



# Quantum Computing, Networking and Security

Version 1.0

March 2021

## **About the GSMA**

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at [www.gsma.com](http://www.gsma.com).

Follow the GSMA on Twitter: **@GSMA**.

## **About the GSMA Internet Group**

The GSMA Internet Group (IG) is the key working group which researches, analyses and measures the potential opportunities and impacts of new web and internet technologies on mobile operator networks and platforms. We maintain the most up-to-date knowledge base of new internet and web innovations through intelligence gathering of available global research and active participation in key Standards organisations.

[www.gsma.com/workinggroups](http://www.gsma.com/workinggroups)

# Table of Contents

<b>Quantum Computing, Networking and Security</b> .....	<b>1</b>
<b>1 Introduction</b> .....	<b>4</b>
1.1 Overview and Scope .....	4
1.2 Abbreviations.....	5
1.3 References .....	6
<b>2 Quantum Technologies - state of the art Overview</b> .....	<b>17</b>
2.1 Quantum-safe Security .....	17
2.1.1 Quantum Key Distribution (QKD).....	17
2.1.2 Quantum Random Number Generators (QRNG) .....	19
2.1.3 Blockchain and Quantum Security.....	20
2.2 Quantum Computing .....	21
2.2.1 Quantum Annealer and Gate-based Quantum Computers.....	22
2.2.2 Simulating Gate-based Quantum Computers .....	24
2.2.3 Quantum Algorithms and Software .....	24
2.2.4 Optical Quantum Computing.....	25
2.3 Quantum Technologies for Machine Learning .....	28
2.4 Quantum Networking Integration .....	29
2.5 Quantum Sensing and Metrology .....	32
<b>3 Proof-of-Concepts (PoCs)</b> .....	<b>35</b>
3.1 PoCs and use-cases on safe Security and Networking .....	35
3.1.1 SKT PoC and Use Cases .....	36
3.1.2 Madrid Quantum Network (Telefonica) .....	38
3.1.3 Other examples of use cases .....	40
3.2 PoCs and use-cases on Quantum Technologies for Machine Learning .....	41
3.3 PoCs and use-cases on Quantum Computing.....	42
3.3.1 Application of quantum computing to cell-ID planning of 4.5G and 5G networks (TIM) 42	
3.4 PoCs and use-cases Quantum Sensing and Metrology .....	45
<b>4 Roadmapping and Recommendations</b> .....	<b>48</b>
4.1 Roadmapping .....	48
4.2 Recommendations.....	49
4.2.1 Calls for action.....	51

<b>5</b>	<b>Conclusions</b> .....	<b>52</b>
<b>6</b>	<b>Appendix</b> .....	<b>53</b>
6.1	Quantum Internet and Quantum Communications .....	53
6.1.1	<i>Experiments on Quantum Communications</i> .....	53
<b>Annex A</b>	<b>Document Management</b> .....	<b>55</b>
A.1	Document History .....	55
A.2	Other Information.....	55

# 1 Introduction

The transformative role of Telecommunications and Information Communication Technologies (ICT) has long been witnessed as a precursor of the scientific progress and economic growth in the modern world. Today, like never before, we are witnessing a pervasive diffusion of ultra-broadband fixed-mobile connectivity, the deployment of Cloud-native 5G network and service platforms and a wide adoption of Artificial Intelligence.

This Digital Transformation is surely bringing far reaching techno-economic impacts on our Society. Nevertheless, this transformation is still laying its foundations on Electronics and the impending end of Moore's Law: therefore, a rethink of the ways of computing and communications has initiated already. Quantum technologies are one of the new ways of performing these functions.

As a matter of fact, a first quantum revolution started decades ago and has already brought quantum technologies in our everyday life. In fact, there are many devices available today which are fundamentally based on the effects of quantum mechanics: these include transistor, lasers, LEDs and other semi-conductor devices, Magnetic Resonance Imaging (MRI) and Positron Emission Tomography (PET) systems, etc. Today, a second revolution is underway leveraging on quantum technologies which aim at going further in manipulating quantum phenomena such as superposition and entanglement. In the former (superposition), particles show or have multiple states until they are observed, in the latter (entanglement), the properties of quantum systems — such as particles' spin and polarization — can be intertwined together.

This potential second revolution is expected to lead to new future applications mainly in four domains [1]:

- **Quantum Communication:** quantum effects are employed for transmitting digital data in a provably secure way (QKD, QRNG), for Quantum Networking, or even “teleporting” quantum information (Quantum Internet);
- **Quantum Computation:** quantum effects are employed to speed up certain calculations, such as number factoring;
- **Quantum Sensing and Metrology,** where the high sensitivity of coherent quantum systems is exploited to enhance the performance of measurements of physical quantities;
- **Quantum Simulation:** where well-controlled quantum systems are used to reproduce the behavior of other, less accessible quantum systems.

## 1.1 Overview and Scope

This document provides an overview of threats, challenges and the business opportunities brought by Quantum technologies on Operators' networks and services infrastructures.

Scope of the document is to provide:

- (1) An overview of the state-of-the-art of the quantum technologies and the related levels of maturity (for example for example in terms of the indicator Technology Readiness Level - TRL). The focus will be on below areas which are expected to have higher TRL and potential impacts in the short-medium term) on Telecommunications and ICT:
  - Quantum-safe Security;
  - Quantum Computing;
  - Quantum Networking;
  - Quantum Sensing and Metrology.
- (2) An analysis of the ongoing experimental Proof-of-Concepts (PoC) and use-cases demonstrating and testing the above technologies.
- (3) Main requirements (for example, in terms of orchestration/management/control) for a seamless integration of quantum nodes/systems/devices in the Network Operators' infrastructures (for example, without service disruption and large additional investments costs).
- (4) Recommendations for quantum services road-mapping and possible proposals for setting actions/synergies in other standardization activities (for example, ITU, IRTF, ETSI, etc.).

The appendix has mainly an educational scope. It contains an overview of contents and references for those quantum technologies which appear to have a TRL rather low and, as such, are not expected to have concrete industrial impacts in the short-medium term (for example, Quantum Internet).

Detailed technical analysis, architectures and specifications of Quantum technologies are out of scope, but references to the state-of-the-art are listed for the readers willing to get more details.

## 1.2 Abbreviations

Term	Description
QRNG	Quantum Random Number Generator
QKD	Quantum Key Distribution
CV-QKD	Continuous Variable Quantum Key Distribution
DV-QKD	Discrete Variable Quantum Key Distribution
OpenCL	Open Computing Language
QML	Quantum Machine Learning
QNN	Quantum Neural Network
TRL	Technology Readiness Level
SHA3	Secure Hash Algorithm 3
WOTS	Winternitz One-Time Signatures
Ed25519	Edwards Curve Digital Signature Algorithm

### 1.3 References

Ref	Doc Number	Title
[1]	Quantum technologies roadmap: a European community view	<a href="https://iopscience.iop.org/article/10.1088/1367-2630/aad1ea/pdf">https://iopscience.iop.org/article/10.1088/1367-2630/aad1ea/pdf</a>
[2]	Quantum cryptography: Public key distribution and coin tossing	C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984.
[3]	Quantum cryptography based on Bell's theorem	Ekert, Artur K. "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett., Vol. 67, 5 August 1991.
[4]	Quantum cryptography without Bell's theorem	C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem" Phys. Rev. Lett. 68, 557 (1992)
[5]	Decoy state quantum key distribution	Lo, Hoi-Kwong, Xiongfeng Ma, and Kai Chen. "Decoy state quantum key distribution" Physical review letters 94.23 (2005): 230504
[6]	Measurement-device-independent QKD	Lo, Hoi-Kwong, Marcos Curty, and Bing Qi. "Measurement-device-independent quantum key distribution." Physical review letters 108.13 (2012): 130503.
[7]	Measurement-device-independent QKD over a 404 km optical fiber	Yin, Hua-Lei, et al. "Measurement-device-independent quantum key distribution over a 404 km optical fiber." Physical review letters 117.19 (2016): 190501.
[8]	Measurement-device-independent QKD coexisting with classical communications	Valivarthi, Raju, et al. "Measurement-device-independent quantum key distribution coexisting with classical communication." <i>Quantum Science and Technology</i> 4.4 (2019): 045002.
[9]	The UK Market for Quantum Enabling Photon Sources 2018-2022	The UK Market for Quantum Enabling Photon Sources 2018-2022. Gooch & Housego, Milner Strategic Marketing & University of Bristol. (March 2018).

Ref	Doc Number	Title
[10]	QRNG chip for mobile IoT and edge app.	<a href="https://www.quantaneo.com/ID-Quantique-launches-an-ultra-small-Quantum-Random-Number-Generator-QRNG-chip-for-mobile-IoT-and-edge-applications_a467.html">https://www.quantaneo.com/ID-Quantique-launches-an-ultra-small-Quantum-Random-Number-Generator-QRNG-chip-for-mobile-IoT-and-edge-applications_a467.html</a>
[11]	ITU-T Recs.	<a href="https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14095&amp;lang=en">https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14095&amp;lang=en</a>
[12]	Mitre Technical Report, Blockchain and Quantum Computing	Mitre Technical Report, Blockchain and Quantum Computing, B. Rodenburg, PhD and S. R. Pappas, PhD, June 2017. <a href="https://www.mitre.org/publications/technical-papers/blockchain-and-quantum-computing">https://www.mitre.org/publications/technical-papers/blockchain-and-quantum-computing</a>
[13]	A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain	A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain, Yu-Long Gao et al. April 2018 <a href="https://ieeexplore.ieee.org/document/8340794">https://ieeexplore.ieee.org/document/8340794</a>
[14]	Towards Post-Quantum Blockchain	Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks, T. M. Fernández-Caramès et al. January 2020. <a href="https://ieeexplore.ieee.org/document/8967098">https://ieeexplore.ieee.org/document/8967098</a>
[15]	OIDA Quantum Photonic Roadmap	OIDA Quantum Photonic Roadmap, Every Photon Counts - March 2020
[16]	Quantum Information	Quantum Information Portal and Wiki, available at <a href="https://quantiki.org/wiki/list-qc-simulators">https://quantiki.org/wiki/list-qc-simulators</a>
[17]	Simulating quantum computers using OpenCL	Kelly, A. Simulating quantum computers using OpenCL. arXiv preprint arXiv:1805.00988 (2018).
[18]	Quantum Algorithms Zoo	Quantum Algorithms Zoo, available at <a href="http://quantumalgorithmzoo.org/#acknowledgments">http://quantumalgorithmzoo.org/#acknowledgments</a>
[19]	Open source software in quantum computing	Fingerhuth, M.; Babej, T.; Wittek, P. Open source software in quantum computing. PLoS ONE 2018, 13, e0208561.
[20]	Measurement-Device-Independent QKD over asymmetric channel and unstable channel	Hu, X., Cao, Y., Yu, Z. et al. Measurement-Device-Independent Quantum Key Distribution over asymmetric channel and unstable channel. Sci Rep 8, 17634 (2018) doi:10.1038/s41598-018-35507-z.
[21]	Measurement-Device-Independent Twin-Field QKD	Yin, Hua-Lei, and Yao Fu. "Measurement-Device-Independent Twin-Field Quantum Key Distribution." Scientific reports 9.1 (2019): 3045. Rare-earth-based quantum memories

Ref	Doc Number	Title
[22]	Coexistence of continuous variable QKD with intense DWDM classical channels	Kumar, Rupesh, Hao Qin, and Romain Alléaume. "Coexistence of continuous variable QKD with intense DWDM classical channels." <i>New Journal of Physics</i> 17.4 (2015): 043027.
[23]	Dense wavelength multiplexing of 1550 nm QKD	Peters, N. A., et al. "Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments." <i>New Journal of physics</i> 11.4 (2009): 045012.
[24]	Secure NFV orchestration over an SDN-controlled optical network with time-shared QKD resources	Aguado, E. Hugues-Salas, P. A. Haigh, J. Marhuenda, A. B. Price, P. Sibson, J. E. Kennard, C. Erven, J. G. Rarity, M. G. Thompson, A. Lord, R. Nejabati, and D. Simeonidou, "Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources," <i>J. Lightwave Technol.</i> , vol. 35, no. 8, pp. 1357–1362, Apr. 2017.
[25]	Experimental demonstration of QKD for energy-efficient software-defined Internet of Things	Mavromatis, F. Ntavou, E. Hugues-Salas, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Experimental demonstration of quantum key distribution (QKD) for energy-efficient software-defined Internet of Things," in <i>Proc. Europ. Conf. Opt. Commun.</i> , Rome, Italy, Sept. 2018.
[26]	Resource allocation in optical networks secured by QKD	Zhao, Y. Cao, W. Wang, H. Wang, X. Yu, J. Zhang, M. Tornatore, Y. Wu, and B. Mukherjee, "Resource allocation in optical networks secured by quantum key distribution," <i>IEEE Commun. Mag.</i> , vol. 56, no. 8, pp. 130–137, Aug. 2018.
[27]	Toward the integration of CV quantum key distribution in deployed optical networks	Karinou, H. H. Brunner, C.-H. F. Fung, L. C. Comandar, S. Bettelli, D. Hillerkuss, M. Kuschnerov, S. Mikroulis, D. Wang, C. Xie, M. Peev, and A. Poppe, "Toward the integration of CV quantum key distribution in deployed optical networks," <i>IEEE Photon. Technol. Lett.</i> , vol. 30, no. 7, pp. 650–653, Apr. 2018.
[28]	Time-scheduled QKD over WDM networks	Cao, Y. Zhao, Y. Wu, X. Yu, and J. Zhang, "Time-scheduled quantum key distribution (QKD) over WDM networks," <i>J. Lightwave Technol.</i> , vol. 36, no. 16, pp. 3382–3395, Aug. 2018.
[29]	Wavelength assignment in hybrid quantum-classical networks	Bahrani, M. Razavi, and J. A. Salehi, "Wavelength assignment in hybrid quantum-classical networks," <i>Sci. Rep.</i> , vol. 8, no. 1, pp. 3456, Feb. 2018.
[30]	Field-trial of machine learning-assisted QKD networking with SDN	Ou, E. Hugues-Salas, F. Ntavou, R. Wang, Y. Bi, S. Yan, G. Kanellos, R. Nejabati, and D. Simeonidou, "Field-trial of machine learning-assisted quantum key distribution (QKD) networking with SDN," in <i>Proc. Europ. Conf. Opt. Commun.</i> , Rome, Italy, Sept. 2018.

