Using Quantum Memories in Entanglement-based Networks

Aliro Quantum

Contents

Quantum networks are a new paradigm in secure communications, offering unparalleled capabilities. Central to this quantum leap are quantum memories. Quantum memories harness and preserve the properties of quantum bits, or qubits, that are the core of quantum communication and computation. This paper delves into the intricacies of quantum memories and their function in quantum networks. These advanced technologies are not theoretical constructs, but are rapidly evolving practical tools that are poised to redefine the landscape of data transmission, cybersecurity, and computational power. Understanding the mechanics, applications, and potential of quantum memories is imperative for organizations as they step into the quantum era.

Quantum networking overview

Entanglement-based quantum networks are being deployed around the globe. These entanglement-based quantum networks are the modern quantum network, building on the foundations of QKD networks of the past to create versatile quantum communication channels. These entanglement-based quantum networks are multipurpose and are capable of supporting a variety of applications simultaneously.

These applications include:
- **Quantum Secure Communication.**
  Because of the physical properties of entanglement, entanglement-based quantum networks are resistant to eavesdropping. For example, in the event of a man-in-the-middle attack, the actual eavesdropping can be detected to determine that a particular link is no longer secure. These links can include fiber optic cables, and even satellites in some cases. Entanglement-based quantum networks allow the sharing of secret keys without the transmission of public keys across a network. They can replace public key exchange that is heavily relied upon today, but is vulnerable to attack by a quantum computer capable of using Shor's algorithm. The day a quantum computer is capable of using Shor's algorithm is commonly referred to as Q-Day, at which point encryption schemes such as RSA and Diffie-Hellman will be completely broken.
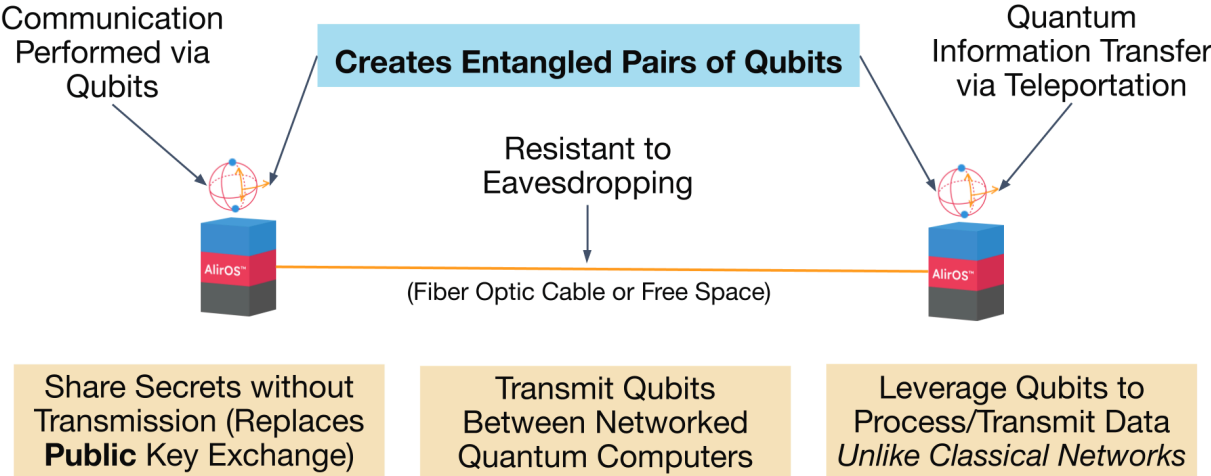
- **Networked quantum computing.**
  By networking quantum computers with entanglement-based networks, computational tasks can be distributed across different machines. This enables more efficient processing. Entanglement-based networks could

be used to link smaller quantum computers together, creating a system with greater computational power than a single machine could achieve alone. Entanglement-based quantum networks also support the development of quantum cloud services. In this scenario, users would access quantum computational resources remotely, without requiring their own quantum computer.

- **Networked quantum sensors.**
  - Quantum sensors can be networked together to significantly enhance their capabilities and applications. Entanglement-based quantum networks can distribute entanglement to quantum sensors in different locations. This shared entanglement can be used to increase the sensitivity and precision of measurements beyond what is achievable with classical methods. Entanglement-based quantum networks also enable large-scale sensor networks, where data from individual quantum sensors can be aggregated and processed collectively. This is useful for a wide range of applications, including environmental monitoring, seismic detection, and astronomical observations.

