Draft new Technical Report ITU-T TR.QN-UC

Use cases of quantum networks beyond QKDN

Summary

This Technical Report analyses use cases of quantum networks beyond quantum key distribution network (QKDN) 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 problem statement, technical considerations along with a short description of each use case. This Technical Report also provides analyses for future applications and potential standardization considerations.

Keywords

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

Table of Contents

Page

1 Scope ... 3

2 References ... 3

3 Definitions ... 3

3.1 Terms defined elsewhere ... 3

3.2 Terms defined in this Technical Report ... 3

4 Abbreviations and acronyms ... 3

5 Introduction ... 4

6 Use cases ... 5

6.1 Quantum time synchronization use cases ... 5

6.1.1 UC-QTS-001: Quantum time synchronization in telecommunications ... 5

6.1.2 UC-QTS-002: Secure quantum clock synchronization ... 6

6.1.3 UC-QTS-003: A quantum network of entangled clocks ... 7

6.2 Quantum computing use cases ... 8

6.2.1 UC-QC-001: Quantum cloud computing ... 8

6.2.2 UC-QC-002: Distributed quantum computing ... 9

6.2.3 UC-QC-003: Blind quantum computing ... 11

6.2.4 UC-QC-004: Quantum simulator in centralized/distributed quantum computing ... 12

6.2.5 UC-QC-005: Hybrid classical and quantum computing 14
6.3 Quantum communication use cases beyond QKD 17
6.3.1 UC-QCOM-001: Quantum digital signatures 17
6.3.2 UC-QCOM-002: Quantum anonymous transmission 18

Appendix I Overview of use cases 20
I.1 Quantum time synchronization use cases 21
I.1.1 Quantum time synchronization in telecommunications 21
I.1.2 Secure quantum clock synchronization 21
I.1.3 A quantum network of entangled clocks 21
I.2 Quantum computing use cases 22
I.2.1 Quantum cloud computing 22
I.2.2 Distributed quantum computing 22
I.2.3 Blind quantum computing 22
1.2.4 Quantum simulator in centralized/distributed quantum computing 23
1.2.5 Hybrid classical and quantum computing 23
I.3 Quantum random number generator use cases 23
I.3.1 Quantum randomness beacon service for smart contract 23
I.3.2 Quantum randomness beacon service for confidential disclosure 23
I.4 Quantum communications use cases 23
I.4.1 Quantum digital signatures 24
I.4.2 Quantum anonymous transmission 24

Bibliography 25

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 quantum key distribution network (QKDN) under four categories as follows:

- Quantum time synchronization use cases;
- Quantum computing use cases;
- Quantum random number generator use cases;
- Quantum communication use cases beyond QKD.

In particular, the content of this Technical Report presents 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

[FG QIT4N D1.2] ITU-T FG QIT4N (2022), *Quantum information technology for networks use cases: Network aspects of quantum information technologies.*

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses QIT-related terms in [b-QIT4N D1.1].

3.2 Terms defined in this Technical Report

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BIPM	Bureau International des Poids et Mesures
BQC	Blind Quantum Computing
DIQRNG	Device Independent Quantum Random Number Generator
DML	Distributed Machine Learning
DQC	Distributed Quantum Computing
EC	Entangled Clock
ELS	Entanglement Light Source
IoT	Internet of Things
PTP	Point to Point
QAOA	Quantum Approximate Optimization Algorithm
QC	Quantum Computing

QCC	Quantum Cloud Computing
QIN	Quantum Information Network
QIT	Quantum Information Technology
QML	Quantum Machine Learning
QND	Quantum Non Demolition
QRNG	Quantum Random Number Generator
QTS	Quantum Time Synchronization
QTSI	Quantum Time Synchronization Information
QTSN	Quantum Time Synchronization Network
Qubit	Quantum bit
RDMA	Remote Direct Memory Access
SPDC	Spontaneous Parameter Down Conversion
SQL	Standard Quantum Limit
TAI	International atomic time
UC	Use Case
VQA	Variation Quantum Algorithm
VQE	Variation Quantum Eigen solver

5 Introduction

This Technical Report elaborates on use cases of quantum networks beyond QKDN, from the use cases of the network aspects of QIT.

The use cases described in this Technical 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.

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

6 Use cases

6.1 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 Quantum time synchronization in telecommunications** 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 Secure quantum clock synchronization** describes the applicability of quantum technology in resisting security attacks in synchronous networks.
- **UC-QTS-003 A quantum network of entangled clocks** 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.

