Aliro QUANTUM®

The Evolution of Quantum Repeaters

Aliro Quantum

www.aliroquantum.com @aliroquantum @aliroquantum

Introduction

Entanglement-based secure networks are capable of transmitting and manipulating quantum states across far distances. These networks hold the promise of revolutionizing secure communication, enhancing computation power, and enabling breakthroughs in distributed quantum sensing across many industries. However, the inherent fragility of quantum states poses a significant challenge when it comes to transmitting quantum information over long distances. While other methods exist for extending the distance of quantum communication channels, quantum repeaters will help pave the way to the realization of large-scale wide area quantum networks.

This white paper addresses the role of quantum repeaters in extending the reach and reliability of Quantum Secure Communication. By delving into the fundamental principles and operational mechanisms of these devices, this paper aims to foster a deeper understanding of their operation, as well as set expectations as quantum repeaters advance in development and as they are deployed in entanglement-based quantum networking topologies.

Entanglement-based Secure Networks

Entanglement-based secure networks offer a wide range of use cases by harnessing the unique properties of quantum entanglement to provide unparalleled levels of security and communication capabilities. The primary goal of entanglement-based quantum networks is to distribute the entanglement between members of the network.[ENTANGLEMENT] Aliro entanglement-based secure networks support local area networks, campus area networks, metro area networks, and wide area networks with a secure connection that is maintained end-to-end with direct fiber connections, free space connections, and, as they become commercially available, quantum repeaters or routers.

Over time, this same entanglement-based secure network that reliably maintains real-time quantum secure communications can be scaled to carry traffic beyond establishing encryption keys from site to site. There are a variety of use cases enabled by entanglement-based secure networks, including:

- Secure communication channels: Entanglement-based secure networks can establish highly secure communication channels between distant parties. By exploiting the phenomenon of entanglement, these networks offer tamper-proof transmission of information, providing end-to-end encryption and protecting against unauthorized access.
- Quantum secure direct communication: Entanglement-based secure networks enable direct and secure communication between two parties without the need for transmitting encryption keys. By establishing a shared entangled state, information can be transmitted securely and directly, mitigating potential information leakage.
- Distributed quantum sensing: Entanglement-based secure networks offer significant advantages in sensor networks, enhancing their sensitivity and precision. By entangling the states of multiple sensors, the network can facilitate collective measurement and correlation of physical properties with improved accuracy, enabling applications such as precise metrology, environmental monitoring, and detecting minute changes or anomalies.
- Distributed and blind quantum computing: Entanglement-based secure networks play a crucial role in secure quantum computing. By establishing entanglement between cloud servers and remote sites, data privacy and security are ensured during the computation process, protecting sensitive information from potential attacks or unauthorized access.

Entanglement-based secure networks offer a new paradigm of secure information exchange, revolutionizing industries that demand uncompromising security and privacy, while simultaneously enabling other applications - including the creation of the Quantum Internet.

Scaling Entanglement-based Secure Networks

The need for entanglement-based secure networks is clear. However, progress is hindered by the ability to scale these networks beyond LANs and MANs to WANs. To scale geographically, entanglement-based wide area networks must use a variety of technologies.[ROADMAP] In order of maturity, the following technologies can be used to extend the distance between nodes:

- Free space / Terrestrial satellites
    - Satellite based intercontinental quantum networks.
    - Air-based mobile platforms (e.g. airplanes, drones) connected to the quantum network using free-space lasers.
    - Free space laser telescope communications between stationary endpoints (e.g. buildings without fiber connectivity).
- Ground station to satellite
    - Land-based mobile platforms (e.g. trucks, tanks) connected to the quantum network using free-space lasers.
- Ground deployment (via fiber optic cable)
    - Fiber-based secure communications between locations in a state or country, enabled by quantum repeaters and routers

Satellites and lasers provide the best quantum communication channels today. However, to truly scale up to a global network, quantum repeaters will be required to mitigate the detrimental effects of quantum noise and signal degradation that arise during long-distance ground deployments via fiber optic cable. By leveraging the principles of quantum entanglement and entanglement swapping, quantum repeaters enable the efficient distribution of entanglement across network nodes, facilitating long-range quantum communication with unprecedented fidelity and efficiency.

