The Quantum Network Deployment Guide

Aliro

www.alirotech.com

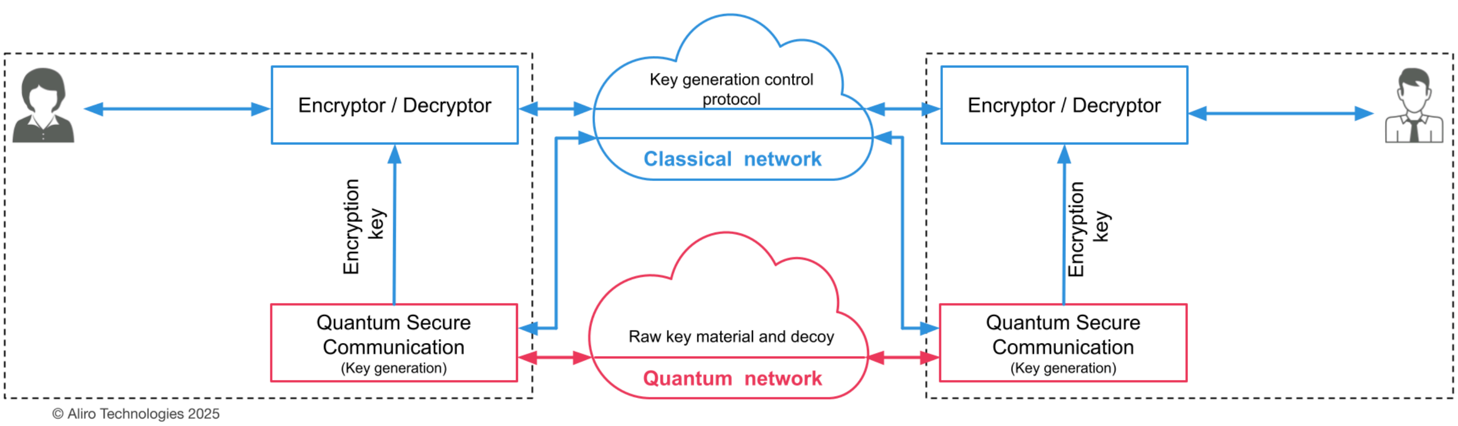
The Quantum Network Deployment Guide by Aliro

Summary

Quantum networking is often talked about in terms that are abstract or futuristic, even though quantum networks are being built today by governments, utilities companies, financial institutions, and other enterprises that need to protect highly sensitive data-in-transit. **This guide is for organizations exploring real-world quantum network implementation.** We explain the basics of what a quantum network is, how it works and why it matters. We unpack the practical advantages quantum networks offer and break down how quantum networks are deployed into three clear, actionable stages. We'll also share the common pitfalls to avoid along the way. This guide turns the seemingly complex vision of quantum communications at-scale into achievable short- and long-term milestones.

What are quantum networks?

A common misconception is that quantum networks can only be used to connect quantum computers, or that quantum computers are required for quantum networking. In fact, quantum networks can be used with a wide variety of devices, including classical computers and other classical devices. The quantum network itself is integrated with the classical network to enable many different applications that leverage quantum physics for a wide range of use cases, such as interconnecting quantum computers for higher compute power, networked quantum sensors for novel sensing applications, and linking quantum memories for Quantum Secure Communications.



A quantum network runs on the same fiber as a classical network. Quantum communications can even be running at the same time on the same line as classical communications. A quantum network uses photons encoded with information, called qubits, across fiber or free space. Quantum network nodes include quantum devices: hardware components that can be used to create, measure, store, transform and/or process quantum information. Qubits are the quantum equivalent of a classical bit, but rather than being a zero or a one, a qubit can also be in a superposition of those states: 1, 0 or anything in between. A qubit value can be anywhere on the surface of a Bloch sphere, as shown below, where the poles are equal to the one state and the zero state.

The Bloch sphere is one way to represent a qubit.

The top of the z-axis represents the |0> quantum state.

The bottom of the z-axis represents the |1> quantum state.

The x-axis and y-axis represent different superposition states with different phase.

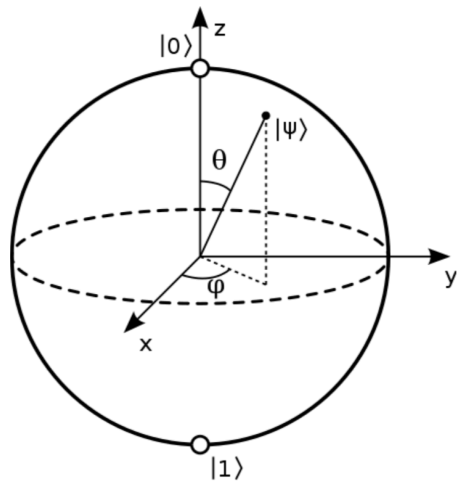


Image from:
https://en.wikipedia.org/wiki/Bloch_sphere

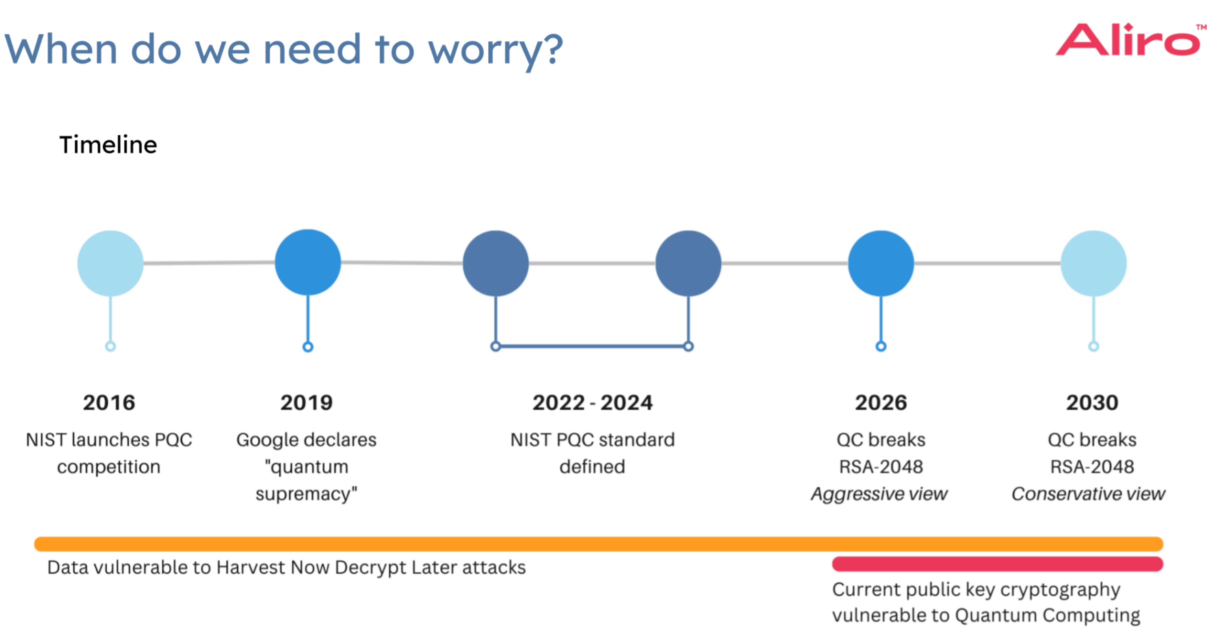
At the core of modern quantum networks is entanglement. Quantum entanglement is a phenomenon where two or more particles become correlated so that the state of one instantly determines the state of the other, no matter what distance separates them. When distributed across a network, entanglement enables a variety of applications, including ultra-secure communications. Entanglement ensures that any attempt to intercept or tamper with the communication is immediately detected.

Introduction to the Quantum Networking Landscape

The quantum revolution is not a distant dream, it's already here. Yet, with transformative potential comes a wave of new technological and security challenges. The best way to rise and meet these challenges is to use quantum technologies. **Entanglement-based quantum networks have emerged as a solution that could have a domino effect on other technologies, unlocking and speeding up progress across other quantum technologies.**

Quantum Secure Communications

Today, our digital lives are secured with encryption algorithms that have changed little over the past 30 years. These algorithms are fundamentally vulnerable to quantum computing. Shor's algorithm is a quantum algorithm capable of efficiently factoring large integers, a direct threat to the security of widely used cryptographic systems, including RSA and Diffie-Hellman encryption. Cryptographic systems that rely on the difficulty of factoring large numbers have been a cornerstone of secure internet communications for decades, but quantum computers will completely break these cryptographic systems and expose vast amounts of sensitive data. The threat is especially serious due to Harvest Now Decrypt Later attacks (HNDL), where adversaries collect encrypted data today and decrypt it once quantum computers become powerful enough. While estimates of when a quantum computer will be capable of running Shor's algorithm vary, the timeline is continually shrinking due to giant leaps in qubit scaling, quantum error correction, algorithmic advancements and hardware advancements. In 2022 the common estimate for the arrival of a cryptographically relevant quantum computer was up to 20 years. Today's estimates are hovering at just 3 to 5 years.



Information Source: https://www.idquantique.com/quantum-ready-set-go/

This looming threat has accelerated efforts to find more robust, future-forward alternatives. Entanglement-based quantum networks provide a fundamentally different kind of security: quantum-powered security. By leveraging quantum entanglement and teleportation, these networks enable encryption schemes that can't be hacked, even by quantum computers. Man-in-the-middle attacks become physically impossible because data is transferred from point A to point B without ever being exposed to the network.