Ref	Doc Number	Title
[31]	Cost-efficient QKD over WDM networks	Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "Cost-efficient quantum key distribution (QKD) over WDM networks," J. Opt. Commun. Netw., vol. 11, no. 6, pp. 285–298, June 2019.
[32]	Monitoring and physical-layer attack mitigation in SDN-controlled QKD networks	Hugues-Salas, F. Ntavou, D. Gkounis, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Monitoring and physical-layer attack mitigation in SDN-controlled quantum key distribution networks," J. Opt. Commun. Netw., vol. 11, no. 2, pp. A209–A218, Feb. 2019.
[33]	First demonstration of quantum-secured, inter-domain 5G service orchestration and on-demand NFV chaining over flexi-WDM optical networks	Nejabati, R. Wang, A. Bravalheri, A. Muqaddas, N. Uniyal, T. Diallo, R. Tessinari, R. S. Guimaraes, S. Moazzeni, E. Hugues-Salas, G. T. Kanellos, and D. Simeonidou, "First demonstration of quantum-secured, inter-domain 5G service orchestration and on-demand NFV chaining over flexi-WDM optical networks," in Proc. Opt. Fiber Commun. Conf., San Diego, CA, USA, Mar. 2019.
[34]	Machine Learning for Optimal Parameter Prediction in QKD	Wenyuan Wang, Hoi-Kwong Lo, "Machine Learning for Optimal Parameter Prediction in Quantum Key Distribution," arXiv:1812.07724.
[35]	Open Networking Foundation	Open Networking Foundation TR-502 Issue 1, "SDN architecture". Available at <a href="https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf">https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf</a>
[36]	Zero-touch network and Service Management	ETSI GS ZSM ZSM 002 V1.1.1 "Zero-touch network and Service Management (ZSM); Reference Architecture". Available at <a href="https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010101p.pdf">https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010101p.pdf</a>
[37]	QKD: A Networking Perspective	Quantum Key Distribution: A Networking Perspective, ACM Computing Surveys, September 2020, <a href="https://doi.org/10.1145/3402192">https://doi.org/10.1145/3402192</a>
[38]	A diamond age of masers	Ren-Bao Liu, "A diamond age of masers," Nature, 21 March 2018
[39]	Quantum sensing on a chip	Rob Matheson, "Quantum sensing on a chip," MIT News, September 25, 2019
[40]	Quantum sensing radio	<a href="https://phys.org/news/2020-03-scientists-quantum-sensor-entire-radio.html">https://phys.org/news/2020-03-scientists-quantum-sensor-entire-radio.html</a>
[41]	Quantum sensing Army	<a href="https://www.army.mil/article/212935/army_researchers_make_giant_leap_in_quantum_sensing">https://www.army.mil/article/212935/army_researchers_make_giant_leap_in_quantum_sensing</a>
[42]	Digital Communication with Rydberg	David Meyer, Kevin Cox, Fredrik Fatemi, Paul Kunz, "Digital Communication with Rydberg Atoms and Amplitude-Modulated

Ref	Doc Number	Title
	Atoms and Amplitude-Modulated Microwave Fields	Microwave Fields", App. Phys. Lett. (R) 112, 211108 (2018). [arXiv:1803.03545]
[43]	Quantum-Limited Receiver in the Electrically Small Regime	K. Cox, D. Meyer, F. Fatemi, P. Kunz, "Quantum-Limited Receiver in the Electrically Small Regime", Phys. Rev. Lett. 112, 110502 (2018). [arXiv:1805.09808]
[44]	A Secure Quantum Communications Infrastructure for Europe," European Commission JRC technical Report	A. M. Lewis, M. Travagnin, "A Secure Quantum Communications Infrastructure for Europe," European Commission JRC technical Report.
[45]	The Madrid Quantum Network: A Quantum-Classical Integrated Infrastructure	V. Martin, A. Aguado, P. Salas, A.L. Sanz, J.P. , Brito, D. R. Lopez, V. Lopez, A. Pastor, J. Folgueira, H. H. Brunner, S. Bettelli, F. Fung, L. C. Comandar, D. Wang, A. Poppe, and M. Peev, "The Madrid Quantum Network: A Quantum-Classical Integrated Infrastructure," Photonic Networks and Devices 2019, Burlingame, California United States. 29 July–1 August 2019
[46]	Field trial of a three-state quantum key distribution scheme in the Florence metropolitan area,	Davide Bacco, Ilaria Vagniluca, Beatrice Da Lio, Nicola Biagi, Adriano Della Frera, Davide Calonico, Costanza Toninelli, Francesco S. Cataliotti, Marco Bellini, Leif K. Oxenløwe & Alessandro Zavatta, "Field trial of a three-state quantum key distribution scheme in the Florence metropolitan area," EPJ Quantum Technology, 28 October 2019.
[47]	ITU-T Workshop	<a href="https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Andrew_Shields_Presentation.pdf">https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Andrew_Shields_Presentation.pdf</a>
[48]	Quantum network from Boston to Washington	<a href="https://techcrunch.com/2018/10/25/new-plans-aim-to-deploy-the-first-u-s-quantum-network-from-boston-to-washington-dc/">https://techcrunch.com/2018/10/25/new-plans-aim-to-deploy-the-first-u-s-quantum-network-from-boston-to-washington-dc/</a>
[49]	IDQuantique	<a href="https://marketing.idquantique.com/acton/attachment/11868/f-15ec7f60-f467-4360-871a-48c62e1fb3f4/1/-/-/-/Telecom%20Service%20Provider_SKT%20QKD%20for%205G%20Use%20Case.pdf">https://marketing.idquantique.com/acton/attachment/11868/f-15ec7f60-f467-4360-871a-48c62e1fb3f4/1/-/-/-/Telecom%20Service%20Provider_SKT%20QKD%20for%205G%20Use%20Case.pdf</a>
[50]	IDQuantique	<a href="https://marketing.idquantique.com/acton/attachment/11868/f-4343f2df-afe9-4a47-a3e8-b839565e7f97/1/-/-/-/Quantum%20Technologies%20for%205G_App%20Note.pdf?sid=TV2:5gwvisKIR">https://marketing.idquantique.com/acton/attachment/11868/f-4343f2df-afe9-4a47-a3e8-b839565e7f97/1/-/-/-/Quantum%20Technologies%20for%205G_App%20Note.pdf?sid=TV2:5gwvisKIR</a>

Ref	Doc Number	Title
[51]	Press on koeratimes	<a href="https://www.koreatimes.co.kr/www/tech/2019/03/133_265557.html">https://www.koreatimes.co.kr/www/tech/2019/03/133_265557.html</a>
[52]	5G smartphone with quantum	<a href="https://www.forbes.com/sites/daveywinder/2020/05/15/samsungs-surprising-new-5g-smartphone-is-worlds-first-with-quantum-technology/#27b5909530e0">https://www.forbes.com/sites/daveywinder/2020/05/15/samsungs-surprising-new-5g-smartphone-is-worlds-first-with-quantum-technology/#27b5909530e0</a>
[53]	OSM ETSI	<a href="https://osm.etsi.org/">https://osm.etsi.org/</a>
[54]	Quantum Technologies in Support for 5G services	A. Aguado, D. Lopez, V. Lopez, F. de la Iglesia, A. Pastor, M. Peev, W. Amaya, F. Martin, C. Abellan, V. Martin, "Quantum Technologies in Support for 5G services: Ordered Proof-of-Transit". 45th European Conference on Optical Communication (ECOC 2019), <a href="https://doi.org/10.1049/cp.2019.1075">https://doi.org/10.1049/cp.2019.1075</a>
[55]	CIVIQ	<a href="https://civiquantum.eu/about-civiq/">https://civiquantum.eu/about-civiq/</a>
[56]	OPENQKD	<a href="https://openqkd.eu/objectives/">https://openqkd.eu/objectives/</a>
[57]	Reducing the Dimensionality of Data with Neural Networks	Hinton, G.E.; Salakhutdinov, R.R. Reducing the Dimensionality of Data with Neural Networks. <i>Science</i> 2006, 313, 504–507.
[58]	The renormalization group	Wilson, K.G.; Kogut, J. The renormalization group and the $\epsilon$ expansion. <i>Phys. Rep.</i> 1974, 12, 75–199.
[59]	Quantum fields as deep learning	Lee, J.W. Quantum fields as deep learning. arXiv 2017, arXiv:1708.07408.
[60]	Complex deep learning with quantum optics	Manzalini, A. (2019). Complex deep learning with quantum optics. <i>Quantum Reports</i> , 1(1), 107-118.
[61]	Deep learning with coherent nanophotonic circuits	Shen, Y.; Harris, N.C.; Skirlo, S.; Prabhu, M.; Baehr-Jones, T.; Hochberg, M.; Sun, X.; Zhao, S.; LaRochelle, H.; Englund, D.; et al. Deep learning with coherent nanophotonic circuits. <i>Nat. Photonics</i> 2017, 11, 441–446.
[62]	Photonic Nambu-Goldstone bosons	García-March, M.Á.; Paredes, A.; Zacarés, M.; Michinel, H.; Ferrando, A. Photonic Nambu-Goldstone bosons. <i>Phys. Rev. A</i> 2017, 96, 053848.
[63]	All-optical machine learning using diffractive deep neural networks	Lin, X.; Rivenson, Y.; Yardimci, N.T.; Veli, M.; Luo, Y.; Jarrahi, M.; Ozcan, A. All-optical machine learning using diffractive deep neural networks. <i>Science</i> 2018, 361, 1004–1008.
[64]	Quantum Internet	W. Kozłowski, S. Wehner, R. Van Meter, B. Rijsman, A. S. Cacciapuoti, and M. Caleffi, "Architectural Principles for a Quantum Internet," Internet Engineering Task Force (Work in Progress), Mar. 2020.
[65]	When Entanglement Meets Classical Communications:	A. S. Cacciapuoti, M. Caleffi, R. Van Meter, and L. Hanzo, "When Entanglement Meets Classical Communications: Quantum Teleportation for the Quantum Internet," <i>IEEE Transactions on Communications</i> (Invited Paper), 2020.

Ref	Doc Number	Title
	Quantum Teleportation for the Quantum Internet	
[66]	Teleporting an Unknown Quantum State	C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels," <i>Physical Review Letters</i> , vol. 70, no. 13, pp. 1895–1899, 1993.
[67]	Quantum Internet: Networking Challenges in Distributed Quantum Computing	A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, "Quantum Internet: Networking Challenges in Distributed Quantum Computing," <i>IEEE Network</i> , vol. 34, no. 1, pp. 137–143, 2019.
[68]	Security considerations for QKD	Technical Report "Security considerations for quantum key distribution networks," ITU-T SG17 <a href="https://www.itu.int/pub/T-TUT-QKD-2020-1">https://www.itu.int/pub/T-TUT-QKD-2020-1</a>
[69]	Quantum security, preparing the next era	Dong-Hi SIM, "Quantum security, preparing the next era," ITU-T Workshop on Quantum Information Technology for Networks <a href="https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/DongHi_Sim_Networks_Presentation.pdf">https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/DongHi_Sim_Networks_Presentation.pdf</a>
[70]	Quantum security standardization activities in ITU-T SG17	Dong-Hi SIM, "Quantum security standardization activities in ITU-T SG17," ITU-T Workshop on Quantum Information Technology for Networks <a href="https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/DongHi_Sim_SG17_Presentation.pdf">https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/DongHi_Sim_SG17_Presentation.pdf</a>
[71]	Quantum Noise Random Number Generator Architecture	ITU-T Recommendation X.1702 "Quantum Noise Random Number Generator Architecture," ITU-T SG17, <a href="https://www.itu.int/rec/T-REC-X.1702">https://www.itu.int/rec/T-REC-X.1702</a>
[72]	ITU-T Recommendation X.1710	ITU-T Recommendation X.1710 "Security framework for quantum key distribution networks," ITU-T SG17, <a href="https://www.itu.int/rec/T-REC-X.1710/en">https://www.itu.int/rec/T-REC-X.1710/en</a>
[73]	ITU-T Recommendation X.1714	ITU-T Recommendation X.1714 "Key combination and confidential key supply for quantum key distribution networks," <a href="https://www.itu.int/rec/T-REC-X.1714/en">https://www.itu.int/rec/T-REC-X.1714/en</a>
[74]	Event-ready-detectors' Bell experiment via entanglement swapping	Żukowski, M., Zeilinger, A., Horne, M. A. & Ekert, A. K. 'Event-ready-detectors' Bell experiment via entanglement swapping. <i>Phys. Rev. Lett.</i> 71, 4287–4290 (1993).
[75]	A. Experimental entanglement swapping: entangling	Pan, J.-W., Bouwmeester, D., Weinfurter, H. & Zeilinger, A. Experimental entanglement swapping: entangling photons that never interacted. <i>Phys. Rev. Lett.</i> 80, 3891–3894 (1998).

Ref	Doc Number	Title
	photons that never interacted	
[76]	Entanglement purification for quantum communication	Pan, J.-W., Simon, C., Brukner, Č. & Zeilinger, A. Entanglement purification for quantum communication. <i>Nature</i> 410, 1067–1070 (2001).
[77]	Experimental entanglement purification of arbitrary unknown states	Pan, J.-W., Gasparoni, S., Ursin, R., Weihs, G. & Zeilinger, A. Experimental entanglement purification of arbitrary unknown states. <i>Nature</i> 423, 417–422 (2003).
[78]	Functional quantum nodes for entanglement distribution over scalable quantum networks	Chou, C.-W. et al. Functional quantum nodes for entanglement distribution over scalable quantum networks. <i>Science</i> 316, 1316–1320 (2007).
[79]	Entanglement of single-atom quantum bits at a distance	Moehring, D. et al. Entanglement of single-atom quantum bits at a distance. <i>Nature</i> 449, 68–71 (2007).
[80]	Experimental demonstration of a BDCZ quantum repeater node	Yuan, Z.-S. et al. Experimental demonstration of a BDCZ quantum repeater node. <i>Nature</i> 454, 1098–1101 (2008).
[81]	Measurement-based quantum repeaters	Zwenger, M., Dür, W. & Briegel, H. J. Measurement-based quantum repeaters. <i>Phys. Rev. A</i> 85, 062326 (2012).
[82]	Quantum communication without the necessity of quantum memories	Munro, W., Stephens, A., Devitt, S., Harrison, K. & Nemoto, K. Quantum communication without the necessity of quantum memories. <i>Nat. Photon.</i> 6, 777–781 (2012).
[83]	Ultrafast and fault-tolerant quantum communication across long distances	Muralidharan, S., Kim, J., Lütkenhaus, N., Lukin, M. D. & Jiang, L. Ultrafast and fault-tolerant quantum communication across long distances. <i>Phys. Rev. Lett.</i> 112, 250501 (2014).
[84]	Experimental nested purification for a linear optical quantum repeater	Chen, L.-K. et al. Experimental nested purification for a linear optical quantum repeater. <i>Nat. Photon.</i> 11, 695–699 (2017).

Ref	Doc Number	Title
[85]	Two-hierarchy entanglement swapping for a linear optical quantum repeater	Xu, P. et al. Two-hierarchy entanglement swapping for a linear optical quantum repeater. Phys. Rev. Lett. 119, 170502 (2017).
[86]	Entanglement distillation between solid-state quantum network nodes	Kalb, N. et al. Entanglement distillation between solid-state quantum network nodes. Science 356, 928–932 (2017).
[87]	Blake2	<a href="https://blake2.net">https://blake2.net</a>
[88]	Rydberg Blockade Entangling Gates in Silicon	<a href="https://arxiv.org/abs/2008.11736">arXiv:2008.11736</a>
[89]	Impact of ionizing radiation on superconducting qubit coherence	<a href="https://www.nature.com/articles/s41586-020-2619-8">https://www.nature.com/articles/s41586-020-2619-8</a>
[90]	Engineering telecom single-photon emitters in silicon for scalable quantum photonics, August 21, 2020	<a href="https://arxiv.org/abs/2008.09425">https://arxiv.org/abs/2008.09425</a>
[91]	High-performance quantum light source for an optical quantum computer chip	<a href="https://www.ntt.co.jp/news2020/2003e/200330b.html">https://www.ntt.co.jp/news2020/2003e/200330b.html</a>
[92]	Verizon-achieves-milestone-future-proofing-data-hackers	<a href="https://www.verizon.com/about/news/verizon-achieves-milestone-future-proofing-data-hackers">https://www.verizon.com/about/news/verizon-achieves-milestone-future-proofing-data-hackers</a>
[93]	Fiber-Based UTC Dissemination Supporting 5G Telecommunications Networks	Sliwczynski, L., Krehlik, P., Imlau, H., Ender, H., Schnatz, H., Piester, D., & Bauch, A. (2020). Fiber-Based UTC Dissemination Supporting 5G Telecommunications Networks. IEEE Communications Magazine, 58(4), 67-73.
[94]	Experimental quantum repeater without quantum memory	<a href="https://arxiv.org/abs/1908.05351">https://arxiv.org/abs/1908.05351</a>
[95]	Quantum Flagship	<a href="https://qt.eu/">https://qt.eu/</a>

Ref	Doc Number	Title
[96]	Quantum Internet Team	<a href="http://quantum-internet.team/">http://quantum-internet.team/</a>
[97]	Large-scale integration of artificial atoms in hybrid photonic circuits,	Large-scale integration of artificial atoms in hybrid photonic circuits, Nature July 8, 2020 - <a href="https://www.nature.com/articles/s41586-020-2441-3">https://www.nature.com/articles/s41586-020-2441-3</a>
[98]	REFIMEVE	<a href="http://www.refimeve.fr/index.php/en/">http://www.refimeve.fr/index.php/en/</a>
[99]	Machine Learning for Long-Distance Quantum Communication	Machine Learning for Long-Distance Quantum Communication <a href="https://journals.aps.org/prxquantum/abstract/10.1103/PRXQuantum.1.010301">https://journals.aps.org/prxquantum/abstract/10.1103/PRXQuantum.1.010301</a>
[100]	Topological Photonics for Optical Communications and Quantum Computing	"Topological Photonics for Optical Communications and Quantum Computing" published in Quantum Reports as part of the Special Issue Quantum Technologies for Future Internet <a href="https://www.mdpi.com/2624-960X/2/4/40">https://www.mdpi.com/2624-960X/2/4/40</a>
[101]	Quantum Key Distribution (QKD) and Quantum Cryptography (QC)	<a href="https://www.nsa.gov/what-we-do/cybersecurity/quantum-key-distribution-qkd-and-quantum-cryptography-qc/">https://www.nsa.gov/what-we-do/cybersecurity/quantum-key-distribution-qkd-and-quantum-cryptography-qc/</a>
[102]	Stipcevic M (2012) Quantum random number generators and their applications in cryptography. In: Advanced photon counting techniques VI, international society for optics and photonics, vol 8375, p 837504	<a href="https://spie.org/Publications/Proceedings/Paper/10.1117/12.919920?SSO=1">https://spie.org/Publications/Proceedings/Paper/10.1117/12.919920?SSO=1</a>
[103]	On the effects of pseudorandom and quantum-random number generators in soft computing	<a href="https://link.springer.com/article/10.1007/s00500-019-04450-0">https://link.springer.com/article/10.1007/s00500-019-04450-0</a>
[104]	Experimental Demonstration of Quantum Key Distribution (QKD) for Energy-Efficient	<a href="https://research-information.bris.ac.uk/ws/portalfiles/portal/177112937/Alex_Movromatis_Experimental_Demonstration_of_Quantum_Key_Distribution.pdf">https://research-information.bris.ac.uk/ws/portalfiles/portal/177112937/Alex_Movromatis_Experimental_Demonstration_of_Quantum_Key_Distribution.pdf</a>

Ref	Doc Number	Title
	Software-Defined Internet of Things	
[105]	TIM is the first operator in Europe to use quantum computing live on its mobile networks (4.5G and 5G)	<a href="https://www.gruppotim.it/en/press-archive/corporate/2020/TIM-Quantum-computing-250220.html">https://www.gruppotim.it/en/press-archive/corporate/2020/TIM-Quantum-computing-250220.html</a>

# 2 Quantum Technologies - state of the art Overview

This section provides an overview of the state-of-the-art of quantum technologies.

