Quantum Technologies: Telecom Use Cases
Version 1.0
25 February 2026

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Compliance Notice

Table of Contents

1 Introduction

1.1 Overview and Scope

The scope of this document is to give an overview on the state of development of the quantum technologies most relevant for Telecoms. Firstly, quantum computing and its potential for offering quantum-computing-as-a-service, for uses in network optimisation and for AI/ML applications is assessed. Secondly, quantum communications, such as quantum key distribution, general quantum networking (i.e. entanglement-based networking) and distributed quantum computing are assessed. Subsequently, quantum random number generators, followed by quantum sensing and quantum clocks. For all technologies, a brief overview, description of the technology, telecom-relevant use cases, potential solutions, status of the technology, challenges, opportunities and GSMA's role is given.

1.2 Previous Work

In document [1], this working group published a comprehensive overview on quantum-safe security based on Quantum Key Distribution (QKD), Quantum Random Number Generators (QRNGs) and blockchain, quantum computing (including, annealing, gate-based quantum computing, optical quantum computing and associated quantum algorithms and software and the relevance for telecoms).

Subsequently, the integration of quantum nodes and systems in current networks, an overview on standardisation efforts, the long-term perspective towards quantum networks and the model of quantum-as-a-service were explored [2].

[3] outlines the benefits of a standardised Quantum Hardware Abstraction Layer (Quantum-HAL) to accelerate the development of quantum computing and networking. It explains that while quantum technologies like QKD are advancing, progress is slowed by fragmented hardware and inconsistent terminology. A unified Quantum-HAL would provide common APIs, making it easier to develop interoperable quantum platforms and applications regardless of underlying hardware. The paper reviews current standardisation efforts and concludes that harmonising terminology and interfaces is essential for building scalable, integrated quantum infrastructures.

The document [4] analysed the opportunities and challenges of hybrid security scenarios that combine QKD and post-quantum cryptography (PQC). This work has to be seen in the context that PQC generally has a broader applicability compared to QKD. The paper provides a taxonomy of hybrid security, reviews current standardisation efforts, and presents proof-of-concept implementations. It concludes that integrating QKD and PQC can enhance security and flexibility for telecom networks, offering resilience against both current and future cryptographic threats, and recommends hybridisation as a practical path for secure communications in the quantum era.

1.3 Intended Audience

This whitepaper targets decision makers, senior experts and academics in the broader telecom industry and ecosystem (telecom operators and suppliers), and is intended for people looking to gain a broader/detailed understanding of use cases, relevance and maturity of quantum technologies in the telecom context.

1.4 Abbreviations

Term	Description
6G	Sixth Generation (mobile networks)

AES	Advanced Encryption Standard
AHS	Analogue Hamiltonian Simulation
AI	Artificial Intelligence
API	Application Programming Interface
AR/VR	Augmented Reality and Virtual Reality
AWS	Amazon Web Services
BB84	First QKD protocol by Bennett & Brassard (1984)
BBM92	Entanglement-based QKD protocol
BIQAIN	Bizkaia Quantum Advanced Industries
BSI	Federal Office for Information Security (Germany)
BSM	Bell State Measurement
CA	Certificate Authority
CapEx	Capital Expenditure
CEF	Connecting Europe Facility
CHERI	Capability Hardware Enhanced RISC Instructions
CPU	Central Processing Unit
CRP	Challenge-Response Pair
CUDA-Q	Compute Unified Device Architecture Quantum
CV-QKD	Continuous-Variable Quantum Key Distribution
DC	Data Centre
DQC	Distributed Quantum Computing
DQI	Decoded Quantum Interferometry
DQN	Deep Q-Network
DRBG	Deterministic Random Bit Generator (Software Random Number Generator)
DT	Data Centre
DV-QKD	Discrete-Variable Quantum Key Distribution
DWDM	Dense Wavelength Division Multiplexing
EaaS	Entropy-as-a-Service
E2E	End-to-End
ESA	European Space Agency
ETSI	European Telecommunications Standards Institute
EuroQCI	European Quantum Communication Infrastructure
FOADM	Fixed Optical Add-Drop Multiplexer
GNSS	Global Navigation Satellite System
GPU	Graphics Processing Unit

GR	Group Reports
GS	Group Specifications
GSMA	GSM Association
HAL	Hardware Abstract Layer
HES	Hardware Entropy Source (Hardware Random Number Generator)
HPC	High Performance Computing
HSM	Hardware Security Modules
ID	Identifier
ILP	Integer Linear Programming
IMT	International Mobile Telecommunication
ISG QKD	Industry Specification Group on QKD
ITSCC	IT Security Certification Center
ITU	International Telecom Union
KDI	Key Distribution Infrastructure
KMS	Key Management System
KPI	Key Performance Indicator
KRISS	Korea Research Institute of Standards and Science
LEO	Low Earth Orbit
LIDAR	Light Detection and Ranging
LLM	Large Language Model
MDI-QKD	Measurement-Device-Independent Quantum Key Distribution
ML	Model Language
NCSC	National Cyber Security Centre
NISQ	Noisy Intermediate-Scale Quantum
NIST	National Institute for Standards and Technology (US)
NP	Nondeterministic Polynomial
NSR	National Security Research Institute
NV	Nitrogen-Vacancy
OFC	Optical Fibre Communications Conference and Exhibition
OPex	Operational Expenditure
OSI	Open Systems Interconnection (encryption levels)
OTDR	Optical Time-Domain Reflectometry
PCI	Physical Cell ID
PCIe	Peripheral Component Interconnect Express
PC-OTDR	Photon-Counting Optical Time-Domain Reflectometry

PEC	Probabilistic Error Cancellation
PM-QKD	Prepare and Measure Quantum Key Distribution
PNR	Photon Number Resolution
PNT	Positioning, Navigation, and Timing
PP	Protection Profile
PQC	Post-Quantum Cryptography
PRNG	Pseudo-Random Number Generators
PUF	Physical Unclonable Function
QAOA	Quantum Approximate Optimization Algorithm
QBM	Quantum Boltzmann Machine
QC	Quantum Computing
QCaaS	Quantum-Computing-as-a-Service
QCI	Quantum Communication Infrastructure
QDS	Quantum Dice System
QEaaS	Quantum-Entropy-as-a-Service
QEC	Quantum Error Correction
QELM	Quantum Extreme Learning Machine
QIA	Quantum Internet Alliance
QIO	Quantum-Inspired Optimization
QIR	Quantum Intermediate Representation
QIRG	Quantum Internet Research Group
QKD	Quantum Key Distribution
QKMS	Quantum Key Management System
QML	Quantum Machine Learning
QMS	Quantum Management System
QNN	Quantum Neural Network
QNS	Quantum Networks and Services
QPU	Quantum Processing Unit
qPUF	Quantum Physical Unclonable Function
QR-PUF	Quantum Readout Physical Unclonable Function
QRC	Quantum Reservoir Computing
QRNG	Quantum Random Number Generator
QRPUF	Quantum Readout Physical Unclonable Function
QUBO	Quadratic Unconstrained Binary Optimisation
QSA	Quantum Security Architecture
RA	Radio Access

R&D	Research & Development
RAQ-MIMO	Rydberg Atomic Quantum Multiple-Input Multiple-Output
RAN	Radio Access Network
RF	Radio Frequency
RISC	Reduced Instruction Set Computer
RSI	Root Sequence Index
SAC	Subscriber Acquisition Cost
SDE	System Detection Efficiency
SDK	Software Development Kit
SDN	Software Defined Networking
SDO	Standardization Development Organizations
SG	Study Groups
SLA	Service Level Agreements
SON	Self-Optimizing Networks
SQL	Structured Query Language
SMQC	Secure Multi-Party Quantum Computation
SME	Small & Medium Enterprises
SNSPD	Superconducting Nanowire Single-Photon Detector
SP	Service Provider
SPAD	Single-Photon Avalanche Diode
SPD	Single-Photon Detectors
SRAM	Static Random Access Memory
SRC	Subscriber Retention Cost
SWAP	Size, Weight and Power
TF-QKD	Twin-Field Quantum Key Distribution
TTA	Telecommunications Technology Association
THz	TeraHertz
VEN	Virtual Extended Network
VQAs	Variational Quantum Algorithms
VQE	Variational Quantum Eigensolver
VPN	Virtual Private Network
ZNE	Zero Noise Extrapolation

Table 1: Abbreviations

1.5 References

Reference	Title/ URL
[1]	IG.11 Quantum Computing Networking and Security - Newsroom
[2]	IG-12-Quantum-Networking-and-Service.pdf
[3]	IG-14-Quantum-Hardware-Abstraction-Layer-for-Quantum-Computing-and-Networking.pdf
[4]	Hybrid (QKD and PQC) security scenarios and use cases - Whitepaper
[5]	IBM Quantum Computing | Qiskit: https://www.ibm.com/quantum/qiskit
[6]	QiliSDK, https://qilimanjaro-tech.github.io/qilisdk/main/index.html
[7]	QIR Aliance https://www.qir-alliance.org/
[8]	NVIDIA CUDA-Q: https://developer.nvidia.com/cuda-q
[9]	Quantum Flagship, 2024: https://qt.eu/working-groups/standardization
[10]	Q# Language: https://learn.microsoft.com/en-us/azure/quantum/qsharp-overview
[11]	Jupyter: https://jupyter.org/
[12]	Bizkaia's Quantum Strategy https://www.bizkaia.eus/en/web/quantum-ecosystem
[13]	Kandala, A., Temme, K., Córcoles, A. D., Mezzacapo, A., Chow, J. M., & Gambetta, J. M. (2019). Error mitigation extends the computational reach of a noisy quantum processor. *Nature*, *567*(7749), 491-495.
[14]	Van Den Berg, E., Minev, Z. K., Kandala, A., & Temme, K. (2023). Probabilistic error cancellation with sparse Pauli–Lindblad models on noisy quantum processors. *Nature physics*, *19*(8), 1116-1121.
[15]	Maurer, T., Bühler, M., Kröner, M., Haverkamp, F., Müller, T., Vandeth, D., & Johnson, B. R. (2025). Real-time decoding of the gross code memory with FPGAs. *arXiv preprint arXiv:2510.21600*.
[16]	Microsoft Magne: https://news.microsoft.com/source/emea/features/microsoft-opens-state-of-the-art-quantum-lab-in-lyngby-denmark-accelerating-progress-toward-scalable-quantum-computing/
[17]	Tianyan Quantum Group (2025). Tianyan: Cloud services with quantum advantage. arXiv preprint arXiv:2512.10504.
[18]	Long-Term Forecast for Quantum Computing Still Looks Bright | BCG
[19]	World Economic Forum (2025), Embracing the Quantum Economy: A Pathway for Business Leaders
[20]	https://hellofuture.orange.com/en/orange-launches-a-quantum-computing-research-initiative-to-optimise-network-operations/
[21]	https://quantum-or.euro-online.org/
[22]	Wurtz, J., Lopes, P. L., Gorgulla, C., Gemelke, N., Keesling, A., & Wang, S. (2022). Industry applications of neutral-atom quantum computing solving independent set problems. *arXiv preprint arXiv:2205.08500*.
[23]	Bouchmal, Oumayma, et al. "Quantum computing approach for multi-objective routing and spectrum assignment optimization." *Journal of Optical Communications and Networking* 17.6 (2025): B15-B27.
[24]	Macaluso, S., Geraci, G., Combarro, E. F., Abadal, S., Arapakis, I., Vallecorsa, S., & Alarcon, E. (2025). Quantum Computing for Large-Scale Network Optimization: Opportunities and Challenges. *IEEE Communications Magazine*.
[25]	Gao, D., Fan, D., Zha, C., Bei, J., Cai, G., Cai, J., ... & Zhu, C. (2025). Establishing a new benchmark in quantum computational advantage with 105-qubit Zuchongzhi 3.0 processor. *Physical Review Letters, 134(9)*, 090601.
[26]	Acharya, Rajeev, et al. "Quantum error correction below the surface code threshold." *Nature (2024)*.

Reference	Title/ URL
[27]	N. Cáliz, A., Riu, J., Bosch, J., Torrente, P., Miralles, J., & Riera, A. (2025). A coherent approach to quantum-classical optimization. *Communications Physics*, *8*(1), 197.
[28]	Telefónica and Multiverse Computing develop an AI-based model to support customer service agents with 75% energy savings
[29]	Jascha Sohl-Dickstein, Eric Weiss, Niru Maheswaranathan, and Surya Ganguli. 2015. Deep unsupervised learning using nonequilibrium thermodynamics. In Proceedings of the International Conference on Machine Learning (ICML).
[30]	Jonathan Ho, Ajay Jain, and Pieter Abbeel. 2020. Denoising diffusion probabilistic models. In Advances in Neural Information Processing Systems. H. Larochelle, M. Ranzato, R. Hadsell, M. F. Balcan, and H. Lin (Eds.), Vol. 33, Curran Associates, Inc., 6840–6851. Retrieved from https://proceedings.neurips.cc/paper_files/paper/2020/file/4c5bcfec8584af0d967f1ab10179ca4b-Paper.pdf
[31]	Villaizán-Vallelado, Mario, et al. "Diffusion models for tabular data imputation and synthetic data generation." *ACM Transactions on Knowledge Discovery from Data* 19.6 (2025): 1-32.
[32]	Tero Karras, Miika Aittala, Samuli Laine, and Timo Aila. 2024. Elucidating the design space of diffusion-based generative models. In Proceedings of the 36th International Conference on Neural Information Processing Systems (NIPS '22). Curran Associates Inc., Red Hook, NY, Article 1926, 13 pages.
[33]	Bingzhi Zhang, Peng Xu, Xiaohui Chen, and Quntao Zhuang. 2024. Generative quantum machine learning via denoising diffusion probabilistic models. *Physical Review Letters* 132, 100602
[34]	Gino Kwun, Bingzhi Zhang, and Quntao Zhuang. 2025. Mixed-State Quantum Denoising Diffusion Probabilistic Model. *arXiv preprint* arXiv:2411.17608.
[35]	Michael Kölle, Gerhard Stenzel, Jonas Stein, Sebastian Zielinski, Björn Ommer, and Claudia Linnhoff-Popien. 2024. Quantum Denoising Diffusion Models. *arXiv preprint* arXiv:2401.07049
[36]	Yunfei Wang, Ruoxi Jiang, Yingda Fan, Xiaowei Jia, Jens Eisert, Junyu Liu, and Jin-Peng Liu. 2025. Towards efficient quantum algorithms for diffusion probability models. *arXiv preprint* arXiv:2502.14252
[37]	Huang, H. Y., Broughton, M., Eassa, N., Neven, H., Babbush, R., & McClean, J. R. (2025). Generative quantum advantage for classical and quantum problems. *arXiv preprint arXiv:2509.09033*.
[38]	Recio-Armengol, E., & Bowles, J. (2025). IQPopt: Fast optimization of instantaneous quantum polynomial circuits in JAX. *arXiv preprint arXiv:2501.04776*.
[39]	Minervini, M., Patel, D., & Wilde, M. M. (2025). Evolved quantum Boltzmann machines. *arXiv preprint arXiv:2501.03367*.
[40]	Kobayashi, K., Fujii, K., & Yamamoto, N. (2024). Feedback-driven quantum reservoir computing for time-series analysis. *PRX quantum*, *5*(4), 040325.
[41]	De Lorenzis, A., Casado, M. P., Estarellas, M. P., Lo Gullo, N., Lux, T., Plastina, F., ... & Settino, J. (2025). Harnessing quantum extreme learning machines for image classification. *Physical Review Applied*, *23*(4), 044024.
[42]	Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, *560*, 7-11.

Reference	Title/ URL
[43]	A Multiplane Architecture Proposal for the Quantum Internet draft-lopez-qirg-qi-multiplane-arch-05 https://datatracker.ietf.org/doc/draft-lopez-qirg-qi-multiplane-arch/
[44]	Ekert. A, Phys. Rev. Lett. 67, 661-663 (1991).
[45]	Grosshans, F. et al. Quantum key distribution using gaussian-modulated coherent states. *Nature* **421**, 238–241 (2003).
[46]	Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
[47]	Weedbrook, C. et al. Quantum cryptography without switching. *Phys. Rev. Lett.* **93**, 170504 (2004).
[48]	B. Amies-King *et al.*, "Quantum Communications Feasibility Tests over a UK-Ireland 224 km Undersea Link", *Entropy* **25**, 1572 (2023)
[49]	https://www.idquantique.com/quantum-detection-systems/products/id281-snspd-system/
[50]	https://www.idquantique.com/quantum-detection-systems/products/id281-pro-snspd-system/
[51]	London Quantum-Secured Metro Network Andrew Lord, Robert Woodward, Shinya Murai, Hideaki Sato, James Dynes, Paul Wright, Catherine White, Russell Davey, Mark Wilkinson, Piers Clinton-Tarestad, Ian Hawkins, Kristopher Farrington, and Andrew Shields Author Information (2023) https://opg.optica.org/abstract.cfm?uri=ofc-2023-W4K.4
[52]	Martin, V., Brito, J. P., Ortíz, L., Méndez, R. B., Buruaga, J. S., Vicente, R. J., ... & Lopez, D. (2024). MadQCI: a heterogeneous and scalable SDN-QKD network deployed in production facilities. *npj Quantum Information*, *10*(1), 80.
[53]	Position Paper on Quantum Key Distribution https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf?__blob=publicationFile&v=4
[54]	Melgar, A., Iqbal, M., Rivas-Moscoso, J. M., Tabares, J., Moreolo, M. S., Villanueva, B., & Folgueira, J. (2024, September). Coexistence of commercial CV-QKD and DWDM 100G/400G transmission in amplified FOADM-based metro links. In *ECOC 2024; 50th European Conference on Optical Communication* (pp. 1416-1419). VDE.
[55]	Melgar, A., Iqbal, M., Moreolo, M. S., Rivas-Moscoso, J. M., Tabares, J., Arminqol, P., Villanueva, B., Etcheverry, S., & Folgueira, J. (2025) Coexistence of Commercial CV-QKD in FOADM-based Metro Networks with Full or Partial C-Band Utilization, *2025 Optical Fibre Communications Conference and Exhibition (OFC)*. IEEE, 2025.
[56]	Nejabati R. in GSMA Webinar "Quantum in telecom: towards real-world impact" Quantum in telecom: towards real-world impact | LinkedIn
[57]	S. Donadello *et al.*, "Seismic monitoring using the telecom fiber network", *Communications Earth & Environment* **5**, 178 (2024).

Reference	Title/ URL
[58]	IBM and Cisco Announce Plans to Build a Network of Large-Scale, Fault-Tolerant Quantum Computers
[59]	iQuila
[60]	Quantum Dice and AT&T to present Entropy-as-a-Service - Inside Telecom
[61]	Quantum Dice teams with secure systems startup SCI Semi ...
[62]	Samsung QRNG Use Case | ID Quantique
[63]	Cui, M., Zeng, Q., & Huang, K. (2025). Rydberg atomic receiver: Next frontier of wireless communications. *IEEE Communications Magazine*.
[64]	https://publications.jrc.ec.europa.eu/repository/bitstream/JRC136355/JRC136355_01.pdf
[65]	Krokosz, W., Nowosielski, J., Kasza, B., Borówka, S., Mazelanik, M., Wasilewski, W., & Parniak, M. (2025). Electric-field metrology of a terahertz frequency comb using Rydberg atoms. *Optica*, *12*(11), 1854-1864.
[66]	Gong, T., Yuen, C., See, C. M. S., Debbah, M., & Hanzo, L. (2025). Rydberg atomic quantum receivers for the multi-user MIMO uplink. *arXiv preprint arXiv:2501.18382*.
[67]	The Finnish Research Impact Foundation supports Tampere University's quantum-assisted 6G research | Tampere universities
[68]	https://www.idquantique.com/quantum-detection-systems/products/id-qube-uln/
[69]	https://www.idquantique.com/quantum-detection-systems/snspd-technology/
[70]	I. Holzman and Y. Ivry, "Superconducting Nanowires for Single-Photon Detection: Progress, Challenges, and Opportunities", *Advanced Quantum Technologies* **2**, 1800058 (2019)
[71]	L. Stasi *et al.*, "Enhanced Detection Rate and High Photon-Number Efficiencies with a Scalable Parallel SNSPD", *ACS Photonics* **12**, 320 (2024)
[72]	S. B. Jones *et al.*, "Time domain reflectometry measurement principles and applications", *Hydrological processes* **16**, 141 (2002).
[73]	M. Makhlouf *et al.*, "Photon-Counting Optical Time Domain Reflectometer Using Superconducting Nanowire Single Photon Detector Based on Time to Digital Converter", *7th International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE)*, IEEE, (2025).
[74]	J. Gasser *et al.*, "Distributed temperature sensor combining centimeter resolution with hundreds of meters sensing range", *Optics Express* **30**, 6768 (2022)
[75]	T. Staffas *et al.*, "Temperature measurements in deployed optical fiber networks using single photon optical time domain reflectometry", *Optics Express* **31**, 8170 (2023).
[76]	K. Wei et al., "Implementation security of quantum key distribution due to polarization-dependent efficiency mismatch", Physical Review A 100, 022325 (2019)
[77]	A. Boaron et al., "Secure Quantum Key Distribution over 421 km of Optical Fiber", Physical Review Letters 121, 190502 (2018)
[78]	https://infleqtion.com/inertial-sensing/
[79]	Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. Science, 362(6412), eaam9288.
[80]	Delle Donne, C., et al. "An operating system for executing applications on quantum network nodes." Nature 639.8054 (2025): 321-328.

Table 2: References

2 Quantum Technologies in the Telecom Context

Quantum technologies are redefining the telecom landscape by introducing capabilities that go far beyond classical systems. One of the more imminent applications is Quantum Key Distribution (QKD), which ensures ultra-secure communications by exploiting quantum states that cannot be copied or intercepted without detection. This is critical for telecom operators managing sensitive data across global networks, especially as quantum computers threaten traditional encryption standards. While QKD still has notable limitations (especially distance limitations, cost and scalability), QKD-based solutions are already being piloted on fibre and satellite links, paving the way for quantum-secure backbone networks. Quantum Random Number Generators (QRNGs) can improve the security of cryptographic protocols with Quantum-Entropy-as-a-Service (QEaaS).

Quantum computing offers telecoms a powerful tool to tackle computationally intensive problems that classical systems struggle with. Optimisation tasks in the telecom domain, such as traffic routing, network parameter planning and energy-efficient network design, can have massive combinatorial complexity. Quantum algorithms have the potential to significantly reduce computation time and improve efficiency. In the era of 5G and 6G, where ultra-low latency and dynamic resource allocation are essential, quantum computing could enable real-time decision-making and unlock new services, such as predictive maintenance and advanced network orchestration.

The evolution of quantum sensing also enables new applications. In the future, Quantum Radio Frequency (RF) sensing could further improve signal processing capabilities. Already today, Superconducting Nanowire Single Photon Detectors (SNSPDs) are key in new QKD protocols, and other quantum communications protocols.

Beyond computation, sensing and security, quantum networking introduces a paradigm shift by enabling the transmission of quantum information across distributed systems. This involves creating entanglement-based links between nodes, forming the foundation of a future quantum internet. For telecoms, quantum networking could lead to ultra-secure cloud services, distributed quantum computing, and new business models around “quantum-as-a-service”. While challenges remain, such as maintaining entanglement over long distances and integrating quantum repeaters, global initiatives and standardisation efforts are accelerating progress. Early adoption can position telecom operators at the forefront of next-generation connectivity.

3 Quantum Technologies Use Cases

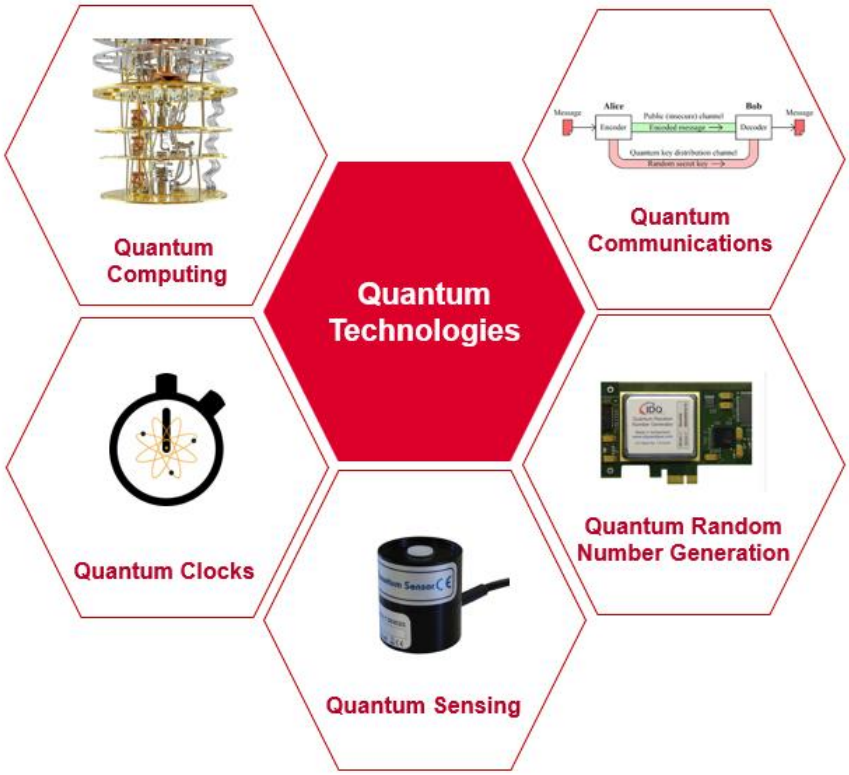


Figure 1**:** Overview on quantum technologies

Figure 1**Figure** 1 gives an overview of the quantum technologies investigated in this white paper. All of them have potential use cases for telecoms and are analysed in detail. Quantum computing is investigated in 3.1. Quantum communications such as (terrestrial and space-based) QKD, entanglement networking and distributed quantum computing are elaborated in section 3.2. Section 3.3 analyses QRNGs for quantum entropy. Use cases of quantum sensing, such as RF sensing and SNSPDs, are described in 3.4. Quantum Positioning, Navigation, and Timing is touched upon in 3.5, but the detailed analysis is left to future documents. Section 3.6 concludes the document with an outlook to the quantum internet vision.

Note that the mitigation of risks to encryption via adoption of PQC is outside the scope of the Quantum Networks and Services (QNS) working group, and so for this we refer the reader to whitepapers of GSMA's Post Quantum Telecom Network task force (PQTN).

3.1 Quantum Computing

Among the different technologies shown in Figure 1, quantum computing is of high relevance, as this could offer new ways to tackle previously unsolved computational problems. For telecoms, this offers two possibilities: They can offer quantum-computing-as-a-service to enterprise customers, which is detailed in section 3.1.1. They can also apply it to telecom optimisation problems, which is evaluated in 3.1.2. Finally, there is increasing interest in Quantum AI/ML by the telco industry (e.g. vendors, select network operators), which we cover in 3.1.3.

3.1.1 Quantum-Computing-as-a-Service (QCaaS)

Quantum-Computing-as-a-Service (QCaaS) may represent a transformative shift in how organisations access and leverage quantum computing capabilities. Traditionally, quantum computing has been confined to specialised laboratories, largely due to the complexity and cost of building and maintaining quantum hardware. QCaaS breaks this barrier by delivering quantum computing power to end-users through cloud platforms, enabling enterprises, researchers, and developers to run quantum algorithms remotely, without the need for physical infrastructure.

Quantum computing on the cloud provides an important mechanism to make quantum accessible. This is critical in building skills, fostering open innovation and accelerating progress, by providing access to the latest, most performant systems. By lowering entry barriers, QCaaS empowers a broader community to build and leverage the potential that quantum computing offers across sectors, as quantum compute capabilities rapidly evolve. As quantum hardware continues to evolve, QCaaS platforms are positioned to scale with the technology, offering users access to diverse quantum backends, developer tools, and orchestration engines. This ensures that organisations can begin their quantum journey today, with the flexibility to adopt more advanced capabilities as they become available.

QCaaS may represent a key transitional phase in the evolution of computing, bridging the gap between theoretical research and practical application. This enables organisations to experiment with quantum algorithms, benchmark emerging hardware, and develop hybrid quantum–classical workflows that integrate with existing High-Performance Computing (HPC) infrastructures. In this model, quantum resources are accessed as part of the broader cloud ecosystem, facilitating scalable innovation and incremental adoption.

Although current quantum devices remain within the Noisy Intermediate-Scale Quantum (NISQ) era and continue to underperform classical computing systems in most use cases, QCaaS provides the framework required for advancing toward practical quantum computing and quantum advantage, offering a controlled environment in which algorithms, middleware, and skills can evolve alongside hardware progress. The future of quantum computing is therefore expected to be complementary rather than competitive, with quantum systems acting as specialised accelerators embedded within hybrid computational architectures, rather than as replacements for classical HPC.

The following subsections examine QCaaS in detail. Subsection 3.1.1.1 describes its architecture and access models. Subsection 3.1.1.2 outlines representative use cases and problem domains. Subsection 3.1.1.3 presents current algorithmic and operational solutions. Subsection 3.1.1.4 assesses the technological maturity of the field. Subsection 3.1.2.5 discusses the main challenges that constrain its scalability and adoption, while Subsection 3.1.1.6 identifies emerging opportunities for research, innovation, and industry development. Subsection 3.1.1.7 concludes the QCaaS section by describing the role for GSMA in QCaaS.

