REVIEW

QUANTUM INFORMATION

Quantum internet: A vision for the road ahead

Stephanie Wehner[1]*, David Elkouss[1], Ronald Hanson[1,2]

The internet—a vast network that enables simultaneous long-range classical communication—has had a revolutionary impact on our world. The vision of a quantum internet is to fundamentally enhance internet technology by enabling quantum communication between any two points on Earth. Such a quantum internet may operate in parallel to the internet that we have today and connect quantum processors in order to achieve capabilities that are provably impossible by using only classical means. Here, we propose stages of development toward a full-blown quantum internet and highlight experimental and theoretical progress needed to attain them.

The purpose of a quantum internet is to enable applications that are fundamentally out of reach for the classical internet. A quantum internet could thereby supplement the internet we have today by using quantum communication, but some researchers go further and believe all communication will eventually be done over quantum channels (1). The best-known application of a quantum internet is quantum key distribution (QKD), which enables two remote network nodes to establish an encryption key whose security relies only on the laws of quantum mechanics. This is impossible with the classical internet. A quantum internet, however, has many other applications (Fig. 1) that bring advantages that are unattainable with a classical network. Such applications include secure access to remote quantum computers (2), more accurate clock synchronization (3), and scientific applications such as combining light from distant telescopes to improve observations (4). As the development of a quantum internet progresses, other useful applications will likely be discovered in the next decade.

Central to all these applications is that a quantum internet enables us to transmit quantum bits (qubits), which are fundamentally different from classical bits. Classical bits can take only two values, 0 or 1, whereas qubits can be in a superposition of 0 and 1 at the same time. Importantly, qubits cannot be copied, and any attempt to do so can be detected. It is this feature that makes qubits naturally well suited for security applications but at the same time makes transmitting qubits over long distances a truly formidable endeavor. Because qubits cannot be copied or amplified, repetition or signal amplification are ruled out as a means to overcome imperfections, and a radically new technological development—such as quantum repeaters—is needed in order to build a quantum internet (Figs. 2 and 3) (5).

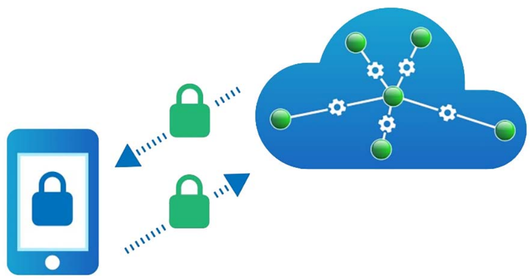

Fig. 1. Applications of a quantum internet. One application of a quantum internet is to allow secure access to remote quantum computers in the cloud (2). Specifically, a simple quantum terminal capable of preparing and measuring only single qubits can use a quantum internet to access a remote quantum computer in such a way that the quantum computer can learn nothing about which computation it has performed. Almost all other applications of a quantum internet can be understood from two special features of quantum entanglement. First, if two qubits at different network nodes are entangled with each other, then such entanglement enables stronger than classical correlation and coordination. For example, for any measurement on qubit 1, if we made the same measurement on qubit 2, then we instantaneously obtain the same answer, even though that answer is random and was not determined ahead of time. Very roughly, it is this feature that makes entanglement so well suited for tasks that require coordination. Examples include clock synchronization (3), leader election, and achieving consensus about data (53), or even using entanglement to help two online bridge players coordinate their actions (39). The second feature of quantum entanglement is that it cannot be shared. If two qubits are maximally entangled with each other, then it is impossible by the laws of quantum mechanics for a third qubit to be just as entangled with either of them. This makes entanglement inherently private, bringing great advantages to tasks that require security such as generating encryption keys (12) or secure identification (24, 25).

We are now at an exciting moment in time, akin to the eve of the classical internet. In late 1969, the first message was sent over the nascent four-node network that was then still referred to as the Advanced Research Projects Agency Network (ARPANET). Recent technological progress (6–9) now suggests that we may see the first small-scale implementations of quantum networks within the next 5 years.

At first glance, realizing a quantum internet (Fig. 3) may seem even more difficult than building a large-scale quantum computer. After all, we might imagine that in full analogy to the classical internet, the ultimate version of a quantum internet consists of fully fledged quantum computers that can exchange an essentially arbitrary number of qubits. Thankfully, it turns out that many quantum network protocols do not require large quantum computers to be realized; a quantum device with a single qubit at the end point is already sufficient for many applications. What's more, errors in quantum internet protocols can often be dealt with by using classical rather than quantum error correction, imposing fewer demands on the control and quality of the qubits than is the case for a fully fledged quantum computer. The reason why quantum internet protocols can outperform classical communication with such relatively modest resources is because their advantages rely solely on inherently quantum properties such as quantum entanglement, which can be exploited already with very few qubits. By contrast, a quantum computer must feature more qubits than can be simulated on a classical computer in order to offer a computational advantage. Given the challenges posed by the development of a quantum internet, it is useful to reflect on what capabilities are needed to achieve specific quantum applications and what technology is required to realize them.

