AliroNet™ Solution Brief

Full-Stack Quantum Networking Solution

Enterprises and governments are racing to address the evolving threat landscape which includes Harvest Now Decrypt Later (HNDL) infiltrations, sophisticated Man-in-the-Middle attacks, and hacks by evolving quantum computers. Attention is turning to Quantum Networks which leverage entanglement to mitigate these security threats while supporting new applications unaddressable with existing networks.

Addressing the challenges and leveraging the benefits of Quantum Networking using entanglement

Existing networks use legacy encryption making them obsolete and vulnerable to attacks. Quantum Networks are necessary to support modern encrypted data, voice, and video communications requirements.

Data, Voice, and Video Security

The security of asymmetric algorithms (e.g. RSA, DSA, DH, ECDH), used for authentication and key establishment for nearly all of today's encrypted traffic, relies on the assumption that it is infeasible for classical computers to solve certain mathematical problems. These math-based encryption algorithms are used pervasively to protect communications, access, and data. Once quantum computing reaches its potential, it will be able to break encryption that relies on prime factorization or discrete logarithms.

Encrypted systems, networks, communications, devices, and data will be rendered transparent as these asymmetric schemes will be easily broken by practical quantum computers. Legacy encrypted VPNs and SSL connections will be no more effective at safeguarding sensitive data than delivering the information unencrypted over the open Internet.

Due to Harvest Now Decrypt Later attacks, it must be assumed that all of an organization's encrypted information transmissions and communications before implementing Quantum Networking is non-secure. With HNDL an adversary steals encrypted data they cannot currently decrypt, and holds onto this encrypted data until they are able to decrypt the contents using quantum computers. Methods to address the security vulnerabilities posed by these threats include:

Quantum Key Distribution (QKD) - "prepare-and-measure" quantum key distribution protocols that run on and are enabled by prepare-and-measure single-purpose networks (QKD networks). These networks only facilitate the exchange of a key protecting data - no other application is supported over this type of single-purpose network. In addition, they rely on trusted nodes, where all encrypted information is decrypted and exposed during transmission.

Post Quantum Cryptography (PQC) - replace or augment in-use classical cryptographic algorithms with those that are assumed to be quantum-secure, but are not yet provably quantum-secure *and* classically-secure. At least two of the National Institute of Standards and Technology (NIST) finalist PQC algorithms have already been found to be non-secure, and were cracked using conventional computers meaning this approach may not be a viable solution.

Quantum Secure Communication (QSC) - security protocols that run on entanglement-based multipurpose quantum networks. QSC protocols are provably secure and enable other applications, such as private access to clouds and data centers, networked quantum computers, and interconnected quantum sensors to run over the same quantum networking infrastructure making them future proof.

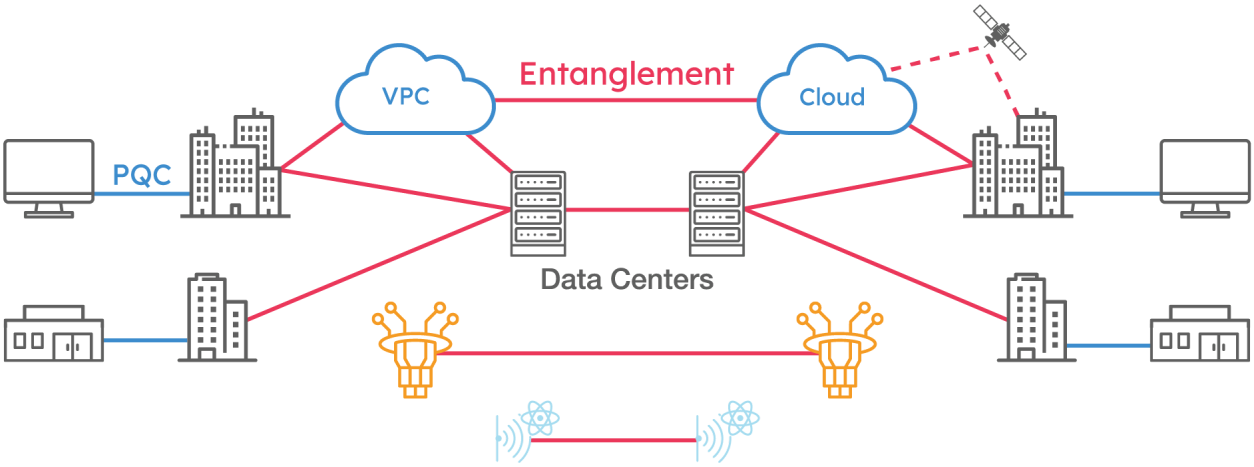
Advanced Secure Network (ASN) - an end-to-end solution, incorporating PQC at the edges of the network and leveraging quantum networks for secure data transmission using QSC. These networks are resilient against current and future cryptographic threats, and maintain the flexibility of entanglement-based quantum networks.

