Quantum Internet
by Joseph Burr, Abhishek Parakh, and Mahadevan Subramaniam

Editor’s Introduction

While quantum computing faces many implementation challenges, practical quantum communication technologies exist today. This means quantum networking services such as quantum key distribution (QKD) can already be utilized. Adoption of quantum technologies into existing infrastructure will likely evolve into fully-fledged quantum networks that grow in tandem with advances in quantum computing. This article describes the unique challenges, evolving stakeholders, and possible architectural components of the coming quantum internet.
Quantum Internet

by Joseph Burr, Abhishek Parakh, and Mahadevan Subramaniam

Quantum computing poses the greatest threat ever faced by modern cryptography. Numerous articles and blog posts explain its devastating impact to the encryption schemes we use for secure communication on the internet every day [1, 2, 3]. An entire field of research known as post-quantum cryptography (PQC) has emerged to prepare for the day when theoretical quantum computers become a reality [4]. The National Institute of Standards and Technology (NIST) has already begun a standardization process of PQC algorithms with the intent to begin replacing the Internet’s infrastructure with cryptography strong enough to withstand quantum computers as soon as possible [5]. Much like their predecessors, the security of these post-quantum schemes is based on assumptions of computational complexity; there is no guarantee that new classical or quantum algorithms will ever be able to crack them. Quantum networking and cryptography, on the other hand, turns the same fundamental strengths utilized by quantum computing against it to provide a provably secure communication alternative. Though general-purpose quantum computing is not currently practical, quantum networking can already offer its security benefits using today’s technologies. This implies the initial users of the quantum internet will be classical rather than quantum computers; however, quantum computers, once practical, will require quantum networks for their communication. Thus, the quantum internet’s purpose and benefits will evolve over time as it serves the needs of both classical and quantum devices.

QUANTUM BASICS

Before proceeding into the future evolution of the quantum internet, let us explore the fundamentals. Simply put, a quantum computer is a device that utilizes the laws of quantum mechanics for computation, and a quantum network, therefore, is a network that uses these laws for communication. Much like bits in classical computing, qubits represent the logical units of quantum computing. Qubits are physically represented in quantum hardware by subatomic particles such as photons or quantum dots. It is the use of subatomic particles that introduces the laws of quantum mechanics into the computer, and these principles provide the fundamental differences between classical and quantum computation:
• The no-cloning theorem states that unknown qubits cannot be copied (see Figure 1). Though the classical internet often employs the ability to copy strings of bits received on one device to other devices, this simply cannot be done on a quantum internet. Therefore, devices in quantum networks must perform blind computations.

• Superposition of qubits allows a quantum computer to exist in many quantum states at once (see Figure 2). This capability lies at the heart of quantum algorithms and provides a performance advantage over classical computers because a quantum computer can evaluate multiple possibilities simultaneously—often called quantum parallelism [6].

• Measurement is used to find out information about a qubit, but this process destroys the qubit’s superposition and forces it into a single state. The exact properties of an arbitrary qubit cannot be known. Thus, the ability to transmit superposed qubits over a quantum network without measurement is essential for the receiving quantum device to utilize the property of superposition to speed up algorithms.

• Quantum errors can occur while measuring, storing, or transmitting qubits. A measured qubit collapses to a particular state with a certain probability so the exact state cannot always be perfectly predicted. Qubits in storage or transmission are also particularly susceptible to error caused by other particles in their surrounding environment that alter their properties; this makes reliable quantum computers difficult to build [7].
error correction seeks to overcome these obstacles, but it must use creative techniques that do not violate the no-cloning theorem.

- Entanglement describes a mysterious phenomenon between qubits where they are so closely linked that their states can no longer be described independently (see Figure 3). Furthermore, measurement of one of the qubits predicts the state of the other qubit. This amazing capability was discovered by Einstein, Podolsky, and Rosen [8] and they found entanglement could exist between two qubits irrespective of their physical distance.

![Figure 3. Entanglement](image)

- Quantum teleportation utilizes an entangled pair of qubits that allows one party to send an exact replica of a qubit to another. In the process, the sender’s original qubit is destroyed; thus, no violation of the no-cloning theorem occurs. The entangled pair of qubits are also destroyed and cannot be re-used. Finally, the sender must send two classical bits of information to the receiver for the receiver to correctly recover the teleported qubit. Though teleportation sacrifices three qubits the outcome is extraordinarily valuable: A qubit correctly replicated across a physical distance without the need to physically send the qubit itself provides the ability for quantum machines to share entire superposed qubits.

