Internet Research Task Force (IRTF)
Request for Comments: 9340
Category: Informational
ISSN: 2070-1721

W. Kozlowski
S. Wehner
QuTech
R. Van Meter
Keio University
B. Rijsman
Individual
A. S. Cacciapuoti
M. Caleffi
University of Naples Federico II
S. Nagayama
Mercari, Inc.

March 2023

Architectural Principles for a Quantum Internet

Abstract

The vision of a quantum internet is to enhance existing Internet technology by enabling quantum communication between any two points on Earth. To achieve this goal, a quantum network stack should be built from the ground up to account for the fundamentally new properties of quantum entanglement. The first quantum entanglement networks have been realised, but there is no practical proposal for how to organise, utilise, and manage such networks. In this document, we attempt to lay down the framework and introduce some basic architectural principles for a quantum internet. This is intended for general guidance and general interest. It is also intended to provide a foundation for discussion between physicists and network specialists. This document is a product of the Quantum Internet Research Group (QIRG).

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Research Task Force (IRTF). The IRTF publishes the results of Internet-related research and development activities. These results might not be suitable for deployment. This RFC represents the consensus of the Quantum Internet Research Group of the Internet Research Task Force (IRTF). Documents approved for publication by the IRSG are not candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9340.

Table of Contents

1. Introduction

Quantum networks are distributed systems of quantum devices that utilise fundamental quantum mechanical phenomena such as superposition, entanglement, and quantum measurement to achieve capabilities beyond what is possible with non-quantum (classical) networks [Kimble08]. Depending on the stage of a quantum network

[Wehner18], such devices may range from simple photonic devices capable of preparing and measuring only one quantum bit (qubit) at a time all the way to large-scale quantum computers of the future. A quantum network is not meant to replace classical networks but rather to form an overall hybrid classical-quantum network supporting new capabilities that are otherwise impossible to realise [VanMeterBook]. For example, the most well-known application of quantum communication, Quantum Key Distribution (QKD) [QKD], can create and distribute a pair of symmetric encryption keys in such a way that the security of the entire process relies on the laws of physics (and thus can be mathematically proven to be unbreakable) rather than the intractability of certain mathematical problems [Bennett14] [Ekert91]. Small networks capable of QKD have even already been deployed at short (roughly 100-kilometre) distances [Elliott03] [Peev09] [Aguado19] [Joshi20].

The quantum networking paradigm also offers promise for a range of new applications beyond quantum cryptography, such as distributed quantum computation [Cirac99] [Crepeau02]; secure quantum computing in the cloud [Fitzsimons17]; quantum-enhanced measurement networks [Giovannetti04]; or higher-precision, long-baseline telescopes [Gottesman12]. These applications are much more demanding than QKD, and networks capable of executing them are in their infancy. The first fully quantum, multinode network capable of sending, receiving, and manipulating distributed quantum information has only recently been realised [Pompili21.1].

Whilst a lot of effort has gone into physically realising and connecting such devices, and making improvements to their speed and error tolerance, no proposals for how to run these networks have been worked out at the time of this writing. To draw an analogy with a classical network, we are at a stage where we can start to physically connect our devices and send data, but all sending, receiving, buffer management, connection synchronisation, and so on must be managed by the application directly by using low-level, custom-built, and hardware-specific interfaces, rather than being managed by a network stack that exposes a convenient high-level interface, such as sockets. Only recently was the first-ever attempt at such a network stack experimentally demonstrated in a laboratory setting [Pompili21.2]. Furthermore, whilst physical mechanisms for transmitting quantum information exist, there are no robust protocols for managing such transmissions.

This document, produced by the Quantum Internet Research Group (QIRG), introduces quantum networks and presents general guidelines for the design and construction of such networks. Overall, it is intended as an introduction to the subject for network engineers and researchers. It should not be considered as a conclusive statement on how quantum networks should or will be implemented. This document was discussed on the QIRG mailing list and several IETF meetings. It represents the consensus of the QIRG members, of both experts in the subject matter (from the quantum and networking domains) and newcomers who are the target audience.

2. Quantum Information

In order to understand the framework for quantum networking, a basic understanding of quantum information theory is necessary. The following sections aim to introduce the minimum amount of knowledge necessary to understand the principles of operation of a quantum network. This exposition was written with a classical networking audience in mind. It is assumed that the reader has never before been exposed to any quantum physics. We refer the reader to [SutorBook] and [NielsenChuang] for an in-depth introduction to quantum information systems.

2.1. Quantum State

A quantum mechanical system is described by its quantum state. A quantum state is an abstract object that provides a complete description of the system at that particular moment. When combined with the rules of the system's evolution in time, such as a quantum circuit, it also then provides a complete description of the system at all times. For the purposes of computing and networking, the classical equivalent of a quantum state would be a string or stream of logical bit values. These bits provide a complete description of what values we can read out from that string at that particular moment, and when combined with its rules for evolution in time, such as a logical circuit, we will also know its value at any other time.

Just like a single classical bit, a quantum mechanical system can be simple and consist of a single particle, e.g., an atom or a photon of light. In this case, the quantum state provides the complete description of that one particle. Similarly, just like a string of bits consists of multiple bits, a single quantum state can be used to also describe an ensemble of many particles. However, because quantum states are governed by the laws of quantum mechanics, their behaviour is significantly different to that of a string of bits. In this section, we will summarise the key concepts to understand these differences. We will then explain their consequences for networking in the rest of this document.

2.2. Qubit

The differences between quantum computation and classical computation begin at the bit level. A classical computer operates on the binary alphabet { 0, 1 }. A quantum bit, called a qubit, exists over the same binary space, but unlike the classical bit, its state can exist in a superposition of the two possibilities:

$$|\text{qubit}\rangle = a\,|0\rangle + b\,|1\rangle,$$

where $|X\rangle$ is Dirac's ket notation for a quantum state (the value that a qubit holds) -- here, the binary 0 and 1 -- and the coefficients a and b are complex numbers called probability amplitudes. Physically, such a state can be realised using a variety of different technologies such as electron spin, photon polarisation, atomic energy levels, and so on.

Upon measurement, the qubit loses its superposition and irreversibly collapses into one of the two basis states, either $|0\rangle$ or $|1\rangle$. Which of the two states it ends up in may not be deterministic but can be

determined from the readout of the measurement. The measurement result is a classical bit, 0 or 1, corresponding to |0⟩ and |1⟩, respectively. The probability of measuring the state in the |0⟩ state is |a|^2; similarly, the probability of measuring the state in the |1⟩ state is |b|^2, where |a|^2 + |b|^2 = 1. This randomness is not due to our ignorance of the underlying mechanisms but rather is a fundamental feature of a quantum mechanical system [Aspect81].

The superposition property plays an important role in fundamental gate operations on qubits. Since a qubit can exist in a superposition of its basis states, the elementary quantum gates are able to act on all states of the superposition at the same time. For example, consider the NOT gate:

NOT (a |0⟩ + b |1⟩) → a |1⟩ + b |0⟩.

It is important to note that "qubit" can have two meanings. In the first meaning, "qubit" refers to a physical quantum *system* whose quantum state can be expressed as a superposition of two basis states, which we often label |0⟩ and |1⟩. Here, "qubit" refers to a physical implementation akin to what a flip-flop, switch, voltage, or current would be for a classical bit. In the second meaning, "qubit" refers to the abstract quantum *state* of a quantum system with such two basis states. In this case, the meaning of "qubit" is akin to the logical value of a bit, from classical computing, i.e., "logical 0" or "logical 1". The two concepts are related, because a physical "qubit" (first meaning) can be used to store the abstract "qubit" (second meaning). Both meanings are used interchangeably in literature, and the meaning is generally clear from the context.

2.3. Multiple Qubits

When multiple qubits are combined in a single quantum state, the space of possible states grows exponentially and all these states can coexist in a superposition. For example, the general form of a two-qubit register is

a |00⟩ + b |01⟩ + c |10⟩ + d |11⟩,

where the coefficients have the same probability amplitude interpretation as for the single-qubit state. Each state represents a possible outcome of a measurement of the two-qubit register. For example, |01⟩ denotes a state in which the first qubit is in the state |0⟩ and the second is in the state |1⟩.

Performing single-qubit gates affects the relevant qubit in each of the superposition states. Similarly, two-qubit gates also act on all the relevant superposition states, but their outcome is far more interesting.

Consider a two-qubit register where the first qubit is in the superposed state (|0⟩ + |1⟩)/sqrt(2) and the other is in the state |0⟩. This combined state can be written as

(|0⟩ + |1⟩)/sqrt(2) x |0⟩ = (|00⟩ + |10⟩)/sqrt(2),

where x denotes a tensor product (the mathematical mechanism for combining quantum states together).

The constant 1/sqrt(2) is called the normalisation factor and reflects the fact that the probabilities of measuring either a |0⟩ or a |1⟩ for the first qubit add up to one.

Let us now consider the two-qubit Controlled NOT, or CNOT, gate. The CNOT gate takes as input two qubits -- a control and a target -- and applies the NOT gate to the target if the control qubit is set. The truth table looks like

IN	OUT
00	00
01	01
10	11
11	10

Table 1: CNOT Truth Table

Now, consider performing a CNOT gate on the state with the first qubit being the control. We apply a two-qubit gate on all the superposition states:

CNOT (|00⟩ + |10⟩)/sqrt(2) → (|00⟩ + |11⟩)/sqrt(2).

What is so interesting about this two-qubit gate operation? The final state is *entangled*. There is no possible way of representing that quantum state as a product of two individual qubits; they are no longer independent. That is, it is not possible to describe the quantum state of either of the individual qubits in a way that is independent of the other qubit. Only the quantum state of the system that consists of both qubits provides a physically complete description of the two-qubit system. The states of the two individual qubits are now correlated beyond what is possible to achieve classically. Neither qubit is in a definite |0⟩ or |1⟩ state, but if we perform a measurement on either one, the outcome of the partner qubit will *always* yield the exact same outcome. The final state, whether it's |00⟩ or |11⟩, is fundamentally random as before, but the states of the two qubits following a measurement will always be identical. One can think of this as flipping two coins, but both coins always land on "heads" or both land on "tails" together -- something that we know is impossible classically.

Once a measurement is performed, the two qubits are once again independent. The final state is either |00⟩ or |11⟩, and both of these states can be trivially decomposed into a product of two individual qubits. The entanglement has been consumed, and the entangled state must be prepared again.

