Quantum Internet Alliance

Participant No	Beneficiary organisation name	Acronym	Country
1	Technische Universiteit Delft - ***coordinator***	TUD	Netherlands
2	Institut de Ciencies Fotoniques	ICFO	Spain
3	Universität Innsbruck	UIBK	Austria
4	Austrian Academy of Sciences, Innsbruck	IQOQI	Austria
5	Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V.	MPQ	Germany
6	Centre National de la Recherche Scientifique	CNRS	France
7	Kobenhavns Universitet	UCPH	Denmark
8	Sorbonne Université	SU	France
9	Université de Genève	UNIGE	Switzerland
10	Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek	TNO	Netherlands
11	Universität Basel	UNIBAS	Switzerland
12	Universität Stuttgart	USTUTT	Germany
13	Instituto de Telecomunicacoes	IT	Portugal
14	MyCryoFirm	MYCRYO	France
15	Swabian Instruments	Swabian	Germany
16	TOPTICA Photonics AG	TOPTICA	Germany
17	VeriQloud	VQ	France
18	Element Six	E6	United Kingdom
19	SAP SE	SAP	Germany
20	SURFsara BV	SURFsara	Netherlands
21	Crystalline Mirror Solutions GmbH	CMS	Austria
22	Muquans	MQS	France
23	Janssen Precision Engineering B.V.	JPE	Netherlands
	Associated/Third party name	**Acronym**	**Country**
	Amsterdam Internet Exchange B.V.	AMS-IX	Netherlands
	ID Quantique	IDQ	Switzerland
	I2CAT	I2CAT	Spain
	Koninklijke KPN N.V.	KPN	Netherlands
	RIPE NCC	RIPE	Netherlands
	SURFnet B.V.	SURFnet	Netherlands
	Toshiba	Toshiba	United Kingdom
	Quanticor Security	Quanticor	Germany
	Toyota Motor Europe N.V./S.A.	Toyota	Belgium
	CNAM	CNAM	France
	ABN-AMRO Bank N.V.	ABN-AMRO	Netherlands

Ambition

The internet - a vast network connecting devices anywhere on earth using long-range classical communication - has had a revolutionary impact on our world. The vision of a *Quantum Internet* is to provide fundamentally new internet technology by enabling quantum communication between any two points on earth. Such a Quantum Internet will – in synergy with the 'classical' internet that we have today - connect quantum processors in order to achieve unparalleled capabilities that are *provably impossible* using classical communication.

As with any radically new technology, it is hard to predict all uses of the future Quantum Internet, but several major applications have already been identified. One striking application of quantum communication is *quantum key distribution*[1] (QKD), which allows two remote network nodes to generate an encryption key, enabling the exchange of secret information between any users connected to the Quantum Internet. The security of QKD is guaranteed by the fundamental laws of nature, and thus fully future proof even against any attacker possessing a large-scale quantum computer. Other promising known applications are clock synchronization[2], extending the baseline of telescopes[3], secure identification[4], achieving efficient agreement on distributed data[5], exponential savings in communication[6], quantum sensor networks, as well as secure access to remote quantum computers in the cloud[7].

Central to all these applications is the ability to send quantum bits (qubits). Qubits are fundamentally different from classical bits. While a classical bit can take only two values, '0' and '1', a qubit can be in a superposition of being '0' and '1' at the same time. Qubits can be entangled with each other, even when separated by a large distance. This entanglement provides a source of coordination that is stronger than any classical information could give, and is central to many applications of the Quantum Internet. Crucially, qubits cannot be copied. Moreover, any attempt to read their state can be detected, which makes qubits naturally well suited for security applications. At the same time, it makes transmitting qubits over long distances a truly formidable endeavour. Since qubits cannot be copied or amplified with sufficient fidelity, repetition or signal amplification are ruled out as a means to overcome imperfections, and radically new technology is needed for a Quantum Internet.