6.1.1 UC-QTS-001: Quantum time synchronization in telecommunications

- **Use case ID**: UC-QTS-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:** 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.

6.1.2 UC-QTS-002: Secure quantum clock synchronization

- **Use case ID**: UC-QTS-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, the specific constraint standards of dynamic scenarios could be considered.

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

6.1.3 UC-QTS-003: A quantum network of entangled clocks

- **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.

6.2 Quantum computing use cases

The quantum computing use cases described in this Technical Report are focused on the application and method of quantum computing, each with different requirements and features as shown in Table 1.

Table 1 – 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.

6.2.1 UC-QC-001: Quantum cloud computing

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

- **Use case description**

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.

- **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**

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 1. 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.

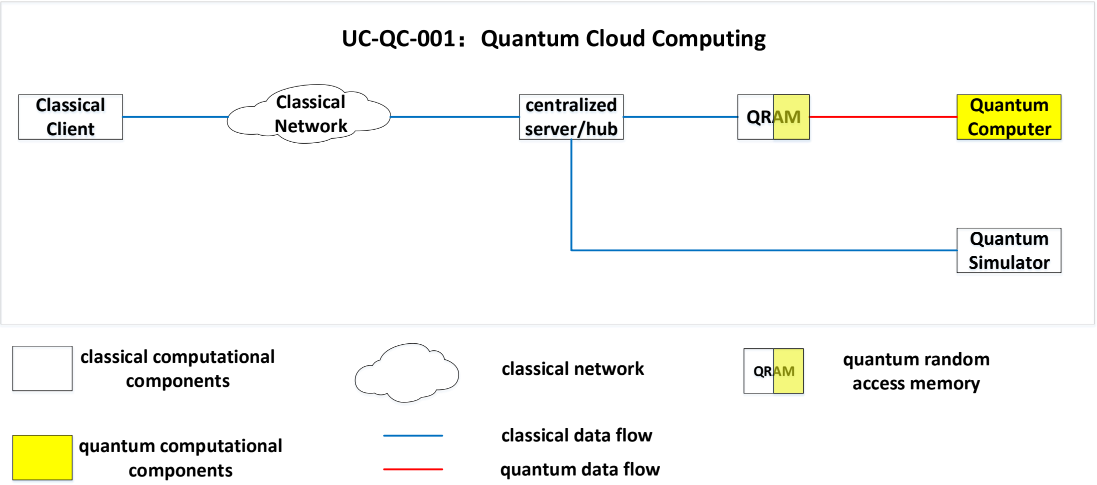

Figure 1 – Networking and computation model of quantum cloud computing

- **Standardization considerations**

For example Quantum programming languages and interface standards could be considered. Define standard programming languages and interfaces for writing and performing quantum computing tasks to ensure interoperability between quantum cloud computing platforms from different vendors.

- **Others**

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

6.2.2 UC-QC-002: Distributed quantum computing

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

- **Use case description**

Similar to UC-QC-001, distributed quantum computing (DQC) 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.

- **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**

DQC is a technology based on networks of distributed quantum chips that allow computational power multiplications of individual quantum devices, see Figure 2.

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.

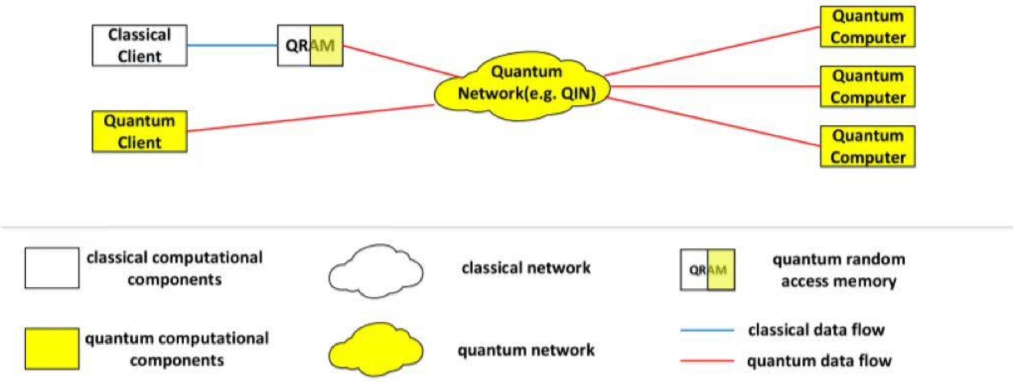

Figure 2 – Networking and computation model of distributed quantum computing

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.