Quantum Computing Scalability

There is a lot of excitement for quantum computing's potential to transform industries, from pharmaceuticals to logistics. However, quantum computers today do not yet have the ability to realize these truly groundbreaking applications. Even with ambitious roadmaps from hardware vendors, the path to fault-tolerant, large-scale quantum computing is bottlenecked by challenges.

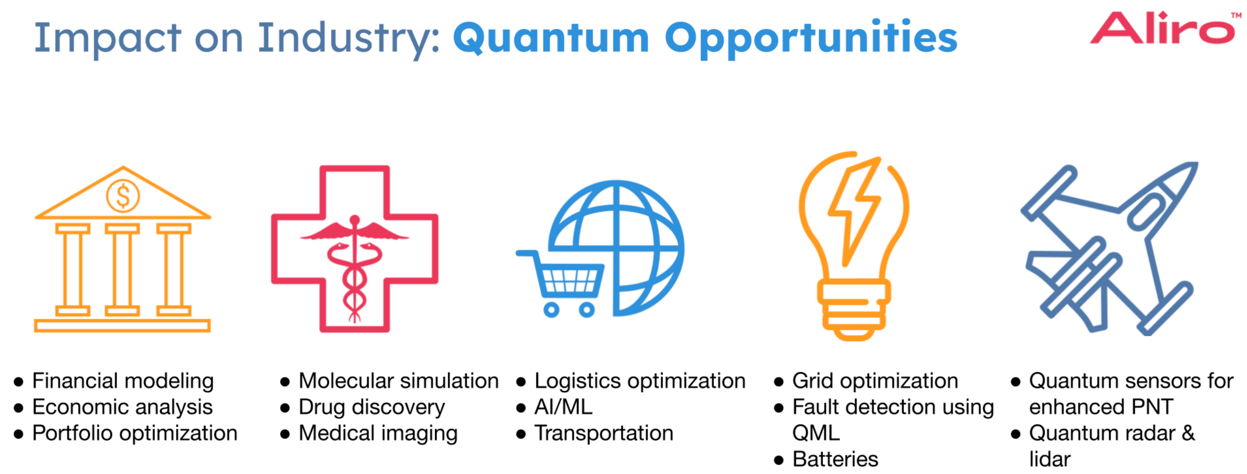
Interestingly, when it comes to quantum computing, bigger truly does mean better. A critical component of scaling a quantum computer's power is scaling its qubit counts. Reaching the scale required for quantum computers to achieve their potential is a significant engineering and physics challenge, one that entanglement-based quantum networks can help to address by connecting smaller processors into distributed quantum systems. Entanglement-based quantum networks can be used to interconnect quantum processing units (QPUs), whether they use optical qubits, superconducting qubits, or other modalities. By networking QPUs together computational power can be scaled beyond the limits of a single machine and represents a viable path to realizing the high-impact use cases quantum computing promises.

Quantum Technology Interoperability

Today's quantum ecosystem can appear fragmented. A variety of architectures and qubit modalities exist, from trapped ions to superconducting circuits, each with strengths and challenges. There is little standardization across devices, making it difficult to integrate and optimize their capabilities. This lack of interoperability not only limits collaboration but also restricts innovation. **Entanglement-based quantum networks can be used to create a shared operating environment where different quantum devices and architectures can interoperate seamlessly.** This enables optimized performance across use cases, supports collaborative development across platforms, and lays the foundation for a robust, diverse quantum ecosystem.

Multi-purpose, Multi-vendor Possibilities

Acting as a common backbone, entanglement-based quantum networks can support multi-vendor environments and enable co-development across hardware types. This is the foundation for building a quantum network stack that is modular, scalable, and ready to seamlessly support a variety of quantum applications.



Quantum computing, sensing, and communications will revolutionize industries.

Distributed Quantum Sensing

Quantum sensors already outperform their classical counterparts by exploiting the fragile yet powerful properties of quantum systems to detect phenomena. Interconnecting multiple quantum sensors via entanglement could further boost quantum sensing capabilities. A network of small quantum sensors may effectively functions as one extremely large sensor, achieving measurements that were previously unobtainable. This capability will be transformational for fields like astronomy, where entangled sensor arrays could function as enormous virtual telescopes, letting us see deeper into the cosmos with greater detail. Distributed sensors offer enormous promise for Earth-bound applications, too: from industrial automation and logistics to defense and geospatial intelligence.

Enabling Blind Quantum Computing

A powerful future use case is blind quantum computing. Today, quantum computing platforms are mostly accessed via cloud platforms, but when these quantum computers in the cloud are being used to process sensitive data or proprietary algorithms, there is a risk that the data could be visible to the cloud provider or even exposed in a data breach. This is a risk many industries can't afford to take due to regulatory, privacy, or intellectual property concerns.

Entanglement-based quantum networks could eliminate this vulnerability by enabling blind quantum computing: cloud providers and hardware vendors can execute quantum computations without ever exposing the data or algorithms involved. This unlocks secure quantum computing for industries such as finance, healthcare, and national security, where confidentiality is non-negotiable.

The Quantum Internet

Entanglement-based quantum networks are not a solution to the challenges we've articulated here, and they're a gateway to future possibilities. They can enable secure communication, distributed sensing, scalable quantum computing, and, ultimately, the Quantum Internet. Much like the classical Internet, which began as a simple way to share data but evolved into a platform for social media, video conferencing, and global commerce, the Quantum Internet will inspire applications we can't yet imagine.

Your timeline for implementing quantum networking

The transformative potential of entanglement-based quantum networks is undeniable. From fundamentally secure communication to scaling quantum computing, these networks are reshaping how organizations, governments, and industries are approaching secure networks. At Aliro, we believe the case for early adoption is urgent. Starting today offers huge advantages, especially to early movers.

1. **Global competitiveness.**
   Quantum networking is a strategic endeavor. Much like the space race of the 20th century, the quantum race will define technological leadership and national security. The organizations and nations that build and deploy first will enjoy significant strategic advantages. Waiting means falling behind, and catching up may not be an option.

2. **Time to identify and optimize your use cases.**
   It takes time to move from a proof-of-concept use case to a production-ready deployment of technology. Large organizations in particular require spacious lead times to pilot, evaluate, and integrate new technologies into their workflows. Starting now allows you to align quantum capabilities with your operational needs and identify the strongest approach for adoption.

3. **Ease of evaluation.**
   Quantum devices and prototypes are entering the market at a rapid pace. Now is the time to test and compare them. Getting started early with evaluating hardware and software gives you the luxury to assess performance, interoperability, and security without the pressure of immediate deployment deadlines.

4. **Build internal familiarity and practical experience.**
   By beginning your quantum networking journey now, you enable your internal teams to grow with the technology. Training today's technicians, engineers, and operators means they'll be ready to lead your organization's quantum network roll-out. This practical experience is where real value is created, building institutional knowledge in quantum technologies.

At Aliro, we work with a diverse set of customers across industries, and we've seen firsthand the breadth and depth of interest in quantum networks. What's driving this demand? At the heart of it is a universal need to secure sensitive data in transit. As new categories of threats arise, classical security tools won't be able to maintain the level of security required. Nearly every industry sends information that must be protected: customer records, operational data, intellectual property, and more.

Quantum threats are not a hypothetical risk. Government agencies and national infrastructure companies are among the earliest adopters of quantum networks. The public sector is responsible for safeguarding national secrets, citizen data, and critical infrastructure from power grids and water systems to transportation networks and emergency services. The stakes are very high: through Harvest Now Decrypt Later attacks, adversaries seeking to compromise national infrastructure and undermining public key cryptography.

Public key infrastructure is specifically used for:

- documents, messages, certificates, code, and transactions can be forged
- identity over the internet is not guaranteed
- software authenticity is not guaranteed
- secret keys can be exposed
- internet traffic no longer secure
    - secure online banking
    - transaction verification on blockchain
    - communicate sensitive data like patient records, pharmaceutical intellectual property, and medical research data
    - making online purchases
- energy distribution in our power plants and control centers
- protecting sensitive data being shared from business to business and intellectual property for private defense

A majority of digital systems that demand trust, privacy, and safety rely on public key infrastructure and these exact systems are the most vulnerable to Q-Day impacts. RSA, ECDSA, ECDH, and DSA are all vulnerable to HNDL and quantum attacks.

