REVIEW SUMMARY

QUANTUM INFORMATION

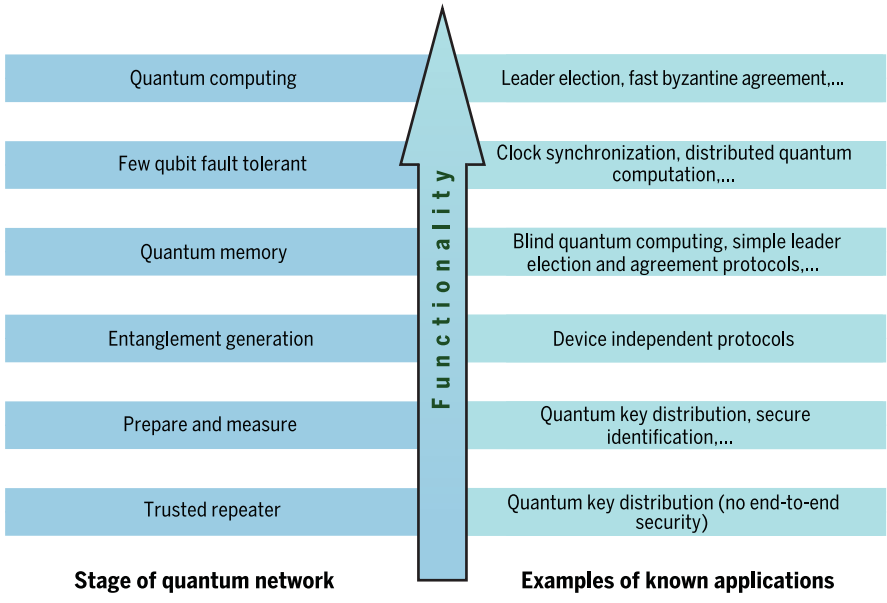
Quantum internet: A vision for the road ahead

Stephanie Wehner*, David Elkouss, Ronald Hanson

BACKGROUND: The internet has had a revolutionary impact on our world. The vision of a quantum internet is to provide fundamentally new internet technology by enabling quantum communication between any two points on Earth. Such a quantum internet will—in synergy with the "classical" internet that we have today—connect quantum information processors in order to achieve unparalleled capabilities that are provably impossible by using only classical information.

As with any radically new technology, it is hard to predict all uses of the future quantum internet. However, several major applications have already been identified, including secure communication, clock synchronization, extending the baseline of telescopes, secure identification, achieving efficient agreement on distributed data, exponential savings in communication, quantum sensor networks, as well as secure access to remote quantum computers in the cloud.

Central to all these applications is the ability of a quantum internet to transmit quantum bits (qubits) that are fundamentally different than classical bits. Whereas classical bits can take only two values, 0 or 1, qubits can be in a superposition of being 0 and 1 at the same time. Moreover, qubits can be entangled with each other, leading to correlations over large distances that are much stronger than is possible with classical information. Qubits also cannot be copied, and any attempt to do so can be detected. This feature makes qubits well suited for security applications but at the same time makes the transmission of qubits require radically new concepts and technology. Rapid experimental progress in recent years has brought first rudimentary quantum networks within reach, highlighting the timeliness and need for a unified framework for quantum internet researchers.



Stages in the development of a quantum internet. Each stage is characterized by an increase in functionality at the expense of greater technological difficulty. This Review provides a clear definition of each stage, including benchmarks and examples of known applications, and provides an overview of the technological progress required to attain these stages.

ADVANCES: We define different stages of development toward a full-blown quantum internet. We expect that this classification will be instrumental in guiding and assessing experimental progress as well as stimulating the development of new applications by providing a common language and reference frame for the different scientific and engineering disciplines involved.

More advanced stages are distinguished by a larger amount of functionality, thus supporting ever more sophisticated application protocols. 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. 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 an opportunity 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. Last, we review technological progress in experimental physics, engineering, and computer science that is required to attain such stages.

ON OUR WEBSITE

Read the full article at http://dx.doi.org/10.1126/science.aam9288

OUTLOOK: Building and scaling quantum networks is a formidable endeavor, requiring sustained and concerted efforts in physics, computer science, and engineering to succeed. The proposed stages of development will facilitate interdisciplinary communication by summarizing what we may actually want to achieve and providing guidelines both to protocol design and software development as well as hardware implementations through experimental physics and engineering. Although it is hard to predict what the exact components of a future quantum internet will be, it is likely that we will see the birth of the first multinode quantum networks in the next few years. This development brings the exciting opportunity to test all the ideas and functionalities that so far only exist on paper and may indeed be the dawn of a future large-scale quantum internet. ■

The list of author affiliations is available in the full article online.
*Corresponding author. Email: s.d.c.wehner@tudelft.nl
Cite this article as S. Wehner *et al.*, *Science* **362**, eaam9288 (2018). DOI: 10.1126/science.aam9288

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*).

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.

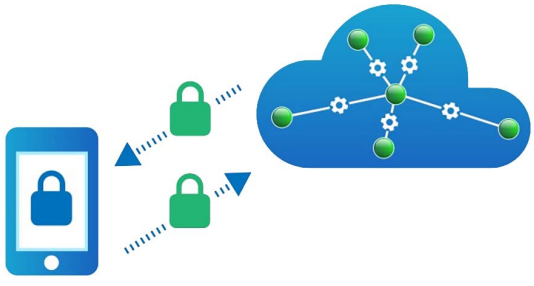


Fig. 1. Applications of a quantum internet. One application of a quantum internet is to allow secure access to remote quantum computers in the cloud (*2*). Specifically, a simple quantum terminal capable of preparing and measuring only single qubits can use a quantum internet to access a remote quantum 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*).

[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.

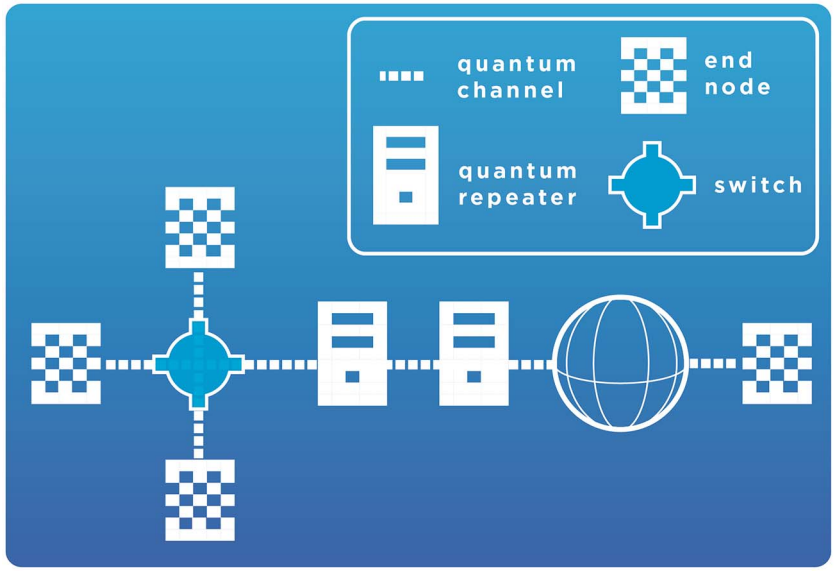


Fig. 2. A quantum internet consists of three essential quantum hardware elements. First, we need a physical connection (quantum channel) that supports the transmission of qubits. Examples are standard telecom fibers because they are presently used to communicate classical light. Second, we need a means 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.

