Annex

Draft Technical Report ITU-T TR.QEFN

ITU-T's Views for Quantum-Enabled Future Networks

1. Scope

The scope of this Technical Report is to describing ITU-T's Views for Quantum-Enabled Future Networks (QEFN) for the future networks study to act as a document to help SG13 to study the future network evolution towards Quantum era.

2. Definitions

2.1. Terms defined elsewhere

2.1.1 quantum key distribution (QKD) [b-ETSI GR QKD 007]: Procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory.

2.1.2 quantum key distribution (QKD) module [ITU-T Y.3800]: A set of hardware and software components that implements cryptographic functions and quantum optical processes, including quantum key distribution (QKD) protocols, synchronization, distillation for key generation, and is contained within a defined cryptographic boundary.

2.1.3 quantum information networks [ITU-T FG QIT4N D1.1]: A network that incorporates quantum communication technology for the purpose of transmitting quantum states.

2.2. Terms defined in this Recommendation

2.2.1 quantum-enabled future network: A network that connects quantum devices using fundamental quantum information technologies which are based on quantum

[Editor's Note] The definition of 'quantum devices' should be further studied.

3. Introduction

QEFN is connected quantum devices using fundamental quantum information technologies which are based on quantum theory such as superposition and entanglement. The well-known quantum devices are quantum computer, quantum sensor, and quantum key distribution (QKD) module.

The basic distinction of QEFN comparing to current digital network is derived from quantum information technologies. The below <Table 1> introduces those distinctions.

<Table 1. Basic distinction between digital and quantum information technologies

	Digital Information Technology	Quantum Information Technology
Theoretical Background	Classical Physics	Quantum Physics
Delivered Signal	Digital bits	Quantum bits (qubits)

Amplification/Repeating of the signal	Possible	Only repeating is possible (with quantum memory)

4. Status of Quantum-Enabled Future Networks Study

4.1. SDOs

[Editor's note – Details of each SDO are in Appendix.]

4.1.1. ITU-T FG on QIT4N

The ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N) was established to provide a collaborative platform for pre-standardization aspects of QIT for networks.

Throughout ITU-T FG QIT4N D1.1, necessary technologies for QIN and explanations of related terms for QIN development are mentioned. In ITU-T FG QIT4N D1.2, the use case of QIN and applied QIT are introduced. Finally, ITU-T FG QIT4N D1.4 is about the standardization outlook and technology maturity of quantum information technologies which either comprise or impact the requirements for QIN.

The FG defines Quantum Information Networks (QIN) as any network that incorporates quantum communication technology for the purpose of transmitting quantum states.

4.1.2. IETF/IRTF QIRG, etc.

The IETF/IRTF will be beneficial in quantum network engineering because it has a lot of existing network engineering experience. With this background, two documents were published.

'Architectural Principles for a Quantum Internet' proposes a quantum Internet framework to realize a quantum Internet vision and explains some basic architectural principles. It explains the basic principles of quantum Internet, such as cubits and quantum entanglement, and describes the direction of development of quantum Internet-related technologies. In particular, this document proposes a quantum network architecture inspired by classical network architectures.

'Application Scenarios for the Quantum Internet' provides an overview of some expected application categories for the Quantum Internet, and then details selected application scenarios. Some general requirements for the Quantum Internet are also provided.

The group defines Quantum Networks as a collection of nodes that is able to exchange qubits and distribute entangled states amongst themselves. Quantum Internet is defined as a network of Quantum Networks. The Quantum Internet is expected to be merged into the Classical Internet to form a new Hybrid Internet.

4.2. Research Institutes & Academia

4.2.1. United States Department of Energy (DOE) and associated research institutes

In 2020, the U.S. Department of Energy published a strategic report that presents a blueprint for the implementation of the quantum Internet. This resulting report identifies four Priority Research Directions (PRDs) for the implementation of the quantum internet and outlines five Blueprint Roadmap Milestones that must be achieved to facilitate an eventual national quantum Internet.