Asymmetric Protocol	Key Size	Security Level (now)	Post-Q-Day Level
RSA-1024	1024	80	0
RSA-2048	2048	112	0
ECC-256	256	128	0
ECC-384	384	256	0

Impact on Industry: **Quantum Threats**

- Online banking
- Cryptocurrency transaction verification

- Patient records
- Pharmaceutical IP
- Medical research

- E-commerce
- SSL/TLS or Wi-Fi encryption
- Email encryption
- Logistics/transport

- Energy distribution
- Power plants
- Control centers

- Intellectual property
- Sensitive B2B data

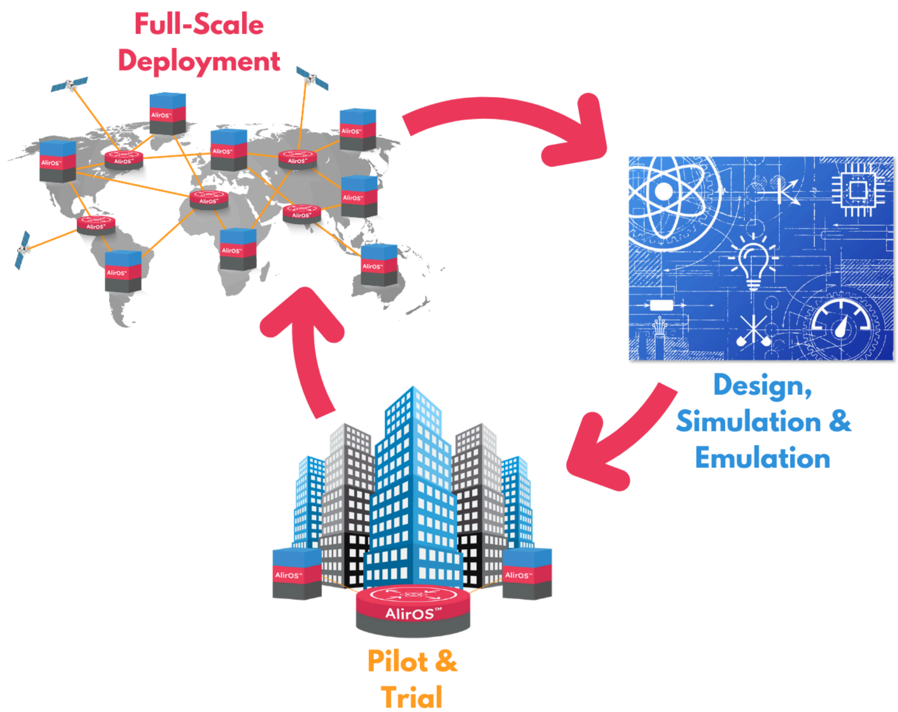
The majority of digital systems that demand trust, privacy, and safety will be impacted.

Governments, defense contractors, utility companies, financial institutions, pharmaceutical companies, and telecommunications providers are already working to deploy quantum networks to counter these threats. These organizations recognize that quantum networking provides not just stronger encryption, but fundamentally different security that can be relied upon to protect critical data transmissions.

The 3-Phase Framework for Deploying Your Quantum Network

As with any cutting edge technology, success depends on strategic, well-paced implementation. To guide organizations through the process of implementing quantum networks, Aliro has created a three-phase framework for building entanglement-based quantum networks:

- Phase 1: Design and Emulation
- Phase 2: Pilot and Trial
- Phase 3: Full-Scale Deployment



This methodology is designed to be adaptable across industries and sectors, to help you and your organization make informed, data-driven decisions about your quantum network.

Building quantum networks with Aliro's framework reduces risk, fosters interoperability, and cultivates hands-on expertise with quantum communications. In the pages that follow, we explore each phase in detail. We begin with the Design and Emulation phase, where virtual modeling, simulation, and protocol testing enable organizations to plan quantum networks intelligently before committing to physical buildouts. Next, we discuss the Pilot and Trial phase, where small-scale, functional networks provide validation and real-world troubleshooting. Finally, we address Full-Scale Deployment, the moment where a well-prepared organization can scale confidently and build to the full potential of their quantum network.

The countdown to advanced quantum computation has already begun, and attackers are harvesting encrypted traffic today in hopes of decrypting it tomorrow. Fortunately, you don't have to wait for new standards or hardware to start hardening your organization's security posture. Proactively addressing your organization's threat readiness now can help you on the path to quantum resilience:

- Identify where cryptography is being used in your systems
- Identify vulnerabilities
- Inventory long-term sensitive data

- Identify high-risk “HNDL” vectors
- Assess telecom vendor quantum-readiness
- Design, validate, and build quantum secure networking pilots
- Engage with standards bodies (e.g., ETSI, ITU-T, NIST)

Phase 1: Design and Emulation

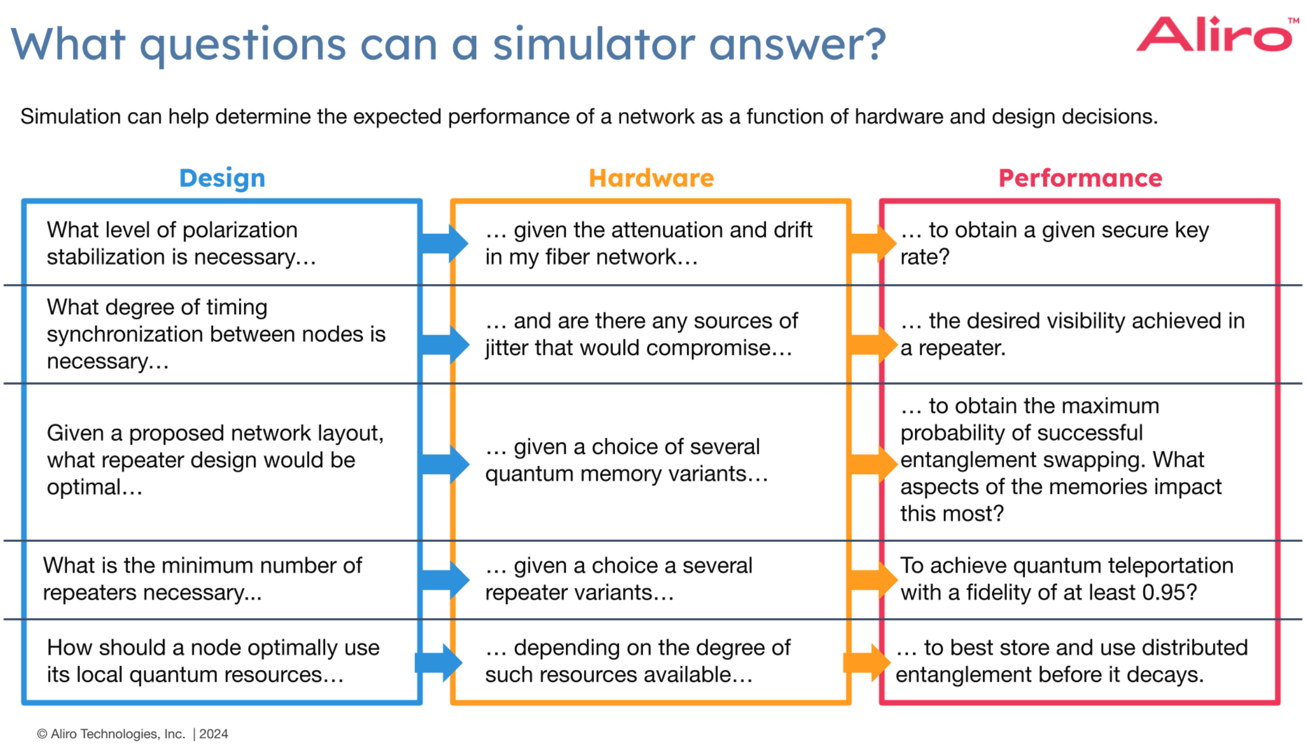
The first stage of building a quantum network is the Design and Emulation phase. In this phase, organizations evaluate architectural options, simulate quantum network behavior, and prepare protocols and personnel for practical deployment. The Design and Emulation process enables faster development, cost savings, and a reduced risk in implementation by replacing guesswork with data-driven planning.

The Design and Emulation phase has two critical functions:

1. Defining a network architecture tailored to specific organizational needs such as network communications security, interconnecting quantum processor units (QPUs) / quantum computers, or quantum cloud infrastructure.
2. Simulating and emulating network behavior to test protocols, hardware configurations, and performance under realistic conditions.

This phase ensures that before investing in expensive quantum hardware, an organization is able to:

- Evaluate use-case feasibility.
- Identify optimal node placement.
- Assess performance trade-offs (for example, fidelity vs. throughput).
- Test interoperability between quantum devices.
- Design and validate a complete protocol stack.



Some other critical questions that simulation can answer include:

1. **What is the optimal network topology for my use case?**
   Simulation helps determine how to position nodes, repeaters, and links to maximize performance metrics like entanglement rate, fidelity, or reach given certain design constraints (such as geography) and selected hardware.

2. **How will performance change with different hardware configurations?**
   By modeling different quantum components such as quantum memories, entangled photon sources, detectors, and interfaces, simulation can reveal how hardware choices impact a network's behavior.

3. **What are the expected entanglement rates and fidelities across the network?**
   These performance metrics can be forecast under different loss and noise conditions. Understanding how the conditions your network will operate under impacts performance can help you make informed decisions about purification and error correction strategies.

4. **Where are the bottlenecks in my network design?**
   Simulation helps identify which links, components, or protocols are limiting

performance due to loss, latency, decoherence, or clock mismatches.

5. **How sensitive is the network to loss, noise, or timing errors?**
   You can test how the design will perform under real-world variabilities such as photon loss in fiber, decoherence in memory, or clock jitter between nodes.

6. **What level of synchronization is required for successful operation?**
   Quantum protocols often require sub-nanosecond timing precision. Simulation helps assess how much synchronization error your system can tolerate.

7. **How many entangled pairs are needed to meet the desired application requirements?**
   Applications like quantum key distribution or teleportation need a certain rate and fidelity of entangled photon pairs. Simulation helps quantify this and determine if the design meets those thresholds.

8. **What protocol stack and control logic are necessary?**
   Simulation enables you to test protocol implementations for entanglement generation, swapping, purification, and teleportation before committing to firmware or control software.