3.1.1.1 Description

QCaaS refers to the exposure of quantum computing capabilities via cloud platforms, allowing users to access quantum processors on-demand without the need to acquire and manage specialised hardware. In the evolving landscape of computing infrastructure, QCaaS is emerging alongside traditional HPC and Artificial Intelligence (AI) infrastructure as a technology that may further enable network acceleration. While HPC is designed for general computationally intensive tasks (e.g. large-scale simulations, genomics) leveraging multi-core Central Processing Units (CPUs), and AI platforms are optimised for machine learning and data-driven workloads using Graphics Processing Units (GPUs), quantum computing is intended for a narrower class of extremely complex problems that are intractable or inefficient on classical systems. QCaaS makes this specialised power available as a cloud service,

meaning telecom operators and enterprises can incorporate quantum algorithms into their workflows without the need to build quantum data centrs, assuming quantum computing technology is adequately advanced and stable.

QCaaS platforms provide structured access to quantum computing resources through a layered architecture that standardises user interaction, system orchestration, and hardware execution. This architecture generally comprises three functional layers: frontend, middleware and backend. The frontend layer refers to the user interface and software environment for developing and deploying quantum algorithms. Frameworks such as IBM Qiskit [5] or Qilimanjaro QiliSDK [6] enable developers to construct quantum circuits (for digital systems) or Hamiltonians (for analogue models), manage job execution, and visualise results. These toolkits typically integrate with classical programming languages, such as Python, facilitating hybrid algorithm design where quantum subroutines are embedded in classical control loops.

However, since some providers are also maintaining proprietary software development kit (SDKs) and programming interfaces, developers can face difficulties when porting algorithms across different QCaaS platforms. This fragmentation increases the learning curve needed to overcome, reduces code reusability, and inhibits cross-platform adoption. The industry is therefore moving toward a standardised frontend layer capable of abstracting hardware-specific details and offering a unified programming model. Initiatives such as the Quantum Intermediate Representation (QIR), developed by the QIR Alliance [7], aim to address this challenge by defining a hardware-agnostic intermediate representation between quantum programming languages and various back-end architectures. QIR acts as a bridge that enables multi-vendor interoperability and software portability, ensuring that the same algorithmic logic can execute seamlessly on different quantum devices. This approach is used by Compute Unified Device Architecture Quantum (CUDA-Q) [8] to allow the job execution in different backends without the need to modify the algorithm developed by the user.

Complementing this, the Quantum Flagship Standardisation Working Group emphasises that international and European standards are critical to "facilitate the growth of new technologies and the development of efficient and effective supply chains" by enabling "the harmonisation of technologies, methodologies, and interfaces" ([9]). These efforts aim to align diverse SDKs, interfaces, and representations under common frameworks, reducing fragmentation across the QCaaS ecosystem.

The middleware layer takes the role of the orchestration layer, responsible for job scheduling, optimisation, and hybrid execution, translating high-level circuit descriptions into hardware-specific gate instructions, handling error mitigation, and managing communications between quantum and classical resources. Middleware services also implement quantum resource schedulers and execution queues to allocate limited quantum hardware among multiple users, ensuring fairness and reproducibility.

Last, the backend layer refers to the physical quantum processors and simulators hosted in highly controlled environments. Implementations include superconducting qubits, trapped-ion systems, photonic processors, neutral-atom systems, and others such as Nitrogen-Vacancy (NV) centres or spin-based.

In the QCaaS model, quantum technology providers adopt different provisioning strategies. Some of them, offer direct access via dedicated web portals, dashboards, and APIs, providing users with full control of workload submission and monitoring within proprietary ecosystems optimised for their specific hardware.

HPC Infrastructure	AI Infrastructure	Quantum Computing

Designed specifically for computationally intensive tasks	Designed specifically for AI training inferencing and development	Designed for very specific extremely complex problems
Hardware, networking, storage software	Hardware, software, storage, networking, frameworks	Highly specialized hardware and software
High speed, distributed serial processing	Extreme parallel processing, massive scale up and out	Quantum mechanics applied for processing
Relies heavily on multi-core CPU	Relies heavily on GPU	Relies on qubits and quantum processing unit (QPUs)

Table 3: Overview on HPC infrastructure vs. AI infrastructure vs. quantum computing

How QCaaS Works: A QCaaS provider operates various QPUs in their cloud and users write quantum programs in high-level languages and submit jobs through a web interface or API. The QCaaS platform then handles job scheduling, qubit control, and result retrieval. From a telecom perspective, this means a developer could, for example, send a network optimisation problem to a high-powered analogue quantum computer, quantum annealer or gate-based quantum computer via the cloud and get back an optimised solution without ever dealing with the cryogenics or quantum hardware maintenance. In essence, QCaaS turns quantum computers into a remotely accessible resource, much like cloud HPC makes supercomputers remotely accessible.

This cloud delivery is crucial because current quantum hardware is expensive and delicate. By centralising resources, QCaaS allows many organisations to share quantum machines. This also enables rapid updates: as new quantum chips or technologies become available, the provider can incorporate them, and clients automatically get access. For telecoms, QCaaS lowers the barrier to experiment with quantum algorithms for things like network planning or cryptography; they can iterate on use cases now, rather than waiting years to possibly own a quantum computer. Moreover, QCaaS encourages hybrid computing: tying quantum jobs into classical workflows. For example, a classical system might pre-process telecom data, call a quantum subroutine via QCaaS for an optimisation step, and then post-process the results – all orchestrated in the cloud.

In summary, QCaaS offers telecom operators a practical route to start leveraging quantum computing today as a scalable, pay-per-use service, extending the existing cloud computing model to include quantum accelerators, positioning quantum computing not as a distant lab experiment, but as a readily accessible tool. This is particularly powerful for an industry like telecoms, which often deals with optimisation and security problems that push the limits of classical computing.

3.1.1.2 Use Case / Problem Statement

The increasing complexity of digital ecosystems across industries, such as telecommunications, finance, logistics, energy, and materials science, has revealed the computational limits of classical computing architectures. Many industrial and research problems are combinatorial, non-linear, or high-dimensional, which means that the number of possible solutions grows exponentially with problem size. Traditional HPC systems often cannot process these workloads efficiently within acceptable time or energy constraints. The problem QCaaS seeks to address is the intractability of complex optimisation and simulation tasks when using classical computing systems alone. Quantum computing introduces a new computational paradigm that leverages superposition, allowing simultaneous evaluation of multiple states, and entanglement, enabling the representation of interdependencies between variables. By accessing these capabilities through QCaaS, organisations can experiment with

and deploy quantum algorithms without owning quantum hardware. QCaaS platforms act as quantum accelerators within cloud ecosystems, making it possible to integrate quantum processing into existing computational pipelines. This model is particularly suited for iterative optimisation tasks, simulation workloads, and hybrid machine learning processes that benefit from quantum parallelism.

Currently, only a small subset of problems that network operators face are well served by quantum computing. Quantum computing currently is still at a lower technology readiness level, its role in standardisation frameworks (e.g. 3GPP or ITU IMT) has yet to be studied. Microsoft has designed a process to advocate a structured approach (a decision tree) to identify when a telecom problem is a good candidate for a quantum solution. Below (and in table 4) is a step-by-step logic that can be used (often in sequence) to evaluate potential quantum use cases:

Steps	Questions	Actions	
1	Can computation solve the problem?	If **yes**, continue to next step	If **no**, reduce to computational problem
2	Is computational performance the blocker?	If **yes**, continue to next step	If **no**, resolve blockers, such as lack of data
3	Is the computation solution limited by input/output?	If **no**, continue to next step	If **yes**, explore HPC and AI solutions
4	Is there a quantum algorithm with a superpolynomial quantum speedup	If **yes**, to super polynomial speedup up, skip to step 6	If practical quantum advantage found, continue to next step
5	Exploration research		
6	Implement quantum solutions and estimate resources needed		

Table 4: Structured approach for identifying problem candidates for quantum solutions

1. **Is the problem definable as a computational problem?** – First, ensure the challenge can be framed in computational terms. If the issue is something like an organisational or policy problem (not solvable by calculation), then quantum computing is irrelevant. Only if you can formulate the problem as an algorithm or mathematical model should you proceed. For example, “improve customer satisfaction” is too vague, whereas “optimise the placement of 5G towers for coverage” is computational.

2. **Is current computing performance the bottleneck?** – If classical computers (even high-end servers or HPC) already solve the problem efficiently, there’s no value in a quantum approach. However, if you identify that no matter how much classical computing you utilise, the problem remains intractable (e.g. it would take years or would require simplifying assumptions), then there is a performance-driven need. Telecom examples might include extremely large combinatorial optimisations (like globally optimal routing of millions of connections) where classical solvers give suboptimal results or run too slowly.

3. **Is the problem I/O-bound rather than compute-bound?** – Sometimes the slow part of a task is reading/writing data or waiting for events (I/O), not crunching numbers. If a task is bottlenecked by data transfer or latency (common in real-time network control), a faster computer – quantum or not – will not help. In such cases, optimising data pipelines or using edge computing is the solution, not quantum. Only if the core computation itself is the roadblock should one consider new computing paradigms.

4. **Does a suitable quantum algorithm exist (with super-polynomial speedup)?** – This is a critical checkpoint. Quantum computing is not a magic wand; it excels only for certain problems with known quantum algorithms that outperform classical ones by a significant margin (superpolynomially, meaning exponentially faster or similar). For instance, in cybersecurity, Shor's algorithm factors large numbers exponentially faster than known classical methods – a clear quantum advantage. In optimisation, algorithms like Grover's offer quadratic speedups for unstructured search, and quantum annealing might find better optima for specific Nondeterministic Polynomial (NP)-hard problems. If no known quantum algorithm can tackle your problem type faster than classical, then quantum computing will not help today. In telecom, if you consider a problem like "route planning," quantum heuristic algorithms exist (e.g. Quantum Approximate Optimization Algorithm (QAOA) for graph problems), which is promising. But if one considers something like basic arithmetic (which classical does well), quantum offers no benefit.

5. **Exploration and prototyping:** – If the above conditions suggest a potential quantum use case (i.e. it is a compute-bound, performance-limited problem, and a candidate quantum algorithm is known), the next step is to engage in Research & Development and small-scale experimentation. This might involve simplifying the problem and running it on a quantum simulator or a small QCaaS backend to see how the quantum algorithm behaves. At this stage, one might discover practical issues (like the problem mapping is too complex, or it needs too many qubits) – in which case one might defer the project and re-explore with HPC/AI enhancements. If the prototype shows practical quantum advantage on smaller instances (or evidence that advantage will emerge at scale)[1], that is a good sign to proceed.

6. **Implement the quantum solution & estimate resources:** – Finally, if exploration is successful, implement a full quantum solution via QCaaS or hybrid architecture. Plan out the resources needed – how many qubits, what runtime, and what cost on QCaaS. It is crucial to also integrate it with classical systems: e.g., feeding network data into the quantum algorithm and applying the output back into the network operations. At this stage, one should also monitor *when* a quantum solution becomes worthwhile: perhaps the solution works, but only on a quantum computer with, say, 1000 qubits. In that case, one might schedule the switchover when hardware reaches that point. On the other hand, if a current 100-qubit quantum computer can already solve the sub-problem better than classical, one might deploy it immediately for that niche task.

This decision framework (illustrated by a flowchart in the graph above) is essentially about being pragmatic, preventing wasted effort on quantum hype by filtering out cases where classical computing is sufficient or where quantum is not ready. At the same time, it flags truly hard problems – common in telecom optimization, security, and large-scale simulations – where quantum could be revolutionary and worthwhile pursuing. By asking these questions, telecom engineers and strategists can focus their quantum efforts where they matter most, such as massively complex scheduling problems, cryptographic vulnerabilities, or network algorithms that dominate CPU time.

The range of problems that challenge classical computational capacity extends across multiple industrial and scientific domains:

- In **telecommunications and network optimisation**, tasks such as dynamic spectrum allocation, interference mitigation, and handover coordination in 5G and upcoming 6G systems require exploration of vast configuration spaces in near real time. The scale and dynamism of these networks make exhaustive search approaches computationally impractical for classical systems.

- In the **financial sector**, quantum computing holds potential to address portfolio optimisation, risk assessment, and derivative pricing, all of which involve evaluating numerous interdependent variables under uncertain market conditions. Classical solvers typically rely on heuristic approximations, which can compromise accuracy and convergence speed when managing large and volatile datasets.

- **Logistics and supply chain management** face optimisation challenges in route planning, scheduling, and resource allocation. As the number of constraints and decision points grows, the computational cost of finding globally-optimal solutions increases exponentially, often exceeding the capabilities of even advanced HPC clusters.

- In **energy systems**, the need to balance production and consumption within distributed smart grids introduces a further layer of complexity. Managing variable renewable generation, demand response, and grid stability requires solving large-scale optimisation problems under real-time and uncertain conditions.

- In **quantum chemistry and materials science**, simulating molecular interactions, reaction pathways, and material properties at high accuracy requires modelling quantum mechanical effects that scale exponentially with system size. Even state-of-the-art classical supercomputers struggle to perform such simulations efficiently or with sufficient precision. Together, these domains exemplify the computational bottlenecks inherent in classical architectures and highlight the pressing need for novel paradigms such as quantum computing, which can address the combinatorial nature and exponential scaling.

3.1.1.3 Solution

QCaaS may provide a practical and scalable solution to the computational challenges that classical systems cannot efficiently address. By delivering quantum capabilities through cloud infrastructure, QCaaS allows users to remotely design, test, and execute quantum algorithms on both simulated and real hardware. This delivery model significantly reduces entry barriers, by eliminating the need for organisations to invest in costly, specialised infrastructure, while providing access to cutting-edge quantum resources for experimentation, benchmarking, and research in the first instance.

At the core of QCaaS lies the concept of hybrid quantum–classical computation, where classical and quantum systems collaborate within a unified workflow. In this model, classical computing handles data pre-processing, parameter optimisation, and results analysis, while quantum processors perform the tasks that exploit quantum phenomena such as superposition and entanglement. This division of labour maximises computational efficiency and compensates for the limitations of current NISQ hardware. The hybrid approach enables users to embed quantum subroutines into existing software environments and execute them seamlessly through cloud interfaces.

Developers access these capabilities through standardised software development kits (SDKs) and application programming interfaces (APIs) that support high-level programming languages such as Python. Quantum algorithms can be constructed, deployed, and managed

through these interfaces, which link directly to the provider's orchestration layer. This middleware coordinates job scheduling, hardware calibration, and error mitigation while maintaining efficient communication between quantum and classical resources. Such integration ensures that quantum workloads are executed efficiently, reproducibly, and in synchrony with traditional computing systems.

Two algorithmic paradigms have proven particularly relevant within QCaaS environments. The first is Variational Quantum Algorithms (VQAs), which rely on iterative feedback loops between quantum hardware and classical optimisation routines. Representative examples include the Variational Quantum Eigensolver (VQE), used for molecular and materials modelling, and the QAOA, applied to combinatorial optimisation problems. The second paradigm involves quantum annealing and analogue computing, where quantum systems evolve continuously toward low-energy configurations that represent optimal or near-optimal solutions. This approach, implemented by platforms such as Qilimanjaro Quantum Tech and D-Wave Systems, is well suited to optimisation problems formulated as Quadratic Unconstrained Binary Optimisation (QUBO) models.

From an operational perspective, QCaaS platforms offer cloud-based portals and dashboards through which users can submit quantum jobs, monitor their execution, and retrieve results. These environments also support automated workflow integration, allowing hybrid tasks to be orchestrated across classical HPC resources and quantum backends. Users can begin development within simulators for cost-efficient prototyping and then migrate to real hardware for experimental validation. Major providers such as IBM Quantum, AWS Braket, Microsoft Azure Quantum, and Qilimanjaro Quantum Tech support these operations through tiered service models ranging from open research access to dedicated enterprise deployments with enhanced security and priority scheduling.

By offering on-demand access to quantum computation through a flexible and interoperable infrastructure, QCaaS enables organizations to accelerate innovation while managing cost and technical risk. It democratises access to quantum hardware, promotes integration with existing digital ecosystems, and provides a structured pathway toward quantum readiness. Through this model, industries can develop the expertise, tools, and hybrid workflows required to benefit from quantum-enhanced computation as the technology continues to mature toward large-scale, fault-tolerant operation.

Example – Azure Quantum:

One example of QCaaS is Microsoft's Azure Quantum platform. Azure Quantum is a full-stack cloud ecosystem that provides users with an environment to develop, test, and run quantum applications, while also seamlessly integrating with classical cloud resources (see overview in Figure 2). The platform can be understood in three layers:

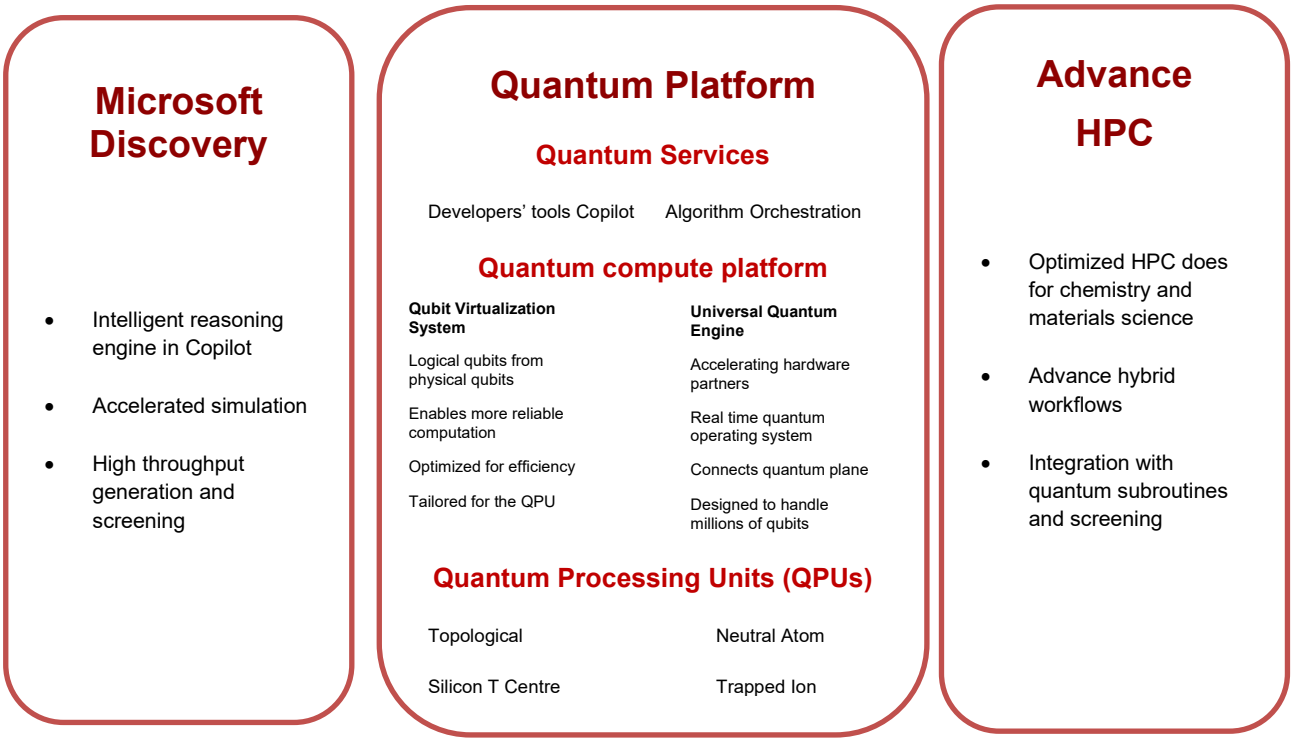


Figure 2**:** Overview on Azure Quantum platform

Quantum Services (Software Layer): This layer consists of developer tools, libraries, and cloud services such as Microsoft's QDK with the Q# language [10], Jupyter [11] integrations, and sample algorithms. Azure Quantum provides an AI-assisted Copilot for generating and optimizing quantum code, along with pre-built algorithms and optimization solvers. The orchestration service coordinates classical and quantum tasks; for instance, it may handle data pre-processing classically, perform core computations with a quantum solver, and finalize results classically. These processes are abstracted from the end user.

Quantum Compute Platform (Middleware Layer): Azure's middleware, including the Qubit Virtualisation System and Universal Quantum Engine, acts as a bridge between user software and hardware. The Qubit Virtualisation System manages error correction by mapping users' logical qubits to physical qubits on the QPU, using methods like error correction codes or dynamical decoupling. The Universal Quantum Engine functions as a quantum operating system, handling quantum operation timing, job distribution among QPUs, and integration with classical computing. This setup allows user code to automatically take advantage of hardware upgrades without modification.

Quantum Processing Units (Hardware Layer): Azure Quantum gives users access to various QPU types from multiple hardware partners through its portal. Options include ion-trap QPUs (IonQ, Quantinuum) with high fidelity but slower gates, superconducting QPUs with faster gates but shorter coherence times, and soon neutral atom QPUs (Atom Computing). Microsoft is also developing topological qubits and supports quantum annealers (D-Wave) for optimisation tasks. Azure Quantum's hardware-agnostic approach enables experimentation with different qubit technologies using the same SDK, letting teams match hardware type to problem—like choosing ion-trap

QPUs for error-correction accuracy or superconducting QPUs for machine learning speed.

Integrated Solution (Hybrid Capabilities): A key strength of of QCaaS offerings is integration with classical cloud services. Quantum jobs invariably need classical pre- and post-processing. Azure allows quantum jobs to directly pull data from Azure Storage or databases, and then write results back for analysis with Azure's AI or analytics tools. For example, if a telecom operator uses Azure Quantum to run a scheduling optimisation for network maintenance tasks, they might use Azure Functions to trigger that quantum job weekly, feed it data from an Azure Structured Query Language (SQL) database (with current network status), then have the results (optimal maintenance schedule) stored or sent to a visualisation dashboard. This hybrid approach is especially relevant in the NISQ era: often a quantum algorithm alone is not enough to solve the whole problem optimally, but when used as a subroutine it can accelerate a bottleneck. In practice, this might mean a classical simulation runs and whenever it hits a particularly hard part (like a combinatorial optimisation), it calls a quantum subroutine – all orchestrated by Azure's platform.

For telecom use cases specifically even without large-scale quantum hardware operational, Azure offers Quantum-Inspired Optimization (QIO) services accessible through the same Azure Quantum interface. These run on classical hardware but use algorithms inspired by quantum annealing to solve use cases such as tower placement or traffic routing problems more efficiently than standard solvers. This is a stepping stone – telecom operators can start by using quantum-inspired solvers (via QCaaS) and smoothly transition to actual quantum hardware as it becomes available and surpasses those solvers. Most operators have not yet chosen to take this step though, at the current technology readiness level.

Quantum Computing as a Telecom Service: Reference Case

Bizkaia's Quantum Strategy (BIQAIN**)** [12] aims to position the territory (located in the Basque Country, Spain) as an international reference in the development and deployment of quantum technologies, fostering strong public–private collaboration. Over recent years, a diverse ecosystem has taken shape, bringing together the Provincial Council of Bizkaia, companies of all sizes (from large enterprises to startups), technology centres, universities, industry clusters, and training institutions (see also Figure 3). All these actors share the common objective of driving innovation, sustainability, and technological sovereignty.

As a strategic technological partner of the Provincial Council of Bizkaia, Telefónica provides the ecosystem with both advanced tools and specialized talent.

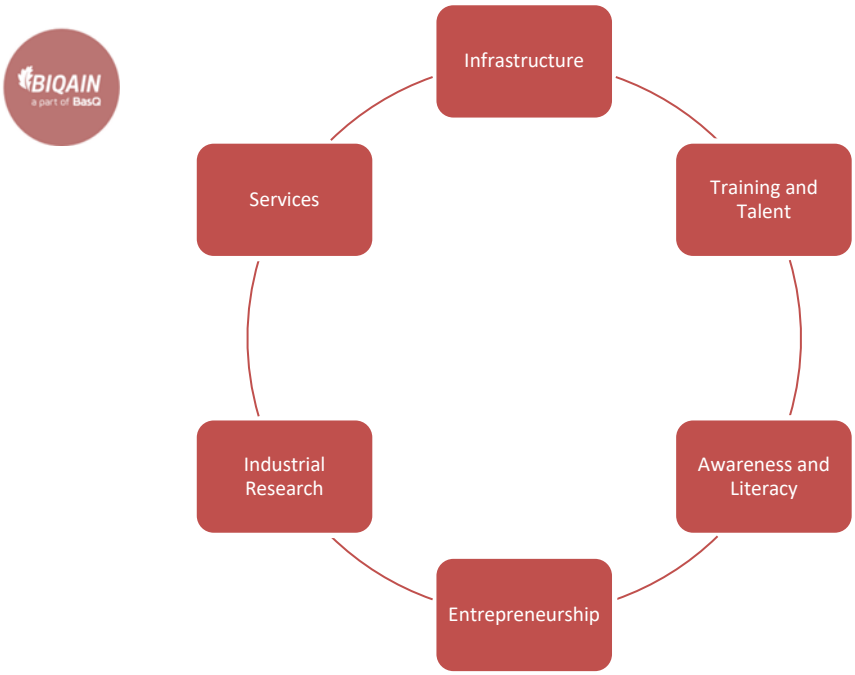


Figure 3: BIQAIN ecosystem

This integrated management approach enables Telefónica to simultaneously oversee the full set of available online emulators and quantum systems and the users who interact with them, providing differentiated services to the Provincial Council of Bizkaia, and with strong potential for organisations, clusters, universities, and other entities. Within this framework, Telefónica ensures controlled access and usage, budget monitoring, and the extraction of usage patterns that support informed, data-driven strategic decisions.

3.1.1.4 Status of the Technology

Current State (NISQ era): As of the end of 2025 / the beginning of 2026, quantum computing is in the NISQ phase. This means there exists quantum processors with tens to a few hundred physical qubits, but they are noisy (error-prone) and not yet error-corrected. The practical implication is that these NISQ processors can run only relatively short quantum programs before errors overwhelm the computation. Achieving a clear advantage for useful tasks is challenging under these constraints. For example, some companies are working on 127-qubit devices that can demonstrate certain research feats (like a random circuit sampling task), but for real-world problems, their results are often not better than classical methods as the problem size must be kept very small and/or error mitigation adds overhead. Researchers worldwide are using NISQ machines for experiments in chemistry, optimisation, etc., but with careful techniques to eke out results despite noise.

Progress toward Error Correction: The industry is heavily focused on overcoming these limitations through Quantum Error Correction (QEC). Error correction in quantum computers is far more complex than in classical ones, because measuring qubits (to check for errors) usually destroys their state. Nevertheless, there has been landmark progress recently. In 2023, for the first time, researchers achieved a scenario where a logical qubit (comprised of many physical qubits in an error-correcting code) had better fidelity than any single physical qubit – essentially demonstrating a net improvement by QEC. Some companies have reported incremental steps: e.g., repeating an algorithm with and without error-correction to show the error-corrected version lasts longer or is more reliable.

IBM for example has taken a phased approach towards fault tolerance. In recent years two general purpose error mitigation methods were developed and implemented: Zero Noise

Extrapolation (ZNE) [13] and Probabilistic Error Cancellation (PEC) [14] The ZNE method cancels subsequent orders of the noise affecting the expectation value of a noisy quantum circuit by extrapolating measurement outcomes at different noise strength. More recently, theoretical and experimental advances have shown that PEC can already enable noise-free estimators of quantum circuits on noisy quantum computers. Error correction requires an error correction decoder that can decode errors in real time. Earlier this year, RelayBP) was announced, a flexible, accurate, fast and compact decoding algorithm [15].

Microsoft and Atom Computing made headlines by announcing the world's first planned "Level-2" quantum computer, codenamed Magne [16], to be deployed at the QuNorth initiative in Europe. In Microsoft's terminology, a Level 2 quantum computer is one that incorporates true error correction and can sustain reliable quantum computations, paving the way for a practical quantum advantage on certain problems (Level 1 being the NISQ devices, and Level 3 being a large-scale fault-tolerant machine). The Magne system will use neutral atom qubits with Microsoft's error correction software. Neutral atoms (atoms trapped in an array by lasers) are a promising hardware platform: they can scale to hundreds or thousands of qubits relatively easily (several quantum computing hardware start-ups have shown 100+ atom arrays), and they have decent stability. By adding Microsoft's expertise in QEC, the goal is to have a mid-scale machine where maybe dozens of logical qubits are functioning. The press release in late 2025 touted this as *"the world's most powerful quantum computer"*, and importantly, an operational deployment – meaning it is not just a lab experiment, but will be running tasks for researchers and potentially external users in the next couple of years. This indicates that by ~2027, we could have a quantum computer that, for example, can run certain small algorithms consistently enough to beat a supercomputer at that task. It is a stepping stone, but a crucial one: the difference between an unreliable demonstration and a service one can rely on to get correct results even after many operations.

The notion of "levels" highlights that quantum computing hardware is on the cusp of transitioning from Level 1 to Level 2. Once a few logical qubits are operational, then deeper circuits (more operations in a row) can be run more reliably. This is when *practical* quantum advantage is expected to be demonstrated. There is optimism in the community that within the next 2-3 years there will exist a quantum computer that can solve a useful problem faster or better than a classical supercomputer – something often termed "Quantum Advantage" or "Quantum Supremacy 2.0" (since the first supremacy demonstration in 2019 was a contrived problem). Likely, domains for this milestone are specialised: quantum chemistry (where even a small advantage in simulating molecules is huge), or optimisation problems crafted to fit current hardware abilities. For instance, a Level-2 machine might be able to exactly simulate the behaviour of a small but industrially-relevant molecule (say, a catalyst with 50 electrons) that no classical computer can solve exactly.