Also, in April 2019, scientists from the U.S. Department of Energy (DOE)'s Brookhaven National Laboratory, Stony Brook University (SBU), and DOE's Energy Sciences Network (ESnet) achieved long-distance entanglement over 18 km using unique portable quantum entanglement sources and an existing DOE ESnet communications fiber network. Argonne National Laboratory has created a 52-mile quantum loop entanglement distribution network that will be connected to Fermilab, establishing a three-node, 80-mile testbed for quantum communication.

4.2.2. Quantum Internet Alliance (QIA) & QuTech

The Quantum Internet Alliance (QIA) targets a Blueprint for a pan-European Quantum Internet by ground-breaking technological advances, culminating in the first experimental demonstration of a fully integrated stack running on a multinode quantum network.

In 2018, QuTech of the Netherlands published a comprehensive paper that could implement quantum Internet, and suggested six stages to complete quantum Internet using Qubit.

4.2.3. EU QCI project

In 2019, the EU's QCI project introduced a project plan aimed at commercializing a complete quantum information network from 2021 to 2035.

4.2.4. Quantum Internet Task Force

The Quantum Internet Task Force take into account the history of the current Internet, and while valuing the diversity and interconnectedness of technologies, aim to create a future information society based on the Quantum Internet through its activities.

They also aim to create a Quantum Internet testbed that includes all layers, and through this they implement standardization and commitments to society.

5. Implications for Quantum-Enabled Future Networks

5.1. Implications from status of existing study

QEFN is going to be implemented in Testbed stage. It is expected to be realized in near future, in spite of how to be named; Quantum Internet, Quantum Network, Quantum Information Network, etc. Some studies proposed protocol stack which is a layered model and primitive protocol as well. It implies that QEFN-related fundamental technology is well developing nowadays and should be standardized for real world-wide implementation. Considering IETF/IRTF is trying to develop RFCs for Quantum Internet, the initiation of the QEFN study in ITU-T is now required in collaboration with other SDOs.

5.2. Implications for standardization activity on Study Group 13

Quantum Internet is expected to introduce classical Internet-like study items such as addressing, routing protocol, resource allocation, quality of service, etc. Considering the mandate of ITU-T SG13, Future networks and emerging network technologies, standardizing networked quantum devices; quantum network, is the role of SG 13. The requirements, architectures and capabilities of quantum network should be specified and led by SG13.

6. Conclusions

Quantum Network is considering one of future networks should be studied in SG13. It is required that SG13 initiates quantum network-related studies.

Appendix

Summary of other standardization documents related to Quantum-Enabled Future Networks

1. SDOs

1.1 ITU-T FG on QIT4N

1) Quantum information technology for networks terminology: Network aspects of quantum information technologies [ITU-T FG QIT4N D1.1]

Summary

The scope of this document FG QIT4N D1.1 is as follows :

- Building blocks for QINs: Necessary technologies for QIN
- Application-driven network requirements: Quantum information technologies that impose requirements onto a QIN to function within it.
- Supports the deliverables of FG QIT4N Working Group 1 on Network aspects of QIT:

Throughout this document, explanations of related terms for QIN development are mentioned.

2) Quantum information technology for networks use cases:Network aspects of quantum information technologies [ITU-T FG QIT4N D1.2]

summary

The scope of this document FG QIT4N D1.2 is the use cases of network aspects of quantum information technology (QIT).

The contents related to QIN are mentioned in Quantum Communication in clause 7.

The security function of quantum communication is much stronger than the existing security function. The development stage of the quantum communication network required to implement quantum communication is currently between QKD and the large-scale quantum Internet that connects quantum computers and quantum communication channels.

3) Standardization outlook and technology maturity: Network aspects of quantum information technologies [ITU-T FG QIT4N D1.4]

Summary

The scope of this document FG QIT4N D1.4 is the standardization outlook and technology maturity of quantum information technologies which either comprise or impact the requirements for a quantum information network (QIN), at the period of performance of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N).

