cuántico se reduzca e

incluso que el modelo cuántico supere al clásico en problemas de mayor escala y complejidad.

Capítulo 7. CONCLUSIONES Y TRABAJOS FUTUROS

7.1 CONCLUSIONES

A lo largo de este trabajo de investigación, se ha logrado cumplir con los objetivos planteados en el Capítulo 3. , tanto el objetivo general como los objetivos específicos. Se ha explorado en profundidad la aplicación del entrelazamiento cuántico y la computación cuántica en el campo de la ingeniería de telecomunicaciones, con un enfoque particular en la optimización de portafolios financieros.

En relación con el primer objetivo (explorar protocolos QKD), se ha llevado a cabo una revisión de los protocolos de comunicación basados en la Distribución Cuántica de Claves (QKD), como el BB84 y el BBM92. Se han analizado los principios fundamentales de QKD y se ha evaluado su uso en sistemas de telecomunicación modernos. Este estudio ha permitido comprender las ventajas y desafíos de utilizar la física cuántica para garantizar la seguridad en las comunicaciones.

Respecto al segundo objetivo (desarrollar un modelo cuántico), se ha desarrollado con éxito un modelo cuántico para la optimización de recursos, específicamente en el contexto de la optimización de portafolios financieros. Utilizando la plataforma Qiskit de IBM y el lenguaje de programación Python, se ha diseñado y analizado un modelo matemático basado en la teoría cuántica que ha demostrado su capacidad para mejorar la gestión de recursos y la asignación de activos. Los resultados obtenidos sugieren que el modelo cuántico puede ofrecer ventajas en comparación con los enfoques clásicos. Sin embargo, a medida que el número de activos aumenta, los tiempos de ejecución del modelo cuántico son más prolongados debido a la complejidad inherente de los algoritmos cuánticos y las limitaciones actuales del software y hardware cuántico.

En cuanto al tercer objetivo, este trabajo ha sentado una base sólida para futuras investigaciones en el campo de la Ingeniería de Telecomunicación. Los hallazgos y

Conclusiones presentadas no solo generan conocimiento en el ámbito de las comunicaciones cuánticas, sino que también establecen un punto de partida y referencia para proyectos de investigación posteriores. Se espera que este estudio estimule el avance en este campo en constante evolución, abriendo nuevas oportunidades para la aplicación de tecnologías cuánticas en la industria de las telecomunicaciones.

Este trabajo de investigación ha contribuido a la comprensión y aplicación del fenómeno de *Quantenverschränkungen* en el campo de la Ingeniería de Telecomunicación. Se han explorado protocolos cuánticos de comunicación seguros, se ha desarrollado un modelo cuántico para la optimización de recursos y se ha establecido una base sólida para futuras investigaciones. Los resultados obtenidos destacan el potencial transformador de las tecnologías cuánticas en la industria de las telecomunicaciones y abren nuevas perspectivas para la innovación y el desarrollo.

7.2 TRABAJOS FUTUROS

A partir de los resultados y conclusiones de este trabajo de investigación, se abren diversas oportunidades para trabajos futuros que pueden profundizar y ampliar el alcance de la aplicación del entrelazamiento cuántico y la computación cuántica en la Ingeniería de Telecomunicación.

En primer lugar, se podría explorar la implementación de los protocolos de comunicación basados en QKD en sistemas de telecomunicación reales. Si bien este trabajo ha evaluado la aplicación teórica de estos protocolos, sería interesante llevar a cabo pruebas experimentales y estudios de caso para analizar su desempeño en entornos prácticos. Esto permitiría identificar desafíos técnicos y operativos, así como desarrollar estrategias para su implementación efectiva.

Otro aspecto importante que considerar en trabajos futuros es la optimización y escalabilidad del modelo cuántico desarrollado para la optimización de portafolios. Si bien los resultados obtenidos son prometedores, sería beneficioso investigar técnicas y estrategias para mejorar

aún más el rendimiento y la capacidad del modelo para manejar problemas de mayor tamaño y complejidad. Esto podría incluir la exploración de nuevos algoritmos cuánticos, la optimización de los circuitos cuánticos y la integración con técnicas clásicas de optimización.