Entanglement-based Quantum Networks

The Modern Quantum Network

Communication Performed via Qubits

Creates Entangled Pairs of Qubits

Quantum Information Transfer via Teleportation

Resistant to Eavesdropping

(Fiber Optic Cable or Free Space)

AlirOS™

AlirOS™

Share Secrets without Transmission (Replaces **Public** Key Exchange)

Transmit Qubits Between Networked Quantum Computers

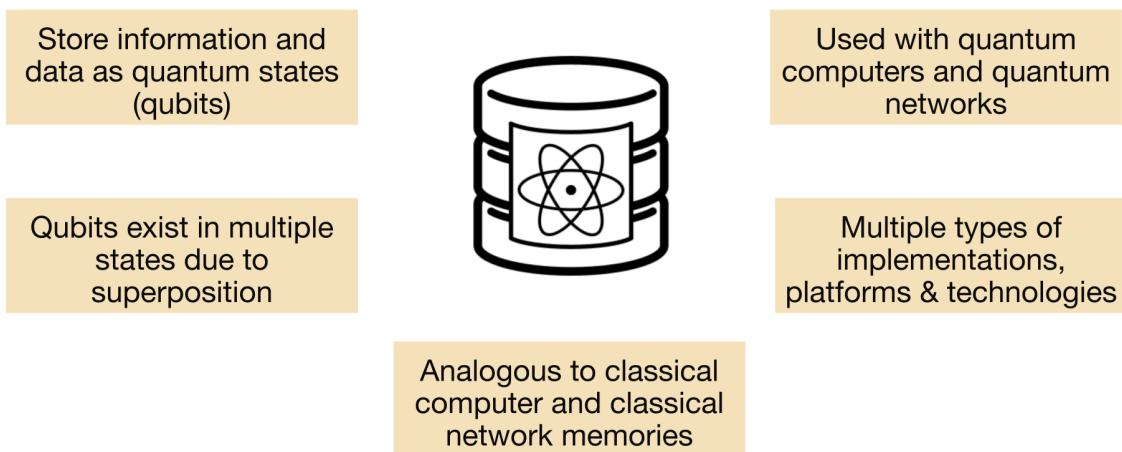Leverage Qubits to Process/Transmit Data *Unlike Classical Networks*

The need for quantum memories

Quantum networks are different from classical networks that use bits, bytes and packets, where classical information can be copied and amplified. Quantum information is subject to the no-cloning theorem, which states that quantum information cannot be copied the way classical data can. This property makes quantum information extremely secure, but complicates transmission of quantum information across very long distances.

Quantum Memories
Enable Critical Quantum Information Storage and Processing

Aliro QUANTUM®

- Store information and data as quantum states (qubits)

- Used with quantum computers and quantum networks

- Qubits exist in multiple states due to superposition

- Multiple types of implementations, platforms & technologies

- Analogous to classical computer and classical network memories

4

Quantum memories are a foundational technology, enabling quantum information storage and processing within quantum systems. While quantum memories are analogous to classical memories in classical computers and classical networks in that they store data, quantum memories operate fundamentally differently. This is due in part to the no-cloning theorem and the fact that entanglement decoheres quickly, which can result in qubits degrading in quality so as to be unusable for applications like computing and data transfer. Qubits also exist in multiple states, known as superposition. This property enables ultra-secure data transmission and exponential computational power, but also requires a device unique to quantum applications.

Quantum memory platforms

There are many types of implementations, platforms, and technologies for quantum memories, each with capabilities in different applications, in different environments, and for different purposes.

Solid state systems. Solid state quantum system quantum memories store quantum information in solid-state systems, which are typically easier to integrate into electronic devices compared to other forms of quantum memories, such as those based on atomic systems.This type of quantum memory includes nitrogen-vacancy centers in diamonds and solid state systems used to trap and release quantum information, and therefore operate as quantum memories.

Atomic ensembles. Atomic ensembles use a large group of atoms as a medium to store quantum information. This approach leverages the collective quantum states of atoms to create a robust and efficient storage mechanism for quantum information. These systems are distinct from solid-state quantum memories in that they typically use gasses or vapors of atoms as the medium for quantum storage. Examples of atomic ensemble quantum memories include rubidium vapor cells, cavity QED (quantum electrodynamics), and cold atoms using electromagnetically induced transparency (EIT).

Optical systems. Optical systems for quantum memories involve using light to store and manipulate quantum information. These systems are critical for quantum communication and computing, as they provide an interface between transmitted qubits (photons) and stationary qubits. An example of this type of memory are rare-earth ion doped crystals that use quantum properties of light to be able to store and retrieve quantum information.

As a building block for many different aspects of quantum technology, quantum memories are being used today in quantum computers and in quantum networking applications. In some cases, rack-mountable quantum memories are used to enable these applications. Quantum memories also continue to develop across different platforms by different vendors.

Quantum memories in quantum networks

Quantum networks use quantum memories in several ways, to achieve various objectives such as:

Extending link distances. Because quantum information can decohere, quantum memories are critical to extending the range of a secure quantum communication system over longer distances. By extending the reach of these networks to cover a larger geographical area, it becomes possible to interconnect data centers, sites, campuses, and locations over longer distances. Quantum memories can also mitigate the effects of signal loss in optical fibers.

Enhancing security. Quantum memories enhance the security of key exchange protocols that can be implemented over quantum networks, and are capable of mitigating side channel attacks on detectors resulting in a more secure entanglement-based key distribution. Quantum memories enable delayed-choice QKD. In delayed-choice QKD, the method of measuring the quantum states (for example, which polarization basis to use) is made after the states have already been sent and possibly even after they have been received. This method adds an extra layer of security to the QKD process, as delaying the choice of measurement basis makes it more challenging for an eavesdropper to obtain information about the key without being detected.