In this document, QIN standardization considerations are mentioned as follows:

- QITs that are building blocks for QINs: These are necessary technologies for QIN, which provide fundamentally enabling aspects of a quantum information network, from lower-level essential components up through higher level systems. For example, these technologies may include quantum memories, quantum repeaters, quantum network end-nodes, and respective technologies that extend traditional network control technology to allow QIN functionality.

1.2. IETF QIRG, etc.

1) Architectural Principles for a Quantum Internet [draft-irtf-qirg-principles-07]

Summary

This document proposes a quantum Internet framework to realize a quantum Internet vision and explains some basic architectural principles. It explains the basic principles of quantum Internet, such as cubits and quantum entanglement, and describes the direction of development of quantum Internet-related technologies.

1. Introduction

Quantum networks are distributed systems of quantum devices that utilise fundamental quantum mechanical phenomena such as superposition, entanglement, and quantum measurement to achieve capabilities beyond what is possible with non-quantum (classical) networks.

Fully quantum networks capable of transmitting and managing entangled quantum states in order to send, receive, and manipulate distributed quantum information are now imminent. There are no worked out proposals for how to run these networks. Also, whilst physical mechanisms for transmitting quantum states exist, there are no robust protocols for managing such transmissions.

2. Quantum information

In order to understand the framework of quantum networking, a basic understanding of quantum information is required, and the basic concepts mentioned are as follows.

- Qubit
- Multiple qubits
- Entanglement as the fundamental resource
- Bell pair & teleportation

3. Entanglement as the fundamental resource

Entanglement is created through local interactions between two qubits or as a product of the way the qubits were created (e.g. entangled photon pairs). To create a distributed entangled state, one can then physically send one of the qubits to a remote node. Therefore, it is the transmission of qubits that draws the line between a genuine quantum network and a collection of quantum computers connected over a classical network.

A quantum network is defined as a collection of nodes that is able to exchange qubits and distribute entangled states amongst themselves. A quantum node that is able only to communicate classically with another quantum node is not a member of a quantum network.

4. Achieving quantum connectivity

A quantum network cannot be built by simply extrapolating all the classical models to their quantum analogues. Sending qubits over a wire like we send classical bits is simply not as easy to do. There are several technological as well as fundamental challenges that make classical approaches unsuitable in a quantum context.

To achieve quantum connectivity, this section explains the meaning of quantum connectivity and the necessary physical processes.

5. Architecture of a quantum internet

Since the basic services provided by quantum networks are very different from existing networks, the architecture of quantum Internet is very different from that of classical Internet. This section describes with the main basic challenges of building quantum networks.

6. Architectural principles

6.1. Goals of a quantum internet

Quantum network architectures are similar to classical Internet architectures, but the architectural details are fundamentally different. It is necessary to set goals that will lead the architecture of the quantum Internet, and the goals are as follows:

- Support distributed quantum applications
- Support tomorrow's distributed quantum applications
- Support heterogeneity
- Ensure security at the network level
- Make them easy to monitor
- Ensure availability and resilience

6.2. The principles of a quantum internet

The principles of the quantum Internet provide guidance on the direction to be achieved and should be considered when designing quantum networks.

- Entanglement is the fundamental service
- Bell Pairs are indistinguishable
- Fidelity is part of the service
- Time is an expensive resource
- Be flexible with regards to capabilities and limitations

7. A thought experiment inspired by classical networks

In conclusion, the quantum network architecture conceived based on the classical network is to provide an idea about the elements necessary for its construction. Based on the classical and well-known MPLS(Multi-Protocol Label Switching), it can be applied to the architecture of quantum networks.

Quantum networks can be thought of as quantum virtual circuits with multiple endpoints to create multilateral entanglement. Similarly, MPLS networks have the concept of LSP(Label-Switched Path) for multicast. Based on these similar characteristics, the quality of service parameters of quantum networks can be expressed.