Asimismo, sería de interés extender la aplicación del modelo cuántico a otros problemas de optimización en el ámbito de las telecomunicaciones. Por ejemplo, se podrían abordar desafíos como la asignación óptima de recursos en redes, la planificación eficiente de rutas en sistemas de comunicación o la optimización de la calidad de servicio en redes inalámbricas. La adaptación del modelo cuántico a estos escenarios permitiría evaluar su versatilidad y potencial para resolver una variedad de problemas en la industria.

En conclusión, los trabajos futuros presentan un amplio abanico de oportunidades y desafíos. Desde la implementación práctica de protocolos de comunicación seguros hasta la optimización y escalabilidad de modelos cuánticos, pasando por la integración con la infraestructura existente y la ampliación de las aplicaciones. La investigación en esta área tiene el potencial de transformar la industria de las telecomunicaciones y abrir nuevas fronteras en la transmisión y procesamiento de información. La colaboración interdisciplinaria y el compromiso continuo con la innovación serán fundamentales para aprovechar al máximo el potencial de las tecnologías cuánticas.

Capítulo 8. BIBLIOGRAFÍA

- [1] A. Einstein, B. Podolsky, and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?,” *Physical review*, vol. 47, no. 10, p. 777, 1935.
- [2] E. Schrödinger, “Discussion of probability relations between separated systems,” in *Mathematical Proceedings of the Cambridge Philosophical Society*, Cambridge University Press, 1935, pp. 555–563.
- [3] E. Schrödinger, “Probability relations between separated systems,” *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 32, no. 3, pp. 446–452, 1936, doi: DOI: 10.1017/S0305004100019137.
- [4] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, “Quantum entanglement,” *Rev Mod Phys*, vol. 81, no. 2, p. 865, 2009.
- [5] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, “Experimental quantum teleportation,” *Nature*, vol. 390, no. 6660, pp. 575–579, 1997.
- [6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev Mod Phys*, vol. 74, no. 1, p. 145, 2002.
- [7] “Qiskit - An Open-source Framework for Quantum Computing.” Accessed: Jun. 01, 2024. [Online]. Available: <https://www.ibm.com/quantum/qiskit>
- [8] “Qiskit Terra Documentation.” Accessed: Jun. 01, 2024. [Online]. Available: <https://docs.quantum.ibm.com/api/qiskit/0.26>

- [9] “Qiskit Aer Documentation. .” Accessed: Jun. 01, 2024. [Online]. Available: <https://qiskit.github.io/qiskit-aer/apidocs/aer.html>
- [10] “Qiskit Finance Documentation.” Accessed: Jun. 01, 2024. [Online]. Available: <https://qiskit-community.github.io/qiskit-finance/>
- [11] “Qiskit Optimization Documentation.” Accessed: Jun. 01, 2024. [Online]. Available: <https://qiskit-community.github.io/qiskit-optimization/>
- [12] “Qiskit Machine Learning Documentation.” Accessed: Jun. 01, 2024. [Online]. Available: <https://qiskit-community.github.io/qiskit-machine-learning/>
- [13] “Qiskit Experiments Documentation.” Accessed: Jun. 01, 2024. [Online]. Available: <https://qiskit-extensions.github.io/qiskit-experiments/>
- [14] “Qiskit IBM Runtime Documentation.” Accessed: Jun. 01, 2024. [Online]. Available: <https://docs.quantum.ibm.com/api/qiskit-ibm-runtime>
- [15] “IBM Quantum Platform. URL.” Accessed: Jun. 01, 2024. [Online]. Available: <https://quantum.ibm.com>
- [16] “IBM Quantum-as-a-Service.” Accessed: Jun. 01, 2024. [Online]. Available: <https://www.ibm.com/quantum/pricing>
- [17] “NumPy: The Fundamental Package for Scientific Computing with Python.” Accessed: Jun. 01, 2024. [Online]. Available: <https://numpy.org>
- [18] “SciPy: Scientific Computing Tools for Python.” Accessed: Jun. 01, 2024. [Online]. Available: <https://scipy.org>
- [19] “Pandas: Python Data Analysis Library.” Accessed: Jun. 01, 2024. [Online]. Available: <https://pandas.pydata.org>
- [20] “Yahoo Finance Library.” Accessed: Jun. 01, 2024. [Online]. Available: <https://pypi.org/project/yfinance/>