Quantum information processing. Quantum memories play an essential role in quantum information processing tasks. Such capabilities enable critical tasks like error correction and purification, as well as storing and manipulating quantum states for computation. Performing error correction and purification improves the fidelity of qubits in a network.

Synchronization and distribution of quantum states. In classical networks, synchronization and timing are critical in ensuring seamless data transfer. For example, in a video broadcast, timing and synchronization occur seamlessly to prevent packet drops, jitter, and delay. In quantum networks, synchronization and timing is even more critical because of the fragility of quantum states carried by qubits. Quantum memories are able to perform storage and processing of

quantum information that improves synchronization, deterministic timing, and operating system operations from end-to-end across multiple network nodes all the way to endpoints within that network.

Quantum communication protocols. Quantum protocols are essential to the implementation of a reliable quantum network. These protocols leverage unique properties of quantum states, such as superposition and entanglement, to achieve communication tasks that are either not possible or inefficient with classical methods. The ability of quantum memories to maintain the quantum state of qubits is crucial for various quantum communication tasks.

The modern entanglement-based quantum network uses quantum memories in a variety of locations to enable the operations of a quantum network, including those detailed above, and they can be located at endpoints as well as in nodes throughout the network to support operations.

Quantum Memory Use in Quantum Networks
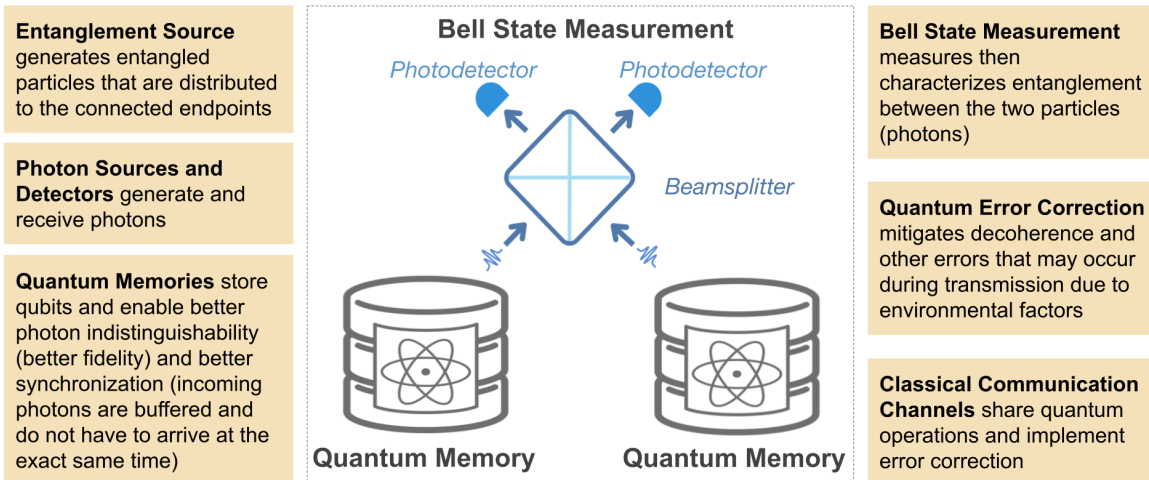### The Modern Entanglement-based Quantum Network
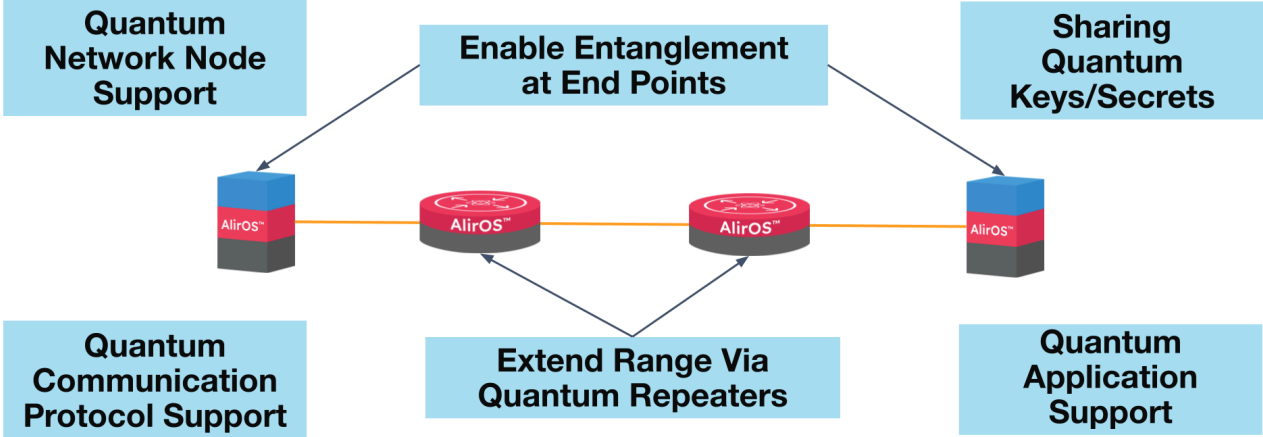
Quantum memories for quantum repeaters