**QUANTUM NETWORKING**

The quantum internet’s fundamental purpose is the transfer of qubits. Three primary methods exist to transfer qubits represented by photons: via electro-magnetic waves across open air, through fiber-optic cables, or from satellite to satellite in space. An open-air transfer demands the least cost but requires a line-of-sight between devices. The fiber-optic approach utilizes a common, existing networking technology, but qubit states decay rapidly as the distance of transmission increases resulting in unreliable transfers. Satellites offer more reliable transfers over long distances because less interference exists in space but launching and maintaining a satellite constellation involves great costs.
The quantum internet also requires the ability to transmit classical bits: Quantum teleportation, for example, requires the transfer of two classical bits to correctly recover the teleported qubit. Fortunately, the same fiber-optic cables used to transfer qubits can also be used to transfer classical bits even though the devices on either end are distinctly quantum or classical. This means much of the classical internet’s infrastructure can be used in the quantum internet.

**EVOlution of the Quantum Internet**

The necessary technologies for quantum networking exist today, but the quantum internet will evolve with each new quantum development. These advances will affect both the userbase and capabilities of the quantum internet across three stages.

**Stage 1: Classical devices use quantum key distribution.** In today’s classical internet, traffic must be encrypted using secret keys known only to the sender and receiver. However, these keys must be safely shared, and the security of the current classical key distribution protocols is based on mathematical problems and assumptions around how hard they are to solve with computers [4]. Quantum key distribution (QKD), on the other hand, offers key distribution protocols whose security is based on unbending laws of quantum mechanics. QKD protocols are practical to implement; in fact, companies already sell QKD devices. The networks to support QKD protocols are also quite simple because most quantum communication protocols do not require storage of qubits for long periods. As a result, these can operate at room temperature and on existing optical networks and free space channels. China holds the record for the largest QKD network in existence—the Micius satellite network—which allows communication over 4,600 kilometers using an integrated ground-satellite approach [9]. The Toshiba research laboratory in Cambridge holds the record for longest quantum transmission over optical fiber for their 600-kilometer result [10]. The experimental successes in quantum key distribution demonstrate a quantum internet could already provide more secure key distribution alternatives to existing devices on the classical internet, which implies that the early quantum internet will be used primarily for QKD.

**Stage 2: Classical and quantum devices use entanglement services.** Scaling has been a constant issue with quantum networking because classical repeater techniques cannot work; entanglement offers a solution. In classical communication, long distances are divided by repeater devices that are placed along short segments of fiber optic cable to receive series of bits and repeat them down the line. The no-cloning theorem prohibits this capability for quantum transmissions; therefore, quantum repeaters must accomplish the same goal but without the...
need to copy qubits. Quantum repeaters achieve this using entanglement swapping to establish a pair of entangled qubits between communicating parties to facilitate quantum teleportation between them. In this process, each intermediate repeater transmits entangled pairs over short fiber distances to its neighbors, and these entangled pairs are continuously swapped down the line to the final device. Unfortunately, quantum repeaters are currently difficult to implement because they require quantum memories to store volatile entangled qubits until the entanglement swapping operations can be completed. The implementation of hardware to store quantum memories remains an active and promising area of research. The current record for successful storage of a qubit is approximately one millisecond, which may be just enough to start seeing practical quantum repeaters [11].

Entanglement established by quantum repeaters provides an important security advantage over the QKD networks possible in Stage 1. Without entanglement, the effective transmission range of quantum networks is limited. To overcome this obstacle, early QKD networks employed trusted relay nodes placed between communicating parties that establish intermediate keys; however, this means intermediate devices contain parts of the overall key material. Quantum repeaters, on the other hand, have no knowledge of the final key qubits being teleported; they never possess any qubit other than the entangled pairs used to facilitate teleportation. Once quantum repeaters become practical, the classical devices using the Stage 1 quantum internet will be able to distribute keys across the world without physically sending sensitive key qubits anywhere.