- [21] “Anaconda: The World’s Most Popular Data Science Platform.” Accessed: Jun. 01, 2024. [Online]. Available: <https://www.anaconda.com>
- [22] “Git: Distributed Version Control System.” Accessed: Jun. 01, 2024. [Online]. Available: <https://git-scm.com>
- [23] “GitHub: Where the World Builds Software.” Accessed: Jun. 01, 2024. [Online]. Available: <https://github.com>
- [24] “Visual Studio Code.” Accessed: Jun. 01, 2024. [Online]. Available: <https://code.visualstudio.com>
- [25] “Matplotlib: Python Plotting Library.” Accessed: Jun. 01, 2024. [Online]. Available: <https://matplotlib.org>
- [26] “Seaborn: Statistical Data Visualization.” Accessed: Jun. 01, 2024. [Online]. Available: <https://seaborn.pydata.org>
- [27] Karel Dumon, “The computational power of Quantum Computers: an intuitive guide.” Accessed: Jun. 01, 2024. [Online]. Available: <https://medium.com/@kareldumon/the-computational-power-of-quantum-computers-an-intuitive-guide-9f788d1492b6>
- [28] “Trello - Herramienta para la gestión de tareas.” Accessed: Jun. 02, 2024. [Online]. Available: <https://trello.com/>
- [29] J. S. Bell, “On the einstein podolsky rosen paradox,” *Physics Physique Fizika*, vol. 1, no. 3, p. 195, 1964.
- [30] A. Aspect, P. Grangier, and G. Roger, “Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A new violation of Bell’s inequalities,” *Phys Rev Lett*, vol. 49, no. 2, p. 91, 1982.

- [31] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V Sergienko, and Y. Shih, “New high-intensity source of polarization-entangled photon pairs,” *Phys Rev Lett*, vol. 75, no. 24, p. 4337, 1995.
- [32] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Theor Comput Sci*, vol. 560, pp. 7–11, 2014.
- [33] P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in *Proceedings 35th annual symposium on foundations of computer science*, Ieee, 1994, pp. 124–134.
- [34] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 212–219.
- [35] I. L. Chuang, L. M. K. Vandersypen, X. Zhou, D. W. Leung, and S. Lloyd, “Experimental realization of a quantum algorithm,” *Nature*, vol. 393, no. 6681, pp. 143–146, 1998.
- [36] C. Wang and A. Rahman, “Quantum-enabled 6G wireless networks: Opportunities and challenges,” *IEEE Wirel Commun*, vol. 29, no. 1, pp. 58–69, 2022.
- [37] J. Yin *et al.*, “Entanglement-based secure quantum cryptography over 1,120 kilometres,” *Nature*, vol. 582, no. 7813, pp. 501–505, 2020.
- [38] Z. C. Seskir, R. Korkmaz, and A. U. Aydinoglu, “The landscape of the quantum start-up ecosystem,” *EPJ Quantum Technol*, vol. 9, no. 1, p. 27, 2022.
- [39] “Quantum Technology Market Report sees Developments in the areas of Hybrid Quantum Applications, Quantum Machine Learning, and more.” Accessed: Jun. 01, 2024. [Online]. Available: <https://www.researchandmarkets.com/reports/5317365/quantum-technology-market-by-computing>