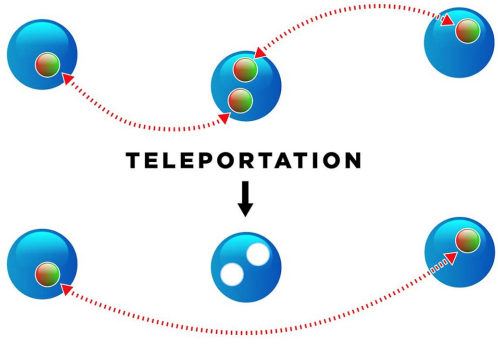


Fig. 3. Quantum repeaters work in a fundamentally different way from classical repeaters. Quantum repeaters are used to transmit quantum information over long distances. In its simplest form, a quantum repeater works by first generating entanglement (dashed line) between the repeater (middle) and each 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.

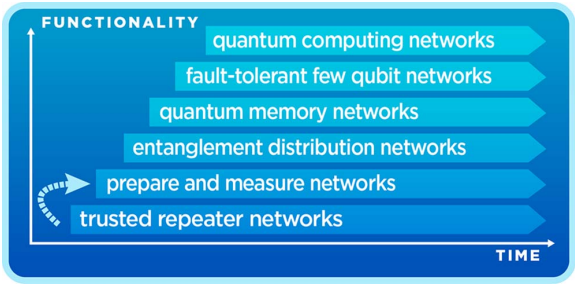


Fig. 4. Stages of quantum internet development. A specific implementation of a quantum internet may, like for a classical network, be optimized for distance, functionality, or both. The term network commonly refers to a situation that goes beyond point-to-point communication; the objective of a network 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

entangled qubits themselves. Here, the generation of entanglement is deterministic, conditioned on such a successful heralding signal. Specifically, this prohibits post-selecting on detection events when measuring the entangled qubits. We remark that this stage also includes networks that allow the generation of multipartite entangled states, followed by immediate measurements, but no memory. However, the generation of multipartite entanglement is not required to attain this stage.

Application protocols

The main advance over the previous stage is that this stage allows the realization of device-independent protocols, in which the quantum devices are largely untrusted. Specifically, the concept of device independence (*36*, *37*) models the end nodes as black boxes, to which we can give classical instructions to perform specific measurements and receive the resulting measurement outcomes. No guarantees are given about the actual quantum state or measurements performed by the device, where the device may even be constructed by the adversary. The classical software used to control such quantum devices is trusted, and it is assumed that the quantum device merely exhibits input/output behavior. In particular, devices can record their inputs and outputs (*38*) but cannot transmit the key back to the adversary. The coordination allowed by entanglement now also in principle allows players to "cheat" an online bridge game (*39*).

Low errors in preparation (ε_P) and measurement (ε_M) as $\varepsilon_P + \varepsilon_M \leq 0.057$ (Table 1) are sufficient to ensure the implementability of device-independent QKD (*36*), in which necessary and sufficient conditions for the parameters to implement general tasks in this stage are unknown.

Quantum memory networks

The fourth stage is distinguished by the capability of the end nodes to have local memory while simultaneously allowing universal local control (Table 1). This allows the implementation of much more complex protocols that require temporary storage of a quantum state during further quantum or classical communication. Examples include protocols for solving distributed systems tasks. This stage also implies the ability to perform entanglement distillation and generate multipartite entangled states from bipartite entanglement by exploiting the ability for local memory and control. A crucial difference between this stage and the previous one is that we are now able to transfer

Table 1. Formal definitions of the stages, parameters for protocol design, and classification of known protocols. Higher stages include all functionality available at the previous ones. It is an open question to determine necessary and sufficient conditions for these parameters to realize general protocols. In the future, quantum network programmers may be able to find protocols for the same tasks that can be realized with lower stages of a quantum internet. It is an interesting open question what minimum stage is required in order to realize a specific task.

Stage	Additional functionality	Parameters	Example protocols
Prepare and measure	For any two end nodes i, j, any one qubit state $\|\Psi\rangle$ and any one qubit projective measurement M, there exists a way for i to prepare $\|\Psi\rangle$, transfer it to j, so that either (i) j performs measurement M on $\|\Psi\rangle$ or (ii) j concludes the qubit was lost.	Distances ε_T and ε_M from the ideal transmission and measurement operations (Box 1). Probability p that the state is not lost.	QKD, Two-party cryptography, position verification, imperfect coin flipping
Entanglement distribution	For any two end nodes i, j, (i) the network allows the heralded creation of a maximally entangled state $\|\Phi_{ij}\rangle$ and (ii) nodes i and j can deterministically perform any single-qubit measurements M_i and M_j.	Distances ε_P from the ideal preparation, and ε_M from the idealized measurement (Box 1).	Device independence for QKD and other protocols in the prepare and measure stage
Quantum memory	For any two end nodes i, j, the network allows the execution entanglement generation and the following additional tasks in any order: (i) preparation of a one qubit ancilla state $\|\Psi\rangle$ by end node i or j, (ii) measurements of any subset of the qubits at node, and (iii) application of an arbitrary unitary U at node. Storage of the qubits for a minimum time $k \cdot C_m \cdot t$, where t is defined as the time that is required to generate one Einstein–Podolsky–Rosen (EPR) pair and send a classical message from node i to j maximized over all pairs of nodes, and C_m is the time that it takes for the execution of a depth m quantum circuit at the end node.	Number of rounds k, circuit depth m, number of physical qubits q. For each of the operations, an estimate ε_j from the ideal operation (Box 1).	Blind quantum computing (using remote quantum servers), improved coin flipping, anonymous quantum transmissions, extending baseline of telescopes, secret sharing, simple leader election and agreement protocols, and time-limited clock synchronization
Few-qubit fault-tolerant	Fault-tolerant execution of a universal gate set on q logical qubits, where $q \geq 1$ is small enough such that the local processor can efficiently be simulated on a classical computer.	Number of logical qubits q	Clock synchronization and distributed quantum computation
Quantum computing	q is larger than the number of qubits that can effectively be simulated on a classical computer.	Number of logical qubits q	Leader election, fast byzantine agreement, and weak coin flipping with arbitrarily small bias

unknown qubits from one network node to another—for example, by performing deterministic teleportation. This capability is not guaranteed in the previous stage: Technology that can be used to deterministically relay qubits over long distances by means of large-scale quantum error correction implies the technological capability of realizing a good local quantum memory. We emphasize that a quantum memory network does not require operations to be performed with an accuracy that would be above threshold for fault-tolerant computation.