Scalability and Roadmaps: Achieving fault-tolerant large-scale quantum computing hardware will require major scaling: on the order of thousands of logical qubits, which in turn might mean millions of physical qubits, if using standard error correction codes. Different qubit technologies have different roadmaps to get there. Superconducting qubits are doubling qubit counts nearly every year. Ion-trap systems are connecting multiple smaller processors with photonic links to scale up. Neutral atom systems aim to leverage 3D arrays and better lasers to control more atoms simultaneously. There is even a path via topological qubits (Microsoft's approach) which could drastically reduce the number of physical qubits needed by making them inherently more stable. Microsoft recently announced "Majorana 1", a prototype topological qubit processor, claiming progress toward that goal of a million-qubit machine on a chip.

The next few years (2025–2030) of quantum computing hardware development will likely be dominated by hybrid quantum-classical computing using small error-corrected quantum resources to do things classical computers cannot, primarily in niche areas. By the 2030s, if technology continues to mature, then general-purpose quantum computers, that change the game across many industries, including telecom, might exist. For now, any telecom company

exploring QCaaS must be mindful of NISQ limitations: algorithms must be noise-tolerant and small-scale.

Example – Status in Telecom Context: Today, a telecom might use a 100-qubit QCaaS offering to run a toy optimisation of, say, 10 cell towers. In a couple of years, that same telco could potentially use a 1000-qubit error-corrected machine to optimise 100 towers or a whole city's network configuration, achieving a result better than any classical algorithm and saving cost or improving performance. If there comes a time there exists quantum computers with millions of qubits, telecoms may use quantum computing for things like real-time network control, AI for signal processing, or even to power customer-facing applications (Augmented Reality and Virtual Reality (AR/VR) or advanced encryption schemes).As of today, classical computing is still better in all, use cases right now, but it is possible that the first use cases with quantum advantage might appear as soon as in 3-5 years.

3.1.1.5 Challenges

Despite recent progress of quantum computing, the technology faces significant challenges on the road to wider adoption, especially in an industry as practical and reliability-focused as telecommunications. These challenges span hardware performance, algorithmic development, interoperability, and user adoption, and they collectively define the pace at which quantum computing can transition from experimental research to commercial applications.

Some of the key hurdles include:

- **Hardware Fragility and Scalability:** Current quantum devices are extremely sensitive to environmental disturbances, which lead to loss of quantum information over time, such as stray electromagnetic fields, vibrations, or imperfect control pulses. Superconducting qubits require ultra-cold temperatures and still typically maintain coherence for only microseconds; ion-traps need ultra-high vacuum and delicate laser tuning. Building and operating these systems at scale presents significant engineering challenges. Scaling from 50 to 500 to 5,000 qubits, whilst maintaining qubit stability and entanglement is exponentially harder. The challenge is not only technical but also architectural, requiring innovations in cryogenics, control electronics, and manufacturing. Moreover, each additional qubit introduces more points of potential failure, and scaling often introduces noise faster than linear (crosstalk between qubits, heating issues, etc.). In short, quantum hardware is still "beta technology" – impressive in labs, but not yet robust like classical chips.

- **Error Correction Overhead:** As discussed, error correction is the way out of fragility, but it comes at a steep price: overhead. The leading QEC codes might need 50-100 physical qubits to encode a single logical qubit that is reliable. This overhead means that to do anything significant (requiring, say, 100 logical qubits), one might need on the order of 10,000 physical qubits. No quantum computing hardware vendors have that many yet (the best devices are ~100 qubits). Even with projected growth, we might not see 10,000 physical qubits until later in the decade, unless a breakthrough reduces overhead or a more qubit-efficient error correction method is found. This is why some experts say truly fault-tolerant quantum computing is still potentially a decade away. There is also a runtime overhead: error correction entails constantly checking and correcting errors (through complex multi-qubit operations), which can slow down computations and demands extremely fast classical co-processors to manage the error correction loop in real time. Facing quantum computation from the analogue paradigm escapes the need for logical qubits as the continuous evolution of Hamiltonians reduces the noise coming from chip operation.

- **Algorithm and Software Readiness:** On the software side, the field of quantum algorithms is still maturing. A small number of established algorithms exists, such as Shor's algorithm for factoring, along with several quantum heuristics including QAOA for optimisation, and variational circuits for chemistry. However, for many telecom-specific problems, algorithms remain in the research stage. It is not yet clear, for instance, which quantum algorithm is the best suited to maximise 5G network throughput; current efforts are largely focussed on mapping such problems to existing quantum optimisation or Quantum Machine Learning (QML) approaches, but substantial R&D is still required. Additionally, quantum programming expertise is scarce. The skills required (quantum physics, linear algebra, probabilistic thinking) are specialised. Whilst development tools such as QiliSDK [6] or Q# help [10] , the talent gap means telecom companies might struggle to find or train people who can take a network engineering problem and implement it on a quantum computer. Over time, as curricula incorporate quantum computing and more engineers cross-train, this will likely improve.

- **Integration into Existing Systems:** Telecom networks are vast, complex systems with high reliability requirements. Introducing QCaaS means dealing with issues of integration: latency, data transfer, security, and compatibility. For example, if a quantum optimiser takes 60 seconds to return an answer, can the network wait that long for a reconfiguration decision? In some cases, the answer is yes (offline planning tools), but, in others, no (real-time control loops). Hence, figuring out *where quantum fits* in operational workflows is a challenge. This may require redesigning some processes to be more batch or asynchronous to accommodate a quantum call. There is also the challenge of trust and verification – how does one verify the solution given by a quantum computer is correct or optimal? With classical algorithms, engineers have decades of experience; with quantum, it might sometimes output an answer that is hard to classically verify. Tools and methods for testing quantum outputs (perhaps smaller sanity-check problems or new theoretical guarantees) need to develop.

- **Cost and Accessibility:** Currently, using QCaaS can be expensive; quantum hardware is scarce and each operation require investment. Running a complex algorithm might require thousands of shots to get a reliable distribution of results, which could run up costs. For a telecom use case, one must evaluate if the benefit (e.g., a slightly more optimal solution) justifies the compute cost compared to classical. In many cases today, classical computing is so cheap (cloud CPU/GPU time) compared to quantum, that quantum would need to deliver a *substantial* improvement to be cost-effective.

- **Regulatory and Security Concerns:** For telecom, any new technology integrated into networks raises questions of reliability and security. If a quantum computer is used to help manage network resources, there will be regulatory scrutiny (e.g. does it meet the reliability standards? Is there a fallback if the quantum service is down?). Moreover, sending sensitive network data to a cloud quantum service must be done securely. QCaaS runs through the (classical) internet, and so one must ensure that the connection is secure (which currently relies on classical encryption, soon to be upgraded to PQC). Some telecom operators might be hesitant to rely on an external quantum service for critical operations without strong Service Level Agreements (SLAs) and perhaps on-premises options in the future.

- **Scarcity of Skilled Professionals:** The multidisciplinary nature of quantum computing requires knowledge of mathematics, physics, algorithm design, and software development, which remains a rare combination in the current workforce. This talent gap slows the pace of adoption and limits the ability of enterprises to integrate quantum approaches into their digital transformation strategies. This lack of

professionals is accentuated in hardware vendor companies, due to the absence of practical training in quantum hardware at graduate or master levels.

In summary, quantum computing today is promising but not production-ready for most telecom needs. Telecom leaders need to be aware of these challenges to set realistic expectations. This involves strategic planning: investing in R&D, securing incremental gains (such as a quantum-inspired optimisation delivering), while clearly communicating internally that transformative outcomes (i.e., real-time quantum network control or quantum-secure end-to-end encryption) remain several years away. The good news is each challenge is actively being worked on by a growing global quantum tech community, and the progress is steady.

3.1.1.6 Opportunities in Telecom

For all the challenges, the potential opportunities of quantum computing in telecom are potentially enormous. As the technology matures, it could unlock capabilities and efficiencies that are unattainable with classical computing alone. Here are several key opportunity areas:

- **Unprecedented Optimisation Power:** Telecommunications is rife with complex optimisation problems – from network design (laying fibre, placing towers) to real-time resource allocation (scheduling channel usage, routing packets) – many of which are NP-hard, and only approximated today. Quantum computers, including analogue quantum computers, quantum annealers and gate-model machines running algorithms like QAOA or Grover-based searches, offer a chance to find better solutions to these problems. For example, quantum optimisation might reduce the total length of fibre needed in a network plan by finding more efficient routes, or improve cell-edge performance in a wireless network by optimising antenna parameters and scheduling more effectively than current heuristics. Even a small percentage improvement can save millions for large telecom operators or allow them to serve more customers with the same infrastructure. Early studies (and some pilot projects) have shown encouraging results: a quantum-inspired algorithm improved 4G/5G network, and another quantum trial has increased the gains at cell edges by better scheduling of radio resources. As quantum hardware grows, these optimisations could go from pilot to production, with QCaaS optimisers running nightly or in real-time to continuously fine-tune networks for maximum efficiency.

- **Boosting the Classical Computing Capabilities:** Quantum computing offers a significant opportunity to enhance classical computing capabilities within the telecommunications sector through hybrid quantum–classical integration. Quantum processors are not expected to replace traditional HPC systems; instead, they will operate as accelerators for specific workloads where quantum mechanics can provide computational advantages. Telecommunications networks involve inherently complex decision spaces, and several operational tasks could benefit from quantum-enabled acceleration. Spectrum allocation, interference mitigation, radio resource management, beamforming optimisation, core network routing, and scheduling in highly dynamic environments all require exploration of large combinatorial solution spaces under tight timing constraints. Quantum subroutines embedded within hybrid workflows may, in the future, allow these problems to be addressed more efficiently than with classical methods alone. Hybrid QCaaS platforms also enable the integration of quantum-inspired approaches into network digital twins, predictive network analytics, and Self-Optimizing Networks (SON), supporting more adaptive and energy-efficient architectures. Beyond immediate computational gains, QCaaS provides a strategic opportunity for research and innovation in telecommunications. Access to quantum simulators and early-stage processors allows engineers and researchers to

prototype quantum optimisation and QML models tailored to telecom use cases, investigate new algorithmic formulations, and evaluate quantum-enhanced strategies for network performance, security, and orchestration. As quantum hardware evolves toward higher fidelity and eventually fault-tolerant operation, the techniques and competencies developed today will position the telecommunications sector to leverage quantum acceleration effectively and at scale.

- **New Cryptographic Paradigms (Quantum-Safe and Quantum-Based Security):** On one hand, there is the need to upgrade security to be quantum-safe, but on the other hand, quantum computing also enables new forms of cryptography and security protocols. The eventual ability of quantum computers to solve certain mathematical problems could allow interesting possibilities like homomorphic encryption schemes becoming more usable (quantum can handle the heavy maths to decrypt or transform data without revealing it), thus enabling enhanced privacy in data handling. The broad opportunity is that telecom operators can both secure themselves and become providers of quantum-based security solutions in a world increasingly conscious of cyber threats.

- **New Services and Revenue Streams:** Embracing quantum can enable telecoms to move up the value chain. For instance, a telecom company could evolve to also be a quantum cloud provider. In fact, first operators like China Telecom [17] or Telefónica (see section 3.1.1.3) are already doing this. Telecoms already have distributed data centres, a customer base, and network expertise. Initial QCaaS is also offered by tech companies. One can envision telecoms partnering to host quantum nodes at edge data centres for low-latency access. Telecoms could also offer quantum consulting and integration services: advising businesses in their region on how to leverage QCaaS, much like some telecom operators today consult on IoT or AI solutions beyond just connectivity. This is an opportunity for brand differentiation and early mover advantage – being the “quantum-ready telecom operator” could attract lucrative partnerships with industries like finance or defence that are also exploring quantum.

- **Scientific and R&D Leadership:** Lastly, being involved in quantum computing offers telecoms a chance to contribute to and benefit from cutting-edge research. Telecom has deep expertise in areas like signal processing, information theory, and network science, all of which have analogues in quantum (quantum error correction codes borrow concepts from classical error-correcting codes, quantum networks parallel classical ones). By participating in research (some telecoms are funding quantum computing chairs or research projects, they can influence the development of quantum tech to better suit network needs. This could lead to tailor-made algorithms (perhaps a specific quantum algorithm for routing, that a telecom helped invent, becomes a standard) or early access to breakthroughs (a telecom that helped test a quantum networking technology could adopt it earlier than competitors).

In essence, the opportunities span internal gains (efficiency, cost savings, better services) and external offerings (new products, security guarantees, cutting-edge services).

To put a concrete example: Today at telecom operator might struggle to reduce dropped calls at cell edges because of interference and scheduling issues. In a few years, that telecom operator could use a quantum-enhanced scheduler (running via QCaaS overnight to update scheduling policies or as a real-time aide in the Radio Access Network (RAN) software) to cut interference and boost cell-edge throughput by a few percent, translating to a noticeable reliability improvement for customers. At the same time, the telecom operator could assure enterprise clients that all their critical traffic is secured with quantum-proof encryption *and* optionally QKD. And as quantum computing helps discover new materials, perhaps new battery tech extends device battery life, indirectly benefiting mobile users (this is speculative, but shows the broad ripple effects).

3.1.1.7 GSMA Role

The GSMA is a key industry body that is proactively guiding the telecom sector's approach to quantum computing and quantum security. Recognising both the challenge and the opportunity of quantum technologies, the GSMA has taken on several roles:

- **Defining Telecom Use Cases and Driving Trials:** Beyond security, GSMA has interest groups (like the GSMA QNS Group under its umbrella) looking at broader quantum computing use cases in telecom. GSMA has facilitated workshops on quantum computing for network optimisation, and shared insights on early trials to produce use case whitepapers. This shows GSMA's role in knowledge dissemination: publishing papers and hosting webinars to educate its members about quantum computing, demystifying the technology and providing a realistic outlook (what to do now vs later). By doing so, GSMA helps telecom operators identify where to invest R&D effort. For example, the taskforce suggested focusing on "hybrid quantum optimisation for planning and operations" as a near-term win (treating quantum as an optimiser, not a magic speedup) – essentially advising that telecoms try applying QCaaS to planning problems now. This kind of guidance prevents disillusionment and prevents missed opportunities.

- **Ecosystem Building and External Partnerships:** GSMA often works beyond the telecom industry, bringing in quantum technology firms (like IBM in the taskforce, or smaller startups via its forums) and aligning with broader efforts. GSMA coordinates with entities like the European Telecommunication Standards Institute (ETSI) Quantum-Safe group and the International Telecom Union (ITU) on quantum network standards. GSMA also keeps telecoms connected to academia and national labs exploring quantum technologies, ensuring that when breakthroughs happen, telecoms can adopt them quickly by virtue of being involved early. Essentially, GSMA acts as an innovation hub for quantum in telecom, so that telecom operators don't innovate in isolation.

In summary, the GSMA's role is part evangelist, part coordinator, part standard-bearer. They help telecom companies get quantum-ready. Regarding quantum computing, this means ensuring the industry does not fall behind other sectors in leveraging quantum advancements – by sharing knowledge of use cases and even collectively bargaining with QCaaS providers for features needed by telecoms (for instance, requesting certain optimisation features or supporting particular QoS requirements on quantum jobs). GSMA frame quantum computing as a positive force if harnessed: something that can ultimately help automate and enhance networks. By tackling the risk (quantum threats) and nurturing the opportunity (quantum solutions) through a collaborative industry approach, GSMA is effectively steering the telecom community through this technological inflection point.

3.1.2 Quantum Computing for Telecom Optimization

Quantum computing has the potential to generate value across a variety of use cases in many industries beyond telecom, such as include pharmaceutical, logistics, technology, and government [18,19]. The complexity of telecommunication networks has significantly increased over the past decade due to the integration of compute-intensive workloads and AI-native architectures. Quantum computing provides a paradigm to tackle this complexity. Prior to exploring these possibilities, it is crucial to recognise that existing deployed networks already utilise numerous heuristic algorithms, such as routing protocols, which have been optimised (classically) over many years. This factor plays a vital role when considering

performance KPI improvements through the adoption and integration of new technologies like quantum computing.

There are three distinct strategies for adopting and integrating quantum computing into telecommunication networks: first, using stand-alone or centralised cloud-based quantum processors dedicated to specific tasks like optimisation; second, implementing distributed in-network quantum computing to manage particular telecom workloads; and third, deploying hybrid classical-quantum data centers, featuring quantum islands within a predominantly classical computing environment. The last one uses quantum processors as a co-processor.

To enable the execution of telecom-grade quantum algorithms, Ericsson envisions the deployment of quantum computers as co-processors in a cloud-native manner, as shown in Figure 4.

Each of these quantum computers could comprise multichip QPUs, where information flows between them via a quantum communication channel, thereby delivering improved computational fidelity compared with single-chip quantum processors. On top of these QPUs sits a stack that could be tailored to the transactional, distributed, and online nature of data processing required in many telecom workflows. The stack integrates with classical compute for telecom to enable ultra-reliable, low-latency execution of certain workflows in the different Radio Access (RA) planes where individual subroutines can benefit from quantum algorithms. Beyond this, it could establish interconnects between different devices to enable high-throughput information and secure information exchange.

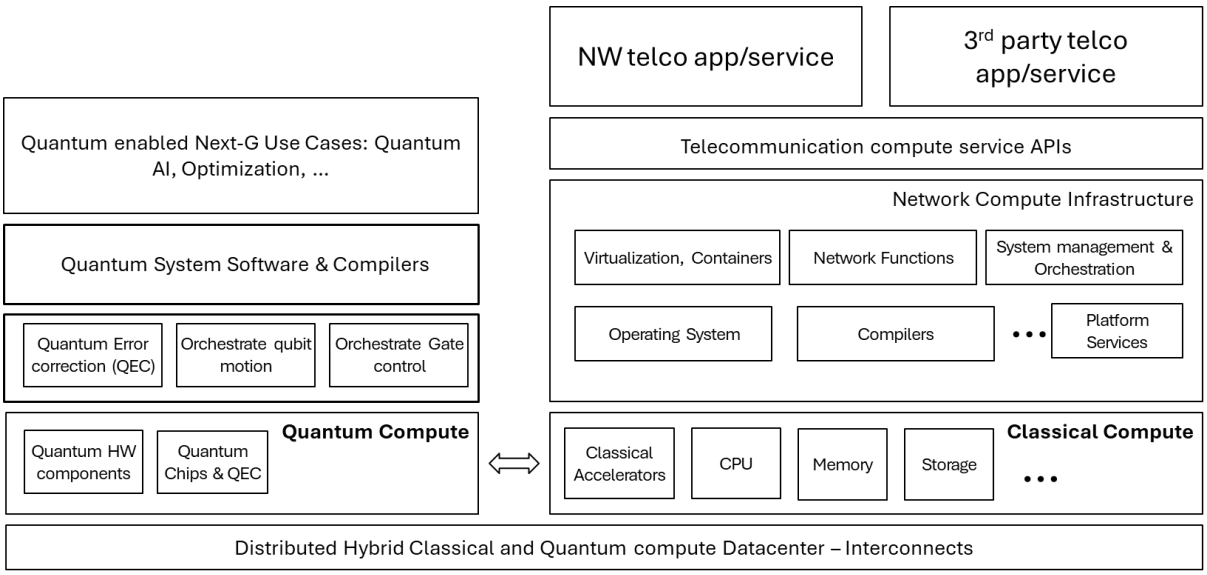


Figure 4**:** Ericsson Hybrid Architecture Overview (Quantum and classical telecom computing stack)

At the algorithm layer, hybrid quantum-classical workflows in telecom could utilise quantum subroutines for certain tasks such as optimisation and machine learning. Examples of these tasks can include but are not limited to RAN antenna-tilt optimisation which improves network performance by balancing capacity, quality, and coverage, traditionally addressed using reinforcement learning with Deep Q-networks (DQN). This is covered further in following sections.

Another example for quantum computing applied to optimisation is from Orange in France, in which Orange launched a quantum computing research initiative to optimise network operations [20]. More broadly, there is a European Consortium dealing with operational research (including optimisation), with Orange involvement [21].

3.1.2.1 Description

In classical computing, the fundamental unit is a classical bit which can take 0 and 1 as states. By contrast, quantum bits (qubits), have several intriguing additional possibilities, enabling new ways for computation:

- **Superposition**: qubits can exist in a state that is a probabilistic combination of both states. Calculations can be performed on a superposition of states using quantum gates.

- **Entanglement**: Qubits can be entangled, meaning the state of one qubit can depend on the state of another, no matter how far apart they are.

The net result of the special properties of quantum spaces is that certain algorithms can traverse a path towards a classical solution by moving through a quantum space in a way that is not possible classically.

3.1.2.2 Use Case / Problem Statement

From the perspective of a telecom operator, there are numerous areas where quantum computing could be beneficial.

Optimization (E.g., Quantum annealing)	**Deep Learning** (E.g., Classification, regression)	**AI Model Simplification**
Network designed optimization, e.g., tower placement, routing, capacity	**Network operation:** e.g., predictive maintenance and repair	**Process efficiency**, e.g., internal chatbot for employees
Subscriber Acquisition Cost and Subscriber Retention Cost (SAC/SRC) optimization through 1:1 segmentation and affinity scoring	**Customer value management**, e.g. improved upscale/x-sell rates	**Content generation**, e.g., targeted message in customize style/tone
Fault detection and recovery including automatic detection and re-routing	**Churn prediction**, e.g., proactive contacting of dissatisfied user	**Customer service chatbot,** e.g., troubleshooting, voice assistant
Energy efficiency, e.g., self-generated vs purchased electricity	**Fraud detection,** e.g., device subsidy fraud, premium calls…	**Call transcription and analysis** for customer experience improvement
Singularity *Quantum Algorithms* / *Quantum-inspired algorithms*		**CompactifAI** *Compressor of large models*

Table 5: Overview on telecom optimization use cases (adopted from Multiverse Computing)

Table 5 gives an overview on quantum annealing, deep-learning and quantum inspired use cases in the telecom context.

Additionally, the following use cases are apply to telecoms:

- **Antenna placement:** Quantum computers could be used for several antenna placement problems, as they can be used to resolve maximum independent set problems (Analogue Hamiltonian Simulation (AHS)) [22],

- **Physical Cell ID / Root Sequence Index (PCI/RSI) planning:** 4G/5G requires to every cell to have an ID to identify it, in which neighbouring cells must have unique IDs. -Optimising for this over an entire network is an interesting optimisation problem which is also described in an earlier whitepaper published by the GSMA [1]

- **Spectrum optimization** in optical networks using gate-based quantum computing [23].

- **Routing optimization** i.e. steering the network traffic in a way that there is no congestion.

- **RAN tilting**

- **Fibre placement**

- **End-to-End Local Commercial and Network Optimisation**

- **Quantum Machine Learning for Churn Prediction and Personalised Customer Management**

- **Optimisation in 6G and beyond networks**

We address some of these use cases in further detail below.

Routing Optimisation:

Increasing mobile traffic and climbing infrastructure costs and complexity put telecom operators in a difficult position. To deliver the best possible service, the current network must not be in an overloaded state. Telecom operators have two broad paths forward: the first is upgrading the current network infrastructure (which is costly and time-intensive), and the second option is finding a more optimal configuration for routing mobile traffic in existing infrastructure (which can mean that overloading and poor network performance can be avoided in many cases).

However, such routing optimisation requires detailed information on the network and routing logic. Telefonica Germany approaches this challenge with a near real-time digital twin of their mobile network infrastructure, containing active device as well as routing information. This unique combination allows network engineers a unique view on their physical and logical network at the same time and opens possibilities to simulate changes to the infrastructure and routing logic. Since current routing configurations are decided based on best knowledge by a skilled network engineer, these configurations are often functional, but far from the best possible configuration.

Having the required information digitally available enables the exploration of exhaustive search approaches, however, given the sheer size of the network, these enumeration methods quickly reach their limitations. Even a small subnetwork of 17 source and 5 potential target nodes leads to a total of $5^{17} \approx 800$bn possible routing combinations. At 1 ms per evaluation,

the deterministic optimisation would take ~24 years. Hence, it is evident that expanding such an approach to the full network with more than 8,000 nodes is simply infeasible.

Alternatively, one can take a heuristic approach, such as simulated annealing to find a better configuration of the network. Such optimisation methods usually allow finding better configurations than human-induced routing. However, these heuristic methods give no information on whether the result is the actual best configuration or if there is room for improvement.

This leads to the exploration by Telefonica Germany of harnessing the potential of quantum technology to optimise the network. Together with Sopra Steria, Telefonica Germany implemented a PoC in which they ran a PoC on Azure Quantum's QIO simulator to optimise the network configuration. Once quantum computing solutions reach their full potential, they can handle full network configurations, resulting in the best configuration with up to an exponential speed-up compared to deterministic methods. Based on roadmap projections, fault-tolerant quantum hardware after 2030 could handle ≥8,000 nodes. In a constantly changing network, this approach allows Telefonica to keep the configurations updated in order to optimise network performance.

RAN Tilting:

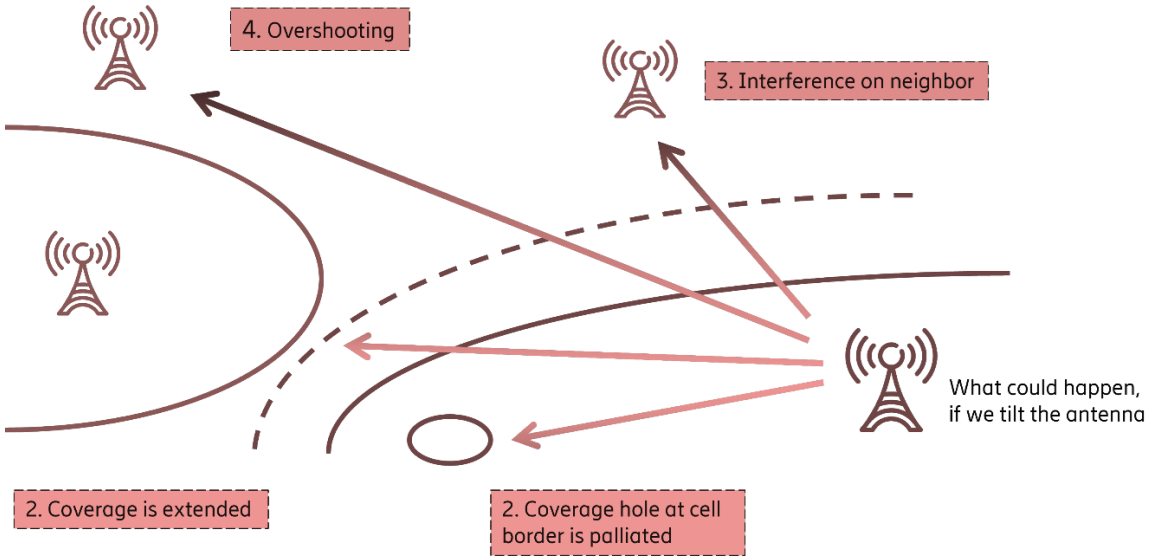


Figure 5: RAN antenna tilt problem view

Antenna tilting involves adjusting the vertical angle of cellular antennas to optimise their coverage area, balancing capacity, quality, and coverage. Improper tilting can either cause coverage gaps or interference with neighbouring cells, affecting network performance. Traditionally, this optimisation has been tackled using classical techniques such as reinforcement learning with Deep Q-networks (DQN).

Ericsson have explored using Quantum Neural Networks (QNNs) for antenna tilt optimisation. This method is based on a QNN trained via supervised learning, utilising an experience replay buffer to predict rewards based on network KPIs and actions. By employing a single expressive ansatz layer on 7 qubits, the QNN achieves comparable prediction accuracy to classical models while using ten times fewer trainable parameters. *Although the current quantum hardware inference is slower than classical methods, moderate entanglement among qubits enables compensation for reduced training data, allowing smaller replay buffers and potentially faster convergence. Challenges such as vanishing gradients persist when training deeper QNNs.*

This research demonstrates a successful proof-of-concept, indicating that quantum machine learning can effectively address complex telecommunications problems. As quantum technology advances, it offers the promise of faster, more accurate, and resource-efficient network optimisation compared to conventional approaches.

Fibre Placement:

Fibre placement in telecommunications networks is a complex optimisation problem involving cost-benefit trade-offs across geographic, economic, and regulatory dimensions. Traditional methods rely on Integer Linear Programming (ILP) and heuristic solvers, which struggle with scalability and approximation guarantees. Quantum computing offers a promising alternative for tackling such NP-hard problems.