Introduction to Quantum Repeaters

Before exploring the role of quantum repeaters in the quantum internet, let's consider a comparable device: the "classical" repeater.

The classical Internet transfers information in the form of bits along conduits such as fiber optic cables. Some of these cables travel long distances, such as the SEA-ME-WE 3 undersea cable that reaches from Germany to Japan. However, as light passes through these fibers, it suffers from loss: the photons can disappear, or they can get lost as they're traversing the fiber. To account for this, a repeater is inserted between nodes. Repeaters measure the signal coming in, copy it, then retransmit it at higher power. As a result, the Internet is able to transmit information reliably over very long distances.

Loss is a problem in quantum networks as well. However, the same technique of measuring, copying, and retransmitting doesn't work in quantum communications. This is due to a fundamental aspect of quantum information: it cannot be copied. This fact is known as the no-cloning theorem.

It turns out that quantum states cannot be measured on their way from point A to point B without destroying them. This actually enables Quantum Secure Communication, but also means the same idea for mitigating loss in classical repeaters won't work for entanglement-based secure networks.

In addition to loss, entanglement-based networks are very sensitive to noise. Noise comes in the form of physical vibrations, temperature, and other environmental factors.

How do we overcome transmission losses and the introduction of noise in an entanglement-based quantum network?

Quantum repeaters play a key role in generating reliable, end-to-end entanglement by fulfilling 3 central roles: establishing link-layer entanglement, building entanglement sessions from elementary links, and detecting and managing errors[VANMETER] caused by noise and loss.

How Quantum Repeaters Work

Despite their name, quantum repeaters use a very different strategy than classical repeaters to handle the problem of loss. Quantum repeaters mitigate this problem of loss by segmenting long links into much shorter links, and using entanglement swapping to extend the range of the entanglement and distribute it across the network.

This is achieved through:

Elementary Entanglement Generation: Entanglement generation starts with a request from two end nodes to generate entanglement. From there, entanglement must first be established on each link. Later we will see how elementary entanglement can be stitched together into end-to-end entanglement.

Entanglement Swapping: Quantum entanglement networks use quantum repeaters to create end-to-end entanglement indirectly. Quantum repeaters consume elementary link-layer entanglement at each hop to produce end-to-end entanglement. This is achieved through a process called entanglement swapping.[SWAPPING]

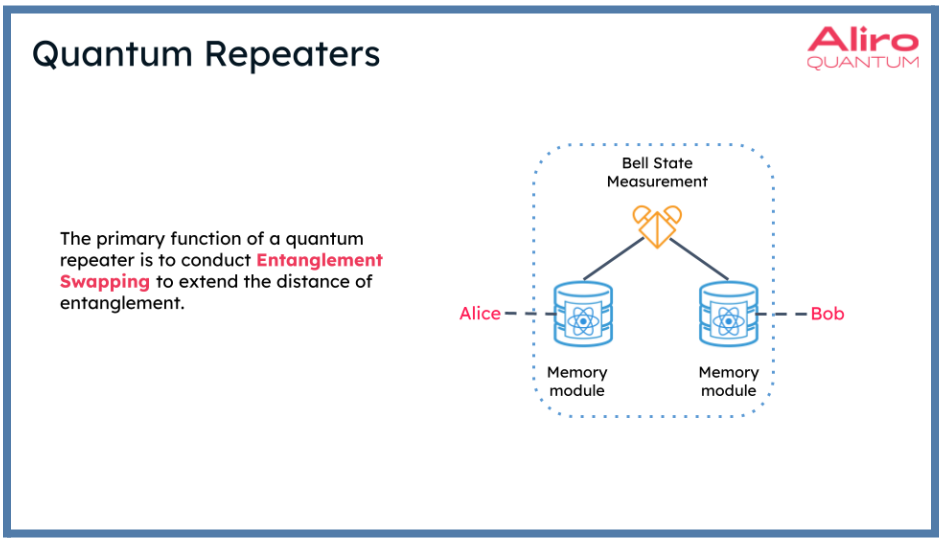
Entanglement Purification: As entangled states are propagated across the network, they accumulate noise, which reduces the quality of entanglement. Purification combats this issue by producing one high-quality entangled pair from a collection of low-quality entangled pairs.

