INTERNATIONAL TELECOMMUNICATION UNION
**TELECOMMUNICATION STANDARDIZATION SECTOR**
STUDY PERIOD 2022-2024

**SG13-TD307/WP3**
**STUDY GROUP 13**
**Original: English**

**Question(s):** 16/13 Geneva, 26 July 2023

**TD**

| | | |
|---|---|---|
| **Source:** | Editors | |
| **Title:** | Draft new Technical Report ITU-T TR.QN-UC: "Use cases of quantum networks beyond QKDN" (output of interim meeting, 17-21 July 2023) | |
| **Contact:** | Chang-Yui Shin<br>Korea University<br>Korea (Rep. of) | Tel: +82-10-6398-0139<br>E-mail: realmine@korea.ac.kr |
| **Contact** | Yuan Gu, ZTE, China | Email: gu.yuan@zte.com.cn |
| **Contact** | Meng Zhang, MIIT, China | Email: zhangmeng@caict.ac.cn |
| **Contact:** | Zhangchao Ma<br>CAS Quantum Network Co., Ltd.<br>China | E-mail: mazhangchao@qtict.com |
| **Contact** | Yongli Zhao, BUPT, China | Email: yonglizhao@bupt.edu.cn |

**Abstract:** This document is the output of draft technical report ITU-T TR.QN-UC – "Use cases of quantum networks beyond QKDN" (Q16/13 meeting, Geneva, 17-21 July 2023).

**Summary**

This TD is the output for the draft Technical Report ITU-T TR.QN-UC – "Use cases of quantum communication networks" based on the following input contributions and the discussion during the Q16/13 meeting, Seoul, 17–21 July 2023.

Base document: **TD269/WP3**

| | | | |
|---|---|---|---|
| C-132 | BUPT | Technical Report ITU-T TR.QN-UC "Use cases of quantum networks beyond QKDN": Proposed supplement on use cases | Q16/13 |

- This contribution purposes to supplement use cases with details according to the given template on Draft Technical Report ITU-T TR.QN-UC: "Use cases of quantum networks beyond QKDN".

| | | | |
|---|---|---|---|
| C-133 | ETRI, Korea University, KT Corporation | Updates for the identified use cases in TR.QN-UC: "Use cases of quantum networks beyond QKDN | Q16/13 |

- This document provides updates for the identified use cases in TR.QN-UC – "Use cases of quantum networks beyond QKDN", based on the result of Q16/13 meeting, Seoul, 7-12 June 2023.

Meeting result

- The meeting has agreed to accept the two input contributions.

**Annex A**

## Draft new Technical Report ITU-T TR.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**

**Page**

# Draft new Technical Report ITU-T TR.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~~ Technical Report 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 Technical Report~~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 Technical Report~~Supplement~~

None.

### 4 Abbreviations and acronyms

This Technical Report~~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:

- ~~—~~**Use case ID**: e.g., UC-QN-00X.
- **Use case description**: presents a short summary, overall explanations for a use case including background, motivations, related technologies and target areas, if possible with a diagram.
- **Problem statement**: identifies problems and/or limitations related to the use case.
- **Technical considerations**: discusses various technical issues and challenges to solve problems and/or limitations identified.
  NOTE: Technology maturity: assesses the maturity of the key technical solutions required to address technical considerations above, e.g., Technology Readiness Level (TRL), etc.
- **Standardization considerations**: identifies relevant standardization items for quantum networks beyond QKDN including any suggestions for future standardization in line with ITU-T SG13 work scope.
- **Others**: 1) Benefits and impact to describe the benefits that the use case would bring, and the impact it would have when applied. 2) Application prospects to assess the relevant application areas and potential markets, etc.

~~**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~~Technical Report 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.*

~~*(Editor's Note) At the SG13 meeting (Geneva, 13 – 24 March 2023), the meeting has agreed to use the following use case template.*~~

- ~~**Use case ID**: e.g., UC-QN-00X.~~
- ~~**Use case description**: presents a short summary, overall explanations for a use case including background, motivations, related technologies and target areas, if possible with a diagram.~~
- ~~**Problem statement**: identifies problems and/or limitations related to the use case.~~
- ~~**Technical considerations**: discusses various technical issues and challenges to solve problems and/or limitations identified.~~
  ~~NOTE: Technology maturity: assesses the maturity of the key technical solutions required to address technical considerations above, e.g., Technology Readiness Level (TRL), etc.~~
- ~~**Standardization considerations**: identifies relevant standardization items for quantum networks beyond QKDN including any suggestions for future standardization in line with ITU-T SG13 work scope.~~
- ~~**Others**: 1) Benefits and impact to describe the benefits that the use case would bring, and the impact it would have when applied. 2) Application prospects to assess the relevant application areas and potential markets, etc.~~

### I.1 Quantum time synchronization use cases

Quantum time synchronization (QTS) describes how quantum technology can be used to achieve high-precision or secure and reliable frequency/time synchronization. The following QTS use cases are provided in this Technical Report:

– **UC-QTS-001** describes the applicability of QTS technology in existing communication networks to achieve ultra-high precision time synchronization. This technology has the potential to evolve into quantum networks in the future.

– **UC-QTS-002** describes the applicability of quantum technology in resisting security attacks in synchronous networks.

– **UC-QTS-003** describes the applicability of quantum frequency/time synchronization technology in quantum star networks. Frequency and time information can be transmitted using entangled qubits and auxiliary classical channels in quantum networks. All nodes in the quantum network can then achieve frequency/time synchronization.

#### I.1.1 UC-QTS-001: Quantum time synchronization in telecommunications

**Use case ID:** UC-QN-001**.**

- **Use case description:** Quantum time synchronization provides a high precision time reference from clock source/timeserver through communication network nodes to end devices/systems (e.g., base stations) for specific applications. Target end users for it include telecommunication operators and time service centres.

- **Problem statement:** As applications evolve, high accuracy of time synchronization is required and, since positioning is an important scenario in the development of IoT, positioning requires much higher time synchronization accuracy, i.e., 1 meter positioning accuracy = 3 ns time synchronization accuracy. Based on these requirements, a ps level of time synchronization accuracy is needed. However, current technical solutions (e.g., PTP) can only achieve ns level of time synchronization accuracy.
- **Technical considerations:** Current technical solutions (e.g., PTP) can only achieve ns level of time synchronization accuracy in typical telecommunication networks which have many nodes

(e.g., 20 nodes in simulation module as standardized in ITU-T Recommendations in the G.827x series). As applications evolve, there may be a big network with more nodes in the future and it is unlikely to meet the time synchronization accuracy by reducing the number of nodes. Two aspects can be considered to improve the time synchronization accuracy of communication networks, i.e., clock source and synchronization protocol. In the past two decades, more results and great progress has been achieved by scientific projects dealing with optical clocks. However, before optical clocks become a universally adopted clock source/timescale, there are still several issues that need to be studied:

① **Service time of optical clocks:** From minutes to hours, the progress has been very slow. It is not clear what the best current performance is, but optical clocks are significantly more modest than the atomic fountains which are the current primary frequency standards.

② **Comparison between optical clocks:** Currently in practice, there is a low possibility of comparing optical clocks to each other in the same laboratory because very few National Measurement Institute (NMI) laboratories have two optical clocks due to their complexity and cost. Comparing optical clocks remotely is an alternative method, however, due to the high performance in frequency stability, it is not possible to use classical methods for remote comparison.

③ **Distribution of optical clock source reference:** As the performance of optical clocks is extremely high in practice, it will take a long time and significant investments to build distribution networks for new reference signals (with protection features) to serve entire networks. Using quantum states, quantum bits, and entangled state transmission is another possible way to build the distribution network.

- **Standardization considerations:** Most of the required technologies in the QTS belong to SG13.In future work, the standardization requirements may include technical framework, new technical requirements from other perspectives, etc.

- **Others:** Synchronization networks are one of the basic networks of communication networks. Current time synchronization networks consist of three parts: time source, time transmission and end application. Improving the time synchronization accuracy can be achieved by using a quantum clock source and/or quantum synchronization protocols in communication networks. With this and the previous description in consideration, the size of the potential market for quantum clock synchronization (QCS) could be estimated at around 100 billion.