3. Entanglement as the Fundamental Resource

Entanglement is the fundamental building block of quantum networks. Consider the state from the previous section:

(|00⟩ + |11⟩)/sqrt(2).

Neither of the two qubits is in a definite |0⟩ or |1⟩ state, and we need to know the state of the entire register to be able to fully describe the behaviour of the two qubits.

Entangled qubits have interesting non-local properties. Consider sending one of the qubits to another device. This device could in principle be anywhere: on the other side of the room, in a different country, or even on a different planet. Provided negligible noise has been introduced, the two qubits will forever remain in the entangled state until a measurement is performed. The physical distance does not matter at all for entanglement.

This lies at the heart of quantum networking, because it is possible to leverage the non-classical correlations provided by entanglement in order to design completely new types of application protocols that are not possible to achieve with just classical communication. Examples of such applications are quantum cryptography [Bennett14] [Ekert91], blind quantum computation [Fitzsimons17], or distributed quantum computation [Crepeau02].

Entanglement has two very special features from which one can derive some intuition about the types of applications enabled by a quantum network.

The first stems from the fact that entanglement enables stronger-than-classical correlations, leading to opportunities for tasks that require coordination. As a trivial example, consider the problem of consensus between two nodes who want to agree on the value of a single bit. They can use the quantum network to prepare the state (|00⟩ + |11⟩)/sqrt(2) with each node holding one of the two qubits. Once either of the two nodes performs a measurement, the state of the two qubits collapses to either |00⟩ or |11⟩, so whilst the outcome is random and does not exist before measurement, the two nodes will always measure the same value. We can also build the more general multi-qubit state (|00...⟩ + |11...⟩)/sqrt(2) and perform the same algorithm between an arbitrary number of nodes. These stronger-than-classical correlations generalise to measurement schemes that are more complicated as well.

The second feature of entanglement is that it cannot be shared, in the sense that if two qubits are maximally entangled with each other, then it is physically impossible for these two qubits to also be entangled with a third qubit [Terhal04]. Hence, entanglement forms a sort of private and inherently untappable connection between two nodes once established.

Entanglement is created through local interactions between two qubits or as a product of the way the qubits were created (e.g., entangled photon pairs). To create a distributed entangled state, one can then

physically send one of the qubits to a remote node. It is also possible to directly entangle qubits that are physically separated, but this still requires local interactions between some other qubits that the separated qubits are initially entangled with. Therefore, it is the transmission of qubits that draws the line between a genuine quantum network and a collection of quantum computers connected over a classical network.

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

Services and applications that are more complex can be built on top of entangled states distributed by the network; for example, see [ZOO].

4. Achieving Quantum Connectivity

This section explains the meaning of quantum connectivity and the necessary physical processes at an abstract level.

4.1. Challenges

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

4.1.1. The Measurement Problem

In classical computers and networks, we can read out the bits stored in memory at any time. This is helpful for a variety of purposes such as copying, error detection and correction, and so on. This is not possible with qubits.

A measurement of a qubit's state will destroy its superposition and with it any entanglement it may have been part of. Once a qubit is being processed, it cannot be read out until a suitable point in the computation, determined by the protocol handling the qubit, has been reached. Therefore, we cannot use the same methods known from classical computing for the purposes of error detection and correction. Nevertheless, quantum error detection and correction schemes exist that take this problem into account, and how a network chooses to manage errors will have an impact on its architecture.

4.1.2. No-Cloning Theorem

Since directly reading the state of a qubit is not possible, one could ask if we can simply copy a qubit without looking at it. Unfortunately, this is fundamentally not possible in quantum mechanics [Park70] [Wootters82].

The no-cloning theorem states that it is impossible to create an identical copy of an arbitrary, unknown quantum state. Therefore, it

is also impossible to use the same mechanisms that worked for classical networks for signal amplification, retransmission, and so on, as they all rely on the ability to copy the underlying data. Since any physical channel will always be lossy, connecting nodes within a quantum network is a challenging endeavour, and its architecture must at its core address this very issue.

4.1.3. Fidelity

In general, it is expected that a classical packet arrives at its destination without any errors introduced by hardware noise along the way. This is verified at various levels through a variety of error detection and correction mechanisms. Since we cannot read or copy a quantum state, error detection and correction are more involved.

To describe the quality of a quantum state, a physical quantity called fidelity is used [NielsenChuang]. Fidelity takes a value between 0 and 1 -- higher is better, and less than 0.5 means the state is unusable. It measures how close a quantum state is to the state we have tried to create. It expresses the probability that the state will behave exactly the same as our desired state. Fidelity is an important property of a quantum system that allows us to quantify how much a particular state has been affected by noise from various sources (gate errors, channel losses, environment noise).

Interestingly, quantum applications do not need perfect fidelity to be able to execute -- as long as the fidelity is above some application-specific threshold, they will simply operate at lower rates. Therefore, rather than trying to ensure that we always deliver perfect states (a technologically challenging task), applications will specify a minimum threshold for the fidelity, and the network will try its best to deliver it. A higher fidelity can be achieved by either having hardware produce states of better fidelity (sometimes one can sacrifice rate for higher fidelity) or employing quantum error detection and correction mechanisms (see [Mural16] and Chapter 11 of [VanMeterBook]).

4.1.4. Inadequacy of Direct Transmission

Conceptually, the most straightforward way to distribute an entangled state is to simply transmit one of the qubits directly to the other end across a series of nodes while performing sufficient forward Quantum Error Correction (QEC) (Section 4.4.3.2) to bring losses down to an acceptable level. Despite the no-cloning theorem and the inability to directly measure a quantum state, error-correcting mechanisms for quantum communication exist [Jiang09] [Fowler10] [Devitt13] [Mural16]. However, QEC makes very high demands on both resources (physical qubits needed) and their initial fidelity. Implementation is very challenging, and QEC is not expected to be used until later generations of quantum networks are possible (see Figure 2 of [Mural16] and Section 4.4.3.3 of this document). Until then, quantum networks rely on entanglement swapping (Section 4.4.2) and teleportation (Section 4.3). This alternative relies on the observation that we do not need to be able to distribute any arbitrary entangled quantum state. We only need to be able to distribute any one of what are known as the Bell pair states

[Briegel98].

4.2. Bell Pairs

Bell pair states are the entangled two-qubit states:

$$|00\rangle + |11\rangle,$$
$$|00\rangle - |11\rangle,$$
$$|01\rangle + |10\rangle,$$
$$|01\rangle - |10\rangle,$$

where the constant 1/sqrt(2) normalisation factor has been ignored for clarity. Any of the four Bell pair states above will do, as it is possible to transform any Bell pair into another Bell pair with local operations performed on only one of the qubits. When each qubit in a Bell pair is held by a separate node, either node can apply a series of single-qubit gates to their qubit alone in order to transform the state between the different variants.

Distributing a Bell pair between two nodes is much easier than transmitting an arbitrary quantum state over a network. Since the state is known, handling errors becomes easier, and small-scale error correction (such as entanglement distillation, as discussed in Section 4.4.3.1), combined with reattempts, becomes a valid strategy.

The reason for using Bell pairs specifically as opposed to any other two-qubit state is that they are the maximally entangled two-qubit set of basis states. Maximal entanglement means that these states have the strongest non-classical correlations of all possible two-qubit states. Furthermore, since single-qubit local operations can never increase entanglement, states that are less entangled would impose some constraints on distributed quantum algorithms. This makes Bell pairs particularly useful as a generic building block for distributed quantum applications.

4.3. Teleportation

The observation that we only need to be able to distribute Bell pairs relies on the fact that this enables the distribution of any other arbitrary entangled state. This can be achieved via quantum state teleportation [Bennett93]. Quantum state teleportation consumes an unknown qubit state that we want to transmit and recreates it at the desired destination. This does not violate the no-cloning theorem, as the original state is destroyed in the process.

To achieve this, an entangled pair needs to be distributed between the source and destination before teleportation commences. The source then entangles the transmission qubit with its end of the pair and performs a readout of the two qubits (the sum of these operations is called a Bell state measurement). This consumes the Bell pair's entanglement, turning the source and destination qubits into independent states. The measurement yields two classical bits, which the source sends to the destination over a classical channel. Based on the value of the received two classical bits, the destination performs one of four possible corrections (called the Pauli corrections) on its end of the pair, which turns it into the unknown

qubit state that we wanted to transmit. This requirement to communicate the measurement readout over a classical channel unfortunately means that entanglement cannot be used to transmit information faster than the speed of light.

The unknown quantum state that was transmitted was never fed into the network itself. Therefore, the network needs to only be able to reliably produce Bell pairs between any two nodes in the network. Thus, a key difference between a classical data plane and a quantum data plane is that a classical data plane carries user data but a quantum data plane provides the resources for the user to transmit user data themselves without further involvement of the network.

4.4. The Life Cycle of Entanglement

Reducing the problem of quantum connectivity to one of generating a Bell pair has reduced the problem to a simpler, more fundamental case, but it has not solved it. In this section, we discuss how these entangled pairs are generated in the first place and how their two qubits are delivered to the end-points.

4.4.1. Elementary Link Generation

In a quantum network, entanglement is always first generated locally (at a node or an auxiliary element), followed by a movement of one or both of the entangled qubits across the link through quantum channels. In this context, photons (particles of light) are the natural candidate for entanglement carriers. Because these photons carry quantum states from place to place at high speed, we call them flying qubits. The rationale for this choice is related to the advantages provided by photons, such as moderate interaction with the environment leading to moderate decoherence; convenient control with standard optical components; and high-speed, low-loss transmissions. However, since photons are hard to store, a transducer must transfer the flying qubit's state to a qubit suitable for information processing and/or storage (often referred to as a matter qubit).

Since this process may fail, in order to generate and store entanglement efficiently, we must be able to distinguish successful attempts from failures. Entanglement generation schemes that are able to announce successful generation are called heralded entanglement generation schemes.

There exist three basic schemes for heralded entanglement generation on a link through coordinated action of the two nodes at the two ends of the link [Cacciapuoti19]:

"At mid-point": In this scheme, an entangled photon pair source sitting midway between the two nodes with matter qubits sends an entangled photon through a quantum channel to each of the nodes. There, transducers are invoked to transfer the entanglement from the flying qubits to the matter qubits. In this scheme, the transducers know if the transfers succeeded and are able to herald successful entanglement generation via a message exchange over the classical channel.