## 2.1 Quantum-safe Security

### 2.1.1 Quantum Key Distribution (QKD)

Quantum communications study the transmission of quantum states between two or more partners. The most common application is Quantum Key Distribution (QKD), indicating any cryptography technique based on quantum physics laws to share a secret key between two or more partners. While classical cryptography relies on the unrealistically long time needed to solve certain mathematical problems, QKD exploits the fact that a manipulation of a quantum state perturbs it irreversibly, so detecting the potential presence of an eavesdropper. QKD prevents the possibility that, due to advances in computation power or introduction of quantum computers, data in transit can be deciphered, even much longer time after they have been transmitted (“record now, decrypt tomorrow”).

Two wide classes of QKD systems exist: Discrete Variable QKD (DV-QKD) and Continuous Variable QKD (CV-QKD).

DV-QKD was introduced first and its testbeds and even first commercial products already exist. BB84 [2] is the most known example of DV-QKD protocol. In BB84, the sender maps 0 or 1 bits using two different bases for the representation of a quantum state of a photon, for example its polarization. The receiver ignores the base used by the sender and measures the state of the incoming photons selecting randomly one of the two bases. When he uses the same base of the sender, he will get the right bit value; otherwise, the result will be correct with 50% probability. After having exchanged a long sequence of photons, sender and receiver compare the used bases, communicating over a classical authenticated channel, and keep only the bits generated and received with the same base, the so called sifted key. In absence of noise, the sifted keys will be equal and could be used as private key. In practical systems, affected by noise or potential attacks, further error correction and privacy amplification steps are performed. Privacy amplification is an algorithm producing a new, shorter key from the error-corrected key, using a hash function, chosen at random from a family (universal<sub>2</sub> family). The length of the new key depends on the number of detected errors. These final steps avoid the need of aborting the communication any time an error occurs, for example due to noise, in absence of an eavesdropper. BB84 is an example of prepare-and-measure protocol, so called because the quantum state of a photon is prepared by the sender and measured by the receiver. Other examples of prepare-and-measure protocols are BB84 variants using physical properties different from the polarization, for example phase or orbital angular momentum. Another class of protocols exploits entangled photon pairs distributed to communicating partners that, as in BB84, choose their own measurement base. As in BB84, if sender and receiver choose the same base, the bit is retained, otherwise it is discarded. E91 and BBM92 are examples of entanglement based protocols [3] [4].

Different from DV-QKD, in CV-QKD the physical variable used for bit encoding varies over a continuous range. CV-QKD relies on components, such as coherent optical transmitters and receivers, already used in classical optical networks, so avoiding the need of the special devices required by DV-QKD, such as single photon sources and single photon detectors. The need of specific devices, with a dedicated supply chain and limited production volumes, is indeed a major issue for the massive deployment of DV-QKD systems. Two classes of CV-QKD protocols exist, based on discrete and Gaussian optical signal modulation in the complex plane (whose quadrants are conventionally referred as “quadratures”). CV-QKD working principle is similar to BB84 but it uses pulses of energy instead of single photons. In the simplest CV-QKD implementation, each pulse is mapped by the sender into one quadrature, adding a different offset to encode 0 or 1 bits. Then, the receiver chooses randomly the quadrature where performing the measure. As in BB84, only the bits for which the correct quadrature choice was made are kept. CV-QKD with more than two states can be implemented, similar to classical modulation formats based on complex constellations, such as Quadrature Amplitude Modulation (QAM). In Gaussian CV-QKD the offset follows a Gaussian distribution instead of assuming discrete values. The security of CV-QKD with a low number of discrete states is not fully proofed, due to “finite-size” statistical effects. For Gaussian CV-QKD, security is guaranteed only for long sequences of transmitted signals. However, from an industrial perspective, CV-QKD is a promising option whenever reuse of installed network infrastructures and coexistence with classical communication networks are important.

Significant research effort is spent to improve the security of real QKD systems, affected by noise and device imperfections (actually device complexities compared to device models used in security proofs). For example, quasi-single photon sources, usually implemented by attenuating the light emitted by a laser, are vulnerable to photon number splitting (PNS) attacks. In a PNS attack, the additional photons emitted by the source are used indeed by an eavesdropper to extract information, without perturbing the photons exchanged by sender and receiver. To deal with PNS attacks, the decoy states protocol [5] was invented, where additional states, different in power compared to the data states, randomly replace the data and are used as decoy to understand if an eavesdropper is trying to having access to the channel. Other kinds of attack exploit some device characteristics deviating from the ideal simplified model, such as saturation power and non-linearity of photodectors. For this reason, a new design paradigm of QKD protocols is to avoid implementation dependencies. A well-known example is the Measurement-Device-Independent (MDI) protocol [6], [7]. MDI introduces a centralized node, to which the communicating partners send photons. The node can be untrusted and the photons are jointly projected in a base with four maximally entangled states. As in regular QKD, any eavesdropper would perturb the measurement in a way that can be detected by the communicating partners. MDI was experimentally demonstrated in several works [8].

No industrialization will be possible for QKD systems until they can be realized with cost effective technology. As happened in classical optical networks, integrated photonics is expected to lead to a considerable decrease of cost, size and power consumption. Examples are III-V single-photon or entangled-photons sources integrated on silicon or silicon nitride. The technology of single photon detectors is at an earlier maturity level: III-V single-photon avalanche diodes (SPADs) are already being developed but waveguide single-photon avalanche diodes (WG-SPADs) monolithically integrated in silicon are potentially more suitable of massive production and room temperature

operation. Two dimensional materials, such as Graphene, may lead to further advances, such as true single photon emitters at quasi room temperature.

QKD has several application domains, very different in timeline, target cost and system requirements. QKD optical links are the most known application and probably the first to come to market. For example, the distance between data centers is often in the order of tens of kilometers, which is very achievable with QKD. Moreover, big service providers may afford the economical effort needed to build dedicated quantum communication infrastructures. Service critical or military infrastructures are other use cases for dedicated QKD links. In terrestrial optical networks, CV-QKD has an advantage, compared to DV-QKD, in its compatibility with commercial devices but many implementations still have more limitations in terms of security and distance.

With respect to telco networks, the compatibility with installed classical networks remains a big issue, with both DV- and to a lesser extent CV-QKD, and it will be discussed in section 3.1.2 of this paper. Aerospace applications are another short term opportunity for QKD, due to their low cost sensitiveness compared to terrestrial networks. In low and medium earth orbit (LEO/MEO), the proximity to the earth surface ensures acceptable link losses, but the high satellite speed is a drawback. Vice versa, in geostationary earth orbit (GEO), the high distance from the earth to the satellite is an issue, but the link can be maintained continuously. In space or air, DV-QKD is easier to implement than CV-QKD since the polarization state is unaffected by propagation in free space, while CV-QKD requires an accurate channel estimation, difficult to perform in presence of a highly variable atmospheric channel and rapidly changing position of the satellite. Other potential applications segments for QKD are the Industry 4.0 and the Internet of Things (IoT) as recently demonstrated in [104] Keeping sensors and devices small and cheap is crucial in the IoT. So, QKD is expected to fly only if highly integrated devices operating at ambient temperature, such as silicon photonic devices, will come. Since the devices are mostly mobile, guided communication is not suitable and free space QKD with polarization encoding is likely to be used.

In general, severe cost reduction actions are required to make QKD commercially appealing. In [9] it is estimated that at current prices a small QKD network with less than ten nodes would cost today about one million euros, only for the equipment, and similar numbers hold for satellite systems. In telecom networks, the cost is dominated by light sources and detectors (about 100k euro each). Their cost is expected to decrease to about 10k euro by 2022.

### **2.1.2 Quantum Random Number Generators (QRNG)**

Quantum Random Number Generators (QRNG) [70] will be probably the first quantum based device to achieve cost effectiveness. Their cost starts from thousands of euros, for the most performing ones, and is expected to decrease to tens of euros in a couple of years for cost effective QRNGs for IoT applications.

If QRNG is to be generally used in various types of mobile devices, the size and power consumption of QRNG chip should be as minimized as possible. Especially, QRNG based on quantum optical processes was not easy to implement in smaller size enough to be embedded in mobile devices because of the size of optical components inside QRNG which are necessary to generate random numbers. However, with the help of advanced semiconductor manufacturing technology, the state-of-the-art QRNG chip was recently developed in the smallest size in the

market enough to be embedded in mobile and IoT devices. This is the first step to go forward with QRNG technology in many secure IoT environment. [10] [68]

On the other hand, there is no certification procedure for QRNG as yet and this is another obstacle to overcome in order to proliferate QRNG technology in many secure areas. A certification procedure for QRNG can be developed on the basis of standards but there are currently no existing standards that explicitly distinguish between noise sources based on classical physics and ones based on quantum physics. Along the standardization activity for this purpose, ITU-T approved the first recommendation (ITU-T X.1702 [70]) in QRNG in 2019 and this recommendation is an add-on to existing noise or entropy source standards that allow specification of the noise source under evaluation based on quantum physics. [11] [69]

In summary, QRNGs, which generate random numbers using actual quantum physical process, in principle can guarantee the maximum entropy, i.e. level of randomness. Clearly, it should be mentioned also that today there is long-established cryptographic communications trust in well-designed PRNGs with well-generated seeds. Hardware-based True Random Number Generators (TRNGs) are also widely available. Potential advantages of using QRNG vs TRNG / PRNG require further study [102], [103]; they may also depend on the application areas (communications, Internet of Things, Artificial Intelligence and Machine Learning, Soft Computing etc).

### **2.1.3 Blockchain and Quantum Security**

As carriers and enterprises adopt and deploy public-private blockchains whether Hyperledger, Ethereum, and Corda (as examples) it is essential to assess current blockchain security weaknesses that could be eventually quantum resistant. Some of the algorithms deployed today include:

- RSA (Rivest–Shamir–Adleman) for encryption and based on the hardness in solving the factorization problem for example discovering the factors of a large composite number is difficult when the integers are prime numbers.
- ECDSA (Elliptic Curve Digital Signature Algorithm): As a signature scheme that is based on the hardness of solving the discrete logarithm problem.

Peter Shor, a mathematician invented a quantum algorithm in 1994 that breaks the RSA algorithm in polynomial time vs 300 trillion years on a classical computer for RSA with 2048-bits.

ECDSA has demonstrated to be vulnerable to a modified version of Shor's algorithm and is easier to solve than RSA with quantum computers because of the smaller space. For example, a 160-bit elliptic curve cryptographic key could be broken on a quantum computer deploying circa 1000 qubits whilst considering the security-wise equivalent 1024 bits RSA modulus that would require about 2000 qubits.

#### **2.1.3.1 Blockchain Cryptographic Primitives Review**

Within blockchain, the hashing function is to generate a fingerprint or “hash” of an arbitrary sized input. With a secure hashing function, it is difficult to revert the hash's function output to the original input [12] [13] [14].

Hash functions can be implemented for various purposes, for example for creating identifiers for transactions or blocks, generating addresses, generating random numbers, confirming the integrity of transactions and blocks or zero-knowledge proofs.

Unpredictability of the hash function output is a key attribute in cryptographic hash Functions. There are numerous hash functions. Secure Hash Algorithm 3 (SHA3) is a family of hash functions selected by the US National Institute of Standards and Technology. Bitcoin uses the older SHA2 family of hash functions for computing addresses, transaction hashes and block hashes in addition for its Proof of Work consensus algorithm. Ethereum uses Keccak a predecessor of SHA3 for similar purposes. Blake2 is another hash function which is purported quicker than the aforementioned hash functions (and secure) [87].

Digital Signature Algorithm [DSA] is another blockchain primitive for review. DSA may be implemented to publicly verify the authenticity of a transaction. Within the blockchain domain, DSAs are used to on Elliptic Curves (ECDSA), as a public -key primitive. Recall that a public cryptography key-pair consists of a private key and a public key. The private key is used to sign a transaction and the public key is used for signature verification.

An alternative to elliptic curves are hash based signatures like Winternitz One-Time Signatures (WOTS). When using WOTS, one needs to create a key-pair for each signature. With WOTS the digital signature is assumed to remain “unforgeable”. In practice, Bitcoin and Ethereum use elliptic curve secp256k1 for digital signatures. Secp256k1 was designed by the NSA (National Security Agency). Bernstein’s Curve25519 was designed to be faster than secp256k1. WOTS is believed to be quantum-resistant (at the moment) but requires more space. Edwards Curve Digital Signature Algorithm (Ed25519) is an elliptic curve digital signature algorithm that implements a variant of Schnorr signature based on twisted Edwards curves.

In summary, there is a need of exploring threads, challenges and also the potential opportunities in adopting quantum technologies, and the post-quantum approaches, in the blockchain domains applications.

## 2.2 Quantum Computing

Current computers manipulate individual bits, which code information in terms of sequences of binary states 0 and 1. Quantum computers leverage on quantum mechanical phenomena to manipulate qubits, which are the basic unit of quantum information.

A qubit can be coded by a quantum entity having two-states or levels. For instance, electrons which can have spin up and spin down, and photons which possess several independent properties such as polarization, spin angular momentum or orbital angular momentum.

While a bit is either 0 or 1, a qubit can stay simultaneously in the overlapping of two values 0 and 1 (superposition of states), until it collapses, for example, when a measurement is made.

This is a remarkable quantum phenomenon: a qubit can be seen as a linear combination of the two states (0, 1) with coefficients which are complex numbers. This means that two qubits can be in a superposition of four states, three qubits can be in a superposition of eight states... and so on. Therefore, generalizing while N bit can take one of  $2^N$  possible permutations, N qubit can stay in a superposition of all  $2^N$  possible permutations.

This allows quantum computers to perform “a sort of parallel computation” reducing the processing time (from exponential to polynomial time) for solving certain highly complex problems. In fact, for instance, a quantum register - associated to N qubits - may have a state which is the superposition of all  $2^N$  values simultaneously: therefore, by applying a quantum operation to the quantum register, this would result in altering all  $2^N$  values at the same time.

### 2.2.1 Quantum Annealer and Gate-based Quantum Computers

There are two main classes of quantum computers: analog and gate-based quantum computers. In particular:

- Quantum annealers are examples of analog quantum computers. On the other hand, it should be mentioned that quantum annealers are not proper quantum computers: they are specialized computing systems based on quantum heuristics. In most cases, the problem to be solved is encoded into an Ising-type Hamiltonian, which is then embedded into a quantum hardware graph to be solved by a quantum annealer.
- Gate-based quantum computers, sometimes referred to as universal quantum computers, use logical gate operations (AND, OR, etc.) on qubits. Quantum logic gates are the building blocks of quantum circuits: for example, CNOTs (controlled NOT gate) and unitary single qubit operations form a universal set of quantum computing.