Teleportation: Once reliable high-quality entanglement is established between endpoints, qubits can be transported using quantum teleportation. This is the service provided by the quantum transport layer. Teleportation consumes an entangled pair provided by the network in order to transmit a user qubit from one endpoint to another. This process is inherently secure, since no quantum data is transmitted across the network. A classical message, which does not include any state-related information, is required to correct the output state.

Entanglement distribution unlocks all kinds of applications, including even transmitting qubits.

Example 1: What happens inside a quantum repeater (basic)

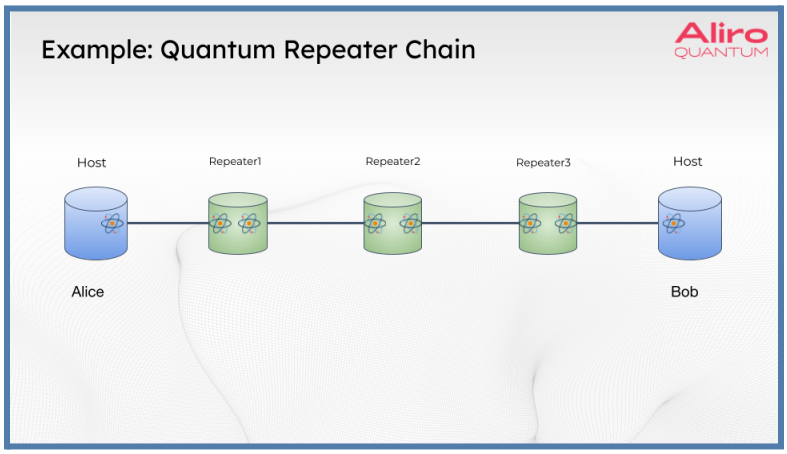
There is entanglement between Alice and a memory module in the repeater. Similarly, Bob is entangled with another memory module inside the same repeater.



Once those entanglements are established, the entangled photons can be emitted to a Bell state measurement station to perform the entanglement swapping operation. The entanglement swapping operation essentially creates a direct entanglement between Alice and Bob in this example.

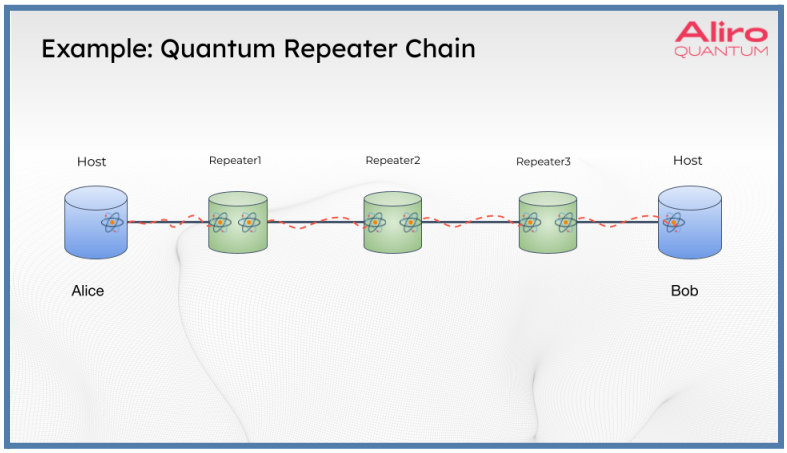
Example 2: Entanglement swapping in a chain of repeaters

This is a five node network in a chain topology. Alice and Bob are too far apart to make a direct link between each other in this entanglement-based secure network. There are three repeaters between Alice and Bob.