"At source": In this scheme, one of the two nodes sends a flying qubit that is entangled with one of its matter qubits. A transducer at the other end of the link will transfer the entanglement from the flying qubit to one of its matter qubits. Just like in the previous scheme, the transducer knows if its transfer succeeded and is able to herald successful entanglement generation with a classical message sent to the other node.

"At both end-points": In this scheme, both nodes send a flying qubit that is entangled with one of their matter qubits. A detector somewhere in between the nodes performs a joint measurement on the flying qubits, which stochastically projects the remote matter qubits into an entangled quantum state. The detector knows if the entanglement succeeded and is able to herald successful entanglement generation by sending a message to each node over the classical channel.

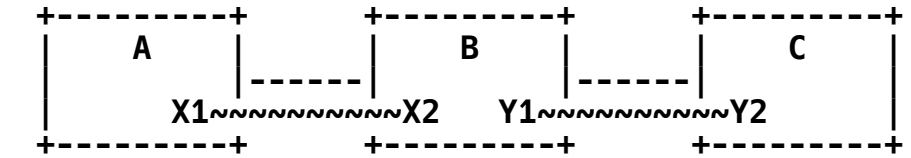
The "mid-point source" scheme is more robust to photon loss, but in the other schemes, the nodes retain greater control over the entangled pair generation.

Note that whilst photons travel in a particular direction through the quantum channel the resulting entangled pair of qubits does not have a direction associated with it. Physically, there is no upstream or downstream end of the pair.

4.4.2. Entanglement Swapping

The problem with generating entangled pairs directly across a link is that efficiency decreases with channel length. Beyond a few tens of kilometres in optical fibre or 1000 kilometres in free space (via satellite), the rate is effectively zero, and due to the no-cloning theorem we cannot simply amplify the signal. The solution is entanglement swapping [Briegel98].

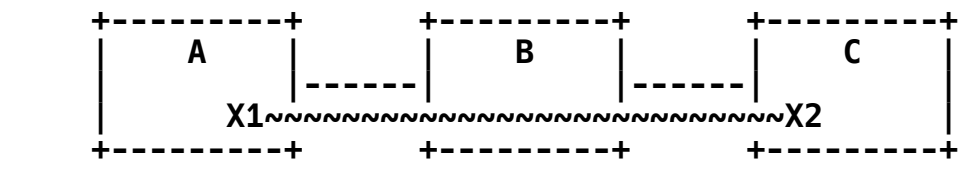
A Bell pair between any two nodes in the network can be constructed by combining the pairs generated along each individual link on a path between the two end-points. Each node along the path can consume the two pairs on the two links to which it is connected, in order to produce a new entangled pair between the two remote ends. This process is known as entanglement swapping. It can be represented pictorially as follows:



where X1 and X2 are the qubits of the entangled pair X and Y1 and Y2 are the qubits of entangled pair Y. The entanglement is denoted with ~~. In the diagram above, nodes A and B share the pair X and nodes B and C share the pair Y, but we want entanglement between A and C.

To achieve this goal, we simply teleport the qubit X2 using the pair Y. This requires node B to perform a Bell state measurement on the

qubits X2 and Y1 that results in the destruction of the entanglement between Y1 and Y2. However, X2 is recreated in Y2's place, carrying with it its entanglement with X1. The end result is shown below:



Depending on the needs of the network and/or application, a final Pauli correction at the recipient node may not be necessary, since the result of this operation is also a Bell pair. However, the two classical bits that form the readout from the measurement at node B must still be communicated, because they carry information about which of the four Bell pairs was actually produced. If a correction is not performed, the recipient must be informed which Bell pair was received.

This process of teleporting Bell pairs using other entangled pairs is called entanglement swapping. Quantum nodes that create long-distance entangled pairs via entanglement swapping are called quantum repeaters in academic literature [Briegel98]. We will use the same terminology in this document.

4.4.3. Error Management

4.4.3.1. Distillation

Neither the generation of Bell pairs nor the swapping operations are noiseless operations. Therefore, with each link and each swap, the fidelity of the state degrades. However, it is possible to create higher-fidelity Bell pair states from two or more lower-fidelity pairs through a process called distillation (sometimes also referred to as purification) [Dur07].

To distil a quantum state, a second (and sometimes third) quantum state is used as a "test tool" to test a proposition about the first state, e.g., "the parity of the two qubits in the first state is even." When the test succeeds, confidence in the state is improved, and thus the fidelity is improved. The test tool states are destroyed in the process, so resource demands increase substantially when distillation is used. When the test fails, the tested state must also be discarded. Distillation makes low demands on fidelity and resources compared to QEC, but distributed protocols incur round-trip delays due to classical communication [Bennett96].

4.4.3.2. Quantum Error Correction (QEC)

Just like classical error correction, QEC encodes logical qubits using several physical (raw) qubits to protect them from the errors described in Section 4.1.3 [Jiang09] [Fowler10] [Devitt13] [Mural16]. Furthermore, similarly to its classical counterpart, QEC can not only correct state errors but also account for lost qubits. Additionally, if all physical qubits that encode a logical qubit are located at the same node, the correction procedure can be executed locally, even if

the logical qubit is entangled with remote qubits.

Although QEC was originally a scheme proposed to protect a qubit from noise, QEC can also be applied to entanglement distillation. Such QEC-applied distillation is cost effective but requires a higher base fidelity.

4.4.3.3. Error Management Schemes

Quantum networks have been categorised into three "generations" based on the error management scheme they employ [Mural16]. Note that these "generations" are more like categories; they do not necessarily imply a time progression and do not obsolete each other, though the later generations do require technologies that are more advanced. Which generation is used depends on the hardware platform and network design choices.

Table 2 summarises the generations.

	First generation	Second generation	Third generation
Loss tolerance	Heralded entanglement generation (bidirectional classical signalling)	Heralded entanglement generation (bidirectional classical signalling)	QEC (no classical signalling)
Error tolerance	Entanglement distillation (bidirectional classical signalling)	Entanglement distillation (unidirectional classical signalling) or QEC (no classical signalling)	QEC (no classical signalling)

Table 2: Classical Signalling and Generations

Generations are defined by the directions of classical signalling required in their distributed protocols for loss tolerance and error tolerance. Classical signalling carries the classical bits, incurring round-trip delays. As described in Section 4.4.3.1, these delays affect the performance of quantum networks, especially as the distance between the communicating nodes increases.

Loss tolerance is about tolerating qubit transmission losses between nodes. Heralded entanglement generation, as described in Section 4.4.1, confirms the receipt of an entangled qubit using a heralding signal. A pair of directly connected quantum nodes repeatedly attempt to generate an entangled pair until the heralding signal is received. As described in Section 4.4.3.2, QEC can be applied to complement lost qubits, eliminating the need for reattempts. Furthermore, since the correction procedure is composed

of local operations, it does not require a heralding signal. However, it is possible only when the photon loss rate from transmission to measurement is less than 50%.

Error tolerance is about tolerating quantum state errors. Entanglement distillation is the easiest mechanism to implement for improved error tolerance, but it incurs round-trip delays due to the requirement for bidirectional classical signalling. The alternative, QEC, is able to correct state errors locally so that it does not need any classical signalling between the quantum nodes. In between these two extremes, there is also QEC-applied distillation, which requires unidirectional classical signalling.

The three "generations" summarised:

1. First-generation quantum networks use heralding for loss tolerance and entanglement distillation for error tolerance. These networks can be implemented even with a limited set of available quantum gates.

2. Second-generation quantum networks improve upon the first generation with QEC codes for error tolerance (but not loss tolerance). At first, QEC will be applied to entanglement distillation only, which requires unidirectional classical signalling. Later, QEC codes will be used to create logical Bell pairs that no longer require any classical signalling for the purposes of error tolerance. Heralding is still used to compensate for transmission losses.

3. Third-generation quantum networks directly transmit QEC-encoded qubits to adjacent nodes, as discussed in Section 4.1.4. Elementary link Bell pairs can now be created without heralding or any other classical signalling. Furthermore, this also enables direct transmission architectures in which qubits are forwarded end to end like classical packets rather than relying on Bell pairs and entanglement swapping.

Despite the fact that there are important distinctions in how errors will be managed in the different generations, it is unlikely that all quantum networks will consistently use the same method. This is due to different hardware requirements of the different generations and the practical reality of network upgrades. Therefore, it is unavoidable that eventually boundaries between different error management schemes start forming. This will affect the content and semantics of messages that must cross those boundaries -- for both connection setup and real-time operation [Nagayama16].

4.4.4. Delivery

Eventually, the Bell pairs must be delivered to an application (or higher-layer protocol) at the two end nodes. A detailed list of such requirements is beyond the scope of this document. At minimum, the end nodes require information to map a particular Bell pair to the qubit in their local memory that is part of this entangled pair.

5. Architecture of a Quantum Internet

It is evident from the previous sections that the fundamental service provided by a quantum network significantly differs from that of a classical network. Therefore, it is not surprising that the architecture of a quantum internet will itself be very different from that of the classical Internet.

5.1. Challenges

This subsection covers the major fundamental challenges involved in building quantum networks. Here, we only describe the fundamental differences. Technological limitations are described in Section 5.4.

1. Bell pairs are not equivalent to packets that carry payload.

   In most classical networks, including Ethernet, Internet Protocol (IP), and Multi-Protocol Label Switching (MPLS) networks, user data is grouped into packets. In addition to the user data, each packet also contains a series of headers that contain the control information that lets routers and switches forward it towards its destination. Packets are the fundamental unit in a classical network.

   In a quantum network, the entangled pairs of qubits are the basic unit of networking. These qubits themselves do not carry any headers. Therefore, quantum networks will have to send all control information via separate classical channels, which the repeaters will have to correlate with the qubits stored in their memory. Furthermore, unlike a classical packet, which is located at a single node, a Bell pair consists of two qubits distributed across two nodes. This has a fundamental impact on how quantum networks will be managed and how protocols need to be designed. To make long-distance Bell pairs, the nodes may have to keep their qubits in their quantum memories and wait until control information is exchanged before proceeding with the next operation. This signalling will result in additional latency, which will depend on the distance between the nodes holding the two ends of the Bell pair. Error management, such as entanglement distillation, is a typical example of such control information exchange [Nagayama21] (see also Section 4.4.3.3).

2. "Store and forward" and "store and swap" quantum networks require different state management techniques.

