Draft new Technical Report ITU-T Y.Supp.QN-UC

Use cases of quantum networks beyond QKDN

Summary

Based on the deliverable (D1.2) of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N), this Technical Report sorts and analyses use cases of quantum networks beyond QKDN collected from FG QIT4N in the context of networking technologies as the mandate of ITU-T SG13.

The uses cases which are only applied by quantum networks beyond QKDN are collected, investigated and summarized; all use cases are analysed by current bottlenecks, application scenarios, technical requirements and solutions. This Technical Report also provides analyses for future applications and potential standardization requirements.

Keywords

Quantum networks; Use cases; Network aspects of quantum information technology.

Table of Contents

Draft new technical Report ITU-T Y.Supp.QN-UC

Use cases of quantum networks beyond QKDN

1 Scope

This Technical Report presents the use cases of quantum networks beyond QKDN under three categories as follows:

- **Use cases based on quantum information networks (QINs):** use cases that depend on QIN to realize their function as for example, but not exclusive, to distributed quantum computing, distributed quantum sensing, quantum clock network, etc.
- **Use cases beneficial for classic networks:** use cases that can provide additional functionality, new characteristics, or improved performance for classic ICT networks as for example, but not exclusive to, quantum random number generator (QRNG), quantum time synchronization (QTS), quantum cryptography beyond QKD, etc.
- **Use cases where the network plays an intrinsic role for the QIT application:** use cases in which the QIT application is significantly defined or enhanced by the functionality provided by a QIN and/or a classical network and is beyond simple remote access of a QIT application via a classical network. Some examples include synchronization of quantum clocks, distributed QRNG beacons for smart contracting, etc.

NOTE – QIN could be defined as any network that incorporates quantum communication technologies for the purpose of transporting quantum states.

In particular, the content of this Supplement includes use cases of quantum networks beyond QKDN in various relevant fields of application and provides an analysis of their technical advantages, key enabling technologies, maturity and application prospects.

2 References

TBD

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following term defined elsewhere:

3.1.1 **<Term 1>** [Reference]: <optional quoted definition>.

3.1.2 **<Term 2>** [Reference]: <optional quoted definition>.

TBD

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

TBD

5 Introduction

This Technical Report elaborates on use cases of quantum networks beyond QKDN, from the use cases of the network aspects of QIT submitted during the lifetime of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N).

The use cases described in this report provide sufficient detail on the following aspects at a level that is understandable by readers who are not experts in this specific field:

– **Problem statement:** Describes an existing and relevant problem that a specific use case addresses from an end user's perspective.

– **Use case description:** Provides more detail on the application background of the use case, typical application scenarios or fields, etc. It also identifies the target end users of a given use case. An end user can be, e.g., an individual, organization, administrative entity, a commercial company, or combination(s) of these.

– **Motivation/advancement:** Describes the limitations and/or problems of the most relevant current solution(s) of the use case and clarifies how the application of quantum technology to a use case provides a technical advantage and other possible benefits.

– **Technical solution:** Provides a high-level description of the quantum technology-based solution, explaining its functional architecture, modes of operation, etc. Also discusses the challenges of the quantum technology solution, particularly compared to a standard solution (if available).

– **Application prospects:** Discusses the relevance of the use case (importance and frequency) and the existence of alternative solutions that solve the same problem. Also assesses the general cost structure and applicability to certain markets (public, administrative, military) estimating the size of the potential market.

Moreover, this Supplement summarizes key findings, suggestions for further application and standardization requirements and provides a repository of all collected use cases in Appendix I.

6 Use cases

(Editor’s Note) After reviewing the use cases from the FG-QIT4N in the Appendix, it’s necessary to select QCN related use cases in the context of networking technologies as the mandate of ITU-T SG13. Then, the selected use cases will be moved into this clause with details.

<TBD>

Appendix I

Overview of QIT4N use cases

(Editor's Note) This Appendix is the collection of QIT4N use cases as the result of FG-QIT4N. New use cases can be identified and reviewed. Contributions are invited.

This Appendix provides an overview of the QIT4N use cases considered by the Focus Group on Quantum Information Technology for Networks.

I.1 Quantum time synchronization use cases

I.1.1 Quantum time synchronization in telecommunications

Use case ID	UC-QTS-001
Short description	This use case provides high precision time reference from clock source/time server through communication network nodes to end devices/systems for specific applications (e.g., base station).
Target end users	Communications operator, time centre.

I.1.2 Secure quantum clock synchronization

Use case ID	UC-QTS-002
Description	Secure quantum clock synchronization is introduced to realize safe and reliable transmission of synchronization information to the end node. This use case is applicable to communication network, industrial Internet and other time-sensitive network applications.
Target end users	Communications operator, time centre.