9. **How will different applications compete for shared quantum resources?**
   In multi-user networks, simulation can model traffic patterns and resource use, which is helpful for understanding the orchestration layer design and the scheduling policies required for a successful network.

10. **What trade-offs exist between cost, fidelity, and scale?**
    Simulation lets you explore multiple configurations and plot out trade-offs, supporting decision-makers in balancing performance with budget and deployment constraints. Simulation will also help you account for timing constraints. Because quantum information cannot be copied (as per the no-cloning theorem), and because it also decoheres rapidly, the design of quantum networks must address timing, synchronization, and loss from the outset.

Preparing for Design and Emulation

Before sitting down to design and simulate your quantum network, it's helpful to begin with answering a set of questions to frame the purpose and constraints of your implementation.

These questions help define what you're building, who it's for and how it will evolve, ensuring that your network design is aligned with your specific objectives.

1. Who will use the network and for what purpose?
    - Will the network be used internally, or are you building infrastructure for others?
    - Do your users intend to use the network for secure communications, quantum computing, distributed quantum sensing, or quantum device testing? A mix of these?
    - Clarifying the core applications your network will enable helps to define the architecture, protocol design, and more.
2. What is the scope of your network deployment?
    - How many locations / nodes will the network serve?
3. What are your budget and time constraints?
4. How should the network evolve over time?
    - What will the next stage of your network enable your organization and users to do?
    - What functionality do you expect to add in later phases?
    - How will your architecture accommodate upgrades?
    - How flexible do you need your network to be, and in what ways?
5. What performance targets does your network need to meet?
    - What fidelity and entanglement rate does your use case require?
    - What are acceptable levels of latency, loss, and error?
    - Later sections of this guide will explore the key metrics available for characterizing quantum network performance.

Understanding the Design of Quantum Networks

Entanglement-based quantum networks distribute entanglement between nodes. In this way, entanglement is akin to a resource that makes a variety of applications possible simultaneously, such as Quantum Secure Communication and distributed quantum computing on the same network. To extend entanglement across distances, a quantum network typically executes three main steps:

1. Elementary Entanglement Generation between adjacent nodes via fiber or other channels.
2. Purification (or Distillation) to enhance the fidelity of weakly entangled pairs by combining multiple low-quality pairs into a single high-quality one.
3. Entanglement Swapping, performed by quantum repeaters, to stitch intermediate nodes together into long-distance entanglement links.

Once established, this entanglement can be used, or consumed, for tasks like teleporting quantum states, effectively enabling transmission of qubits without sending them directly across the network. Qubits are the basic unit of information in a quantum network, analogous to classical bits we are accustomed to using every day. Qubits are typically transmitted using single photons, but how the quantum state is encoded in those photons impacts their reliability and compatibility. Common encoding methods include:

- Single-Rail (Presence/Absence) Qubits. Simple to implement but fragile; loss is indistinguishable from a zero bit.
- Dual-Rail Qubits. More robust and includes formats like:
  - Polarization (horizontal = 0, vertical = 1)
  - Time-bin (early vs. late arrival)
  - Frequency-bin
- Combinations of these types of qubits.

Each encoding type has specific hardware and synchronization requirements, and the choice of how a qubit is encoded can affect system performance and interoperability.

Quantum systems operate at highly precise time scales. Successful entanglement swapping, memory interfacing, and qubit detection all require synchronization. For example, a quantum memory must know exactly when to expect an incoming photon in order to capture its quantum state correctly. Poor timing destroys the entanglement or may cause the qubit to be missed entirely.

Quantum memories are used to store and process qubits. Different quantum memory technologies offer different trade-offs. Quantum memories can be classified based on the type of of qubit architecture they use:

- Superconducting. Fast but short coherence times.
- Trapped Ions. Long coherence and gate operations but slower speeds.
- Photonic. Natively integrated with optical systems but still maturing.

Each memory type differs in time scale, noise characteristics, gate operation capabilities, and interfacing requirements, all of which must be factored into your quantum network design.

In addition to these factors, there are two fundamental metrics that determine whether a quantum network can meet a user's needs:

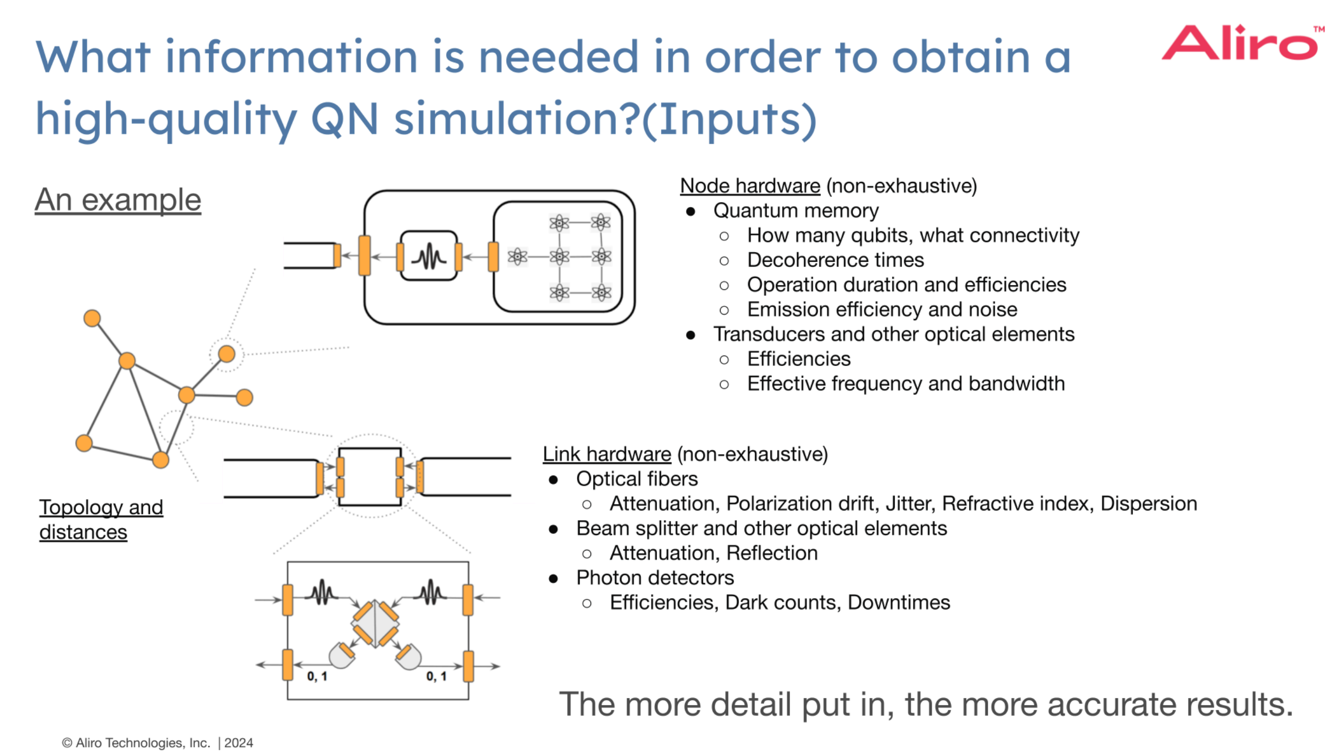
- Fidelity. The accuracy, or quality, of the entangled states.
- Entanglement Rate. The number of usable entangled pairs distributed per second.

These two metrics are often in tension, where optimizing one reduces the other. For example, higher fidelity means fewer errors, but also typically means the entanglement rate decreases, especially if entangled pairs are being used for purification, a process for increasing the fidelity. Network designers must balance fidelity and entanglement rate depending on the application: high-fidelity for precision or security, high entanglement rate for throughput-focused use cases.

Entanglement-based quantum networks contain several core hardware components:

- Entangled Photon Sources. Devices that produce entangled photon pairs (also known as qubits) for distribution between nodes.
- Quantum Memories. Devices that store qubits, enabling entanglement purification and swapping.
- Photon Detectors. Required to verify entanglement and perform Bell-state measurements.
- Transducers. Devices that translate quantum signals between different physical forms. For example, a transducer would essentially convert a photonic qubit traveling through optical fiber into a superconducting qubit that can be stored in a specific quantum memory.
- Quantum Repeaters. Nodes that extend the range of entanglement by performing entanglement swapping and error correction.

Each quantum device in the network will have particular timing and synchronization requirements. They may use different qubit modalities. Using a quantum network simulator can help an organization balance all of these technical requirements and performance needs, and experiment rapidly with the options available to them.



Trade-Offs in Quantum Network architecture

Designing a quantum network requires balancing interdependent variables such as performance, cost, interoperability, and complexity. Each architectural decision has implications for what the network can do and how reliably it can perform.

Encoding methods. Time-bin encoding is robust over optical fiber making it ideal for long-haul links. Polarization encoding, while easier to implement, is more sensitive to environmental factors. Other options like frequency-bin or hybrid encodings offer flexibility but usually at the cost of more complex hardware requirements.

Fidelity vs. Rate. Higher fidelity is achieved through purification techniques that consume multiple low-fidelity entangled pairs, thereby reducing the overall entanglement rate. Applications demanding high precision, such as secure communications or quantum metrology, prioritize fidelity. Other use cases may favor higher throughput at lower fidelity.

Node placement. Physical distance between nodes directly impacts photon loss. As photons are the primary carriers of quantum information, longer distances increase the likelihood of qubit loss or decoherence, necessitating additional infrastructure such as quantum repeaters for long distance links.

