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 $\lvert\Psi\rangle$ and any one qubit projective measurement M, there exists a way for i to prepare $\lvert\Psi\rangle$, transfer it to j, so that either (i) j performs measurement M on $\lvert\Psi\rangle$ 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 $\lvert\Phi_{ij}\rangle$ 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 $\lvert\Psi\rangle$ 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.

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.

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

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 $0(\sqrt{n/\log n})$, 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