An important parameter in application protocols is the number of communication rounds k (Table 1), the number of times information is sent back and forth between two end nodes during the course of the protocol. In order to realize useful application protocols, the storage time t thus needs to be compared with the communication time in the network instead of an absolute time. This means that networks of nodes that are far apart do in fact need to exhibit longer memory times in order to attain this stage, and the quality of the memory is time dependent. That this time t is related to the maximum time that it takes any two nodes to communicate is because a stage is attained only if the functionality is available to any two nodes in the network, even the two that are farthest apart.

Application protocols

The availability of quantum memories and the deterministic transmission of qubits opens up many new protocols in this stage. We start with cryptographic tasks: To allow clients to make use of these computers securely—that is, without revealing the nature or outcome of their computation—it is possible to perform secure assisted quantum computation (*40*), or blind quantum computation (*2*, *41*). Here, a simple quantum device capable of preparing and measuring single qubits is sufficient to perform a computation on a large-scale quantum computer so that the quantum computer cannot gain information about the program and result. That we need one large-scale quantum computer does not imply that a quantum computing network (the highest stage) is required to run such protocols; we only need a quantum internet that allows a client to communicate with the computing server. A network attains a specific stage only if the functionality is available to all nodes.

Other cryptographic tasks in this domain are tools such as protocols for the sharing of classical (*42*) or quantum (*43*) secrets, including verifiable secret-sharing schemes (*44*) and anonymous transmissions (*45*). Evidently, the number of qubits determines the size of the secrets or qubits transmitted, but no fault tolerance is in principle required.

This stage also opens the door to interesting applications outside the domain of cryptography. For example, proposals exist for exploiting long-distance entanglement to extend the baseline of telescopes (*4*), for basic forms of leader election (*46*), and for improving the synchronization of clocks (*3*). Depending on the demands made on such synchronization, the proposed protocols could be realized with quantum memory or few-qubit fault-tolerant networks.

Necessary and sufficient parameter requirements for solving the above mentioned tasks are not yet known in general. It is also conceivable that an improved analysis considering whether deterministic qubit delivery is really necessary, or whether maybe post-selected transmission of qubits is enough, can push some of the protocols above to a lower stage. Initial results for blind quantum computation indicates that this might indeed be the case (*47*).

Few-qubit fault-tolerant networks

The next stage differs by demanding that the local operations can be performed fault-tolerantly, which is considerably more challenging. Fault tolerance is not necessary for many known quantum internet protocols, but fault-tolerant operations being available would allow the execution of local quantum computation of high circuit depth as well as an (in theory) arbitrary extension of storage times to execute protocols with an arbitrary number of rounds of communication.

The term "few qubits" here refers to the fact that the number of qubits available is still small enough so that the end nodes themselves can be simulated effectively on a classical computer. This does not imply that the entire network can be simulated efficiently or that there would exist equivalent classical protocols; the effects of entanglement cannot generally be replicated classically.

Here, we are only interested in the performance of the fault-tolerant scheme, not how it is realized. Fault tolerance implies that all error parameters (Table 1) of a quantum memory network can be made negligible by adding more resources. As a guideline to relevant experimental parameters, we refer to works in distributed quantum computing (*48*).

Application protocols

Having access to fault-tolerant gates allows higher-accuracy clock synchronization (*3*) and protocols that require many rounds of communication and high circuit depth to be useful. This includes distributed quantum computing as well as applications for full-scale quantum computing networks, restricted to few qubits. This could be of great practical interest, especially for applications in the domain of distributed systems, but as with the implementation of quantum algorithms on quantum computers, the power of having only a limited number of qubits at our disposal is an important subject of investigation.

Quantum computing networks

The final stage consists of quantum computers that can arbitrarily exchange quantum communication. In some sense, it breaks with our paradigm that the next stage is not "more of the same." However, in this case, we really do gain a new ability: finding solutions to computational problems that can no longer be found efficiently on classical computers.

Application protocols

It is clear that this ultimate stage of a quantum internet allows in principle all protocols to be realized. Small-scale versions of the protocols below can also be realized in the few-qubit fault-tolerant stage, and further development may yield more sophisticated protocols and analysis that places them in lower stages.

First, we again focus on cryptography. In this stage, it is possible to perform coin flipping with an arbitrarily small bias (*49*, *50*). We can also solve genuinely quantum tasks, such as secure multiparty quantum computation, which forms an extension of classical secure function evaluation to the quantum regime. Classically, this means that node j holds an input string x_j, and all

Box 1. Performance of quantum internet protocols.

A general quantum internet protocol is composed of a series of operations consisting of state preparation, transmission, unitary operations, and measurements. In reality, each of these operations is noisy, so instead of executing a sequence of ℓ ideal operations $\mathcal{J} = \mathcal{J}_\ell \circ \ldots \circ \mathcal{J}_1$, we are executing the real (noisy) protocol $\mathcal{R} = \mathcal{R}_\ell \circ \ldots \circ \mathcal{R}_1$. To assess the performance of the real protocol execution, it is sufficient to estimate the diamond norm distance (*20*)

$$D_\diamond(\mathcal{R}, \mathcal{J}) = \max_{\rho_{SE}} D[\mathcal{R} \otimes \mathrm{id}_E(\rho_{SE}), \mathcal{J} \otimes \mathrm{id}_E(\rho_{SE})]$$

where $D(\tau, \sigma)$ is the well-known trace distance (*18*) that determines how well two states τ and σ can be distinguished by any physical process, and S denotes the system that the protocol acts on which may be part of a larger system SE. Because $D_\diamond$ is (unlike the fidelity) a metric, it is straightforward to show that having estimated individual errors $\|\mathcal{R}_j - \mathcal{J}_j\|_\diamond \leq \varepsilon$ allows an estimate of the overall error as

$$D_\diamond(\mathcal{R}, \mathcal{J}) \leq \ell \cdot \varepsilon$$

For unitary operations and projective measurements, the diamond norm distance is directly related to the average gate fidelity (*111*). If the ideal operation $\mathcal{J}(\rho) = \Phi$ simply aims to prepare a state Φ, and the real operation prepares $\mathcal{R}(\rho) = \tilde{\Phi}$, then the diamond norm distance satisfies $D_\diamond(\mathcal{R}, \mathcal{J}) \leq \sqrt{1 - F(\Phi, \tilde{\Phi})}$, where F is the fidelity. Evidently, the end-user—who desires to run application protocols—should be able to perform tests that give confidence for any possible operation instead of having to test the exact unitaries and measurements in any conceivable protocol.

n nodes jointly want to compute $y = f(x_1, ..., x_n)$. The goal is that malicious nodes cannot infer anything more about the inputs x_j of the honest nodes than they can by observing the output y. An example of such a problem is secure voting, in which $x_j \in \{0, 1\}$ corresponds to the choice one of two possible candidates, and f is the majority function. The quantum version of this primitive (*51*) allows each party to hold a quantum state $|\Psi_j\rangle$ as input, and the parties jointly wish to compute a quantum operation U.