Quantum networks can employ the routing protocols and traffic engineering of classical communications to ensure optimal paths, speed, or fidelity to quantum virtual circuits. However, there may be some differences between the classical Internet and the quantum Internet.

Hardware blocking is required to determine the delivery rules of quantum networks. In quantum networks, control traffic (routing and signal messages) is exchanged over classical channels, while data plane traffic (actual bell pair qubits) is exchanged over separate quantum channels. This is in contrast to most classical networks in which control and data unit traffic share the same channel and a single packet includes both user and header fields. However, there are classical similarities to the way quantum networks work. A generalized MPLS (MPLS) network uses a separate channel for control traffic and data unit traffic.

2) Application Scenarios for the Quantum Internet [draft-irtf-qirg-quantum-internet-use-cases-08]

Summary

This document provides an overview of some applications expected to be used on the Quantum Internet, and then categorizes them using various classification schemes. Some general requirements for the Quantum Internet are also discussed. The intent of this document is to describe a framework for applications, and describe a few selected application scenarios for the Quantum Internet.

1. Introduction

Research and experiments have picked up over the last few years for developing the Quantum Internet [Wehner]. End-nodes will also be part of the Quantum Internet, in that case called quantum end-nodes that may be connected by quantum repeaters/routers. These quantum end-nodes will also run value-added applications which will be discussed later.

The connections between the various nodes in the Quantum Internet are expected to be primarily fiber optics and free-space optical lasers. Photonic connections are particularly useful because light (photons) is very suitable for physically realizing qubits. Qubits are expected to be transmitted across the Quantum Internet.

The Quantum Internet will operate according to quantum physical principles such as quantum superposition and entanglement [I-D.irtf-qirg-principles]. The Quantum Internet is not anticipated to replace, but rather to enhance the Classical Internet. The intent of this document is to provide a common understanding and framework of applications and application scenarios for the Quantum Internet.

2. Terms and acronyms List

For clarity, several terms and concepts related to quantum information technology are briefly defined and described; Bell pair, Entanglement Swapping, Quantum End-node, Quantum Teleportation, Qubit,, etc.

3. Quantum Internet Applications

3.1. Overview

The expected applications for the Quantum Internet are still being developed as we are in the formative stages of the Quantum Internet. However, an initial (and non-exhaustive) list of the applications to be supported on the Quantum Internet can be identified and classified using two different schemes. Note, this document does not include quantum computing applications that are purely local to a given node (e.g., quantum random number generator).

3.2. classification by Application Usage

It was classified into three categories according to the amount of application use, and the details are as follows.

- Quantum cryptography applications
    - Secure communication setup
    - - Fast Byzantine negotiation
    - - Quantum money
- Quantum sensors applications
    - Network clock synchronization
    - High sensitivity sensing

- Quantum imaging

- Quantum computing applications
  - Distributed quantum computing
  - Secure quantum computing with privacy preservation
  - Quantum chemistry

3.3. Control vs Data Plane Classification

Nodes in the Quantum Internet applications may also use the classification paradigm of control plane functionality versus data plane functionality where:

- Control Plane - Network functions and processes that operate on (1) control bits/packets or qubits (e.g., to setup up end-user encryption); or (2) management bits/packets or qubits (e.g., to configure nodes).
- Data Plane - Network functions and processes that operate on end- user application bits/packets or qubits (e.g., voice, video, data). Sometimes also referred to as the user plane.

	Classical Internet Examples	Quantum Internet Examples	Hybrid Internet Examples
Control Plane	ICMP; DNS	Quantum ping; Signalling for controlling entanglement distribution;	QKD-based secure communication setup
Data Plane	Video conference	QKD; Entanglement distribution	Video conference using QKD-based secure communication setup

Table xx. Examples of Control vs Data Plane Classification

4. Selected Quantum Internet Application Scenarios

This document also introduced several quantum Internet application scenarios.