- [40] V. O. Tolcheev, “Scientometric analysis of the current state and prospects of the development of quantum technologies,” *Automatic Documentation and Mathematical Linguistics*, vol. 52, pp. 121–133, 2018.
- [41] M. Riedel, M. Kovacs, P. Zoller, J. Mlynek, and T. Calarco, “Europe’s quantum flagship initiative,” *Quantum Sci Technol*, vol. 4, no. 2, p. 020501, 2019.
- [42] M. A. Rossi, “EU technology-specific industrial policy. The case of 5G and 6G.,” *Telecomm Policy*, vol. 48, no. 2, p. 102639, 2024.
- [43] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” *Rev Mod Phys*, vol. 81, no. 3, p. 1301, 2009.
- [44] M. Sasaki, “Quantum key distribution and its applications,” *IEEE Secur Priv*, vol. 16, no. 5, pp. 42–48, 2018.
- [45] S. Wehner, D. Elkouss, and R. Hanson, “Quantum internet: A vision for the road ahead,” *Science (1979)*, vol. 362, no. 6412, p. eaam9288, 2018.
- [46] S. Pirandola *et al.*, “Advances in quantum cryptography,” *Adv Opt Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.
- [47] W. H. Zurek, “Decoherence, einselection, and the quantum origins of the classical,” *Rev Mod Phys*, vol. 75, no. 3, p. 715, 2003.
- [48] L. Huynh, J. Hong, A. Mian, H. Suzuki, Y. Wu, and S. Camtepe, “Quantum-Inspired Machine Learning: a Survey,” *arXiv preprint arXiv:2308.11269*, 2023.
- [49] A. Carrasco-Casado, V. Fernández, and N. Denisenko, “Free-space quantum key distribution,” *Optical Wireless Communications: An Emerging Technology*, pp. 589–607, 2016.

- [50] C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without Bell’s theorem,” *Phys Rev Lett*, vol. 68, no. 5, p. 557, 1992.
- [51] C. Erven, “On Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source,” 2007. [Online]. Available: <https://api.semanticscholar.org/CorpusID:7953345>
- [52] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Phys Rev Lett*, vol. 67, no. 6, p. 661, 1991.
- [53] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations,” *arXiv preprint quant-ph/0211131*, 2002.
- [54] K. Inoue, E. Waks, and Y. Yamamoto, “Differential phase shift quantum key distribution,” *Phys Rev Lett*, vol. 89, no. 3, p. 037902, 2002.
- [55] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, “Fast and simple one-way quantum key distribution,” *Appl Phys Lett*, vol. 87, no. 19, 2005.
- [56] M. Stanley, Y. Gui, D. Unnikrishnan, S. R. G. Hall, and I. Fatadin, “Recent progress in quantum key distribution network deployments and standards,” in *Journal of Physics: Conference Series*, IOP Publishing, 2022, p. 012001.
- [57] C. E. Shannon, “A mathematical theory of communication,” *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.
- [58] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun ACM*, vol. 21, no. 2, pp. 120–126, 1978.
- [59] J. Daemen and V. Rijmen, *The design of Rijndael*, vol. 2. Springer, 2002.
- [60] C. E. Shannon, “Communication in the presence of noise,” *Proceedings of the IRE*, vol. 37, no. 1, pp. 10–21, 1949.

- [61] T. Pratt and J. E. Allnutt, *Satellite communications*. John Wiley & Sons, 2019.
- [62] E. Merzbacher, *Quantum mechanics*. John Wiley & Sons, 1998.
- [63] H. J. Kimble, “The quantum internet,” *Nature*, vol. 453, no. 7198, pp. 1023–1030, 2008.
- [64] P. W. Shor, “Scheme for reducing decoherence in quantum computer memory,” *Phys Rev A (Coll Park)*, vol. 52, no. 4, p. R2493, 1995.
- [65] R. H. Hadfield, “Single-photon detectors for optical quantum information applications,” *Nat Photonics*, vol. 3, no. 12, pp. 696–705, 2009.
- [66] C. Harney, A. I. Fletcher, and S. Pirandola, “End-to-end capacities of hybrid quantum networks,” *Phys Rev Appl*, vol. 18, no. 1, p. 014012, 2022.
- [67] H. Markowitz, “Portfolio Selection,” *J Finance*, vol. 7, no. 1, pp. 77–91, 1952, doi: 10.2307/2975974.
- [68] M. Frank and P. Wolfe, “An algorithm for quadratic programming,” *Naval research logistics quarterly*, vol. 3, no. 1–2, pp. 95–110, 1956.
- [69] D. P. Bertsekas, *Constrained optimization and Lagrange multiplier methods*. Academic press, 2014.
- [70] R. Roll, “A mean/variance analysis of tracking error,” *Journal of portfolio management*, vol. 18, no. 4, p. 13, 1992.
- [71] R. L. Rardin and R. Uzsoy, “Experimental evaluation of heuristic optimization algorithms: A tutorial,” *Journal of Heuristics*, vol. 7, pp. 261–304, 2001.
- [72] G. J. Alexander and A. M. Baptista, “A comparison of VaR and CVaR constraints on portfolio selection with the mean-variance model,” *Manage Sci*, vol. 50, no. 9, pp. 1261–1273, 2004.