Right now, point-to-point QKD over metropolitan distances (order ~100 km) connecting simple quantum devices is a relatively mature technology, with QKD systems being commercially available from several European and international vendors. In contrast, long-distance quantum communication connecting advanced quantum devices is an outstanding technological challenge that must be overcome in order to unlock the advantages of quantum communication for industry, governments and other end-users all over Europe and beyond.

The long-term ambition of the European Quantum Internet Alliance is to build a Quantum Internet that enables quantum communication applications between any two points on Earth.

In analogy to the internet we know today, the future Quantum Internet will consist of the following subsystems: quantum repeaters, end nodes, infrastructure technology, control and applications. First, **quantum repeaters** are needed to transmit qubits, and generate entanglement between distant quantum nodes. As qubit signals cannot be amplified, these require fundamentally new technology. End-to-end security of QKD, as well as all other applications of a Quantum Internet require the ability for end-to-end transmission of qubits, and hence a true quantum repeater.[8] The best way to distribute quantum information over long distances on the ground is to use photons in optical fibres. However, the maximal distance for direct photon transmission is limited to a few hundred km, due to the exponential loss in optical fibres. This attenuation strongly limits the scale and the speed of quantum networks that use only direct photon transmission, requiring the development of repeaters. At present, no quantum repeaters have been realized that provide an advantage over direct transmission. Second, **end nodes** –the quantum analogues of laptops and phones connected to the internet– are required to enable the execution of applications, and hence to make Quantum Internet technology available to end users. Thankfully, it turns out that most quantum-network protocols do not require these end nodes to be large quantum computers: an end node that is a simple quantum device capable of preparing and measuring a single qubit is already sufficient for many applications such as QKD. What's more, errors in Quantum Internet protocols can often be dealt with using classical rather than quantum error correction, imposing fewer demands on the quality of the qubits. The reason why Quantum Internet protocols can outperform classical communication with such relatively modest resources at the end nodes is due to the fact that their advantages rely solely on inherently quantum properties such as quantum entanglement, which can be exploited already with very

---

[1] C. H. Bennett and G. Brassard. *Int. Conf. Comp. Sys. Sig. Proc.* pp. 175–179 (1984); A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
[2] P. Komar, et al. *Nat. Phys.* **10**, 582 (2014).
[3] D. Gottesman, T. Jennewein and S. Croke. *Phys. Rev. Lett.* **109**, 070503 (2012).
[4] I. Damgaard, et al. *Theo. Comp. Sci.* **560**, 12 (2014); F. Dupuis, O. Fawzi and S. Wehner. *IEEE Trans. Inf. Theo.* **61**, 1093 (2014).
[5] M. Ben-Or and A. Hassidim. *Symp Theo. Comp. (STOC)* pp. 481–485 (2005).
[6] H. Buhrman, R. Cleve, S. Massar and R. de Wolf. *Rev. Mod. Phys.* **82,** 665 (2010).
[7] A. Broadbent, J. Fitzsimons and E. Kashefi. *Found. Comp. Sci. (FOCS)* pp. 517–526 (2009).
[8] As opposed to trusted nodes/repeaters (https://en.wikipedia.org/wiki/Quantum_network#Trusted_repeaters), which do not allow end-to-end qubit transmission, and hence no end-to-end security: QKD is secure only if the intermediary "repeaters" are trusted.

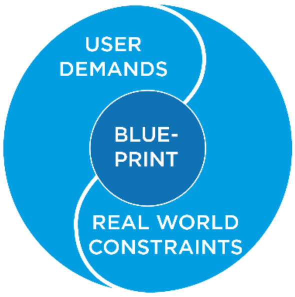
few qubits. It is fundamentally impossible to replicate the properties of entanglement using classical communication. (In contrast, a quantum computer must feature more qubits than can be simulated on a classical computer in order to offer an advantage.) Third, we need **technology to maximize the use of existing network infrastructure.** This includes, for example, high-efficiency frequency conversion to the telecom band, enabling the use of existing telecom fibres.