Vodafone Group collaborated with ORCA Computing to explore quantum optimisation using Bosonic sampling devices, focussing on modelling fibre layout as a variant of the Steiner Tree Problem. The Steiner Tree Problem seeks a minimum-cost tree that connects a subset of terminal nodes in a graph, potentially using additional non-terminal nodes to reduce overall OpEx and CapEx incurred as a result of deployment (i.e., labour, maintenance, etc.). The optimisation goal is to maximise network coverage and benefit while minimising deployment cost; this formulation is well-suited for quantum optimisation due to its combinatorial complexity. Specifically, in the context of fibre placement, Vodafone depicted the network as a graph with weights on nodes and edges. The weights on nodes are modelled as benefits, and represent the potential strategic/economic value of connecting that node to the network. Whereas weights on edges are modelled as optimisation costs, which can represent OpEx/CapEx associated with engineering and regulatory constraints around physical installation of the fibres. For example:

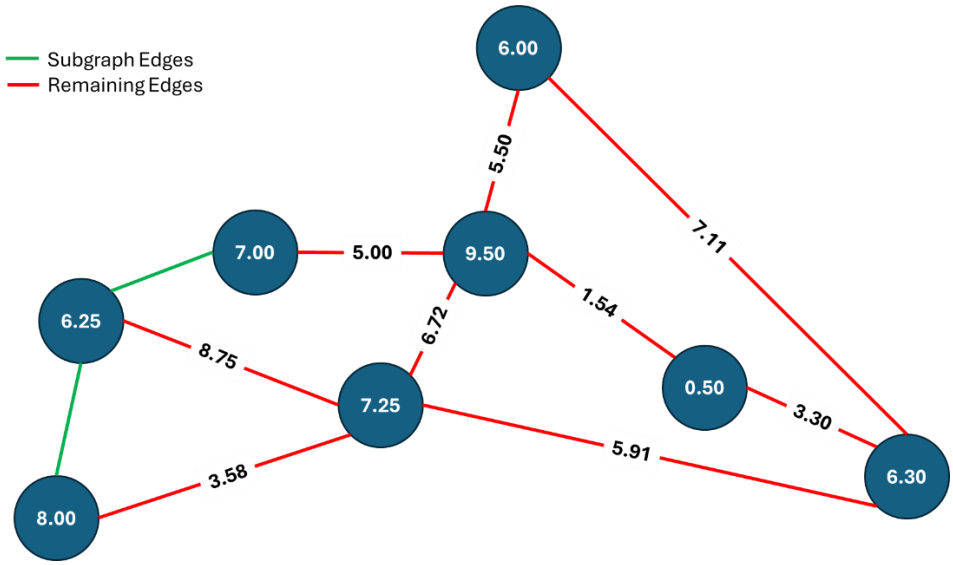


Figure 6: Network Cost Node representation

In this network, three nodes are already connected, as depicted by the green “subgraph edges”. The aim here is to add fibres into the network (represented as edges) such that there is a path of connectivity to all nodes, but not requiring that all nodes are connected (as in a mesh network). Optimisation of the above network on ORCA Computing’s PT-2 Series photonic quantum computing gave the following result:

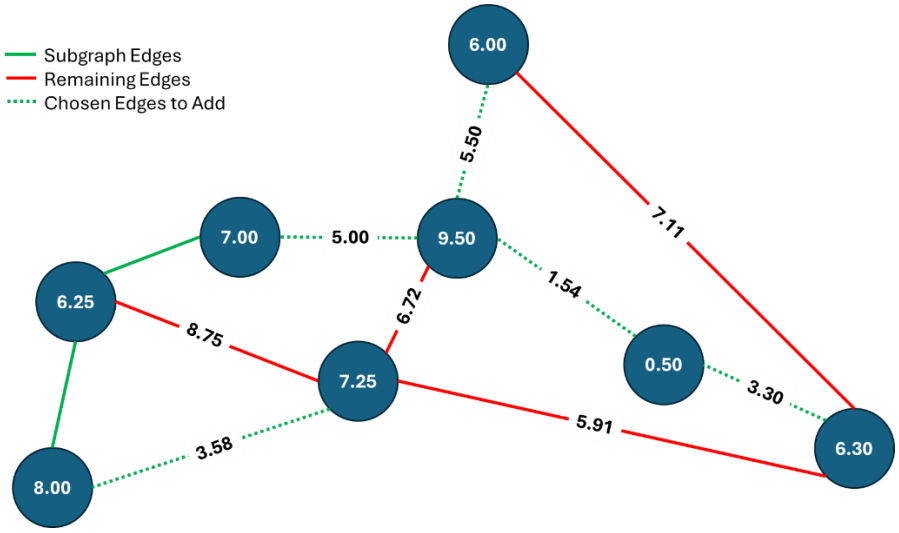


Figure 7: Network Cost Node Quantum Computing Optimisation

The fibres which have been selected to be installed to connect network nodes are now depicted by green dotted lines ("chosen edges to add").

Whilst it is useful to model a network as per this example, it is evident that telecom networks are vastly more complex, containing many more nodes – current quantum computing hardware supports limited qubit counts which restricts the size of the problem (network) which can be modelled. Moreover, denoting the weighting values is a complex problem as this requires detailed geographic and economic data for accurate modelling, which remains a mostly manual job. Nevertheless, this demonstrates the viability of quantum computing for fibre placement optimisation. While current hardware limits scalability, the foundational work in algorithm development, problem modelling, and hybrid strategies lays the groundwork for future breakthroughs.

End-to-End Local Commercial and Network Optimisation (Annealing):

Many of today's telecom operators are still siloed into functions like network operations, sales and marketing, customer operations and distribution/sales. Quantum annealing enables telecom operators to create an optimisation layer, transcending those siloes, offering the capability to optimise decisions across both network and commercial domains.

Traditional function-specific tools (e.g., network planning) struggle to integrate constraints that telecom operators cannot fully control but are impacting the local commercial landscape. These include shared/leased towers, micro-sites, shared fibre, municipal access rights, wholesale dependencies, third party backhaul and competition from city owned networks or local broadband providers, all of which are mapped onto different local purchasing power and population density values.

All these local constraints form boundary conditions in a vast optimisation space. Quantum annealers can encode those directly into the model and find optima for larger and more complex conditions than traditional (mostly siloed) tools. This allows telecom operators to optimise local contribution margins of each neighbourhood or micro market with greater precision than today.

The result is a new, highly dynamic decision space in which Capital Expenditure (CapEx), OpEx, micro-targeting and bundling are optimised jointly rather than in isolation. Telecom operators can identify the best sequence of actions for each micro-market automatically and improve both resource allocation and profitability across their footprint.

Quantum Machine Learning for Churn Prediction and Personalised Customer Management:

Gate based quantum computing, although still emerging, has the potential to offer the ability to solve computational challenges beyond today's largest AI models; among the most pressing ones for telecoms are granular customer insight and retention strategies. Classical churn models often fail to capture behavioural nuances across usage patterns, contract structures, network experience, device cycles and support interactions.

Once enabled, quantum machine learning can represent this complexity in much larger feature spaces. This allows telecom operators to detect the tipping points at which the probability of cancellation increases, revealing subtle behavioural patterns and potential remedial actions—from new device offerings to personalised streaming bundles to enhanced in-home signal—that remain undetected by classical analytics.

Quantum enhanced generative models can then shape a personalised retention message and select the channel that is most likely to resonate, such as mobile app, short message, electronic mail or even a physical letter. The outcome is a shift from reactive churn mitigation toward predictive and highly personalised churn prevention, supported by models capable of capturing more complex facets of customer behaviour.

Optimisation in Future 6G-and-Beyond Networks:

Recent research by Telefónica investigated the role of quantum computing for optimisation of 6G-and-beyond networks, finding that quantum annealing and quantum reinforcement learning can be used to address the complex, large-scale graph-centric optimisation problems in such networks. This includes cellular RAN deployment, user-centric mobility management, and virtual network function scheduling. This research, however, found that quantum computing is still facing challenges related to algorithm development, hardware scalability, and architectural integration for practical deployment [24]. At the time of writing, 3GPP in development toward 6G has not taken quantum computing technology into consideration for 6G standards.

3.1.2.3 Solution

Quantum computing for telecom optimisation use cases is still in the PoC/development stage. Industry agnostic turn-key QCaaS is available and detailed in the previous section, but turn-key solutions for telecom specific optimisation problems have yet to emerge.

3.1.2.4 Status of the Technology

Quantum computing is still in a very early maturity stage. There are already prototypes for research & development purposes available, for example on hyper-scaler platforms or via dedicated cloud access (see chapter 3.1.1 Quantum-Computing-as-a-Service (QCaaS)). However, logical qubit numbers must increase significantly until a broader application in production-relevant use cases is possible. While there have been isolated claims of quantum advantage for selected problems, these have typically been disputed shortly afterwards. Nevertheless, there are an increasing number of publications and announcements reporting significant advancements [25, 26] making it credible that more powerful quantum computers capable of addressing relevant use cases could be available within 3-5 years.

Due to the current limitations of quantum hardware, current state-of-the-art approaches tend to use quantum algorithms as subroutines to improve and/or accelerate classical optimisation workflows. In particular, recent research from Qilimanjaro exemplifies how to refine hybrid algorithms for classical optimization tasks [27]. This work demonstrates how variational quantum algorithms can be used in combination with tensor network techniques to solve larger-scale optimisation tasks, maximising the impact of the quantum subroutine while minimising the amount of resources required.

3.1.2.5 Challenges

As quantum computing is still an emerging field, there are numerous challenges for applying it for telecom optimisation purposes. Most notably, the availability of logical qubits still needs to increase significantly, i.e. the evolution from NISQ to the era of fault-tolerant quantum computing must happen before more complex telecom problems of real relevance can be tackled. Also, although first use cases are visible, off-the-shelf solutions, tailored to specific needs of a telecom operator, are not yet available and are essential for a broader adoption. A further challenge to adoption is that quantum computing requires new skills, which, in many cases, are not yet available to a sufficient extent in the workforce of telecom organisations.

3.1.2.6 Opportunities

As the field evolves from NISQ towards fault-tolerant quantum computing, telecom optimisation can benefit from a staged adoption of quantum methods, starting with hybrid workflows and progressing to algorithms with fundamentally stronger asymptotic advantages. In this context, different quantum paradigms offer distinct value profiles and time horizons, across use cases such as RAN parameter tuning and scheduling, network planning and rollout, transport routing/traffic engineering, spectrum and interference coordination, and energy-aware network operation.

- **Quantum Annealing for Near-Term Hybrid Optimisation:** Quantum annealing can be integrated as a heuristic subroutine within classical optimisation pipelines for problems such as cell clustering, radio resource scheduling, traffic engineering / path selection, or maintenance and rollout sequencing. In the short term, refined techniques (e.g., catalysts and counter-diabatic driving) may improve solution quality and robustness for relevant combinatorial structures, even if the long-term asymptotic impact is more limited than fully error-corrected approaches.

- **Decoded Quantum Interferometry for Long-Term Exponential Impact:** Decoded Quantum Interferometry (DQI) represents a pathway to exponential advantage on selected structured optimisation classes in the fault-tolerant era, making it a strong candidate for transformative performance once logical-qubit scale and error correction overheads become favourable. This is particularly applicable for large-scale instances arising in joint planning under constraints, multi-domain resource allocation, and end-to-end optimisation across RAN, transport and core.

- **Multi-Modal and Digital–Analogue Platforms to Bridge Capability Gaps:** Platforms that combine digital circuits with analogue primitives (or digital–analogue hybrids) can offer a pragmatic route to stronger performance earlier by matching algorithmic components to the most resource-efficient execution mode. This enables better trade-offs between depth, noise, and problem size in workflows like digital-twin-driven planning, near-real-time reconfiguration, and multi-objective optimisation (QoS, cost, energy, resilience).

- **Hybrid Algorithm Design as a Durable Capability:** Independently of hardware timelines, developing decompositions (in which quantum subroutines accelerate the hardest bottlenecks, whilst classical solvers handle the remainder) creates a “quantum-ready” optimisation stack that can scale with improving qubit counts and fidelities, for recurring telecom workloads such as daily planning cycles, automated troubleshooting, and continuous energy optimisation.

3.1.2.7 GSMA Role

The GSMA can play a pivotal role in advancing quantum computing within the telecommunications industry by fostering collaboration among key stakeholders, including telecom operators, technology providers, and regulatory bodies. By promoting research,

standardisation, and the sharing of best practices, the GSMA can aim to accelerate the integration of quantum technologies into telecom networks. Furthermore, the GSMA could actively support initiatives that address the challenges associated with quantum computing, such as enhancing qubit numbers and improving software solutions, thereby paving the way for future advancements and applications of quantum computing in telecommunications.

3.1.3 Quantum AI/ML

3.1.3.1 Description

QML refers to the use of quantum algorithms to enhance or accelerate traditional machine learning tasks. Most current approaches rely on variational quantum circuits such as Quantum Neural Networks (QNNs), which combine a quantum model with a classical optimisation subroutine; or on quantum kernel methods, which aim to capture complex relations in data more effectively than classical methods. Other distinct lines of research include the quantum reservoir computing for time-series prediction, or quantum-enhanced generative models.
In the telecommunications sector, QML has its most immediate applications in areas where classical ML is already central to operations. These applications include network maintenance, security, customer analytics, and signal processing, where QML could provide advantages under conditions of data sparsity, imbalance, and heterogeneity, which are all common features of telecom data. In parallel, a second trajectory points towards the future quantum internet, where QML may be used to analyse quantum states directly for tasks such as channel monitoring, entanglement assessment, or QKD enhancement.

3.1.3.2 Use Case / Problem Statement

Just like for AI/ML in general, it can be expected that there will be countless use cases for quantum AI/ML. A preliminary stage is quantum-inspired AI.

Quantum-Inspired LLM Compression:

Telefónica, in collaboration with Multiverse Computing, has implemented quantum-inspired compression techniques on large language models (LLMs) such as Meta's Llama 3.1 8B and Llama 3.3 70B to enhance customer service operations [28]. The compressed models, achieving up to 80% size reduction, enable faster response times and significantly lower energy consumption (up to 75% compared to uncompressed models) while preserving response accuracy. These compressed models are powering chat systems that assist customer service agents. As a result, Telefónica can lower its infrastructure costs and reduce its environmental footprint. Because the models can be run locally in Telefónica's facilities, powered by renewable energy, the company is also able to keep CO_2 emissions to a minimum, supporting its goals around sustainability and open technology.

Generative Quantum Diffusion Models:

The objective of this research carried out by Telefónica and Qilimanjaro is to develop a generative quantum diffusion model for tabular data, capable of addressing two fundamental tasks: synthetic data generation and missing data imputation. In many telco applications, business-critical predictive AI models rely on tabular datasets that are often incomplete due to communication issues or collection errors. Reliable imputation of missing values is therefore essential to ensure robust downstream predictions.

Recent advances in diffusion models [29 30] have demonstrated their ability to generate high-quality data across complex and multimodal distributions. Telefónica has successfully adapted diffusion models to the tabular domain [31], achieving competitive performance in both data generation and imputation tasks. However, these models face a major limitation: the inference process is computationally expensive, as the denoising operation relies on a sequential Markov chain, requiring multiple iterative steps. While optimisation techniques [32] can reduce

the number of steps, the bottleneck of sequential denoising remains. To overcome this, the project explores quantum-enhanced diffusion models. The central hypothesis is that quantum computation, through its inherent parallelism and high- dimensional state space, can accelerate the denoising process without sacrificing data quality.

In the digital (gate-based) model, recent works target the core bottleneck of diffusion: sampling is slow because it requires many small denoising steps in sequence. Work such as [33] teaches small, parametrized quantum circuits (PQCs) to perform the denoising in short, repeatable stages, moving from very noisy to clean samples with fewer steps. Newer variants [34] build the device's real imperfections into the design, so the method is more practical on today's hardware. The limitation is that demonstrations are still small proofs of concept rather than large, real-world datasets.

In parallel, some efforts address latency and model size in classical denoisers. Here, parts of the denoiser are replaced with quantum circuits, and in some cases the entire trajectory is compressed into a single quantum sampling step to cut inference time dramatically [35]. In practice, however, current hardware runs involve only a handful of qubits, and the cost of loading data into the device and reading results out can erode the theoretical gains. Reported quality is promising on modest benchmarks but needs to be validated at enterprise scale, especially for tabular data.

There is also work that looks directly at the compute and energy cost of fast few-step samplers used at inference. These methods reframe the sampler's core mathematics so a quantum computer could, in principle, execute it more efficiently without retraining the model [36]. The catch is that the required building blocks are still deep and error-sensitive on today's machines, so practical advantages depend on hardware that is not yet widely available.

Motivated by the limits of gate-based proposals, we focus on analogue quantum processors. Unlike digital machines that rely on long sequences of gates (each introducing calibration overhead and potential error) analogue devices harness the native, continuous-time evolution of a quantum system, reducing cumulative errors and easing the need for heavy error correction on near-term hardware. Despite this promise, diffusion on analogue hardware is largely unexplored. Qilimanjaro and Telefónica investigate two complementary approaches: the first is a hybrid scheme in which the diffusion trajectory is executed classically, while the denoising neural network is replaced with an analogue quantum model; the second is a fully quantum diffusion process in which an analogue quantum state implements the generative evolution and measurements yield the final synthetic samples.

This research evaluates whether analogue quantum diffusion can reduce inference time while maintaining, or improving, the fidelity of generated and imputed data, paving the way for scalable quantum generative AI in enterprise Telecom applications.

3.1.3.3 Solution

Regarding available solutions for quantum AI/ML, there is the quantum-inspired solution "CompactifAI" from Multiverse for LLM compression, which is also mentioned in the previous use case section. Beyond that, Quantum AI/ML is still a research field, and, as such, no turn-key solutions exist yet.

One of the promising quantum methods to address telecom ML pain points (sparse/imbalanced events, heterogeneous telemetry, rare-fault regimes) is quantum generative modelling: instead of predicting labels directly, learn a high-dimensional data distribution and use it for data augmentation (rare outage/failure traces, intrusion patterns), imputation/denoising (missing KPI streams), and scenario generation (traffic/load patterns for capacity planning and closed-loop control). In the long term, fully-quantum generative models are especially attractive, as they have recently been proven to provide "generative quantum

advantage" for carefully constructed target distributions. This is an important proof point, even though its translation to relevant industrial/telecom datasets remains to be demonstrated [37].

In the nearer term, practical strategies include Born-type models (e.g., quantum circuit Born machines / quantum Born machines) and, in particular, iQP-based generative models, where training can be done efficiently on classical hardware (e.g., via efficiently computable expectation values/gradients) while sampling from the learned distribution is delegated to quantum hardware. This creates a plausible pathway to advantage specifically in the inference/sampling step that underpins synthetic-data generation for operations and security analytics [38]. In the analogue (or digital–analogue) model, Quantum Boltzmann Machines (QBMs) and evolved QBMs [39] provide another fit for telecom because they naturally model joint distributions over many correlated discrete/continuous factors (alarms, counters, configuration states), and recent formulations provide routes to quantum-efficient gradient estimation, which is often the bottleneck for training energy-based models. This supports use cases like anomaly detection, root-cause analysis, and probabilistic forecasting from multimodal network telemetry.

Quantum Reservoir Computing (QRC) is another attractive near-term QML strategy for telecom because it targets the bread-and-butter of operations: time-series. The core idea is to drive a fixed, dynamical quantum system (the "reservoir") with streaming inputs and train only a lightweight classical readout, avoiding deep trainable circuits and making it well matched to NISQ/analogue implementations [40]. This maps naturally to telecom use cases such as traffic/load forecasting, KPI-based anomaly detection and early warning, predictive maintenance from multivariate telemetry, and signal-processing tasks (e.g., channel monitoring/equalization) where temporal memory and nonlinear feature generation are key, potentially enabling compact, low-latency models deployable closer to the edge.

3.1.3.4 Status of the Technology

Research into QML for classical telecom use cases is still at an exploratory stage, but some encouraging demonstrations already exist. Variational quantum models and quantum kernel methods have been benchmarked on tasks such as churn prediction, outage data analysis, and anomaly detection. In these cases, QML models sometimes reach comparable performance to classical baselines while relying on fewer trainable parameters, which hints at possible efficiency gains. Early pilots and proof-of-concept studies have been carried out by academic and industrial groups, and industry surveys on 6G security explicitly list QML as a candidate technology, signalling that, even if preliminary, it is being considered within the telecom roadmap.

Still, the field as a whole faces general challenges that extend well beyond telecom. Benchmarking remains underdeveloped: most studies use small or toy datasets, comparisons are inconsistent, and there is a lack of domain-specific benchmarks to evaluate whether QML offers genuine advantages. This creates a gap between promising theoretical claims and measurable progress on real-world data.

A further distinction is that QML approaches do not all follow the same paradigm. Broadly, we can identify at least three directions:

- **End-to-end quantum models**, where the data is encoded into a quantum circuit and the output (e.g., classification) is produced directly by a quantum algorithm such as a variational circuit.

- **Hybrid quantum-classical models**, where a quantum subroutine acts as a feature extractor, kernel, or generative component, while a classical algorithm (e.g., SVM, generative models) handles the final output.

- **Quantum data processing stages**, where quantum devices are used not for the model itself, but to enhance the data before training with a classical learner. The main machine learning pipeline remains classical, but benefits from quantum pre-processing for tasks such as dimensionality reduction, feature selection or feature enhancement through quantum embeddings.

The majority of recent work in telecoms has explored the second and third variants, since they are less demanding in terms of quantum resources. Fully end-to-end quantum pipelines remain limited to very small problem sizes due to hardware constraints.
For quantum-native use cases, such as channel characterisation, entanglement quality assessment, or QKD stream monitoring, research is largely theoretical or confined to laboratory experiments. Algorithms exist that can classify quantum states or noise processes, but these are far from integratable into operational networks.

Beyond the hardware maturity problem (NISQ devices can only support shallow models with limited precision), quantum-native applications face additional integration requirements. For example, in a photonic quantum network, probe states must be converted into a form that a quantum processor can analyse in real time, raising questions about where this processing occurs. Running such tasks locally at the network edge, rather than in the cloud, may be necessary to meet latency and reliability constraints.

3.1.3.5 Challenges

Scalability remains the central challenge for QML in telecom. Most existing demonstrations still rely on simulators or toy datasets, leaving uncertainty as to whether quantum models can ever outperform strong classical approaches. Current hardware is constrained by noise, limited qubit counts, and poor connectivity, which restricts the depth and expressivity of algorithms. Progress will require not only more qubits but also better ones, with lower error rates and higher-quality interconnections, before QML can offer a tangible advantage in real-world telecom applications.

Trainability and optimisation pose a further obstacle. While gradients through quantum layers are, in principle, available (e.g., via the parameter-shift rule or adjoint methods), they are costly and fragile on current devices. Mitigations (problem-inspired shallow ansatz, local losses, careful initialisation, layer-wise training, SPSA/gradient-free optimizers, and hybrid pretraining) help, but do not eliminate, the risk. Additionally, non-gradient paradigms like quantum reservoir computing and quantum extreme learning machines avoid backprop through the quantum layer, making them promising in the short term [41].

Benchmarking is another pressing issue. The lack of standardised datasets and metrics makes it difficult to assess whether QML provides a genuine advantage. Most studies rely on toy problems or inconsistent baselines, and results are hard to compare across groups. This is not unique to telecom: benchmarking remains an open challenge across the entire QML field, slowing progress toward identifying truly promising directions.
For quantum-native use cases, such as channel characterisation or entanglement quality monitoring, integration is particularly complex. The real challenge lies in orchestration: unlike classical pipelines that can be offloaded to the cloud, quantum data must often be processed on-premises, close to the network infrastructure, and potentially necessitating an extra translation layer between photonic signals and quantum processors. Designing end-to-end workflows that combine photonic hardware, quantum processors, and classical control will require hardware-aware solutions tightly integrated with the telecom stack.
Finally, the maturity gap between use cases is stark: while predictive maintenance and security analytics could be tested on classical telecom data today, quantum-native use cases depend on the rollout of quantum networks, which are still pre-commercial.

3.1.3.6 Opportunities

Even with its current limitations, QML opens a clear opportunity space that spans both the short and the long term. In the near future, the most realistic role for QML is as a complement to classical machine learning, especially in tasks where telecom data are sparse, imbalanced, or exhibit strong spatiotemporal variability. These conditions often frustrate traditional approaches but are exactly the kind of settings where QML's capacity to capture complex correlations may prove advantageous.

In this short-to-medium horizon, some of the most promising use cases include:

- **Predictive maintenance**, where QML could detect early signs of degradation in base stations, routers, or optical devices. Its advantage lie in the potential of handling rare-event imbalance and spatiotemporal heterogeneity more effectively than standard models. In practice, this could mean anticipating failures earlier and reducing service downtime, translating into lower maintenance costs and improved network reliability.

- **Network and Cybersecurity Anomaly Detection:** Quantum classifiers have been proposed for identifying malicious traffic and abnormal network behaviour based on network log data. While still exploratory, 6G security surveys mention QML explicitly as a potential tool.

- **Network-as-a-Sensor (Wireless Sensing):** Telecom infrastructure can act as a distributed sensing platform with QML helping in the interpretation of high dimensional signals used in this setting. Vodafone and others have already tested WiFi/mobile signals for human motion detection, and Mitsubishi demonstrated pose recognition using QML with WiFi channel state information. This points to applications in smart homes and smart cities.

- **Customer Analytics and Churn Prediction:** Customer churn prediction is a long-standing challenge in telecom, where retaining a subscriber is often more valuable than acquiring a new one. Preliminary research shows QML classifiers such as QNNs may achieve comparable churn prediction than some classical baselines while using less trainable parameters, which could support targeted interventions and retention strategies.

- **Root Cause Analysis & Customer Impact During Outages:** When network outages occur, telecom operators need to quickly identify both the technical cause and the set of customers impacted. Outage datasets are typically sparse and noisy, which makes tracing back to the origin of a fault challenging. QML could help uncover latent structures in outage events, enabling faster localisation of failures and more accurate mapping of affected users or services. This would allow telecom operators to shorten recovery times and prioritize response where the impact is greatest.

- **Traffic Forecasting and Network Slicing:** Accurate modelling of traffic patterns is critical for tasks such as optimal network slicing. QML may offer improved generalisation when data is highly non-stationary or heterogeneous, with algorithms such as quantum reservoir computing specialising in that front. More accurate forecasting would enable telecom operators to allocate bandwidth dynamically and improve quality of service during peak demand.

Across these use cases, anomaly detection emerges as a recurring theme: from cybersecurity threats to equipment failures and outage patterns, telecom data often feature imbalance and

rarity, where QML may provide an advantage over classical techniques. Particularly in the context of 6G and beyond generations, networks are envisioned as “AI-native” systems, where tasks such as slicing, security, and resource management are orchestrated automatically by machine learning. Within this vision, QML could serve as a complementary layer by providing models with non-classical capacity to capture correlations in traffic, spectrum, and security data. Many of the use cases already described, such as traffic prediction, wireless sensing, or anomaly detection in network operation, are directly relevant to 6G, where scale and heterogeneity make learning particularly challenging. Although practical deployment will depend on hardware maturity, 6G and beyond may be the first generations to consider integration of quantum accelerators into the network fabric, whether at the edge or in the cloud, making QML a potential design consideration for future architectures.

Looking further ahead, **as quantum communication networks** mature, QML may become not just complementary but essential. Unlike classical ML, QML can process quantum states directly without collapsing them, enabling entirely new capabilities at the quantum layer itself. Potential applications include:

- **Quantum Channel Characterisation & Noise Classification:** Quantum channels are susceptible to different types of noise, such as depolarising, dephasing, or amplitude-damping effects, which can degrade transmitted quantum states. QML models could identify these disturbances without destructive measurement, enabling adaptive error mitigation and more reliable quantum communication.

- **Entanglement Quality Assessment:** Distributed entangled states are fundamental for many quantum network protocols, but their quality can degrade over distance or time. By analysing these states, QML could detect degradation and trigger purification or refinement, supporting reliable entanglement distribution and consistent network performance.

  Network Calibration & Monitoring: Optical components and other network infrastructure can drift or misalign over time, affecting network performance. Probe states transmitted across the network could be analysed by QML systems to infer such instabilities, enabling continuous and non-destructive calibration and maintaining operational integrity.

- **QKD Stream Analysis:** Instead of working only with classical post-processed key bits, QML could classify quantum states directly in a QKD protocol. This may improve detection of eavesdropping or side-channel anomalies at the quantum layer.

Across both time horizons, a recurring theme emerges: anomaly detection. Whether the anomalies lie in equipment failure, cybersecurity threats, outage patterns, or quantum noise processes, QML may offer more sensitive and robust methods for identifying them compared with purely classical techniques.

3.1.3.7 GSMA Role

At the ecosystem level, GSMA is well positioned to connect telco operators with quantum hardware and software providers, catalysing pilot projects that bring academic research closer to operational deployment. GSMA can also provide a policy and advocacy voice, informing regulators and governments about the potential and limitations of QML in newer generation networks.
GSMA can also play a convening role in establishing shared benchmarks and evaluation frameworks for QML in telecom, ensuring that results are comparable across telecom

operators, vendors, and research groups. This would help move the field beyond toy datasets toward industry-relevant testing.
In addition, GSMA could promote knowledge transfer and skills development by creating working groups, training modules, or white papers that help telecom operators understand both the opportunities and limits of QML. Building a shared knowledge base will prevent hype from running ahead of capability, while preparing the workforce for future adoption.
GSMA should discuss that QML is considered in broader discussions around AI-native network architectures for 6G and beyond. If quantum accelerators eventually become part of network infrastructure, at the edge or in the cloud, early alignment on interoperability, latency requirements, and security standards will be critical. This way, GSMA can help position the industry to capture QML's benefits while managing its risks.

3.2 Quantum Communication

3.2.1 Quantum Key Distribution

3.2.1.1 Description

QKD is the most mature application of quantum communication technologies and serves as a foundational pillar in the emerging quantum communications ecosystem. Quantum communication broadly refers to the transmission of quantum states over distance, enabling tasks such as secure key exchange, quantum teleportation, and, in the future, distributed quantum computing. QKD enables two parties to generate symmetric encryption keys with information-theoretic security, relying on principles such as the no-cloning theorem and the disturbance of quantum states upon measurement. These keys are typically used in conjunction with classical encryption protocols to enhance communication confidentiality.