Here, we propose stages of development toward a full-blown quantum internet. These stages are functionality driven: Central to their definition is not the difficulty of experimentally achieving them but rather the essential question of what level of complexity is needed to actually enable useful applications. Each stage is interesting in its own right and distinguished by a specific quantum functionality that is sufficient to support a certain class of protocols. To illustrate this, for each stage we give examples of known application protocols in which a quantum internet is already known to bring advantages.

[1] QuTech, Delft University of Technology, Post Office Box 5046, 2600 GA Delft, Netherlands. [2] Kavli Institute of Nanoscience, Delft University of Technology, Post Office Box 5046, 2600 GA Delft, Netherlands.
*Corresponding author. Email: s.d.c.wehner@tudelft.nl

Realizing a quantum internet demands substantial development to realize quantum repeaters as well as end nodes (Figs. 2 and 3). It is clear that in the short term, one may optimize both repeaters and end nodes relatively independently. That is, one can imagine a quantum internet that uses relatively simple end nodes while using repeaters powerful enough to cover larger distances. Similarly, a near-term quantum internet may be optimized for shorter—for example, pan-European—distances, while using much more powerful end nodes capable of realizing a larger set of protocols. Ideally, these designs would ensure forward compatibility to achieve the ultimate goal of a full-blown worldwide quantum internet. Although the quantum repeaters, which enable communication between distant end nodes, need to be able to support the functionality of each stage, an application-centric view makes no other statements regarding their capabilities.

Last, we discuss progress toward implementing a quantum internet, which poses substantial challenges to physics, engineering, and computer science.

Stages of functionality and applications

Let us formulate the functionality-driven stages of quantum internet development. Each successive stage is distinguished by an increasing amount of functionality, at the expense of increasing experimental difficulty. We say that an experimental implementation has reached a certain stage only if the functionality of that stage and all previous stages (Fig. 4) is available to all the end nodes using the network.

Crucial to the distinction between the stages is that the subsequent stage offers a fundamentally new functionality not available in the previous one rather than simply improving parameters or offering "more of the same" by increasing the number of qubits. For the sake of clarity, the stages and tests described below target systems that prepare and transmit qubits, but it is also possible to phrase both in terms of qudits (higher-dimensional quantum systems) or continuous variables. For each stage, we describe some of the application protocols that are already known and that can be realized with the functionality provided in that stage (Table 1). It is conceivable that a simpler protocol, or better theoretical analysis, may be found in the future that solves the same task but is less demanding in terms of functionality. In parallel to the daunting experimental challenges in making quantum internet a reality, there is thus a challenge for quantum software developers to design protocols that can realize a task in a stage that can be implemented more easily. We identify relevant parameters for each stage to establish a common language between hardware and software developers. These parameters can be estimated by using a series of simple tests, allowing us to certify the performance of an experimental implementation in attaining a specific stage, as well as the performance of protocols depending on these parameters.