In addition, scaling a Quantum Internet requires the development of an efficient classical **control plane** including a **quantum network stack** that allows fast and reactive decisions in controlling the quantum network and delivering qubits to the right destination, in order to mitigate the effect of limited quantum memory lifetimes. Finally, such a quantum network stack should enable a fully programmable Quantum Internet that allows the **realization of any application supported by the end nodes in software**, as well as the seamless integration of quantum network middleware and applications in existing programming and real-world software environments. At present, only basic elements of such a network stack have been suggested[9], and neither a full quantum network stack nor an elementary control plane for repeater networks has been developed and tested.

Mission

The European Quantum Internet Alliance (QIA) is an interdisciplinary team consisting of partners from industry, a research & technology organisation (RTO) and academia. Our mission is to:

Develop a Blueprint for a pan-European entanglement-based Quantum Internet, by developing, integrating and demonstrating all the functional hardware and software subsystems.



QIA's **systematic Blueprint** forms a systems architecture and design for a large-scale Quantum Internet, and thus provides a roadmap for the targeted development of a European Quantum Internet in the main phase of the Flagship programme. This Blueprint is based on a methodical improvement of all key components – many of which already now define the world-wide state of the art – guided by an overall systems design process including the verification and validation of all sub-systems. By pushing forward the state of the art of hardware and software within a tightly knit consortium that includes many of the world-wide academic and industrial leaders, we will place Europe centre stage in the development and use of Quantum Internet technology. The Blueprint is derived from:

User Demands A requirements analysis of what Quantum Internet hardware and control software actually needs to deliver. Outcomes include:

- Identification of use cases and software embedding of quantum network applications.
- Determination of parameter requirements for desired protocols (e.g. quality of qubits, measurements and quantum operations) to satisfy such end-user demands.

Real-World Constraints: hardware and software development Simultaneously, we will push forward the development of Quantum Internet technology, leveraging the state-of-the-art hardware platforms for quantum repeaters and end nodes, and a matching efficient control plane and software stack.

- First demonstration of key enabling technologies for high-rate quantum repeaters:
    - Quantum memories for non-classical light with sufficiently long storage time, efficiency, and multi-mode capability.
    - Long-distance entanglement between a photon and a quantum memory, as well as multiplexed, heralded and scalable entanglement between remote quantum memories.
- First demonstration of a quantum network stack providing the basis for scalable control of a Quantum Internet.
- First multi-node networks linking few-qubit quantum processors.
- First demonstration of a universal software stack for a Quantum Internet that will make this network fully programmable.
- First interfacing between high-speed repeater platforms and end nodes.

All hardware platforms will be subject to component benchmarks according to the same criteria. We will conduct early-stage integration tests and a comparative assessment of their long-term scalability. This leads to scalability in the main phase of the flagship programme.

Blueprint: Network architecture Using an existing discrete-event simulation platform for quantum networks as a design and validation tool, we will work together to determine a Blueprint for a scalable Quantum Internet:

[9] R. Van Meter, J. Touch, *IEEE Communications Magazine* **51**, 64 (2013).

- 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.)

This feasibility and scalability analysis will yield crucial insights into the relative importance of the many different hardware parameters to optimize going forward.

Blueprint demo Next to testing and benchmarking the individual hardware and software subsystems, we will perform an overall systems test to demonstrate the integration between the combined hardware and software stack by executing a high-level application on a demonstration network connecting multiple network nodes.

- To show the power of the combined hardware and software stack, this systems test will consist of executing an application more complex than QKD, where quantum communication is used to send qubits into a remote quantum processor to perform secure delegated quantum cloud computing.

This will provide a benchmark of hardware/software integration and set the stage for early adopters from industry to use the European Quantum Internet developed during the main phase of the Flagship programme as soon as first prototypes come online.

Website: http://quantum-internet.team

Alliance Coordinator:

Prof. Dr. Stephanie Wehner

QuTech, Delft University of Technology

s.d.c.wehner@tudelft.nl

Assistant: Judith de Keijzer J.deKeijzer@tudelft.nl

Press Coordination: Michel van Baal M.vanBaal@tudelft.nl

Coordination Office: Zoe Lachmann Z.N.Lachmann@tudelft.nl