Hardware coherence time. The time a quantum memory can hold a qubit without degradation is its coherence time. In multi-node protocols like entanglement swapping, if one qubit arrives before the other, the memory must preserve its state until both qubits are ready. Coherence times are another factor to balance in your network design.

Synchronization requirements. Many quantum protocols demand ultra-precise timing. Devices have to be clock-aligned so that photons arrive simultaneously at measurement points. Misalignment could prevent entanglement from forming or introduce noise, requiring careful calibration and often specialized synchronization infrastructure.

Device interoperability and frequency matching. Quantum nodes may operate at different optical frequencies or use distinct timing and control protocols. Interconnecting diverse hardware could require quantum transduction.

Quantum memory selection. The choice of quantum memory platform affects time scales, noise resilience, and how well components integrate with optical systems. Designing for compatibility across different memory types, especially in heterogeneous networks, is nontrivial!

The Design and Emulation phase allows organizations to test these variables before committing to a specific architecture.

Simulation and Emulation Tools

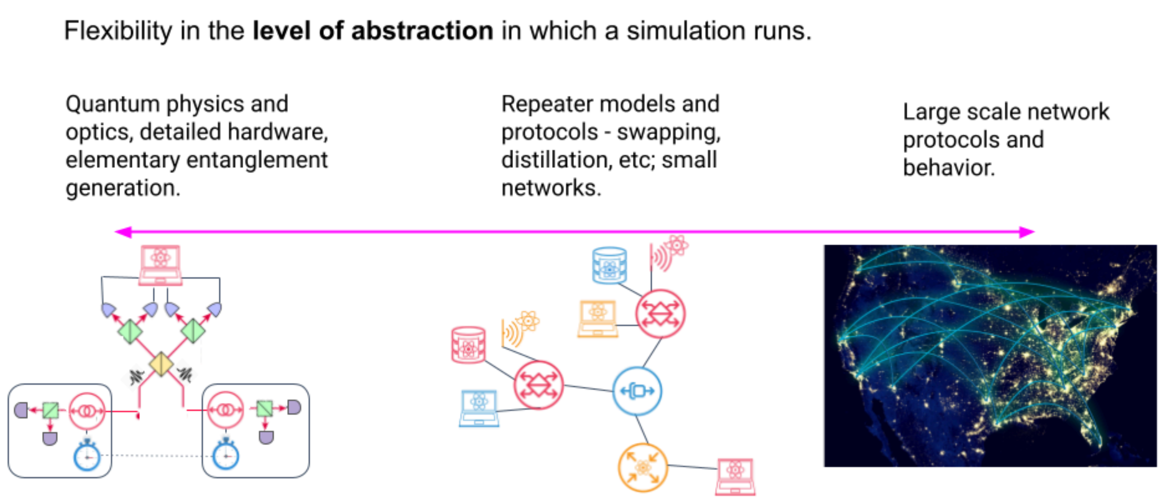
The complexity of quantum networking demands a radically different approach to system design than what is used in classical networking. Unlike conventional networks, where protocols and performance can be prototyped on off-the-shelf hardware, quantum networks operate under a completely new set of physical principles and constraints. Photon loss, entanglement fidelity, memory decoherence, and clock synchronization down to the nanosecond must all align in order to successfully fulfil the network's purpose.

For this reason, simulation and emulation tools are not optional: they are foundational. These tools enable organizations to explore network architectures, validate performance assumptions, and develop protocol logic in a cost-effective, low-risk digital environment. They provide the sandbox in which quantum networks can be envisioned, iterated, and prepared for real-world deployment.

What to look for in a quantum network simulator

The simulator you choose should be purpose-built for designing, testing, and optimizing quantum networks. Ideally, the simulator you choose should provide a modular, realistic toolset for understanding the behavior of the quantum network.

Layered abstraction, from low-level photon interactions to high-level entanglement protocols. The ideal quantum network simulator should be capable of modeling the entire quantum network stack, from physical layer optics (sources, detectors, fiber loss) to high-level protocols (entanglement generation, purification, and swapping). This holistic approach allows users to test complete workflows in addition to isolated components.



Flexible hardware models to simulate different types of sources, detectors, and memories. The quantum network simulator should enable users to swap components to try out different quantum memory platforms or entangled photon sources from various vendors, change network topologies, and iterate rapidly. This supports agile prototyping and accelerates the design process.

Noise and decoherence modeling for accurate performance prediction. The quantum network simulator should incorporate realistic quantum effects, including decoherence, photon loss, and quantum noise. This ensures that simulated outcomes closely mirror physical reality and eliminates the risk of purchasing components that aren't compatible. This modeling should also include the timing and synchronization resolution. Quantum protocols often require synchronization at the nanosecond level. Accounting for precise timing alignment between nodes helps in evaluating timing-sensitive applications like entanglement swapping and memory interfacing.

Integration with control software scales with expanded deployment. Users can test the physical performance as well as protocol logic and orchestration software. Ideally, your quantum network simulator will be able to help you grow and change the quantum network over time as the network becomes more sophisticated. This enables realistic planning for the future capabilities and reach of the network.

Emulation capabilities with real hardware that allows quantum hardware to be integrated into a simulated environment. Beyond pure simulation, emulation allows users to test real quantum devices such as entangled photon sources, detectors, or memory modules within a virtual network stack, making it possible to assess real-world performance within a broader network context.

Performance metrics for evaluating a quantum network design

Performance metrics help you evaluate design trade-offs, optimize your network for efficiency and effectiveness, and determine if your design is ready to move on to the next phase of quantum network implementation. There are four critical performance metrics that guide both design and decision-making. While there are many other metrics that a quantum network simulator can provide, these metrics are central to evaluating whether a quantum network is ready for real-world use: fidelity, entanglement rate, latency, and robustness.

Metric	What It Measures	Why It Matters	What It Affects
Fidelity	Quality of entanglement; how close the quantum state is to the ideal on a 0 to 1 scale.	Ensures secure, reliable operations. Low fidelity introduces error or insecurity.	Communications security, computational precision, need for purification
Entanglement Rate	Number of usable entangled pairs per second	Determines how many quantum operations can be executed per unit time.	Network throughput, user concurrency, responsiveness
Latency	Time needed to generate & verify entanglement	Quantum protocols often fail if not executed within tight timing windows.	Synchronization-dependent tasks, user experience, real-time operations
Robustness	Tolerance to noise, drift, and hardware variability	Ensures performance under real-world (non-ideal) conditions.	Reliability, environmental sensitivity, deployment feasibility

***For more on this topic, see our on-demand webinar, Performance Metrics for Quantum Networks. ***

Using performance metrics in a simulation environment allows organizations to optimize architectures, quantify readiness, and make informed investments. By leveraging simulation, teams can move forward confidently with building scalable, secure, and future-ready quantum infrastructure.

Transitioning to the next phase in Quantum Network implementation

The Design and Emulation phase is the most cost-effective and strategic entry point into quantum networking. It helps organizations reduce R&D risk, accelerate innovation, and ensure that future hardware deployments are successful. After a rigorous Design and Emulation phase, the next step in quantum network implementation is Phase 2: Pilot and Trial.

In this phase, organizations typically build out a small, controlled quantum network deployment consisting of 2 - 5 nodes with all the required hardware.

Are you looking for a Quantum Network simulator that reduces risk, accelerates timelines, and ensures your design decisions are grounded in physics and aligned with your goals? Aliro Simulator is not a general-purpose quantum tool; it's tailored for designing, optimizing, and scaling quantum networks. This means it directly supports the architectures and protocols that underpin next-generation Quantum Secure Communication, distributed quantum sensing, and scaling up of quantum computing. Aliro is one of the only companies focused exclusively on entanglement-based quantum networking. Aliro Simulator reflects best practices, insights from real deployments, and deep experience across telecom, defense, and research sectors.

Phase 2: Pilot and Trial

The Pilot and Trial phase focuses on implementing a small-scale quantum network. As the bridge between your quantum networking blueprint and your full-scale quantum network, your pilot quantum network serves to validate the design in real-world conditions.

The Pilot and Trial phase has two primary objectives:

1. Construct an operational pilot network based on the architecture, protocols, and hardware configurations identified during the design phase.
2. Testing and benchmarking this quantum network to gather data, tune protocols, and refine deployment strategies.

This phase offers several important benefits. Jumping directly from the Design and Emulation phase to Phase 3, Full-Scale Deployment, increases the chance of costly surprises. The Pilot and Trial phase offers both technological and strategic benefits:

1. A smaller network will require less lead time and makes it possible to build out a sample portion of your quantum network as hardware orders for expanding the deployment are being fulfilled. This means fewer delays throughout the full-scale deployment.
2. Identify and resolve interoperability issues early, validate simulation assumptions, and prevent large-scale investment in technologies that are incompatible or underperform in real-world scenarios.
3. Unnecessary spending can be avoided by starting small and then scaling. Many insights can be uncovered by building at a small scale before committing to a large scale deployment.
4. Evaluate which hardware components meet performance, reliability, and integration needs and identify the vendors and suppliers who are best suited for long-term partnerships.
5. Even if simulations were thorough, physical networks introduce variables like noise, jitter, or environmental disruption. This phase presents valuable opportunities for tuning of entanglement generation, purification, and teleportation protocols to the specific operating environment of your network. Timing, synchronization, and classical control systems can be validated. Topology, link distances, repeater placement, and other architecture can be further optimized for full-scale deployment.
6. Quantum networking requires new operational skills. The Pilot and Trial phase helps organizations build internal familiarity with quantum networking, and presents an opportunity to establish the necessary processes and best practices within your organization prior to scaling.