Gate name	# Qubits	Circuit Symbol	Unitary Matrix	Description
Hadamard	1		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	Transforms a basis state into an even superposition of the two basis states.
T	1		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$	Adds a relative phase shift of $\pi/4$ between contributing basis states. Sometimes called a $\pi/8$ gate, because diagonal elements can be written as $e^{-i\pi/8}$ and $e^{i\pi/8}$ .
CNOT	2		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	Controlled-not; reversible analogue to classical XOR gate. The input connected to the solid dot is passed through to make the operation reversible.
Toffoli (CCNOT)	3		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$	Controlled-controlled-not; a three-qubit gate that switches the third bit for states where the first two bits are 1 (that is, switches  110> to  111> and vice versa).
Pauli-Z	1		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	Adds a relative phase shift of $\pi$ between contributing basis states. Maps  0> to itself and  1> to - 1>. Sometimes called a “phase flip.”
Z-Rotation	1		$\begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$	Adds a relative phase shift of (or rotates state vector about z-axis by) $\theta$ .
NOT	1		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	Analogous to classical NOT gate; switches  0> to  1> and vice versa.

Figure 1 – Quantum Logic Gates

The following figure shows a comparison of the two approaches, quantum annealers and quantum gate-based computing, in solving a problem. In the gate-based approach the problem is formulated in a way for selecting a proper quantum algorithm. Then the quantum algorithm is transformed in a quantum circuit (i.e., using quantum gates) which is either executed on a quantum processor or simulated.

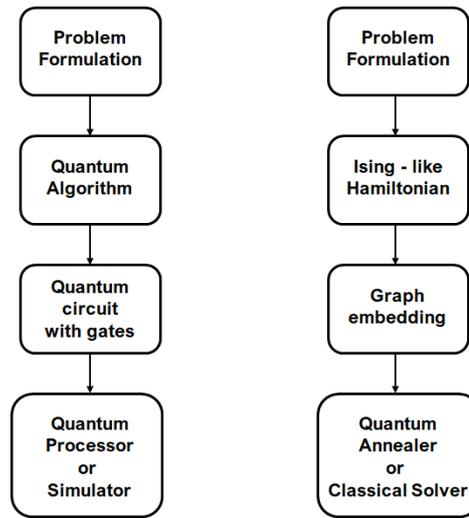


Figure 2 – Comparison of quantum annealers and quantum gate-based computing

There are multiple ways to build gate-based quantum computers manipulating qubits. Table 1 provides an overview (not exhaustive): superconductors and trapped ions are presently the most advanced implementations [15].

Superconducting currents	Electrons Spin	Rydberg Atoms	Topological	Ion Trap	Neutral Atoms	Photons
Superpositions of currents flowing in superconductors	Qubits encoded in spin of electrons confined in quantum dots or in holes	Qubits Encoded in Rydberg Blockade entangled gates in Silicon	Topological quasi-particles (for example, Majorana particles)	Ions trapped in electric fields	Atoms trapped in magnetic or optical fields	Qubits encoded in quantum states of photons
IBM Rigetti	Intel, QuTech	In progress [88]	Microsoft	IonQ Honeywell	CloudQuanta Atom Computing	Psi Quantum Xanadu

Google				AQT		ORCA
Alibaba						

Table 1 - Examples of approaches for developing quantum computers

Random fluctuations (for example, heat, ionizing particles [89] or quantum-mechanical phenomena) could occasionally flip or randomize the state of qubits: this is introducing errors and potentially derailing the validity of the calculations.

This is also why many of these quantum systems require special vacuum environments, the adoption of cryogenic systems and error corrections methods. In particular, quantum error correction involves a substantial multiplication of resources: the number of physical qubits required may be orders of magnitude greater than the number of error-free logical qubits seen by the algorithm.

### 2.2.2 Simulating Gate-based Quantum Computers

It should be mentioned that it is also possible to simulate sufficiently small quantum-gates computers by using classical computers. There exists a variety of software libraries that can be used, each with different purposes: a comprehensive list of tools is available on Quantiki [16]. Simulation can be made, for instance, using OpenCL (Open Computing Language) [17] which is a general-purpose framework for heterogeneous parallel computing on standard hardware, such as CPUs, GPUs, DSP (Digital Signal Processors) and FPGAs (Field-Programmable Gate Arrays).

### 2.2.3 Quantum Algorithms and Software

Most of the optimization problems in the fields of ICT and Telecommunications are currently solved with algorithms for finding suboptimal solutions, because of the excessive cost of finding an optimal solution. Some of these problems includes: for example, network planning, joint optimization of multiple functions, such as radio channel estimation, data detection and synchronization, Data Center resources and energy optimization.

In general, we may say that there are two main classes of quantum algorithms, derived as generalization from the Shor’s algorithm for factoring (capable of breaking a lot of public-key cryptography) and the Grover algorithm for searching.

The website “Quantum Zoo” [18] has gathered a comprehensive list of said classes of algorithms, briefly describing their operation.

For near term quantum applications, hybrid quantum/classical algorithms are also very promising. A common characteristic of these approaches is that the quantum computer is rather simplified: it is only in charge of carrying out a subroutine, acting as a “coprocessor” while the larger scale algorithm is governed by a classical computer. In this case a higher error rate per operation is tolerable. It may even be possible to implement such quantum algorithms without quantum error correction.

In summary, when comparing quantum algorithms with their classical counterparts, it appears that employing quantum systems specific performance targets may be reached at a lower computational complexity: on the other hand, an analytical demonstration of the levels of efficiency of quantum computers and algorithms in addressing computational complexity require further studies.

Concerning software languages and tools, the scenario is very active but still rather fragmented: the reference [19] provides an overview of open-source software projects and encourages the coalition of larger communities.

## 2.2.4 Optical Quantum Computing

It is possible to use photons to perform quantum computation tasks, in different technological sectors. The oldest solution was to use one different optical mode to encode the different values of qubits (for example  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$  and  $|11\rangle$ ). A more interesting way are the superpositions of coherent states.

Example of Xanadu: they use continuous variables for on-chip photonic processing using optical nonlinearity to produce “qumodes”. These basic quantum variables can perform both quadratures and mode operators on three different states (coherent, squeezed and number states). Different gates are possible and measurements are homodyne or heterodyne or photon-counting types. The main goals of this technology are photonic integration, room temperature operation and implementation of machine learning techniques in their future optical computers (see example in 2.3 Quantum Technologies for Machine Learning chapter). Above are examples of micro-ring (magnified picture) and Xanadu elementary circuit:

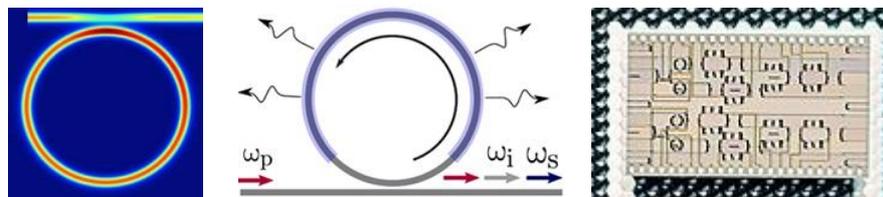


Figure 3 – Xanadu Micro-Ring views and its first optical chip

The other example is a french project from Quandela start-up. They work on a future optical computing platform (integrated photonic qubit generator Promotheus). Again the goals are integrated photonics and use of Quantum Dots (single photon qubits), taken advantage of their single and identical source of photons expertise:

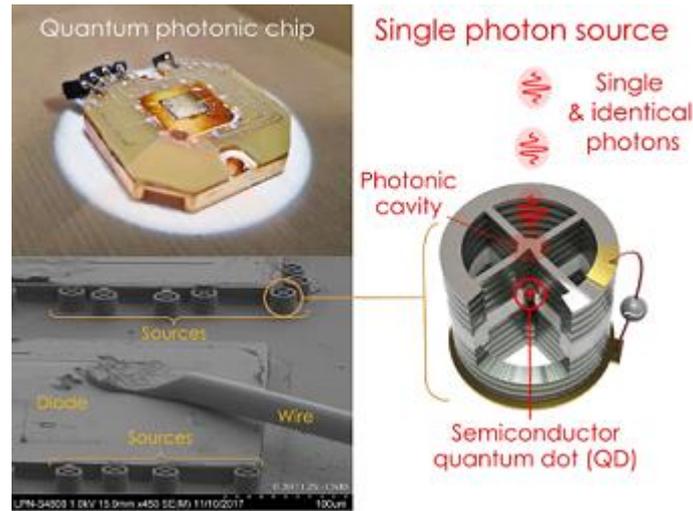


Figure 4 – Quandela single and identical photon source, used in Optical Computing.

Last examples use different technology but are also very interesting in the use of Photonic Integration:

USA example of ARL (Army Research Laboratory): Photonic Integrated Circuit (PIC) for a 128-qubit prototype chip for quantum computing [97]. They use QMC (Quantum Micro-chiplet), something as diamond waveguide arrays containing highly coherent colour centres. It is the first example of prototype chip with 128-channel, defect-free array of germanium-vacancy (GeV) and silicon-vacancy (SiV) color centers in an aluminum nitride PIC:

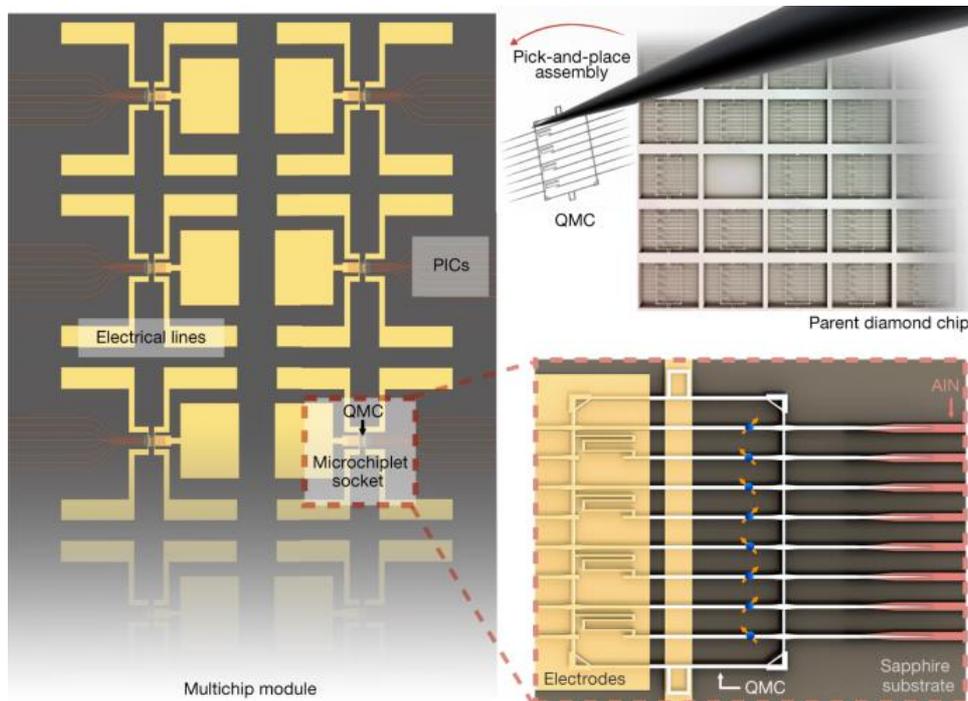


Figure 5 – ARL artificial atoms integration in photonics (pick-and-place method).

German (Helmholtz-Zentrum Dresden-Rossendorf, Technische Universität Dresden) example: Creation of high brightness single-photon emitters in classical silicon-on-insulator (SOI) wafers [90]: Emitted photons in the infrared spectral range (see telecom O-band), emitters are carbon color centers in silicon (so-called G centers), use of  $^{12}\text{C}$  and  $^{28}\text{Si}$  isotopes:

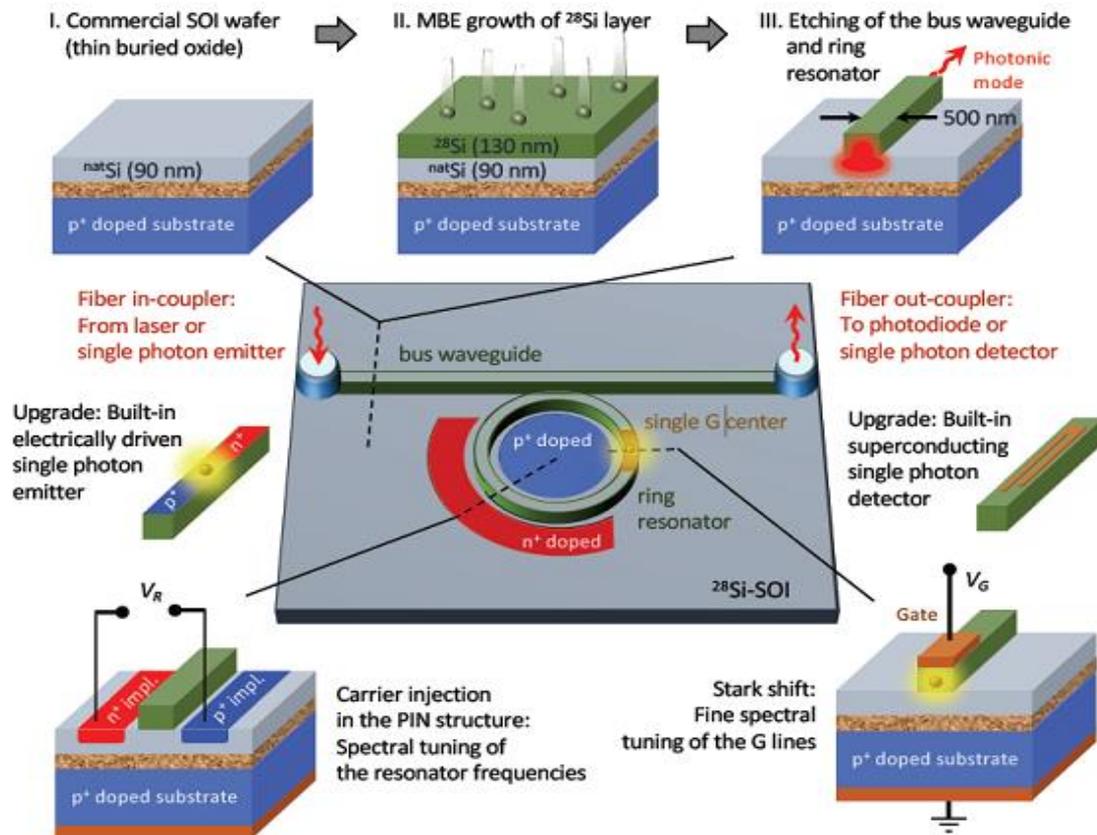


Figure 6 - Engineered single G centers in SOI wafers for quantum photonics

Synthesis of German work is a path to scalable quantum photonic platform (with single-photon sources, waveguides and detectors on SOI chip).

In general, among the different technological approaches for optical computing and networking, topological photonics is a rapidly growing field of innovation. Since the discovery of the quantum Hall effect and topological insulators in condensed matter, progressive advances in topological photonics hold great promise for optical networking and quantum computing applications.

As a matter of fact, a future scenario pursuing deeper and deeper integration of optical communications and quantum optical computing would offer several techno-economic advantages and topological photonics using OAM could be the technology playing this role. For instance, it would be possible to use OAM not only for optical quantum computing, but also for routing, switching and dropping photonic channels in the spatial domain. The common element is taking advantage of the beam structure and orthogonality among different OAM photonic modes [100].

The development and exploitation of this technology would greatly benefit from advances in the devices and subsystems (e.g., processors, transmitters, (de)multiplexers and receivers) based on quantum materials. Applications would be far-reaching and cover a range of applications, from super-dense coding to teleportation in quantum communications and quantum optical computation.

## 2.3 Quantum Technologies for Machine Learning

Machine Learning methods are more and more used in telecommunications operators.

For example, three methods can be cited: supervised learning (as a pupil with a teacher), unsupervised (unlabeled data), and reinforcement (the algorithm learns by feedback mechanism and previous tests).

Classical machine learning for telecommunications operators can be used from customer's data banks (as in Big Data context) or IoT data, but can be very useful for network data (as fiber optical links operational measurements).

Quantum Machine Learning (QML) is an emerging domain but already with several of tools and methods. The first reflex is to think of QML with current quantum computers. But considering the price and the operational complexity of these machines, one can imagine the success of quantum computing methods in the cloud.

Below few examples can be highlighted, both from suppliers and operators. In a more interesting way, it will be certainly possible to work in the future with simplified and miniaturized quantum computers (some kind of quantum co-processors) or with small quantum optical processors, for example Xanadu's proposal.