Since the introduction of the first QKD protocol, BB84, by Charles Bennett and Gilles Brassard in 1984 [42], numerous protocols have been proposed. Although they differ in implementation and are based on varying physical principles, QKD protocols can be broadly classified into two main categories:

1) **Discrete-Variable QKD (DV-QKD) Protocols**: These protocols encode information in discrete quantum states, such as the polarisation or phase of photons. The most well-known example is BB84 [74], which originally used the polarization of single photons to represent binary values. DV-QKD protocols are widely implemented due to their simplicity and compatibility with existing optical fibre infrastructure.

    a. **Prepare-and-Measure QKD (PM-QKD):** These are the most widely implemented QKD protocols in industry. In this model, the transmitter (Alice) prepares quantum states and sends them to the receiver (Bob), who measures them using randomly chosen bases. This approach forms the foundation of many practical QKD systems. Notable examples include BB84 [42], and B92 [43], a simplified variant that uses only two non-orthogonal states for encoding.

    b. **Entanglement-Based Protocols:** Unlike prepare-and-measure protocols, entanglement-based QKD involves a third party that generates pairs of entangled photons and distributes them to two distant receivers. Each receiver performs measurements on their respective photons, and the shared key is derived from the correlations between these measurements. Prominent examples include Ekert 91 [44] protocol, which is based on Bell inequality violations, and BBM92 [42], a practical entanglement-based adaptation of BB84 [42]. These protocols offer strong theoretical security guarantees and form the foundation for quantum networks and quantum repeaters, enabling scalable and long-distance quantum communication.

2) **Continuous-Variable QKD (CV-QKD) Protocols:** Unlike discrete-variable QKD, CV-QKD encodes information using the continuous properties of light waves, such as amplitude and phase quadratures. One of the key advantages of CV-QKD is that it does not require specialised components, such as single-photon detectors. Instead, it uses standard telecom equipment such as homodyne or heterodyne detectors, making it more compatible with existing fibre-optic infrastructure. Because CV-QKD operates in a high-power regime, rather than relying on single-photon transmission, it integrates more easily into conventional optical networks. The security of protocols like GG02 [45, 46, 47] relies on the fundamental quantum principle that an eavesdropper cannot simultaneously measure both amplitude and phase with high precision without introducing detectable disturbances.

A current key limitation (see also subsection 3.2.1.5) of QKD is its distance constraint. Quantum signals degrade due to signal loss in optical fibre or free-space channels, and amplification is not possible without destroying the quantum state. Fibre-based QKD systems are typically constrained to distances of 100–150 km. To extend coverage, trusted-node architectures are used, where keys are decrypted and re-encrypted at physically secure intermediate nodes. Although effective, this model assumes the trustworthiness of each node, which may be unsuitable for some threat models.

Another mitigation technique for overcoming distance limitations in QKD is to enhance the detection capabilities by employing advanced single-photon detection technologies [48]. SNSPDs are particularly well-suited for this purpose due to their high detection efficiency, low timing jitter, and minimal dark counts. Commercially available systems such as the ID281 [49,50] and ID281 Pro [49,50] from ID Quantique exemplify this technology's maturity and accessibility.

To address the two main limitations of practical QKD implementations—limited transmission distance and the reliance on trusted nodes—advanced QKD protocols have been developed and successfully demonstrated by the academic community.

One such protocol is Measurement-Device-Independent QKD (MDI-QKD), which eliminates one of the most critical vulnerabilities in conventional QKD systems: detector side-channel attacks. This is achieved by relocating the detection system to a third, untrusted central node. In MDI-QKD, both communicating parties send quantum states to this central node, which performs a joint measurement. The key is then generated based on the correlations between the sent states, rather than the measurement outcomes themselves.

Similarly, Twin-Field QKD (TF-QKD), which is often regarded as a next-generation QKD protocol, also uses a central node. However, in this case, the two communicating parties transmit weak coherent pulses to the node, where single-photon interference is measured. This approach allows the parties to agree on a shared key while significantly extending the secure communication distance, surpassing the fundamental rate-distance limit of traditional QKD. Quantum repeaters, which remain in early-stage development, rely on quantum memory and entanglement swapping to extend QKD without intermediate trust. Satellite-based QKD has also demonstrated long-distance key exchange via entangled or prepared states between ground stations, opening the door for global-scale quantum-secure communications.

In the near-term and mid-term, key relay techniques will be essential for the massive deployment and interconnection of QKD networks. Key relay techniques allow to generate a secure End-to-End (E2E) quantum-safe key based on QKD keys, regardless of the number of QKD links present between both ends. Therefore, these key relay techniques extend the range of QKD networks from metropolitan areas to wider areas (e.g. EuroQCI initiatives). Furthermore, key relay techniques allow to interconnect the terrestrial and the space QKD

segments allowing to interconnect two remotes terrestrial QKD networks through a satellite QKD link.

Another advantage of key relay techniques is extending the range of QKD networks to locations where QKD could not be physically deployed due to physical or other limitations.

3.2.1.2 Use Case / Problem Statement

Telco and fibre network operators manage the critical infrastructure that underpins national and global connectivity. As quantum computing advances and cyber threats grow more sophisticated, ensuring long-term data confidentiality has become a strategic imperative, especially for traffic involving government, financial, or industrial data.

QKD enables forward secrecy based on the principles of quantum mechanics. Keys generated through QKD are immune to retrospective decryption, offering enduring protection against future computational advances. Quantum key distribution is particularly relevant for industries with sensitive data with a long shelf-life, such as financial services, government & military as well as health care. Therefore, numerous areas with use cases for QKD exist and are elaborated in the following.

Datacenter Interconnect Based on Shared QKD Infrastructure:

Modern organisations increasingly rely on external providers to optimise costs, streamline operations, and ensure high availability. This reliance often involves implicitly sharing infrastructure, platforms, and systems, such as co-location Data Centres (DCs), in which multiple tenants operate and may be interconnected across sites. While this shared model offers operational and economic benefits, it introduces significant cybersecurity challenges. In particular, the concept of "sharing" is not inherently aligned with secure practices, especially when it comes to sensitive operations like key management.

The critical challenge is to design a quantum-safe, future-proof Key Distribution Infrastructure (KDI) that balances security, affordability, and operational efficiency. Such a model must:

- Ensure strong isolation between tenants and systems.
- Be resilient against emerging threats, including those posed by quantum computing.
- Support scalability and interoperability across diverse environments.
- Remain cost-effective for widespread adoption.

QKD for Sensitive Healthcare Data:

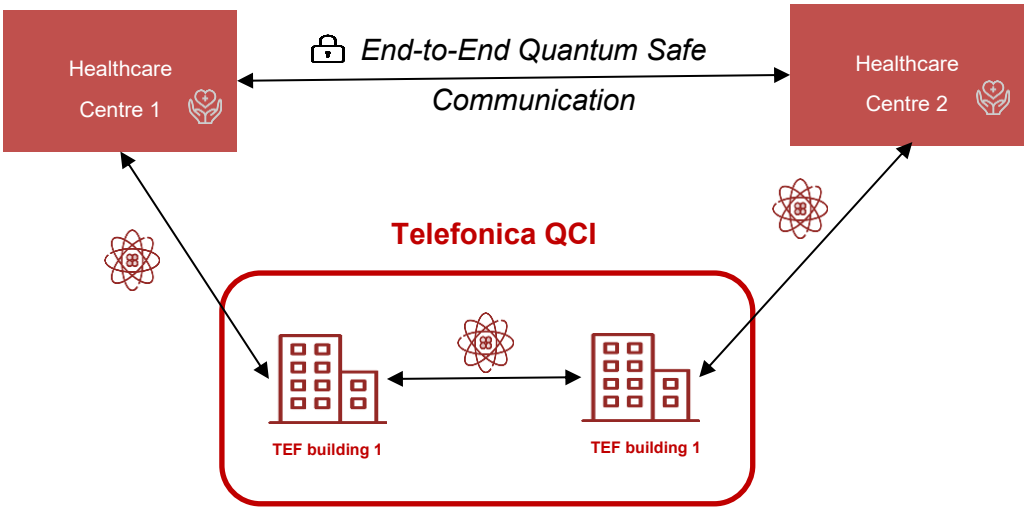


Figure 8: Overview of Telefónica QKD trial with Health Care centre in Madrid

Telefónica for example, in collaboration with Vithas and technology partners LuxQuanta and QoolNet, has implemented a QKD system to secure communications between two hospitals in Madrid. This setup (show in **Figure** 8) also uses quantum fibre optic links and QKD equipment to generate encryption keys based on quantum physics principles, aiming to protect sensitive healthcare data from potential future threats posed by quantum computing. The project demonstrates the feasibility of using QKD to enhance data confidentiality in healthcare environments, particularly for applications like teleconsultation and remote patient monitoring.

QKD in Metropolitan Networks:

Launched in June 2025 by Orange Business, the Orange network and digital integrator, this new offer (“Orange Quantum Defender”) was designed through a partnership between Orange and Toshiba. This offer brings a new multi-layer quantum-safe network with QKD and PQC technologies. Currently, only Paris and Ile-de-France region are in Orange’s sights for this offer.

London QKD Trial [51]:

BT and Toshiba have launched the Quantum Secure Metro Network, which is the world’s first commercial pilot of quantum secured communication services via a metro network in London. Figure 9 shows the high-level system design. This initiative uses QKD to protect data transmission between trial locations including head offices of triallists such as EY and HSBC in Canary Wharf, central London private data-centres, and colocation data-centres in Slough. This marks a significant demonstration of a secure and high-performance network, which can offer encryption as service based on keys from QKD, and an option for hybridisation of the QKD keys with the PQC algorithm for key exchange (ML-KEM).

BT operates the network using Openreach's private fibre infrastructure, and supplies the high-speed private encrypted links, while Toshiba provides the QKD hardware and key management system. The trial showcases how quantum-secured data can be transmitted over standard fibre links, offering enhanced protection against future cyber threats posed by quantum computing, while also showing the feasibility of transmitting quantum states over standard fibre in operational environments.

Telefonica QCI

Telefónica's QCI is a multi-technology, multi-vendor quantum communications infrastructure deployed at Telefónica's production facilities, providing a realistic metropolitan network scenario in which the different components of a QCI can be tested, ranging from QKD devices to encryption systems.

This infrastructure presents a coexistence scenario between classical and quantum communications over a Dense Wavelength Division Multiplexing (DWDM) optical network, reflecting the conditions of real-world telecom deployments. In addition, Telefónica's QCI is designed with security principles that emulate those of a real telecommunications production network, allowing different manufacturers to understand and comply with these requirements. This contributes to advancing the technological maturity and interoperability of QKD network devices.

Telefónica's QCI is integrated into MadQCI, serving as one of its key testbeds. As part of MadQCI, it supports multi-vendor experimentation and SDN-based control and orchestration, helping validate the deployment of quantum-secure communications in operational environments. This integration reinforces Spain's leadership in the development of quantum-ready infrastructure and contributes to the broader objectives of the EuroQCI initiative.

Madrid Quantum Communication Infrastructure (MadQCI)

MadQCI (Madrid Quantum Communications Infrastructure) is a pioneering QKD network deployed across production-grade telecom environments in Madrid. Unlike traditional QKD setups, MadQCI integrates quantum and classical communications using software-defined networking (SDN) principles, enabling dynamic routing, multi-vendor interoperability, and scalable deployment [52].

Key features include:

- 28 QKD modules from five manufacturers across 9 production sites
- 45 dynamic quantum links with shared infrastructure for quantum and classical signals
- Use of ETSI standards for seamless integration and key management
- Support for OSI encryption levels 1, 2, and 3
- Execution of 85,000+ use case instances including cloud services, 5G, e-health, and critical infrastructure protection

MadQCI demonstrates that QKD can be deployed cost-effectively in real-world networks, offering a blueprint for future European quantum communication infrastructures. The European Quantum Communication Infrastructure (EuroQCI) is a flagship initiative launched by the European Union in 2019 to establish a quantum-secure communication network across all 27 Member States and their overseas territories. It is a cornerstone of the EU's Cybersecurity Strategy and a key enabler of European digital sovereignty.

European Quantum Communication Infrastructure (EuroQCI):

EuroQCI is designed as a dual-segment infrastructure:

- Terrestrial Segment: Built on fibre-optic networks connecting strategic national and cross-border sites.
- Space Segment: Enabled by satellites such as EAGLE-1 and the ESA SAGA missions, forming part of the broader IRIS² secure connectivity program.

The infrastructure integrates QKD technologies to ensure ultra-secure transmission of cryptographic keys. These technologies are being developed and certified under EU programs like Digital Europe and Connecting Europe Facility (CEF).

Each Member State is responsible for deploying its own national QCI network, with Spain's EuroQCI-SPAIN project serving as a prominent example. It includes:

- QKD nodes in Madrid and Barcelona.
- Long-distance cities interconnection study using terrestrial and satellite links
- Cross-border links with Portugal and France.
- Initial experiments of quantum repeater nodes for future quantum internet capabilities.

Use cases span both public and private sectors:

- Public Sector: Emergency coordination, health data protection, lawful interception, and secure government communications.
- Private Sector: Banking backbone, insurance, and financial services.

EuroQCI addresses the looming threat of quantum computing to classical encryption. By embedding quantum technologies into existing infrastructure, it provides a future-proof security layer. This is vital for safeguarding sensitive data in hospitals, government institutions, and energy grids.

The initiative is supported by a consortium of European industry leaders, research institutions, and Small & Medium Enterprises (SMEs). Projects like PETRUS coordinate deployment and standardization efforts, ensuring interoperability across national networks. The project Nostradamus is setting up a test- and evaluation infrastructure for QKD devices and systems.

Since 2024 and until 2028, EuroQCI will expand its terrestrial and space segments, deploy cross-border links, and establish testing and certification infrastructures. The goal is to create a pan-European quantum communication backbone, reinforcing Europe's leadership in cybersecurity and quantum technologies.

Satellite QKD:

SES, together with European Space Agency (ESA) and European Commission, have co-financed a large space program to demonstrate long distance satellite-based QKD. The initial demonstrator mission named EAGLE-1, targets a demonstration of the QKD protocol specifically designed for a Low Earth Orbit (LEO) satellite mission with an initial coverage zone over continental Europe. The demonstrator is composed of a single satellite, expected to provide testing capabilities by Q2-2027 and will provide an in-orbit test bed to assess the performance, future service models, concept of operations, interoperability of equipment and the sensitivity of the space segment to various parameters and conditions. The initial capability allows 60 Ground terminals to be served for test purposes during a 3 year mission.

The system is designed to provide quantum keys, for demonstration, over very long distance. Satellite QKD is relevant when terrestrial QKD is:

- Not providing very large coverage:

  - Not yet available in neighbouring countries: the dissemination of terrestrial QKD segment requires time to cover intercity long distances, installation of Ground station might be booster to disseminate the technology
  - Out of reach: the typical case of Cyprus, which is an island that is too far away from the nearest countries implementing terrestrial QKD to implement undersea cables. QKD technology is not compatible with repeated subsea optical transmission system and is therefore limited to roughly 100 km reach of non-repeated subsea cables.
  - Requires an “any-to-any” or star topology which satisfies the need for more than two entities or systems to establish a secure channel without relying on a dedicated terrestrial infrastructure between the nodes.

- Costly to operate: because quantum memories are not yet commercially available, covering long distance via terrestrial QKD requires one trusted nodes every ~120 km. A trusted node is a physical enclave where devices are operated to process quantum keys and relay them further to the next trusted node. As an example, covering the distance between Madrid and Warsaw would require 24 trusted nodes, while the same service would require three trusted nodes, the satellite and the two ground terminala on a satellite segment.
- Too complex to operate: sharing a secret between Finland and Spain through terrestrial QKD would require crossing around multiple territories, each with their own legal frameworks and national security agency requirements. The space segment significantly lowers the complexity given that only the legal framework of the two ground terminals is enforced; the space segment is considered an international zone.

Satellite QKD is not expected to be positioned on the same market segment as last mile QKD, but rather as a complementary solution to local provider distributing quantum keys in a dense urban area. Therefore, there are essential questions that must be answered:

- **Key volume capabilities** to distribute or relay keys between two dense urban areas or over a wide-meshed network: would the key performance be sufficient according to the needs?
- **Trust in the service** carried over a spacecraft: will the satellite acting as a trusted nodebe accepted from a security point of view?
- **Mutualisation of costly infrastructure**: there is a common interest in the initial phase of QKD deployment to derisk the investment in costly infrastructure. Therefore, interoperability with terrestrial technology is an essential ingredient to offer a system globally accepted by telecoms throughout the world. This interoperability of technology at the key management layer would help defining bespoke and/or standardised wholesale services to support the quantum-safe service ecosystem.

3.2.1.3 Solution

QKD delivers secure key exchange by using quantum principles to detect eavesdropping and guarantee key confidentiality, fitting naturally into telecom network architectures, and offering a physics-based complement to algorithmic encryption.

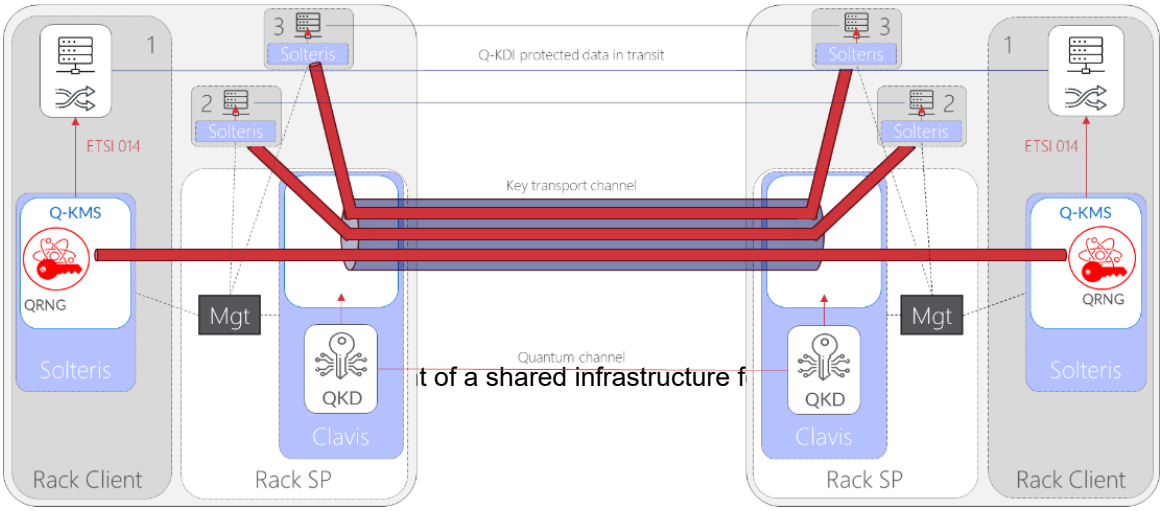
In a typical deployment, two endpoints establish a shared symmetric key via quantum state exchange over fibre or free-space and the key is then used in classical encryption schemes

(e.g. AES). Because QKD only distributes keys—not encrypted data—it can be integrated modularly into existing network infrastructure. Integration, however, requires explicit support for ETSI QKD 014 (see also discussion of standards in 3.1.1.4), otherwise custom integration is needed.

QKD can be deployed across point-to-point fiber links between strategic nodes like data centres or cable landing stations. Where distances exceed QKD's practical range, trusted-node architecture allows hop-by-hop regeneration of keys. For international or remote connections, satellite QKD provides a viable alternative through key exchange between ground stations via orbiting satellites.

Integration into telecom workflows involves linking QKD systems with key management infrastructure, including key management systems (KMSs), certificate authorities (CAs), and provisioning tools. Emerging standards define APIs and delivery mechanisms to support compatibility with conventional cryptographic modules. QKD links can also be orchestrated via SDN controllers and integrated into service routing or network slicing strategies, enabling dynamic provisioning of quantum-secure links for selected workloads.

While PQC provides an essential response to future quantum attacks, QKD covers real-time physical-layer intrusion detection and information-theoretic security.[2] Together, they enable layered security architectures tailored to different risk profiles and operational constraints.



For the data centre use case mentioned in the previous section, one approach, as suggested by ID Quantique, is to establish a single trusted service provider (SP) within a co-location data centre (DC) environment (Figure 14**Error! Reference source not found.**). A Service Provider (SP) operates a QKD connection between two DCs using a Clavis XG QKD System. The users in the co-location DC host KDI endpoints (Solteris) managed by the SP. In this way, each user has its own private end-to-end key distribution channel while sharing the QKD infrastructure. ETSI 014 is used to deliver the keys to the user's encryptors. In this model:

[2] Several national cybersecurity agency recommendations (such as NCSC, BSI, ANSSI, etc.) have published a more critical perspective on QKD and recommend using PQC (see also the subchapter Challenges)

- The SP provides and manages KDI endpoints—such as Solteris Network Appliances—which are hosted by individual DC clients in their respective bays.
- These appliances perform quantum-safe key generation, secured end-to-end using post-quantum cryptography (PQC).
- The QKD infrastructure itself is shared among clients, but key transport remains independent and doubly protected:
    - End-to-end PQC secures the communication between endpoints.
    - QKD-based encryption is applied when client keys are transported outside the DC environment.

Importantly, the users' encryption devices may or may not be serviced by the same SP, offering flexibility while maintaining strong security guarantees.

This architecture enables a scalable and cost-effective deployment of quantum-safe key distribution, while preserving client autonomy and ensuring robust protection against both classical and quantum threats.

Satellite QKD

In satellite-based QKD (see **Figure 10**), the system has to be designed to provide optimised performance, according to a consistent security concept and according to the nature of a space-to-ground communication channel. This free space optical channel is characterised by fluctuations of attenuation along the overfly of the satellite above a ground terminal and by several types of impairments (geometric impairments, moonlight, weather conditions, etc.). Unlike QKD through fiber, there is a high uncertainty of the continuity of a contact between the QKD transmitter and the QKD receiver.

This uncertainty poses a significant challenge for entanglement-based QKD, in which the probability of having two ground terminals in visibility at the same time and for a significant time slot is not taken for granted. When these visibility conditions are met, entanglement-based QKD has a very strong security concept, as mentioned later. Given the challenge of serving two ground terminals on the pass of the satellite at the same time, an alternative is prepare-and-measure QKD, which offers a trade-off between the capability in terms of key volume per contact time (i.e., cost for the final product), the security concept and the complexity of the solution.

The key volume per contact time: due to characteristics of the channel and the attenuation on the path, typically around 50 dB, the key rate is drastically lower compared to terrestrial QKD, with typical attenuation around 20 db. Therefore, the usage of the quantum keys, shared between system usage and product made available to customer shall be carefully considered. A layer of automation to minimise the waste of quantum key material is required together with further improvement on the QKD chain (link budget, RNG bit stream, detection strategy, etc.)

The complexity of prepare-and-measure QKD comes from the need to command combinatory logic to have a symmetric secret made available at two ground terminals. The quantum channel is established from the transmitter Alice, in the satellite, and a receiver Bob in one ground terminal. However, the user expects to receive a symmetric quantum key between two ground locations. In this concept, a QKD controller provides instructions to Alice and both Bobs served, to perform combinatory logic that contributes to the pair-wise key sharing between both Bobs.

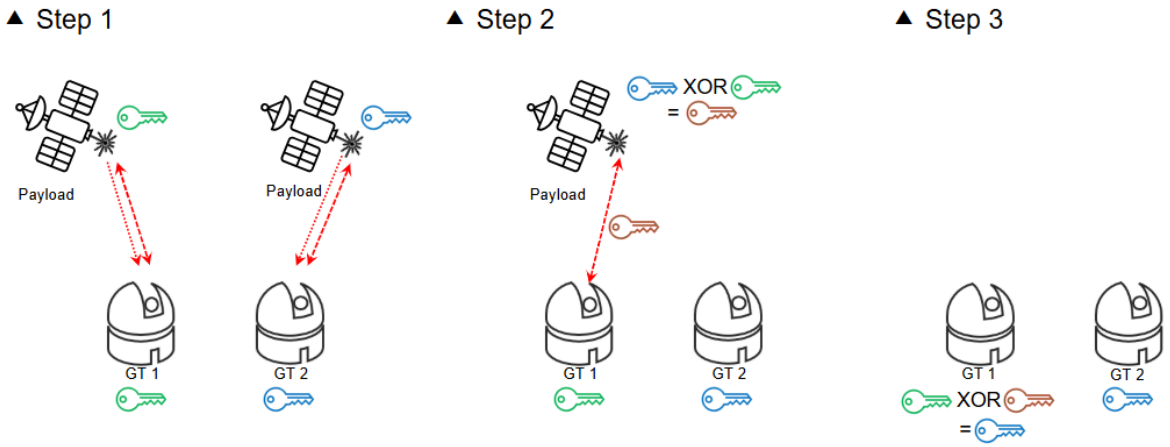


Figure 10: Simplified process for pair wise key sharing in a P&M space QKD segment

The security concept: entanglement-based QKD is conceptually straightforward; a single source provides information sent in two different directions at the same time with no possibility to intercept the signal without changing it. Because the receiving nodes are driving the agreement of the shared secret, there is no need to trust in the source of qubits, operated by a third party, the satellite operator.

In prepare-and-measure QKD, because the satellite flies over several ground stations, with a copy of their key in memory, it has full knowledge of the key involved in the end-user service and shall be consequently considered a trusted node. This significantly complexifies the security concept and requires managing physical access security at the ground terminals. Prepare-and-measure QKD requires a baseline of three trusted nodes to deliver quantum keys worldwide.

To raise trust in these trusted nodes, several options, non-mutually exclusive, can be proposed: *certification* where the implementation and the technology are checked by an independent expert, *transparency* where consistent ad-hoc reporting is offered to the end-user of the system , complemented with auditing capabilities, etc.

The demonstrator for prepare-and-measure QKD will clarify the key volume expected in various locations and various conditions of operations. This capability depends on the design (link budget, pace of random number generation, detection efficiency, etc.) and the combined impairment. As such, SES plan to collect significant amounts of Key Performance Indicator (KPI) data to refine modelling and improve the technology to expand its capability through a fleet of satellite and predictive impairment. The main objective of EAGLE-neXt is to provide worldwide satellite-based quantum safe commercial services to private customers, which can also be made available to interested governmental entities. To this end, the focus will be on the following customer segments: cloud providers, healthcare, banking, insurance, and telecom operators, while also considering the requirements of governmental entities for secure data.

EAGLE-neXt System overview

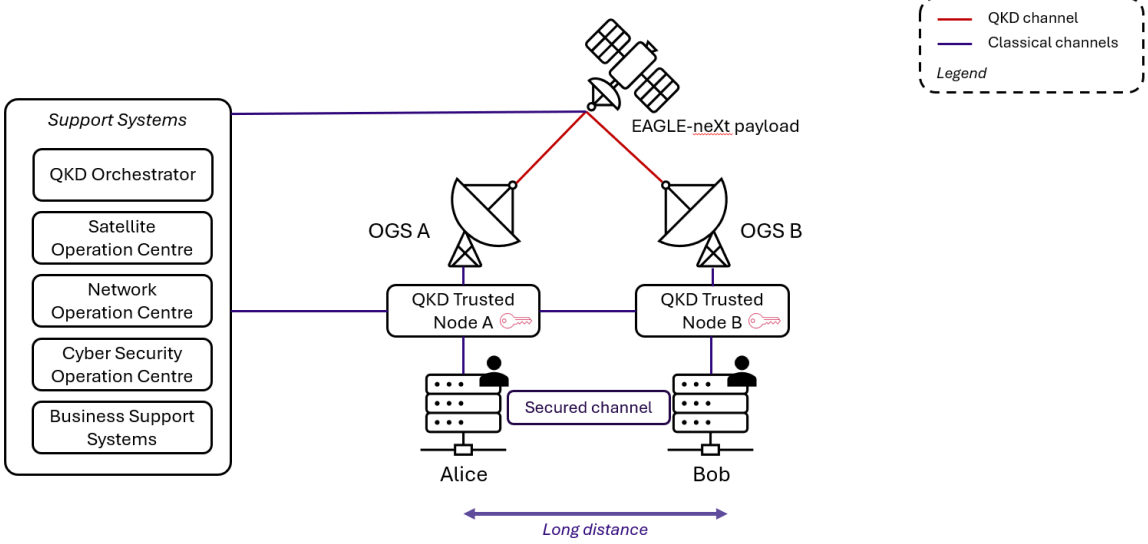


Figure 11**:** Overview of Eagle-neXt system

This first version of the service will serve as a basis for more specific projects in cooperation with Member States and other partner countries. To provide this service, EAGLE-neXt is being developed as a scalable fully operational constellation, where not only the overall quantum key volume can be easily increased with additional satellites as the number of users grows, but where each additional satellite also increases the resilience of the overall system and enables specific customer requirements to be addressed. The EAGLE-neXt system as a whole and its individual satellites will therefore be developed with a clear focus on the following three main points:

- **Interoperability**: A network orchestration layer will enable seamless integration of the space and terrestrial networks, ensuring a smooth customer experience and enabling collaboration with telecom operators at the landing points served.
- **Security**: Since the sole purpose of the system is to securely distribute quantum keys between any two points on Earth, security will be the main driver from the very beginning of the project and the basis on which the system will be built.
- **Performance**: Compared to the in-orbit validation mission, several system-level parameters will be adjusted based on the lessons learned during the development phase to improve price/performance ratio for a user's ground station, thereby significantly increasing the ultimate cost-effectiveness.

3.2.1.4 Status of the Technology

QKD has moved from the realm of theory to early commercial deployment, with systems in use across national, regional, and enterprise networks. While not yet widespread, the technology has reached a maturity level suitable for targeted use in sectors requiring high-assurance communication.

Prepare-and-measure protocols are the most widely deployed, typically over dark fibre routes. These systems support key generation rates sufficient for refreshing symmetric keys and are

constrained to distances under 150 km without repeaters. Trusted node configurations are used to scale deployments to national or regional scopes.