Simple quantum computers will also be able to join the quantum internet in this stage to utilize the entangled qubits established by quantum repeaters. Using entanglement, a team of Austrian researchers demonstrated the ability to reliably teleport arbitrary qubits for the first time using a special quantum error correction technique [12, 13]. Teleportation of arbitrary qubits allows quantum computers to share pure quantum states. The quantum computers of this stage do not even need to be fully practical, standalone computers. Instead, entanglement services allow even basic or specialized quantum computers, which can only physically support a small number of qubits, the ability to combine their resources [14]. Note, as well, that entangled qubits can interact regardless of physical distance; so, distributed quantum computers with entangled states are not necessarily bound by the same performance constraints as distributed classical computers.

Stage 3: Quantum computers communicate. Ironically, the quantum internet will likely have existed long before general-purpose quantum computers, though not for lack of effort. Governments and private entities have invested in both research and development of quantum computing as well as training a largescale workforce that is ready to take advantage of this new technology.² The United States passed the National Quantum Initiative Act in 2018 with a budget

---

² Quantum Flagship
National Quantum Initiative
http://ubiquity.acm.org

2022 Copyright held by the owner/author(s). Publication rights licensed to ACM.
of more than $1 billion. This act calls for a coordinated research and development effort between U.S. government agencies and organizations for the “economic and national security of the United States” [15]. Within the past five years, several prototypes of quantum computers have emerged [16, 17, 18]. Researchers and students can access the latest quantum backends upon request. Many companies have proposed extremely ambitious and optimistic timelines for scaling up of this new technology with practical computers available by 2030 [19, 20]. However, skeptics of this field have wondered if the smaller prototypes can ever be scaled up to have enough qubits to do something useful that cannot already be done with special purpose algorithms and classical hardware [21]. Whether powerful quantum computers exist or not, the quantum internet offers many uses in Stages 1 and 2. However, if the dream of large quantum computers is realized one day, the Stage 3 quantum internet will benefit from the same achievements.

ARCHITECTURE OF THE QUANTUM INTERNET

Like its classical predecessor, the quantum internet will begin as a series of local networks that are combined over time. Many of the architectural concepts may be familiar; others, designed to solve specifically quantum problems, may not [22].

Quantum transmission. Whether it occurs over fiber-optic links or open-air, quantum transmission requires a point-to-point connection because qubits cannot be copied or broadcasted to several devices at once. Efficiently establishing such a point-to-point connection in fiber will require switching and multiplexing to allow multiple quantum devices to utilize the same fiber-optic cable while ensuring the correct devices are the only recipients of their intended qubits. Figure 4 depicts a simple, local quantum network with a quantum switch to connect devices. Note that both classical computers (with integrated quantum components such as QKD devices) and quantum computers may share the network. The switch is the crucial component used to physically link the quantum fiber-optic channels between devices. Physically switching between devices will require control information in order to properly set up paths through the network. Classical rather than quantum channels will best transmit such control information; thus, every device also connects to the switch via a fiber optic cable used for classical transmission.

A simple procedure for desktop 1 in Figure 4 to transmit a qubit to Server 2 may be:

1. Desktop 1 sends “Switch to Server 2” to the switch on the classical channel.
2. After switching the quantum channel to Server 2, the switch replies “Ready.”
3. Desktop 1 sends its qubit to Server 2 via the quantum channel (through the switch).
Quantum repeaters. As the physical distance spanned by quantum networks increases quantum repeaters will be required. As shown in Figure 5, multiple quantum repeaters connected by switches may provide more concurrent and reliable service: Routing/switching algorithms for the quantum internet must handle scenarios where a repeater goes offline or is currently in use [23]. Note the classical channels required by the quantum repeaters used to facilitate entanglement swapping. Though repeaters offer the most cost-effective choice, satellite networks as shown in Figure 6 offer stunning capabilities. A satellite network utilizes open-air channels to beam information between ground stations and satellites. Less interference in space provides the performance advantages, and satellite constellations will likely facilitate intercontinental quantum communication. As always, classical channels are required for command and control.
Figure 5. Repeater network

Figure 6. Satellite network
**Performance.** The quantum internet’s performance is limited by the separate capabilities of the classical and quantum channels. Classical channel performance will coincide with the well-researched capabilities of standalone classical networks. Quantum channel performance limitations, on the other hand, will require further analysis as the quantum internet takes shape. Entangled qubits represent an important resource because they are consumed so often. Recall that quantum teleportation destroys an entangled pair of qubits for every single transmission, and entanglement swapping among quantum repeaters—necessary to create the end-to-end entangled pair—also destroys each intermediate entangled pair in the process. Quantum repeaters should have the ability to generate their own entangled qubits rather than rely on external entanglement providers because transmission of entangled qubits to repeaters would consume network resources. Ideally, quantum repeaters will continuously generate entangled pairs to prevent bottlenecks. Simple network-layer routing algorithms have already been studied to efficiently utilize repeater networks with constantly available entangled pairs [24, 25, 26], but further practical research in this area is required to maximize resource utilization.