- Examples of methods and tools :
  - Variational Quantum Eigensolver (VQE), Quantum Support Vector Machines (QSVM), Quantum Neural Networks (QNN), QUBO (Quadratic Unconstrained Binary Optimization), ...
- Examples of relevant telecommunications topics for QML :
  - Infrastructure layout, network capacity, resilience, security, Operations Administration Maintenance (OAM); content distribution, client recommendation, ...
- QML from the cloud :
  - [Quantum Tensorflow](#) from Google. It is a quantum machine learning library for rapid prototyping of hybrid quantum-classical ML models. Research in quantum algorithms and applications can leverage Google's quantum computing frameworks, all from within TensorFlow. TensorFlow Quantum focuses on quantum data and building hybrid quantum-classical models. It integrates quantum computing algorithms and logic designed in Cirq, and provides quantum computing primitives compatible with existing TensorFlow APIs, along with high-performance quantum circuit simulators.
  - [Quantum Azure](#) from Microsoft. It provides an open-source development kit to develop quantum applications and solve optimisation problems. It includes the high-level quantum programming language Q#, a set of libraries, simulators, support for Q# in environments like Visual Studio Code and Jupyter Notebooks and

interoperability with Python or .NET languages. The ecosystem involves partners such as Honeywell, IONQ, Quantum Circuits, Inc., 1Qloud.

- [Pennylane](#) from Xanadu. It is a cross-platform Python library for quantum machine learning, automatic differentiation, and optimization of hybrid quantum-classical computations.

- Example of QML on Continuous Variables (as in CV-QKD) from Xanadu :

Figure below is an example of circuit structure for a single layer of a [CV Quantum Neural Network \(QNN\)](#):

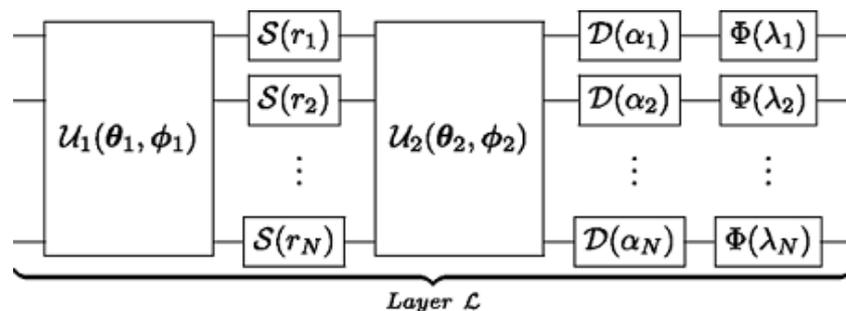


Figure 7 - Circuit structure for a single layer of a CV quantum neural network

The sub-elements of this figure are (from left to right): An interferometer, local squeeze gates, a second interferometer, local displacements, and finally local non-Gaussian gates.

The first four components carry out an affine transformation, followed by a final nonlinear transformation.

## 2.4 Quantum Networking Integration

The scope of this section is addressing the main issues about the networking integration of Quantum Nodes and Systems (not only QKD, if any others) in a legacy/traditional telecommunication network (for example, 4G/5G).

Most of current QKD systems [59] run over point-to-point fiber links. This requires the availability of dark fibers and, for long distances, the need to regenerate the key in trusted nodes, with a negative impact on cost and security. Moreover, practical QKD systems use one-time pad encryption only for the secret key and need a parallel classically-authenticated communication channel. Building a wide-area optical network where classical data channels and quantum key channels coexist is critical for deploying QKD systems in telecom operator's infrastructures. A first issue to deal with is the difference in transmitted optical power of classical and quantum channels, since quantum channels use single or few photons transmitters. In systems where classical and quantum channels are wavelength multiplexed, this may result in significant crosstalk or non-linear effects penalty. A second issue is given by the limited achievable link distance with QKD, a few hundreds of kilometres, due to channel loss and noise. Classical amplified long-haul systems can

reach thousands of kilometres but optical amplification is not an option for QKD, due to the no-cloning theorem. Quantum repeaters would in principle be a solution but their technology is far from maturity. In addition to this, some Measure Device Independent (MDI) protocols [20], [21] may allow extending twice the reach using untrusted intermediate nodes.

A list of general requirements for a wavelength multiplexed network carrying both quantum and classical optical channels is: the adoption of a wavelength plan to minimize the transfer of linear and nonlinear noise from classical channels onto quantum channels; the use of high-isolation optical filters to remove from the QKD wavelengths any crosstalk from classical channels and optical amplification spontaneous emission noise; optical devices for allowing the quantum channels to bypass the optical amplifiers; and means for accurate estimation of noise. However, no optical filter can remove in-band noise generated by linear and non-linear scattering in fiber. Raman scattering is especially detrimental [22] and requires a proper wavelength allocation plan and channel power control. Reconfiguration is also highly desirable in an optical network. Today optical networks use tunable lasers and reconfigurable optical add drop multiplexers (ROADMs) to reroute optical channels. Depending on the underlying technology, ROADMs can be used also with quantum channels [23] but they are not currently designed for them. For example, the inter-channel crosstalk could be too high.

Facing physical impairments is not the only challenge to deploy QKD networks on large scale: easy network control and configuration are the key. Examples of extension of Software Defined Networking (SDN) and Network Function Virtualization (NFV) to quantum communication networks are reported in [24]- [33]. Also recent advances in Machine Learning (ML) can help the automated configuration of QKD networks, which is critical considering that their performance depends of many parameters to be finely tuned [31], [34]. Finally, standardization is important to develop interoperable multi-vendor systems. QKD standardization started at ITU-T in Study Group 13, resulting in the Y.QKDN draft Recommendation series. Security aspects of QKD Networks were studied in Study Group 17, resulting in Technical Report on security considerations on QKD networks [59], and several recommendations including X.1710 as security framework for QKD networks [70], and X.1714 for key combinations and confidential key supply for quantum key distribution networks [71]. At ETSI, the Industry Specification Group (ISG) on quantum key distribution for users was established to enable digital keys to be shared privately without relying on computational complexity. At IETF, the Quantum Internet Proposed Research Group (QIRG) investigates the new communication and remote computation capabilities offered by quantum technologies.

When telecom operators consider introducing QKD network into their existing classical optical networks, there are a few architectural options to choose from, for example, integration of quantum channel and classical optical channel in a single optical fiber or separation of them in different optical fibers. As there are two major technical issues in the case of transmitting both quantum channel and classical optical channel in a single optical fiber as pointed out in the previous section in terms of differences of transmitted optical power and achievable link distances of both channels, telecom operators can optionally choose to separate quantum channel in quantum key distribution (QKD) network from classical optical channel in optical transport network (OTN) for the sake of the stable performance of QKD network in fiber rich environment. In this separation case, along the design principle of software-defined network architecture, QKD network and OTN can be controlled by each software-defined network controller (SDNC), respectively. However, if the cryptographic

keys generated by QKD network are to be supplied to encryptors in OTN for cryptographic use, telecom operators should know which QKD nodes in QKD network can supply the generated cryptographic keys to which encryptors in OTN. Each SDNC has only its controlled network resource information, that is, QKD nodes or encryptors, respectively. Therefore, for the overall operation of cryptographic key generation in QKD network and its use in OTN, telecom operators need to control both QKD network and OTN through each SDNC under the same SDN orchestrator (SDNO). This SDNO and SDNC architecture plays the role of matching the addresses of QKD nodes in QKD network and encryptors in OTN to supply encryptors in OTN with cryptographic keys generated by QKD network. In addition, telecom operators can operate and maintain overall QKD network and OTN via an SDN orchestrator with respect to each network configuration and topology, management policy, and statistics, etc. So, this architectural option can mitigate the burden of adopting QKD network into the current telecom networks which already have an SDNO for SDNCs of OTNs.

To consider the mechanisms for integrating future quantum and current classical networks, it is necessary to start by identifying the foundations for this integration, describing the appropriate abstractions defined by the current trends in networking, based on the SDN reference architecture [35], and identifying which are the interfaces that need to be considered to analyse the achievable integration levels and implement them.

In general terms, an abstraction can be defined as the representation of an entity in terms of those of its characteristics relevant for a particular purpose, while hiding or summarizing characteristics irrelevant to this purpose. In networking, abstractions are consistently associated to a layered approach, where each layer (termed here a *plane* to distinguish it from the layered approach used in end-to-end data exchange) focuses on a particular concern, at specific management domains, under the control of a management authority that decides which capabilities (on information and control) are exposed to other collaborating domains.

The SDN architecture distinguishes three of these planes plus a common set of management functions:

- The Application Plane is where SDN applications specify network services by the behaviour of network elements in a programmatic manner. These make use of the abstracted view of the network elements provided by the SDN controller.
- The Control Plane provides a means to control the behaviour of network resources, as instructed by the application plane. The capabilities exposed to SDN applications are abstracted by means of information and data models.
- The Data Plane is where the network elements perform the forwarding and the processing of data according to the decisions made by the upper planes.
- The Management Functions provide functionalities for managing, as appropriate, the functionalities of the planes.

At the application plane, classical networks implement the network functions associated with current network operations. For quantum networks, these functions will be associated with the purpose of the quantum links being used and likely with qubit addressability in most quantum computer interconnection scenarios. Currently, when practically all quantum network functions are associated with QKD, many applications of these keys are related to classical communications, and classical network functions act as key consumers. Further on, the application of NFV,

irrespective of whether they belong to the classical or quantum environments, should put the lifecycle management of all network functions under a common entity (in a given management domain) running on a unique MANO stack.

While the network elements to be abstracted by the control plane are radically different in classical and quantum networks, a general set of abstractions is applicable, especially in what relates to topology representations. The distinct nature of network elements and the mediator nature of the SDN control plane do not make advisable the use of common quantum/classical SDN controllers, but common abstractions could be applied to support cross-interactions within this plane, coordinated through shared topology views, or even an integrated controller.

The radical difference between the network elements in quantum and classical networks, makes interactions at the data plane not feasible, with only one exception: the possibility of co-propagation over the same physical media of quantum and classical signals. In this case, a proper control of physical parameters has to be applied to minimize interferences. Though co-propagation is not always technically possible, it constitutes a desirable property in many cases that demands lower deployment and operation costs.

At any given management domain, and whatever its nature, the availability of integrated management functions is an essential goal. These management functions constitute the backbone of network operations, coordinating not only the work of the different planes in the SDN architecture, but also enabling essential functions such as planning, accounting and provisioning, and therefore both quantum and classical network will need to be coordinated. With this purpose, a loosely-coupled, open, SBA-based architecture like the one proposed by ETSI ZSM [36] seems the most appropriate. This architecture is suitable as well for inter-domain cooperation, essential for many, if not all, network application. For a very recent synthesis about QKD in the networks, see reference [37].

## 2.5 Quantum Sensing and Metrology

As first remark, we can underline that the new international Units System (S.I. in short) is defined from May 2019, using quantum constants as means to define all the main [units](#) thus facilitating the adoption of quantum technologies in metrology.

In classical metrology, the main artefacts come from imperfections for the device used for measurements, the limits of the method used and the fundamental limits from the physics. These limits are shot-noise level (SNL) and at the limit Heisenberg uncertainty relations (for example energy-time or position-velocity). In quantum metrology, we can use quantum resources (for example entanglement or squeezing) to improve the performance of measurements (going below shot-noise level), both in precision and sensitivity.

As shot-noise level is cited, we can specify that for the photons (for example with a laser), quantum noise has two parts, photon shot noise (at high frequencies) and photon radiation pressure noise (at low frequencies). This remark allows us to define Standard Quantum Limit as the minimal sum of shot noise and radiation pressure noise.

Again in the case of laser, the emitted light has an average frequency and amplitude, in the figures below it is the blue arrow, but individual photons have uncertainty around these average values, it is the ball in gradient of red.

Thanks to squeezing resource in quantum physics, it is possible to choose a transformation applied to this uncertainty disk (which has a minimal area due to Heisenberg,  $\Delta X_1 \Delta X_2 \geq 1$ ) to have less uncertainty in one quadrature but more on the other:

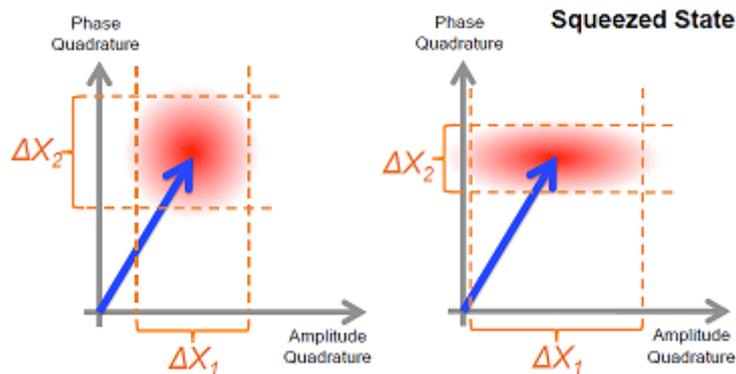


Figure 8 - Pictorial explanation of noise squeezing

There's a family of possible squeezing operations (quadrature, amplitude, phase (above figure), both on coherent or on vacuum states).

There are numerous examples of squeezing features used in physical systems, as in quantum metrology of course, but also in quantum communications and quantum computation [91].

The other very important resource is entanglement.

Again in optical domain, we have the example of interferometer device. It has shot-noise limited sensitivity (statistical-sampling) that scales like  $1/\sqrt{N}$ , where  $N$  is the number of particles passing through the interferometer per unit time. With the entanglement feature for the photons, the interferometer sensitivity scales like  $1/N$  (Heisenberg uncertainty limit).

But using the entanglement resource is not a limited to a single device. Entanglement can be used in distributed quantum devices, to enhance their performances.

In any sensor, a probe interacts with a system so that a measurement of the probe reveals some feature of interest of the system. In quantum sensors, the probe becomes entangled with the probed object, and quantum state superposition is exploited to obtain new functionalities or improved performances. Quantum sensing encompasses many different applications, such as: atomic clocks; gravitational, electrical and magnetic field sensors; force, pressure, and acceleration sensors; temperature sensors; ultra-high-precision spectroscopy and microscopy, etc. This section will focus on quantum technologies for mobile systems as example of application.

The size of a traditional antenna is comparable to half the wavelength of the transmitted or received radio frequency. Quantum processes can be exploited to overcome this limitation, leading to smaller footprint, broader bandwidths or improved beam pointing accuracy. Microwave Amplification by Stimulated Emission of Radiation (maser) and Rydberg Atoms are examples of technologies that can be used to generate and receive radio frequencies, respectively. The working principle of a maser is similar to laser's: a coherent beam having a definite propagation

direction is generated by stimulated emission, but in a maser the photons frequency lays in the microwave spectrum rather than the infrared or visible spectrum. Masers have a long history but traditionally they required very low temperatures to operate, making them impractical for mobile networks. Recent technology advances show the possibility for a maser to work at room temperature. In [38] a diamond with defects called nitrogen-vacancy (NV) centers is used as gain medium. Any NV center has three possible spin states. A magnetic field is applied to the diamond to separate the energy levels of the three spin states. Then, a laser pumps the NV centers into the state with the highest energy, to achieve population inversion. When the NV centers come back to the fundamental energy level, radiation is emitted. Due to the high frequency stability, these devices find application also as highly accurate clock references. Moreover, the quantum states of the NV centers have long lifetimes and long coherence times, making those suitable candidates for quantum computing. If the coherence time is higher than the photon lifetime in the cavity, superimposed quantum states are created resulting in a super radiant maser that has a frequency insensitive to temperature fluctuations.

Quantum sensors based on NV centers in diamonds can be used also at the receiving antenna, based on the fact that the NV centers have photoluminescence properties, i.e. they emit photons when their spin changes, for example due to an incident magnetic field. So, information about the incident field can be derived measuring the number of emitted photons. A quantum sensor based on NV centers in diamond has been demonstrated on a silicon chip [39], using cost effective complementary metal-oxide-semiconductor (CMOS) technology. In the chip, a laser excites the NV centers and the current in a nanowire generates microwaves close to the NV centers. The NV centers emit a different amount of red photons depending on the relative power of light and microwaves. Finally, the photons are collected by a photodiode, whose output gives the received signal.