- [73] H. L. Tang *et al.*, “qubit-adapt-vqe: An adaptive algorithm for constructing hardware-efficient ansätze on a quantum processor,” *PRX Quantum*, vol. 2, no. 2, p. 020310, 2021.
- [74] J. Choi and J. Kim, “A tutorial on quantum approximate optimization algorithm (QAOA): Fundamentals and applications,” in *2019 international conference on information and communication technology convergence (ICTC)*, IEEE, 2019, pp. 138–142.
- [75] S. Morita and H. Nishimori, “Mathematical foundation of quantum annealing,” *J Math Phys*, vol. 49, no. 12, 2008.
- [76] F. Phillipson and H. S. Bhatia, “Portfolio optimisation using the d-wave quantum annealer,” in *International Conference on Computational Science*, Springer, 2021, pp. 45–59.
- [77] A. Bouland, W. van Dam, H. Joorati, I. Kerenidis, and A. Prakash, “Prospects and challenges of quantum finance,” *arXiv preprint arXiv:2011.06492*, 2020.
- [78] R. Orús, S. Mugel, and E. Lizaso, “Quantum computing for finance: Overview and prospects,” *Reviews in Physics*, vol. 4, p. 100028, 2019.
- [79] D. J. Egger *et al.*, “Quantum computing for finance: State-of-the-art and future prospects,” *IEEE Transactions on Quantum Engineering*, vol. 1, pp. 1–24, 2020.
- [80] J. Preskill, “Quantum computing in the NISQ era and beyond,” *Quantum*, vol. 2, p. 79, 2018.
- [81] Z. Cai *et al.*, “Quantum error mitigation,” *Rev Mod Phys*, vol. 95, no. 4, p. 045005, 2023.
- [82] M. R. Pulicharla, “Hybrid Quantum-Classical Machine Learning Models: Powering the Future of AI,” *Journal of Science & Technology*, vol. 4, no. 1, pp. 40–65, 2023.

- [83] G. Aad *et al.*, “Observation of a new particle in the search for the Standard Model Higgs boson with the ATLAS detector at the LHC,” *Physics Letters B*, vol. 716, no. 1, pp. 1–29, 2012.
- [84] “Qiskit – Portfolio Optimization Documentation.” Accessed: Jun. 01, 2024. [Online]. Available: https://qiskit-community.github.io/qiskit-finance/tutorials/01_portfolio_optimization.html
- [85] F. Glover, G. Kochenberger, and Y. Du, “Quantum Bridge Analytics I: a tutorial on formulating and using QUBO models,” *4or*, vol. 17, no. 4, pp. 335–371, 2019.
- [86] “Qiskit – CPLEX Optimizer Documentation.” Accessed: Jun. 01, 2024. [Online]. Available: https://qiskit-community.github.io/qiskit-optimization/stubs/qiskit_optimization.algorithms.CplexOptimizer.html
- [87] “IBM ILOG CPLEX Optimization Studio - Lista de parametros CPLEX.” Accessed: Jun. 01, 2024. [Online]. Available: <https://www.ibm.com/docs/en/icos/22.1.1?topic=cplex-list-parameters>
- [88] “IBM Support - A note on reproducibility of CPLEX runs.” Accessed: Jun. 01, 2024. [Online]. Available: <https://www.ibm.com/support/pages/note-reproducibility-cplex-runs>
- [89] F. W. Glover and G. A. Kochenberger, *Handbook of metaheuristics*, vol. 57. Springer Science & Business Media, 2006.
- [90] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge university press, 2010.
- [91] R. Wiersema, C. Zhou, Y. de Sereville, J. F. Carrasquilla, Y. B. Kim, and H. Yuen, “Exploring entanglement and optimization within the hamiltonian variational ansatz,” *PRX Quantum*, vol. 1, no. 2, p. 020319, 2020.