Quantum Secure Communications Using Entanglement

Now that public organizations and Enterprises are understanding the evolving threat landscape from HNDL, sophisticated man-in-the-middle attacks, and hacks by quantum computers, they're investing in a long-term solution to protect their data, voice, and video while leveraging the new benefits that are only possible with a modern entanglement-based quantum network that interoperates with PQC.

Quantum Networks simultaneously enable superior security and support for newer entanglement applications:

- Provably quantum-secure methods of protecting access and data are physics-based instead of math-based, which are necessary due to HNDL attacks.
- Multiple types of entanglement technology supported simultaneously: sensors, computers, qubit architectures, etc.
- Existing classical network and PQC interoperability.



for Secure Communications • Quantum Sensors • Quantum Computers

Scaling Compute Power

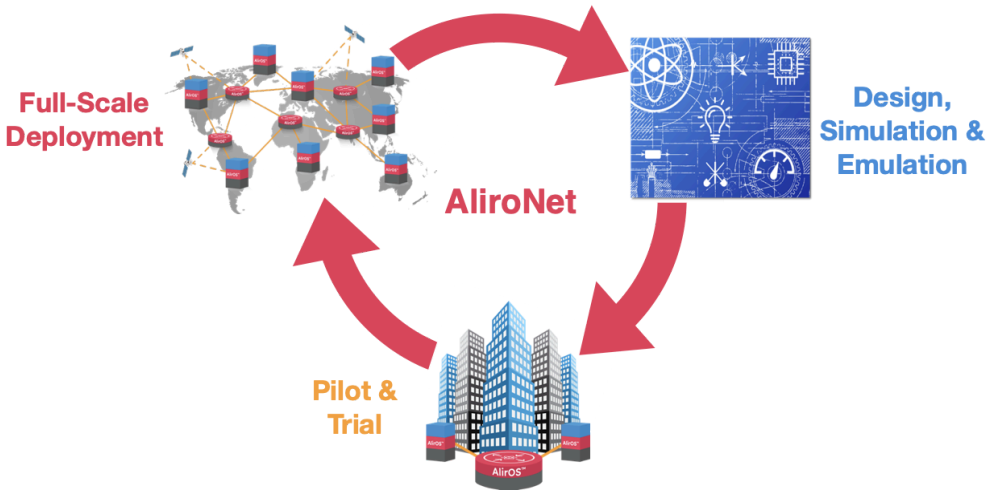
To reach a sophisticated level, quantum computers will need to be linked securely and be able to exchange and manage data between different nodes.

Securely networking quantum computers located in a single location or across larger geographic locations will enable quantum computing to scale in performance more rapidly to capabilities their classical counterparts may never be able to provide. Quantum computer clusters will be able to achieve substantially higher performance and have the potential of solving more complex problems including logistics optimization, cryptanalysis, and material design.

Similarly, quantum sensors offer superior accuracy, stability, sensitivity, and precision over their classical counterparts and can enable tasks that are infeasible with classical sensors. Networking multiple quantum sensors connects multiple geographically dispersed quantum sensors to one another and to centralized processing, storage, and analytical systems. This enables non-local measurements for advanced use cases for energy, utilities, geography, and environmental measurements, analysis, and correlation.

AliroNet

AliroNet™ is the world's first software-defined quantum network architecture. AliroNet quantum networks are capable of supporting a wide variety of applications including modern secure communications, secure access to cloud and data centers, and networking of quantum computers and sensors. Aliro also provides quantum network simulation as a professional service or as an on-premises offer.



AliroNet includes three modes of operation: (1) Full Quantum Network Deployment Mode for a scalable Quantum Network and integration of end-to-end applications, (2) Pilot Mode for implementing a small-scale Quantum Network testbeds (3) Emulation Mode for designing, simulating, emulating, and validating Quantum Networks before ever having to purchase hardware. Each mode of AliroNet corresponds directly to one of the three necessary phases of building a Quantum Network with a deliverable of Deployment Mode being the user's deployed full-scale entanglement-based Quantum Network. AliroNet includes Aliro's proprietary operating system, AlirOS™, which runs on or adjacent to quantum network hardware devices.

Emulation Mode

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

Effectively and efficiently designing a Quantum Network requires the use of a quantum network simulator capable of emulation of quantum network hardware equipped with user-chosen components, configurations, and protocols.

AliroNet Emulation Mode includes Aliro Simulator, world-leading quantum network simulator software, 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 as well as Aliro familiarity and relationships with hardware vendors.

These services include: an initial assessment consultation, technical, use-case, logistics, and frequent (often user-directed) enhancements.

Pilot Mode

An organization can then move forward with building a pilot – a small-scale quantum network used to test and optimize performance and gain internal familiarity with the technology.