An alternative technology for a receiving antenna uses Rydberg atoms, i.e. atoms with a highly excited outer electron. Excited outer electrons are very loosely bound to the atom, making it very sensitive to an applied electric field. Rydberg atoms can result in very small antennas with a band ranging from kHz to THz. A receiver exploiting Rydberg atoms was first demonstrated by the US Army in 2018 [40], [41]. In the experiment, atoms were placed in a glass cell at room temperature, and excited by two lasers at different wavelength, to simultaneously excite the electron state and measure the response to an applied electric field. The device correctly operated from 103 Hz to 10<sup>12</sup> Hz, i.e. over nine frequency decades [42]. The Army team also demonstrated that the receiver can achieve the best theoretically allowed performance, given by the collapse of the collective wave-function of an ensemble of absolutely identical quantum objects, i.e. the atoms [43].

# 3 Proof-of-Concepts (PoCs)

This section provides an overview of ongoing experimental Proof-of-Concepts (PoC) and use-cases experimenting the Quantum technologies describes in the previous section.

## 3.1 PoCs and use-cases on safe Security and Networking

In the short term, the deployment of QKD systems is likely to be limited to data sensitive point-to-point connections between industries, financial institutions and government agencies and offices, due to both high cost and technical reasons, such as absence of repeaters and coexistence issues with classical communication networks. Aerospace applications may grow faster than terrestrial ones, being less cost sensitive and already used for critical services: in the first deployments, satellite QKD links might be included to overcome the distance and connectivity gaps of the current fiber optics network. In the medium term, coexistence of quantum and classical communications will be tested in operator's metro networks, over short distances. The first application may be inter-datacenter interconnection networks characterized by simple network topologies, short distances and low number of network nodes.

Various publicly funded initiatives are underway worldwide to foster a Quantum Communication Infrastructure (QCI). Examples are reported in the following [44].

Several EU programmes (Quantum Technologies Flagship, QuantERA, etc.) fund quantum communications projects, including devices and systems for a quantum internet (for example QIA project), QKD enabling photonics technologies (e.g. UNIQORN project) and CV-QKD (for example CiViQ project). In 2018, the EU commission launched a 15 M€ pilot project to validate the feasibility of a QCI, with focus on multivendor interoperability, standardization and security certification (see also Appendix).

The European Space Agency (ESA), with the QUARTZ and the QKDSat projects, aims at providing QKD commercial services on LEO. GEO applications are also under study, though at an earlier technology maturity level.

In parallel, individual European countries have their own programs: quantum networks are being deployed in the Netherlands, Austria and Switzerland. Germany has recently funded a 15 M€ project for the development of quantum repeaters. In Spain, the Madrid Quantum Network (MQN), owned by Telefonica, intends to verify the technical maturity of the components of a QKD network, extending to it concepts such as network function virtualization and software defined networking [45]. Italy developed a QKD backbone from Turin to Florence and a QKD metropolitan network in Florence [46]. In the United Kingdom, the integration of QKD and 100G encrypted data transport has been demonstrated over fiber links between Cambridge, London and Bristol [47].

China is spending considerable scientific and financial effort to the development of a QCI. China launched in 2016 the LEO satellite Micius, currently used to perform several quantum communications experiments with other countries in Europe and Asia. China will launch four more LEO satellites and a GEO satellite shortly. In addition, a 2000km QKD fibre link with 32 trusted nodes connects Beijing and Shanghai and is being expanded with local networks for connecting government offices, agencies, the army, banks and utilities.

Several public and private initiatives on QKD are ongoing also in USA [1]. As relevant examples, we just report that the Los Alamos National Laboratories are working with Oak Ridge National Laboratories and a utility company to use QKD in smart grid applications and that Quantum Xchange plans to connect Boston and Washington with an 800-km QKD link based on dark fibers and trusted nodes, having the financial market as target customer [48].

In South Korea, the government is funding 250 km quantum backbone for optical metro and mobile networks, having the Korea Institute of Science and Technology Information (KISTI) and SK Telecom as main Player.

### 3.1.1 SKT PoC and Use Cases

SK Telecom has proven the feasibility of QKD technology over its LTE back-haul and 5G mid-haul networks, respectively, since 2016 and the operator has been deploying and operating QKD network in connection with its 5G network since the operator launched 5G network in 2019.

In June 2016, SK Telecom deployed QKD system for LTE backhaul network between Daejeon operation center and Sejong city over shorter distance of 38km and longer distance of 50km without trusted nodes and this deployment has been in data encryption operation to serve more than 3.5 million subscriber's data usage with cryptographic key generate rate.

As validation purpose in securing a large volume of confidential data from a smart factory through 5G network to reach SK Telecom cloud servers and to be sent back to machines and robots in the smart factory, SK Telecom deployed QKD system in point-to-point configuration on 5G mid-haul network between Ansan city and Sungsoo operation center in December 2018. A Distribution Unit (DU) is located on the smart factory site in Ansan (A) while the Central Unit (CU) is located at the SK Telecom network operation center in Sungsoo (B). Since the 5G DU to CU connectivity is using a fibre optic network, it was possible to combine QKD with the encryption on the 5G mid-haul network. The two 5G nodes are connected through a network Point of Presence defined as a Hub (H) for the encryption and QKD design as shown on the diagram below explaining the components of this use case. At this time, the overall distance is around 70km and trusted nodes were not used between QKD nodes along QKD links. [49]

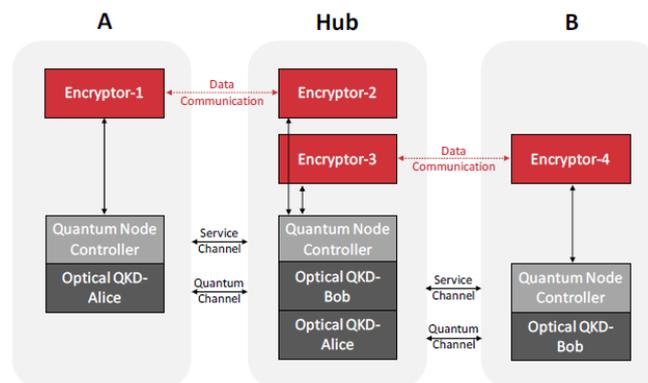


Figure 9 - QKD systems in point to point configuration

With the above proof-of-feasibility, SK Telecom deployed QKD system for 5G/LTE backbone network between Sungsoo operation center in Seoul and Dunsan operation center in Daejeon along 221 km of transmission line in April 2019 and extended QKD network to Taepyung operation center in Daegu along 380 km of total transmission line in 2020. This backbone network takes charge of about 30% of SK Telecom’s total data traffic. After this successful installation and operation in 5G network, SK Telecom has been extending QKD network rollout to reach main cities nationwide. Trusted nodes have been developed in order to extend the reach of the key exchange used by the encryptors in both ends and they are positioned in highly secure locations in SK Telecom’s premise. [49], [50]

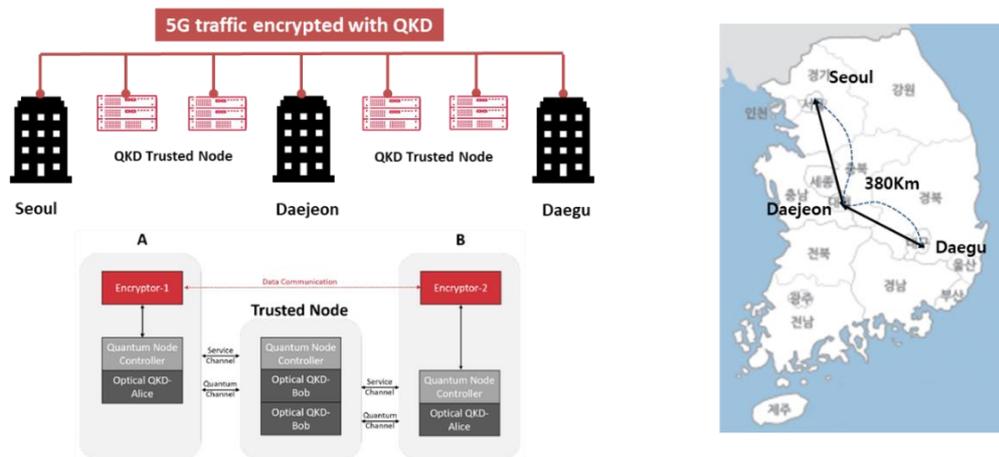


Figure 10 - Trusted node overview [50]

As another way of endeavoring to secure its 5G network, SK Telecom has begun to apply Quantum Random Number Generator (QRNG) technology to the subscriber authentication center of 5G network as well as 4G LTE network since March 2019. The authentication procedure specified in the 5G standard uses the authentication vector and one of the main parameters of the authentication vector is the random number, RAND, which provides the seed for other key generation procedures used for authentication and ciphering. QRNGs theoretically can guarantee maximum entropy, i.e. level of randomness, however today there are also established trust mechanisms in cryptographic communications with well-designed PRNGs with well-generated seeds. After identifying that the true randomness of the key used during the mobile authentication procedure was essential to achieve a high security level and the use of Pseudo Random Number Generator (PRNG) or even True Random Number Generator (TRNG) based on classical physics process is may not be enough to resist a strong computational pattern analysis, SK Telecom chose to replace the PRNG by a QRNG and this QRNG server was connected to the Home Subscriber Server providing the authentication vector to the network and 5G user equipment. Therefore, in SK Telecom’s view it improves the security of user authentication and data encryption by thwarting any attempt of analyzing secret keys. In addition, with this future-proof solution, securely connecting a high number of 5G devices for IoT applications will be possible through the authentication procedure. [51]

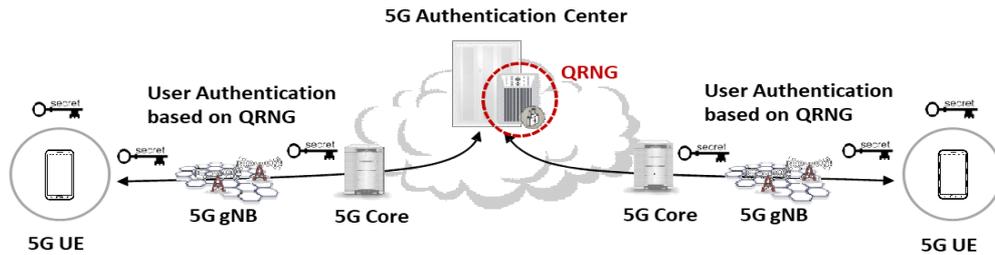


Figure 11 - QRNG in SK Telecom's 5G Authentication Center

Following the strategic direction of providing secure 5G network and services with quantum technologies, together with Samsung Electronics and ID Quantique, SK Telecom launched the Galaxy A Quantum, the world's first 5G smartphone equipped with the smallest QRNG chipset in May 2020. It allows subscribers to experience the benefits of quantum security technologies in their everyday lives with 3 kinds of SK Telecom's own services in the first phase [52].

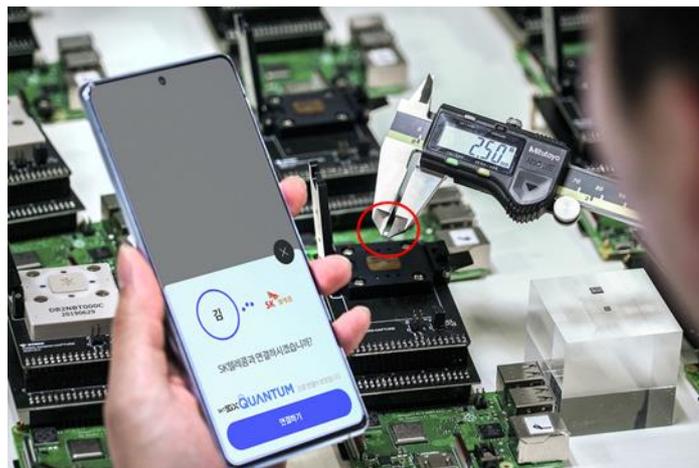


Figure 12 - ID Quantique's QRNG chip in SK Telecom's Galaxy A Quantum phone

### 3.1.2 Madrid Quantum Network (Telefonica)

The first PoC run on the Madrid Quantum Network was intended to explore technologies for a broad adoption of quantum communications technologies by means of demonstration, focusing on:

- Coexistence of quantum and classical communication on a common physical infrastructure.
- Integration with current network operation and management technologies to demonstrate achieving *carrier grade* is feasible.

- There are practical use cases in current networking practices that can benefit from the availability of a QKD deployment.

The PoC was run using three CV-QKD system developed by Huawei Research in Munich, integrated with cryptographic modules provided by researchers at Universidad Politécnica de Madrid (UPM), and managed using SDN elements developed by Telefónica Research. For demonstrating the different use cases, different pieces of open-source software (like Open-Source MANO, OSM [53]) and ad-hoc software modules when necessary, as in the case of the Ordered Proof-of-Transit presented in [54].

The overall system was integrated in a production-level network, owned by Telefonica of Spain, in downtown Madrid, connecting three production points of presence, according to the topology shown in the figure below, including distances and attenuations for the three links.

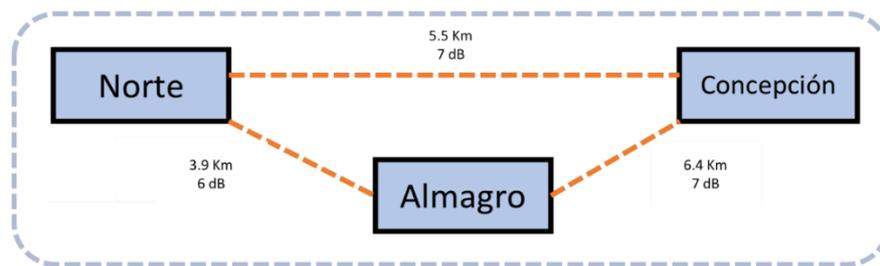


Figure 13 - Madrid Quantum Network (Telefonica)

Using this deployment, the following features were demonstrated during a period of several months, running in parallel with the commercial use of the infrastructure:

- End-to-end quantum-encrypted connections, with aggregated up to 10x10G cyphered channels sharing the fiber with the quantum channel.
- SDN-enabled management of the QKD network, demonstrating physical QKD link management, the provision and decommission of virtual QKD links, and the management of QKD applications.
- QKD support to enhance network virtualization and programmability, including the securing of network infrastructure management, the provisioning of customer managed security data services, and the application to support ordered proof-of-transit in virtualized networks.

After this field trial, another demonstration campaign is planned, in the framework of the European Quantum Flagship Initiative, within the project CiViQ [55]. Furthermore, the original quantum ring (in red in the following figure) is being extended (yellow lines) within the OpenQKD [56] project, including nodes of the Madrid academic network, Redimadrid.

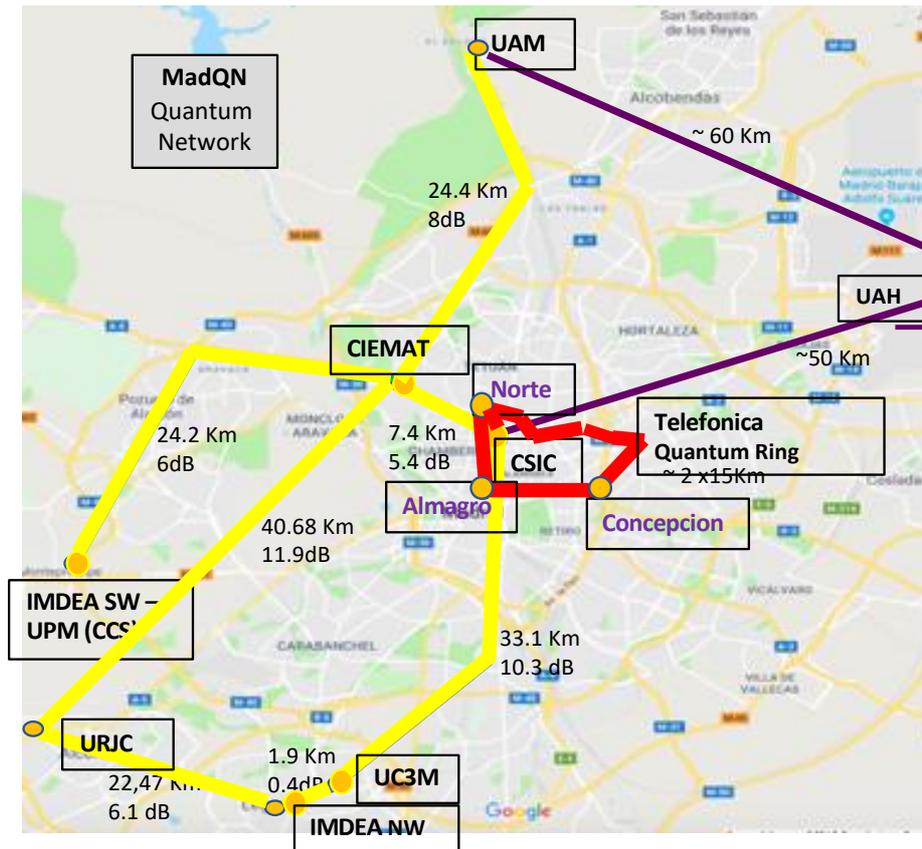


Figure 14 - Madrid Quantum Network extended in OpenQKD

For this new deployments, evolved use cases, more oriented to direct services to operational units and customers, are being planned for the coming two years, including:

- Network attestation, covering infrastructure and function attestation in NFV deployments, as well as topology attestation for SDN environments.
- Critical infrastructure protection.
- QKD as a cloud service, making available key streams to third-party applications running at different datacenters.
- B2B enabled by edge and 5G networks, supporting stronger crypto for edge deployments.
- Self-healing network management, with enhanced security to vouch for autonomic decisions and data flows.