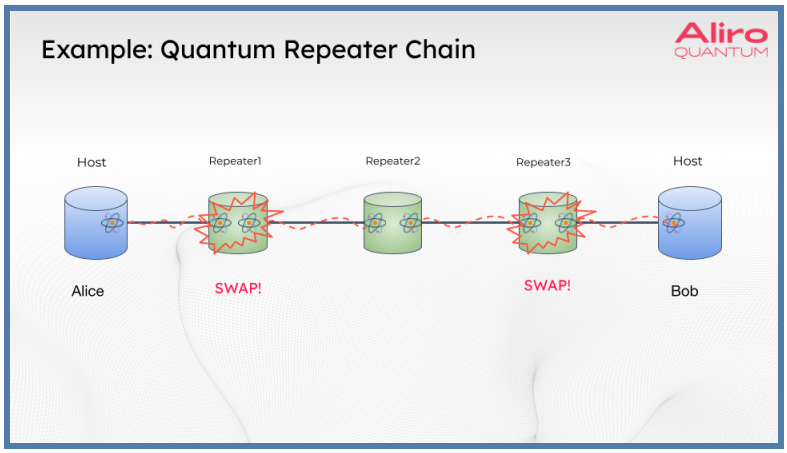


The goal of this small network, the service it is providing, is entanglement between these 2 distant end nodes, Alice and Bob, at a high rate of high fidelity. Photons are used in this network to generate and distribute entanglement. However, single photons are fragile and can be lost in the fiber along the way. The probability that photons actually are lost increases exponentially with distance, which is why direct links to every node aren't possible. Quantum repeaters will need to extend the distance of this entanglement.

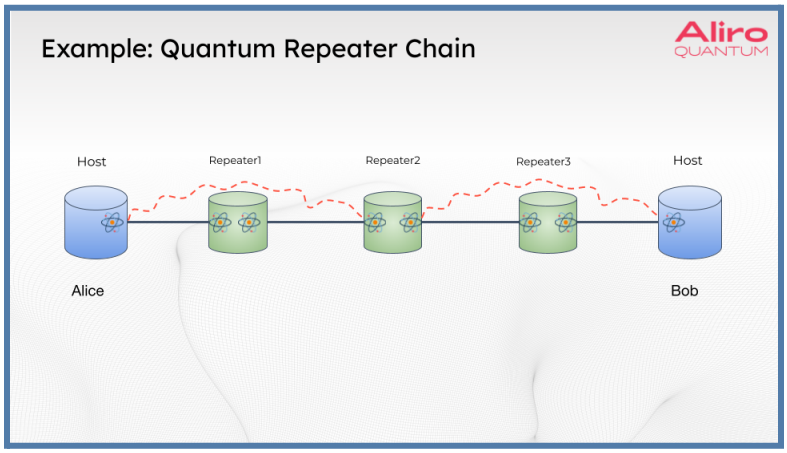
The first step in entangling Alice to Bob is elementary entanglement generation, or point-to-point entanglement. This is short distance entanglement between neighboring nodes.



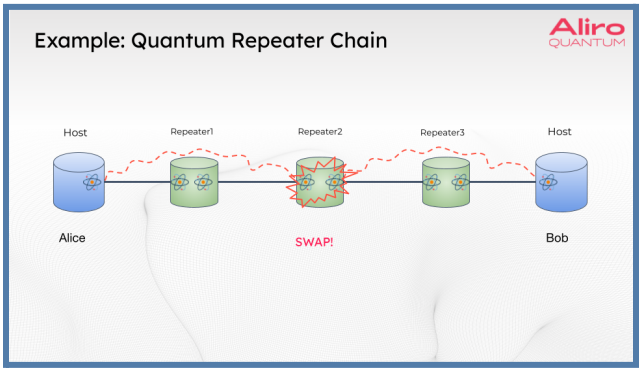
This begins with point-to-point links, and then these point-to-point links are stitched together with entanglement swapping. Entanglement swapping is a clever way to resolve the problem of loss without violating the no-cloning theorem. A quantum repeater uses entanglement swapping to create long distance entanglement between nodes. In this case, repeater one does the first entanglement swap, resulting in a slightly longer distance entanglement between Alice and repeater two in the middle. Bob's node undergoes the same process as repeater three does a swap.

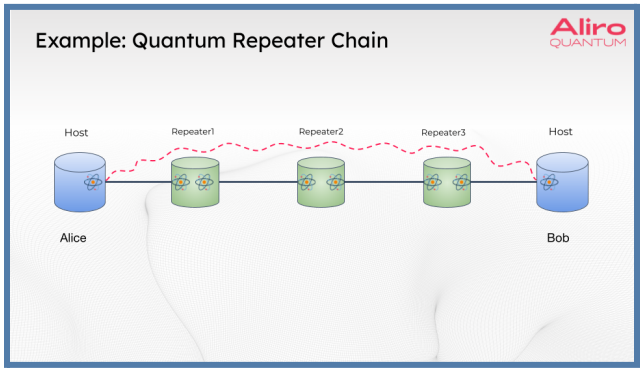


At this point, there are two entanglement segments spanning the distance between Alice and Bob.