   As described in Section 4.4.1, quantum links provide Bell pairs that are undirected network resources, in contrast to directed frames of classical networks. This phenomenological distinction leads to architectural differences between quantum networks and classical networks. Quantum networks combine multiple elementary link Bell pairs together to create one end-to-end Bell pair, whereas classical networks deliver messages from one end to the other end hop by hop.

   Classical networks receive data on one interface, store it in local buffers, and then forward the data to another appropriate interface. Quantum networks store Bell pairs and then execute

entanglement swapping instead of forwarding in the data plane. Such quantum networks are "store and swap" networks. In "store and swap" networks, we do not need to care about the order in which the Bell pairs were generated, since they are undirected. However, whilst the ordering does not matter, it is very important that the right entangled pairs get swapped, and that the intermediate measurement outcomes (see Section 4.4.2) are signalled to and correlated with the correct qubits at the other nodes. Otherwise, the final end-to-end entangled pair will not be created between the expected end-points or will be in a different quantum state than expected. For example, rather than Alice receiving a qubit that is entangled with Bob's qubit, her qubit is entangled with Charlie's qubit. This distinction makes control algorithms and optimisation of quantum networks different from those for classical networks, in the sense that swapping is stateful in contrast to stateless packet-by-packet forwarding. Note that, as described in Section 4.4.3.3, third-generation quantum networks will be able to support a "store and forward" architecture in addition to "store and swap".

3. An entangled pair is only useful if the locations of both qubits are known.

   A classical network packet logically exists only at one location at any point in time. If a packet is modified in some way, whether headers or payload, this information does not need to be conveyed to anybody else in the network. The packet can be simply forwarded as before.

   In contrast, entanglement is a phenomenon in which two or more qubits exist in a physically distributed state. Operations on one of the qubits change the mutual state of the pair. Since the owner of a particular qubit cannot just read out its state, it must coordinate all its actions with the owner of the pair's other qubit. Therefore, the owner of any qubit that is part of an entangled pair must know the location of its counterpart. Location, in this context, need not be the explicit spatial location. A relevant pair identifier, a means of communication between the pair owners, and an association between the pair ID and the individual qubits will be sufficient.

4. Generating entanglement requires temporary state.

   Packet forwarding in a classical network is largely a stateless operation. When a packet is received, the router does a lookup in its forwarding table and sends the packet out of the appropriate output. There is no need to keep any memory of the packet any more.

   A quantum node must be able to make decisions about qubits that it receives and is holding in its memory. Since qubits do not carry headers, the receipt of an entangled pair conveys no control information based on which the repeater can make a decision. The relevant control information will arrive separately over a classical channel. This implies that a repeater must store temporary state, as the control information

and the qubit it pertains to will, in general, not arrive at the same time.

5.2. Classical Communication

In this document, we have already covered two different roles that classical communication must perform the following:

* Communicate classical bits of information as part of distributed protocols such as entanglement swapping and teleportation.

* Communicate control information within a network, including background protocols such as routing, as well as signalling protocols to set up end-to-end entanglement generation.

Classical communication is a crucial building block of any quantum network. All nodes in a quantum network are assumed to have classical connectivity with each other (within typical administrative domain limits). Therefore, quantum nodes will need to manage two data planes in parallel: a classical data plane and a quantum data plane. Additionally, a node must be able to correlate information between the two planes so that the control information received on a classical channel can be applied to the qubits managed by the quantum data plane.

5.3. Abstract Model of the Network

5.3.1. The Control Plane and the Data Plane

Control plane protocols for quantum networks will have many responsibilities similar to their classical counterparts, namely discovering the network topology, resource management, populating data plane tables, etc. Most of these protocols do not require the manipulation of quantum data and can operate simply by exchanging classical messages only. There may also be some control plane functionality that does require the handling of quantum data [QI-Scenarios]. As it is not clear if there is much benefit in defining a separate quantum control plane given the significant overlap in responsibilities with its classical counterpart, the question of whether there should be a separate quantum control plane is beyond the scope of this document.

However, the data plane separation is much more distinct, and there will be two data planes: a classical data plane and a quantum data plane. The classical data plane processes and forwards classical packets. The quantum data plane processes and swaps entangled pairs. Third-generation quantum networks may also forward qubits in addition to swapping Bell pairs.

In addition to control plane messages, there will also be control information messages that operate at the granularity of individual entangled pairs, such as heralding messages used for elementary link generation (Section 4.4.1). In terms of functionality, these messages are closer to classical packet headers than control plane messages, and thus we consider them to be part of the quantum data plane. Therefore, a quantum data plane also includes the exchange of

classical control information at the granularity of individual qubits and entangled pairs.

5.3.2. Elements of a Quantum Network

We have identified quantum repeaters as the core building block of a quantum network. However, a quantum repeater will have to do more than just entanglement swapping in a functional quantum network. Its key responsibilities will include the following:

1. Creating link-local entanglement between neighbouring nodes.

2. Extending entanglement from link-local pairs to long-range pairs through entanglement swapping.

3. Performing distillation to manage the fidelity of the produced pairs.

4. Participating in the management of the network (routing, etc.).

Not all quantum repeaters in the network will be the same; here, we break them down further:

Quantum routers (controllable quantum nodes): A quantum router is a quantum repeater with a control plane that participates in the management of the network and will make decisions about which qubits to swap to generate the requested end-to-end pairs.

Automated quantum nodes: An automated quantum node is a data-plane-only quantum repeater that does not participate in the network control plane. Since the no-cloning theorem precludes the use of amplification, long-range links will be established by chaining multiple such automated nodes together.

End nodes: End nodes in a quantum network must be able to receive and handle an entangled pair, but they do not need to be able to perform an entanglement swap (and thus are not necessarily quantum repeaters). End nodes are also not required to have any quantum memory, as certain quantum applications can be realised by having the end node measure its qubit as soon as it is received.

Non-quantum nodes: Not all nodes in a quantum network need to have a quantum data plane. A non-quantum node is any device that can handle classical network traffic.

Additionally, we need to identify two kinds of links that will be used in a quantum network:

Quantum links: A quantum link is a link that can be used to generate an entangled pair between two directly connected quantum repeaters. This may include additional mid-point elements as described in Section 4.4.1. It may also include a dedicated classical channel that is to be used solely for the purpose of coordinating the entanglement generation on this quantum link.

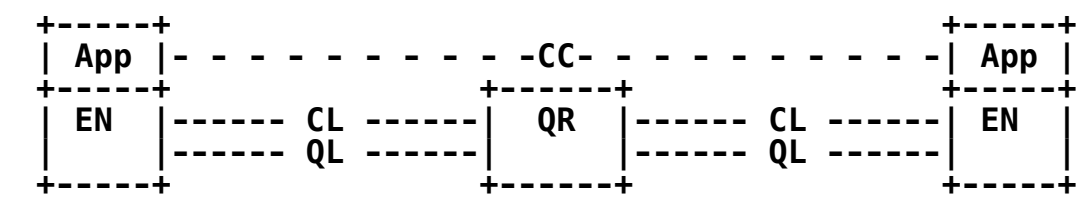
Classical links: A classical link is a link between any node in the

network that is capable of carrying classical network traffic.

Note that passive elements, such as optical switches, do not destroy the quantum state. Therefore, it is possible to connect multiple quantum nodes with each other over an optical network and perform optical switching rather than routing via entanglement swapping at quantum routers. This does require coordination with the elementary link entanglement generation process, and it still requires repeaters to overcome the short-distance limitations. However, this is a potentially feasible architecture for local area networks.

5.3.3. Putting It All Together

A two-hop path in a generic quantum network can be represented as follows:



App - user-level application
EN - End Node
QL - Quantum Link
CL - Classical Link
CC - Classical Channel (traverses one or more CLs)
QR - Quantum Repeater

An application (App) running on two End Nodes (ENs) attached to a network will at some point need the network to generate entangled pairs for its use. This may require negotiation between the ENs (possibly ahead of time), because they must both open a communication end-point that the network can use to identify the two ends of the connection. The two ENs use a Classical Channel (CC) available in the network to achieve this goal.

When the network receives a request to generate end-to-end entangled pairs, it uses the Classical Links (CLs) to coordinate and claim the resources necessary to fulfill this request. This may be some combination of prior control information (e.g., routing tables) and signalling protocols, but the details of how this is achieved are an active research question. A thought experiment on what this might look like be can be found in Section 7.

During or after the distribution of control information, the network performs the necessary quantum operations, such as generating entanglement over individual Quantum Links (QLs), performing entanglement swaps at Quantum Repeaters (QRs), and further signalling to transmit the swap outcomes and other control information. Since Bell pairs do not carry any user data, some of these operations can be performed before the request is received, in anticipation of the demand.

Note that here, "signalling" is used in a very broad sense and covers

many different types of messaging necessary for entanglement generation control. For example, heralded entanglement generation requires very precise timing synchronisation between the neighbouring nodes, and thus the triggering of entanglement generation and heralding may happen over its own, perhaps physically separate, CL, as was the case in the network stack demonstration described in [Pompili21.2]. Higher-level signalling with timing requirements that are less stringent (e.g., control plane signalling) may then happen over its own CL.

The entangled pair is delivered to the application once it is ready, together with the relevant pair identifier. However, being ready does not necessarily mean that all link pairs and entanglement swaps are complete, as some applications can start executing on an incomplete pair. In this case, the remaining entanglement swaps will propagate the actions across the network to the other end, sometimes necessitating fixup operations at the EN.

5.4. Physical Constraints

The model above has effectively abstracted away the particulars of the hardware implementation. However, certain physical constraints need to be considered in order to build a practical network. Some of these are fundamental constraints, and no matter how much the technology improves, they will always need to be addressed. Others are artifacts of the early stages of a new technology. Here, we consider a highly abstract scenario and refer to [Wehner18] for pointers to the physics literature.

5.4.1. Memory Lifetimes

In addition to discrete operations being imperfect, storing a qubit in memory is also highly non-trivial. The main difficulty in achieving persistent storage is that it is extremely challenging to isolate a quantum system from the environment. The environment introduces an uncontrollable source of noise into the system, which affects the fidelity of the state. This process is known as decoherence. Eventually, the state has to be discarded once its fidelity degrades too much.

The memory lifetime depends on the particular physical setup, but the highest achievable values in quantum network hardware are, as of 2020, on the order of seconds [Abobeih18], although a lifetime of a minute has also been demonstrated for qubits not connected to a quantum network [Bradley19]. These values have increased tremendously over the lifetime of the different technologies and are bound to keep increasing. However, if quantum networks are to be realised in the near future, they need to be able to handle short memory lifetimes -- for example, by reducing latency on critical paths.