### 3.1.3 Other examples of use cases

#### 3.1.3.1 Verizon trail on QKD

Verizon set-up a trial QKD network in the Washington D.C. area [92]. Live video was captured outside of three Verizon locations in the D.C. area, including the Washington DC Executive

Briefing Center, the 5G Lab in D.C and Verizon's Ashburn, VA office. Using a QKD network, quantum keys were created and exchanged over a fiber network between Verizon locations. Video streams were encrypted and delivered more securely allowing the recipient to see the video in real-time while ensuring hackers are instantly detected. A QKD network derives cryptographic keys using the quantum properties of photons to prevent against eavesdropping. Verizon also demonstrated that data can be further secured with keys generated using a QRNG that creates truly random numbers that can't be predicted. With QKD, encryption keys are continuously generated and are immune to attacks because any disruption to the channel breaks the quantum state of photons signaling eavesdroppers are present.

### 3.1.3.2 BT deployment of QKD

[BT has announced](#) that, in partnership with Toshiba Europe, it has installed the "UK's first industrial deployment of a quantum-secure network" on a 6km link between the National Composites Centre (NCC) and the Centre for Modelling and Simulation (CFMS) in Bristol.

No special fibre is required for such a deployment: link uses fibre already laid by BT's semi-autonomous fixed access network division Openreach. Toshiba's QKD system enables the distribution of thousands of cryptographic keys per second, with the data and the quantum keys transmitted on the same fibre, "*eliminating the need for costly dedicated infrastructure for key distribution,*" notes BT in this announcement about the deployment.

BT notes that the current maximum distance for QKD-enabled connections is 120 kilometers, but that would be enough to at least enable highly secure data transmission across major cities, and even between them.

## 3.2 PoCs and use-cases on Quantum Technologies for Machine Learning

One of the most demanding tasks of Machine Learning and Artificial Intelligence is extracting patterns and features directly from collected big data. Amongst the various most promising approaches for accomplishing this goal, Deep Neural Networks (DNNs) [57] are outperforming. The reason for the efficiency of DNNs is not fully explained, but one possible explanation, elaborated in literature, is that DNNs are based on an iterative coarse-graining scheme, which reminds us of an important tool in theoretical physics, called the renormalization group (RG) [58]. In fact, in a DNN, each high-level layer learns increasingly abstract higher-level features, providing a useful, and at times reduced, representation of the features to a lower-level layer. This similarity, and other analysis described in literature [59], suggests the intriguing possibility that the principles of DNNs are deeply rooted in quantum physics. In fact, photonic crystals, plasmonics, metamaterials, metasurfaces, and other materials performing photonic behaviors have already been considered for developing DNNs.

In [60], an interesting PoC of an all-optical diffractive deep neural network (D<sup>2</sup>NN) is described. A D<sup>2</sup>NN is made of a set of diffractive layers, where each point (equivalent of a neuron) acts as a secondary source of an EM wave directed to the following layer. The amplitude and phase of the secondary EM wave are determined by the product of the input EM wave and the complex-valued transmission or reflection coefficient at that point (following the laws of transformation optics). In this example, the transmission/reflection coefficient of each point of a layer is a learnable network parameter, which is iteratively adjusted during the training process (for example, performed in a computer) using a classical error back-propagation method. After the training, the design of the

layer is fixed as the transmission/reflection coefficients of all the neurons of all layers are determined.

Another PoC of a nanophotonic DNN is reported in [61]. This is generalizing the model of the D<sup>2</sup>NN, where the neural layers are physically formed by multiple layers of programmable metasurfaces. In this case, each point on a given metasurface represents a neuron that is connected to other neurons of the following metasurface through the transformation optics principles. On the other hand, the programmability of the metasurface allows a change in the refractive index of each point of the metasurface, dynamically. A training phase is still required to iteratively adjust the refractive indices, but these indices are not fixed (as in D<sup>2</sup>NN). There are already examples of programmable metasurfaces with switching diodes and mechanical micro/nano-systems [60], [63].

A global vision of benefits of Machine Learning for Quantum Communication (including for quantum repeaters) can be found in the reference [99]

### 3.3 PoCs and use-cases on Quantum Computing

#### 3.3.1 Application of quantum computing to cell-ID planning of 4.5G and 5G networks (TIM)

In this PoC TIM has optimised the planning of radio cells, framing the problem within a QUBO (quadratic unconstrained binary optimisation) algorithmic model, carried out on D-Wave's 2000Q™ quantum computer. All this has made it possible to develop radio cell planning that ensures reliable mobile services with high performance [105].

In the mobile network, the "cell" is defined as the elementary unit of territory corresponding to a transmitting antenna and a specific frequency band. The identification of the cell, precisely through the PCI (Physical Cell Identifier), allows mobile terminals to manage mobility procedures in the handover between geographically adjacent cells.

The PCI identifier is assigned to each cell of the mobile network within a predefined set of values, which varies from system to system based on the specific characteristics of the network and is expressed through the relationship:

$$PCI = 3 \cdot Group\_ID + Cell\_ID$$

Equation 1

where *Group\_ID* is a number that identifies the site, and *Cell\_ID* is a number used to distinguish the cell within the site (a site can group up to 3 cells).

The values *Group\_ID* and *Cell\_ID* may span different ranges, depending on the network being 4G or 5G:

For 5G:  
*Group\_ID* ∈ [0; 335]; *Cell\_ID* ∈ [0; 2]

For 4G:  
*Group\_ID* ∈ [0; 167]; *Cell\_ID* ∈ [0; 2]

The ultimate goal of PCI planning is the definition of a "plan" that avoid or at least minimizes the problems related to the so-called cases of "collision" (equal PCI assigned to adjacent cells) and "confusion" (equal PCI assigned to cells having adjacency in common) briefly illustrated in Figure 15:



Figure 15 - Collision and confusion conditions between cells of 4.5G or 5G networks

The cases of collision and confusion lead to interruptions of the mobility procedures that are especially critical on LTE and 5G as the voice service (VoLTE) is provided through the data connection; so any interruption of VoLTE is experienced by the subscribers in a more direct and timely way.

### 3.3.1.1 PCI Modelling

Failing to properly reuse the PCIs determines a cost ("degradation") of performance that is evaluated through a cost function that is a straightforward and easy way of evaluating the quality of a PCI plan. These costs depend on both the geographical conformation and coverage of the territory and the importance given by the Telco operator to the unfulfilled requirement based on the know-how of the company.

Taking two generic cells, *i* and *j*, we have two costs binding them:

- $C_{i,j}$  : cost of assigning the two cells the same PCI number;
- $S_{i,j}$  : cost of assigning the two cells the same *Group\_ID*

The total cost is thus defined:

$$Tot_{cost} = \sum_i \sum_j C_{i,j} \cdot v_{i,j} + \sum_i \sum_j S_{i,j} \cdot w_{i,j}$$

Equation 2

where:

$$V_{i,j} = \begin{cases} 1 & \text{if the same PCI is assigned to both cells} \\ 0 & \text{otherwise} \end{cases}$$

$$W_{i,j} = \begin{cases} 1 & \text{if the same Group_ID is assigned to both cells} \\ 0 & \text{otherwise} \end{cases}$$

The goal is to minimize the amount of different *Group\_ID* satisfying the following constraints:

- each cell of the same site must have:
  - the same *Group\_ID*
  - a different *Cell\_ID*
- the cost  $\sum_i \sum_j C_{i,j} \cdot v_{i,j}$  must be zero
- Tot<sub>cost</sub> must be minimized

### 3.3.1.2 PCI algorithmic formulation

As the PCIs span over a limited set of numbers, their assignment is a typical combinatorial optimization problem to avoid the reuse of the same cell identifier on adjacent cells and is similar to the map colouring problem. The Quadratic Unconstrained Binary Optimization (QUBO) model has gained prominence in recent years as it can embrace a rich variety of important combinatorial optimization problems.

Embodying the definition of the cell identifiers, the reuse constraints expressed through the costs function, and the structural constraints that derive from the network topology, the mapping of the problem on a QUBO model Translates in a mathematical formulation made of Hamiltonian operators, as follows:

$$QUBO = \lambda_1 H_{PCI_{HC}} + \lambda_2 H_{GROUP_{HC}} + \lambda_3 H_{PCI_{SC}} + \lambda_4 H_{GROUP_{SC}} + \lambda_5 H_{GROUP_{YHC}}$$

Where:

- $H_{PCI_{HC}}$  expresses the constraint that two adjacent cells have to get two different PCIs
- $H_{GROUP_{HC}}$  expresses the constraint that two different sites have to get two different *Group\_IDs*
- $H_{PCI_{SC}}$  expresses the cost related to the reuse of the same PCI on two adjacent cells
- $H_{GROUP_{SC}}$  expresses the cost related to the reuse of the same *Group\_ID* on two adjacent sites
- $H_{GROUP_{YHC}}$  expresses the constraint to use different *Cell\_IDs* on cells of the same site.

### 3.3.1.3 Results

The QUBO algorithm was applied to the PCI planning of 5G and LTE and compared to the legacy procedure (Fast Greedy Algorithm).

From the processing times point of view, it is not easy to make a "homogeneous" comparison since the stop criteria of the legacy and QUBO algorithms are profoundly different. Nevertheless, from indicative measures and taking into account the overall process, the clear indication of a time reduction of a factor of 10x emerges, with the prospect of further improvement margins.

In order to analyze the potential of the algorithm on plans of variable complexity, a series of tests were performed decreasing the number of *Group\_IDs* (compared to the maximum). In fact, as the number of groups decreases, the probability of violating the constraints increases. In this way the performance of the QUBO algorithm was compared to the legacy procedure from two perspectives:

- comparing the minimum number of PCI necessary to define a plan without violation of PCI "reuse" constraints (optimal plan area)
- comparing the overall costs of the plans (taking into consideration both the "primary" constraints on the PCI and the "secondary" constraints on the *GROUP\_ID* evaluated by means of [Eq 2]) in the area of calculus where one or more constraints of "reuse" on the PCI are violated (no optimal plan area)

As an example, we present the results obtained in the case of a sample set of 450 cells of the TIM network, shown in Figure 16:

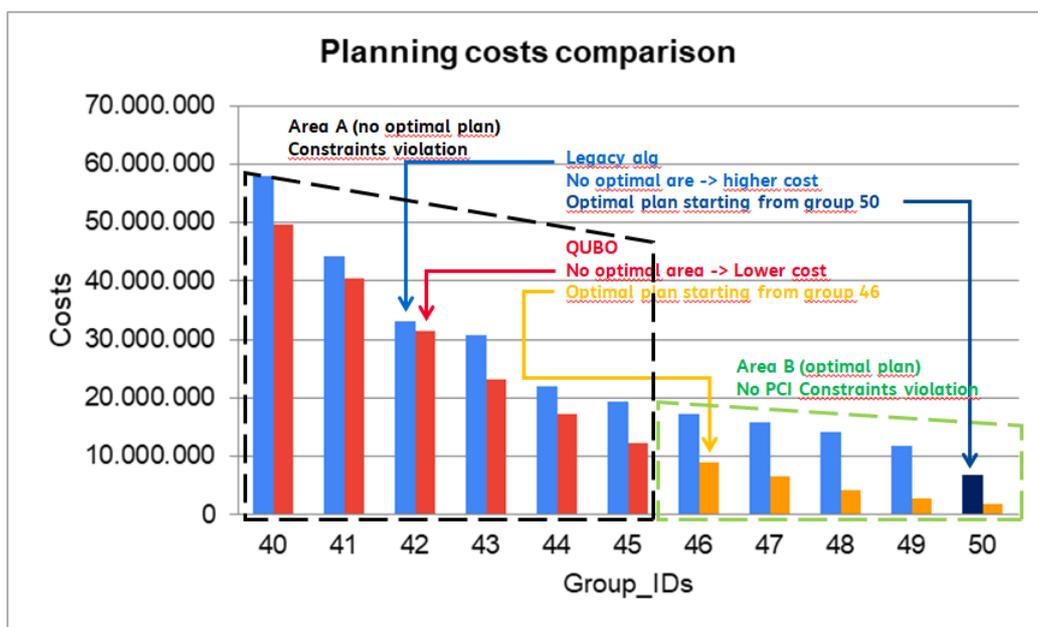


Figure 16 - Comparison chart on sample set

As it can be seen, in all cases there is a better behavior of the QUBO algorithm. In zone A (no optimal plan area), the latter obtains solutions breaking a lower number of constraints (lower cost) than the legacy algorithm, while in zone B - i.e. in the absence of violated constraints on PCI reuse - it guarantees lower cost functions thanks to the lower number of *Group\_IDs* used (46 versus 50) and more effective management of the "reuse" constraint relating to *GROUP\_IDs*.

### 3.4 PoCs and use-cases Quantum Sensing and Metrology

Many quantum sensing and metrology use cases may be usable in the future for telecom operators, but very few are available today in usable form. For example, Rydberg atoms for MW sensing are yet in laboratory form. But other resources are already available for some telecom needs. A good example is the miniaturized form of atomic clocks, in progress for 20 years. They use for example the CPT technique (Coherent Population Trapping), which permits compact Rb

(Rubidium) and Cs (Cesium) cell clocks. Other refinements also allowed the availability of miniaturized atomic clocks from some vendors, two examples are pictured below (so-called CSAC and MMAC modules):

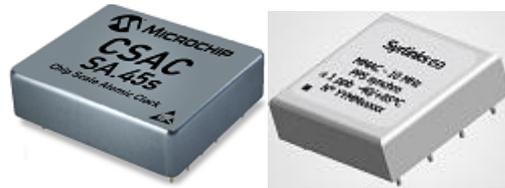


Figure 17 – Examples of miniaturized atomic clocks

These very small atomic clocks are very interesting for reference clocks in metrological equipments. (In-the-field measurements).

For more ambitious goals, there are also several scientific projects to disseminate the reference signal originated from optical clocks (unlike conventional atomic clocks which have a reference signal in the GHz range, these emit a reference signal in the optical range), which are (for the moment) of two types: trapped single ion type or lattice neutral atoms type. An example is pictured below:

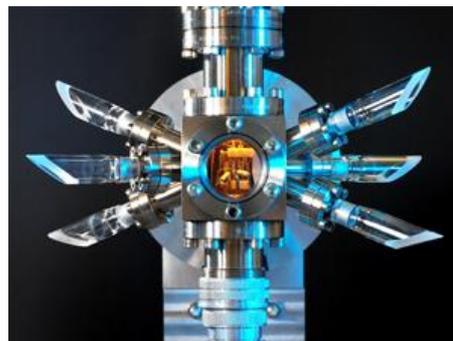


Figure 18 – NPL optical clock

These very new types of clocks will be used to redefine in few years the second, which is the S.I. (International System) unit of time. For this, international comparisons of these optical clocks are mandatory, and classical metrological comparison methods (with GNSS for example) are not sufficiently precise (these methods are not as stable as the new optical reference signals). So, scientific teams in the world designed solutions to be able to transport these new optical reference signals over telecom type fibers. The biggest challenge was to dramatically improve the stability of these conventional fibers (sensitive mainly to temperature, but also to vibrations and other physical parameters) by means for example of interferometric techniques. The medium used has become, thanks to these extremely refined solutions, more stable than the signal from optical clocks. An example of scientific solution is figured below (French REFIMEVE+ solution, on WDM type network) [98]:

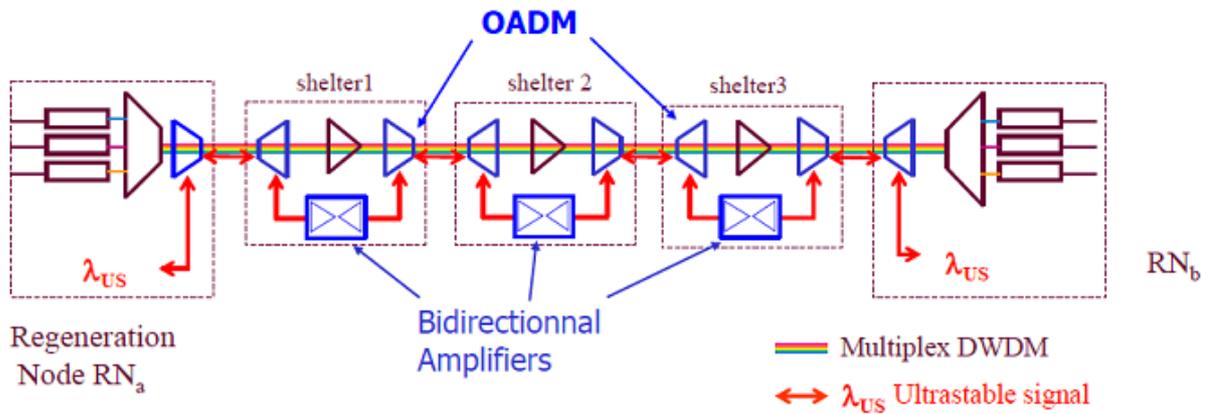


Figure 19 – Example of very high quality synchronisation reference optical fiber transfer

It is also a very interesting scientific advance for telecom operators. With this type of scientific solutions, it will be possible in the future to have access to the top time frequency reference signals in the world, from different NMI (National Measurement Institute) in the world. It will be a solution to the over-dependence in GNSS systems through the world, for a lot of critical infrastructures, including that of the telecom operators [93].