The final entanglement swap in the middle will stitch these two entanglements together, creating a long range entanglement between Alice and Bob. In this way, a first generation quantum repeater distributes entanglement.



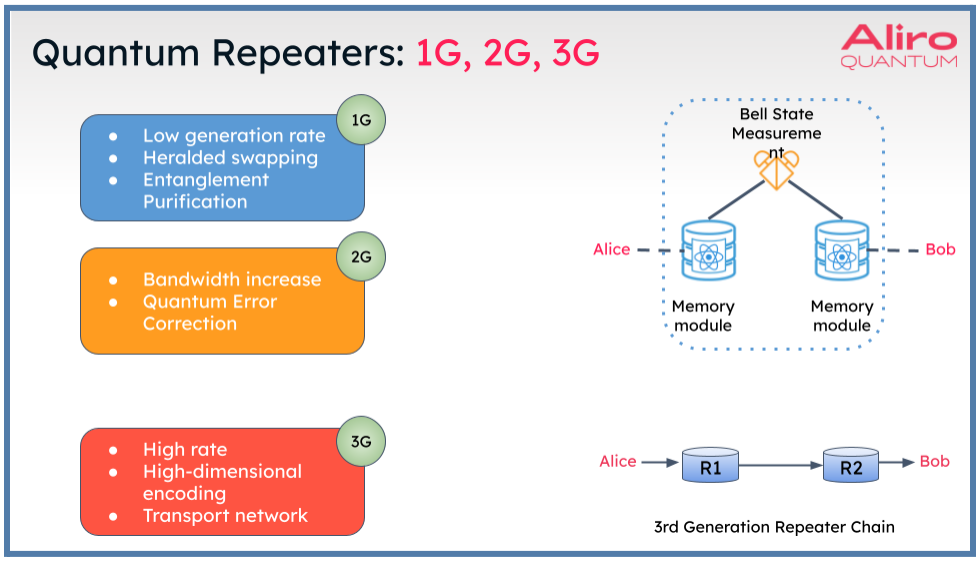


While the act of stitching together two separate entanglement links may sound magical, the quantum repeater accomplishes this stitching by using a simple operation called teleportation. As long as the quantum repeater has qubits that are entangled with pairs at each node, in this case Alice and Bob, it can perform a measurement and report to Alice and Bob the information they need to use their newly entangled connection. Building up a chain of repeaters breaks down long distances into more manageable segments over which to send photons.

Another process that early quantum repeaters will enable is entanglement purification. The quality of the entanglement, also known as fidelity, may not be high enough for the intended purpose. If this is the case, an operation called distillation or purification can be performed. This involves taking multiple entangled qubit pairs that are weakly entangled and combining them into a single pair that is strong, with high enough fidelity for your purposes. By performing multiple rounds of swapping and distillation, the elementary entanglements produced in the first step are converted into a stream of high-fidelity end-to-end entanglements.

The Evolution of Quantum Repeaters

A step-by-step evolution of quantum repeater technology has emerged, separating repeaters into three categories: 1st generation, 2nd generation, and 3rd generation.[REPEATERS] These generations do not necessarily make the previous generation obsolete, but they show how networks can expand to support increasingly powerful applications as the technology improves. Each new generation is better at meeting the challenges of the two biggest hurdles to long distance quantum networking: loss and noise.



1G quantum repeaters

First generation quantum repeaters can conduct entanglement swapping operations in a heralded manner. The swapping operation is confirmed as successful or not successful.

Quantum repeaters rely on quantum processors to accomplish their task. However, today's quantum processors are error-prone. To make up for this, first generation repeaters will use a process called entanglement distillation. Entanglement distillation "distills" a high quality entanglement from many copies of low quality entanglement. While a network with 1G quantum repeaters will enable groundbreaking applications, its communication rate is limited by the process of distillation.

2G quantum repeaters

2G quantum repeaters will increase bandwidth, as these repeaters are better at generating entanglement at a higher rate and higher fidelity. As error rates improve, quantum repeaters will transition from relying on entanglement distillation to using quantum error correction to fix operation errors. 2G quantum repeaters have quantum processing capabilities to perform quantum operations on these quantum states at the actual repeater, and can perform quantum error correction to detect and correct for errors that may have occurred on the quantum state.