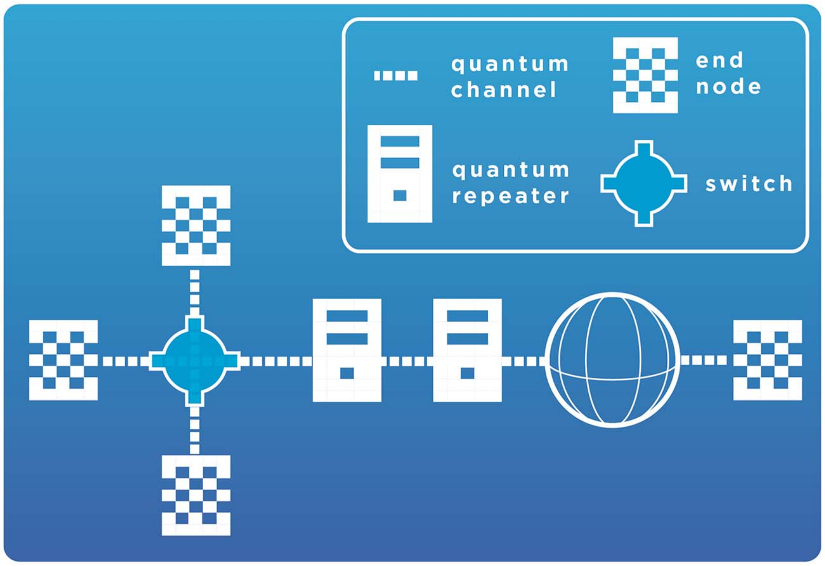

Fig. 2. A quantum internet consists of three essential quantum hardware elements. First, we need a physical connection (quantum channel) that supports the transmission of qubits. Examples are standard telecom fibers because they are presently used to communicate classical light. Second, we need a means to extend these short distances. Quantum channels are inherently lossy. For instance, the transmissivity of fiber optical channels scales exponentially with distance. This scaling has strong implications for applications because for both entanglement and key distribution, the achievable rates can at most be proportional to the transmissivity (106, 107). Hence, in order to reach longer distances, intermediate nodes called quantum repeaters are necessary [(97, 108–110), and (91, 92), reviews]. Such a repeater is placed at certain intervals along the optical fiber connection, in theory allowing qubits to be transmitted over arbitrarily long distances. In the future, powerful repeaters may also double as long-distance routers in a quantum network. The final element are the end nodes—that is, the quantum processors connected to the quantum internet. These may range from extremely simple nodes that can only prepare and measure single qubits to large-scale quantum computers. End nodes may themselves act as quantum repeaters, although this is not a requirement. A quantum internet is not meant to replace classical communication but rather to supplement it with quantum communication. We hence assume all nodes can communicate classically—for example, over the classical internet—in order to exchange control information.

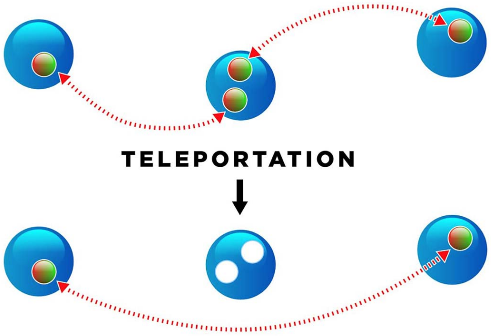

Fig. 3. Quantum repeaters work in a fundamentally different way from classical repeaters. Quantum repeaters are used to transmit quantum information over long distances. In its simplest form, a quantum repeater works by first generating entanglement (dashed line) between the repeater (middle) and each of the end nodes (left and right) individually. Intuitively, this can be done because the distance of each end point to the repeater is still sufficiently small to allow direct entanglement generation by transmitting photons over telecom fiber. Subsequently, the repeater teleports one of the qubits entangled with node 1 onto node 2. This procedure is known as entanglement swapping and allows the creation of entanglement over distances at which direct transmission is infeasible. After establishing long-distance entanglement, a data qubit may now be sent by using quantum teleportation.

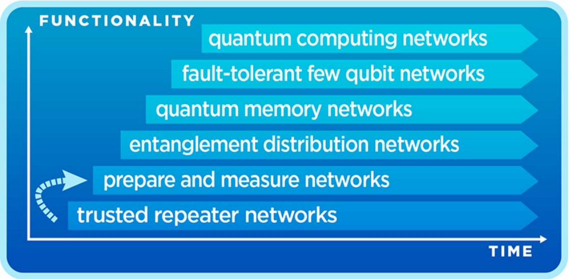
FUNCTIONALITY
quantum computing networks
fault-tolerant few qubit networks
quantum memory networks
entanglement distribution networks
prepare and measure networks
trusted repeater networks
TIME

Fig. 4. Stages of quantum internet development. A specific implementation of a quantum internet may, like for a classical network, be optimized for distance, functionality, or both. The term network commonly refers to a situation that goes beyond point-to-point communication; the objective of a network is to provide any end nodes (connected to the network) with the means to exchange data, making three end nodes the smallest instance of a true network. Outside the laboratory, only trusted repeater networks (first stage) have been realized in metropolitan areas (*62*–*65*). Two single far-away end nodes (*68*) have also been connected via satellite.

So far, most application protocols have only been analyzed for perfect parameters. As such, the exact requirements of many application protocols on these parameters have not yet been determined and deserve future investigation. Although functionality-driven stages make demands on the communication links and quantum repeaters, it will not be important in this section how these links are realized; they may be realized by direct transmission in fiber, by being relayed by any kind of quantum repeater, or even by means of teleportation using preshared entanglement. What matters is that these links can be used to generate the necessary quantum states for a specific stage.

Trusted repeater networks

The first stage differs substantially from the others in the sense that it does not allow the end-to-end transmission of qubits. Nevertheless, from a technological perspective, trusted repeater networks can form an interesting stepping stone toward a quantum internet, spurring infrastructure deployment and engineering developments; depending on the underlying technology, trusted repeaters (*10*) can be upgraded to true quantum repeaters later on.

Specifically, a trusted repeater network (sometimes called a trusted node network) has at least two end nodes and a sequence of short distance links that connect nearby intermediary repeater nodes. Each pair of adjacent nodes uses QKD (*11*–*13*) to exchange encryption keys. These pairwise keys allow the end nodes to generate their own key, provided that all intermediary nodes are trusted (*14*). A first step toward upgrading such networks could be measurement device–independent QKD (*15*–*17*), which is a QKD protocol that is secure even with untrusted measurement devices that can be implemented with standard optical components and sources (*17*); this protocol already incorporates some useful ingredients for later stages, such as two-photon Bell measurements.