In order to scale to global coverage, quantum networks require quantum repeaters. A Local Area Network with short distances from node to node does not require a repeater to be effective at those distances. Even many Metro Area Networks do not require repeaters in order to be implemented: the distances are short enough that qubit fidelity can be maintained over those links, without the use of a quantum repeater. As quantum networks scale to Wide Area Networks, and even some larger Metro Area Networks, quantum repeaters become essential. Quantum repeaters will be used for extending distances between quantum network nodes, and are mandatory for creating networks that span a country, a region, and internationally. Quantum memories are a core component of quantum repeaters.

Inside a quantum repeater

Quantum Repeater Internal Design
Multiple Quantum Network Devices and Components Form a Repeater

Entanglement Source generates entangled particles that are distributed to the connected endpoints

Photon Sources and Detectors generate and receive photons

Quantum Memories store qubits and enable better photon indistinguishability (better fidelity) and better synchronization (incoming photons are buffered and do not have to arrive at the exact same time)

Bell State Measurement
Photodetector   *Photodetector*

Beamsplitter

Quantum Memory   **Quantum Memory**

Bell State Measurement measures then characterizes entanglement between the two particles (photons)

Quantum Error Correction mitigates decoherence and other errors that may occur during transmission due to environmental factors

Classical Communication Channels share quantum operations and implement error correction

11

Components of internal design
The image above is a simplified overview of the elements of a quantum repeater. Quantum repeaters are not a single, monolithic device today.

Multiple discrete components are brought together to perform the function of a quantum repeater:

- An entanglement source. Entanglement sources generate entangled photons, which are then distributed to the connected endpoints.
- Photon sources and detectors. Photon sources generate individual photons that carry quantum information encoded in their quantum states (such as polarization). The quality of the photon source is vital to quantum communication. These photon sources must produce photons with high purity and stability to maintain the integrity of the quantum state during transmission. Photon detectors receive photons to enable the reading of quantum states of incoming photons from other nodes in the network, or to verify entanglement between distant nodes.
- Quantum memories. Quantum memories temporarily store qubits and maintain their quantum states until all parts of the network are ready to proceed with the next step in the communication process. This technology is crucial for managing the timing and coordination of quantum communication across the network.
- Bell state measurement. Bell state measurement in a process used to measure the entangled state between a pair of photons. This process enables entanglement swapping, which can be used to effectively create entanglement in a chain of repeaters or across the network.
- Quantum error correction. Quantum error correction mitigates quantum decoherence so that quantum information can be stored longer in the quantum memories within the repeater by detecting and correcting the errors that may have occurred as quantum states are transmitted.
- Classical communication. Classical communication is used for coordination across the quantum network.

In a quantum repeater, these components work together to achieve long-distance quantum communication. The process involves generating entangled photons, transmitting them to different nodes, using Bell state measurements to extend entanglement across multiple nodes, employing quantum error correction to maintain data integrity, and using classical channels for necessary coordination and feedback. This process enables quantum information to be transmitted over much greater distances than is currently possible with direct quantum communication.

Internal operations of quantum repeaters

The internal operation of quantum repeaters is complex. Quantum repeaters require specialized components like quantum memories, and advanced software to manage internal and external communications. Significant software capability and communication must be in place for a quantum repeater to perform tasks such as the ability to store quantum information, enable entanglement, perform entanglement swapping functions, and to ensure that quantum error correction is applied effectively. Both configuration and communication within the repeater itself are software-driven.

In short, while hardware components in quantum repeaters are the backbone of these devices, software is critical for their operation.
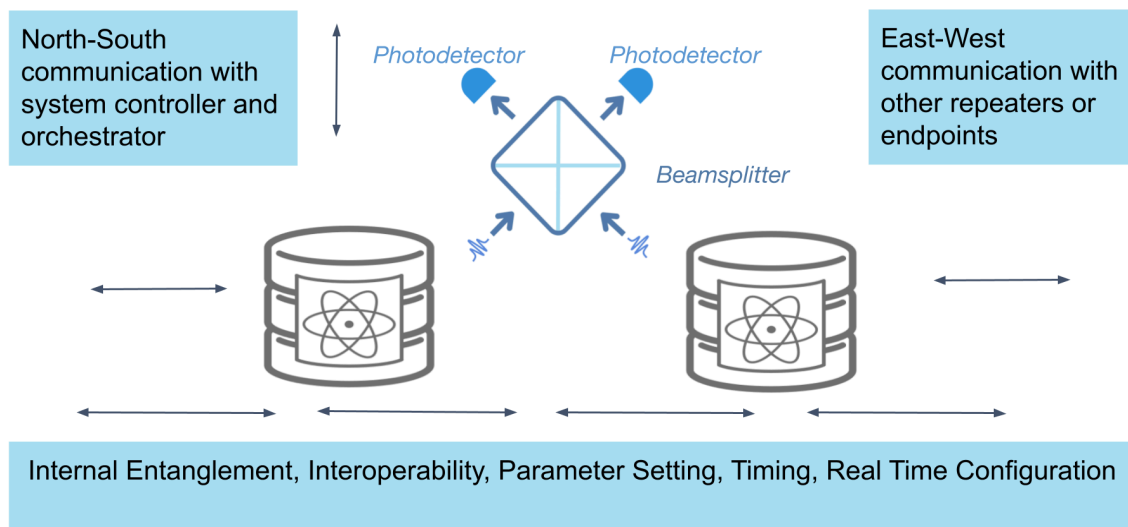
Configuration, communication, and protocols