Next, we focus on distributed systems, which are formed when several computing devices are connected, sometimes colloquially referred to as a cloud. Many challenges arise in the coordination and control of such systems that may be less familiar to a physicist. As a very simple example, consider a bank transaction being recorded redundantly on several backup servers. If one or more of the backup servers fail during the update, then they may later show inconsistent data (for example, $1 million versus $0). Tool protocols for achieving consensus between processors are widely deployed in practice—for example, in Google's Chubby system (*52*). Outside the domain of the internet itself, examples include the reliability in smart grids, flight control systems, and sensor arrays.

Although this area is presently much less developed in the quantum domain (*53*), several protocols are known that show that a quantum internet has great potential for solving the problems in distributed systems much more efficiently than what is possible classically. Very intuitively, the reason why quantum communication could help solve these problems is that entanglement allows coordination among distant processors that greatly surpasses what is possible classically. It is this that yields advantages for distributed systems tasks such as consensus and agreement. One of the most striking examples of a quantum advantage in distributed systems can be found for the task of byzantine agreement. Here, the goal is to allow n processors to agree on a common bit, while some fraction of them may be faulty. The term "byzantine" refers to the very demanding model of arbitrarily correlated faults, in which the faulty processors essentially collude to thwart the protocol. In (*54*), it is shown that in some regimes, there exists a quantum protocol to solve this task by using only a constant number of rounds of quantum communication, while the amount of classical communication scales as $O(\sqrt{n}/\log n)$, where n is the number of processors. The protocol given in (*54*) requires many qubits, thus demanding the final stage of a quantum internet. The objective of leader election is to elect a distinct leader from a number of distributed processors, which is an important tool, for example, for deciding which processor gets to use a particular resource. This task is particularly challenging in an anonymous network, in which no node has an identifier. In this setting, there is no exact classical algorithm for leader election for general network topologies, whereas quantumly, leader election is possible (*55*). The protocol proposed in (*55*) requires each end node to process a number of qubits that scales with the number of processors (end nodes). To be used in networks of reasonable size, we thus require a quantum computing network. A number of other leader-election protocols have been proposed in a variety of models (*56*, *57*).

Last, this stage allows distributed computational tasks to be solved by transmitting in some cases even exponentially fewer (*58*) qubits than classical bits. A notable example is fingerprinting (*59*). However, these protocols generally require a large number of qubits at each end node to achieve a substantial advantage. Specific variants of such protocols with energy constraints can also be realized at lower stages (*60*). Last, the presence of entanglement also brings new security issues for existing classical protocols (*61*), requiring new insights and analysis.

Implementation status and challenges

The current experimental status of long-distance quantum networks is at the lowest stage—trusted-repeater networks—with several commercial systems for QKD on the market. The first extended trusted repeater networks have already been implemented over metropolitan distances (*62*–*65*), and a long-distance implementation has recently been completed (*66*). The hardware required at the lowest stage (mainly light sources, optical links, and detectors) has been described in detail in previous literature (*14*, *23*). Realizing the first stage with end-to-end quantum functionality—prepare-and-measure networks—over long distances demands the use of quantum repeaters to bridge long distances via intermediate qubit storage or error correction, as well as routers to forward the quantum state to the desired node. Several recent experiments have demonstrated elements belonging to this and higher stages at short distances, suggesting that higher-functionality networks are within reach. To put these experiments into the right perspective, we briefly summarize the main requirements for three types of quantum internet hardware.

Photonic communication channels

Photonic channels establish quantum links between the distant repeater stations and between the end nodes. Two types of photonic channels can be distinguished: free-space channels [potentially via satellites (*67*, *68*)] and fiber-based channels. Each has its own advantages and disadvantages, and a future quantum internet—similar to the current classical internet—may use a combination of them. We require these channels to exhibit minimal photon loss and decoherence. The effect of photon loss on fidelity can in general be dealt with by photon-heralding protocols, but photon loss unavoidably affects the communication rate across the network. For photons in the telecom frequency bands, loss in fibers can be as low as 0.2 dB/km. Decoherence can in general be overcome through entanglement distillation (*69*–*71*), which requires additional levels of qubit processing. Last, the bandwidth of the channels is of practical importance; multiplexing in frequency, time, spatial, and/or polarization degrees of freedom allows for increases of the communication rates.

End nodes

For the quantum internet to reach its full potential, the end nodes need to meet the following requirements.

(i) Robust storage of quantum states during the time needed to establish entanglement between end nodes. This robustness must persist under quantum operations performed on the end node.

(ii) High-fidelity processing of quantum information within the node. For the more advanced tasks, multiple qubits will be required, making the end nodes similar to small-scale quantum computers.

(iii) Compatibility with photonic communication hardware: efficient interface to light at the relevant wavelength (telecom bands for fiber-based networks).

Several experimental platforms are currently being pursued for the end nodes. Each of these combines well-controlled matter-based qubits with a quantum optical interface via internal electronic transitions. The generation of photon-mediated entanglement between distant matter qubits has been achieved with trapped ions (*72*), atoms (*73*, *74*), nitrogen-vacancy (N-V) centers in diamond (*75*), and semiconductor quantum dots (*76*, *77*) over distances up to 1.3 km (*78*). By using measurement-based schemes with heralding, high-fidelity entangled states could be created in these experiments, even though substantial photon loss was present. The major challenge in extending these point-to-point entangled links into true networks is the robust storage of quantum states. The intrinsic coherence times of most above-mentioned platforms are very long (for instance, more than a second for ions and N-V centers). However, cross-talk caused by unwanted couplings or imperfect individual addressability can severely affect the coherence of a memory qubit under operations on another qubit in the same node (*79*, *80*).

A promising approach is to use different types of qubits within a node. For instance, trapping different species of ions allows for individual addressing of the ions via their different electronic transition frequencies (*81*–*83*). In a similar fashion, carbon-13 nuclear spins near a diamond N-V center provide a robust register of memory qubits that do not interact with the laser control fields on the N-V electron spin (*84*). In a very recent experiment, such hybrid network nodes enabled the generation of two remote entangled states on which entanglement distillation could then be performed (*85*). If several of such robust memories can be successfully integrated into a multi-qubit network node, the highest stages of the quantum internet may come into reach.