The organization will acquire the hardware components, choose an operating system (i.e., the distributed on-device software that generates high-fidelity end-to-end entanglement at a high rate), choose a controller (i.e., the centrally located software that manages each instance of the operating system and/or devices), and select an orchestrator (i.e., the user interface that allows operators to setup, configure, manage, and monitor their network and controller). The organization can then assemble, install, connect, and integrate components according to the network design of 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. In addition to all the products and services included in AliroNet Emulation Mode, AliroNet Pilot Mode includes access to AlirOS, Aliro Controller, and Aliro Orchestrator, 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.

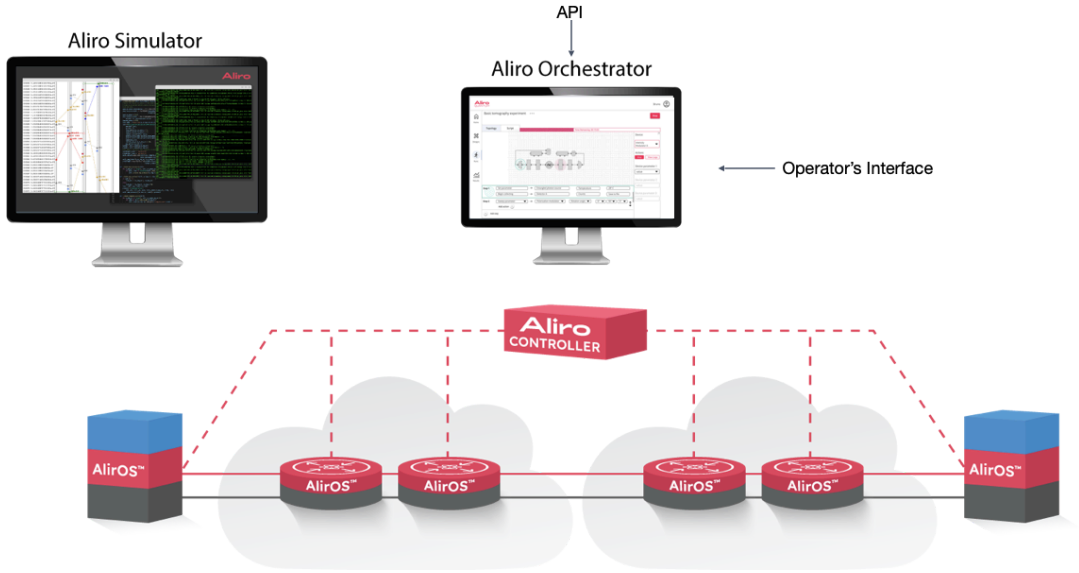
Deployment Mode

Ultimately, the organization will scale its pilot to a full-scale Quantum Network, potentially incorporating PQC as well as QSC. This network is capable of running all 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 requirements evolve and the organization's topology changes, changes, upgrades and scales of the network is inevitable.

The organization will also want to be able to use its Quantum Network to its full potential with as few challenges as possible. Hence, deployment mode includes services to help continue to upgrade, change and expand the deployed network as well as network management and maintenance support.

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



AliroNet Software Components

AliroNet includes Aliro Orchestrator, Aliro Controller, AlirOS, and Aliro Simulator. **Aliro Orchestrator** software manages the entire life cycle of a Quantum Network and provides a unified, intuitive application through which network operators can see everything, control everything, and leverage automated network operations. **Aliro Controller** software serves as a centralized brain for the Quantum Network stack, controlling all end devices and AlirOS instances. **AlirOS** is the software stack that runs on or adjacent to the quantum network end-nodes, devices, components, and repeaters. **Aliro Simulator** software is a versatile, modular, insight generating Quantum Network simulator equipped to model the smallest optical components up to large heterogeneous networks with extreme physical accuracy.

Getting Started

AliroNet mitigates technology lockout by allowing your organization to test, validate, and incorporate more powerful quantum network hardware as it becomes available, ensuring you're ready for any new advances. The next step is to begin the planning and preparation phase: assessment, design, and simulation of your Quantum Network needs. Send an email to info@AliroTech.com to get started.

About Aliro

Aliro, The Quantum Networking Company®, offers AliroNet™ to run entanglement-based Quantum Networks for applications such as Quantum Secure Communications (QSC), secure access to clouds and data centers, networking of quantum computers, and networking of distributed quantum sensors. AliroNet is also used to implement comprehensive Advanced Secure Networks which include Post-Quantum Cryptography (PQC). Aliro provides quantum network simulation as a professional service or as an on-premises offer. AliroNet™ users include utility companies, telecommunications providers, public sector organizations, enterprises, and researchers who are simulating, designing, piloting, orchestrating, and building the world's first quantum networks. Visit us at AliroTech.com.