- **Standardization considerations**

It could include quantum computing task distribution standards, as well as node communication and data transfer standards.

- **Others**

As shown in Figure 3, 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. 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.

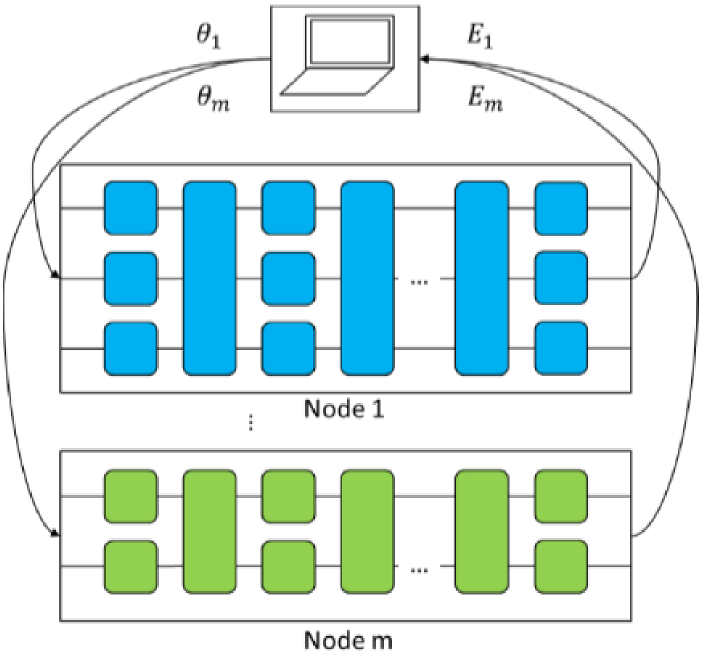

Figure 3 – An application of quantum computing on distributed networks

6.2.3 UC-QC-003: Blind quantum computing

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

- **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.

- **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.

As shown in Figure 4, 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.

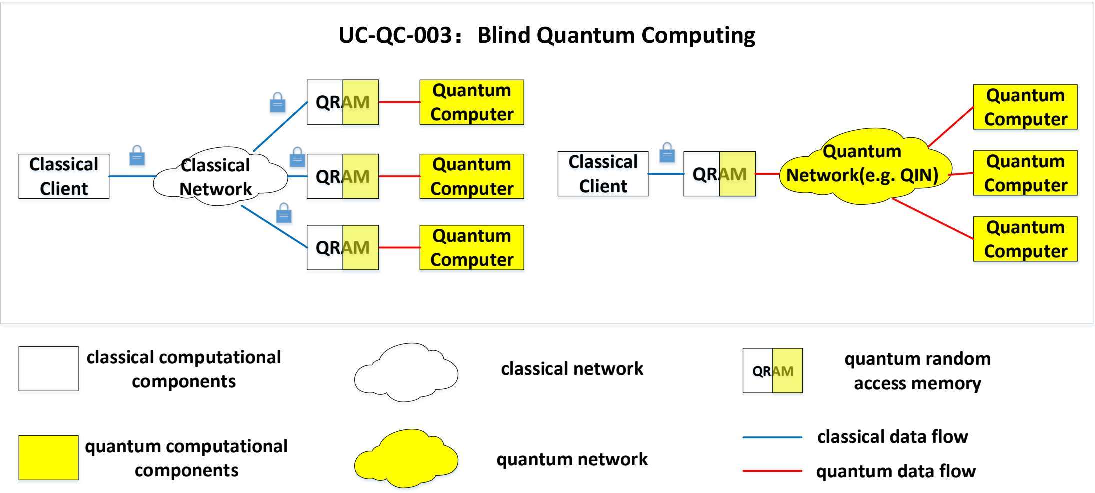

Figure 4 – Networking and computation model of blind quantum computing

- **Standardization considerations**

Standardization schemes for communication and protocols can be considered, as well as standards for encryption.

- **Others**

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.

6.2.4 UC-QC-004: Quantum simulator in centralized/distributed quantum computing

- **Use case ID**: UC-QC-004.

- **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 . 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 5, 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.