### I.1.2 UC-QTS-002: Secure quantum clock synchronization

~~**Use case description**~~

~~Security attacks on time synchronization have a serious adverse impact on services that depend on accurate time. Secure quantum clock synchronization is introduced to realize safe and reliable transmission of synchronization information to the end node.~~

~~Target end users for UC-QTS-002 include telecommunication operators and time service centres.~~

~~**Problem statement**~~

~~In recent years, with the introduction of various attacks on the clock synchronization protocol, the security of clock synchronization has received widespread attention. Therefore, when using a clock synchronization protocol outside of a fully trusted network environment, it needs to be protected. The clock synchronization protocol is particularly susceptible to delay attacks because changes in the time at which messages are sent and received can cause errors in the calculation of the clock difference between two nodes. Delayed attacks, in particular, decrease the accuracy of clock~~

~~synchronization which can cause applications that depend on it to fail. Such attacks can seriously affect time-sensitive network applications.~~

**Use case ID:** UC-QN-002.

- **Use case description:** Security attacks on time synchronization have a serious adverse impact on services that depend on accurate time. Secure quantum clock synchronization is introduced to realize safe and reliable transmission of synchronization information to the end node.

- **Problem statement:** In recent years, with the introduction of various attacks on the clock synchronization protocol, the security of clock synchronization has received widespread attention. Therefore, when using a clock synchronization protocol outside of a fully trusted network environment, it needs to be protected. The clock synchronization protocol is particularly susceptible to delay attacks because changes in the time at which messages are sent and received can cause errors in the calculation of the clock difference between two nodes. Delayed attacks, in particular, decrease the accuracy of clock synchronization which can cause applications that depend on it to fail. Such attacks can seriously affect time-sensitive network applications.
- **Technical considerations:** Entangled photon pairs generated by spontaneous parameter down conversion (SPDC) have been widely used in quantum information protocols. Alice and Bob each have a source of polarization entangled pairs generated by SPDC. Each entangled photon pair can be detected by either the local or remote detector. Both Alice and Bob use the local clock to record the moment when the photon is detected and these differences between the time labels can be extracted by calculating a crosscorrelation between events at both sides. Such a protocol based on quantum communication technology can provide a verified and secure time synchronization protocol.Unlike classical protocols designed to improve the security of time distribution, this quantum synchronization protocol does not require any assumptions about the distance or propagation time between clocks.Even though eavesdroppers could potentially master quantum non-demolition (QND) measurement or direct generation of controllable coherent single photon non-reciprocity in future, at present there is no means to do so thus, the quantum clock synchronization protocol is secure when the adversary cannot perform QND measurements on a single photon.

- **Standardization considerations:** In addition to conforming to the standardized content stipulated by existing standards, we can also consider the specific constraint standards of dynamic scenarios.

- **Others:** Secure quantum clock synchronization is currently in the experimental research stage and does not meet conditions for commercialization.

### I.1.3 UC-QTS-003: A quantum network of entangled clocks

~~**Use case 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 for UC-QTS-003 include telecommunication operators and time service centres.~~

~~**Problem statement**~~

~~The standard time generally used around the world is Coordinated Universal Time (UTC), which is produced by the international atomic time cooperation led by BIPM: about 80 punctuality~~

~~laboratories distributed around the world use more than 500 commodity punctual clocks to generate their own local time. Each laboratory reports the relevant data to BIPM through satellite comparison and weighs all atomic clock data to obtain the free atomic time (evaluation assurance level (EAL)). The frequency reference (PFS) developed by a few countries is used to control and correct the system deviation to generate the international atomic time (TAI) which is corrected by irregular leap seconds to get UTC. The process of weighted average of clock group usually adopts the classical method so that the precision of classical algorithm cannot exceed the standard quantum limit (SQL).~~

~~On the other hand, in recent years many new types of synchronous security attacks such as GPS satellite retreat, satellite simulator interference, time source switching caused by PTP disoperation, message attacks and delay attacks against synchronous transmission protocol, etc. have brought many negative impacts on business activities and network operations. With the large-scale construction and operation of 5G networks, the openness of the network and the diversification of service types have made the security problems of synchronization networks increasingly prominent.~~

**Use case ID:** UC-QN-003.

- **Use case 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.

- **Problem statement:** The standard time generally used around the world is Coordinated Universal Time (UTC), which is produced by the international atomic time cooperation led by BIPM: about 80 punctuality laboratories distributed around the world use more than 500 commodity punctual clocks to generate their own local time. Each laboratory reports the relevant data to BIPM through satellite comparison and weighs all atomic clock data to obtain the free atomic time (evaluation assurance level (EAL)). The frequency reference (PFS) developed by a few countries is used to control and correct the system deviation to generate the international atomic time (TAI) which is corrected by irregular leap seconds to get UTC. The process of weighted average of clock group usually adopts the classical method so that the precision of classical algorithm cannot exceed the standard quantum limit (SQL).On the other hand, in recent years many new types of synchronous security attacks such as GPS satellite retreat, satellite simulator interference, time source switching caused by PTP disoperation, message attacks and delay attacks against synchronous transmission protocol, etc. have brought many negative impacts on business activities and network operations. With the large-scale construction and operation of 5G networks, the openness of the network and the diversification of service types have made the security problems of synchronization networks increasingly prominents.
- **Technical considerations:** There is a quantum-based cooperative protocol for operating a network of geographically remote optical atomic clocks. By using non-local entangled states, an optimal utilization of global resources can be realized. This kind of network can operate near the basic precision limit set by quantum theory. In addition, the internal structure of the network, combined with quantum communication technology, ensures the security against internal and external threats. The realization of such a global quantum clock network can enable a real time single international time scale (World Clock) with unprecedented stability and accuracy to be built.

- **Standardization considerations:** In addition to conforming to the standardized content stipulated by existing standards, its future standardization can also consider the specific constraint standards of dynamic scenarios.

- **Others:** A quantum network of clocks can have important scientific, technological and social implications. Besides creating a worldwide platform for time and frequency metrology, such a network may find important applications in other areas such as earth science, precise navigation

of autonomous vehicles and space probes (requiring high refresh rate) and the testing of and search for fundamental laws of nature, including relativity and the connection between quantum and gravitational physics.

Formatted: Font:

## I.2 Quantum computing use cases

The quantum computing use cases described in this report are focused on the application and method of quantum computing, each with different requirements and features as shown in Table 2.

*Table 2 – Features of different use cases for quantum computing*

| ID | Name | Features |
|---|---|---|
| UC-QC-001 | Quantum cloud computing | User data, code, resources, etc. are fully hosted in the cloud computing platform. |
| UC-QC-002 | Distributed quantum computing | In the distributed quantum computing network, the quantum chipsets realize the expansion of computing power in the form of tensor product in the entangled state |
| UC-QC-003 | Blind quantum computing | Quantum/classical client and quantum server adopt the security enhancement technology of quantum cryptographic protocol |
| UC-QC-004 | Quantum simulator in centralized/distributed quantum computing | Within the data centre or across the WAN networking scenario, the classical computing server cluster performs meaningful quantum computing circuit simulation tasks |
| UC-QC-005 | Hybrid classical and quantum computing | The classical and quantum computing units cooperate and work together via classical communication networks. |

### I.2.1 UC-QC-001: Quantum cloud computing

**Use case description**

Potential applications of UC-QC-001 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 for UC-QC-001 include researchers, students, governmental organizations, and private companies interested in the study and use of quantum computing techniques for research, education, and industry applications.

**Problem statement**

Resources required for quantum computing may be beyond what an end user can afford. The question is thus: *Is there a solution that gives access to quantum computation technology to as many end users as possible at an affordable cost per end user?*

**Technical considerations**

The amount of data today's society processes per day continues to grow exponentially. The electronic circuit line width of silicon-based computer chips has been narrowed down to nearly the

atomic scale where quantum effects take over. It is well-known that in the atomic domain, quantum computing techniques show exponential speedup or use significantly less resources than classical computers to solve some difficult problems such as factorizing a big number into primes. However, the manufacturing techniques to produce a quantum computer are not mature yet and may be too expensive to allow an individual or small organization to exclusively own one. The solution presented in clause 6.2.1.4 and Figure 10 brings the benefits of quantum technology to many end users while remaining at low cost per user.