Another challenge for most of the above systems is that these do not intrinsically couple to light in the telecom band. To fulfill requirement (iii), wavelength conversion at the single-photon level can be used. Pioneering experiments using nonlinear optics (*86*, *87*) have already demonstrated

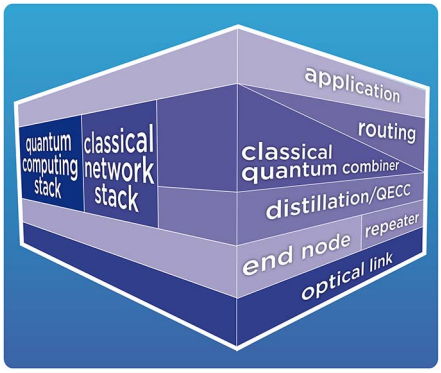


Fig. 5. Possible elements of a future quantum network stack.

the feasibility of such conversion; the current challenge is to realize a robust and high-efficiency (say, >50%) converter that exhibits a high signal-to-noise ratio (say, >100).

As an alternative to the above systems with intrinsic optical interface, the end nodes could be formed from a quantum processor with qubit frequencies in the microwave domain, such as a superconducting qubit circuit, in combination with a microwave-to-optical conversion process. The physics of such a conversion—for instance, by use of mechanical resonators (*88*, *89*) or atomic transitions (*90*)—is currently being investigated in many laboratories.

Quantum repeater requirements

Quantum repeater stations need to improve the rate of photonic qubit transfer. The requirements for quantum repeaters are similar to but less strict than for the end nodes. In particular, depending on the exact architecture [(*91*), review], the storage of quantum states may only be required for the time needed to establish entanglement between the nearest active nodes; this storage time can deviate substantially from that required for the end nodes. Also, the qubit processing capabilities required are limited, and therefore systems different from the ones above can be considered. As a prime example, an ensemble of atoms and ions either in gas phase or in a solid can be used as an on-demand quantum memory (*92*). If the memory can herald the arrival of a photon and store the photon's quantum state, photon loss can be efficiently mitigated. Storage and on-demand retrieval have already been achieved (*93*–*96*), although efficiencies are still to be improved. Such memories also allow for multiplexing within a single device. Furthermore, they are compatible with current-day down-conversion sources for entangled photon pairs. Current challenges are to combine heralding and on-demand high-efficiency retrieval with long coherence times.

A radically different approach to quantum repeaters has emerged in recent years in which the quantum state of interest is encoded in multiple photons so that error correction performed at the repeater stations can erase errors caused by photon loss and decoherence during transmission (*97*–*100*). The main advantage of such a scheme is that the classical two-way communication of standard repeater schemes (necessary to convey the heralding signal of whether or not the photons arrived at the stations) becomes obsolete. The communication rates of these schemes are therefore potentially much higher. However, the experimental demands seem daunting at present; for encoding the qubit, the near-deterministic generation of a many-photon cluster state is required, which is far beyond the state of the art (*101*). Furthermore, because these schemes require quantum error correction, they will only work if the error thresholds associated with the desired transmission qualities are met, thus placing more stringent requirements on the control and readout fidelities within the repeater nodes. That being said, theory research (*102*) in this direction is likely to yield more insights, and experimental progress may bring such schemes closer to reality in the future.

Last, the end nodes that are currently being developed may also function themselves as repeaters.

Network stack requirements

In order to enable widespread use and application development, it is essential to develop methods that allow quantum protocols to connect to the underlying hardware implementation transparently and to make fast and reactive decisions for generating entanglement in the network in order to mitigate limited qubit lifetimes (Fig. 5). Classically, this is achieved by a series of layered protocols such as the Transmission Control Protocol/Internet Protocol (TCP/IP) (*103*) that provide an abstraction that ultimately allows application protocols to exchange data between two end nodes without having to know any details on how this connection is actually realized. No such network stack presently exists for a quantum internet, and only some basic elements have been noted (*104*). As a trivial example on why a new stack is required for a quantum network, the first novel feature is a mapping between classical control information (header) and the underlying qubits. By contrast, classically a header and data may be nicely combined in one piece of data to be transmitted. Another example is the use of error detection at the link layer of the classical network stack that does not easily translate to a realistic quantum network. Clearly, error detection can theoretically be realized by using quantum error-correcting codes, but this method may be prohibitively expensive in practice, and other methods (*105*) may be more suitable. These are just two simple examples of the challenges involved in designing such a network stack, calling for substantial development.

Although it is hard to predict what the exact physical components of a future quantum internet will be, it is likely that we will see the birth of the first multinode quantum networks in the next few years. This development brings the exciting opportunity to test all the ideas and functionalities that so far only exist on paper and may indeed be the dawn of a future large-scale quantum internet.