I.1.3 A quantum network of entangled clocks

Use case ID	UC-QTS-003
Description	A quantum clock network that uses non-local entangled states can realize shared high precision (near the fundamental precision limit by quantum theory) timing by combining precision metrology and quantum networks for some applications like satellite navigation.
Target end users	National time service center, Telecom operators, etc.

I.2 Quantum computing use cases

I.2.1 Quantum cloud computing

Use case ID	UC-QC-001
Description	Potential applications range from basic research to commercial use such as big-data processing, artificial intelligence (AI), material design, and traffic flow optimization. One well-known application of quantum cloud computing is variation quantum Eigen (VQE) solver-based quantum chemistry simulations, where a classical computing server (cloud) is iteratively used to adjust control parameters of a quantum chip to find the energy spectrum of a given chemical structure. The result of the VQE simulation can be used for medicine design, oil processing and so on
Target end users	Researchers, students, governmental organizations, and private companies interested in the study and use of quantum computing techniques for research, education, and industry applications.

I.2.2 Distributed quantum computing

Use case ID	UC-QC-002
Description	This use case employs quantum computing technologies based on a distributed network of quantum devices to run quantum algorithms. Its applications cover both basic research and commercial uses like big-data processing, artificial intelligence, material design, and optimization of complex systems, etc.
Target end users	Quantum device owners, researchers, students, governmental organizations and companies interested in the study and use of quantum computing techniques for research, education, and commercial applications.

I.2.3 Blind quantum computing

Use case ID	UC-QC-003
Description	Focusing on enhancement of security and authorization schemes for computation and data when running quantum computing over networks, its applications cover both basic research and commercial uses like big-data processing, artificial intelligence, material design, and optimization of complex systems, etc.
Target end users	Quantum device owners, researchers, students, governmental organizations and companies interested in the study and use of quantum computing techniques for research, education, and commercial applications.

1.2.4 Quantum simulator in centralized/distributed quantum computing

Use case ID	UC-QC-004
Description	Recent technical advances have brought us closer to realizing practical quantum (circuit) simulators: engineered quantum many-particle systems that can controllably simulate complex quantum phenomena. Quantum simulators can address questions across many domains of physics and scales of nature, from the behaviour of solid-state materials and devices, chemical and biochemical reaction dynamics, to the extreme conditions of particle physics and cosmology that cannot otherwise be readily probed in terrestrial laboratories.
Target end users	Quantum device owners, researchers, students, governmental organizations and companies interested in the study and use of quantum computing techniques for research, education, and commercial applications.

1.2.5 Hybrid classical and quantum computing

Use case ID	UC-QC-005
Description	QAOA is a variational based quantum-classical hybrid algorithm to solve combinatorial optimization problems in near-term gate-based noisy intermediate-scale quantum computer. The original form of QAOA aims at finding the ground states of some special Hamiltonian, which encode the solutions of specifying combinatorial optimization problems such as Max-Cut problem, satisfiability problems (SAT). More recently, QAOA is developed as the quantum alternating operator ansatz which can also be useful for tackling those problems with some constraints such as the max independent set, traveling salesperson problem. In addition, QAOA is also found to be helpful for solving the problems of linear equations and factoring problem.
Target end users	Quantum device owners, researchers, students, governmental organizations and companies interested in the study and use of quantum computing techniques for research, education, and commercial applications.

I.3 Quantum random number generator use cases

I.3.1 Quantum randomness beacon service for smart contract

Use case ID	UC-QRNG-001
Description	This technology – randomness beacon –utilizes public randomness service from a trusted third party that meets certain requirements, or the randomness beacon. In order that the randomness beacon service is trusted, a beacon must provide full-entropy random numbers that are unpredictable before generation and verifiable after broadcasting.
Target end users	Users who have needs for business signatures in e-commerce, anonymous networks (such as block chain systems) and other services.

I.3.2 Quantum randomness beacon service for confidential disclosure

Use case ID	UC-QRNG-002
Description	Consider the situation that Alice, a keeper of a data bank of personal files, agrees to disclose a confidential content DIS to Bob. It is assumed that Alice is responsible for the authenticity of the DIS, and Bob agrees to keep it confidential. Let DIS denotes the actual string of the secret, referred to as a number dis. Alice must be sure that when she discloses the secret to Bob, she will have his receipt for DIS.
Target end users	Those who need the disclosure of confidential information from data centre.