Quantum cloud computing (QCC) is a commercial model that allows many users to run quantum computing programs at an affordable price per user, see Figure 10. In a QCC system, a simulator and/or real quantum computing hardware is settled in a centralized server/hub, as called cloud, and the remote end users (or classical client) can access it via traditional internet/network or perhaps the quantum internet/network in the future. Presently, the technologies of the classical network and computing, such as the quantum simulator and software in cloud platform, are ready to support QCC solutions.

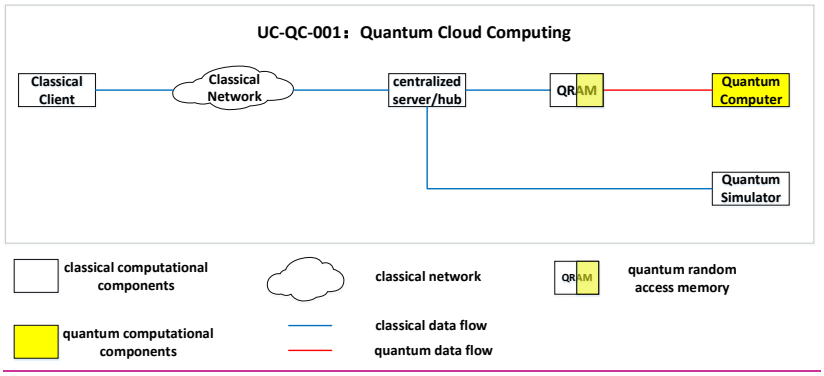



**Figure 10 – Networking and computation model of quantum cloud computing**

## Standardization considerations

Quantum computing is usually described in a quantum circuit model with N qubits, which can be spanned into a $2^N \times 2^N$ matrix space mathematically. Due to the nature of quantum computing, a user would have to load a great amount of data if they wanted to read out an N-qubit quantum system faithfully. Petabyte order of magnitude of classical bit data has been generated when simulating a 45-qubit quantum circuit [b-Häner]. Of course, in a real physical quantum circuit or by using some tricks, readable data can be sampled by measuring some quantum observables and this process might reduce the amount of classical data to be transferred to an end user. However, it will still yield a great pressure of load to the classical network when the number of qubits is large. As the simulators and physical chips of quantum computers scale up, current networks will need to be upgraded in all aspects for the quantum computing service to be hosted over a communication network. New types of networks are even required to be built if the output of data is transferred over a pure quantum internet.

The QCC service, either deployed using simulators or quantum hardware, has emerged and is providing free or low-cost computing experience to a broad range of end users in the frontier of quantum studies. In the foreseeable future, it could bring revolutionary and cost-efficient computational capability to a broad spectrum of applications including in civil administration, medicine development, material industry, environmental preservation, etc. In comparison to

Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight

alternative technologies, QCC is believed to have the best performance-to-cost ratio as different users keep using the machine without owning it.

**Others**

### I.2.2 UC-QC-002: Distributed quantum computing

**Use case description**

Similar to UC-QC-001, UC-QC-002 also 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 for UC-QC-002 include 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.

**Problem statement**

A quantum computing chip is very difficult to scale up while remaining at good fidelity. This is due to the growing coupled noise in the chip and with the environment when the system expands. However, there are many small-scale quantum devices distributed in various labs. The question, thus, is: *Is it possible to build a network of distributed quantum hardware to lift the computational power beyond any single quantum chip has?*

**Technical considerations**

**Standardization considerations**

**Others**

*(Editor's Note) From C-075 (Q16/13 e-meeting, 11-16 January 2023), the following use case on distributed quantum computing has been added.*

Formatted: Font color: Auto, English (United Kingdom)

Formatted: Normal, Left, Tab stops: Not at 0.63 cm + 1.63 cm

Formatted: Highlight

## 6.1 D~~istributed~~istributed quantum computing

Use cases based on quantum information networks (QINs) refer to use cases that depend on QIN to realize their function. Distributed quantum computing is one of the most representative examples.

### 6.1.1 Use case description

Distributed quantum computing (DQC) 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.

### 6.1.2 Technical solution

DQC is a technology based on networks of distributed quantum chips that allow computational power multiplications of individual quantum devices, see Figure 1.

Two types of technical solutions for distributed quantum computing[b-Denchev] are identified as follows.

Firstly, it is leveraging quantum mechanics to enhance classical distributed computing. For example, entangled quantum states can be exploited to improve leader election in classical distributed computing, by simply measuring the entangled quantum states at each party (e.g., a node or a device) without introducing any classical communications among distributed parties. It generally does not need to transmit qubits among distributed parties.

Secondly, it is distributing quantum computing functions to distributed quantum computers. A quantum computing task or function (e.g., quantum gates) is split and distributed to multiple physically separate quantum computers. And it may or may not need to transmit qubits (either inputs or outputs) among those distributed quantum computers. Entangled states will be needed and actually consumed to support such distributed quantum computing tasks.

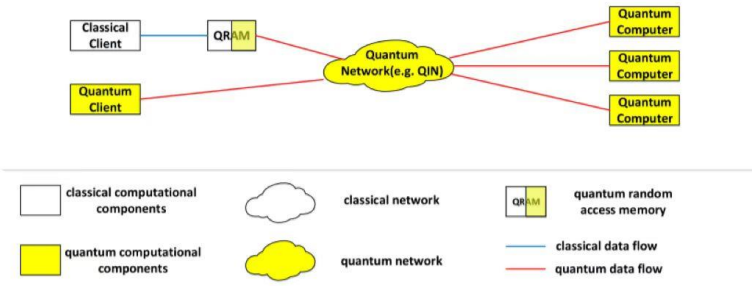



Figure.1 Networking and computation model of distributed quantum computing

In a DQC system, the tensor-product-like coupling of the joint quantum computing network generates computational advantages over the sum of individual chips' capability. Presently, technologies of quantum computational components and quantum networks require further study, therefore this solution is still in very early stages of development.

### 6.1.3 Application prospects

As shown in Figure 2, one of the most promising quantum algorithms that can run on near-term intermediate scale quantum (NISQ) computing hardware is variation quantum algorithm (VQA). VQA can be adapted to quantum chemistry applications through variation quantum eigen solver (VQE) and optimization applications through quantum approximate optimization algorithm (QAOA). Both algorithms can be realized using a DQC system by encoding the original problems with compound Hamiltonian terms. Taking the QAOA case, for instance, a full QAOA quantum circuit can be decomposed into many smaller sub-circuits which can be scheduled and executed on individual nodes of a DQC system. Then, the expectation value of an observable of the whole system can be calculated on a classical computer (the master node) by collecting measurement results of individual nodes with a given set of control parameters for distributed sub-circuits. To find a solution of the corresponding quantum chemistry problem or the combinatorial optimization problem, one iteratively calculates the expectation value by updating the set of control parameters until convergence.

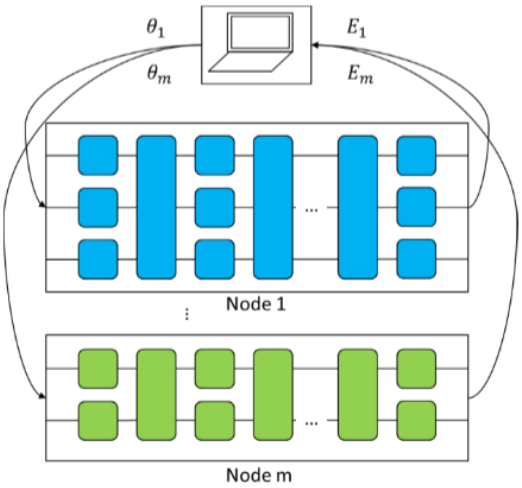



Figure.2 An application of quantum computing on distributed networks

A DQC system is expected to be implemented over classical and/or quantum networks to enhance the computational power beyond any single unit's capability in the network. In the foreseeable future, it may bring revolutionary and cost-efficient computational capability to a broad spectrum of applications including in civil administration, medicine development, material industry, environmental preservation, etc. It may also solve the scale-up problem that limits individual chips.

### I.2.3 UC-QC-003: Blind quantum computing

**Use case description**

Focusing on enhancement of security and authorization schemes for computation and data when running quantum computing over networks, the applications of blind quantum computing cover both basic research and commercial uses like big-data processing, artificial intelligence, material design, and optimization of complex systems, etc.

Target end users for UC-QC-003 include 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.