Quantum error correction corrects errors by encoding information into blocks of qubits, where errors can be more easily mitigated. This allows networks to transfer information at much higher speeds and enable further applications.

3G quantum repeaters

As quantum devices improve, quantum error correction will be used to handle both loss and operation errors. Essentially, this allows nodes to trust that their information will travel safely to other nodes, without having to listen and hear from each repeater that entanglement was established.

In 3G quantum repeaters, there is an important paradigm shift. In first and second generation repeaters, each link in the path from node to node will need to establish link-wise entanglement independently, and these are subsequently stitched together via entanglement swapping to generate the end-to-end entanglement between distant nodes. Third generation quantum repeaters do not use entanglement swapping and behave more like a transport network, similar to the classical Internet. Third generation quantum repeaters will enable

similar performance in quantum networks. At each hop in the path, a 3G quantum repeater will use error correction to correct for any errors that the logical quantum state may have incurred while traveling from the previous node. This is similar to classical networks with feed-forward error correction. For example, in the case of entanglement distribution from node A to node Z, the entangled state can just be physically transported from A to Z via 3G repeaters. These 3G repeaters operate at high rates, enabling even more complex applications on the entanglement-based quantum network.

Building Entanglement-based Quantum Networks Today

To build a universal entanglement-based quantum network is no easy task. It requires:

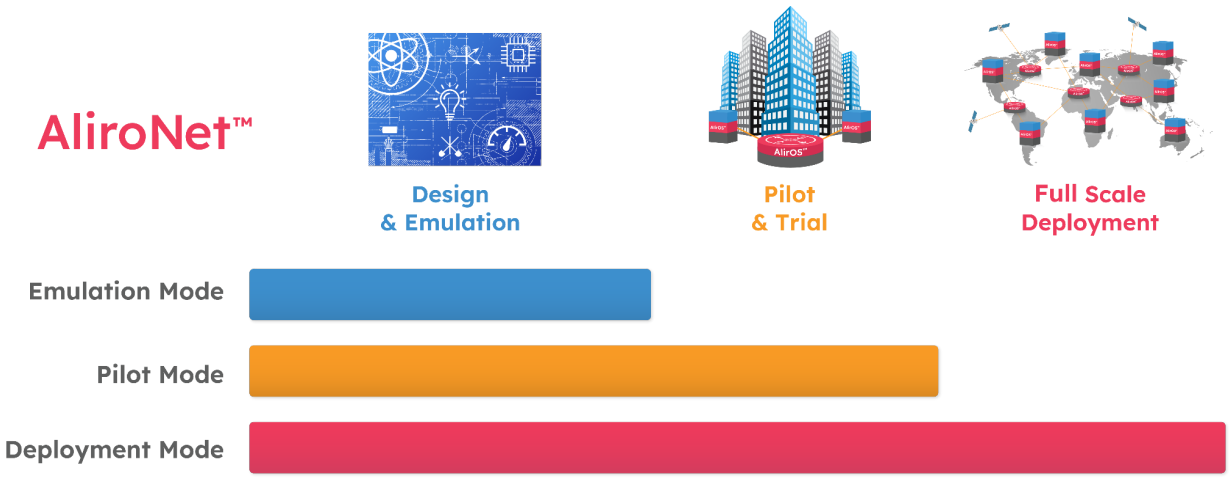
- Emerging hardware components necessary to build the quantum network.
- The software necessary to design, simulate, run, and manage the quantum network.
- A team with expertise in quantum physics and classical networking.
- Years of hard work and development.

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 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 journey, 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. Each mode of AliroNet™ corresponds to three phases of building a quantum network with the deliverable of Deployment Mode being the user's deployed full-scale entanglement-based quantum network. We discuss how each AliroNet™ mode provides the software and services necessary to best meet the requirements of its corresponding phase in accordance with the user's needs.



Emulation Mode

Before an organization builds a quantum network of any scale, they must first identify their quantum networking plans, goals, budget, and risks. Then the organization must design (e.g. choose (or build) and optimize hardware, configurations, protocols, etc.) the quantum network in accordance with this information.

Designing a quantum network in the most effective and efficient way requires the use of a quantum network simulator capable of emulation of quantum network hardware equipped with user-chosen components, configurations, and protocols. Users will need to gain familiarity with the software and leverage relevant knowledge and experience to use it for their design needs. Even with these pieces, building the desired models and protocols is time-consuming and can require intimate (and not publicly-available) knowledge of existing hardware.