Apart from the demand for entangled qubits, quantum network throughput will be reduced by the requirement for extra qubits to perform important verification functions. Entanglement swapping requires additional qubits for purification to ensure the final entangled state does not decay after multiple intermediate swaps. Network layer health and security checks will require transmission of extra qubits to verify devices are functioning and uncompromised [27]. Application layer quantum protocols consume additional qubits to perform quantum error correction, and QKD protocols often sacrifice qubits to perform random checks to ensure an eavesdropper is not present. These requirements, though limiting throughput, each serve an important purpose and should be considered essential to any quantum network implementation.

**CONCLUSIONS**

Implementing the quantum internet now could provide value to existing classical devices today while also preparing the way for the powerful quantum computers of tomorrow. Governments, companies, and researchers have all devoted enormous efforts to further all quantum technologies because they truly believe in their value. On the other hand, some groups are less optimistic. The National Security Agency (NSA), for example, doubts pure quantum cryptography will ever be more useful than classical post-quantum schemes [28]. However, this reservation simply highlights an important foundational principle: Some problems will best be solved by classical computers, and others by quantum computers. Perhaps classical post-quantum cryptographic schemes are more practical for key distribution today, but there are no guarantees that these schemes will always remain secure against classical or quantum computers. Other skeptics, like Mikhail Dyakonov, a theoretical physics researcher, have questioned whether practical quantum computers can ever be built. In his 2018 article, Dyakonov pointed out that among the plethora of quantum research publications, one can find very few containing practical
hardware implementations. He also speaks for most naysayers by discussing the difficulties with error handling and correction that drastically hamper quantum systems [21]. These are very real and fundamental roadblocks to achieving general-purpose quantum computing. However, these obstacles do not prevent further advances in quantum networking and cryptography. In fact, a renewed focus on perfecting what we can already achieve with quantum technologies may provide the impetus we need to overcome these challenges. Each person contributing to the quantum internet offers new insights that just might become breakthroughs in other areas. Though it is difficult to implement powerful quantum computers today, smaller quantum devices could work together over the quantum internet to combine their processing power. One day we may even start using small, distributed quantum computers to help solve the very issues that prevent us from designing and building more powerful devices.

References

[1] Malonson, J. Quantum computing threatens everything—could it be worse than the apocalypse? Entrepreneur. January 28, 2022.

[2] Hollebeek, T. The impact of quantum computing on society. DigiCert. March 12, 2021.

[3] Daly, J. How tomorrow’s quantum computing raises cybersecurity risks today. IBM. June 21, 2021.

[4] Bernstein, D. J. and Lange, T. Post-quantum cryptography. Nature, 549, 188–194 (2017). https://doi.org/10.1038/nature23461.

[5] Post-Quantum Cryptography Standardization. National Institute of Standards and Technology. January 3, 2017.

[6] Rasmusson, A. The power of quantum computing: Parallelism. Indiana University. July 13, 2019.

[7] Pakin, S. and Coles, P. The problem with quantum computers. Scientific American. June 10, 2019.

[8] Einstein, A., Podolsky, B., and Rosen, N. Can quantum-mechanical description of physical reality be considered complete? Phys. Rev. 47, 10 (1935), 777–780.

[9] Chen, YA., Zhang, Q., Chen, TY. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature 589, 214–219 (2021).
[10] Toshiba Europe. Toshiba announces breakthrough in long distance quantum communication. June 8, 2021.

[11] Li, C. and Zhang, S. and Wu, Y.-K. and Jiang, N. and Pu, Y.-F. and Duan, L.-M. atomic quantum memory as a hardware-efficient quantum repeater node. PRX Quantum 2, 4 (2021).