**Problem statement**

Quantum computation shows great potential for solving some important problems faster than classical computation. However, a practical quantum computer needs to be large enough to handle sufficient numbers of delicate qubits, perhaps extending into the high millions or low billions of physical qubits. Large-scale quantum "mainframes" will be valuable resources and time-sharing of machines will be economically attractive. Time-sharing quantum cloud services will allow owners of smaller quantum computers to perform large quantum computations. Sometimes the input and output data are private and even the choice of quantum computing algorithms may be sensitive information, so they have to be kept secret even from the server [b-Morimae-1]. The question thus

is: "*Is there a technical solution within quantum aspect that can let the client execute quantum computations on a server without revealing any secret information about the computation?*"

**Technical considerations**

In recent years, several protocols have emerged which seek to tackle the privacy issues raised by delegated quantum computation. Going under the broad heading of blind quantum computing (BQC) provides a way for a client to execute a quantum computation using one or more remote quantum servers while keeping the structure of the computation hidden. While the goal of BQC protocols is to ensure the privacy of the computation, many of them also allow for verification of the computation being performed by embedding hidden tests within the computation.

### 6.2.3.4 Technical solution

As shown in Figure 13, BQC is a technology that combines notions of quantum cryptography protocols [b-Morimae-1], [b-Morimae-2], [b-Sheng], [b-Li] and quantum computation. It can fulfil quantum computation by a client with limited or even no quantum computational power with the help of an unreliable quantum server while keeping the privacy of the client's algorithm and the data. Today's BQC technical solutions, computation and networking protocols are quite active, but it may take a relatively long time to realize BQC in engineering.

Formatted: Highlight

Formatted: Highlight

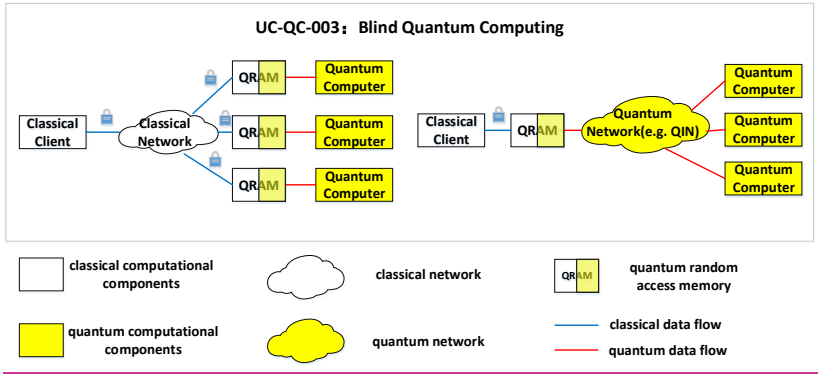



**Figure 13 – Networking and computation model of blind quantum computing**

Formatted: Highlight

**Standardization considerations**

A BQC system is expected to be implemented over classical and/or quantum networks to enhance the security and authorization scheme for computation and data through the network. In the foreseeable future, it may bring revolutionary capability to these applications which are sensitive in data security and personal privacy including e-commerce, finance, banking, insurance, medical treatment, etc.

**Others**

### I.2.4 UC-QC-004: Quantum simulator in centralized/distributed quantum computing

**Use case description**

Recent technical advances have brought the world 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 for UC-QC-004 include 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.

**Problem statement**

Quantum simulators are a promising technology on the spectrum of quantum devices from specialized quantum experiments to universal quantum computers. These quantum devices utilize entanglement and many particle behaviours to explore and solve hard scientific, engineering, and computational problems. Rapid development over the last two decades has produced more than 300 quantum simulators in operation worldwide using a wide variety of experimental platforms [b-Altman]. Recent advances in several physical architectures promise a golden age of quantum simulators ranging from highly optimized special purpose simulators to flexible programmable devices. These developments have enabled a convergence of ideas drawn from fundamental physics, computer science, and device engineering. They have strong potential to address problems of societal importance, ranging from understanding vital chemical processes, enabling the design of new materials with enhanced performance, to solving complex computational problems. In practice, a hybrid system may be helpful to improve the precision of quantum simulators, where a classical computer server is applied to help optimize parameters of quantum simulators based on optimal quantum control technique or feedback/feed-forward mechanism.

Beside the quantum simulation using quantum devices, equivalent quantum circuit models can be derived and simulated on a classical computer or a cluster of classical computers. This type of simulator is called a quantum circuit simulator and they are crucial before quantum devices become mature enough and robust to noise. Currently, quantum circuit simulators are also useful tools to verify quantum computing algorithms and to develop quantum software. Since it usually requires a large scale of clusters to run a meaningful circuit simulation, a quantum circuit simulator is usually deployed on a cloud server.

In many cases, large scale quantum computation tasks with quantum (circuit) simulators may relay on distributed computing clusters over cloud environments in which clients and servers may be in local or wide area networks.

**Technical considerations**

Centralized or distributed quantum computing applications enabled by classical communication networks have many forms. Taking currently available commercial models as an example, quantum circuit simulators on cloud, control pulse optimization service, and classical-quantum hybrid computing service are well-known instances of these forms. However, existing networks are not specifically designed for these quantum computing applications. There are still challenges and requirements for the existing classical communication networks such as big data traffic and communication overheads, deterministic delay and/or low-latency, high security and privacy, reliability or robustness, etc.

These services require massive computing power which could be implemented by centralized or distributed classical computation over classical networks that may not exist for a long time. Three typical network components for a general quantum computation service over classical networks, as illustrated in ~~Figure 14~~, are:

– **Component Class A (inner network):** Interconnection and communication networks of computation clusters merely inside a Data Center (DC).

– **Component Class B (edge network):** Key networks components linking different DCs in a local network.

– **Component Class C (wide network):** Key network components linking different DCs yet across a wide area network.

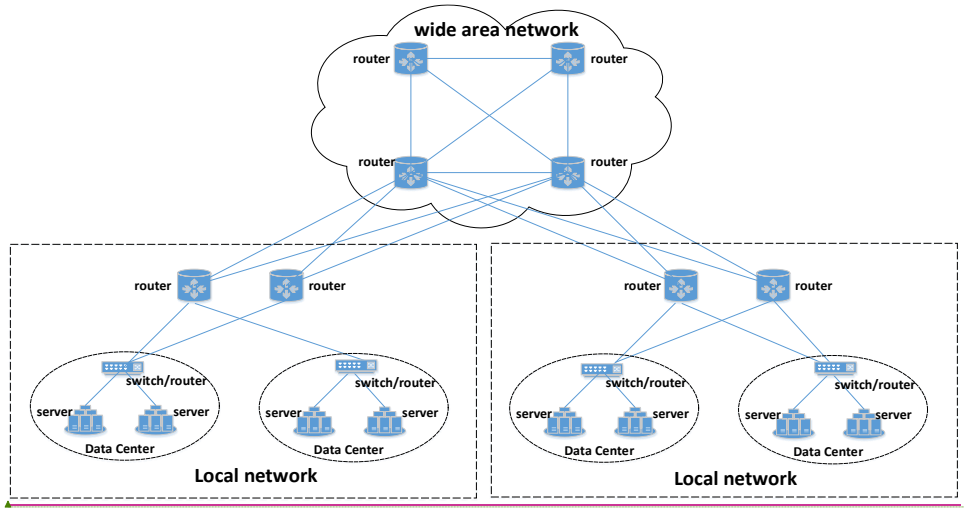



**Figure 14 – Typical network scenario of computation clusters over classical networks**

It should be noted that different network component classes have different network environments (such as physical topology, bandwidth, delay, bit error rate, node/link stability, packet loss rate), which may adopt different computation/communication architectures (such as parameter servers and all-Reduce), parallel modes (such as data parallel and model parallel), and communication methods (such as synchronous communication and asynchronous communication) to form different computation-communication frameworks. Different frameworks have different transmission modes (such as the logical topology of parameter synchronization), communication overhead and communication pace and other traffic characteristics, which have different degrees of impact on synchronization time and system scalability.