REFERENCES AND NOTES

1. D. Castelvecchi, The quantum internet has arrived (and it hasn't). Nature **554**, 289–292 (2018).
2. A. Broadbent, J. Fitzsimons, E. Kashefi, *50th Annual IEEE Symposium on Foundations of Computer Science, 2009.* (IEEE, 2009), pp. 517–526.
3. P. Kómár *et al*., A quantum network of clocks. *Nat. Phys.* **10**, 582–587 (2014). doi: 10.1038/nphys3000
4. D. Gottesman, T. Jennewein, S. Croke, Longer-baseline telescopes using quantum repeaters. *Phys. Rev. Lett.* **109**, 070503 (2012). doi: 10.1103/PhysRevLett.109.070503; pmid: 23006349
5. H. J. Kimble, The quantum internet. *Nature* **453**, 1023–1030 (2008). doi: 10.1038/nature07127; pmid: 18563153
6. A. I. Lvovsky, B. C. Sanders, W. Tittel, Optical quantum memory. *Nat. Photonics* **3**, 706–714 (2009). doi: 10.1038/nphoton.2009.231
7. T. Northup, R. Blatt, Quantum information transfer using photons. *Nat. Photonics* **8**, 356–363 (2014). doi: 10.1038/nphoton.2014.53
8. D. D. Awschalom, R. Hanson, J. Wrachtrup, B. B. Zhou, Quantum technologies with optically interfaced solid-state spins. *Nat. Photonics* **12**, 516–527 (2018). doi: 10.1038/s41566-018-0232-2
9. A. Reiserer, G. Rempe, Cavity-based quantum networks with single atoms and optical photons. *Rev. Mod. Phys.* **87**, 1379–1418 (2015). doi: 10.1103/RevModPhys.87.1379
10. L. Salvail *et al*., Security of trusted repeater quantum key distribution networks. *J. Comput. Secur.* **18**, 61–87 (2010). doi: 10.3233/JCS-2010-0373
11. C. H. Bennett, G. Brassard, *International Conference on Computer System and Signal Processing, IEEE, 1984* (1984), pp. 175–179.
12. A. K. Ekert, Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991). doi: 10.1103/PhysRevLett.67.661; pmid: 10044956
13. S. Wiesner, Conjugate coding. *ACM SIGACT News* **15**, 78–88 (1983). doi: 10.1145/1008908.1008920
14. V. Scarani *et al*., The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009). doi: 10.1103/RevModPhys.81.1301
15. E. Biham, B. Huttner, T. Mor, Quantum cryptographic network based on quantum memories. *Phys. Rev. A* **54**, 2651–2658 (1996). doi: 10.1103/PhysRevA.54.2651; pmid: 9913773
16. S. L. Braunstein, S. Pirandola, Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012). doi: 10.1103/PhysRevLett.108.130502; pmid: 22540685
17. H.-K. Lo, M. Curty, B. Qi, Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012). doi: 10.1103/PhysRevLett.108.130503; pmid: 22540686
18. M. M. Wilde, *Quantum Information Theory* (Cambridge Univ. Press, 2013).
19. C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, H. M. Wiseman, One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Phys. Rev. A* **85**, 010301 (2012). doi: 10.1103/PhysRevA.85.010301
20. A. Gilchrist, N. K. Langford, M. A. Nielsen, Distance measures to compare real and ideal quantum processes. *Phys. Rev. A* **71**, 062310 (2005). doi: 10.1103/PhysRevA.71.062310
21. H.-K. Lo, X. Ma, K. Chen, Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005). doi: 10.1103/PhysRevLett.94.230504; pmid: 16090452
22. A. Extance, *Fibre Systems* (2017); www.fibre-systems.com/feature/quantum-security.
23. E. Diamanti, H.-K. Lo, B. Qi, Z. Yuan, Practical challenges in quantum key distribution. *NPJ Quantum Information* **2**, 16025 (2016). doi: 10.1038/npjqi.2016.25
24. I. Damgård, S. Fehr, L. Salvail, C. Schaffner, Secure identification and QKD in the bounded-quantum-storage model. *Theor. Comput. Sci.* **560**, 12 (2014). doi: 10.1016/j.tcs.2014.09.014
25. F. Dupuis, O. Fawzi, S. Wehner, Entanglement sampling and applications. *IEEE Trans. Inf. Theory* **61**, 1093–1112 (2014). doi: 10.1109/TIT.2014.2371464
26. D. Mayers, Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.* **78**, 3414–3417 (1997). doi: 10.1103/PhysRevLett.78.3414