7. Early success stories from a pilot network helps your organization gain buy-in from stakeholders: executive leadership, board members, public sector sponsors, etc. This can also lead to additional investment or funding for the full-scale deployment.
8. Pilot quantum networks inform future design iterations. What unexpected constraints emerged that were not previously predicted? What changes need to be made before full-scale deployment?

The Pilot and Trial phase helps your organization make smarter, more confident decisions in the implementation of the full-scale quantum network. Here's a high-level look at the process leading up to building the pilot network:

- Before building the pilot network, your organization will identify the hardware, protocols, and use cases for the network, and then define the pilot network architecture: deciding where components will be deployed, how they'll be interconnected, and where nodes will be located (within a single room vs. across campus locations). As previously discussed, this is best accomplished by using a quantum network simulator in the Design and Emulation phase.
- Once a workable design has been identified, the next step is creating detailed testing and benchmarking plans that will verify the real-world performance of both hardware and software, starting with isolated components to ensure that the behavior of each component matches the simulation.
- The last step before actually building your pilot quantum network is to acquire the necessary hardware, software, and operational expertise to test, benchmark, build, and run the pilot network successfully.

Let's take a closer look at selecting hardware and software, and gathering the right expertise to build the pilot quantum network.

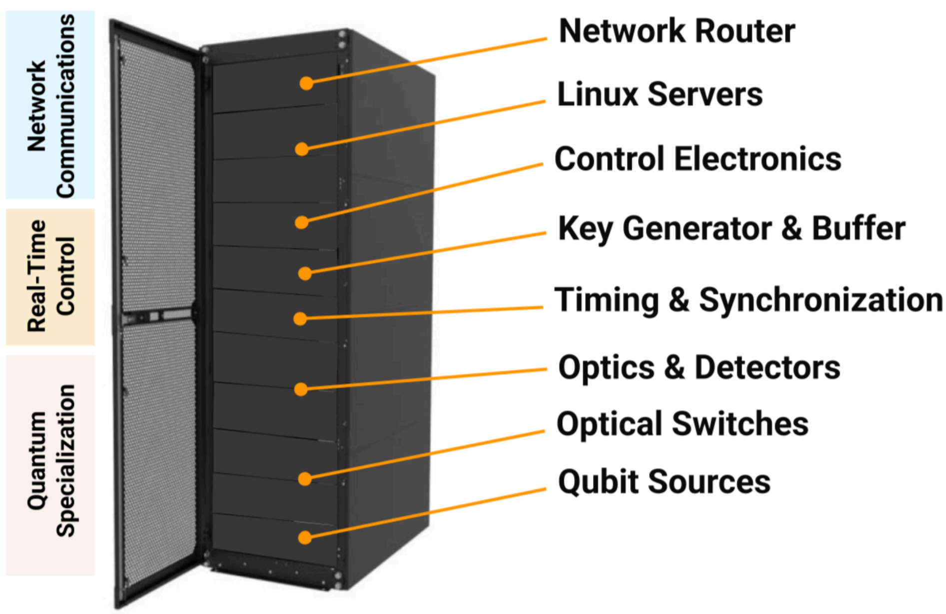
Hardware considerations for your Quantum Network

Transitioning from simulation to an operational pilot quantum network requires close attention to the physical and operational realities of quantum hardware and the expertise required to deploy it effectively.

At the highest level, quantum network hardware must be able to produce, transmit, manipulate, store, and measure quantum data in the form of qubits. For many networks, these qubits will be in the form of photons, which are highly sensitive to environmental noise and degradation. To be effective, this hardware must do more than function, it must perform to a degree that preserves fidelity of quantum data. Poor fidelity undermines the usability of the network and can render even well-designed protocols ineffective.

During the design and emulation phase, several requirements should already have been evaluated:

- The hardware must produce known quantum states, which is particularly critical if using entangled photon pairs.
- It must support all necessary quantum operations and measurements relevant to the network's protocols and applications.
- It must meet quantum memory requirements, storing quantum states reliably until they are needed.



Beyond the core quantum components, several supporting systems are essential:

Classical networking infrastructure. Quantum networks depend on classical communication for control and coordination. Low-latency classical links are needed to exchange synchronization signals, protocol messages, and error correction data between nodes.

Auxiliary hardware components. Auxiliary hardware includes things like mounts and housings as well as thermal and optical stabilization hardware. These may not be fully captured in simulation but are often necessary for real-world deployments. Hardware vendors are key partners in identifying and sourcing these components.

Software compatibility. Hardware must interface cleanly with orchestration and control software. This includes being able to configure devices, issue quantum operations, and respond to network protocols. Oftentimes, quantum hardware components will be packaged with some software, like graphical user interfaces, which are helpful for running experiments in a lab with a minimal number of nodes. However, this software isn't sufficient for the kind of control needed in a more sizable network.

Even the best hardware is ineffective without the right experience to deploy, operate, and maintain it. Quantum network deployments have particular needs when it comes to:

Safe handling and transportation. Quantum hardware, especially optical components, is sensitive to environmental conditions such as bright light or vibration. Mishandling can damage or degrade performance.

Installation and troubleshooting. Teams need to connect systems correctly, detect misconfigurations, and address issues as they arise. This is especially important when integrating components from multiple vendors.

Awareness of environmental factors. Real-world deployments must account for noise sources like mechanical vibrations, stray electromagnetic fields, or temperature fluctuations. Unaddressed, these factors can significantly reduce performance. Solutions may include EM shielding, vibration damping, or site-specific optimizations.

Cultivating relationships with quantum technology vendors can be helpful in building a successful pilot. Vendors bring a deep knowledge of their products, including best practices for handling components and their unique environmental tolerances. Vendors often offer training and documentation to accelerate internal skill-building within your organization. Engaging vendors early and often ensures that pilot networks are installed correctly, maintained effectively, and prepared to scale into full deployments.

Software Considerations

Deploying a pilot quantum network requires a sophisticated and well-integrated software stack for controlling devices, running protocols, orchestrating operations, and supporting applications. As organizations move from the Design and Emulation Phase into the Pilot and Trial Phase, software often becomes an overlooked part of the quantum network infrastructure. Some essential software components are needed:

1. Device control and protocol execution software. Software that controls the hardware on the network and software that enables your desired protocols are frequently packaged together, forming the network operating system. This low-level software runs close to the hardware and interfaces with it directly. Components such as photon sources, quantum memories, and detectors are used to execute essential tasks like state

preparation, entanglement distribution, and qubit measurement. This is the software that coordinates these components, ensuring devices are synchronized and can interact according to the rules defined by quantum communication algorithms.

2. Orchestration software. While not strictly required during the Pilot and Trial stage (especially for small testbeds), orchestration software becomes increasingly important as a network expands. This layer simplifies management by providing centralized tools for configuring devices and monitoring node status. Without orchestration, operators would have to manually manage each network node, which becomes impractical once a network scales beyond a handful of devices. While early pilots might survive without this complexity, planning for an operational network at a useful scale means selecting tools that can grow with the network.
3. Application software. This software sits at the top of the stack. It uses the services, such as entanglement generation and qubit transmission that are provided by the lower layers of the stack in order to execute real-world use cases such as Quantum Key Distribution (QKD), Quantum Secure Communications (QSC), and distributed quantum computing. Control and orchestration software enables the infrastructure. Application software transforms that infrastructure into business value.

Other software considerations include timing and performance requirements. Quantum networks are fundamentally time-sensitive. Many processes must occur within microseconds, milliseconds, or even nanoseconds in order to avoid decoherence or data loss. Any delay caused by the network's software can render stored quantum data unusable.

As such, quantum network software must:

- Operate with ultra-low latency.
- Execute logic in real time.
- Run efficiently on chosen hardware platforms.

These software-related timing requirements are difficult to simulate accurately, making them a critical area of focus during the pilot phase. The software must be validated in real-world conditions to ensure it can keep pace with the hardware.

Effective software must also support informative, actionable diagnostics. During the Pilot and Trial phase, an organization can identify performance bottlenecks and errors quickly. Quantum networking software should provide analytics tools to track metrics like entanglement fidelity and transmission rates, and logging systems to capture time-stamped event data. These tools help teams avoid issues, and when issues do occur, make it possible to pinpoint the root cause of these errors and resolve them efficiently. These features are important for internal debugging and for communicating effectively with vendors about both hardware and software performance.

Sophisticated quantum software must be installed, configured, and maintained by individuals with experience across multiple domains. Teams must be able to deploy software on diverse hardware platforms, troubleshoot installation and runtime issues, and diagnose and resolve communication failures between network nodes. Beyond installation, protocol-level expertise is also important. Quantum network protocols can sometimes behave unpredictably under real-world conditions. Teams need the skills to analyze and debug these behaviors to ensure reliable performance.

Quantum Secure Communications applications rely on several assumptions about the classical infrastructure that the quantum network is integrated into, particularly the use of authenticated channels. Compromise at the classical layer can undermine the security of the entire system. Even below the application at the protocol level, it's necessary to employ techniques like authentication to prevent any unauthorized actors from attacking the network and preventing it from servicing users.