However, existing networks are not fully prepared for these quantum computing applications. There are still some challenging requirements for suitable classical communication networks as described below:

– **Reducing big data traffic and communication overhead:** considering the high capacity and communication of quantum computing, these use cases of QIT over traditional networks may generate considerable amounts of data over the internet and could greatly impact current network infrastructure. [b-Häner] reports that a scheduling algorithm was applied to quantum supremacy circuits in order to reduce the required communication and simulate a 45-qubit circuit on the Cori II super-computer using 8192 nodes and 0.5 petabytes of memory. A large amount of computing performance was used to handle the

Formatted: Highlight

Field Code Changed

Formatted: Highlight

communication load while the communication load could still account for 75% of the calculation time.

– **Deterministic delay and/or low-latency:** some applications such as running some VQE and QAOA instances rely on feedback between classical and quantum components to update the state of computation which may need timely information exchange across wide areas of a network. In addition, quantum machine learning (QML) usually requires multiple iterations of gradient model parameter updates. Bad performance of delay would reduce the efficiency of model convergence and even lead to failure of QML training.

– **High security and privacy:** the security of computation and communication between different nodes in classical networks is essential and, for data-sensitive applications in particular, data privacy and user authentication is even more essential.

– **Reliability or robustness:** the reliability or robustness of a network should be guaranteed during the life cycle of computation tasks and data exchange in distributed quantum computing enabled by classical communication networks. However, this may not be fully satisfied with the TCP/UDP protocols of the current best effort design of the internet.

There are, however, some novel techniques induced by new service requirements over classical networks, for example content delivery networks (CDNs) were designed to improve the performance of real-time video streams, IEEE 802.1 time sensitive network (TSN) was proposed and standardized for low latency and rapid response demand of industrial internet etc.

Existing classical networks are required to either be adapted, adjusted or re-designed to serve these quantum computing applications and novel services.

The technologies of a quantum simulator in centralized/distributed quantum computing are completely implemented within the framework of classical networks and classical computation which can serve as a relatively mature solution at present, see Figure 15. It is noted that quantum computing tasks done using a quantum simulator can be regarded as a new service supported by classical network and classical computing.

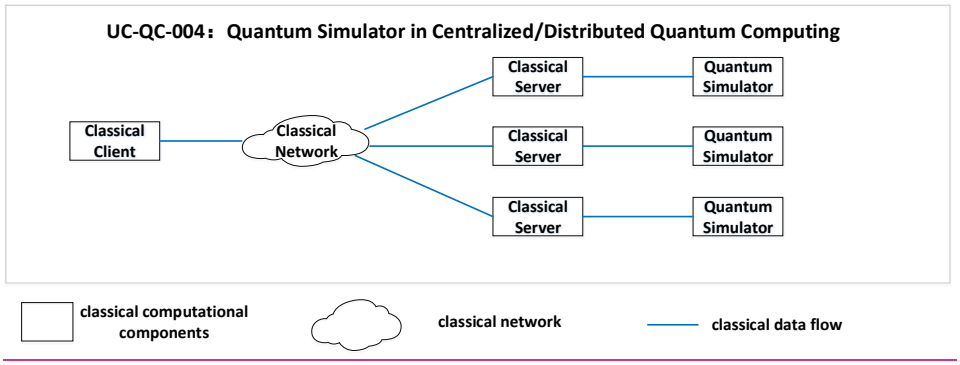



**Figure 15 – Networking and computation model of quantum simulator in centralized/distributed quantum computing**

Formatted: Highlight

However, distributed quantum computing tasks executed on quantum (circuit) simulators over classical networks still face some technical challenges. Potential quantum-computing-motivated technical solutions such as blockchain, RDMA, lightweight cryptography, self-adaptive and intelligent routing schemes as well as resource scheduling mechanisms, etc. are proposed for further discussion:

– To fulfil the reduction of big data traffic and communication overhead, highly-tuned kernels [b-Häner] in combination with novel parallel acceleration and reusing technologies are considered for further studies, including extraction and optimization of communication load characteristics under specific QC services, novel parallel collaboration policy of models, computation and communication architectures, novel logical networking schemes different from traditional fat-tree architecture, novel networking protocols different from TCP/UDP etc.

– To fulfil the low-latency feature of networks for these use cases, one might want to consider remote direct memory access (RDMA) technology as shown in Figure 16. Compared to the classical TCP/IP network, RDMA can directly access the memory of another machine from one machine without any processing of the target machine's operating system. Direct memory access avoids copying data twice from the user mode to core mode and back to user mode, saving the CPU occupancy of the target machine and effectively improving throughput and reducing latency. The flow control technology (namely PFC) used on the switch side of the RDMA network can avoid packet loss caused by buffer overflow in the switch thereby eliminating the in-cast phenomenon.

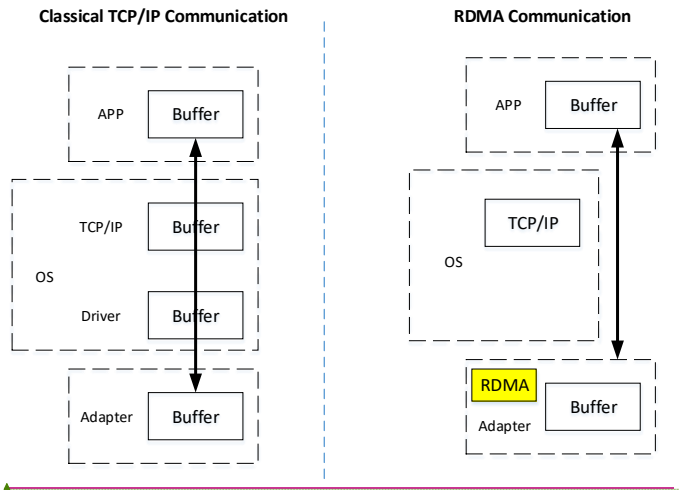


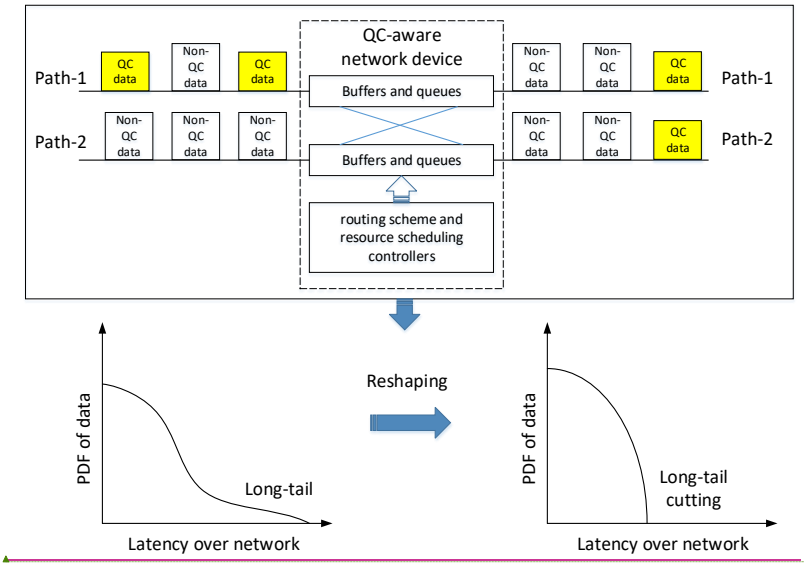

**Figure 16 – Classical TCP/IP communication vs RDMA communication**

For some cases, a determined response latency is crucial for quantum control and some hybrid computing scenarios which may require a self-adapted resource allocation protocol for networking. Furthermore, self-adaptive and intelligent routing schemes and resource scheduling mechanisms are also worth studying to adapt the characteristics of simulated quantum computing and unique service traffic distribution over classical networks to balance local computation and communication over networks. In Figure 17, considering the special characteristics of QC data distribution vs latency over network with a long-tail, a QC-aware device or module can be designed to reshape the probability density function (PDF) of QC data flow vs latency under self-adaptive and intelligent routing scheme and resource scheduling mechanism to control end-to-end delay/latency of specific QC tasks on demand.

Field Code Changed

Formatted: Highlight

Formatted: Highlight




Field Code Changed

**Figure 17 – Latency control over network towards simulated Quantum computing (QC) service**

Formatted: Highlight

– To fulfil the security and privacy requirements of quantum computing applications over classical networks, new lightweight cryptography technologies are required. Otherwise, the encoding process of cryptography over the large amount of data will inevitably increase the time delay and communication overhead from end to end. Hardware-based cryptographic methods may be helpful for this purpose. Blockchain may also be useful for tracking data flow.