27. H.-K. Lo, H. F. Chau, Is quantum bit commitment really possible? *Phys. Rev. Lett.* **78**, 3410–3413 (1997). doi: 10.1103/PhysRevLett.78.3410
28. H.-K. Lo, Insecurity of quantum secure computations. *Phys. Rev. A* **56**, 1154–1162 (1997). doi: 10.1103/PhysRevA.56.1154
29. I. B. DamgÅrd, S. Fehr, L. Salvail, C. Schaffner, Cryptography in the bounded-quantum-storage model. *SIAM J. Comput.* **37**, 1865 (2000). doi: 10.1137/060651343
30. S. Wehner, C. Schaffner, B. M. Terhal, Cryptography from noisy storage. *Phys. Rev. Lett.* **100**, 220502 (2008). doi: 10.1103/PhysRevLett.100.220502; pmid: 18643410
31. R. Konig, S. Wehner, J. Wullschleger, Unconditional security from noisy quantum storage. *IEEE Trans. Inf. Theory* **58**, 1962 (2012). doi: 10.1109/TIT.2011.2177772
32. N. H. Y. Ng, S. K. Joshi, C. C. Ming, C. Kurtsiefer, S. Wehner, Experimental implementation of bit commitment in the noisy-storage model. *Nat. Commun.* **3**, 1326 (2012). doi: 10.1038/ncomms2268; pmid: 23271659
33. J. Ribeiro, F. Grosshans, arXiv:1504.07171 [quant-ph] (2015).
34. A. Chailloux, I. Kerenidis, *Proceedings of the 52th Annual Symposium on Foundations of Computer Science* 10.1109/FOCS.2011.42 (2011).
35. D. Aharonov, A. Ta-Shma, U. V. Vazirani, A. C. Yao, *Proceedings of the Thirty-second Annual ACM Symposium on Theory of Computing* 10.1145/335305.335404 (2000).
36. A. Acín *et al.*, Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007). doi: 10.1103/PhysRevLett.98.230501; pmid: 17677888
37. D. Mayers, A. Yao, *Proceedings of the 39th Annual Symposium on Foundations of Computer Science, 1998* (IEEE, 1998), pp. 503–509.
38. J. Barrett, R. Colbeck, A. Kent, Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.* **110**, 010503 (2013). doi: 10.1103/PhysRevLett.110.010503; pmid: 23383767
39. S. Muhammad *et al.*, Quantum bidding in bridge. *Phys. Rev. X* **4**, 021047 (2014). doi: 10.1103/PhysRevX.4.021047
40. A. M. Childs, *Quantum Inf. Comput.* **5**, 456 (2005).
41. D. Aharanov, M. Ben-Or, E. Eban, *Proceedings of Innovations in Computer Science* (2008), pp. 453–469.
42. M. Hillery, V. Bužek, A. Berthiaume, Quantum secret sharing. *Phys. Rev. A* **59**, 1829–1834 (1999). doi: 10.1103/PhysRevA.59.1829
43. R. Cleve, D. Gottesman, H.-K. Lo, How to share a quantum secret. *Phys. Rev. Lett.* **83**, 648–651 (1999). doi: 10.1103/PhysRevLett.83.648
44. C. Crépeau, D. Gottesman, A. Smith, *Proceedings of EUROCRYPT* (2005), pp 285–301.
45. M. Christandl, S. Wehner, Proceedings of *ASIACRYPT* (2005), pp 217–235.
46. A. Ambainis, H. Buhrman, Y. Dodis, H. Röhrig, *Proceedings of IEEE Complexity* 10.1109/CCC.2004.1313848 (2004).
47. S. Barz *et al.*, Demonstration of blind quantum computing. *Science* **335**, 303–308 (2012). doi: 10.1126/science.1214707; pmid: 22267806
48. N. H. Nickerson, J. F. Fitzsimons, S. C. Benjamin, Freely scalable quantum technologies using cells of 5-to-50 qubits with very lossy and noisy photonic links. *Phys. Rev. X* **4**, 041041 (2014). doi: 10.1103/PhysRevX.4.041041
49. C. Mochon, arXiv:0711.4114 [quant-ph] (2007).
50. A. Chailloux, I. Kerenidis, *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on* (IEEE, 2009), pp. 527–533.
51. C. Crépeau, D. Gottesman, A. Smith, *Proceedings of the Thiry-fourth Annual ACM Symposium on Theory of Computing*, STOC '02 (ACM, 2002), pp. 643–652.
52. M. Burrows, *Proceedings of the 7th symposium on Operating systems design and implementation* (USENIX Association, 2006), pp. 335–350.
53. V. S. Denchev, G. Pandurangan, Distributed quantum computing. *ACM SIGACT News* **39**, 77 (2008). doi: 10.1145/1412700.1412718
54. M. Ben-Or, A. Hassidim, *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing* (2005), pp. 481–485.
55. S. Tani, H. Kobayashi, K. Matsumoto, *Proceedings of STACS: 22nd Annual Symposium on Theoretical Aspects of Computer Science* (2005), pp. 581–592.
56. M. Ganz, Quantum leader election. *Quantum Inform. Process.* **16**, 73 (2017). doi: 10.1007/s11128-017-1528-8
57. N. Aharon, J. Silman, Quantum dice rolling: A multi-outcome generalization of quantum coin flipping. *New J. Phys.* **12**, 033027 (2010). doi: 10.1088/1367-2630/12/3/033027
58. H. Buhrman, R. Cleve, S. Massar, R. de Wolf, Nonlocality and communication complexity. *Rev. Mod. Phys.* **82**, 665–698 (2010). doi: 10.1103/RevModPhys.82.665
59. H. Buhrman, R. Cleve, J. Watrous, R. de Wolf, Quantum fingerprinting. *Phys. Rev. Lett.* **87**, 167902 (2001). doi: 10.1103/PhysRevLett.87.167902; pmid: 11690244
60. J. M. Arrazola, N. Lütkenhaus, Quantum fingerprinting with coherent states and a constant mean number of photons. *Phys. Rev. A* **89**, 062305 (2014). doi: 10.1103/PhysRevA.89.062305
61. C. Crépeau, L. Salvail, J.-R. Simard, A. Tapp, *Proceedings of ASIACRYPT* (2011), pp. 407–430.
62. M. Peev *et al.*, The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **11**, 075001 (2009). doi: 10.1088/1367-2630/11/7/075001
63. M. Sasaki *et al.*, Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **19**, 10387–10409 (2011). doi: 10.1364/OE.19.010387; pmid: 21643295
64. D. Stucki *et al.*, Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New J. Phys.* **13**, 123001 (2011). doi: 10.1088/1367-2630/13/12/123001
65. S. Wang *et al.*, Field and long-term demonstration of a wide area quantum key distribution network. *Opt. Express* **22**, 21739–21756 (2014). doi: 10.1364/OE.22.021739; pmid: 25321550
66. R. Courtland, *IEEE Spectr.* **53**, 11 (2016).
67. G. Vallone *et al.*, Experimental satellite quantum communications. *Phys. Rev. Lett.* **115**, 040502 (2015). doi: 10.1103/PhysRevLett.115.040502; pmid: 26252672
68. J. Yin *et al.*, Satellite-based entanglement distribution over 1200 kilometers. *Science* **356**, 1140–1144 (2017). doi: 10.1126/science.aan3211; pmid: 28619937
69. C. H. Bennett *et al.*, Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.* **76**, 722–725 (1996). doi: 10.1103/PhysRevLett.76.722; pmid: 10061534
70. D. Deutsch *et al.*, Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.* **77**, 2818–2821 (1996). doi: 10.1103/PhysRevLett.77.2818; pmid: 10062053
71. W. Dür, H.-J. Briegel, J. Cirac, P. Zoller, Quantum repeaters based on entanglement purification. *Phys. Rev. A* **59**, 169–181 (1999). doi: 10.1103/PhysRevA.59.169
72. D. L. Moehring *et al.*, Entanglement of single-atom quantum bits at a distance. *Nature* **449**, 68–71 (2007). doi: 10.1038/nature06118; pmid: 17805290
73. S. Ritter *et al.*, An elementary quantum network of single atoms in optical cavities. *Nature* **484**, 195–200 (2012). doi: 10.1038/nature11023; pmid: 22498625
74. J. Hofmann *et al.*, Heralded entanglement between widely separated atoms. *Science* **337**, 72–75 (2012). doi: 10.1126/science.1221856; pmid: 22767924
75. H. Bernien *et al.*, Heralded entanglement between solid-state qubits separated by three metres. *Nature* **497**, 86–90 (2013). doi: 10.1038/nature12016; pmid: 23615617
76. A. Delteil *et al.*, Generation of heralded entanglement between distant hole spins. *Nat. Phys.* **12**, 218–223 (2016). doi: 10.1038/nphys3605
77. R. Stockill *et al.*, Phase-tuned entangled state generation between distant spin qubits. *Phys. Rev. Lett.* **119**, 010503 (2017). doi: 10.1103/PhysRevLett.119.010503; pmid: 28731764
78. B. Hensen *et al.*, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **526**, 682–686 (2015). doi: 10.1038/nature15759; pmid: 26503041
79. D. Hucul *et al.*, Modular entanglement of atomic qubits using photons and phonons. *Nat. Phys.* **11**, 37–42 (2015). doi: 10.1038/nphys3150
80. W. Pfaff *et al.*, Quantum information. Unconditional quantum teleportation between distant solid-state quantum bits. *Science* **345**, 532–535 (2014). doi: 10.1126/science.1253512; pmid: 25082696
81. C. J. Ballance *et al.*, Hybrid quantum logic and a test of Bell's inequality using two different atomic isotopes. *Nature* **528**, 384–386 (2015). doi: 10.1038/nature16184; pmid: 26672554
82. T. R. Tan *et al.*, Multi-element logic gates for trapped-ion qubits. *Nature* **528**, 380–383 (2015). doi: 10.1038/nature16186; pmid: 26672553
83. I. V. Inlek, C. Crocker, M. Lichtman, K. Sosnova, C. Monroe, Multispecies trapped-ion node for quantum networking. *Phys. Rev. Lett.* **118**, 250502 (2017). doi: 10.1103/PhysRevLett.118.250502; pmid: 28696766
84. A. Reiserer *et al.*, Robust quantum-network memory using decoherence-protected subspaces of nuclear spins. *Phys. Rev. X* **6**, 021040 (2016). doi: 10.1103/PhysRevX.6.021040
85. N. Kalb *et al.*, Entanglement distillation between solid-state quantum network nodes. *Science* **356**, 928–932 (2017). doi: 10.1126/science.aan0070; pmid: 28572386
86. S. Tanzilli *et al.*, A photonic quantum information interface. *Nature* **437**, 116–120 (2005). doi: 10.1038/nature04009; pmid: 16136138
87. S. Zaske *et al.*, Visible-to-telecom quantum frequency conversion of light from a single quantum emitter. *Phys. Rev. Lett.* **109**, 147404 (2012). doi: 10.1103/PhysRevLett.109.147404; pmid: 23083285
88. R. W. Andrews *et al.*, Bidirectional and efficient conversion between microwave and optical light. *Nat. Phys.* **10**, 321–326 (2014). doi: 10.1038/nphys2911
89. J. Bochmann, A. Vainsencher, D. Awschalom, A. N. Cleland, Nanomechanical coupling between microwave and optical photons. *Nat. Phys.* **9**, 712–716 (2013). doi: 10.1038/nphys2748
90. S. Probst *et al.*, Anisotropic rare-earth spin ensemble strongly coupled to a superconducting resonator. *Phys. Rev. Lett.* **110**, 157001 (2013). doi: 10.1103/PhysRevLett.110.157001; pmid: 25167299
91. W. J. Munro, K. Azuma, K. Tamaki, K. Nemoto, Inside quantum repeaters. *IEEE J. Sel. Top. Quantum Electron.* **21**, 78 (2015). doi: 10.1109/JSTQE.2015.2392076
92. N. Sangouard, C. Simon, H. De Riedmatten, N. Gisin, Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **83**, 33–80 (2011). doi: 10.1103/RevModPhys.83.33
93. N. Kalb, A. Reiserer, S. Ritter, G. Rempe, Heralded storage of a photonic quantum bit in a single atom. *Phys. Rev. Lett.* **114**, 220501 (2015). doi: 10.1103/PhysRevLett.114.220501; pmid: 26196608
94. C. Kurz *et al.*, Experimental protocol for high-fidelity heralded photon-to-atom quantum state transfer. *Nat. Commun.* **5**, 5527 (2014). doi: 10.1038/ncomms6527; pmid: 25413900
95. H. Tanji, S. Ghosh, J. Simon, B. Bloom, V. Vuletić, Heralded single-magnon quantum memory for photon polarization States. *Phys. Rev. Lett.* **103**, 043601 (2009). doi: 10.1103/PhysRevLett.103.043601; pmid: 19659349
96. A. Delteil, Z. Sun, S. Fält, A. Imamoğlu, Realization of a cascaded quantum system: Heralded absorption of a single photon qubit by a single-electron charged quantum dot. *Phys. Rev. Lett.* **118**, 177401 (2017). doi: 10.1103/PhysRevLett.118.177401; pmid: 28498703
97. K. Azuma, K. Tamaki, H.-K. Lo, All-photonic quantum repeaters. *Nat. Commun.* **6**, 6787 (2015). doi: 10.1038/ncomms7787; pmid: 25873153
98. M. Pant, H. Krovi, D. Englund, S. Guha, Rate-distance tradeoff and resource costs for all-optical quantum repeaters. *Phys. Rev. A* **95**, 012304 (2017). doi: 10.1103/PhysRevA.95.012304
99. S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, L. Jiang, Ultrafast and fault-tolerant quantum communication across long distances. *Phys. Rev. Lett.* **112**, 250501 (2014). doi: 10.1103/PhysRevLett.112.250501; pmid: 25014798
100. W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, K. Nemoto, Quantum communication without the necessity of quantum memories. *Nat. Photonics* **6**, 777–781 (2012). doi: 10.1038/nphoton.2012.243
101. I. Schwartz *et al.*, Deterministic generation of a cluster state of entangled photons. *Science* **354**, 434–437 (2016). doi: 10.1126/science.aah4758; pmid: 27608669
102. T. Rudolph, Why I am optimistic about the silicon-photonic route to quantum computing. *APL Photonics* **2**, 030901 (2017). doi: 10.1063/1.4976737
103. V. G. Cerf, R. E. Kahn, A protocol for packet network intercommunication. *IEEE Trans. Commun.* **22**, 637–648 (1974). doi: 10.1109/TCOM.1974.1092259
104. R. Van Meter, J. Touch, Designing quantum repeater networks. *IEEE Commun. Mag.* **51**, 64 (2013). doi: 10.1109/MCOM.2013.6576340
105. C. Pfister, M. A. Rol, A. Mantri, M. Tomamichel, S. Wehner, Capacity estimation and verification of quantum channels with arbitrarily correlated errors. *Nat. Commun.* **9**, 27 (2018). doi: 10.1038/s41467-017-00961-2; pmid: 29295975
106. M. Takeoka, S. Guha, M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **5**, 5235 (2014). doi: 10.1038/ncomms6235; pmid: 25341406