Government-backed pilots have accelerated adoption across Europe, Asia, and other regions, focusing on inter-ministerial communication, cross-agency coordination, and cable landing station protection. Satellite-based QKD has been successfully demonstrated, providing intercontinental key distribution capabilities. Recently, scientists reported progress in the miniaturisation of satellite and base stations [27], positioning satellite QKD as a potential alternative technology for long distance, international or intercontinental deployments.

Significant progress has been made in the certification and standardization of QKD systems, driven by various stakeholders across the QKD ecosystem. A leading example is the ETSI, which, through its Industry Specification Group on QKD (ISG QKD), has published over 15 documents—including Group Specifications (GS) and Group Reports (GR)—with 11 more currently under development. These documents aim to support the widespread adoption of QKD networks by standardising foundational concepts, component characterization, and network integration and management. One of ETSI's key contributions is the ETSI GS QKD 016 Protection Profile (PP) for prepare-and-measure QKD modules. This is the first dedicated Protection Profile for QKD, aligned with the internationally recognized Common Criteria framework for security certification.

In parallel, the ISO/IEC 23837 standard (in two parts) became the first to target the evaluation of QKD devices within a certification context, outlining security functionalities and providing detailed methodologies, rationales, and setups for evaluation laboratories to assess both QKD transmitters and receivers.

The ITU has also been active, developing recommendations through three Study Groups (SGs). These cover a wide range of topics including conceptual frameworks, functional architectures, key management, security considerations (X.1700 series), and interoperability.

Evaluation is a critical step toward certification. In Europe, the European Commission has launched the Nostradamus project, which aims to establish the first dedicated QKD evaluation laboratory. This facility is expected to be operational and offering services by 2026.

Globally, the principle of "Security Assurance by Evaluation" is emerging as a common approach among national agencies. A notable example is South Korea, where the National Security Research Institute (NSR), in collaboration with Korea Research Institute of Standards and Science (KRISS), Telecommunications Technology Association (TTA), and the IT Security Certification Center (ITSCC), awarded the first national security certification to IDQ's Clavis XG QKD system in early 2025. The certification process involved a rigorous evaluation of both optical and digital subsystems, as well as the software stack and protocols of the embedded QKMS, Clarion KX.

Operationally, QKD systems remain largely appliance-based, interfacing with optical networks via dedicated fiber. Integration with KMS, SDN, and orchestration frameworks is progressing, as is experimentation with QKD signal coexistence on DWDM infrastructure.

Overall, QKD is entering a phase of applied validation, ready for early adoption where risk profiles justify the investment and progressing toward broader adoption as standardisation and integration practices mature.

Satellite QKD

QKD technology for space applications has moved from scientific experiments and initial feasibility demonstrations to the development of practical, operational satellite constellations and integrated global networks. The focus is currently on improving key rates, enabling daytime operation, and reducing CapEx (smaller telescope, compact receivers, etc) and OpEx.

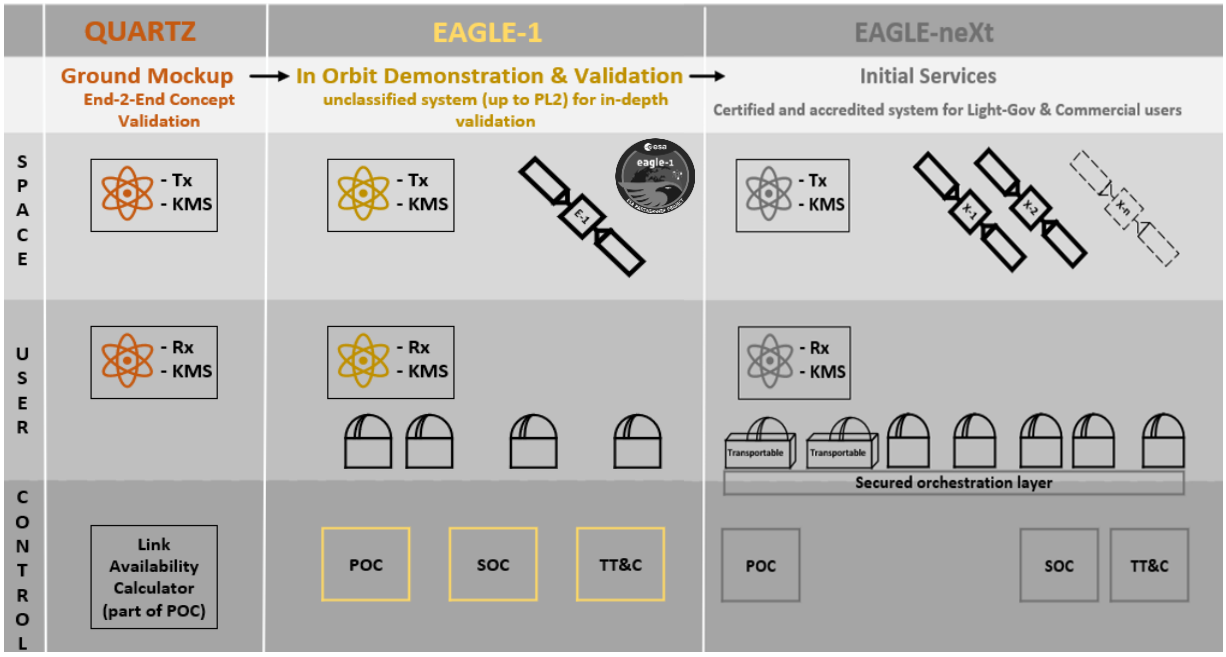


Figure 12**:** SES programs, from Scientific research to commercial services

Demonstration of long distance QKD in space segments: Early missions, notably China's Micius satellite and the Tiangong-2 Space Lab, successfully demonstrated space-to-ground QKD, proving the technology is viable for long-distance, secure communication.

Expanding coverage and service resilience: From a demonstrator of a single satellite to a fleet, a significant complexity of management of space-craft planning must be considered to:

- optimise service of ground terminal: the cost of airtime of a satellite requires a QKD management layer, specific to space, to optimise the probability of contact, therefore optimising the use of QKD payloads.
- achieve service resilience: a limitation of a single satellite segment is that contextual data specific to security and/or the QKD protocol requires a ground terminal to be served by the same satellite. To improve availability of quantum-safe security services, additional system improvements are required to demonstrate resiliency through a fleet of space craft.

Reduce cost for the customer: Optical ground stations for satellite optical communications are mature products, and the challenge is to design a system where the cost of the ground terminal, including the optical ground station, would be either mutualised between different QKD receivers, therefore sharing OpEx of the telescope, or would be reduced in size to accommodate a single user. For the latter, miniaturisation of the receiver is currently explored to increase power efficiency and easy integration on site. Photonic integrated circuits can have a significant impact on in this trend.

Provide trust: there are multiple research papers defining a security proof for QKD, but there is not a specific security proof commonly adopted by the QKD community (security agencies, research centres, companies) that would support the adoption of a space QKD chain

implementation. Such a security proof would certainly support the adoption of QKD and more generally the definition of a standard QKD protocol.

Daytime operations: A key research focus is enabling satellite-based QKD during daylight hours and through cloud cover, which currently limits operation to night-time and good weather conditions.

Standardisation efforts: Public standardisation bodies, such as ETSI and ITU are working on recommendations and standards of interoperability. There is currently no interoperability interface at the QKD layer but rather at the KMS layer, leveraging on the flexibility of software to provide innovative mechanism for horizontal interoperability.

3.2.1.5 Challenges

Despite growing maturity, QKD adoption in telecoms networks faces several practical and systemic challenges.

The **distance limitation** remains a technical constraint; quantum signals cannot be amplified, limiting point-to-point QKD links to metropolitan ranges (~100 km per link). While trusted nodes extend reach, they introduce security dependencies that are not suitable for all environments.

Integration complexity stems from QKD's need to interoperate with higher-layer encryption protocols, key lifecycle management systems, and dynamic orchestration platforms. Interface variability and lack of unified Software-Defined Network (SDN) integration increases deployment complexity.

Interoperability gaps hinder multivendor deployment. While interoperability remains a challenge for QKD deployment, it is actively being addressed by Standardization Development Organizations (SDOs) such as ITU-T and ETSI. Notably, ITU-T is currently working on the development of a Protection Profile for key management entities, which will support the evaluation of key management implementations available in the market. These efforts are essential to ensure compatibility across diverse systems and vendors, and to facilitate the integration of QKD into broader network infrastructures. Interoperability is also key to avoiding vendor lock-in. Multi-vendor scenarios provide various benefits such as resilience, operational continuity, scalability, cost reduction, and reduced dependencies.

Scalability is one of the main challenges that QKD technologies face. Solving technical constraints such as distance limitations, integration complexity, or interoperability gaps will help to partially resolve the scalability issue, but other problems will remain that have been raised to date but not yet resolved, such as mechanisms for interconnecting QKD networks, among others. Scalability will be one of the essential and fundamental factors enabling QKD networks to grow and serve as the basis for offering real value-added services.

Cost and operational overhead are non-trivial. Dedicated fiber, environmental control, and specialised hardware contribute to CapEx and OpEx concerns. Without quantum repeaters, most deployments remain focused on high-value or high-risk links.

Authentication must still rely on classical cryptography, as QKD does not solve the initial trust problem. However, one can use QKD keys as part of an ongoing classical authentication mechanism.

Skills and readiness gaps exist across the industry. Quantum optics and cryptographic integration are not yet mainstream competencies for most telecom engineers. Initiatives such as the UK’s National Quantum Strategy are actively addressing this challenge by investing in talent development. Notably, the strategy includes funding for 1,000 postgraduate research

students in quantum-relevant disciplines (including Quantum Communications) by 2033, helping to build the skilled workforce needed to support future quantum technologies.

Certification of QKD systems is still in the early stages of development and is not yet widely established across the globe. As of the drafting of this document, South Korea hosts the only formal certification scheme, marking a significant milestone. However, there is a clear surge in interest from multiple countries, particularly in Europe, which is leading efforts to build comprehensive certification frameworks. Experts anticipate that certified QKD systems will be available by 2030, a realistic timeline given the growing momentum of national initiatives, international collaboration, and the increasing maturity of evaluation methodologies. Addressing these challenges will require coordinated industry action, further standardisation, and targeted investment to reduce complexity and operational burden.

English, French, German and Swedish authorities have therefore concluded that QKD is currently still “technologically limited” and “not sufficiently mature" for a broad roll-out but that further efforts should be made to remove current limitations [53].

Satellite QKD

There are numerous challenges associated with deploying QKD applications in space. Among these, we will focus on a subset pertaining to the unique characteristics of the space ecosystem, the security market confronting unprecedented threats, and the integration of emerging information technology trends within an environment that is often conservative:

- **Supply chain for cutting-edge technology**: because most components required for terrestrial-based (fibre) QKD are becoming more readily available, most of the components required for a space craft were simply non-existent and needed adaptation or a redesign. This is the reason why derisking this technology through a demonstrator in orbit is so crucial. Eagle-1 will provide significant experience regarding the performance of the system from adapted or tailor-made components for a QKD mission. Unlike continuous-variable QKD, in which the high maturity of components coming from the traditional (classical) optical telecom market drastically reduces the cost of the technology, systems based on satellite-based discrete-variable QKD do not yet benefit from large scale economy. A consistent supply chain strategy is a challenge to remediate bottle necks on some essential component specific to long distance QKD.

- **Interoperability within QKD suppliers, a lack of mutual effort**: there is a common interest among the telecom operators that invested in QKD technology to lower the cost of deploying the technology whilst maximising the coverage of potential customers. To achieve these goals at least two activities should be conducted in parallel:

    - Working on concept-of-operations-defining standards for QCI peering points; there is no identified initiative among the telecom operators involved in QKD technology.

    - Supporting initiatives for standard interface for interdomain peering; currently, there seems to be only one draft of a standard to organise interdomain peering (ETSI QKD GS 020). Given the complexity of QKD peering, the management and control layer will be required to support fast cyber security remediations.

    These two topics show a lack of traction for mutualised effort among telecom operators, while they would drastically lower the barrier to access costly infrastructures (such as trusted node enclaves, telescopes, etc).

- **Adoption of technology**: in security centric services, the procurement decision is mainly driven by compliance with standards, security framework or regulation. Because the maturity of these guidelines is still low, there is currently no traction for decision makers to procure and implement post-quantum cryptography solutions, be them based on PQC or QKD or a combination of both (hybrid). What is true for terrestrial post-quantum solutions is even more true for such solutions implemented in space programmes, which are usually perceived as “futuristic” and in far reach of everyday business for non-tech companies.

- **Gathering data of operational conditions, there is (almost) no precedent**: legacy space systems have a limited orchestration layer, therefore the initiative for predictive modelling was not previously considered crucial. In the case of quantum communications, collecting data to refine models of impairment would provide significant support to automate the spacecraft mission planning. Knowing in advance the probability of contact for a ground terminal on the path of the spacecraft should significantly optimise the contact time of the fleet. To achieve this, data has to be collected over a period of weeks from an in-operation QKD payload, which is one of the ambitions through the Eagle-1 demonstrator. A similar principle is expected from the next phase after Eagle-1; more security-centricity, in which collection of data and modelling of security incidents is expected to provide optimised security remediations, while lowering the false positives.

3.2.1.6 Opportunities

As quantum communications evolve, QKD presents strategic opportunities for telecom operators seeking both defensive security enhancements and competitive service differentiation. QKD enables long-term confidentiality guarantees that appeal to customers with regulatory, sovereignty, or strategic requirements. Deployments across backbone and metro links could allow telecom providers to offer high-assurance services for sensitive applications in government, finance, and healthcare. In mobile networks, QKD can be used to secure control-plane signalling in distributed architectures, particularly as 5G and 6G evolve toward disaggregation and edge integration.

Moreover, telecom operators can support cross-border data protection requirements by deploying QKD at cable landing stations and interconnecting secure regional domains via satellite or trusted-node architectures.

Cloud-native telecom infrastructures also benefit. QKD supports zero-trust designs by enabling cryptographic isolation of network slices or enterprise tenants, aligning with the needs of multi-tenant and regulated environments.

There is additional opportunity in offering “QKD-as-a-service”, with telecoms acting as trust anchors for enterprise clients seeking quantum-secure interconnects, managed keying, or colocation services. By investing early, telecom providers can shape standards, influence regulatory frameworks, and ensure that QKD technologies align with their operational models and strategic goals.

While it has been mentioned above that the importance of dark fibre is one of the main limitations of the technology, there is ongoing research into the co-existence of quantum and classical channels [54, 55].

Satellite QKD

Global Secure Communications:

- **Overcomes terrestrial limitations:** Fibre-based QKD is limited to a few hundred kilometres due to signal loss. Satellites enable secure key exchange over intercontinental distances.
- **Supports critical infrastructure:** Governments, financial institutions, and defence sectors can use space-based QKD for ultra-secure global networks.

Integration with Existing Satellite Networks

- **Leverage current assets:** Organisations with satellite constellations could integrate QKD payloads into existing platforms, reducing deployment costs.
- **Hybrid architectures:** Combining terrestrial QKD with satellite links for end-to-end secure communication.

Technological Leadership

- **Future-proof security:** Space-based QKD addresses vulnerabilities from quantum computing threats to classical encryption.
- **Innovation branding:** Being early in deploying QKD enhances reputation as a secure connectivity leader.

3.2.1.7 GSMA Role

As QKD and broader quantum communication technologies transition from research to deployment, the GSMA is well-positioned to serve as a global convener and enabler for the mobile and telecommunications industry.

The adoption of QKD in telecom networks will require more than technical readiness - it demands alignment across telecom operators, vendors, policymakers, and standards bodies. The GSMA can help bridge these communities by fostering cross-industry dialogue, aggregating best practices, and supporting the development of interoperable and scalable architectures.

Specifically, the GSMA can:

- Facilitate knowledge-sharing amongst member telecom operators to document lessons learned from early QKD pilots and deployments.
- Support the alignment of standards by coordinating telecom input to ETSI, ITU-T, ISO, and others.
- Advocate for funding mechanisms that de-risk early investment.
- Promote interoperability through reference architectures and multi-vendor demonstrations.
- Engage regulators to ensure that quantum-secure deployments align with lawful interception, sovereignty, and compliance frameworks.

- Integrate quantum security into existing GSMA working groups on fraud prevention, 5G/6G security, and network slicing.

By taking an active role, GSMA can help ensure that telecom operators are not only prepared for the quantum era, but actively shaping its secure and resilient infrastructure.

3.2.2 Quantum Physical Unclonable Function (qPUF)

3.2.2.1 Description

Authentication in every form requires secrets. These can be personal secrets like the private keys in RSA and other asymmetric protocols; or shared secrets as used with Wegman-Carter authentication and pre-shared keys. In all cases, one of the largest vulnerabilities for authentication is compromising these secrets. Specifically, the undetected theft, copying or alteration of these secrets lets an attacker impersonate the original owner of those secrets. PUFs were developed as an answer to this vulnerability.

PUFs are essentially hardware versions of one-way functions implemented through physical randomness. They take an input signal of a pre-defined type (the challenge) and impose a complex transformation on it to produce an associated output signal (the response). A Challenge-Response Pair (CRP) refers to one such input-output mapping, and the security of many PUF-based protocols relies on the unpredictability of these CRPs. These one-way functions should be high-dimensional, non-trivial to invert, and high-entropy, such that a small change in the challenge can lead to a vastly different and seemingly uncorrelated response; but for any particular challenge they always produce the same response.

The second defining property of PUFs is their physical nature. Because PUFs are, by definition, physical objects, it is much harder to conceal their removal. Adding in the unclonability provides the same guarantee for tampering or copying. In short, these features patch the vulnerability of their digital authentication counterparts. A simple and widely used example is an Static Random Access Memory (SRAM) PUF, where the random power-up state of memory cells is determined by microscopic transistor-level variations. These variations arise from uncontrollable dopant fluctuations during fabrication and are infeasible to reproduce, making the resulting pattern a stable but unclonable fingerprint.

But the unclonability is simultaneously PUFs' biggest weakness. While PUFs of many types exist, they all rely on the supposition that no fabrication technique allows for the creation of an identical copy, or even a functional copy that could perform the same one-way function with undetectable efficiency. This is a claim that is impossible to prove for most PUF types, which has traditionally put a limit on their usability.

In this section we will describe how PUF-based authentication protocols can be applied to quantum communication, especially in the context of QKD. Moreover, we will discuss how quantum physics itself can ameliorate and potentially even completely remove the main weakness of PUFs.

3.2.2.2 Use Case / Problem Statement

PUFs as a Response to the Authentication Gap
QKD, despite offering information-theoretic security, still lacks a scalable and future-proof authentication method. Current deployments rely either on PQC, which reintroduces the very computational assumptions it aims to avoid, or on pre-shared keys, which are secure but scale poorly and remain vulnerable to undetected key theft. This persistent authentication gap provides the motivation for exploring alternative mechanisms such as PUFs, which may offer

a more robust and scalable foundation for authenticating nodes in quantum communication networks. The relationship between PQC, QKD, and PUF-based authentication is illustrated in Figure 14, which highlights where PUFs can address the remaining authentication gap. For telecom operators, this is particularly relevant because PUF-based authentication offers a way to anchor device identity and trust without relying on large volumes of pre-shared secrets.

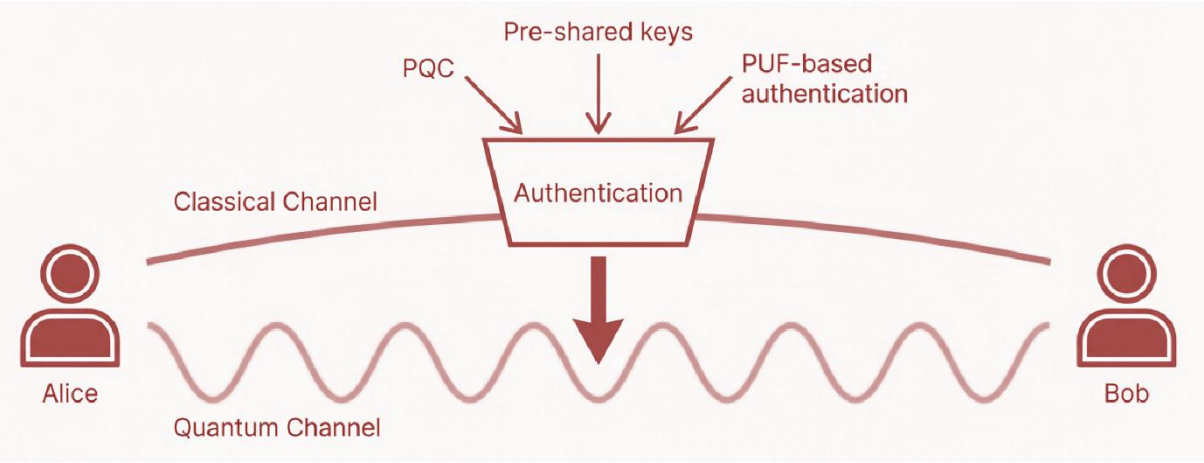


Figure 13**:** PQC and QPUF as authentication possibilities for QKD

Although PUFs have existed for decades, their impact in classical cryptography has been modest, largely because their advantages are mainly tied to their physical nature rather than to fundamentally new security properties. In the context of quantum communications, however, PUFs become significantly more interesting: quantum effects open up new ways of performing challenge-response authentication that are not available in classical systems and that align naturally with the security goals of QKD.

Because the term ‘quantum PUF’ covers several fundamentally different approaches, we treat them here as a family of related techniques rather than a single technology. To navigate this emerging landscape, we distinguish four broad categories: classical PUFs that follow the traditional challenge-response paradigm; superposition-based quantum readout PUFs that exploit weak coherent states and the no-cloning theorem; entanglement-based quantum readout PUFs that rely on correlation statistics; and fully quantum PUFs in which the unclonability arises from the PUF itself being a quantum state. Figure 15 summarises these four categories of PUFs and provides a visual structure for their taxonomy.

Category 1: Classical PUFs

The simplest way to use PUFs in quantum communication is through the familiar classical challenge-response model. During enrolment, a verifier records a set of Challenge-Response Pairs (CRPs) and later authenticates the device by issuing one of these challenges.

Classical PUFs are used in two different ways. Some, such as SRAM PUFs, generate a single device-unique key and are widely deployed as hardware roots of trust. These behave like pre-shared key systems and therefore inherit the same scalability limits; they do not support the challenge-response authentication needed in quantum communication. (In the PUF literature these are often called “weak PUFs.”) Industry activity in this space includes companies such as Fortaegis, whose silicon PUFs follow the key-derivation approach.

Other classical PUFs do support large CRP spaces and genuine challenge-response authentication. A representative example is the arbiter PUF, where manufacturing variations in delay paths determine the response to each challenge. These devices are easy to integrate electronically, but many variants have been shown to be vulnerable to machine learning modelling attacks, once an adversary can collect enough CRPs. In practice, modelling attacks

allows an adversary to learn the PUF's behaviour well enough to predict responses without possessing the device, undermining the core premise of challenge-response authentication. This modelling vulnerability is the main limitation of classical challenge-response PUFs and motivates the quantum readout approaches discussed next. (These correspond to "strong PUFs" in the literature.)

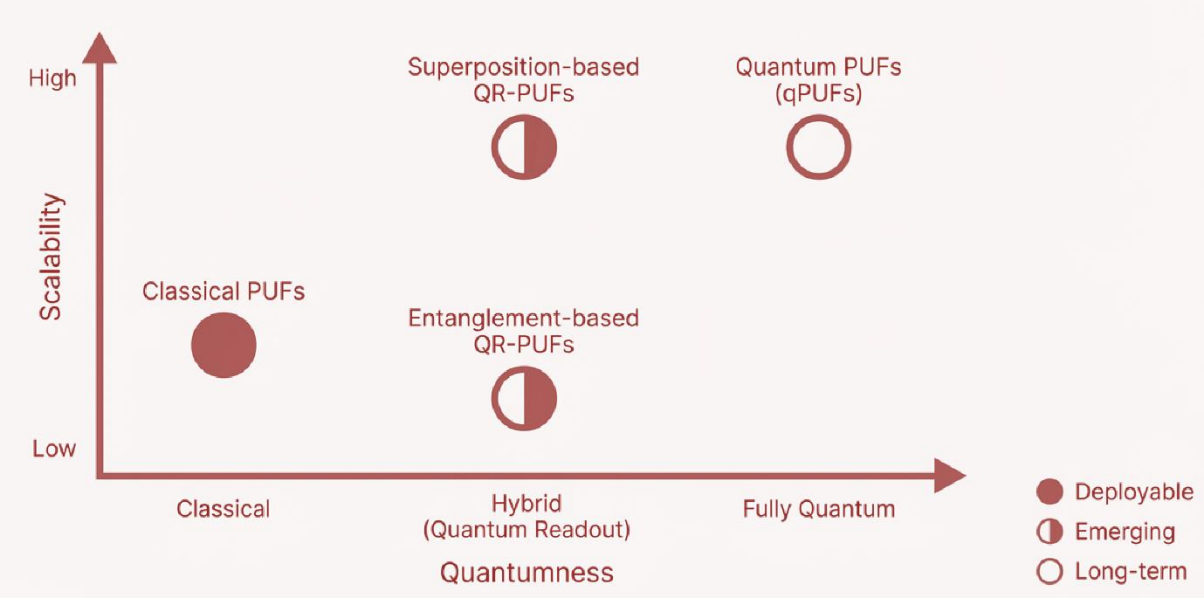


Figure 14**:** Taxonomy for physical unclonable function (PUF)

Category 2: Quantum Readout PUFs

Quantum readout PUFs (QRPUFs) extend the classical challenge-response approach by addressing its main vulnerability: susceptibility to modelling attacks. In these schemes the PUF itself remains entirely classical, but the probing signals become quantum, which restricts the information an adversary can extract. As a result, QRPUFs currently exist only in optical or photonic implementations. Much like other quantum-based communication techniques, they come in two main forms: entanglement-based and superposition-based readout. Figure 16 provides a conceptual overview of quantum readout PUFs, illustrating how quantum probes interact with classical PUF structures.

Entanglement-based Quantum Readout Physical Unclonable Function (QR-PUFs) use correlation statistics to authenticate two parties. During enrolment, two similar, but distinct, PUFs are spectrally characterised and then distributed to Alice and Bob. A source, held by either party or even by a third party, generates frequency-entangled photon pairs, sending one photon to each PUF. The resulting measurement correlations should only appear when both PUFs are in their expected locations, and the photons reach them without disturbance. This approach is being explored commercially, for example by Quantum Computing Inc. A concrete example is a pair of disordered multimode fibres, whose spectral transfer functions depend on thousands of uncontrolled scattering parameters. They are considered good PUFs because reproducing such microscopic disorder is beyond current fabrication capabilities. In addition, any attempt to intercept the entangled photons disturbs the correlations, making spoofing attempts detectable.

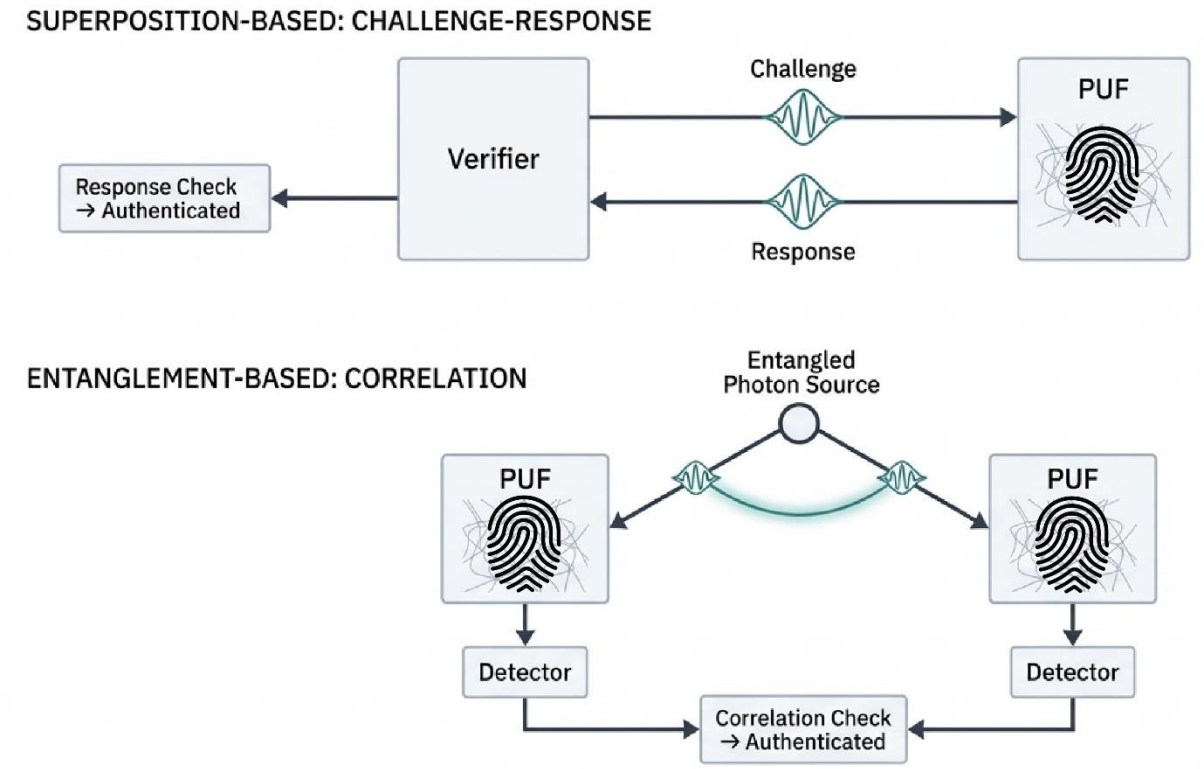


Figure 15**:** QR-PUF

Superposition-based QR-PUFs instead rely on the no-cloning theorem combined with high-dimensional challenge-response pairs. The protocol closely mirrors classical challenge-response authentication, but the challenges are encoded in signals containing far fewer photons than the number of degrees of freedom required to reconstruct them. This ensures that an adversary can never obtain enough information to infer the expected response. Superposition-based schemes are also under active development, with companies such as QSA Technology pursuing this direction. A typical example is a ring resonator based photonic integrated circuit PUF probed with weak coherent states: the challenge may be a spectral light pattern encoded across hundreds of modes, but the probe contains only a handful of photons. Such devices are considered good PUFs because the combined spectral response of many coupled resonators and waveguide imperfections is unique and practically infeasible to reproduce, while the quantum probe prevents an adversary from ever reconstructing the full challenge.