– To fulfil the reliability or robustness of networks while a great amount of data is transferring, high-efficient lossless data transferring technologies should be studied. Naturally, how the channel capacity affects the computational precision of quantum computing scenarios relying on the feedback between classical and quantum components (like some VQE and QAOA algorithms etc.) may be a good direction to pursue. For some quantum computing tasks under NISQ, whether the final calculation performance can allow packet loss over complex and large-scaled networks and tolerate some transmission errors is also a new direction worth studying. In addition, based on the characteristics of quantum simulation computing and unique data distribution, a quantum computing-aware routing and protection strategy should be adopted to design an intelligent logical topology over physical topology of networks.

In summary, descriptions and analysis of QC service, network challenges and potential QC motivated technical solutions are shown in Table 3.

Formatted: Highlight

**Table 3 – Descriptions and relationship of QC service, network challenges and potential QC-motivated technical solutions**

| Challenges and requirements of classical networks | Service of QC by simulators | Potential quantum computing motivated technical solutions |
|---|---|---|
| Reducing big data traffic and communication overhead | Full amplitude QC with large qubits, etc. | Highly tuned kernels in combination [b-Ebubechukwu], novel parallel collaboration policy, novel logical networking scheme, novel networking protocol etc. |
| Deterministic delay and/or low latency | VQE, QAOA, QML, etc. | RDMA, self-adaptive and intelligent routing scheme and resource scheduling mechanism, TSN techniques in IEEE 802.1 AS etc. |
| High security and privacy | 2B service of QC, e.g., Finance, Medical, Aerospace etc. | Blockchain [b-Giovannetti-3], Differential Privacy (DP) [b-Hong], Homomorphic Encryption (HE) [b-Valencia], Federated Learning (FL) [b-Xie] etc. |
| Reliability or robustness | 2C service of QC, QC over scenario C (wide network), etc | high-efficient lossless data transferring technologies, quantum computing-aware routing and protection strategy etc. |

**Standardization considerations**

Emerging quantum (circuit) simulators over classical networks will support creative, cutting-edge research in science and engineering to uncover new paradigms, advance nascent hardware platforms and develop new algorithms and applications for a new generation of quantum simulators. This effort will further support the development of new materials and devices to help accelerate the progress of new technologies and push them out of the research laboratory.

**Others**

### I.2.5 UC-QC-005: Hybrid classical and quantum computing

**Use case 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, travelling salesperson problem. In addition, QAOA is also found to be helpful for solving the problems of linear equations and factoring problem.

Recently there have been some demos of the application of VQE, for example, the first experiment in photonic quantum processor [b-Peruzzo], the experiment to simulate larger systems [b-Kandala-1] and the chemical reaction [b-Arute]. There are also other methods that can be developed based on VQE, such as QAOA and QML. These methods can be used to solve different types of eigenvalue problems which are useful in science and common life.

Target end users for UC-QC-005 include 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.

Formatted: Highlight

Formatted: Font:

**Problem statement**

There are some typical computation problems which may run on classical quantum hybrid computing architecture such as quantum approximate optimization algorithm (QAOA) and variational quantum eigensolver (VQE).

**QAOA problem**

Combinatorial optimization problem is a subfield of mathematical optimization. It has important applications in several fields in the real world, including reducing the cost of supply chains, vehicle routing, job allocation and so on. Generally speaking, the task of combinatorial optimization is to find the object that minimizes the cost function from a limited number of objects.

QAOA is a variational quantum algorithm that promises to solve combinatorial optimization problems by a parameterized quantum circuit. It also has potential to solve linear equations and realize quantum machine learning. In a QAOA implementation, the expectation value of the objective Hamiltonian given by the parameterized circuit represents the objective function of the combinatorial problem and the goal of QAOA is to minimize this objective function via a classical optimizer. Classical computers can also play more roles in QAOA, such as recursive QAOA, adaptive QAOA, and optimizing parameters by machine learning, these approaches are expected to further improve the performance of the algorithm.

As a heuristic algorithm the advantages of QAOA are still uncertain. Therefore, the algorithm performance research on large-scale problems may need to rely on distributed computing clusters over cloud environment.

**VQE problem**

One of the most important problems in science is the eigenvalue problem. For instance, if the ground state and corresponding energy are known in a molecular system, many useful properties can be derived to analyze the system since molecular systems are usually in the ground state. To calculate the ground state, many methods have been developed. However, for large systems over tens of electrons, these methods need so many computation resources that even the best supercomputer cannot give a result with enough accuracy.

Since quantum computation is developing fast these years, scientists are attempting to make use of quantum computers to simulate molecular systems and calculate the ground state energy. The VQE algorithm, which was recently proposed as a method to calculate the ground state energy of molecules, is a method believed to have exponential acceleration compared to classical methods and is believed suitable for the NISQ era.

There is a lot of research related to the development of VQE focusing on resolving these important problems: "*What is the most practical way to run the algorithm on real quantum hardware?*" and "*What problems can be solved by VQE efficiently recently?*".

**Technical considerations**

One of the most significant problems in quantum computing is how to demonstrate quantum supremacy. It is particularly important to achieve this goal by using existing quantum resources, i.e., the noisy intermediate scale quantum computer (NISQ). On the other hand, the combinatorial optimization problems have lots of applications, but most of them are NP hard problems. As the scale increases, finding their solutions will be beyond the ability of the classical computer and although adiabatic quantum algorithms have been proposed to tackle such problems, it is not on

NISQ algorithm. The variational gate-based quantum-classical hybrid algorithm (one of which is the QAOA) is the most promising method to demonstrate quantum supremacy on NISQ.

VQE has been tested in many experiments. Since present quantum hardware is not powerful enough to run VQE algorithm for large systems, it is important to make different adjustments based on the hardware condition. For example, the error in the quantum hardware is not negligible which requires practical error mitigation methods and the coherent time in the quantum hardware is currently short, thus needing careful design of the circuit structure.

In the framework of hybrid classical and quantum computing, as shown in Figure 18, the technologies of the classical part related to computation and networking are relatively mature whereas for the quantum computing part such as QRAM and quantum computer, further development is either still ongoing or have not yet been adopted at a large scale for application.

Formatted: Highlight

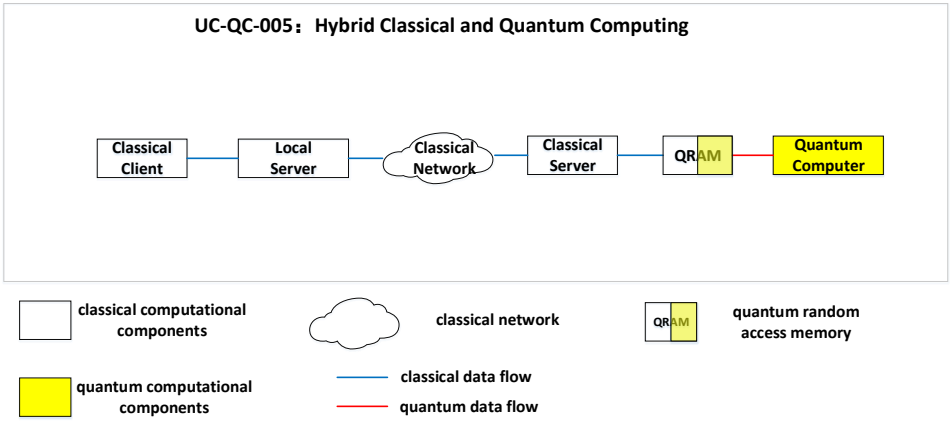



**Figure 18 – Networking and computation model of hybrid classical and quantum computing**

Formatted: Highlight

As for the algorithm and software parts, the VQE algorithm is based on the variation method. Basic steps of VQE include qubit encoding, mapping the operators, ansatz preparation, together with several techniques for improving the performance, including constraining, and error mitigation. There are many efforts dedicated towards improving the performance of VQE and some technical solutions include designing different ansatz for specific problems and hardware [b-Kandala-1], [b-Arute] and developing methods to deal with errors [b-Kandala-2].

Formatted: Highlight

Formatted: Highlight

Nowadays there are some applications of classical and quantum hybrid computing over classical communication networks which can be summarized into two types:

– **Type I**: user accessing the internet, pre-processing data in the local client and uploading the data and computing job to a remote quantum computing device which may pass through a wide area network. Typical applications are some QC services such as quantum annealing (QA) where classical computation is responsible for data processing in the user's local computer while quantum computation is designed for solving combinatorial optimization problems.