The internal software and communication dynamics can be described by North-South and East-West communication.

Quantum Repeater Internal Operation

Configuration, Communication, and Protocols in Quantum Repeaters

North-South communication with system controller and orchestrator

East-West communication with other repeaters or endpoints

Photodetector   Photodetector

Beamsplitter

Internal Entanglement, Interoperability, Parameter Setting, Timing, Real Time Configuration

North-South communication. This communication occurs between the quantum repeater and the network's higher-level control systems, such as a system controller, or the network orchestrator.

East-West communication. This type of communication occurs between other repeaters in the system, other memories in the system, and even other endpoints in the system.

There are a multitude of parameters that must be set and reset, adjusted, read, monitored and controlled in these systems. There are real-time configuration and real-time monitoring needs. Being able to monitor, configure, control, and maintain the system within the time constraints required by quantum communication is essential. All of this typically occurs at the software level.

Quantum repeaters in Wide Area Networks

Pictured below is a simplified modern entanglement-based quantum network.

Quantum Repeaters in Wide Area Networks
Extending Qubit Distances, Quality, and Fidelity

Endpoint   Quantum Repeater   Quantum Repeater   Endpoint
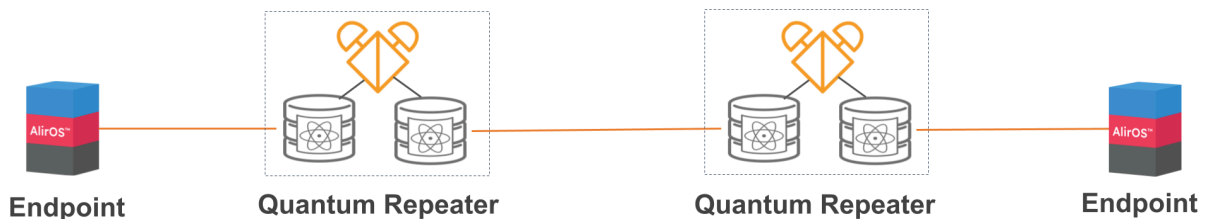
There are two endpoints; these endpoints could be two data centers, for example, that are being connected over a highly secure infrastructure for sharing sensitive information, for data backup or disaster recovery, and creates resilience against ransomware. All of this is possible with an entanglement-based quantum network. Also pictured are two quantum repeaters. The use of quantum repeaters significantly extends the range of this Wide Area Network: these data centers can be located further

from one another and still transmit the same quantum information from point-to-point over long distances, overcoming the limitation of quantum signal loss (decoherence) inherent in quantum communication.

Quantum repeaters can enhance the fidelity of qubits using entanglement purification and entanglement swapping. Entanglement purification improves the quality of entanglement (and thus the fidelity of qubits), while entanglement swapping is used to extend entanglement over long distances, which is key in maintaining the integrity of quantum information. Through these processes and in conjunction with quantum error correction, the fidelity of the qubits as they traverse the system is also increased. Quantum repeaters can facilitate quantum communication between various types of sites, not just data centers as discussed in the example above. Cloud compute sites, classical cloud sites, data centers, headquarters, campuses, and remote sites can all be connected via entanglement-based quantum networks. Entanglement-based networks using quantum repeaters are capable of connecting different types of sites - a significant advantage in quantum network design.
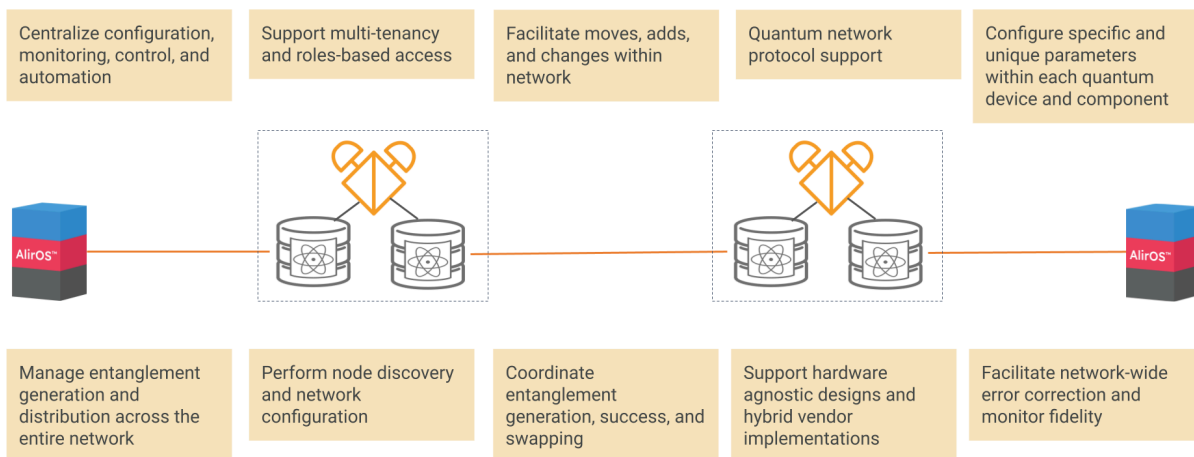
Minimizing complexity with software-defined quantum architecture