4.1. Secure Communication Setup

One requirement for this secure communication setup process is that it should not be vulnerable to any classical or quantum computing attack. This can be realized using QKD which has been mathematically proven to be information-theoretically secure and unbreakable. QKD can securely establish a secret key between two quantum nodes, using a classical authentication channel and insecure quantum communication channel without physically transmitting the key through the network and thus achieving the required security

4.2. Secure Quantum Computing with Privacy Preservation

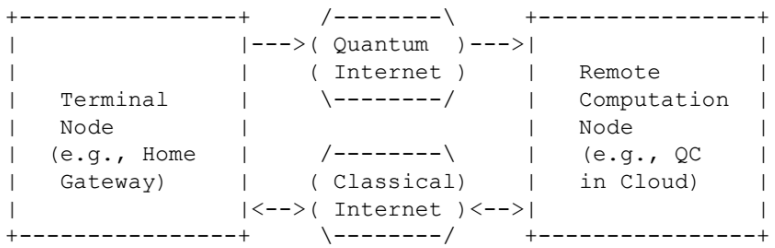

Figure XX. Secure Quantum Computing with Privacy Preservation

A terminal node such as a home gateway has collected lots of data and needs to perform computation on the data. Although the terminal node can upload the data to the cloud to leverage cloud computing without introducing local computing overhead, to upload the data to the cloud can cause privacy concerns. In this particular case, there is no privacy concern since the source data will not be sent to the remote computation node which could be compromised. Delegated quantum computing or Blind Quantum Computation (BQC) can be leveraged to realize secure delegated computation and guarantee privacy preservation simultaneously.

4.3. Distributed Quantum Computing

There are two types of scenarios in distributed quantum computers: utilizing quantum mechanics to improve classic distributed computing problems and distributing quantum computing capabilities to distributed quantum computers.

5. General Requirements

5.1. Background

On the network level, six stages of Quantum Internet development are described in [Wehner] as follows:

- Trusted repeater networks (Stage-1)
- Prepare and measure networks (Stage-2)
- Entanglement distribution networks (Stage-3)
- Quantum memory networks (Stage-4)
- Fault-tolerant few qubit networks (Stage-5)
- Quantum computing networks (Stage-6)

Quantum Internet Stage	Example Quantum Internet Use Cases	Characteristic
Stage-1	Secure comm setup using basic QKD	Trusted nodes
Stage-2	Secure comm setup using the QKD with end-to-end security	Prepare-and-measure capability
Stage-3	Secure comm setup using entanglement-enabled QKD	Entanglement distribution
Stage-4	Secure/blind quantum computing	Quantum memory
Stage-5	Higher-Accuracy Clock synchronization	Fault tolerance
Stage-6	Distributed quantum computing	More qubits

Table xx. Example Application Scenarios in Different Quantum Internet Stages

5.2. Requirements

Some general and functional requirements on the Quantum Internet from the networking perspective, based on the above application scenarios, are identified as follows:

- Methods for facilitating quantum applications to interact efficiently with entangled qubits are necessary in order for them to trigger distribution of designated entangled qubits to potentially any other quantum node residing in the Quantum Internet.

- Quantum repeaters/routers should support robust and efficient entanglement distribution in order to extend and establish high- fidelity entanglement connection between two quantum nodes.
- Quantum end-nodes must send additional information on classical channels to aid in transmission of qubits across quantum repeaters/receivers.
- Methods for managing and controlling the Quantum Internet including quantum nodes and their quantum resources are necessary. Furthermore, new management information model for the Quantum Internet may need to be developed.

6. Conclusion

This document provides an overview of some expected application categories for the Quantum Internet, and then details selected application scenarios. The applications are also classified as either control plane or data plane functionality as typical for the Classical Internet. This set of applications may, of course, naturally expand over time as the Quantum Internet matures. Finally, some general requirements for the Quantum Internet are also provided. This document can also serve as an introductory text to readers interested in learning about the practical uses of the Quantum Internet.

7. Security Considerations

This document does not define an architecture nor a specific protocol for the Quantum Internet. It focuses instead on detailing application scenarios, requirements, and describing typical Quantum Internet applications.

