Aliro QUANTUM®

AliroNet™ Solution Brief

The World's First Full-Stack Entanglement-Based Quantum Network Solution

Industries, organizations, and governments across the globe are racing to implement quantum technology to achieve advancements needed to solve the most pressing and challenging problems of our time. Attention is turning to quantum networking as a path to mitigate security threats posed by classical and quantum computing while simultaneously scaling the potential of quantum technology to solve problems we cannot address using classical technology alone.

Addressing the challenges and leveraging the benefits of the quantum technology revolution

Quantum technology is the next technological revolution, bringing transformation and disruption across entire industries as it reaches its full potential.

Communication, information and data security

The security of asymmetric algorithms (e.g., RSA, DSA, DH, ECDH), used for authentication and key establishment, rely on the assumption that it is infeasible for classical computers to solve certain mathematical problems. These math-based encryption algorithms are commonly used 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. Secured systems, networks, communications, devices, and data will be rendered transparent as these asymmetric schemes will be easily broken by practical quantum computers. Traditional encrypted VPNs and SSL connections will be no more effective at safeguarding sensitive data than hosting the information on the open Internet. Due to "harvest now, decrypt later" attacks, it must be assumed that all of an organization's encrypted information and communications from before it implements appropriate quantum-safe security measures (regardless of the state of quantum computing at that time) is non-secure. Harvest now, decrypt later (HNDL) attacks are attacks in which an adversary steals encrypted data they cannot currently decrypt, and holds onto this encrypted data until they are able to decrypt the data using quantum computers.

Existing methods to address the security vulnerabilities posed by quantum computing are:

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

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

Quantum Secure Communication (QSC) - entanglement-based quantum security protocols that run on entanglement-based multipurpose quantum networks. QSC protocols are provably secure and

enable other applications, such as distributed quantum computing and distributed quantum sensing to run over the same multipurpose quantum network infrastructure which provides additional value to the users.

Scaling computing and sensing power

To reach a sophisticated level, quantum technology will need to be linked securely and capable of exchanging and managing quantum data between different nodes, such as quantum computers, and quantum sensors.

Networking quantum computers located within 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 computing clusters will be able to achieve substantially higher performance and the potential of solving much more complex problems such as logistics optimization, cryptanalysis, or 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, called distributed quantum sensing, 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.

Entanglement-based quantum network solution

Now that public and private organizations are understanding the potential threats and opportunities created by quantum technology, they're investing in solutions to protect their security and data while leveraging the benefits that are possible with it. Entanglement-based quantum networks simultaneously enable both quantum-safe data security and the interconnecting of quantum technology for advanced computing and sensing performance:

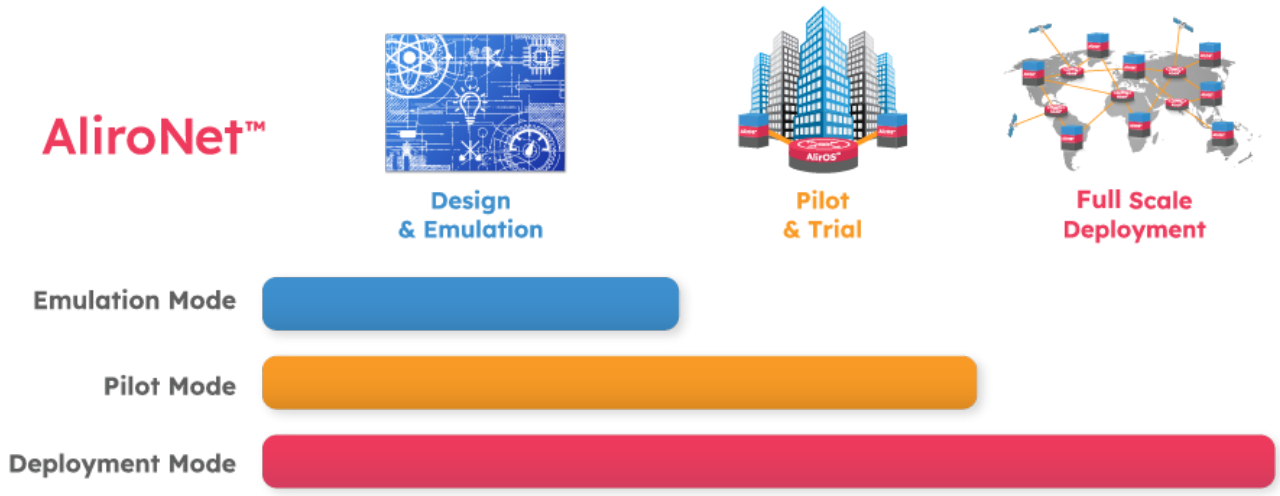
- Provably quantum-secure methods of protecting access and data are physics-based instead of math-based, which are necessary in the short term due to HNDL attacks.
- Capable of supporting multiple types of quantum technology simultaneously: quantum sensors, quantum computers, varying qubit architectures, etc.
- Compatible with existing classical networks
- Minimize the difficulty, resource-intensiveness, and time to implementation.

Migrating to quantum networks can often be difficult, resource-intensive, and time-consuming to implement – but there's a simpler, more efficient way to meet the challenges and leverage the benefits of quantum technology: AliroNet™.

AliroNet™

AliroNet™ is the world's first full-scale entanglement-based quantum network solution.
AliroNet™ is the most efficient and effective implementation – no matter where you are in your quantum networking journey. In Deployment Mode, AliroNet™ is your full-scale quantum network, simultaneously enabling both quantum-safe data security and the interconnecting of quantum technology for advanced computing and sensing performance.

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.



AliroNet™ is available in three modes: (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. 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. 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.

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. 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 acquire (or build) the hardware components, choose an operating system (i.e., the distributed on-device software that is run to generate 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 select an 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.

In addition to all the products and services included in AliroNet™ Emulation Mode, AliroNet™ Pilot Mode includes access to AlirOS™ (Aliro operating system software), Aliro Controller (Aliro controller software), and Aliro Orchestrator (Aliro 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 and the organization's requirements change, 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 network 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.

Getting Started

AliroNet™ mitigates technology lockout by allowing your organization to test, validate, and incorporate more powerful quantum hardware as it becomes available, ensuring you're ready for the tipping point of quantum technology deployment across the globe. 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@aliroquantum.com to get started.

About Aliro Quantum

Aliro Quantum, the first pure play quantum networking company, offers AliroNet™ to emulate, pilot, and deploy entanglement-based quantum networks that are capable of running a wide variety of applications from secure communications to clustered quantum computing and distributed quantum sensing. Aliro, spun out of NarangLab at Harvard University, includes world-class experts in quantum and classical networking and is leading the charge in quantum network development by offering the foundational technologies needed for organizations around the world to build scalable and powerful distributed quantum systems. 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 entanglement-based quantum networks. Aliro is working with industry and academic partners through the Quantum Economic Development Consortium (QED-C), the NSF Center for Quantum Networks (CQN), and the NSF Quantum Leap Challenge Institute Hybrid Quantum Architectures and Networks (HQAN). To learn more, visit www.aliroquantum.com.