Quantum networks, with their intricate web of quantum repeaters, multiple endpoints, and reliance on both fiber optic and free space connections, are complex. Simplifying quantum network configuration, monitoring, and control is critical to their efficient and effective operation. Quantum networks consist of diverse components such as qubit sources, quantum memory modules, and optical switches. Each of these elements requires precise configuration to function correctly. Typically, quantum networks are very manually intensive to manage, requiring careful initial configuration. The risk of human error in this process is significant, and once set up, there's often a reluctance to make changes for fear of disrupting this complex quantum system.

Leveraging software-defined networking, a proven concept in classical networking, is the key to managing the complexities of quantum networks. This includes using software to define network configurations, automate processes, and make changes to the system. This offers flexibility, scalability, and the ability to integrate diverse components and protocols efficiently. It simplifies network management and ensures that all parts of the quantum network operate cohesively.

Software-defined quantum networks create a separation between the data plane (which handles the actual quantum data transmission) and the control plane (which manages how data is routed and handled). This separation simplifies network management and enhances flexibility. With a software-defined entanglement-based quantum network, administrators are able to control and monitor the entire quantum network in a centralized manner. This includes managing configurations, deploying updates, and troubleshooting. This model also allows for easier integration of new technologies and scaling of the network. As quantum technology evolves, this adaptability becomes more and more critical. A software-defined architecture enables a uniform operating model across various devices and components in the network, including different types of quantum memories and optical switches. The centralized control offered by this architecture also allows for consistent monitoring of network performance metrics, such as entanglement generation rates and qubit coherence times. An orchestrator can be deployed to automate routine tasks, reducing the risk of human error and improving the efficiency of network operations.

Simplifying Quantum Networks is a Necessity
Software-Defined Network Architecture is the Solution

Centralize configuration, monitoring, control, and automation

Support multi-tenancy and roles-based access

Facilitate moves, adds, and changes within network

Quantum network protocol support

Configure specific and unique parameters within each quantum device and component

Manage entanglement generation and distribution across the entire network

Perform node discovery and network configuration

Coordinate entanglement generation, success, and swapping

Support hardware agnostic designs and hybrid vendor implementations

Facilitate network-wide error correction and monitor fidelity

A software-defined quantum network offers:

- Centralized control: Quantum networks demand centralized configuration, monitoring, and control for efficient operation. This includes automating routine tasks and dynamically adjusting network parameters in real-time.
- Role-based access and multi-tenancy: Different users, from classical network operators to quantum specialists and security teams, require customized access and control capabilities to ensure each user can perform necessary tasks without compromising the network's integrity or security.
- Network modifications: The ability to seamlessly add new components like quantum memories or repeaters, remove devices, and decommission parts of the network (e.g., a site that is no longer in use) is crucial. This requires a system that can adapt to changes quickly and efficiently.
- Quantum protocol support: The specialized algorithms and procedures designed to facilitate communication and information processing in a quantum network - from secure key sharing to quantum error correction and all the protocols required for secure communication, efficient quantum information processing, and the realization of wide area quantum networks.
- Custom configuration support: Components within the quantum network has unique configuration requirements. Settings may need to be adjusted frequently, sometimes in real-time, based on network conditions or operational demands.
- Management of entanglement: Managing the generation and distribution of entanglement is continuous and dynamic. Entanglement pairs degrade over time and must be frequently re-established to maintain network integrity.
- Discovery support: The ability to discover different nodes within the system, and perform network configuration within the system across those nodes.
- Entanglement coordination: Precise synchronization and timing that must be coordinated across the network to ensure entanglement generation, success, and swapping.
- Hardware Agnosticism: Supporting a wide range of hardware devices and systems, regardless of manufacturer or design, is essential for a flexible and scalable network.
- Network-wide error correction and fidelity monitoring: Implementing and managing error correction protocols across the network is crucial to maintain the fidelity of quantum information. The ability to continuously monitor and evaluate qubit fidelity, from node-to-node and network-wide ensures the quality and integrity of quantum information across the network.