– **Type II**: distributed classical and quantum hybrid computing applications over local/wide area classical networks. e.g., algorithm applications such as VQE, QAOA, QML etc. working under schemes of classical training/measured/controlled data's feedback which needs classical and quantum computation working together.

In this report, some results analysis is provided aiming at two aspects, i.e., network latency and data reliability which may impact the quality of service utilizing classical and quantum hybrid computing over classical communication network.

**Type I application related to network latency and data reliability**

Taking the example illustrated in Figure 19 where users develop a traffic optimization application, some requirements for the Type I application are listed below:

– The system contains such essential software components as Component-1 (data import and demand mapping), Component-2 (solving combinatorial optimization problem) and Component-3 (visualization of results analysis)

– Users would expect to develop Component-2 under the service provided by real quantum computation infrastructure such as a QA device via the internet because of its computational advantage aiming to solve this problem for traffic optimization

– With consideration for software property rights and service protection, Component-1 and Component-3 are not allowed to be uploaded but are ran on a cloud platform

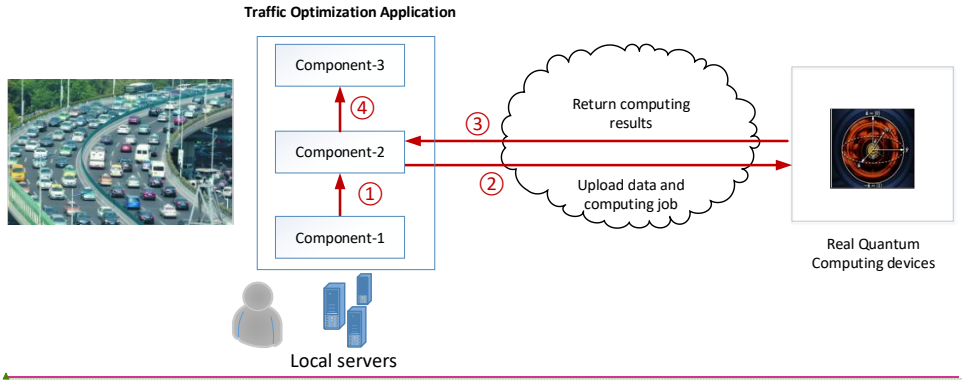



**Figure 19 – Type I application over classical networks**

Based on the analysis above, it is clear that the quantum computation in Component-2 and classical computation in Component-1 and Component-3 should work together to provide an integral service for the traffic optimization application.

As illustrated in Figure 19, datasets are pre-processed in the user's local computer and uploaded to the server or platform equipped with real quantum computing devices, then computing results are returned to users over classical networks. For example, when designing a QA algorithm to solve the optimization and combination problem, data may first be formulated as quadratic unconstrained binary optimization (QUBO) or Ising model with some classical operation and then the model uploaded to the remote real quantum device to finish the QA process. It is noted that this application requires only one ping-pong communication over classical networks.

The impact analysis of the QC service with respect to network latency and data reliability is thus:

– **Impact of network latency for QC service:** The uploaded data, computation job and returned results may transfer over a wide area network thus the user may have to wait for long time to receive the results and have difficulty estimating the completion time for the whole process. Although the execution speed of quantum computing is very fast, the long delay leads to a decline in competitiveness with classical computing.

Formatted: Highlight

Field Code Changed

Formatted: Highlight

Formatted: Highlight

– **Impact of data reliability for QC service:** Data loss is likely to cause the failure of quantum computing tasks, especially in the case of large amounts of dataset uploading, which seriously affects the user experience. In this case, huge amounts of burst data may pour into wide area networks which bring great challenges to networking technology such as flow control, routing, scheduling etc. to guarantee low or determinate latency and big data reliability.

**Type II application related to network latency and data reliability**

Some machine learning (ML) applications are sensitive to users' data and as illustrated in Figure 20, federated machine learning (FML) introduced in [b-IEEE P3652.1] shows a distributed computation framework where data from different owners is prohibited to move out of local nodes so that the ML model is trained or inferred across classical networks to make a double-win for data privacy and ML implementation.

Formatted: Highlight

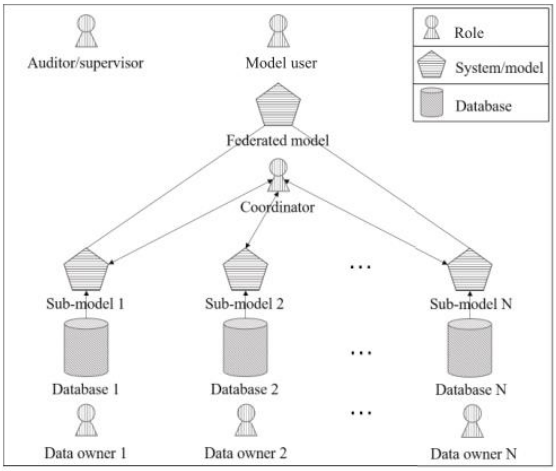
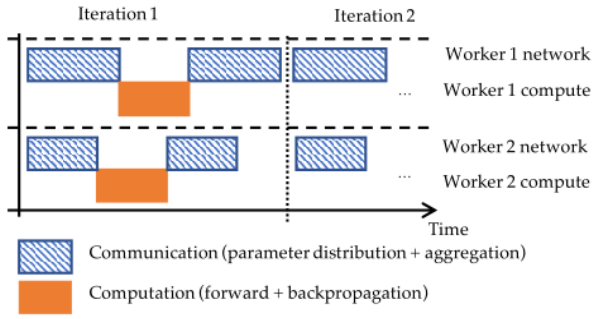



**Figure 20 – A schematic diagram of FML framework introduced in [b-IEEE P3652.1]**

Formatted: Highlight

One consideration for introducing quantum computation in FML is that encryption and decryption of the ML model and data unavoidably brings a huge computational overhead. For example, holomorphic encryption (HE) employed in FML produces at least 100 times more computation than original distributed machine learning (DML). Quantum computation can accelerate the speed of computation for encryption and decryption during the pipeline of FML. The hybrid computation solution can promote the quality of service for DML/FML.

Taking the example of DML applications, synchronized distributed training is often used to handle huge datasets. In the distributed training process, multiple worker nodes train the same model. In each iteration, workers fetch the current parameters of the models, train the model locally and exchange their results to update a global model, as Figure 21 shows.




**NOTE:** Common pattern of distributed ML jobs. Workers need to wait for other workers to finish the current iteration before starting the next iteration.

**Figure 21 – DML jobs of applications over distributed workers in networks [b-Xia]**

The major content in communication in DML can be viewed as a vector of floating-point numbers describing the model. In contrast to the workflow of type I, the pipeline here needs several iterations to finish training the model with distributed computing over classical networks.

The impact against QC service with respect to network latency and data reliability is thus:

– **Impact of network latency for QC service:** To keep workers' model up to date, the model is synced in every iteration. At the beginning and end of each iteration, multiple flows are generated almost simultaneously to exchange data among workers, generating burst network traffic. Meanwhile, many ML models are trained under strong synchronization requirements, i.e., *all workers need to update their parameters prior to starting next iteration*. Therefore, the performance is determined by the tail completion time of all the flows in one iteration.

– **Impact of data reliability for QC service:** Data loss is likely to reduce the efficiency of convergence during training models. In Figure 21, it is shown that with the increasing of random data loss probability, convergence of the model also needs to be more rounded.

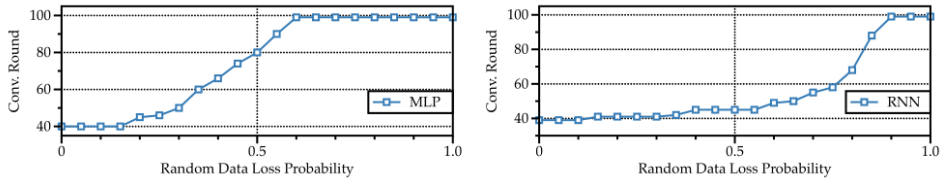



*Figure 22 – Impact of data loss on convergence for DML [b-IEEE P3652.1]*

Existing ML frameworks rely on existing protocols like TCP or UDP to transmit messages. TCP and its variants seek to minimize the time to transfer all data which inevitably suffers from tail latency even under a tiny fraction of packet delays/losses. UDP, on the other hand, tolerates the tail effect but without the guarantee that at least a certain part of data must be delivered, and this can result in poor eventual accuracy and/or require more iterations to converge.