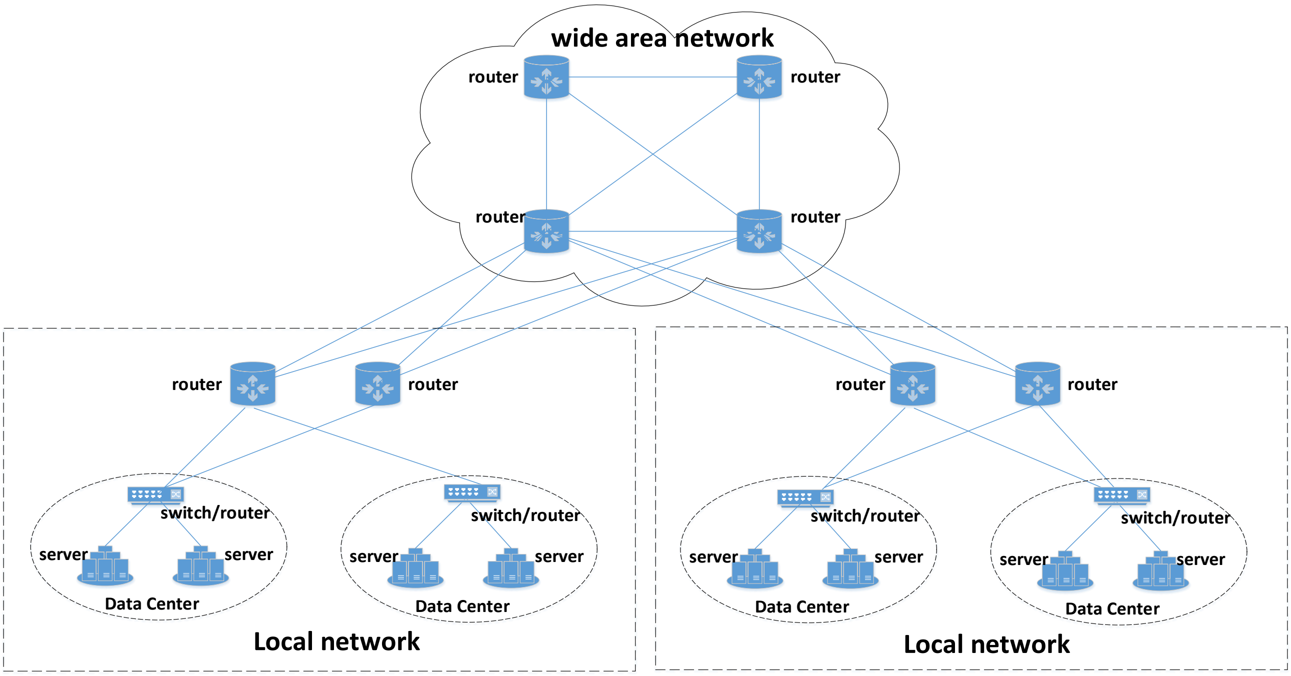

Figure 5 – Typical network scenario of computation clusters over classical networks

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.

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

- **Standardization considerations**

Ssecurity standards as well as interoperability standards could be considered. Ensuring that hardware and software from different vendors can interoperate is a key issue. Interoperability standards ensure that different components can work together within an ecosystem.

- **Others**

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.

6.2.5 UC-QC-005: Hybrid classical and quantum computing

- **Use case ID**: UC-QC-005.

- **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.

- **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 6,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.