5.4.2. Rates

Entanglement generation on a link between two connected nodes is not a very efficient process, and it requires many attempts to succeed [Hensen15] [Dahlberg19]. For example, the highest achievable rates

of success between nitrogen-vacancy center nodes -- which, in addition to entanglement generation are also capable of storing and processing the resulting qubits -- are on the order of 10 Hz. Combined with short memory lifetimes, this leads to very tight timing windows to build up network-wide connectivity.

Other platforms have shown higher entanglement rates, but this usually comes at the cost of other hardware capabilities, such as no quantum memory and/or limited processing capabilities [Wei22]. Nevertheless, the current rates are not sufficient for practical applications beyond simple experimental proofs of concept. However, they are expected to improve over time as quantum network technology evolves [Wei22].

5.4.3. Communication Qubits

Most physical architectures capable of storing qubits are only able to generate entanglement using only a subset of available qubits called communication qubits [Dahlberg19]. Once a Bell pair has been generated using a communication qubit, its state can be transferred into memory. This may impose additional limitations on the network. In particular, if a given node has only one communication qubit, it cannot simultaneously generate Bell pairs over two links. It must generate entanglement over the links one at a time.

5.4.4. Homogeneity

At present, all existing quantum network implementations are homogeneous, and they do not interface with each other. In general, it is very challenging to combine different quantum information processing technologies.

There are many different physical hardware platforms for implementing quantum networking hardware. The different technologies differ in how they store and manipulate qubits in memory and how they generate entanglement across a link with their neighbours. For example, hardware based on optical elements and atomic ensembles [Sangouard11] is very efficient at generating entanglement at high rates but provides limited processing capabilities once the entanglement is generated. On the other hand, nitrogen-vacancy-based platforms [Hensen15] or trapped ion platforms [Moehring07] offer a much greater degree of control over the qubits but have a harder time generating entanglement at high rates.

In order to overcome the weaknesses of the different platforms, coupling the different technologies will help to build fully functional networks. For example, end nodes may be implemented using technology with good qubit processing capabilities to enable complex applications, but automated quantum nodes that serve only to "repeat" along a linear chain, where the processing logic is much simpler, can be implemented with technologies that sacrifice processing capabilities for higher entanglement rates at long distances [Askarani21].

This point is further exacerbated by the fact that quantum computers (i.e., end nodes in a quantum network) are often based on different

hardware platforms than quantum repeaters, thus requiring a coupling (transduction) between the two. This is especially true for quantum computers based on superconducting technology, which are challenging to connect to optical networks. However, even trapped ion quantum computers, which make up a platform that has shown promise for quantum networking, will still need to connect to other platforms that are better at creating entanglement at high rates over long distances (hundreds of kilometres).

6. Architectural Principles

Given that the most practical way of realising quantum network connectivity is using Bell pair and entanglement-swapping repeater technology, what sort of principles should guide us in assembling such networks such that they are functional, robust, efficient, and, most importantly, will work? Furthermore, how do we design networks so that they work under the constraints imposed by the hardware available today but do not impose unnecessary burdens on future technology?

As quantum networking is a completely new technology that is likely to see many iterations over its lifetime, this document must not serve as a definitive set of rules but merely as a general set of recommended guidelines for the first generations of quantum networks based on principles and observations made by the community. The benefit of having a community-built document at this early stage is that expertise in both quantum information and network architecture is needed in order to successfully build a quantum internet.

6.1. Goals of a Quantum Internet

When outlining any set of principles, we must ask ourselves what goals we want to achieve, as inevitably trade-offs must be made. So, what sort of goals should drive a quantum network architecture? The following list has been inspired by the history of computer networking, and thus it is inevitably very similar to one that could be produced for the classical Internet [Clark88]. However, whilst the goals may be similar, the challenges involved are often fundamentally different. The list will also most likely evolve with time and the needs of its users.

1. Support distributed quantum applications.

   This goal seems trivially obvious, but it makes a subtle, but important, point that highlights a key difference between quantum and classical networks. Ultimately, quantum data transmission is not the goal of a quantum network -- it is only one possible component of quantum application protocols that are more advanced [Wehner18]. Whilst transmission certainly could be used as a building block for all quantum applications, it is not the most basic one possible. For example, entanglement-based QKD, the most well-known quantum application protocol, only relies on the stronger-than-classical correlations and inherent secrecy of entangled Bell pairs and does not have to transmit arbitrary quantum states [Ekert91].

The primary purpose of a quantum internet is to support distributed quantum application protocols, and it is of utmost importance that they can run well and efficiently. Thus, it is important to develop performance metrics meaningful to applications to drive the development of quantum network protocols. For example, the Bell pair generation rate is meaningless if one does not also consider their fidelity. It is generally much easier to generate pairs of lower fidelity, but quantum applications may have to make multiple reattempts or even abort if the fidelity is too low. A review of the requirements for different known quantum applications can be found in [Wehner18], and an overview of use cases can be found in [QI-Scenarios].

2. Support tomorrow's distributed quantum applications.

   The only principle of the Internet that should survive indefinitely is the principle of constant change [RFC1958]. Technical change is continuous, and the size and capabilities of the quantum internet will change by orders of magnitude. Therefore, it is an explicit goal that a quantum internet architecture be able to embrace this change. We have the benefit of having been witness to the evolution of the classical Internet over several decades, and we have seen what worked and what did not. It is vital for a quantum internet to avoid the need for flag days (e.g., NCP to TCP/IP) or upgrades that take decades to roll out (e.g., IPv4 to IPv6).

   Therefore, it is important that any proposed architecture for general-purpose quantum repeater networks can integrate new devices and solutions as they become available. The architecture should not be constrained due to considerations for early-stage hardware and applications. For example, it is already possible to run QKD efficiently on metropolitan-scale networks, and such networks are already commercially available. However, they are not based on quantum repeaters and thus will not be able to easily transition to applications that are more sophisticated.

3. Support heterogeneity.

   There are multiple proposals for realising practical quantum repeater hardware, and they all have their advantages and disadvantages. Some may offer higher Bell pair generation rates on individual links at the cost of entanglement swap operations that are more difficult. Other platforms may be good all around but are more difficult to build.

   In addition to physical boundaries, there may be distinctions in how errors are managed (Section 4.4.3.3). These differences will affect the content and semantics of messages that cross these boundaries -- for both connection setup and real-time operation.

   The optimal network configuration will likely leverage the advantages of multiple platforms to optimise the provided service. Therefore, it is an explicit goal to incorporate varied hardware and technology support from the beginning.

4. Ensure security at the network level.

   The question of security in quantum networks is just as critical as it is in the classical Internet, especially since enhanced security offered by quantum entanglement is one of the key driving factors.

   Fortunately, from an application's point of view, as long as the underlying implementation corresponds to (or sufficiently approximates) theoretical models of quantum cryptography, quantum cryptographic protocols do not need the network to provide any guarantees about the confidentiality or integrity of the transmitted qubits or the generated entanglement (though they may impose requirements on the classical channel, e.g., to be authenticated [Wang21]). Instead, applications will leverage the classical networks to establish the end-to-end security of the results obtained from the processing of entangled qubits. However, it is important to note that whilst classical networks are necessary to establish these end-to-end guarantees, the security relies on the properties of quantum entanglement. For example, QKD uses classical information reconciliation [Tang19] for error correction and privacy amplification [Elkouss11] for generating the final secure key, but the raw bits that are fed into these protocols must come from measuring entangled qubits [Ekert91]. In another application, secure delegated quantum computing, the client hides its computation from the server by sending qubits to the server and then requesting (in a classical message) that the server measure them in an encoded basis. The client then decodes the results it receives from the server to obtain the result of the computation [Broadbent10]. Once again, whilst a classical network is used to achieve the goal of secure computation, the remote computation is strictly quantum.

   Nevertheless, whilst applications can ensure their own end-to-end security, network protocols themselves should be security aware in order to protect the network itself and limit disruption. Whilst the applications remain secure, they are not necessarily operational or as efficient in the presence of an attacker. For example, if an attacker can measure every qubit between two parties trying to establish a key using QKD, no secret key can be generated. Security concerns in quantum networks are described in more detail in [Satoh17] and [Satoh20].

5. Make them easy to monitor.

   In order to manage, evaluate the performance of, or debug a network, it is necessary to have the ability to monitor the network while ensuring that there will be mechanisms in place to protect the confidentiality and integrity of the devices connected to it. Quantum networks bring new challenges in this area, so it should be a goal of a quantum network architecture to make this task easy.

   The fundamental unit of quantum information, the qubit, cannot be actively monitored, as any readout irreversibly destroys its

contents. One of the implications of this fact is that measuring an individual pair's fidelity is impossible. Fidelity is meaningful only as a statistical quantity that requires constant monitoring of generated Bell pairs, achieved by sacrificing some Bell pairs for use in tomography or other methods.

Furthermore, given one end of an entangled pair, it is impossible to tell where the other qubit is without any additional classical metadata. It is impossible to extract this information from the qubits themselves. This implies that tracking entangled pairs necessitates some exchange of classical information. This information might include (i) a reference to the entangled pair that allows distributed applications to coordinate actions on qubits of the same pair and (ii) the two bits from each entanglement swap necessary to identify the final state of the Bell pair (Section 4.4.2).

6. Ensure availability and resilience.

Any practical and usable network, classical or quantum, must be able to continue to operate despite losses and failures and be robust to malicious actors trying to disable connectivity. A difference between quantum and classical networks is that quantum networks are composed of two types of data planes (quantum and classical) and two types of channels (quantum and classical) that must be considered. Therefore, availability and resilience will most likely require a more advanced treatment than they do in classical networks.

Note that privacy, whilst related to security, is not listed as an explicit goal, because the privacy benefits will depend on the use case. For example, QKD only provides increased security for the distribution of symmetric keys [Bennett14] [Ekert91]. The handling, manipulation, sharing, encryption, and decryption of data will remain entirely classical, limiting the benefits to privacy that can be gained from using a quantum network. On the other hand, there are applications like blind quantum computation, which provides the user with the ability to execute a quantum computation on a remote server without the server knowing what the computation was or its input and output [Fitzsimons17]. Therefore, privacy must be considered on a per-application basis. An overview of quantum network use cases can be found in [QI-Scenarios].