Field Code Changed

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

There are some opening technical solutions for distributed computing as below:

– **Reducing tail latency:** Several research efforts on data centre network areas have been proposed to reduce the tail latency. Pfabric [b-Alizadeh-1] and cutting payload [b-Cheng] optimizes tail latency with fast detection of lost packets. While these methods are effective, they require changes to the switch hardware. TCP based schemes like DCTCP [b-Alizadeh-2] generally improve latency, but they have no guarantee on the worst-case performance.

– **Loss tolerance transport layer protocol:** Some protocols for real-time streaming applications tolerate packet loss, e.g., RTCP [b-Huitema]. However, related applications do not have a strong tolerance bound as ML application does. It remains to be explored whether a dynamic loss tolerance similar to the quality of service (QoS) concept is applicable to DML jobs. Some QC-aware and motivated technical solutions enabled by classical networks are still encouraged to be studied further to improve the quality of QC service.

**Standardization considerations**

Even at the lowest circuit depth, QAOA offers non-trivial provable performance which is expected to increase with the circuit depth. The QAOA has been proved to be a noise tolerant algorithm. Only with simple quantum circuit structure can QAOA be implemented on NISQ hardware. Therefore, QAOA is a promising quantum algorithm for supporting the quantum supremacy.

The VQE scheme can be applied to solve many kinds of ground state energy problems, and, in the near future, it can be widely used to help chemical synthesis, material designing, drug searching and even road planning, etc. Many calculations that are difficult now may be easily solved with the help of a quantum computer.

**Others**

Formatted: Font:

## I.4 Quantum communication use cases beyond QKD

This clause presents quantum communication tasks that will be available at later stages of developments of quantum networks. These stages of developments are characterized by the availability of hardware such as quantum repeaters, quantum memories or entanglement distribution [b-Wehner]. The tasks introduced in this section then become available, with these pieces of hardware added to the quantum network equipment.

The following quantum communication use cases are considered in this technical report:

– **UC-QCOM-001:** Quantum digital signatures
– **UC-QCOM-002:** Quantum anonymous transmission
– **UC-QCOM-003:** Quantum money

### I.4.1 UC-QCOM-001: Quantum digital signatures

**Use case description**

Digital signatures allow the exchange of digital messages from a sender to multiple recipients, with a guarantee that the signature comes from a genuine sender. This can be used to authenticate the sender of a message.

The security of quantum digital signatures (QDS) relies on *transferability* (a signature can be transferred to a third party), *non-repudiation* (same as classical) and *unforgeability* (a signature cannot be forged by a third party). QDS are used to sign classical messages but not quantum messages.

Quantum digital signatures can be made unconditionally secure which ensures long-term security and quantum resistance. The security requires the pre-distribution of keys amongst the participants of the protocol. With no prior agreement, the sender could repudiate its messages. In particular, preventing the tampering of a message by the sender after it was signed reduces to the security of bit commitment, a task that cannot be achieved with unconditional security, even using quantum resources [b-Lo].

Classically, digital signatures often rely on public key infrastructures. In the quantum case, more advanced resources are usually involved, such as a trusted key distribution centre. This distribution phase is a strong requirement which mitigates the advantage of unconditional security.

**Problem statement**

None.

**Technical considerations**

The requirements of quantum digital signatures protocol have been decreased by a series of work following the research of [b-Gottesman]. The original protocol assumed non-destructive state comparison and a secure quantum channel; however, these assumptions have now been refuted to assume only a long-time quantum memory [b-Amiri]. Less efficient protocols exist that only require prepare-and-measure operations which are available in QKD networks. These protocols typically require sending very long qubit strings for signing a single bit of information. Nevertheless, they can be implemented with current technology at a small scale or using quantum repeater to reach long distances. End-to-end security and distribution to arbitrary distant parties nevertheless require the use of quantum repeaters.

**Standardization considerations**

Quantum digital signatures could be used for authenticating network nodes. New threat models appear with the growing number of devices connected to internet, and in particular the increase of IoT. QDS could be useful for critical IoT devices in industries such as transport, maritime, oil and gas, mining or agriculture, in which updating keys can be difficult. Quantum digital signatures are bringing long-term security to the security of such devices, ensuring that their signatures cannot be counterfeited, regardless of the time these devices remain in use.

Beyond device identification, digital signatures can also be used to guarantee the integrity of stored data. The unforgeability of the signature ensures that the data is stored by a legitimate party and checking the signature guarantees they have not been altered. The quantum benefit is to maintain this guarantee for a long time.

**Others**

### I.4.2 UC-QCOM-002: Quantum anonymous transmission

**Use case 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. In particular, 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 their identity. The main goal of anonymous transmission is to fully hide the identities of the sender and the receiver but does guarantee the reliability of the transmitted message.

Several classical protocols for anonymous transmission have been proposed since the late 1980s. The most widely spread practical solutions are proxy anonymizers, which are based on trusted third parties, and networks based on computationally secure problems and a chain of forwarding. Famous examples of the latter include MixMaster, PipeNet, OnionRouting and its best-known implementation, Tor.

Quantum protocols for anonymous transmission are traceless, i.e., the sender cannot be reconstructed afterwards; they do not rely on a trusted third party nor use computational assumptions. Moreover, they seem well-suited for small scale infrastructures since they do not require using a chain of servers, unlike the protocols based on chains of forwarding.

**Problem statement**

None.

**Technical considerations**

Various protocols for quantum anonymous transmission have been introduced which differ in the hardware they require. State of the art protocols can be implemented by distributing large, entangled states [b-Lipinska] and [b-Unnikrishnan]. Progress on the generation and distribution of entangled states may allow scaling quantum anonymous transmission to a larger number of parties.

**Standardization considerations**

Formatted: Font:

Anonymous transmission allows quantum distributed computation to be performed without revealing the identity of the agent that provides the information. It is therefore useful in cases where data from various sources must be aggregated while hiding the identity of the agents providing the data. This is a simplified version of secure-multiparty computing which aims at hiding all information that cannot be deduced from the output of the computation.

For example, monitoring car traffic can lead to a better road management. Drivers, however, might not be willing to share their private information, in particular regarding their speed and position. Quantum anonymous transmission could be used to hide the drivers' identities while collecting valuable data.

Anonymous transmission can be used to design applications that are private by design. This could be interesting to develop GDPR-compliant applications and more generally for the protection of free speech or whistle-blowers. This can be useful for international institutions to enforce human rights by design.

**Others**

# 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.

To select related use cases, the following table has been made to show use cases in the FG-QIT4N deliverable D1.2 (Appendix of TR-QC-UC) and related SG.

| Use cases | Related SG |
|---|---|
| I.1 Quantum time synchronization use cases | |
| I.1.1 Quantum time synchronization in telecommunications | SG13, SG15 |
| I.1.2 Secure quantum clock synchronization | SG13, SG15 |
| I.1.3 A quantum network of entangled clocks | SG13, SG15 |
| I.2 Quantum computing use cases | |
| I.2.1 Quantum cloud computing | SG13 |
| I.2.2 Distributed quantum computing | SG13 |
| I.2.3 Blind quantum computing | SG13 |
| I.2.4 Quantum simulator in centralized/distributed quantum computing | SG13 |
| I.2.5 Hybrid classical and quantum computing | SG13 |
| I.3 Quantum random number generator use cases | |
| I.3.1 Quantum randomness beacon service for smart contract | SG17 |
| I.3.2 Quantum randomness beacon service for confidential disclosure | SG17 |
| I.4 Quantum communications use cases | |
| I.4.1 Quantum digital signatures | SG13, SG17 |
| I.4.2 Quantum anonymous transmission | SG13 |
| I.4.3 Quantum money | TBD |

## 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

[b-Denchev] Denchev, V.S. and et. al., "Distributed Quantum Computing: A New Frontier in Distributed Systems or Science Fiction?", SIGACT News ACM, 2018, <https://doi.org/10.1145/1412700.1412718>.

_____