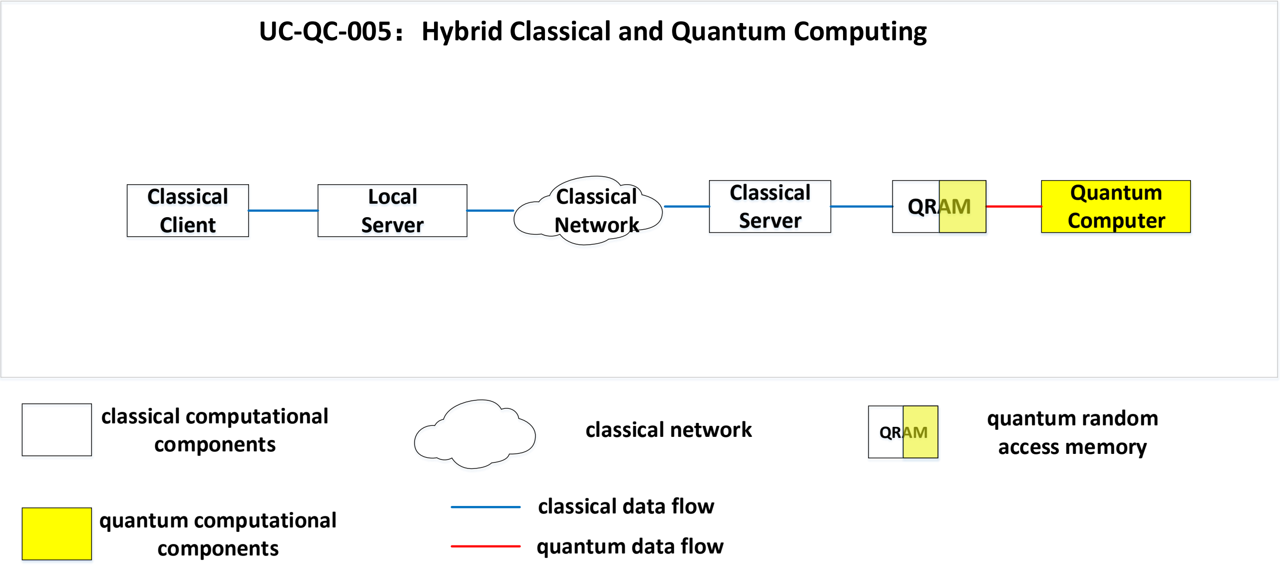
UC-QC-005：Hybrid Classical and Quantum Computing
Classical Client
Local Server
Classical Network
Classical Server
QRAM
Quantum Computer
classical computational components
classical network
QRAM
quantum random access memory
quantum computational components
classical data flow
quantum data flow

Figure 6 – Networking and computation model of hybrid classical and quantum computing

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.

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.

- **Standardization considerations**

A quantum instruction set architecture (QISA) will be needed. It is similar to the instruction set architecture of classical computers, and quantum computers also need a standard instruction set so that classical computers can send commands and instructions to quantum processors.

- **Others**

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.

6.3 Quantum communication use cases beyond QKD

This section 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

6.3.1 UC-QCOM-001: Quantum digital signatures

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

- **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.

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**

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.

- **Technical considerations**

The requirements of quantum digital signatures protocol have been decreased by a series of work. 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**

The performance and efficiency of Quantum digital signatures algorithms need to be considered to ensure that they will operate effectively in real-world applications. This includes considerations such as the speed of signature and verification, the computing and storage resources required, and so on.

- **Others**

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.

6.3.2 UC-QCOM-002: Quantum anonymous transmission

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

- **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.

- **Problem statement**

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.

- **Technical considerations**

Various protocols for quantum anonymous transmission have been introduced which differ in the hardware they require. Progress on the generation and distribution of entangled states may allow scaling quantum anonymous transmission to a larger number of parties.

- **Standardization considerations**

Protecting the security of the transmitted data is a key element of anonymous transmission. Therefore, the algorithms and protocols used to encrypt and decrypt quantum communication data need to be standardized to ensure the confidentiality of communications.

- **Others**

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. 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.

Appendix I

Overview of use cases

To select related use cases, the following table has been made to show use cases 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.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.

Bibliography

[b-QIT4N D1.1] Deliverable FG-QIT4N D1.1 (2021), *Quantum information technology for networks terminology: Network aspects of quantum information technologies.*

[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>.

[b-Morimae-1] Morimae, T. and Fujii, K. (2012), *Blind Quantum computation protocol in which Alice only makes measurements*. Physical Review A, Vol. 87, No. 5.

[b-Morimae-2] Morimae, T. and Fujii, K. (2013), *Secure entanglement distillation for double-server blind quantum computations*. Physical Review Letters Vol.111, No. 2, pp. 47-89.

[b-Sheng] Sheng, Y. B. and Zhou, L. (2015), *Deterministic entanglement distillation for double-server blind quantum computations*. Scientific Reports, Vol. 5, No. 7815.

[b-Li] Li, Q., Chan, W. H., Wu, C. and Wen, Z. (2014), *Triple-server blind quantum computation using entanglement swapping*. Physical Review A, Vol. 89, No. 4, pp. 2748-2753

[b-Wehner] Wehner, S., Elkouss, D. and Hanson, R. (2018), *Quantum internet: A vision for the road ahead*, Science, Vol. 362, No. 16412.

[b-Amiri] Amiri, R. and Andersson, E. (2015), *Unconditionally Secure Quantum Signatures*, Entropy, Vol. 17, No. 18, pp. 5635-5659.