I.4 Quantum communications use cases

I.4.1 Quantum digital signatures

Use case ID	UC-QCOM-001
Description	Digital signatures allow the exchange of digital messages from sender to multiple recipients, with a guarantee that the signature comes from a genuine sender. Quantum digital signatures can be made unconditionally secure, which ensures long-term security and quantum resistance.
Target end users	For critical IoT devices in industries such as transport, maritime, oil and gas, mining or agriculture, in which updating keys can be difficult.

I.4.2 Quantum anonymous transmission

Use case ID	UC-QCOM-002
Description	Anonymous transmission is a task that enables two nodes to communicate in a network anonymously. More precisely, one of the nodes of the network, the sender, communicates a quantum state to the receiver such that their identities remain completely hidden throughout the protocol. It implies that the sender's identity remains unknown to all the other nodes, whereas for the receiver it implies that no one except the sender knows her identity.
Target end users	Useful in cases where data from various sources must be aggregated while hiding the identity of the agents providing the data.

I.4.3 Quantum money

Use case ID	UC-QCOM-003
Description	Classical decentralized digital currencies are based on the use of a ledger called a blockchain. Operations such as token emission and spending are reported to the public ledger. Quantum money does not aim at decentralizing the transaction, but rather to strengthen their security. Quantum resources lead to tokens whose integrity can be verified by anyone, but that can only be spent once.
Target end users	Could be helpful in designing secure operations running across different blockchains.

Bibliography

TBD

Annex A

A.13 Justification for proposed draft new Technical Report TR.QN-UC

<table>
<tr><td>Question:</td><td>16/13</td><td>Proposed new ITU-T Technical Report</td><td colspan="2">Geneva, 14-25 November 2022</td></tr>
<tr><td>Reference and title:</td><td colspan="4">TR.QN-UC – “Use cases of quantum networks beyond QKDN”</td></tr>
<tr><td>Base text:</td><td colspan="2">Annex B</td><td>Timing:</td><td>Q4 2023</td></tr>
<tr><td>Editor(s):</td><td colspan="2">Chang-Yui Shin, Korea University, Korea, realmine@korea.ac.kr
Yuan Gu, ZTE, China, gu.yuan@zte.com.cn
Meng Zhang, MIIT, China, zhangmeng@caict.ac.cn
Zhangchao Ma, CAS Quantum Network Co., Ltd., China, mazhangchao@qtict.com
Yongli Zhao, BUPT, China, yonglizhao@bupt.edu.cn</td><td>Approval process:</td><td>Agreement</td></tr>
</table>

Purpose and scope (Define what this document will address and its intent or objectives in order to indicate the limits of its applicability):

This Supplement presents the use cases of quantum networks beyond QKDN under three categories as follows:

- **Use cases based on quantum information networks (QINs):** use cases that depend on QIN to realize their function as for example, but not exclusive, to distributed quantum computing, distributed quantum sensing, quantum clock network, etc.
- **Use cases beneficial for classic networks:** use cases that can provide additional functionality, new characteristics, or improved performance for classic ICT networks as for example, but not exclusive to, quantum random number generator (QRNG), quantum time synchronization (QTS), quantum cryptography beyond QKD, etc.
- **Use cases where the network plays an intrinsic role for the QIT application:** use cases in which the QIT application is significantly defined or enhanced by the functionality provided by a QIN and/or a classical network and is beyond simple remote access of a QIT application via a classical network. Some examples include synchronization of quantum clocks, distributed QRNG beacons for smart contracting, etc.

NOTE – QIN could be defined as any network that incorporates quantum communication technologies for the purpose of transporting quantum states.

In particular, the content of this technical report includes use cases of quantum network beyond QKDN in various relevant fields of application and provides an analysis of their technical advantages, key enabling technologies, maturity and application prospects.

Summary (provides a brief overview of the proposal):

Based on the deliverable (D1.2) of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N), this Technical Report sorts and analyses use cases of quantum networks beyond QKDNcollected from FG QIT4N in the context of networking technologies as the mandate of ITU-T SG13.

The uses cases which are only applied by quantum networks beyond QKDN are collected, investigated and summarized; all use cases are analysed by current bottlenecks, application scenarios, technical requirements and solutions. This Supplement also provides analyses for future applications and potential standardization requirements.

Relations to ITU-T Recommendations or to other standards (approved or under development):

ITU-T Recommendation Y.3800 series – Quantum key distribution networks

Liaisons with other study groups or with other standards bodies:

ITU-T SG11, SG17, ETSI ISG-QKD, IRTF QIRG

Supporting members that are committing to contributing actively to the work item:

Korea (Rep. of), KT Corp, ETRI, KAIST, Korea University, ZTE, CAICT, CAS Quantum Network Co., Ltd., BUPT

____