Prepare and measure networks

This stage is the first to offer end-to-end quantum functionality. It enables end-to-end QKD without the need to trust intermediary repeater nodes and already allows a host of protocols for other interesting tasks. Informally, this stage allows any node to prepare a one-qubit state and transmit the resulting state to any other node, which then measures it (definition is provided in Table 1). Transmission and measurement are allowed to be post-selected; that is, a signal that the qubit is lost may be generated instead. For instance, the receiving node is allowed to ignore nondetection events and conclude that such qubits are lost. If the sender can prepare an entangled state of two qubits, then this stage also includes the special case in which the sender transmits the first and second qubit to two different nodes in the network (or to another node and itself). Such entanglement distribution is then also post-selected.

Such a post-selected prepare-and-measure functionality is not equivalent to transmitting arbitrary qubits across the network (*18*). The task of transmitting arbitrary qubits demands the ability to transfer an unknown state $|\Psi\rangle$ (which the sender does not know how to prepare) deterministically to the receiver—that is, no post-selection on detection events is allowed.

The classical reader may wonder what is the use of transmitting qubits at all if there is a procedure for the sender to prepare the state $|\Psi\rangle$. After all, we might imagine that the sender simply sends classical instructions for this procedure to the receiver, who then prepares the qubit itself. The difference between such a classical protocol and sending different quantum states $|\Psi\rangle$ directly is that in the latter case, an eavesdropper, or indeed the receiver, cannot make a copy of $|\Psi\rangle$ without disturbing the quantum state. This means that attempts to gain information from $|\Psi\rangle$ by an eavesdropper may be detected, enabling QKD.

Application protocols

This stage is already sufficient to realize protocols for many interesting cryptographic tasks, as long as the probability of loss (p) and the inaccuracies in transmission (ε_T) and measurement (ε_M) (Table 1) are sufficiently low. The most famous of such tasks is QKD, which provides a solution to the task of generating a secure encryption key between two distant end nodes (Alice and Bob) (*11*–*13*). QKD is secure even if the eavesdropper trying to learn the key has access to an arbitrarily large quantum computer with which to attack the protocol, and remains secure at any point in the future, even if such a quantum computer becomes available later on. This is provably impossible when using classical communication. The BB84 QKD (*11*) protocol can be realized by using only single-qubit preparations and measurements tolerating some amount of post-selection p (*19*). For known protocols in this stage, $\varepsilon_T + \varepsilon_M \leq 0.11$ is sufficient and can be estimated by testing for only a small number of states (*20*). In practice, single-qubit preparation can be replaced with attenuated laser pulses, using also decoy-state BB84 to guarantee security (*21*). QKD is commercially available at short distances by using standard telecom fibers (*22*), and a variety of protocols are known [(*23*), survey].

Another class of protocols in this stage is in the domain of two-party cryptography. Here, there is no eavesdropper, but rather Alice and Bob themselves do not trust each other. An example of such a task is secure identification, in which Alice (a potentially impersonating user) may wish to identify herself to Bob (a potentially malicious server or automated teller machine) without revealing her authentication credentials (*24*, *25*). It is known that even by using quantum communication, such tasks cannot be implemented securely without imposing assumptions on the power of the adversary (*26*–*28*). Classical protocols rely on computational assumptions, whose security against an attacker who holds a quantum computer is unclear. Nevertheless, it is possible to achieve provable security for all such relevant tasks by sending more qubits than the adversary can store easily within a short time frame, which is known as the bounded (*29*) or more generally noisy-storage model (*30*, *31*). This assumption only needs to hold during the execution of the protocol, and security is preserved into the future even if the adversary later obtains a better quantum memory. There exist protocols for which it is sufficient to prepare and measure single qubits, in which the sufficient values of p, ε_M, ε_T (Table 1) depend on the storage assumption (*32*).

Other known protocols in this stage include position verification (*33*); weakened forms of two-party cryptographic tasks that can form building blocks, such as imperfect bit commitments (*34*); and coin-flipping (*35*). Here, the requirements in terms of p, ε_M, and ε_T have not been analyzed yet; no task exists for which a full set of necessary and sufficient conditions on these parameters is known.

Entanglement distribution networks

The third stage allows the end-to-end creation of quantum entanglement in a deterministic or heralded fashion, as well as local measurements. The end nodes require no quantum memory for this stage (Table 1).

The term "deterministic entanglement generation" refers to the fact that the process succeeds with (near) unit probability. Heralding is a slightly weaker form of deterministic entanglement generation in which we signal the successful generation of entanglement with an event that is independent of the (immediate) measurement of the