A key advantage of both of these QR-PUF variants is that their security no longer depends on keeping the PUF model secret; the schemes remain secure even if the CRP database is public, eliminating the modelling-attack vulnerability that limits classical PUFs. Superposition-based QR-PUFs additionally offer improved scalability, since any verifier can authenticate the device using the public CRP data, conceptually resembling a public-key-style system. Nonetheless, these methods still ultimately rely on the physical unclonability of the underlying PUF, which, while generally accepted as a good security prior, is still often regarded as unsatisfactory when compared to the information-theoretical security provided by QKD.

Category 3: Quantum PUFs

Quantum PUFs (qPUFs) represent the most ambitious direction in the evolution of PUF-based authentication. Rather than relying on fabrication imperfections as the source of unclonability, they aim to encode the PUF directly into a quantum state or quantum system whose properties are guaranteed by physics to be impossible to copy, measure fully, or simulate. In this

paradigm the PUF itself becomes a quantum object: its response to a quantum challenge is determined by a state that cannot be cloned, and any attempt to probe it inevitably disturbs it. This makes the interaction with other quantum states inherently unspoofable and, in principle, provides the strongest possible form of authentication.

Despite their conceptual elegance, qPUFs remain firmly in the realm of fundamental research. Proposed designs range from ensembles of non-orthogonal quantum states to systems with deliberately engineered decoherence pathways, but all share the same practical bottleneck: they require stable, long-lived quantum states and extremely high-fidelity measurements. These capabilities depend on quantum memories, quantum repeaters, and error-corrected quantum devices that are far beyond current technological maturity. As a result, qPUFs are best viewed as a long-term vision for quantum-native authentication; they are promising in theory, but unlikely to be deployable until the broader quantum-networking stack has advanced by several orders of magnitude. A representative example is a qPUF based on non-orthogonal state ensembles stored in a quantum memory. Such systems are considered good PUFs because non-orthogonal states cannot be cloned or perfectly distinguished, ensuring that any attempt to probe them irreversibly disturbs the state.

Quantum readout PUFs are also called quantum PUFs by part of the scientific community as they consider the probing with quantum states for both challenge and response a sufficient minimal benchmark. For the purposes of this document, we have chosen to go with the more conservative view and only call PUFs quantum when the unclonability itself is based on quantum effects.

Summary

The landscape of PUF-based authentication spans everything from practical, hardware-anchored classical devices to highly speculative quantum-state constructions. Each category addresses a different aspect of the challenge posed by QKD's lack of native authentication: classical PUFs offer immediate deployability, quantum-readout PUFs introduce genuine quantum resistance to modelling attacks, and quantum PUFs promise the strongest form of unclonability once supporting quantum technologies mature. Together, these approaches outline a full suite of options for establishing trust in quantum-enabled networks.

3.2.2.3 Solution

PUF-based authentication is most effective when viewed as part of a layered security architecture rather than a standalone mechanism. As quantum communication capabilities expand, scalability becomes a central constraint, and approaches that rely on distributing or refreshing secret material begin to show their limits. QR-PUFs address this by enabling authentication that remains secure even when the underlying models are public, avoiding the quadratic scaling associated with key-distribution-based methods.

Among the available approaches, superposition-based QR-PUFs are the only quantum-enhanced option with a realistic path from laboratory demonstrations to deployment in current telecom environments. They rely on weak coherent states and standard photonic components, require no entanglement distribution, and integrate cleanly with existing optical hardware.

QSA Technology's implementation follows this architecture. By combining integrated photonic PUFs with telecom-compatible weak-coherent-state probing, the system supports high-throughput, low-latency authentication without specialised quantum equipment. This provides a practical route to quantum-secure device identity today, while remaining compatible with future quantum networking developments. As the broader ecosystem evolves, this class of QR-PUFs offers a deployable bridge between classical infrastructure and quantum-native trust mechanisms.

3.2.2.4 Status of the Technology

PUF technologies relevant to quantum communications vary significantly in maturity. Classical PUFs are well-established and straightforward to integrate, but their long-term security depends on managing large CRP databases and mitigating modelling attacks. Superposition-based QR-PUFs are the most advanced quantum-enhanced option with near-term deployment potential, using only weak coherent states and standard photonic components, avoiding entanglement distribution, and supporting public CRPs, making them the only approach with a credible path to large-scale deployment today.

Entanglement-based QR-PUFs remain experimentally interesting but face substantial practical barriers, including entangled-pair distribution, synchronised detection, and dual-path stability. These requirements limit their scalability relative to both classical PUFs and superposition-based QR-PUFs. Fully quantum PUFs (qPUFs), where unclonability arises from the quantum nature of the PUF itself, remain a research-stage concept and depend on technologies such as quantum memories that are not yet suitable for telecom environments. At present, only superposition-based QR-PUFs offer a realistic route from laboratory prototypes to deployment at scale.

3.2.2.5 Challenges

Several practical challenges remain before PUF-based authentication can be adopted widely. There is currently no standardised framework for evaluating or comparing PUF-based approaches, and security guarantees are often expressed using different assumptions and metrics. Integration into existing network equipment requires clear interfaces and operational models, which are still emerging. The supply chain for photonic PUF components is developing, and long-term maintenance models for PUF-based identity anchors need to be established. These factors shape how quickly PUF-based methods can transition from demonstrations to large-scale deployment.

3.2.2.6 Opportunities

There are numerous opportunities for the application of qPUF based on the use cases mentioned in 3.2.2.2. We however leave the detailed exploration to future work

3.2.2.7 GSMA Role

As quantum communication technologies progress from research prototypes to interoperable network components, industry bodies such as the GSMA can play a pivotal role in shaping how PUF-based authentication is adopted. One immediate contribution is the development of shared terminology and classification frameworks, ensuring that classical PUFs, QR-PUFs, and qPUFs are discussed with consistent definitions across vendors and telecom operators. Beyond terminology, the GSMA can help establish interoperability profiles for PUF-enabled devices, specifying how challenge-response protocols should be integrated into QKD systems, quantum-safe key management layers, and emerging quantum network control planes.

Certification and compliance frameworks represent another important area. Because PUF security depends on physical properties that are difficult to verify remotely, standardised testing procedures, covering stability, uniqueness, modelling resistance, and quantum-readout performance, would provide telecom operators with confidence in device behaviour. The GSMA is also well positioned to convene industry and academic stakeholders to accelerate the maturation of QR-PUFs, identify realistic deployment models, and evaluate how PUF-based authentication interacts with existing PQC-based approaches. Finally, by incorporating PUF-based authentication into broader discussions on quantum-safe network architectures, the GSMA can help ensure that future quantum communication systems balance scalability, interoperability, and long-term security in a coherent and globally aligned

way. With clear standards and coordinated development, PUF-based authentication promises to become a practical and scalable component of future quantum networks, helping ensure that trust keeps pace with the capabilities of the technologies it protects.

3.2.3 Quantum Networking (incl. Entanglement Networking)

3.2.3.1 Description

Quantum entanglement is a non-classical correlation between particles (i.e. photons) such that the state of one particle instantaneously affects the state of another, regardless of the distance separating them. This phenomenon defies classical intuitions about locality and causality and is central to a range of quantum communications protocols. Quantum entanglement networking is emerging as a transformative technology for the telecommunications sector. By enabling fundamentally secure communication and laying the groundwork for the quantum internet and future networks, entanglement networking offers telecoms a strategic opportunity to lead in next-generation infrastructure. Deployment of a large-scale network of distributed entanglement enables a wide range of use cases across quantum technologies, including, but certainly not limited to:

- **Quantum communications:** entanglement-based QKD, such as the Ekert 91 [80] or BBM92 [42] QKD protocols. Entanglement-based QKD is often preferred over standard (non-entanglement-based) QKD due to the increased security offered as a result of avoiding many side-channel attacks present in standard QKD protocols, as well as removing the need to trust repeater nodes.
- **Quantum computing:** connecting distributed quantum computers via entanglement to increase the overall computational power – this can be done locally (i.e. within a data centre) or non-locally. Entanglement can also be used for blind quantum computing, in which a quantum computing end-user is able to connect to a device and perform quantum computation algorithms without the hardware (and therefore quantum computing vendor) knowing the output of the result, which is highly important for IP-sensitive calculations.
- **Quantum sensing:** precise detection and fault monitoring (stress, temperature, etc.) in fibre networks in telecoms (and other, such as gas and water) infrastructure, as well as quantum radar systems and radio-frequency quantum sensor networks. Entangling distributed quantum sensors enhances measurement sensitivity and accuracy.
- **Quantum position, navigation and timing (PNT):** entangled photons can enhance timing precision and synchronisation across telecom networks, which could replace or augment GPS for ultra-precise timing in 5G/6G networks, especially in GPS-denied environment. Quantum-time transfer can be used for ultra precise and secure time synchronisation in telecom networks (via satellite or over fiber).

Quantum networking marks the beginning of a new communication paradigm, enabling the transmission of quantum information between distant nodes and unlocking capabilities such as distributed quantum computing, ultra-low-latency communication, and advanced physical-layer processing. Beyond security, these networks support the sharing of entanglement and true quantum randomness as computational resources, powering applications like synchronised clocks, shared quantum states, and hybrid quantum-classical systems. This creates a path for integrating quantum processors across networks, enabling collaborative quantum computation and boosting classical systems with quantum enhancements at the edge.

For the telecom industry, investing in quantum networking is a strategic move towards building infrastructure that supports low-latency services, analogue signal processing at the physical layer, and the seamless integration of quantum technologies into existing fibre networks, positioning telecom providers at the core of tomorrow’s quantum internet.

The quantum internet envisions a global infrastructure for generating, distributing, storing, and exposing entangled quantum states between users and devices. By leveraging entanglement as a shared resource, it enables communication models and applications (such as quantum teleportation, enhanced sensing, and distributed quantum computing) that are impossible with classical networks. Telecom operators are uniquely positioned to lead this evolution by offering "entanglement-as-a-service" at network nodes. Through managing entanglement distribution across their fibre infrastructure, telecoms can enable powerful quantum applications and emerge not just as data carriers, but as essential providers of next-generation quantum connectivity.

Entanglement-as-a-service is built on two core architectural building blocks: the *distribution* and the *exposure* of entangled quantum states. It is the responsibility of the network provider to manage and expose entangled states stored at quantum internet nodes, making them accessible to quantum applications. Entanglement is established between neighbouring network nodes through specialised quantum communication protocols - specifically the "node sends photon" and "node receives photon" protocols. In the “node sends photon” protocol, a quantum internet node prepares an atom of a quantum memory entangled with a photon and transmits the photon to another node or a central station. In the “node receives photon” protocol, a node is designed to capture incoming entangled photons and entangle them with atoms of its local quantum memory. To connect distant nodes, entanglement swapping is used, enabling the creation of pairwise entangled states across the entire network. The quantity and placement of these entangled pairs are driven by traffic matrices that reflect the demands of quantum communication protocols. Once entanglement is distributed and stored in quantum memories, the next step is “exposure”, allowing quantum applications to access and consume these entangled states for tasks such as teleportation, distributed computation, or coordinated sensing.

Quantum communication applications leverage entangled and photonic quantum states in various ways, depending on their functional and architectural needs. These applications can be grouped into distinct categories based on their interaction with the quantum network infrastructure:

- First, some applications consume entangled quantum states (such as QKD)—by requesting entanglement from the provider, which then delivers the required pairs to the endpoints.
- Second, applications may load photonic quantum states into the network’s quantum memory; these stored states can later be teleported to target nodes, enabling integration of remote quantum processors or memory networks.
- Third, applications may request entanglement swapping, whereby the provider hands over ready-to-use, remotely entangled quantum states; this allows applications to perform quantum communication protocols independently of the network infrastructure.
- Fourth, classical messages can be sent to the provider for conversion into quantum communication protocols, such as superdense coding or hybrid classical-quantum messaging, allowing enhanced communication capacities.
- Finally, applications may request the provider to establish dedicated quantum channels, bypassing teleportation, when a direct transmission of quantum states is required, such as in real-time analogue quantum communications, or when specific physical-layer characteristics are desired.

To enable entanglement-as-a-service as a reliable and scalable offering, a comprehensive suite of protocols must be established to manage the interaction among the various technical

building blocks within the provider-operated quantum infrastructure. This includes physical-layer protocols for photon transmission and entanglement generation, as well as classical control protocols to coordinate timing, synchronisation, and error handling across quantum internet nodes. Additionally, robust access management mechanisms are required, covering both classical and quantum APIs, to enforce authentication, authorisation, and role-based access control for users and applications interfacing with the network. Beyond internal infrastructure management, a separate layer of interoperability protocols is needed to define and govern the classical and quantum interactions between third-party quantum applications and the provider infrastructure. These protocols must handle entanglement requests, state loading, channel establishment, and data exchange, ensuring secure, reliable, and policy-compliant operation across heterogeneous systems and administrative domains.

A critical aspect of entanglement distribution in quantum networks is heralding. For quantum storage devices, it is essential to know precisely when a photon will arrive so it can be captured and stored with high fidelity. Similarly, Bell state measurements (BSMs), which areused for entanglement swapping, must be tightly synchronised to ensure that incoming photons arrive at the same time and overlap coherently, enabling proper quantum interference. Achieving this level of coordination requires picosecond-level timing precision to manage heralding signals, activate detector gates, and implement accurate time binning. Because of these stringent timing requirements, entanglement networks depend on dedicated time synchronisation infrastructures that go beyond conventional methods. One promising solution is OTT-ELSTAB, an optical time transfer technology that enables sub-picosecond synchronisation across fibre links. Integrated into quantum internet architectures, such technologies are essential for maintaining the coherence and performance needed for reliable entanglement-based communication.

Classical network links also play a vital role as an integral part of quantum communication protocols. For instance, QKD, classical channels are used for key sifting, error correction, and verification processes that complement the quantum transmission. These classical links must deliver high speed, low latency, and high bandwidth to support real-time coordination and data exchange across the quantum network. Results from BSMs need to be promptly broadcasted to all participating nodes to signal successful entanglement swaps and enable the correct progression of quantum protocols. To meet these demanding requirements, classical DWDM technology is well-suited, providing robust, scalable, and low-latency communication over existing fibre infrastructure alongside quantum channels.

3.2.3.2 Use Case / Problem statement

The future quantum internet will support a wide range of quantum communication applications that leverage the unique properties of entanglement and quantum states. Key examples include:

- **Quantum key distribution:** Secure generation and sharing of encryption keys with unconditional security guaranteed by quantum mechanics.
- **Quantum teleportation:** Reliable transfer of quantum states between distant nodes, enabling distributed quantum computing and secure information transfer.
- **Distributed quantum computing:** Connecting quantum processors across the network to perform complex computations collaboratively.
- **Quantum clock synchronisation:** Ultra-precise synchronisation of clocks over long distances, improving timekeeping for navigation and communication systems.

- **Quantum sensing and metrology:** Enhanced sensitivity and accuracy in measuring physical parameters through entangled sensor networks.
- **Superdense coding and hybrid protocols:** Increasing classical communication capacity by encoding more information into fewer quantum bits and integrating quantum-classical data transmission.

Use cases for quantum networking can include decision coordination, ultra-precise time synchronisation, secure position verification, and eavesdropper-proof security [56]. Another key use is the distribution of true quantum random numbers across network nodes, providing a fundamental resource for security protocols such as wiretap codes, identification codes, and data compression or decompression codes. Additionally, quantum computation integrated at the physical layer can significantly reduce network latency by performing analogue computations directly on quantum states, eliminating the overhead of classical virtualization layers and improving computational precision at the node level. The quantum internet also opens the door to new cryptographic primitives (such as quantum bit commitment, oblivious transfer, and secure multiparty computation) which enable collaborative tasks like joint network traffic analysis among competing providers, allowing detection of shared threats without revealing a provider's sensitive information. Finally, quantum sensing stands to benefit greatly, as quantum sensors generate quantum states from measurements that can be teleported to central quantum processors for collective analysis, creating large-scale coherent sensor networks capable of highly precise and coordinated measurements across vast distances.

3.2.3.3 Solution

To enable entanglement networking, several components are needed, which are not yet broadly available (entanglement generators, quantum switches, quantum memory etc.). Nevertheless, entanglement-based quantum networking is evolving from theoretical promise to first prototypes and implementation. For example, Cisco recently unveiled its Quantum Network Entanglement Chip. The chip, developed with UC Santa Barbara, generates high-fidelity entangled photon pairs at telecom wavelengths, operates at room temperature, and consumes less than 1mW of power, making it suitable for scalable deployment.

3.2.3.4 Status of the Technology

Many key components for quantum networking still only exist in research labs or as prototypes, and, as such, still need to mature before quantum networking can be deployed on larger scales. In parallel, architectures and conceptual frameworks must be developed. The IETF Draft [43] proposes a multiplane reference architecture for the quantum internet, aiming to provide a consistent and adaptable framework for integrating quantum communication technologies with existing internet infrastructure. The architecture emphasises agility to accommodate evolving quantum technologies, sustainability in terms of open and economical availability, and pliability for seamless integration with current network operations and management. Drawing on experience from QKD deployments, the proposal seeks to unify diverse technological efforts and support the development of quantum-enabled applications

3.2.3.5 Challenges

Despite these early-stage quantum networks beginning to exist, there still exist significant challenges and limitations to overcome before truly large-scale entanglement networks exists, such as:

Challenge	Description	Mitigation
Distance Limitations	Entanglement fidelity decays over distance due to photon loss and decoherence.	Use of quantum repeaters and satellite-based links. Another mitigation technique for overcoming distance limitations is to is to enhance the detection capabilities by employing for instance SNSPD detectors instead of SPAD detectors [48, 57].
Hardware Immaturity	Quantum memories, detectors, and repeaters are still in early-stage development.	Invest in R&D and collaborate with quantum hardware startups and vendors.
Synchronisation	Requires precise timing and coordination between quantum and classical channels.	Use atomic clocks and advanced synchronisation protocols.
Cost and Scalability	High initial investment and operational complexity.	Start with high-value use cases which offer the highest cost-to-benefit trade-off.

Table 6: Quantum Networking Challenges

3.2.3.6 Opportunities

There are numerous opportunities for the application of quantum networking based on the use cases mentioned in section 3.2.3.2. We however leave the detailed exploration to future work.

3.2.3.7 GSMA Role

To support the development and uptake of quantum networking, GSMA can play a crucial role in standardisation with this entirely new way of networking, standards have yet to be defined to ensure interoperability of quantum networking devices and quantum computers. As quantum networking is still in a very early stage, a significant contribution to the field can also come from creating awareness and supporting PoCs.

3.2.4 Quantum Communication for Distributed Quantum Computing

3.2.4.1 Description

Quantum communication leverages the principles of quantum mechanics to enable ultra-secure data transmission, distributed sensing, and novel networked services and applications.

Research and innovation activities aimed at building a large-scale quantum internet, integrated with the current internet, are showing the challenges and the opportunities of

scalable and efficient computation capabilities embedded within the communication infrastructure.

Centralised quantum computing architectures, while powerful, face severe limitations related to maintenance costs, scalability, resilience and energy resource constraints (e.g., for cooling). Distributed Quantum Computing (DQC) emerges as a compelling solution to these challenges. In DQC, multiple quantum nodes, each with limited local resources, collaborate to perform computations through quantum networking and classical communication. This paradigm promises enhanced performance, resilience, and adaptability, especially when applied to quantum communication networks.

Looking beyond the goal of fault-tolerant quantum computing, networking quantum computers through a quantum computing internet will enable scalable quantum compute clusters, larger data centres and geographically distributed networks. IBM has initiated collaborations with governments, academia, and business partners to research and develop the components required to build distributed quantum computers, and in the future, a quantum computing internet. The recent announcement of a partnership between IBM and Cisco [58] is a critical step on this journey, focussing on transducers and optical links between QPUs. IBM and Cisco aim to demonstrate the first proof-of-concept for a network that combines individual, large-scale, fault-tolerant quantum computers, enabling them to work together to run computations over tens to hundreds of thousands of qubits by 2030.

3.2.4.2 Solution

DQC is an architectural paradigm wherein multiple spatially separated quantum nodes, each comprising quantum processors, quantum memories, and interfacing hardware, work collaboratively over a quantum network integrated with a classical network.

At the core of DQC is the use of quantum entanglement as a communication and coordination resource. Entangled qubits can be shared between nodes to facilitate quantum teleportation, distributed algorithms, and joint state manipulations without requiring direct transmission of quantum states. This property enables the realisation of collective operations across geographically separated quantum systems.

DQC systems can adopt various computational models, including client-server architectures, peer-to-peer arrangements, or hybrid schemes involving centralised control and decentralised execution. The choice of model often depends on the target application, network topology, and technological capabilities of the quantum hardware.

3.2.4.3 Status of the Technology

The successful deployment of DQC within quantum communication networks hinges on a well-integrated technological foundation. A robust infrastructure must combine quantum hardware, networking protocols, classical control systems, and software orchestration layers.

Key implementation considerations include:

- **Quantum hardware and node design**: Each quantum node in a DQC system must integrate quantum processors, quantum memories, and photon-based interfaces for entanglement distribution. Hardware platforms vary, including superconducting qubits, trapped ions, photonic qubits, and nitrogen-vacancy centres, and the choice affects coherence times, fidelity, and networking feasibility.

- **Quantum interconnects and repeaters**: Long-distance quantum networking requires high-efficiency optical interconnects and quantum repeaters capable of performing entanglement swapping and error correction. These components must minimise photon loss, mitigate decoherence, and support multiplexing for scalability.

- **Hybrid quantum-classical coordination**: Effective DQC requires a tight integration between classical and quantum systems. Classical control systems manage scheduling, synchronisation, and error feedback loops. Low-latency, high-bandwidth classical channels are essential for real-time coordination.
- **Network synchronisation and timing**: Quantum operations across distributed nodes must be time-aligned to within nanoseconds or less. This requires precision timing protocols and potentially GPS-based or optical clock synchronisation across nodes.
- **Middleware and orchestration software**: A scalable DQC environment necessitates software layers that abstract quantum resources and coordinate operations across multiple nodes. This includes quantum operating systems, distributed compilers, resource schedulers, and fault-tolerant execution frameworks.
- **Security and fault tolerance**: As quantum networks scale, they become increasingly susceptible to errors and malicious threats. Implementing quantum error correction codes, secure classical channels, and quantum authentication protocols is vital to ensure operational integrity.
- **Standardisation and interoperability**: The lack of unified standards for quantum interfaces, protocols, and APIs poses a barrier to widespread adoption. Developing industry-wide standards is essential to ensure cross-vendor compatibility and efficient integration.

Real-world efforts such as the DARPA Quantum Network Testbed, the IBM Quantum-Safe Network, and the EU Quantum Flagship initiatives are actively exploring these infrastructure components.

While DQC is still in infancy, several experimental efforts and simulations have demonstrated its foundational viability. These case studies highlight how DQC principles are beginning to take form in both laboratory and network testbed environments.

- **IBM Quantum-Safe Network demonstrations**: IBM has demonstrated basic distributed quantum protocols across nodes within its quantum network, showcasing entanglement distribution and teleportation using cloud-accessible quantum processors. These experiments validate real-time coordination across geographically separated qubit systems and the use of classical-quantum control integration.
- **QuNetSim and NetSquid simulations**: Software platforms such as QuNetSim and NetSquid allow for the modelling and simulation of quantum network behaviour. These tools have been used to evaluate performance metrics of DQC scenarios, such as latency in entanglement distribution, routing efficiency, and fault tolerance across quantum nodes.
- **European Quantum Internet Alliance (QIA) pilots**: The QIA has established testbeds where simple DQC tasks, such as entanglement-based key distribution and quantum state sharing, are being tested between nodes spanning multiple institutions. These efforts are key to scaling up from point-to-point quantum links to meshed quantum network topologies.
- **Secure Multi-Party Computation (SMQC) prototypes**: Several research groups have implemented early versions of secure distributed quantum protocols, including secret sharing and joint quantum operations across independent nodes. These prototypes are essential for validating the security and correctness of SMQC use cases within quantum communication frameworks.

These case studies demonstrate that while DQC is still in a developmental phase, meaningful progress is being made toward its practical application in quantum networks. Further advancements in quantum memory stability, gate fidelity, and inter-node synchronisation will be crucial to moving beyond experimental validations toward production-level deployments.

3.2.4.4 Challenges

Despite its promise, DQC faces significant challenges. Quantum decoherence, error accumulation, synchronisation complexity, and the need for high-fidelity entanglement all present technical barriers. Moreover, the development of standardised protocols and interfaces for interoperability remains an open research area. Addressing these challenges is critical to realising the full potential of DQC in quantum communication networks.

These challenges span technical, theoretical, and operational domains:

- **Quantum decoherence and error rates**: Quantum systems are highly sensitive to environmental noise, leading to decoherence and operational errors.
- **Scalability of entanglement distribution**: Creating and maintaining entangled links across many nodes remains a significant obstacle.
- **Synchronisation and latency**: Distributed quantum operations often require precise time coordination.
- **Interoperability and standardisation**: Current DQC implementations are highly dependent on the specific hardware and communication models used.
- **Security in hybrid classical-quantum environments**: While quantum communication provides strong theoretical guarantees of security, integrating DQC into classical infrastructure introduces new vulnerabilities.
- **Resource management and scheduling**: Unlike classical systems, quantum resources such as qubit coherence time, entanglement links, and quantum memory are limited and fragile.
- **Theoretical models and algorithms**: Many classical distributed computing models do not translate directly into quantum analogues.

3.2.4.5 Opportunities

As quantum communication networks expand in scale and complexity, DQC is poised to play a pivotal role in enabling advanced capabilities across these systems. DQC can be leveraged not only to enhance performance and scalability but also to solve problems inherent to long-distance quantum communication and multi-party coordination.

One of the most immediate opportunities of DQC lies in entanglement management and distribution. Maintaining high-quality entangled links over a wide-area network requires adaptive, intelligent routing and coordination between quantum repeaters and intermediary nodes. DQC enables these nodes to collaborate in real time, running distributed algorithms to optimise entanglement paths, perform entanglement swapping, and coordinate error correction across the network.

DQC also enhances the execution of quantum communication protocols, such as QKD, by distributing the cryptographic workload and facilitating scalable key management in multi-user environments. In future quantum networks, secure group key distribution and continuous key renewal may require coordinated computation across geographically dispersed nodes, which is a task well suited to DQC architectures.

Another opportunity is to deploy secure multi-party quantum computation, in which different parties perform computations on shared quantum data without revealing their private inputs. DQC provides the necessary platform for orchestrating such protocols efficiently and securely across an interconnected quantum infrastructure.

Furthermore, DQC will underpin emerging quantum applications such as quantum-enhanced consensus algorithms, federated quantum learning, and distributed quantum sensing. Each of these applications depends on the ability to process and share quantum information securely and efficiently between multiple sites.

3.2.4.6 GSMA Role

In summary, DQC is not merely a computational paradigm but an enabling infrastructure that enhances the performance, security, and resilience of future quantum communication systems.

GSMA's role could be to explore in more details the fundamental principles, enabling infrastructure, and emerging applications of DQC within the context of quantum communications. Areas of interests to be monitored include scalable entanglement routing, secure hybrid protocol stacks, quantum-aware network operating systems, and the practical realisation of quantum repeaters and routers with integrated computation. In this sense GSMA's role could also be collaborating in the maturation and standardisation of middleware and orchestration platforms for DQC.

3.3 Quantum Entropy

3.3.1 Description

Entropy is common scientific term borrowed from statistical physics to refer to a way of exactly quantifying uncertainty. Quantum entropy, or quantum randomness, is a concept that has accompanied quantum physics almost from its very inception and is now of the most active areas of applications of quantum technologies. Usually considered in relation to quantum communication schemes such as QKD, it is important to note that Quantum Random Number Generators (QRNGs) are not just an enabling tool for quantum communications. QRNGS have much broader use cases across cybersecurity as a foundational block to any cryptographic protocol (whether traditional, quantum-based, or post-quantum). As such, it's more useful to consider QRNGs separately to quantum communications to better understand how they may be used across the spectrum of cryptographic tools and systems deployed within a telecommunication network.

3.3.2 Use Case / Problem Statement

3.3.2.1 Entropy Starvation Attacks from Poor Entropy

Fundamentally, cryptography is all about keeping information secret from third party access. The various tools, algorithms and protocols which have been developed within that field revolve around the concept of making sure that information is kept private whether in transit (while it is being communicated from one location to another) or at rest (while it is kept on some storage system). There are many different elements that make up any particular cryptographic protocol, however, one of the main common denominators across all of them is randomness.

Randomness is used to create the certificate, keys, nonces and other cryptographic primitives that are of essential importance to the correct functioning of any cryptographic system.