6.2. The Principles of a Quantum Internet

The principles support the goals but are not goals themselves. The goals define what we want to build, and the principles provide a guideline for how we might achieve this. The goals will also be the foundation for defining any metric of success for a network architecture, whereas the principles in themselves do not distinguish between success and failure. For more information about design considerations for quantum networks, see [VanMeter13.1] and [Dahlberg19].

1. Entanglement is the fundamental service.

The key service that a quantum network provides is the distribution of entanglement between the nodes in a network. All distributed quantum applications are built on top of this key resource. Applications such as clustered quantum computing, distributed quantum computing, distributed quantum sensing networks, and certain kinds of quantum secure networks all consume quantum entanglement as a resource. Some applications (e.g., QKD) simply measure the entangled qubits to obtain a shared secret key [QKD]. Other applications (e.g., distributed quantum computing) build abstractions and operations that are more complex on the entangled qubits, e.g., distributed CNOT gates [DistCNOT] or teleportation of arbitrary qubit states [Teleportation].

A quantum network may also distribute multipartite entangled states (entangled states of three or more qubits) [Meignant19], which are useful for applications such as conference key agreement [Murta20], distributed quantum computing [Cirac99], secret sharing [Qin17], and clock synchronisation [Komar14], though it is worth noting that multipartite entangled states can also be constructed from multiple entangled pairs distributed between the end nodes.

2. Bell pairs are indistinguishable.

   Any two Bell pairs between the same two nodes are indistinguishable for the purposes of an application, provided they both satisfy its required fidelity threshold. This observation is likely to be key in enabling a more optimal allocation of resources in a network, e.g., for the purposes of provisioning resources to meet application demand. However, the qubits that make up the pair themselves are not indistinguishable, and the two nodes operating on a pair must coordinate to make sure they are operating on qubits that belong to the same Bell pair.

3. Fidelity is part of the service.

   In addition to being able to deliver Bell pairs to the communication end-points, the Bell pairs must be of sufficient fidelity. Unlike in classical networks, where most errors are effectively eliminated before reaching the application, many quantum applications only need imperfect entanglement to function. However, quantum applications will generally have a threshold for Bell pair fidelity below which they are no longer able to operate. Different applications will have different requirements for what fidelity they can work with. It is the network's responsibility to balance the resource usage with respect to the applications' requirements. It may be that it is cheaper for the network to provide lower-fidelity pairs that are just above the threshold required by the application than it is to guarantee high-fidelity pairs to all applications regardless of their requirements.

4. Time is an expensive resource.

Time is not the only resource that is in short supply (communication qubits and memory are as well), but ultimately it is the lifetime of quantum memories that imposes some of the most difficult conditions for operating an extended network of quantum nodes. Current hardware has low rates of Bell pair generation, short memory lifetimes, and access to a limited number of communication qubits. All these factors combined mean that even a short waiting queue at some node could be enough for a Bell pair to decohere or result in an end-to-end pair below an application's fidelity threshold. Therefore, managing the idle time of qubits holding live quantum states should be done carefully -- ideally by minimising the idle time, but potentially also by moving the quantum state for temporary storage to a quantum memory with a longer lifetime.

5. Be flexible with regards to capabilities and limitations.

   This goal encompasses two important points:

   * First, the architecture should be able to function under the physical constraints imposed by the current-generation hardware. Near-future hardware will have low entanglement generation rates, quantum memories able to hold a handful of qubits at best, and decoherence rates that will render many generated pairs unusable.

   * Second, the architecture should not make it difficult to run the network over any hardware that may come along in the future. The physical capabilities of repeaters will improve, and redeploying a technology is extremely challenging.

7. A Thought Experiment Inspired by Classical Networks

To conclude, we discuss a plausible quantum network architecture inspired by MPLS. This is not an architecture proposal but rather a thought experiment to give the reader an idea of what components are necessary for a functional quantum network. We use classical MPLS as a basis, as it is well known and understood in the networking community.

Creating end-to-end Bell pairs between remote end-points is a stateful distributed task that requires a lot of a priori coordination. Therefore, a connection-oriented approach seems the most natural for quantum networks. In connection-oriented quantum networks, when two quantum application end-points wish to start creating end-to-end Bell pairs, they must first create a Quantum Virtual Circuit (QVC). As an analogy, in MPLS networks, end-points must establish a Label Switched Path (LSP) before exchanging traffic. Connection-oriented quantum networks may also support virtual circuits with multiple end-points for creating multipartite entanglement. As an analogy, MPLS networks have the concept of multipoint LSPs for multicast.

When a quantum application creates a QVC, it can indicate Quality of Service (QoS) parameters such as the required capacity in end-to-end Bell Pairs Per Second (BPPS) and the required fidelity of the Bell

pairs. As an analogy, in MPLS networks, applications specify the required bandwidth in Bits Per Second (BPS) and other constraints when they create a new LSP.

Different applications will have different QoS requirements. For example, applications such as QKD that don't need to process the entangled qubits, and only need measure them and store the resulting outcome, may require a large volume of entanglement but will be tolerant of delay and jitter for individual pairs. On the other hand, distributed/cloud quantum computing applications may need fewer entangled pairs but instead may need all of them to be generated in one go so that they can all be processed together before any of them decohere.

Quantum networks need a routing function to compute the optimal path (i.e., the best sequence of routers and links) for each new QVC. The routing function may be centralised or distributed. In the latter case, the quantum network needs a distributed routing protocol. As an analogy, classical networks use routing protocols such as Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS). However, note that the definition of "shortest path" / "least cost" may be different in a quantum network to account for its non-classical features, such as fidelity [VanMeter13.2].

Given the very scarce availability of resources in early quantum networks, a Traffic Engineering (TE) function is likely to be beneficial. Without TE, QVCs always use the shortest path. In this case, the quantum network cannot guarantee that each quantum end-point will get its Bell pairs at the required rate or fidelity. This is analogous to "best effort" service in classical networks.

With TE, QVCs choose a path that is guaranteed to have the requested resources (e.g., bandwidth in BPPS) available, taking into account the capacity of the routers and links and also taking into account the resources already consumed by other virtual circuits. As an analogy, both OSPF and IS-IS have TE extensions to keep track of used and available resources and can use Constrained Shortest Path First (CSPF) to take resource availability and other constraints into account when computing the optimal path.

The use of TE implies the use of Call Admission Control (CAC): the network denies any virtual circuits for which it cannot guarantee the requested quality of service a priori. Alternatively, the network preempts lower-priority circuits to make room for a new circuit.

Quantum networks need a signalling function: once the path for a QVC has been computed, signalling is used to install the "forwarding rules" into the data plane of each quantum router on the path. The signalling may be distributed, analogous to the Resource Reservation Protocol (RSVP) in MPLS. Or, the signalling may be centralised, similar to OpenFlow.

Quantum networks need an abstraction of the hardware for specifying the forwarding rules. This allows us to decouple the control plane (routing and signalling) from the data plane (actual creation of Bell pairs). The forwarding rules are specified using abstract building

blocks such as "creating local Bell pairs", "swapping Bell pairs", or "distillation of Bell pairs". As an analogy, classical networks use abstractions that are based on match conditions (e.g., looking up header fields in tables) and actions (e.g., modifying fields or forwarding a packet to a specific interface). The data plane abstractions in quantum networks will be very different from those in classical networks due to the fundamental differences in technology and the stateful nature of quantum networks. In fact, choosing the right abstractions will be one of the biggest challenges when designing interoperable quantum network protocols.

In quantum networks, control plane traffic (routing and signalling messages) is exchanged over a classical channel, whereas data plane traffic (the actual Bell pair qubits) is exchanged over a separate quantum channel. This is in contrast to most classical networks, where control plane traffic and data plane traffic share the same channel and where a single packet contains both user fields and header fields. There is, however, a classical analogy to the way quantum networks work: generalised MPLS (GMPLS) networks use separate channels for control plane traffic and data plane traffic. Furthermore, GMPLS networks support data planes where there is no such thing as data plane headers (e.g., Dense Wavelength Division Multiplexing (DWDM) or Time-Division Multiplexing (TDM) networks).

8. Security Considerations

Security is listed as an explicit goal for the architecture; this issue is addressed in Section 6.1. However, as this is an Informational document, it does not propose any concrete mechanisms to achieve these goals.

9. IANA Considerations

This document has no IANA actions.

10. Informative References

[Abobeih18] Abobeih, M.H., Cramer, J., Bakker, M.A., Kalb, N., Markham, M., Twitchen, D.J., and T.H. Taminiau, "One-second coherence for a single electron spin coupled to a multi-qubit nuclear-spin environment", Nature communications Vol. 9, Iss. 1, pp. 1-8, DOI 10.1038/s41467-018-04916-z, June 2018, <https://www.nature.com/articles/s41467-018-04916-z>.

[Aguado19] Aguado, A., Lopez, V., Lopez, D., Peev, M., Poppe, A., Pastor, A., Folgueira, J., and V. Martin, "The Engineering of Software-Defined Quantum Key Distribution Networks", IEEE Communications Magazine Vol. 57, Iss. 7, pp. 20-26, DOI 10.1109/MCOM.2019.1800763, July 2019, <https://ieeexplore.ieee.org/document/8767074>.

[Askarani21] Askarani, M.F., Chakraborty, K., and G.C. do Amaral, "Entanglement distribution in multi-platform buffered-

router-assisted frequency-multiplexed automated repeater chains", New Journal of Physics Vol. 23, Iss. 6, 063078, DOI 10.1088/1367-2630/ac0a35, June 2021, <https://iopscience.iop.org/article/10.1088/1367-2630/ac0a35>.

[Aspect81] Aspect, A., Grangier, P., and G. Roger, "Experimental Tests of Realistic local Theories via Bell's Theorem", Physical Review Letters Vol. 47, Iss. 7, pp. 460-463, DOI 10.1103/PhysRevLett.47.460, August 1981, <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.47.460>.

[Bennett14] Bennett, C.H. and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", Theoretical Computer Science Vol. 560 (Part 1), pp. 7-11, DOI 10.1016/j.tcs.2014.05.025, December 2014, <https://www.sciencedirect.com/science/article/pii/S0304397514004241?via%3Dihub>.

[Bennett93] Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., and W.K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels", Physical Review Letters Vol. 70, Iss. 13, pp. 1895-1899, DOI 10.1103/PhysRevLett.70.1895, March 1993, <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.70.1895>.