Quantum networks with quantum memories offer secure and efficient information infrastructures over longer distances. Specific applications include:

- **Quantum Secure Communication.** Quantum networks are capable of protecting the transmission of sensitive data between sites, such as headquarters, data centers, and campus locations. The security of these networks is grounded in the principles of quantum mechanics, making them resilient against quantum attacks as well as harvest-now-decrypt-later attacks.
- **Data center interconnectivity.** Quantum networks facilitate secure and efficient data center-to-data center communications for backup operations and redundancy. They are instrumental in data sharing and protection against ransomware.
- **Data center quantum computing infrastructure.** Modern classical data centers use classical servers and computers. Those classical servers and computers are connected to one another using leaf and spine networks. Data centers transitioning to quantum computing integration will require robust quantum networking infrastructure within the data center.
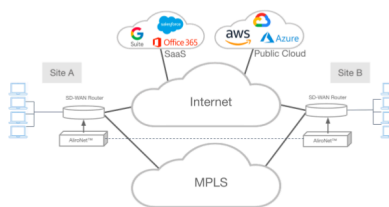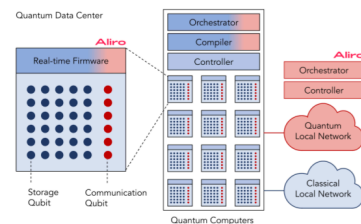
Use Cases for Quantum Networks with Memories

Highly Secure Private Networks

Data Center to Data Center and to Cloud

Quantum Computer Data Center Networks

In each of these use cases, entanglement-based quantum networks can be integrated into existing classical network infrastructures. This hybrid approach allows for leveraging the advantages of both quantum and classical systems.

The Quantum Internet

Where are we headed? Quantum networks being deployed today will be part of the evolution to the Quantum Internet.


Evolution to the Quantum Internet
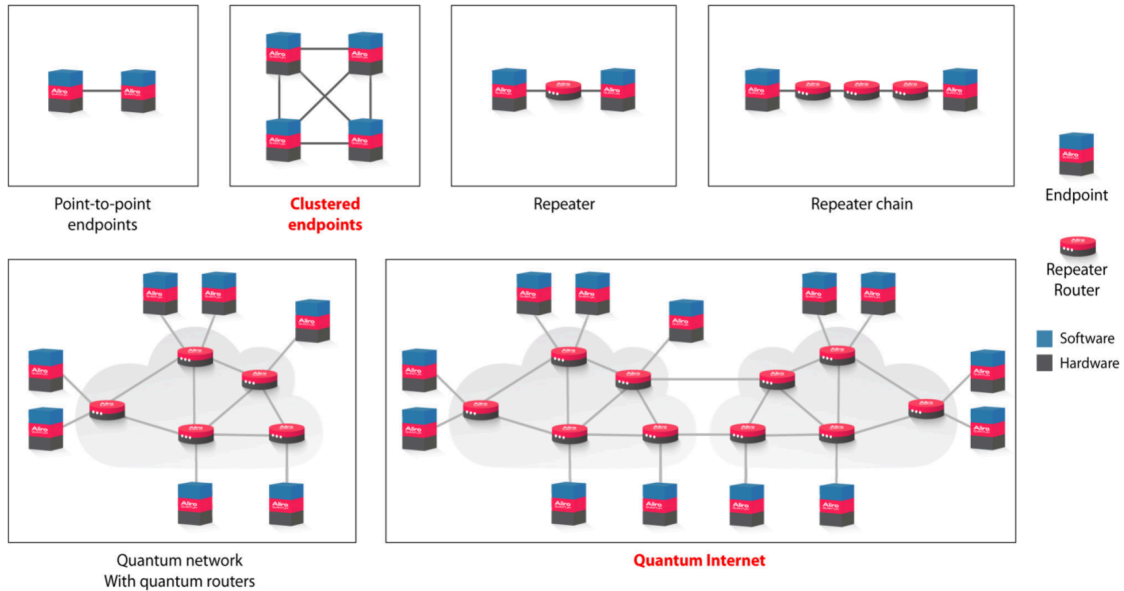
Quantum networks have been establishing point-to-point connections, which are foundational for quantum communication. Clustered endpoints are being linked through quantum communication channels. Quantum repeaters will extend distances from node-to-node. This leads to the development of repeater chains which will then lead to the establishment of more complex network structures across larger geographical areas. What is likely to unfold is the linking of these individual networks will evolve into the Quantum Internet, and it will become the premium secure infrastructure used by individuals, organizations, and agencies.

There will be a shift of the security dimension of the classical network to this more secure Quantum Internet. The development of the Quantum Internet will mirror the early stages of the classical Internet, which started with connecting universities and research labs. A similar trajectory is expected as quantum networks expand and interconnect various institutions. Today, there are a wide range of quantum networks being developed.