It is possible that this type of new very high quality reference signal may be useful also for future quantum networks (for QKD and for other services).

# 4 Roadmapping and Recommendations

This section describes some examples of roadmapping available in literature and provides a list of the main requirements (as seen today) for a seamless integration of available quantum nodes/systems/devices in the Network Operators' infrastructures.

## 4.1 Roadmapping

The overall landscape is that a second wave of quantum technologies are progressing very rapidly and have the potentials of allowing the development of quantum network infrastructures complementing and expanding (both in the radio and fixed domains) the current digital infrastructure.

It is safe to predict that a second wave of quantum technologies could potentially have a major impact in many services markets, ranging from secure communications and transactions to Internet, from future Medicine to Finance, from Energy to Transportation, and so on. Significant investments are being made worldwide across the public and private organizations.

In particular:

- Quantum security is the most mature for the commercialization/implementation of quantum services in the short term (for example, QKD, QRNG). On the other hand, a true technological breakthrough is still needed for developing quantum repeaters: this would be a key step for both long-distance QKD and distributed quantum computing.
- Quantum computing is becoming more and more mature. Today quantum annealers are already available, but they are specialized computers. A main technological breakthrough towards general purposed quantum computing concerns more stable ways of coding qubits and availability of efficient methods of quantum error correction are the expected key milestones.
- Quantum software scenario is very active but rather fragmented: major efforts are directed to define languages to enable Programmers to work at high level of abstraction.
- Multiple standardization groups such as ANSI, ITU, IETF, ETSI, and IEEE are producing significant efforts. Key aspect concerns the architecture and the interfaces for the integration of future quantum nodes and equipment in current infrastructure (for example, 5G) and with management/orchestration and control systems.

In line with above considerations, as an example, the following picture reports the OIDA roadmap: QKD and QRNG are already available today and will be enhanced in the next five years. Today quantum annealers are already available, quantum-based computer are starting to become available but maturity will be reached in five-ten years. Quantum Internet is seen in the long term, by 2035.

A very similar roadmapping is reported also by [1].

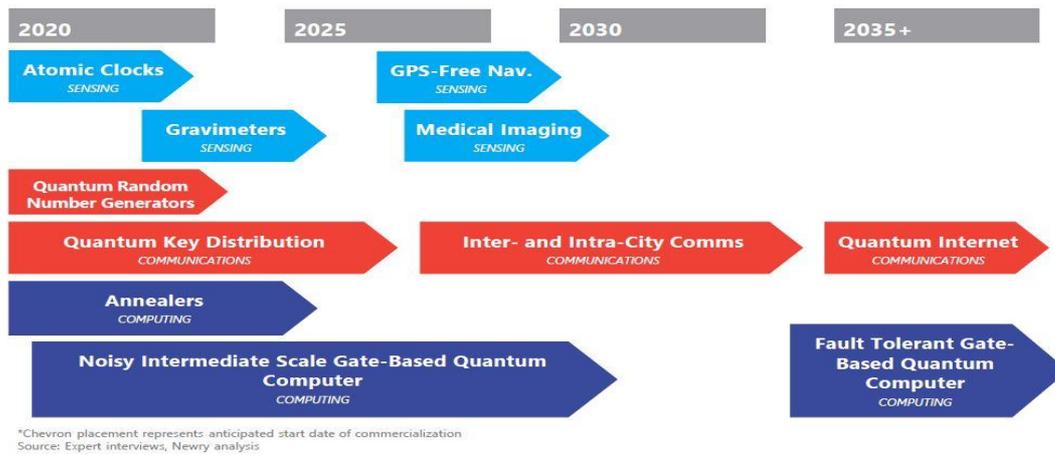


Figure 20 – Roadmap for quantum technologies and services [15]

## 4.2 Recommendations

The following sub-sections report a list of recommendations for specific technology domains (for example, QKD, QRNG, Blockchain and Quantum, etc.) and some calls for actions for next steps.

### QKD

- Any crypto-system based on mathematical complexities are vulnerable to quantum computing attack. The current weakest link from security perspective is the key distribution based on public key cryptography. QKD allows the key exchange between two remote parties as this is guaranteed by quantum physics which means it cannot be broken by any future technology.
- The network management/orchestration would be taken into account when QKD is implemented (i.e. SDN-QKD).
- The key supply to the encryptor (application) shall be working even when QKD network fails which means a key combination mechanism needs to be considered.
- QKD network should provide quantum keys for encryptors and decryptors in telecom networks in a secure manner.
- QKD network should provide its management information for SDN orchestrator in telecom network for the integrated operation of QKD network and transport optical network.
- QKD network should be able to reconfigure the route of distributing quantum keys among end-to-end QKD nodes according to SDN orchestrator's request.
- QKD network should provide quantum key generation, deletion API in case of on-demand QKD service.
- QKD network should provide its FCAPS (fault, configuration, accounting, performance, security) functionality for the network management system of network operator.
- QKD network should provide the solution to detect any hacking to QKD network in real time and inform its network management system of the hacking trials in real time.
- QKD network should be able to compose its components with multi-vendors.

- QKD network should provide long distance (> 120 km) point-to-point quantum channel performance or other relay solutions such as trusted nodes.

## QRNG

QRNGs, which generate random numbers using actual quantum physical process, in principle can guarantee the maximum entropy, i.e. level of randomness. Clearly, it should be mentioned also that today there is long-established cryptographic communications trust in well-designed PRNGs with well-generated seeds. Hardware TRNGs are also widely available. Potential advantages in using QRNG vs TRNG / PRNG may also depend on the application areas (communications, Internet of Thing, Artificial Intelligence and Machine Learning, Soft Computing etc). Further studies are required in this area [102], [103]. Blockchain and Quantum security

- To assess blockchain security, cryptographic primitives and quantum security implications;
- To consider a quantum resistant cryptography framework for blockchain security.

## Quantum Computing

- Quantum annealers already available can be used for solving complex optimization problems (for example, dimensioning 5G networks). The target anyway should be quantum-based computer which are starting to become available but the maturity will be reached in five-ten years.
- In general, performance and fault-tolerance of different quantum computing platforms should be compared considering the Di Vincenzo's criteria. The quantum computing platform should:
  - be based on scalable physical system with well characterized qubit
  - have ability to initialize the state of the qubits to a simple fiducial state
  - have long relevant decoherence times
  - allow a "universal" set of quantum gates
  - have qubit-specific measurement capability

## Quantum Compilers and Quantum Software

- Quantum compilers should allow for hybrid algorithms where a part of the code will be run by a quantum processing unit while the remaining is performed by classical processing units (CPU, GPU, etc.). This is a necessary requirement in order to integrate quantum computing in a common computing infrastructure.
- Quantum software stacks is essential for programming quantum computers and networks in order to run services and applications in platform independent software.

#### 4.2.1 Calls for action

- Technological analysis and testing are required, as the progress pace is accelerating in all quantum technological domains. This could be facilitated by platforms where innovators (for example research institutions, software developers, hardware industry, internet service industry, security professionals) can meet for technology-testing, standards, definitions, protocols and security policies validations. This also could boost the creation and development of ecosystems.
- A main challenge might be the lack of human resources with appropriate skill: know-how should involve electromagnetism and optics as well as quantum physics, ICT and computer science (including network systems, cryptography and security).
- Telecom Operators need to be ready – in the short term - for quantum computer era in terms of security, as TRL of QKD and QRNG is high.
  - The current security solutions use PKI (Public Key Infrastructure) and the security of most PKI algorithms are based on mathematical problems. However, it was already proved that these mathematical problems can be solved by quantum computers.
  - Telecom Operators should compare the expectation of when quantum computers perform enough to break the security of PKI and how long it will take to evolve towards quantum and/or post-quantum [101] secure communications. The recent competitive development of quantum computers among major IT companies, it is time to seriously consider quantum-safe readiness for secure telecom network to protect subscriber's data.
- Interesting application scenarios for quantum security includes: LTE/5G infrastructures, Cloud-Edge Computing, IoT.
- In addition to the security-related quantum services, other innovative quantum services will certainly appear in the medium term, for example, Quantum Cloud Computing. New business models are expected.
- It is perfectly conceivable that quantum technologies will help the telecom operators to be more energy efficient and bring Opex costs reductions. Analysis is required to exploit at best these opportunities.

## 5 Conclusions

A first quantum revolution has already brought quantum technologies in our everyday life, since decades. Chips for computers and smart-phone, systems for medical imaging (Nuclear Magnetic Resonance, Positron Emission Tomography), LED and lasers, etc. are all based on technologies exploiting the quantum mechanics principles.

Now a second revolution seems to be underway, leveraging on the three quantum principles of superposition, (hyper-) entanglement and measurement. It is safe to predict that a second wave of quantum technologies could potentially have a major impact in many markets, ranging from Telecom and ICT, to Medicine, to Finance, to Transportation, and so on.

It appears that significant work is still needed to develop enabling components and systems but in light of the potential opportunities and threats, significant investments are being made worldwide across the public and private organizations.

Quantum security is quite mature for the commercialization/implementation in the actual network (of course the improvements will be needed) compared to other quantum technologies. Concerning quantum computing, a roadblock is mitigating the random fluctuations that could occasionally flip or randomize the state of qubits during processing. Innovative qubits coding (for example, in topological computing) and availability of efficient methods of quantum error correction are the expected key milestones.

Quantum software scenario is very active but rather fragmented: major efforts are directed to define languages to enable Programmers to work at high level of abstraction.

In quantum communications, a technological breakthrough is needed for developing quantum repeaters: this would be a key step for both long-distance QKD and distributed quantum computing.

Standardization efforts are also set to help coordinating and accelerating progresses of quantum technologies. Multiple groups such as ANSI, ITU, IETF, ETSI, and IEEE are producing significant efforts. One key aspect concerns the integration of future quantum nodes and equipment (today for example QKD systems) in classic infrastructure (for example, 5G): this requires the definition of interfaces and abstraction for management and control. The topic is also under study with ongoing experimentation effort in the Quantum Flagship projects of H2020.

# 6 Appendix

This appendix has mainly an educational scope. It will contain an overview of contents and references for those quantum technologies which appear to have a TRL rather low and, as such, are not expected to have concrete industrial impacts in the short-medium term.

## 6.1 Quantum Internet and Quantum Communications

Quantum Internet can be defined as a global network exploiting some principles of Quantum Physics for transmitting, processing and storing qubits: in particular the communications features of the Quantum Internet mainly concerns distributing entangled quantum states among remote quantum nodes and devices. The quantum channels of the Quantum Internet work in synergy with classical links. Some key characteristics of the Quantum Internet have been recently overviewed by an IETF Quantum Internet Draft [64].

It should be noted that while, in the classical Internet, bits can be duplicated within a node or among the different nodes of a network, this is not valid for the Quantum Internet as a consequence of the no-cloning theorem, which forbids any possibility of duplicating an unknown qubit. This means that although a qubit (encoded within an inner state of a photon) can be transmitted directly to a remote node via a fiber link, attenuation or noise can degenerate the qubit but the quantum information cannot be recovered via a measuring process or a duplication. Moreover, the simple act of measuring qubits irremediably alters the encoded quantum information due to the quantum measurement principle.

Quantum Internet for transferring quantum information without actually sending any qubit through the quantum channel by the virtue of quantum teleportation [65], [66].

The quantum teleportation requires two communication links, a classical link for transmitting the pair of classical bits and a quantum link for entanglement generation and distribution. As a matter of fact, the integration of classical and quantum resources is crucial for Quantum Internet [67].

### 6.1.1 Experiments on Quantum Communications

There is a growing interest in quantum communications, motivated by remarkable features of secure communication, quantum teleportation and distributed quantum computing. Optical networks are considered to be the optimal medium for quantum communication.

However the maximum communication distance is severely limited by optical losses in optical fibers. One viable solution is to use satellites as relays to transmit photons over a free-space.

In fibre-based telecommunications networks, quantum repeaters are believed to be the most promising way to overcome the distance limit. The standard paradigm for a quantum repeater consists of three basic technologies [94]:

- entanglement swapping [74], [75]
- entanglement purification [76], [77]
- and quantum memory [78], [79], [80]

Recently, significant progress has been made both theoretically [81], [82], [83], and experimentally [84], [85], [86]. However, the still limited performance remains a major obstacle in realizing practical quantum repeaters.

#### **6.1.1.1 Example of activities in the Quantum Internet Alliance**

The Quantum Flagship (QF) [95] is a European initiative with the goal to consolidate and expand European scientific leadership and excellence in quantum research, to kick-start a competitive European industry in quantum technologies and to make Europe a dynamic and attractive region for innovative research, business and investments in this field. With a budget of €1 billion, a 10-year timescale, is funding a number of European projects addressing key strategic areas of Quantum Technologies and Services.

Among these project, Quantum Internet Alliance (QIA) [96] aims at defining the blueprint for a pan-European Quantum Internet by ground-breaking technological advances, demonstrating a fully integrated stack running on a multi-node quantum network. QIA is addressing Quantum Internet network requirements to enable end-to-end qubit transmission, resulting in:

- (a) Network architecture design;
- (b) Placement and choice of quantum repeaters in accordance with real-world constraints on deployed fibre grids, as well as
- (c) Required hardware parameters and control plane features to achieve end-to-end qubit transmission with desired properties (quality of qubits and entanglement, rate of transmission, overall performance of application protocols, etc.).

QIA is addressing enabling technologies for both end nodes (trapped ion qubits, diamond NV qubits, neutral atom qubits) and quantum repeaters (rare-earth-based memories, atomic gases, quantum dots).

Main goal is to achieve entanglement and teleportation across three and four remote quantum network nodes, demonstrating the key enabling capabilities for memory-based quantum repeaters. The main function of the quantum repeater is to extract the transmitted quantum state information, enhance the fidelity of the quantum state and transfer the measured quantum state to the next user.

Other projects, already mentioned, of the Quantum Flagship include CIVIQ [55], UNIQORN [56], etc.

## Annex A Document Management

### A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0		New PRD (WG Doc nn/nnn).  Acknowledgements: Andrea Boella (TIM), Fabio Cavaliere (Ericsson), Daejoon Cha (SKT), Olivier Le Moul (Orange), Diego Lopez (Telefonica), Antonio Manzalini (TIM), Monique Morrow (Syniverse), Dong-Hi Sim (SKT), Momtchil Peev (huawei) and Fred Fung (Huawei)	IG eVote/ TG	Antonio Manzalini (TIM)

### A.2 Other Information

Type	Description
Document Owner	IG
Editor / Company	Antonio Manzalini (TIM)

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](mailto:prd@gsma.com)

Your comments or suggestions & questions are always welcome.



**GSMA HEAD OFFICE**

Floor 2  
The Walbrook Building  
25 Walbrook  
London  
EC4N 8AF  
United Kingdom  
[www.gsma.com](http://www.gsma.com)