[Bennett96] Bennett, C.H., DiVincenzo, D.P., Smolin, J.A., and W.K. Wootters, "Mixed-state entanglement and quantum error correction", Physical Review A Vol. 54, Iss. 5, pp. 3824-3851, DOI 10.1103/PhysRevA.54.3824, November 1996, <https://journals.aps.org/pra/abstract/10.1103/PhysRevA.54.3824>.

[Bradley19] Bradley, C.E., Randall, J., Abobeih, M.H., Berrevoets, R.C., Degen, M.J., Bakker, M.A., Markham, M., Twitchen, D.J., and T.H. Taminiau, "A Ten-Qubit Solid-State Spin Register with Quantum Memory up to One Minute", Physical Review X Vol. 9, Iss. 3, 031045, DOI 10.1103/PhysRevX.9.031045, September 2019, <https://journals.aps.org/prx/abstract/10.1103/PhysRevX.9.031045>.

[Briegel98] Briegel, H.-J., Dür, W., Cirac, J.I., and P. Zoller, "Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication", Physical Review Letters Vol. 81, Iss. 26, pp. 5932-5935, DOI 10.1103/PhysRevLett.81.5932, December 1998, <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.81.5932>.

[Broadbent10] Broadbent, A., Fitzsimons, J., and E. Kashefi, "Measurement-Based and Universal Blind Quantum Computation", Springer-Verlag 978-3-642-13678-8, DOI 10.1007/978-3-642-13678-8_2, June 2010, <https://link.springer.com/chapter/10.1007/978-3-642-13678-8_2>.

[Cacciapuoti19] Cacciapuoti, A.S., Caleffi, M., Van Meter, R., and L. Hanzo, "When Entanglement Meets Classical Communications: Quantum Teleportation for the Quantum Internet", IEEE Transactions on Communications Vol. 68, Iss. 6, pp. 3808-3833, DOI 10.1109/TCOMM.2020.2978071, June 2020, <https://ieeexplore.ieee.org/document/9023997>.

[Cirac99] Cirac, J.I., Ekert, A.K., Huelga, S.F., and C. Macchiavello, "Distributed quantum computation over noisy channels", Physical Review A Vol. 59, Iss. 6, 4249, DOI 10.1103/PhysRevA.59.4249, June 1999, <https://journals.aps.org/pra/abstract/10.1103/PhysRevA.59.4249>.

[Clark88] Clark, D., "The design philosophy of the DARPA internet protocols", SIGCOMM '88: Symposium proceedings on Communications architectures and protocols, pp. 106-114, DOI 10.1145/52324.52336, August 1988, <https://dl.acm.org/doi/abs/10.1145/52324.52336>.

[Crepeau02] Crépeau, C., Gottesman, D., and A. Smith, "Secure multi-party quantum computation", STOC '02: Proceedings of the thiry-fourth [sic] annual ACM symposium on Theory of computing, pp. 643-652, DOI 10.1145/509907.510000, May 2002, <https://dl.acm.org/doi/10.1145/509907.510000>.

[Dahlberg19] Dahlberg, A., Skrzypczyk, M., Coopmans, T., Wubben, L., Rozpędek, F., Pompili, M., Stolk, A., Pawełczak, P., Knegjens, R., de Oliveira Filho, J., Hanson, R., and S. Wehner, "A link layer protocol for quantum networks", SIGCOMM '19 Proceedings of the ACM Special Interest Group on Data Communication, pp. 159-173, DOI 10.1145/3341302.3342070, August 2019, <https://dl.acm.org/doi/10.1145/3341302.3342070>.

[Devitt13] Devitt, S.J., Munro, W.J., and K. Nemoto, "Quantum error correction for beginners", Reports on Progress in Physics Vol. 76, Iss. 7, 076001, DOI 10.1088/0034-4885/76/7/076001, June 2013, <https://iopscience.iop.org/article/10.1088/0034-4885/76/7/076001>.

[DistCNOT] "Distributed CNOT", Quantum Network Explorer by QuTech, 2023, <https://www.quantum-network.com/applications/7/>.

[Dur07] Dür, W. and H.J. Briegel, "Entanglement purification and quantum error correction", Reports on Progress in Physics Vol. 70, Iss. 8, pp. 1381-1424, DOI 10.1088/0034-4885/70/8/R03, July 2007, <https://iopscience.iop.org/article/10.1088/0034-4885/70/8/R03>.

[Ekert91] Ekert, A.K., "Quantum cryptography based on Bell's theorem", Physical Review Letters Vol. 67, Iss. 6, pp. 661-663, DOI 10.1103/PhysRevLett.67.661, August 1991, <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.67.661>.

[Elkouss11] Elkouss, D., Martinez-Mateo, J., and V. Martin, "Information Reconciliation for Quantum Key Distribution", Quantum Information and Computation Vol. 11, No. 3 and 4, pp. 0226-0238, DOI 10.48550/arXiv.1007.1616, March 2011, <https://arxiv.org/abs/1007.1616>.

[Elliott03] Elliott, C., Pearson, D., and G. Troxel, "Quantum cryptography in practice", SIGCOMM 2003: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, pp. 227-238, DOI 10.1145/863955.863982, August 2003, <https://dl.acm.org/doi/abs/10.1145/863955.863982>.

[Fitzsimons17] Fitzsimons, J.F. and E. Kashefi, "Unconditionally verifiable blind quantum computation", Physical Review A Vol. 96, Iss. 1, 012303, DOI 10.1103/PhysRevA.96.012303, July 2017, <https://journals.aps.org/pra/abstract/10.1103/PhysRevA.96.012303>.

[Fowler10] Fowler, A.G., Wang, D.S., Hill, C.D., Ladd, T.D., Van Meter, R., and L.C.L. Hollenberg, "Surface Code Quantum Communication", Physical Review Letters Vol. 104, Iss. 18, 180503, DOI 10.1103/PhysRevLett.104.180503, May 2010, <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.104.180503>.

[Giovannetti04] Giovannetti, V., Lloyd, S., and L. Maccone, "Quantum-Enhanced Measurements: Beating the Standard Quantum Limit", Science Vol. 306, Iss. 5700, pp. 1330-1336, DOI 10.1126/science.1104149, November 2004, <https://www.science.org/doi/10.1126/science.1104149>.

[Gottesman12] Gottesman, D., Jennewein, T., and S. Croke, "Longer-Baseline Telescopes Using Quantum Repeaters", Physical Review Letters Vol. 109, Iss. 7, 070503, DOI 10.1103/PhysRevLett.109.070503, August 2012, <https://journals.aps.org/prl/abstract/10.1103/

PhysRevLett.109.070503>.

[Hensen15] Hensen, B., Bernien, H., Dréau, A.E., Reiserer, A., Kalb, N., Blok, M.S., Ruitenberg, J., Vermeulen, R.F.L., Schouten, R.N., Abellán, C., Amaya, W., Pruneri, V., Mitchell, M.W., Markham, M., Twitchen, D.J., Elkouss, D., Wehner, S., Taminiau, T.H., and R. Hanson, "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres", Nature Vol. 526, pp. 682-686, DOI 10.1038/nature15759, October 2015, <https://www.nature.com/articles/nature15759>.

[Jiang09] Jiang, L., Taylor, J.M., Nemoto, K., Munro, W.J., Van Meter, R., and M.D. Lukin, "Quantum repeater with encoding", Physical Review A Vol. 79, Iss. 3, 032325, DOI 10.1103/PhysRevA.79.032325, March 2009, <https://journals.aps.org/pra/abstract/10.1103/PhysRevA.79.032325>.

[Joshi20] Joshi, S.K., Aktas, D., Wengerowsky, S., Lončarić, M., Neumann, S.P., Liu, B., Scheidl, T., Currás-Lorenzo, G., Samec, Z., Kling, L., Qiu, A., Razavi, M., Stipčević, M., Rarity, J.G., and R. Ursin, "A trusted node-free eight-user metropolitan quantum communication network", Science Advances Vol. 6, no. 36, eaba0959, DOI 10.1126/sciadv.aba0959, September 2020, <https://www.science.org/doi/10.1126/sciadv.aba0959>.

[Kimble08] Kimble, H.J., "The quantum internet", Nature Vol. 453, Iss. 7198, pp. 1023-1030, DOI 10.1038/nature07127, June 2008, <https://www.nature.com/articles/nature07127>.

[Komar14] Kómár, P., Kessler, E.M., Bishof, M., Jiang, L., Sørensen, A.S., Ye, J., and M.D. Lukin, "A quantum network of clocks", Nature Physics Vol. 10, Iss. 8, pp. 582-587, DOI 10.1038/nphys3000, June 2014, <https://www.nature.com/articles/nphys3000>.

[Meignant19] Meignant, C., Markham, D., and F. Grosshans, "Distributing graph states over arbitrary quantum networks", Physical Review A Vol. 100, Iss. 5, 052333, DOI 10.1103/PhysRevA.100.052333, November 2019, <https://journals.aps.org/pra/abstract/10.1103/PhysRevA.100.052333>.

[Moehring07] Moehring, D.L., Maunz, P., Olmschenk, S., Younge, K.C., Matsukevich, D.N., Duan, L.-M., and C. Monroe, "Entanglement of single-atom quantum bits at a distance", Nature Vol. 449, Iss. 7158, pp. 68-71, DOI 10.1038/nature06118, September 2007, <https://www.nature.com/articles/nature06118>.

[Mural16] Muralidharan, S., Li, L., Kim, J., Lütkenhaus, N., Lukin, M.D., and L. Jiang, "Optimal architectures for long

distance quantum communication", Scientific Reports Vol. 6, pp. 1-10, DOI 10.1038/srep20463, February 2016, <https://www.nature.com/articles/srep20463>.

[Murta20] Murta, G., Grasselli, F., Kampermann, H., and D. Bruß, "Quantum Conference Key Agreement: A Review", Advanced Quantum Technologies Vol. 3, Iss. 11, 2000025, DOI 10.1002/qute.202000025, September 2020, <https://onlinelibrary.wiley.com/doi/10.1002/qute.202000025>.

[Nagayama16] Nagayama, S., Choi, B.-S., Devitt, S., Suzuki, S., and R. Van Meter, "Interoperability in encoded quantum repeater networks", Physical Review A Vol. 93, Iss. 4, 042338, DOI 10.1103/PhysRevA.93.042338, April 2016, <https://journals.aps.org/pra/abstract/10.1103/PhysRevA.93.042338>.