Quantum Networks Will Connect with One Another
Quantum Memories are Necessary for Distance, Quality, & Fidelity
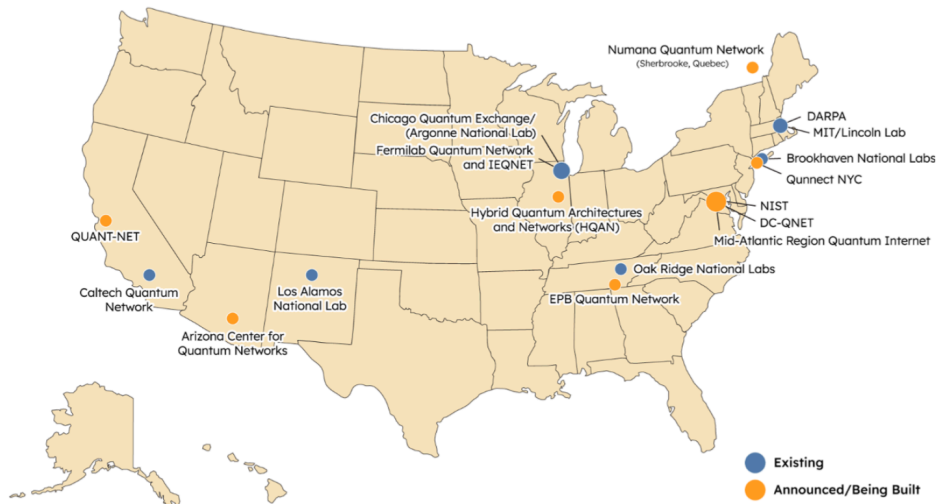
Next steps for networking organizations

Strategic steps can be taken today to ready organizations for quantum networking implementation.

Without the need for immediate investment in physical hardware or specific operating systems, organizations can begin designing and simulating their own quantum networks. This includes exploring various configurations of quantum memories and their integration into existing network architectures. A quantum network simulator can assist in the modeling of different types of quantum memories and their capabilities. This exploration can cover aspects like entanglement generation, entanglement swapping, coherence times, and overall network fidelity. Understanding these dynamics is critical for assessing how quantum networks can be implemented in real-world scenarios.

Organizations can also begin practical trials by setting up experimental quantum networks, either in-house (such as in a lab environment) or by utilizing third-party offerings, like the EPB Quantum Network, where individuals, companies, and agencies can connect to this existing entanglement-based quantum network. These trials provide invaluable experience in operating quantum networks and understanding their nuances. This experience is critical for developing the skills and knowledge required to take advantage of quantum networking technologies.

As quantum technologies continue to evolve, networking organizations should plan for the integration of quantum capabilities into their existing infrastructures and service offerings. Keeping abreast of developments in quantum technologies, regulatory landscapes, and market demands will enable organizations to adapt quickly and effectively. Early adoption and experimentation with quantum networks can lead to significant business advantages, potentially opening up new revenue streams or providing a competitive edge in the market.

Closing

Entanglement-based secure networks are being built today by a variety of organizations for a variety of use cases – benefiting organizations internally, as well as providing great value to an organization's customers. Telecommunications companies, national research labs, intelligence organizations, and systems integrators are just a few examples of the organizations Aliro is helping to leverage the capabilities of quantum networking.

Building entanglement-based quantum networks is no easy task. It requires:

- Emerging hardware components necessary to build the quantum network.
- The software necessary to design, simulate, run, and manage the quantum network.
- A team with expertise in quantum physics and classical networking.
- Years of hard work and development.

This may seem overwhelming, but Aliro Quantum is uniquely positioned to help you build your quantum network. The steps you can take to ensure your organization is meeting the challenges and leveraging the benefits of the quantum revolution are part

of a clear, unified solution already at work in quantum networks like the EPB Quantum Network℠ powered by Qubitekk in Chattanooga, Tennessee.

AliroNet™, the world's first full-stack entanglement-based quantum network solution, consists of the software and services necessary to ensure customers will fully meet their quantum networking goals. Each component within AliroNet™ is built from the ground up to be compatible and optimal with quantum networks of any scale and architecture. AliroNet™ is used to simulate, design, run, and manage quantum networks as well as test, verify, and optimize quantum hardware for network performance. AliroNet™ leverages the expertise of Aliro personnel in order to ensure that customers get the most value out of the software and their investment. Depending on where customers are in their quantum networking journeys, AliroNet™ is available in three modes that create a clear path toward building full-scale entanglement-based secure networks: (1) Emulation Mode, for emulating, designing, and validating quantum networks, (2) Pilot Mode for implementing a small-scale quantum network testbed, and (3) Deployment Mode for scaling quantum networks and integrating end-to-end applications. AliroNet™ has been developed by a team of world-class experts in quantum physics and classical networking.

To get started (or continue on your quantum journey), reach out to the Aliro Quantum team for additional information on how AliroNet™ can enable your quantum network.

For additional information or for any questions you may have about quantum networking or the content of this paper, contact us at info@aliroquantum.com