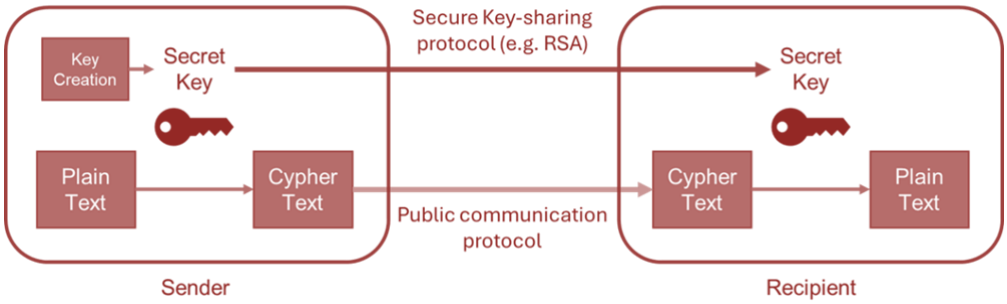


Figure 16**:** Basic representation of how a symmetric key encryption protocol, such as AES, functions. The shared secret itself needs to be securely transmitted through a dedicated protocol which requires even more randomness

Due to its importance in cryptographic systems, reliably generating randomness is a task that has become heavily regulated, and on which a significant amount of research has, and continues to be, carried out. In general, random number generators can be classified into two main categories:

1. **Software-based random number generators:** This class of generators, sometimes also called Pseudo-Random Number Generators (PRNGs) or Deterministic Random Bit Generators (DRBGs), relies on deterministic algorithms to produce a stream of bits that are distributed in such a way to appear uniformly random. This class of generators cannot truly create any randomness of its own, and it is completely dependent on the randomness brought by the seed. Throughout this document, this class will be referred to as DRBGs.

2. **Hardware-based random number generators:** This class of generators relies on the unpredictable nature of some real-world physical processes. Usually, these generators utilise specialised hardware components, such as ring oscillators or noisy diodes, whose behaviour is difficult to predict. There are many different terms for this class of generators, however throughout this document, it will be referred to as a “hardware entropy source” (HES).

Due to the great variety of possible methods for generating randomness, a number of cryptographic standards have been developed to define basic regulations around how RNGs can be constructed. These standards are maintained by organisations such as the National Institute for Standards and Technology (NIST) in the US and the Federal Office for Information Security (BSI) in Germany. Currently, the most common approach is to combine an Hardware Entropy Source (HES) with a DRBG being seeded by randomness extracted from the HES. This means that the properties of each need to be considered carefully to ensure the security of the whole end-to-end system.

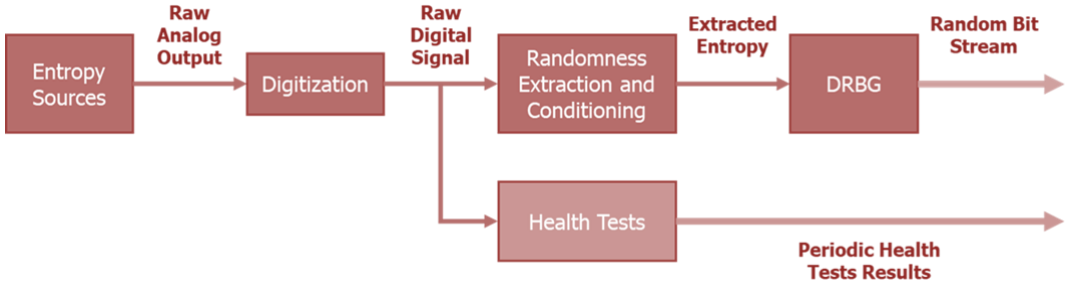


Figure 17: Basic Diagram of an HES seeding a DRBG.

In investigating the security and reliability of any RNG system, the HES is of essential importance as the entire stack depends on it. Additionally, it tends to be the most complex part

since it relies on hardware implementations and not an algorithmic definition. As mentioned above, various HESs have been developed and tested over the years. However, there are still frequent issues that occur, even with the ones that follow the guidelines that exist. Some recent examples include:

- HESs producing insufficient entropy generated by the HES in the ASA firewall appliance (as reported by NIST in 2019 and 2023)
- Entropy loss in RSA keys generated by trusted platform modules (TPMs) (as reported by a Masaryk University group in 2017)
- Insufficient entropy in the generation of cryptographic certificates and tokens by IoT devices (as reported by Keyfactor in 2019)
- Vulnerability in the HES of the Taiwan government smartcard (as reported in 2013)

The most common causes of vulnerabilities, related to insufficient entropy being generated, are either a mis-assessment of the entropy that can be created in the system or a so-called “entropy starvation”, in which the system is incapable of generating enough entropy. With the advent of commercially meaningful quantum hardware components, the research on HESs has moved towards quantum physics to see if this can provide a way to build a better source.

3.3.2.2 Certification of QRNGs

Existing certification frameworks exist for RNGs used in cryptographic applications. These include: NIST SP 800-90B, FIPS 140-3, and Common Criteria. The stringent requirements they impose remain a significant challenge to the commercialisation of certain types of QRNG architectures. These standards demand rigorous testing to ensure that entropy sources consistently produce high-quality randomness under all operating conditions.

In most cases, demonstrating compliance involves not only statistical validation of the entropy output, but also comprehensive documentation of the design, implementation, and health monitoring mechanisms. In addition, certification bodies typically require consistent and reproducible test results, along with long-term reliability evaluations. Such requirements can be particularly demanding for entropy sources susceptible to environmental variations or component aging. These technical and procedural demands, combined with the associated costs, are a hurdle that QRNG developers must overcome to bring users the real benefits of true randomness, that QRNGs can bring to cryptographic solutions over existing pseudo-RNGs and classical hardware-RNGs.

The UK National Cyber Security Centre (NCSC) pinpointed in their 2025 whitepaper on Quantum Networking Technologies that for cryptography, QRNGs could have “the ability to rapidly detect degradation of the source through precise modelling of the quantum components, something that classical sources do not routinely offer”. As will be described below, an array of approaches to build QRNGs exist – not all QRNGs are created equal. For users concerned about the quality of the random numbers coming from a QRNG, the important metric is whether a QRNG allows live entropy verification.

3.3.3 Solution

Over the past 100 years, a class of physical processes was discovered which are governed by very different laws. This was the dawn of quantum physics and the systems that it describes. One of the primary differences is that the outcomes of quantum processes are completely probabilistic. Even the simplest, most basic quantum system has stochastic outcomes; they

cannot be predicted exactly no matter how much additional information one acquires about the system.

For example, consider the system composed of a photon (an individual particle of light) impinging on a beamsplitter (an optical component that lets some light through and reflects the rest). Even when considering the ideal version of each of the components of this system, and assuming one has full control over it in its entirety, the outcomes of any measurement performed after the beamsplitter will be completely random.

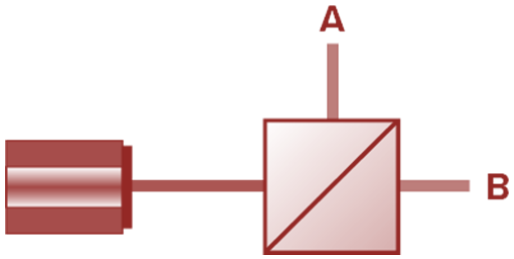


Figure 18**:** Schematic of beam splitter

Figure 19 shows the principle. A source of photons (left) sending a beam of photons impinging on a balanced beamsplitter (centre light blue object). Each photon then has an independent chance of being reflected or transmitted each with a 50%. Therefore, if one were to try to detect the photons at points A or B, it will always be a 50% probability of occurring and there is no additional information that can be gotten about the source, the beamsplitter, or the detector that can change that.

In fact, the main framework of quantum physics is designed to model the evolution of the probabilities of the difference outcomes of measurements done on quantum systems. As such, researchers have looked to use these processes to create QRNGs.

3.3.4 Status of the Technology

Like with other quantum technologies, QRNGs have a large variety of form factors, underlying physics and performance capabilities, such as:

- **Photonic systems:** These systems rely on the interactions and measurements that can be done with light.
- **Electronic systems:** These systems rely on the behaviour of electrons as they move around circuitry.
- **Quantum computers:** Although quantum computers are generally designed to solve hard computational problems, one of their secondary applications is the generation of randomness by leveraging their internal quantum processes.

Other than the underlying physics, another important consideration is the form factor of the QRNG. Currently, the most common QRNG form factors are:

- **Server racks:** here the QRNG is packaged in a standard rack-mountable server. This is usually used for bulky systems or ones that need very high-speed interfaces.
- **PCIe cards:** here the QRNG is mounted on a printed circuit board (PCB) which can then be slotted into a standard peripheral slot found on most motherboards.
- **Chips:** here the QRNG is implemented directly onto an embedded chip that can then be integrated into any kind of hardware system using the appropriate interfaces and packaging.

An important consideration when looking at the form factors is whether what is being implemented is the entire RNG or just a quantum entropy source. This distinction is important since the entropy source on this own cannot directly be used for cryptographic applications, it simply forms a part of a much larger system.

QRNG Access Style

In addition to the form factor, QRNGs can either be integrated into a crypto-system as physical hardware or they can be cloud-hosted. The latter is sometimes referred to as Quantum-Entropy-as-a-Service (QEaaS), building upon the original concept of EaaS, developed by NIST.

3.3.5 Challenges

The above analysis is merely a highly simplified description. In reality, like all physical systems, there is no such thing as an ideal “quantum system". In all physical processes, there is usually a quantum and a classical aspect to how they operate. The main distinction is which behaviour is more dominant. For example, the above-mentioned light interaction, albeit fundamentally quantum mechanical, will necessarily include a lot of the classical noise present in any optical system: the imperfections in the optical devices, the unreliability of the photon sources and the unavoidable internal noise of any detector system designed to measure it. What are then the advantages of QRNGs?

The primary challenge with traditional entropy sources is that they are completely dependent on the correct functioning of their internal components. This is what is usually called full device-dependence. Assumptions are made about the amount of entropy that is being produced, as well as its rate, based on the expected behaviour of the components of the system.

Quantum mechanics offers a way out of this limitation; by exploiting certain aspects of quantum theory, one can construct architectures that have various degrees of device independence:

3. **Full device-independence:** In these kinds of architectures, one can certify a certain amount of entropy from the system without assuming anything about the individual components with which it is made. Merely the quantum measurements are sufficient. In practice however, this is exceedingly difficult to achieve reliably and usually results in interminably slow bitrates, and very complex hardware implementations.
- **Semi-device independence:** With these architectures, the user still needs to trust some elements of the device while being completely free from any assumptions about others. This is much more achievable in practice and allows users to abstract from notoriously unreliable hardware elements such as quantum sources.

In short, device independence, with all its varieties, offers users a tangible measurable way to improve the reliability and quality of the entropy sources that they are using in their encryption stacks. Currently, most QRNG systems are still fully device-dependent with a few recent systems offering differing levels of device-independence. This is due to the complex nature of designing and building the latter in a way to make it practically useable.

3.3.6 Opportunities

QRNGs serve as the basis of any type of cryptographic protocol that a telco wishes to deploy in their networks. As part of a larger system, QRNGs would not be used on their own within a cybersecurity system but as an enabling component forming the backend infrastructure of such systems. As such, QRNGs can be integrated with a wide variety of cryptosystems such as Hardware Security Modules (HSMs), firewall systems, Virtual Private Network (VPN) servers and routers, among others. Additionally, QEaaS can be used to distribute secure quantum entropy to connected low-resource IoT devices that need entropy for their

applications but that cannot be physically connected to a reliable source or have one embedded within them.

A QRNG's main purpose is to generate trusted and verifiable encryption keys which can be used for traditional cryptographic applications, or to enable quantum-secure schemes such as QKD or PQC algorithms.

QRNGs in Classical Security Solutions:

- **QRNG hardware rackmount and PCIe:** UK scale-up, iQuila, known for pioneering the Virtual Extended Network (VEN) protocol, a more secure and faster alternative to the IPsec protocol used by VPNs, uses Quantum Dice QRNGs. The VERTEX QRNG is used in iQuila's SDN solution [59], allowing customers to benefit from an enhanced level of protection of their encrypted data packets as they pass over the public internet.

4. **Quantum entropy-as-a-service (QEaaS):** US-based MNO AT&T demonstrated with Quantum Dice in the GSMA Foundry Pavillion at MWC Barcelona 2025 [60] how carrier-grade infrastructure could be leveraged as a crypto-agile QEaaS platform when powered by high generation rate QRNGS with live entropy verification. This sets the scene for making QEaaS a standard platform in mobility, whilst offering end-users a selection (or combination) of multiple entropy sources. QEaaS ensures that even the most resource-limited devices and cloud instances receive the secure, certified randomness they need to implement all their cryptographic functions.

QRNG Chips:

One example of QRNG chip deployment is the Quantum Dice and SCI Semiconductor collaboration [62] to co-develop quantum-enhanced semiconductor cryptography systems for use in securing critical infrastructure, telecommunications, industry 4.0, and beyond. SCI Semiconductor selected Quantum Dice's QRNG technology with live-entropy verification, specifically for use within the SCI Semiconductor's Capability Hardware Enhanced RISC Instructions (CHERI) technology.

Another notable example of QRNG chip integration into real-world applications is ID Quantique's Quantis QRNG chip, which has been used by Samsung to enhance trusted authentication and data encryption in the Samsung Galaxy Quantum 6 [62].

QRNGs in Post-Quantum Security Solutions:

QKD require QRNGs, and QRNGs can also be used for one-time pads in certain PQC deployments. ID Quantique and Quantum Dice are examples of two QRNG vendors who have supplied space-suitable QRNGs for satellite-QKD missions, the EAGLE-1European satellite-QKD mission and the SpeQtral-1 UK-Singapore satellite-QKD missions respectively. These are examples of commercial QRNG deployments in advanced secure communication infrastructure.

3.3.7 GSMA Role

GSMA will play a critical role in the development, adoption and access to QRNG technology for the telecommunication community. This can be divided into the following:

- **Standardisation:** Like with any sector, telecoms have their own requirements and constraints depending on where the technology will be deployed (whether on the server side or on the edge).
- **Market education:** GSMA will have an essential role in demystifying some of the claims around QRNGs and clarifying the terminology often used when speaking about them.

- **Adoption:** RNGs have a wide range of specific use cases (from PKI to VPNs among other cybersecurity use cases). The GSMA will work to explain and show to telco users how the integration can work.

5. **Access:** QRNGs can bring benefits to both large and small telco operators. However, the latter may find it difficult to acquire and deploy such solutions. GSMA could offer a shared QRNG resource that would provide telcos with the ability to leverage the benefits of QRNGs without having to deploy them themselves.

3.4 Quantum Sensing

Next to quantum computing, quantum communication and quantum entropy, quantum sensing is another use case for quantum technologies with potential applications in the telecom context. Potential applications are improved RF sensing as well as SNSPDs, which are needed for advanced quantum communication schemes. A simple definition for quantum sensing is the way to measure a physical quantity (e.g., electromagnetic field, acceleration, time or frequency), enabled by a quantum support (photon, atom, quantum dot) in a quantum device called a quantum sensor.

The goal is to utilise the benefit of quantum specificities for better performance of sensing processes: for example, each Rubidium atom is the same, wherever it is used to deliver a measurement (e.g. emitted photon frequency for a specific change in energy level of an electron). Other benefits are numerous with quantum sensors, such as: higher resolution, better sensitivity, permanence over time of the measured physical parameter, resistance to environmental parameter variation, stability of the whole device (e.g., atomic clocks), Size, Weight and Power (SWAP) advantages, and miniaturization.

Better performance will be achievable through entangled distributed quantum sensors, linked by a quantum network (referred to as “distributed quantum sensing”), which is a future use case for the long-term quantum internet paradigm, as discussed in Section 3.2.3 of this document.

3.4.1 Radio Frequency Sensing

Another quantum sensing domain is the Rydberg atoms RF receiver concept. Rydberg atoms are atoms with an external electron in a strongly excited state, and, as such, these atoms are very sensitive to RF fields. Such sensors can support numerous use cases, from defence to telecommunications. Theoretically, Rydberg atom-based devices are able to sense RF ranges from continuous to THz domain. As this is still an emerging research field, we limit ourselves to a short description and overview of potential use cases and leave the detailed study on Solutions and Status of the Technology etc. for future work.

3.4.1.1 Description

Practically, several variations of this technology exist. The simple example of a Rydberg atom sensor is a specific type of alkali atoms (e.g., Rubidium) in gaseous form in a small cell [63]. It is the atomic cell which is the core of the RF sensing feature, acting as a receiving antenna; and two laser beams, one for coupling and the other as a probe.

3.4.1.2 Use Cases

Receiving the entire RF spectrum (from continuous to THz range) is not possible, but already several use cases tor telecommunications are foreseen, such as:

- **Ultra-low frequencies sensing:** There is a possibility to use Rydberg-based quantum antennas for the use of e-Loran signals in a ground-redundancy solution to mitigate Global Navigation Satellite System (GNSS) vulnerabilities [64]. e-Loran is a hyperbolic navigation system, using 100 kHz powerful radio signals. The problem with this very robust navigation solution is the size of receiving antennas. No classical miniature e-Loran antennas exist but the use of Rydberg-based quantum antennas may be a convenient solution in the future.

- **Ultra-high frequencies sensing:** It is possible to use Rydberg-based quantum antennas in the THz domain. Wiktor Krokosz et al. [65] demonstrated that Rydberg-based single-photon detectors can precisely detect and calibrate octave-spanning THz frequency combs with MHz-level selectivity and ultra-high sensitivity at room temperature, advancing THz spectroscopy into the quantum regime.

- **Multi-user MIMO:** Rydberg Atomic Quantum (RAQ) receivers, when integrated into a Multi-user Multiple-Input Multiple-Output (MIMO) uplink system (RAQ-MIMO), enables the use of lower transmit power and higher achievable rates compared to conventional massive MIMO, thanks to their superior RF signal detection and optimised signal processing schemes [66].This use case is one of several possible uses of this technology in the future 6G mobile generation. For example, Finland (at the foremost of 6G research studies) very recently expressed interest in this technology for 6G. Moreover, the Research public fund in Finland, has recently granted funding for research in this area [67].

3.4.2 Superconducting Nanowire Single-Photon Detector (SNSPD)

3.4.2.1 Description

Single-Photon Detectors (SPDs) are a cornerstone of modern photonics and quantum technologies. They enable the detection of individual photons with high precision, which is critical not only for quantum communication protocols like QKD but also for a wide range of applications such as Optical Time-Domain Reflectometry (OTDR), deep-space optical links, Light Detection and Ranging (LIDAR), quantum sensing, among others.

Among SPD technologies, two solutions dominate telecom-related use cases: Single-Photon Avalanche Diodes (SPADs) and SNSPDs. SPADs are semiconductor-based, detecting photons by triggering an avalanche breakdown in a reverse-biased diode, producing a measurable electrical pulse. SPADs are widely used in short-range quantum links and cost-sensitive deployments, but they exhibit moderate detection efficiency (up to 35 % in the spectral range 900 - 1700 nm), dark count rates up to <200 cps (at 10% efficiency), and timing jitter around 100 ps [68, 69]

In contrast, SNSPDs represent the state-of-the-art in single-photon detection [70, 69]. These detectors consist of a thin superconducting nanowire patterned in a meander shape and cooled to cryogenic temperatures (typically 1 K - 4 K). When a photon strikes the nanowire, it creates a localized “hotspot” that temporarily disrupts superconductivity, forcing the current to divert and generating a fast electrical pulse, as depicted in Figure 20.

This mechanism enables exceptional performance metrics: detection efficiencies exceeding 90%, timing jitter below 20 ps, and dark count rates approaching zero (<1 cps) [49, 50]. SNSPDs also offer rapid recovery times of a few nanoseconds, supporting high-speed operation up to ~1 Gcps [46] important for advanced quantum networks as well as Photon

Number Resolution (PNR) capabilities important, for example, for quantum computing [46]. This ultra-low noise and high precision makes SNSPDs indispensable for any photon-starved application demanding ultimate photon detection efficiency.

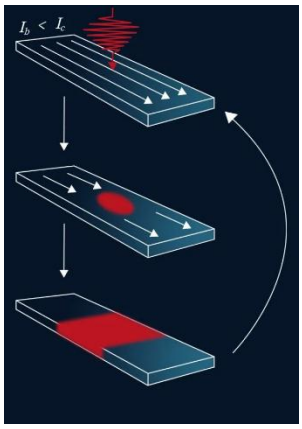


Figure 19: Schematic of SNSPD detector

SNSPD detector operate by holding a nanometer-scale strip of superconducting material below its critical temperature T_c, patterned in a compact meander geometry. A bias current I_b is applied through the nanowire such that it remains at the limit of superconductivity. An absorbed photon by the nanowire hence causes a breaking of the local superconductivity, which, after growing to the entire width of the nanowire, causes a rapid observable spike in the nanowire's resistance. Specifically, this change in the nanowire's resistance is measured with an electrical readout circuit: the resistance spike, in the order of ~1 kΩ, is much larger than the input impedance of the readout amplifier (50 Ω) and so most of the bias current I_b is shunted to the readout amplification circuit.

3.4.2.2 Use Case

Optical Time-Domain Reflectometry (OTDR):

Ensuring the physical integrity of optical fibre networks is critical for maintaining reliable service delivery. An advanced diagnostic tool in this domain is OTDR, which probes the fibre by sending light pulses and analysing the backscattered signal [72]. This enables precise measurement of strain and temperature variations along the fibre, allowing for the detection of faults, bends, or breaks. To achieve higher sensitivity and resolution, especially for detecting minute changes over long distances, Photon-Counting OTDR (PC-OTDR) systems have recently emerged [73]. These systems are powered by SNSPD detectors since they offer exceptional timing resolution and detection efficiency.

Quantum Key Distribution (QKD):

SNSPDs play a critical role in QKD systems, as highlighted in previous sections. Their ultra-high detection efficiency, low timing jitter, and near-zero dark counts make them ideal for long-distance QKD links and advanced protocols such as measurement-device-independent -QKD and twin-field QKD. By enabling reliable single-photon detection over extended fibre spans,

SNSPDs help overcome key limitations in QKD deployments, supporting secure communication in telecom-grade infrastructures.

Other Applications:

The maturity of SNSPD technology has expanded its use well beyond QKD and OTDR. Today, SNSPDs are deployed in diverse domains requiring extreme sensitivity and precision, including deep-space optical communication, LIDAR systems for high-resolution imaging, and advanced bioimaging techniques where single-photon sensitivity enables ultra-low-light fluorescence studies. They are also used in quantum optics experiments, astronomical observations, and emerging quantum computing architectures that require photon-number-resolving detectors. This versatility demonstrates that SNSPDs are not only a cornerstone for secure quantum communication but also a key enabler for cutting-edge scientific and industrial applications.

3.4.2.3 Solution

SNSPDs are already being deployed in in-field experiments and commercial setups, demonstrating their reliability and performance in real-world environments, particularly in OTDR applications [74, 75]. The evolution of OTDR into the quantum domain through PC-OTDR, leveraging the ultra-sensitive detection capabilities of SNSPDs, enables high-resolution, long-distance fibre sensing with enhanced sensitivity to minute changes in the fibre infrastructure [73]. This marks a significant advancement in distributed sensing, empowering telecom operators to monitor network health with unprecedented precision.

3.4.2.4 Status of the Technology

SNSPDs have reached a high level of technological maturity and are now commercially available. Products like the ID281 Pro from ID Quantique offer robust, continuous operation with timing jitter in the tens of picoseconds (or lower) and system detection efficiencies (SDE) exceeding 90% across a broad wavelength range (500–2000 nm), making them ideally suited for integration into telecom-grade sensing systems [50].

3.4.2.5 Challenges

Despite the technological readiness of SNSPDs, several challenges remain in deploying them across existing telecom infrastructure:

- **Legacy network topologies** and heterogeneous fibre deployments complicate integration and calibration, requiring tailored solutions for different environments.
- **Operational inertia** and limited familiarity with quantum technologies among telecom engineers may slow adoption, necessitating targeted training and awareness programmes.
- **Cost and scalability** remain significant concerns, especially for nationwide or global rollouts, where cryogenic cooling and specialised hardware may be required.
- **Data interpretation** from quantum sensing systems demands new analytical frameworks, including AI-driven anomaly detection and quantum-aware signal processing.

- **Polarisation sensitivity of SNSPDs** could hinder deployability and potentially introduce vulnerabilities [76]. While polarisation-insensitive SNSPDs exist, they currently underperform compared to standard models.
- **Environmental constraints**, such as temperature fluctuations and mechanical vibrations, may affect system stability and require robust packaging and shielding.
- **Regulatory and compliance hurdles**, especially in cross-border deployments, may delay integration into existing telecom infrastructure.

3.4.2.6 Opportunities

Quantum-enhanced sensing with SNSPDs could offer transformative opportunities for telecom operators:

- **Improved network health monitoring**, enabling early fault detection, predictive maintenance, and reduced service downtime.
- **Seismic and environmental sensing** using existing fibre infrastructure, turning telecom networks into large-scale sensor arrays [57].
- **Disaster readiness and resilience**, with real-time insights into physical network conditions that support emergency response and infrastructure protection.
- **Future-proofing infrastructure** for seamless integration with quantum communication systems, where SNSPDs play a dual role in sensing and enhancing quantum communication capabilities [77,].
- **Cross-sector collaboration**, enabling partnerships with energy, transportation, and environmental agencies to share sensing data and infrastructure.
- **Enhanced security monitoring**, detecting physical tampering or unauthorised access through fibre disturbance analysis.

New business models, including sensing-as-a-service offerings for municipalities, research institutions, and industrial clients.

3.4.2.7 GSMA Role

GSMA can play a pivotal role in accelerating the adoption and impact of quantum-enhanced fibre sensing technologies:

- **Facilitate knowledge-sharing** amongst member telecom operators by documenting lessons learned from pilot projects and field deployments.
- **Promote interoperability and standardisation**, ensuring that quantum sensing systems can integrate seamlessly across diverse telecom infrastructures.
- **Engage with regulators and standards bodies** to advocate for policies that support innovation in physical network monitoring and quantum technologies.
- **Support training and capacity-building**, helping telecom engineers and decision-makers understand the benefits and requirements of quantum sensing.
- **Coordinate cross-sector initiatives**, bringing together stakeholders from telecom, energy, transportation, and environmental sectors to explore joint sensing applications.

- **Encourage innovation through funding and incubation**, supporting startups and research groups developing next-generation sensing technologies.
- **Develop benchmarking frameworks**, enabling telecom operators to assess the performance and return on investment of quantum sensing deployments.

3.5 Quantum Positioning, Navigation, and Timing (PNT)

Quantum positioning, navigation, and timing (PNT) is another important field of quantum technologies. We leave the detailed assessment of quantum-PNT to a future GSMA QNS document. Nevertheless, here we give the reader a very brief overview.

Positioning and Navigation:

Cold atom interferometers based on Bose-Einstein condensates of neutral atoms such as Rydberg atoms can enable the next generation of gravitational and inertial sensors. Operating at quantum-limited precision, they can outperform classical gyroscopes and provide drift-free navigation in GPS-denied environments. Notable example for emerging offerings in that area is inertial sensing offered by Infleqtion [78].

Timing and Clocks:

Quantum sensing in the time frequency domain has an archetypal example: quantum clocks. In fact, atomic and optical clocks are all quantum in nature, since the very first atomic clock in the 1950s. Here, we focus on atomic/optical clocks that benefit from the so-called “second quantum revolution”. A simple illustration is the use of entanglement resources between clocks.

In the second quantum technologies revolution, quantum entanglement can make clocks and sensors more precise by either reducing noise (spin squeezing) or in entangled clock ensembles (two or more entangled clocks). It is already possible to enhance performances of atomic or optical clocks through quantum squeezing: if amplitude and phase parameters must be measured, it is possible to raise amplitude.

There are numerous efforts around the world to find a replacement for GNSS. Quantum time transfer, making use of the above-mentioned principles, offers the potential to increase precision of global timing services compared to GPS-based GNSS and also make it more difficult to jam and impossible to spoof. Companies like Xairos and Infleqtion are developing, or already offering, solutions in this area.

3.6 Outlook: Towards the Quantum Internet

A network offering distributed entanglement is often referred to as the “quantum internet”, and promises to support the above use cases, and more (and some to still be discovered). The quantum internet will be built upon the following building blocks:

Component	Function
Quantum Nodes	E.g. fault tolerant quantum processing unit; generate, store, and measure entangled qubits. Can be user devices, routers (i.e. repeater nodes), or data centres.

Component	Function
Quantum Channels	Optical fibres or free-space (terrestrial or satellite) links that transmit entangled photons. Require ultra-low loss and noise.
Quantum Repeaters	Extend communication range by performing entanglement swapping and purification.
Quantum Memories	Temporarily store quantum states to synchronise entanglement distribution.
Classical Control Plane	Coordinates quantum operations, timing, and error correction using classical communication.

Table 7: Quantum Internet Building Blocks

Each building block above poses significant investment for research and development, leading to physical deployment in real-life networks. Recent deployments of in-field entanglement distribution networks include:

Quantum computing, quantum communication, and distributed quantum computing as outlined in the previous sections are essential to the quantum internet vision [79 , 80]. As these technologies mature, progress toward this vision will accelerate and will be an important area to investigate as telecom industry in future work.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
V1.0	25 February 2026	First version of the document	QNS	Yolanda Sanz, GSMA

A.2 Editors, Authors, and other Information

Type	Description
Document Owner	Quantum Networks and Services Group
Editor / Company	Yolanda Sanz, GSMA Simon C. Mueller (QNS chair), O_2 Telefónica Ryan Parker (QNS vice chair), Vodafone Group

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.