107. S. Pirandola, R. Laurenza, C. Ottaviani, L. Banchi, Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017). doi: 10.1038/ncomms15043; pmid: 28443624
108. L.-M. Duan, M. D. Lukin, J. I. Cirac, P. Zoller, Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414**, 413–418 (2001). doi: 10.1038/35106500; pmid: 11719796
109. C. Simon *et al*., Quantum repeaters with photon pair sources and multimode memories. *Phys. Rev. Lett.* **98**, 190503 (2007). doi: 10.1103/PhysRevLett.98.190503; pmid: 17677612
110. L. Jiang *et al*., Quantum repeater with encoding. *Phys. Rev. A* **79**, 032325 (2009). doi: 10.1103/PhysRevA.79.032325
111. J. J. Wallman, S. T. Flammia, Randomized benchmarking with confidence. *New J. Phys.* **16**, 103032 (2014). doi: 10.1088/1367-2630/16/10/103032

ACKNOWLEDGMENTS

We thank J. Borregaard, E. Diamanti, D. Englund, R. A. Friedman, T. Northup, I. Kerenidis, W. Tittel, and all members of the Quantum Internet Alliance collaboration for feedback on earlier versions of this document. **Funding:** D.E. and S.W. are funded by an ERC Starting Grant (S.W.) and an NWO VIDI Grant (S.W.). R.H. is funded by an ERC Consolidator Grant and an NWO VICI Grant. R.H. and S.W. are also supported by the NWO Zwaartekracht Grant QSC. D.E., R.H., and S.W. are also funded by the EU H2020 FETFLAG Quantum Internet Alliance. **Competing interests:** There are no competing interests.

10.1126/science.aam9288

Quantum internet: A vision for the road ahead

Stephanie Wehner, David Elkouss and Ronald Hanson

Science **362** (6412), eaam9288.
DOI: 10.1126/science.aam9288

The stages of a quantum internet

As indispensable as the internet has become in our daily lives, it still has many shortcomings, not least of which is that communication can be intercepted and information stolen. If, however, the internet attained the capability of t ransmitting quantum information—qubits—many of these security concerns would be addressed. Wehner *et al.* review what it will take to achieve this so-called quantum internet and propose stages of development that each correspond to increasingly powerful applications. Although a full-blown quantum internet, with functional quantum computers as nodes connected through quantum communication channels, is still some ways away, the first long-range quantum networks are already being planned.

Science, this issue p. eaam9288