- [92] M. Cerezo *et al.*, “Variational quantum algorithms,” *Nature Reviews Physics*, vol. 3, no. 9, pp. 625–644, 2021.
- [93] “Qiskit – RealAmplitudes Documentation.” Accessed: Jun. 01, 2024. [Online]. Available:
<https://docs.quantum.ibm.com/api/qiskit/qiskit.circuit.library.RealAmplitudes>
- [94] D. Kraft, *A Software Package for Sequential Quadratic Programming*. in Deutsche Forschungs- und Versuchsanstalt für Luft- und Raumfahrt Köln: Forschungsbericht. Wiss. Berichtswesen d. DFVLR, 1988. [Online]. Available:
<https://books.google.es/books?id=4rKaGwAACAAJ>
- [95] “Qiskit – SLSQP Documentation.” Accessed: Jun. 01, 2024. [Online]. Available:
https://qiskit-community.github.io/qiskit-algorithms/stubs/qiskit_algorithms.optimizers.SLSQP.html

ANEXO I:

ALINEACIÓN DEL PROYECTO CON LOS ODS

El presente Trabajo Final de Grado (TFG) en el campo de la Ingeniería de Telecomunicación se encuentra estrechamente alineado con varios Objetivos de Desarrollo Sostenible (ODS) establecidos por las Naciones Unidas. Estos objetivos, adoptados en 2015 por los estados miembros de la ONU, representan un llamado universal a la acción para poner fin a la pobreza, proteger el planeta y garantizar que todas las personas disfruten de paz y prosperidad para el año 2030. En este contexto, el TFG contribuye a la consecución de tres ODS específicos: ODS 9 (Industria, Innovación e Infraestructura), ODS 7 (Energía Asequible y no Contaminante) y ODS 17 (Alianzas para Lograr los Objetivos).



Fig. 27 Objetivos de Desarrollo Disponible de la Agenda 2030.

En primer lugar, nuestra investigación se centra en la exploración de protocolos de comunicación basados en la Distribución Cuántica de Claves (Quantum Key Distribution-QKD) para garantizar la seguridad en las comunicaciones. Este enfoque se alinea directamente con el ODS 9, que tiene como objetivo *"construir infraestructuras resilientes, promover la industrialización inclusiva y sostenible y fomentar la innovación"*. La seguridad de las comunicaciones es un aspecto crítico en el desarrollo de infraestructuras de comunicación robustas y confiables. Al investigar y promover la implementación de protocolos QKD, estamos contribuyendo activamente a la mejora de la seguridad en las redes de comunicación, lo que a su vez fortalece la economía digital global.

En segundo lugar, nuestro proyecto aborda el desarrollo de un modelo cuántico para la optimización de recursos y activos utilizando la plataforma de Qiskit. Este aspecto se alinea con el ODS 7, que busca *"garantizar el acceso a una energía asequible, segura, sostenible y moderna para todos"*. La optimización de recursos y activos es fundamental para lograr un uso eficiente y sostenible de la energía y otros recursos escasos. Los modelos cuánticos tienen el potencial de identificar estrategias más eficientes para la gestión de recursos, esto podría conducir a una reducción en el consumo de energía y una mayor sostenibilidad en diversos sectores empresariales, como puede ser el sector financiero y el sector de las telecomunicaciones .

Por último, la tercera dimensión de nuestros objetivos se centra en ofrecer una base sólida para futuras investigaciones en el campo de la Ingeniería de Telecomunicación. Este aspecto se alinea con el ODS 17, que busca *"fortalecer los medios de ejecución y revitalizar la Alianza Mundial para el Desarrollo Sostenible"*. Este trabajo no solo contribuye al avance del conocimiento en el ámbito de las telecomunicaciones, sino que también sienta las bases para futuras colaboraciones y alianzas entre investigadores, instituciones académicas y la industria. Al compartir los hallazgos, metodologías y experiencias, estamos fomentando la transferencia de conocimiento y establece un punto de partida para investigaciones posteriores. Esto promueve la colaboración internacional y multidisciplinaria, que es esencial para abordar los desafíos globales y alcanzar los ODS de manera efectiva.

En conclusión, al alinear el TFG con los ODS, se demuestra nuestro compromiso con la Agenda 2030 para el desarrollo sostenible, contribuyendo a la creación de un mundo mejor para las generaciones presentes y venideras.