As with hardware, software vendors are excellent partners to enlist in a pilot quantum network rollout. Their support can accelerate deployment, streamline troubleshooting, and ensure best practices are followed. Organizations should seek out vendors who give access to clear documentation and deployment guides, availability of hands-on training and onboarding resources, and direct communication channels for support and collaboration. Establishing a strong feedback loop with vendors also helps surface and resolve issues early on, allowing your internal team to focus on integration and expansion of the network.

What makes a “good” pilot quantum network?

A lot of useful, actionable information can be gleaned from a pilot quantum network.

Goals for a pilot network often include providing a proof of concept, validating the hardware / software / architecture of the network design, and testing the performance and interoperability of the individual components at an efficient and manageable scale. Building a pilot network helps organizations predict the performance of a full-scale quantum network and confirm the design assumptions with real-world data. A pilot quantum network also makes it possible to stress-test the likely bottlenecks and failure points that could hinder a full-scale deployment.

There are two approaches to building a pilot quantum network that are both realistic and strategic. One approach is to implement a portion of the full-scale network. Another approach is to build a pilot of what are predicted to be the least performant parts of the network: those scenarios where fidelity, throughput, or protocol success may be limited. The aspects of a quantum network that heavily influence its performance are the physical distance between nodes, the number of intermediate nodes, environmental factors, and the specific hardware configurations or limitations.

Building the Pilot Quantum Network

Step 1: Validating hardware components.

With a pilot network design in hand, you’re ready to test the individual components before assembling them into the pilot quantum network. Validating hardware individually first helps to isolate, identify, and resolve any issues early on.

These initial tests should include assessing the fidelity of entangled photon sources, measuring latency and attenuation in optical fibers, and evaluating the storage and retrieval performance of quantum memories. Because quantum systems are highly sensitive, even small manufacturing variations can significantly impact performance. At times there may be discrepancies between modeled and actual behavior; some components may underperform, requiring replacement or vendor support.

These tests also provide an opportunity to cross-check the assumptions made during the design and emulation phase. By comparing empirical data with simulated results, teams can refine their models and improve future simulations of their expanding network. Insights into hardware variability can be fed back into the simulation and emulation tools, enabling more accurate performance forecasts and better-informed decisions before scaling up the network.

Step 2: Build the pilot quantum network in stages.

Once individual components are verified, you can begin integrating them into increasingly complex configurations. For example, after confirming that a photon source produces high-fidelity entanglement and a spool of optical fiber meets expected transmission characteristics, these can be connected to test the end-to-end flow of quantum data. Adding nodes, links, and protocols in stages creates a step-by-step path toward a fully operational pilot.

It can also be beneficial to begin pilot quantum network integration in a highly controlled environment, such as placing all hardware in a single room with minimal distance between components. This baseline helps isolate issues as the system scales. If performance degrades when components are separated across longer distances or more complex topologies, teams can revert to the known-good configuration, pinpoint the source of the problem, and resolve the issue efficiently and effectively.

This incremental approach to building the pilot quantum network can de-risk broader deployment and improve outcomes. It’s also an opportunity to build internal know-how with quantum networks.

Step 3: Benchmarking the pilot quantum network.

This step is where the design meets reality! Establish clear testing objectives and benchmark metrics aligned with your use-case requirements to test the performance of the pilot quantum network.

For example, a Quantum Secure Communications network must meet two key performance thresholds:

- Entanglement fidelity of at least 0.9
- Distribution rate of at least 10 entangled pairs per second

To test these performance metrics, the pilot quantum network is used to distribute entanglement between two nodes. State tomography, a technique for reconstructing the quantum state, can be used to estimate the average fidelity of entanglement. While we won’t dive into the technical details of state tomography here, it’s important to note that it requires a large number of entangled pairs because quantum states cannot be cloned or fully characterized from a single instance. This naturally supports rate testing as well: by measuring how many entangled pairs are produced over time, it’s possible to evaluate whether the network meets the required 10 entanglements-per-second rate.

Another requirement of a Quantum Secure Communications network is connectivity. Any two nodes in the network must be able to execute the necessary protocols. Assuming the appropriate application software is already in place, this step is a good opportunity to validate that the software runs correctly over the pilot network, ensuring end-to-end functionality.

There are many additional benchmarks to test, including classical communication performance between nodes, correctness / responsiveness of the control and orchestration software, and long-term stability of quantum hardware under sustained operation. The nature of your tests may also vary depending on the generation of repeater technology being evaluated. For example, in networks using first- or second-generation quantum repeaters, testing will focus on fidelity of entanglement and entanglement generation. In networks using third-generation quantum repeaters, the emphasis shifts toward evaluating transmission fidelity and loss rates. By aligning tests with architectural goals and technology selection, organizations can ensure their pilot quantum network meets requirements and also forms the foundation for scaling up.

Frequently asked questions about building a pilot Quantum Network

How much physical space is needed for the pilot quantum network?

The short answer is that it depends! First, it depends on how many nodes and the amount of hardware that is needed to fulfill the goals of the pilot. Additionally, many hardware components in a quantum network have very different space requirements depending on the technology that's used. For example, if using room temperature technologies, then it’s often the case that these hardware components have a much smaller form factor. In contrast, if using something like cryogenically cooled hardware, there's an additional space constraint due to the additional refrigerator that's supplied for cooling the hardware.

What types of applications would be helpful to run on a pilot network?

Quantum Secure Communications (QSC) actually has very low network requirements, so it’s possible to build a pilot quantum network with a limited number of quantum memories and other components. This use case also has more flexibility in how much entanglement needs to be available between network nodes at the same time. For these reasons, QSC is a great application for testing a pilot network, because it has much more accessible requirements for achieving high performance. The benchmarking tests themselves are also really helpful for gauging the performance of the pilot network. For example, state tomography can benchmark the network performance but it's also a good application to target as an indicator of how well different applications would run on the network.

How does Quantum Secure Communication work on a quantum network?

At a high level, Quantum Secure Communication works by using a quantum network to generate shared, secret keys between two parties. Here's how it breaks down:

The quantum network distributes entangled particles across the nodes. From these entangled particles, each party extracts a bit stream: a sequence of raw data bits that are correlated between the two ends.

Once both parties have received their bit streams, they perform a process called key distillation. This involves checking for and correcting any errors that may have occurred during transmission due to noise or hardware imperfections. This also ensures that no eavesdropper has tampered with the communication. If an eavesdropper tries to intercept the entangled particles, the laws of quantum mechanics guarantee that it will introduce detectable anomalies, so QSC has built-in eavesdropper detection!

After these checks, the bit streams are refined into cryptographic keys that both parties can now use to encrypt their communication. In this case, the quantum network's role is to securely generate and deliver the raw material for these shared keys.

Common pitfalls when building a Pilot Quantum Network

There are several easily avoidable but common pitfalls that can prevent your pilot quantum network from being a success.

The most critical pitfall is insufficient hardware verification. Properly functioning hardware is the foundation of any quantum network. If one component fails to perform as expected, it can jeopardize the entire pilot network as a whole. Skipping or rushing this step will lead to costly setbacks, such as deployment of malfunctioning devices that then cause the network to behave unpredictably, or worse, fail entirely without clear explanations.

Closely related to this first pitfall is the proper validation of the network operating system. This software controls the hardware directly and underpins the functionality of all higher-level applications. If the operating system behaves inconsistently or inaccurately reflects the hardware’s actual state, it can lead to serious confusion during testing and debugging. You might find that your software reports one thing while the physical network is actually doing something else entirely.

When using software provided by your hardware vendor, it’s important to confirm that it has been thoroughly tested by the vendor. Just as importantly, vendors should provide clear guidance on how to verify the software within your organization’s pilot network.

Lastly, when it comes to building internal familiarity with quantum technologies, it's important to have ample documentation of the design, testing, installation, troubleshooting, and management of the hardware and software components of the network. Deploying a quantum network is an interdisciplinary effort that requires expertise across many fields such as quantum physics, electronics, and computer science and engineering just to name a few. Because so many diverse fields are involved, it is difficult for any one individual to track all the details. Recording as much of this information for future reference as the pilot quantum network is being built will be extremely helpful, especially when needing to communicate this information between different experts in various fields.

From pilot to full-scale deployment

As you progress through the Pilot and Trial phase of deploying a quantum network, a natural question arises: When and how does a pilot quantum network move to full-scale deployment?

You'll know you're ready to scale when several key conditions have been met:

1. Your pilot network must demonstrate satisfactory performance. This means that the network behaves as expected and aligns with your design and emulation models. The pilot should be fully tested and verified, showing that it's a stable foundation of hardware and software to build on.
2. The application layer must perform reliably. If your application software, such as Quantum Secure Communications or distributed quantum computing consistently runs well over the pilot network, you're in a strong position to move forward. Remember that the pilot likely doesn't cover every possible node combination or topology in the full-scale network. You may need to conduct additional tests on new node arrangements and protocol behaviors as the system expands. This is particularly important if your applications require dynamic or complex routing that wasn't exercised in the limited pilot.
3. A clear and practical scaling plan must be in place. This includes procurement of additional hardware and software as needed, a well-defined network layout and deployment strategy, and testing and verification plans for validating the expanded network.

Pilot network achieves desired benchmarks and passes tests

- Hardware and software looks good

Applications have been tested and work as desired

- Usability of network looks good

Plan for transitioning to full-scale deployment in place

If your pilot is actually a subset of the eventual full-scale network, you can approach scaling incrementally by adding new links and nodes in phases. As you grow the network, repeat the same types of tests used in the pilot and during the design and emulation phase, using your accumulated experience to validate each stage of expansion.