2.1. United States Department of Energy (DOE) and the associated reseach institutes

1) Report of the DOE Quantum Internet Blueprint Workshop

Summary

This resulting report identifies four Priority Research Directions (PRDs) for the implementation of the quantum internet and outlines five Blueprint Roadmap Milestones that must be achieved to facilitate an eventual national quantum Internet.

The four Priority Research Directions (PRDs) is as follows :

- Provide the Foundational Building Blocks for a Quantum Internet
- Integrate Multiple Quantum Networking Devices
- Create Repeating, Switching, and Routing for Quantum Entanglement
- Enable Error Correction of Quantum Networking Functions

The five Key Milestones is as follows :

- Verification of Secure Quantum Protocols over Fiber Networks
- Inter-campus and Intra-city Entanglement Distribution
- Intercity Quantum Communication using Entanglement Swapping
- Interstate Quantum Entanglement Distribution using Quantum Repeaters
- Build a Multi-institutional Ecosystem between Laboratories, Academia, and Industry to Transition from Demonstration to Operational Infrastructure

2.2. Quantum Internet Alliance (QIA) & QuTech

1) Quantum internet: A vision for the road ahead

Summary

In 2018, QuTech of the Netherlands published a comprehensive paper that could implement quantum Internet, and suggested six stages to complete quantum Internet using Qubit.

The six stage of quantum network is as follows :

- Trusted repeater networks (Quantum repeater)
- Prepare and measure networks
- Entanglement distribution networks
- Quantum memory networks
- Fault-tolerant few-qubit networks
- Quantum computing networks

2.3. EU QCI project

1) European industry White paper on the european Quantum Communication Infrastructure

Summary

In 2019, the EU's QCI project introduced a project plan aimed at commercializing a complete quantum information network from 2021 to 2035.

The goals of the QCI implementation program proposed in this document is as follows :

- Define in the coming months the stage 1 (2021-2028, Quantum-Secured Networks) and stage 2 (2028-2035, Quantum Information Networks).
- Define the structuring user requirements and derive them on the terrestrial and space components of the overall architecture.
- Start the development of European terrestrial products to be progressively integrated in metropolis-scale networks.
- Start the space segment trade-off/architecture studies for a development and technology plan definition including necessary in-orbit demonstration.
- Complete the deployment of the terrestrial local networks and develop the operational elements of the space component and of the resulting hybrid network management and operation means by 2028.
- In parallel, launch the preparation of the technology transfer from laboratory to industry for the terrestrial and space equipment needed to reach the second objective of the QCI – building a complete Quantum Information Network (2028-2034).
- In parallel, universities shall be incentivised to educate quantum engineers, a topic of utmost importance for a successful QCI ecosystem.

- In parallel, European law makers should generate the needed legislation in order to regulate the aspects of QCI rights, use and competition, and support industry in the creation of appropriate international standards.Trusted repeater networks (Quantum repeater)

2.4. Quantum Internet Task Force

1) QITF - Quantum Internet Whitepaper

Summary

The Quantum Internet Task Force take into account the history of the current Internet, and while valuing the diversity and interconnectedness of technologies, aim to create a future information society based on the Quantum Internet through its activities.

In this white paper, quantum Internet is a technology for exchanging quantum data, and in this respect, quantum Internet cannot be replaced by digital communication-based technology because it is fundamentally different from the communication base of digital data (hereinafter referred to as digital communication base).

In order to implement quantum Internet, a layered architecture for quantum Internet is required with a communication management protocol, a communication resource reservation algorithm protocol, and quantum entanglement purification. In other words, it is necessary to divide and organize functions and responsibilities necessary to realize quantum Internet by layer, and define interlayer interfaces. In the study from an architectural perspective, as described above, "how many layers of functions required to operate quantum Internet" is an important research task.

Since research of layered architecture is essential to technically and socially extend quantum Internet, they describe the structure of layered architecture of quantum Internet by referring to the layered architecture of classical Internet.

_____