[Nagayama21] Nagayama, S., "Towards End-to-End Error Management for a Quantum Internet", arXiv 2112.07185, DOI 10.48550/arXiv.2112.07185, December 2021, <https://arxiv.org/abs/2112.07185>.

[NielsenChuang] Nielsen, M.A. and I.L. Chuang, "Quantum Computation and Quantum Information", Cambridge University Press, 2010, <http://mmrc.amss.cas.cn/tlb/201702/W020170224608149940643.pdf>.

[Park70] Park, J.L., "The concept of transition in quantum mechanics", Foundations of Physics Vol. 1, Iss. 1, pp. 23-33, DOI 10.1007/BF00708652, March 1970, <https://link.springer.com/article/10.1007/BF00708652>.

[Peev09] Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., Debuisschert, T., Diamanti, E., Dianati, M., Dynes, J.F., Fasel, S., Fossier, S., Fürst, M., Gautier, J.-D., Gay, O., Gisin, N., Grangier, P., Happe, A., Hasani, Y., Hentschel, M., Hübel, H., Humer, G., Länger, T., Legré, M., Lieger, R., Lodewyck, J., Lorünser, T., Lütkenhaus, N., Marhold, A., Matyus, T., Maurhart, O., Monat, L., Nauerth, S., Page, J.-B., Poppe, A., Querasser, E., Ribordy, G., Robyr, S., Salvail, L., Sharpe, A.W., Shields, A.J., Stucki, D., Suda, M., Tamas, C., Themel, T., Thew, R.T., Thoma, Y., Treiber, A., Trinkler, P., Tualle-Brouri, R., Vannel, F., Walenta, N., Weier, H., Weinfurter, H., Wimberger, I., Yuan, Z.L., Zbinden, H., and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna", New Journal of Physics Vol. 11, Iss. 7, 075001, DOI 10.1088/1367-2630/11/7/075001, July 2009, <https://iopscience.iop.org/article/10.1088/1367-2630/11/7/075001>.

[Pompili21.1]
Pompili, M., Hermans, S.L.N., Baier, S., Beukers, H.K.C., Humphreys, P.C., Schouten, R.N., Vermeulen, R.F.L., Tiggelman, M.J., dos Santos Martins, L., Dirkse, B., Wehner, S., and R. Hanson, "Realization of a multinode quantum network of remote solid-state qubits", Science Vol. 372, No. 6539, pp. 259-264, DOI 10.1126/science.abg1919, April 2021, <https://www.science.org/doi/10.1126/science.abg1919>.

[Pompili21.2]
Pompili, M., Delle Donne, C., te Raa, I., van der Vecht, B., Skrzypczyk, M., Ferreira, G., de Kluijver, L., Stolk, A.J., Hermans, S.L.N., Pawełczak, P., Kozlowski, W., Hanson, R., and S. Wehner, "Experimental demonstration of entanglement delivery using a quantum network stack", npj Quantum Information Vol. 8, 121, DOI 10.4121/16912522, October 2022, <https://www.nature.com/articles/s41534-022-00631-2>.

[QI-Scenarios]
Wang, C., Rahman, A., Li, R., Aelmans, M., and K. Chakraborty, "Application Scenarios for the Quantum Internet", Work in Progress, Internet-Draft, draft-irtf-qirg-quantum-internet-use-cases-15, 10 March 2023, <https://datatracker.ietf.org/doc/html/draft-irtf-qirg-quantum-internet-use-cases-15>.

[Qin17] Qin, H. and Y. Dai, "Dynamic quantum secret sharing by using d-dimensional GHZ state", Quantum information processing Vol. 16, Iss. 3, 64, DOI 10.1007/s11128-017-1525-y, January 2017, <https://link.springer.com/article/10.1007/s11128-017-1525-y>.

[QKD] "Quantum Key Distribution", Quantum Network Explorer by QuTech, 2023, <https://www.quantum-network.com/applications/5/>.

[RFC1958] Carpenter, B., Ed., "Architectural Principles of the Internet", RFC 1958, DOI 10.17487/RFC1958, June 1996, <https://www.rfc-editor.org/info/rfc1958>.

[Sangouard11]
Sangouard, N., Simon, C., de Riedmatten, H., and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics", Reviews of Modern Physics Vol. 83, Iss. 1, pp. 33-80, DOI 10.1103/RevModPhys.83.33, March 2011, <https://journals.aps.org/rmp/abstract/10.1103/RevModPhys.83.33>.

[Satoh17] Satoh, T., Nagayama, S., Oka, T., and R. Van Meter, "The network impact of hijacking a quantum repeater", Quantum Science and Technology Vol. 3, Iss. 3, 034008, DOI 10.1088/2058-9565/aac11f, May 2018, <https://iopscience.iop.org/article/10.1088/2058-9565/

aac11f>.

[Satoh20] Satoh, T., Nagayama, S., Suzuki, S., Matsuo, T., Hajdušek, M., and R. Van Meter, "Attacking the Quantum Internet", IEEE Transactions on Quantum Engineering, vol. 2, pp. 1-17, DOI 10.1109/TQE.2021.3094983, September 2021, <https://ieeexplore.ieee.org/document/9477172>.

[SutorBook] Sutor, R.S., "Dancing with Qubits", Packt Publishing, November 2019, <https://www.packtpub.com/product/dancing-with-qubits/9781838827366>.

[Tang19] Tang, B.-Y., Liu, B., Zhai, Y.-P., Wu, C.-Q., and W.-R. Yu, "High-speed and Large-scale Privacy Amplification Scheme for Quantum Key Distribution", Scientific Reports Vol. 9, DOI 10.1038/s41598-019-50290-1, October 2019, <https://www.nature.com/articles/s41598-019-50290-1>.

[Teleportation] "State teleportation", Quantum Network Explorer by QuTech, 2023, <https://www.quantum-network.com/applications/1/>.

[Terhal04] Terhal, B.M., "Is entanglement monogamous?", IBM Journal of Research and Development Vol. 48, Iss. 1, pp. 71-78, DOI 10.1147/rd.481.0071, January 2004, <https://ieeexplore.ieee.org/document/5388928>.

[VanMeter13.1] Van Meter, R. and J. Touch, "Designing quantum repeater networks", IEEE Communications Magazine Vol. 51, Iss. 8, pp. 64-71, DOI 10.1109/MCOM.2013.6576340, August 2013, <https://ieeexplore.ieee.org/document/6576340>.

[VanMeter13.2] Van Meter, R., Satoh, T., Ladd, T.D., Munro, W.J., and K. Nemoto, "Path selection for quantum repeater networks", Networking Science Vol. 3, Iss. 1-4, pp. 82-95, DOI 10.1007/s13119-013-0026-2, December 2013, <https://link.springer.com/article/10.1007/s13119-013-0026-2>.

[VanMeterBook] Van Meter, R., "Quantum Networking", ISTE Ltd/John Wiley and Sons. Inc., Print ISBN 978-1-84821-537-5, DOI 10.1002/9781118648919, April 2014, <https://onlinelibrary.wiley.com/doi/book/10.1002/9781118648919>.

[Wang21] Wang, L.-J., Zhang, K.-Y., Wang, J.-Y., Cheng, J., Yang, Y.-H., Tang, S.-B., Yan, D., Tang, Y.-L., Liu, Z., Yu, Y., Zhang, Q., and J.-W. Pan, "Experimental authentication of quantum key distribution with post-quantum cryptography", npj Quantum Information Vol. 7, pp. 1-7, DOI 10.1038/s41534-021-00400-7, May 2021, <https://www.nature.com/articles/s41534-021-00400-7>.

[Wehner18] Wehner, S., Elkouss, D., and R. Hanson, "Quantum internet: A vision for the road ahead", Science Vol. 362, Iss. 6412, DOI 10.1126/science.aam9288, October 2018, <https://www.science.org/doi/full/10.1126/science.aam9288>.

[Wei22] Wei, S.-H., Jing, B., Zhang, X.-Y., Liao, J.-Y., Yuan, C.-Z., Fan, B.-Y., Lyu, C., Zhou, D.-L., Wang, Y., Deng, G.-W., Song, H.-Z., Oblak, D., Guo, G.-C., and Q. Zhou, "Towards Real-World Quantum Networks: A Review", Laser and Photonics Reviews Vol. 16, 2100219, DOI 10.1002/lpor.202100219, January 2022, <https://onlinelibrary.wiley.com/doi/10.1002/lpor.202100219>.

[Wootters82] Wootters, W.K. and W.H. Zurek, "A single quantum cannot be cloned", Nature Vol. 299, Iss. 5886, pp. 802-803, DOI 10.1038/299802a0, October 1982, <https://www.nature.com/articles/299802a0>.

[ZOO] "The Quantum Protocol Zoo", November 2019, <https://wiki.veriqloud.fr/>.

Acknowledgements

The authors want to thank Carlo Delle Donne, Matthew Skrzypczyk, Axel Dahlberg, Mathias van den Bossche, Patrick Gelard, Chonggang Wang, Scott Fluhrer, Joey Salazar, Joseph Touch, and the rest of the QIRG community as a whole for their very useful reviews and comments on this document.

WK and SW acknowledge funding received from the EU Flagship on Quantum Technologies, Quantum Internet Alliance (No. 820445).

rdv acknowledges support by the Air Force Office of Scientific Research under award number FA2386-19-1-4038.

Authors' Addresses

Wojciech Kozlowski
QuTech
Building 22
Lorentzweg 1
2628 CJ Delft
Netherlands
Email: w.kozlowski@tudelft.nl

Stephanie Wehner
QuTech
Building 22
Lorentzweg 1
2628 CJ Delft
Netherlands

Email: s.d.c.wehner@tudelft.nl

Rodney Van Meter
Keio University
5322 Endo, Fujisawa, Kanagawa
252-0882
Japan
Email: rdv@sfc.wide.ad.jp

Bruno Rijsman
Individual
Email: brunorijsman@gmail.com

Angela Sara Cacciapuoti
University of Naples Federico II
Department of Electrical Engineering and Information Technologies
Claudio 21
80125 Naples
Italy
Email: angelasara.cacciapuoti@unina.it

Marcello Caleffi
University of Naples Federico II
Department of Electrical Engineering and Information Technologies
Claudio 21
80125 Naples
Italy
Email: marcello.caleffi@unina.it

Shota Nagayama
Mercari, Inc.
Roppongi Hills Mori Tower 18F
6-10-1 Roppongi, Minato-ku, Tokyo
106-6118
Japan
Email: shota.nagayama@mercari.com