[12] University of Innsbruck. Error-protected quantum bits entangled for the first time. Phys.org. January 13, 2021.

[13] Erhard, A., Poulsen Nautrup, H., Meth, M. et al. Entangling logical qubits with lattice surgery. Nature 589, 220–224 (2021).

[14] Wehner, S., Elkouss, S., and Hanson, R. Quantum internet: A vision for the road ahead. Science Vol 362, 6412 (2018).

[15] National Quantum Initiative. United States. 2018.

[16] Kaur, D. China has quantum computers that are 1 million times more powerful than Google’s. TechHQ. October 28, 2021.

[17] Hardware | Google Quantum AI. Google.

[18] Chow, J., Dial, O., and Gambetta, J. IBM quantum breaks the 100-qubit processing barrier. IBM Research Blog. November 16, 2021.

[19] Gambetta, J. IBM’s roadmap for scaling quantum technology. IBM Research Blog, September 15, 2020.

[20] Lucero, E. Unveiling our new Quantum AI campus. Keyword. Google. May 15, 2021.

[21] Dyakonov, M. The case against quantum computing. Spectrum IEEE. November 15, 2018.

[22] Mehic, M. et al. Quantum key distribution: A networking perspective. ACM Computing Surveys 53, 5, (2020), 1–41.

[23] Parakh, A. Quantum teleportation with one classical bit. Nature Scientific Reports 12, 3392 (2022).

[24] Amer, O., Krawec, W. O., and Wang, B. Efficient routing for quantum key distribution networks. July 30, 2020. arXiv:2005.12404 [quant-ph].

[25] Burr, J., Parakh, A., and Subramaniam, M. Evaluating different topologies for multi-photon quantum key distribution. In Proc. SPIE. 12093, Quantum Information Science, Sensing, and Computation XIV. SPIE, 2022. https://doi.org/10.1117/12.2620057.
[26] Parakh, A. and Subramaniam, M. Network routing protocols for multi-photon quantum cryptography. In *Proc. SPIE 11835, Quantum Communications and Quantum Imaging XIX, 1183504*. SPIE, 2021. https://doi.org/10.1117/12.2594891.

[27] Satoh, T., Nagayama, S., Suzuki, S., Matsuo, T., Hajdušek, M. and Meter, R. V. Attacking the quantum internet. *IEEE Transactions on Quantum Engineering* 2 (2021), 1–7.

[28] National Security Agency. *Quantum Key Distribution (QKD) and Quantum Cryptography (QC)*.

About the Authors

Joseph Burr is a full-time software engineer and graduate student earning a master’s in cybersecurity from the University of Nebraska–Omaha. His interest in security has motivated his research in homomorphic encryption, quantum cryptography, and quantum networking. Hands-on experience from nearly a decade of enterprise and web application development has influenced his work to bridge the gap between theoretical technologies and practical implementations. While away from his computer, he enjoys a peaceful life with his wife and three sons in smalltown Nebraska.

Abhishek Parakh is the director of the computer science Ph.D. program and an associate professor of Computer science at Kennesaw State University. Prior to joining Kennesaw State, he was the Mutual of Omaha Distinguished Chair of Information Science and Technology and an associate professor of cybersecurity at University of Nebraska at Omaha. He was also the Director of Nebraska University Center for Information Assurance. He received his Ph.D. in computer science from Oklahoma State University. As the director of Quantum Information Science and Cybersecurity laboratory his research interests include quantum computing, quantum algorithms, quantum cryptography and intelligent adaptive quantum education platforms.

Mahadevan Subramaniam is the Chairperson of the Computer Science Department at the University of Nebraska at Omaha. He is a professor of computer science, Charles W. Margre H. Distinguished Professor of Information Technology, and the director of the Intelligent Modeling, Simulation, and Testing Laboratory at the Peter Kiewit Institute. Prior to joining UNO, Subu worked in the high-tech industrial corridor in Silicon Valley, Bay Area, as a research scientist, computer architect, and an entrepreneur. He was a member of the team designing one of the first production quality compiler-compilers for programming language, CHILL and was involved in designing compiler for the hardware programming language, Verilog. He was a founding member of the Automated Software Engineering Group at NASA Ames Research Center, architected a distributed shared memory system, and was a principal architect for one of the first Infiniband Target Channel adapter in a successful start-up company.