AliroNet™ Emulation Mode includes Aliro Simulator, a world-leading quantum network simulator software package, and a suite of services to ensure users meet and exceed their assessment, emulation, and design requirements. These services leverage the Aliro team expertise and experience with quantum networks – and specifically with using Aliro Simulator for internal and external quantum network design purposes – as well as Aliro familiarity and relationships with quantum network hardware vendors. These services include: an initial assessment consultation, user, technical, use-case, and logistics support, and frequent – often user-driven – enhancements.

Pilot Mode

Next, the organization will then build a pilot – a small-scale quantum network used to test and optimize performance and gain internal familiarity with the technology.

The organization will need to acquire (or build) the hardware components, operating system (i.e., the distributed on-device software that is run to generate high-fidelity end-to-end entanglement at a high rate), the controller (i.e., the centrally located software that manages each instance of the operating system), and the orchestrator (i.e., the user interface that allows operators to setup, configure, manage, and monitor their network and controller). The organization must then assemble – install, connect, and integrate components according to the network design (identified in Phase 1) – their pilot quantum network. The organization will use the assembled pilot to test the interoperability of the quantum systems with existing systems, hardware components, software products, and protocol stack. Finally, the organization will use the test results to calibrate its hardware, debug its software, and/or tune its protocols in order to reach its desired network performance. Even if an organization is to acquire existing hardware and software, the process of assembling, testing, and optimizing the network is time-consuming and requires expertise with each part of the network. Building its own hardware and software adds considerable delay to each of these required steps.

Building on all the products and services included in AliroNet™ Emulation Mode, AliroNet™ Pilot Mode includes access to AlirOS™ (Aliro's operating system software), the Aliro Controller (Aliro's controller software), and the Aliro Orchestrator (Aliro's orchestrator software), in addition to a suite of services to ensure users meet and exceed their pilot goals. These services leverage the Aliro team expertise and experience with quantum networks – and specifically with implementing Aliro software on hardware. These services include: hardware acquisition, on-premises implementation, interoperability testing and integration, hardware calibration, software debugging, protocol tuning, and a joint publication, if desired.

Deployment Mode

Finally, the organization will scale its pilot quantum network to a full-scale quantum network capable of running the organization’s desired end-user applications.

Deployment Mode services and requirements are quite similar to those of Pilot Mode, albeit on a much larger-scale and more directly geared toward enterprise applications. However, the story does not end with the deployment of the network. As technology improves, the organization's requirements change, etc. it is likely the organization will want to upgrade and scale its network. The organization will also want to be able to use its quantum network to its full potential with as few complications as possible. Hence, deployment mode includes services to help continue to upgrade and scale the deployed networks as well as network management and maintenance support.

Deployment Mode is also available in an orchestration-only configuration which may be used to configure, control, and manage third-party control software running on third-party hardware components.

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.

info@aliroquantum.com

www.aliroquantum.com

REFERENCES

[ENTANGLEMENT] Briegel, H.J., Cirac, J.I., Dür, W., Giedke, G., Zoller, P. Quantum Repeaters for Quantum Communication. In: Greenberger, D., Reiter, W.L., Zeilinger, A. (eds) Epistemological and Experimental Perspectives on Quantum Physics. Vienna Circle Institute Yearbook [1999], vol 7. Springer, Dordrecht. https://doi.org/10.1007/978-94-017-1454-9_11

[REPEATERS] Muralidharan, S., Li, L., Kim, J. et al. Optimal architectures for long distance quantum communication. Sci Rep 6, 20463 (2016). https://doi.org/10.1038/srep20463

[ROADMAP] Antonio Acín et al. The quantum technologies roadmap: a European community view. New J. Phys. 20 080201 (2018). https://doi.org/10.1088/1367-2630/aad1ea

[SWAPPING] Duan, LM., Lukin, M., Cirac, J. et al. Long-distance quantum communication with atomic ensembles and linear optics. Nature 414, 413–418 (2001). https://doi.org/10.1038/35106500

[VANMETER] Van Meter, Rodney. Quantum Networking. John Wiley & Sons, Ltd. 2014