Pilot and Trial is the critical bridge between network design and full deployment. It allows you to validate your architecture and gain practical experience in building and maintaining a quantum network. Vendor collaboration is essential. You're not in this alone! Maintaining strong communication with your hardware and software providers ensures that you get the right tools, guidance, and support throughout the entire process. Are you looking for a quantum networking vendor that can help your organization build a quantum network aligned with your goals? Aliro is one of the only companies focused exclusively on entanglement-based quantum networking, with the flexibility for integrating with classical networks, PQC, and QKD. Aliro software reflects best practices, insights from real deployments, and deep experience across telecom, defense, and research sectors.

Phase 3: Full-scale Deployment

The deployment of full-scale entanglement-based quantum networks represents an important leap of technological advancement, one that parallels the transistor in its potential to reshape the foundations of technology. Beyond an upgrade, this is a new paradigm in communication and connectivity. With the ability to harness the laws of quantum physics, organizations are stepping into a world where security is no longer a matter of mathematical probability, but of natural physical law.

Phase 3, Full-Scale Deployment, executes a strategic data-driven quantum vision. This is the stage at which quantum potential becomes reality: a production-ready infrastructure enabling a level of secure connectivity we've never before had access to. The primary objectives of this phase are to achieve quantum-secure communication at scale, enable interconnectivity between quantum systems, and support a range of critical applications including:

- **Critical infrastructure protection.** Hardened security posture for cloud providers, telecom networks, defense operations, and public sector infrastructure.
- **Quantum Secure Communications (QSC).** Provably secure key exchange immune to interception and computational attack, essential for safeguarding data centers, national security, and financial networks.
- **Quantum computing and sensing integration.** Seamless interconnection between quantum sensors and quantum processing units across a distributed network.

In this phase, organizations can minimize deployment friction by supporting heterogeneous quantum hardware and using existing fiber infrastructure. Network orchestration and management tools can be integrated into classical networking management tools for real-time monitoring, performance optimization, and fault response. Let's take a look at how organizations transition from pilot quantum networks to production quantum networks, the key technical and organizational considerations involved in deployment at scale, and strategies for integrating entanglement-based quantum technology into your organization's long-term infrastructure and security planning.

Moving from the Pilot & Trial stage to Full-Scale Deployment

By the end of the Pilot & Trial stage, an organization will have successfully deployed and operated a small-scale entanglement-based quantum network. These small-scale quantum networks typically span a single room, building, campus, or a metropolitan area. A pilot network validates core capabilities such as device integration, network orchestration, entanglement generation, and some performance benchmarking.

At this point the network is running, controlled by software, and delivering measurable outcomes. Teams will have done some initial optimization and gained familiarity with both the physical and software components that are used in quantum networking. This hands-on experience is essential groundwork for transitioning to a full-scale quantum network.

Pilot & Trial deliverables:

- ✓ Small-scale quantum network
- ✓ Operational
- ✓ Devices integrated and controlled by software
- ✓ Benchmarking & verification experiments
- ✓ Initial performance assessment and optimization
- ✓ Alignment with network owner preferences
- ✓ Internal familiarity

Scaling up from a pilot to a production-ready quantum network introduces a new set of strategic and architectural considerations. Before moving forward with a full-scale deployment, organizations should be aligned across several dimensions of the proposed design:

1. **Organizational objectives and user model.**
   What is the overarching purpose of the quantum network? Will it be an open-access system serving external users, or a closed, internal resource? Identifying the intended user base (researchers, security teams, compute clusters, etc.) and their desired use cases will inform further implementation decisions.
2. **Target applications and performance requirements.**
   Quantum Secure Communications, distributed quantum sensing, or networked quantum processors for computational power each have different technical expectations as the network grows. These include latency, fidelity, throughput, and other performance metrics.
3. **Geographic and physical scope.**
   Expansion goals should reflect both ambition and reality. Will the network serve additional buildings, campuses, or cities? Physical geography, infrastructure constraints, and organizational priorities will shape whether extending fiber optics, free-space laser links, or satellite-based systems will be the best approach for extending the network's reach.
4. **Integration with classical infrastructure.**
   Quantum capabilities do not exist in isolation. Full-scale deployment must consider

how entanglement-based security and services will interoperate with existing classical networks and digital infrastructure.

5. **Resource and access management.**
As the network grows, so does its complexity. New hardware, channels, and users require careful planning for scheduling, access control, and maintenance.
6. **Budgetary and timeline constraints.**
Real-world constraints such as funding cycles, procurement lead times, and workforce availability must also be factored into any deployment plan. These constraints will directly influence technology selection, phasing strategies, and service rollout.

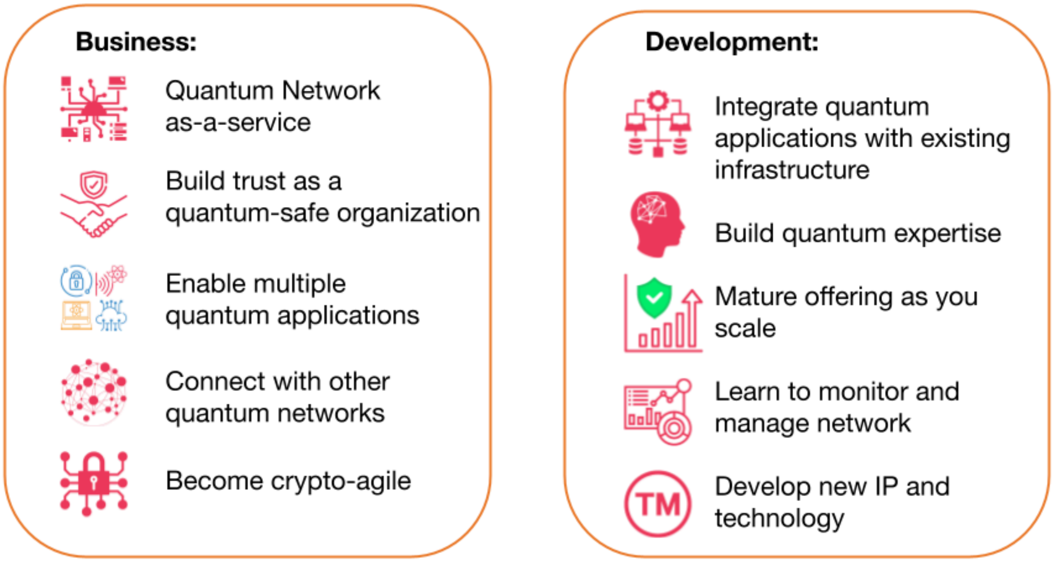
Considerations for Full-Scale Deployment:

- Who are the intended users?
- Open or closed network?
- What applications do I want my network to support?
- What metrics do I need to meet?
- What distances do I want to achieve?
- How will this integrate with existing classical infrastructure?
- What are my constraints?
- How do I want to manage access?

Organizations that clearly articulate intended applications, user access models, geographic scope, and integration points will have a much smoother transition from pilot to full-scale quantum network deployment.

Unique benefits of Full-Scale Deployment

Being at the forefront of quantum networking offers real advantages. Leaders in quantum communications can harden their internal network infrastructure and simultaneously position themselves as trusted providers of quantum services. Enterprises adopting quantum technology today are well-positioned to shape standards, influence the direction of the ecosystem, and capture early market share in what is becoming critical infrastructure.



A full-scale deployment is not limited to a single use case. Unlike single-purpose prepare-and-measure quantum key distribution (QKD) networks, general-purpose entanglement-based networks are designed to support multiple applications beyond secure key distribution.

Entanglement-based quantum networks enable the connecting of Quantum Processing Units for greater quantum computing power, or networking quantum computers together to enable distributed quantum computation. Entanglement-based quantum networks also enable blind quantum computing, where both the data and the algorithms used are kept secret from the quantum computer operator, a valuable use case for secure remote quantum compute access.

Entanglement-based quantum networks are also required for distributed quantum sensing for many diverse applications such as navigation and timing in GPS-denied environments, biomedical magnetometry, and privacy-preserving distributed measurement.

A common misconception is that only quantum computers or other quantum end nodes can be interconnected via entanglement-based quantum networks. However, while Quantum Secure Communication (QSC) is uniquely enabled through entanglement-based quantum networking, it doesn't require the end nodes to be quantum-native: classical end nodes like computers and data center servers can be securely connected. QSC is widely recognized as the most secure method for protecting network communications, offering the highest level of security possible for both classical and quantum end nodes.

The versatility of entanglement-based quantum networks ensures that the infrastructure deployed today can adapt to a broad range of use cases tomorrow. As more quantum networks come online, inter-network connectivity becomes possible, opening the door to new partnerships, shared services, and a growing ecosystem of quantum-enabled enterprises.

Crypto-agility is especially relevant for businesses and enterprises that rely on secure communications. Telecoms, utilities companies, financial institutions, and medical organizations are just a few of the sectors that require provably quantum-secure networks. As more sensitive data becomes digital, organizations must be able to update their defenses continuously. A full-scale quantum network supports this agility by offering quantum-safe capabilities and a platform for innovation.

From a development perspective, organizations have the potential to integrate quantum applications with existing infrastructure, and to enhance existing services while expanding into novel offerings. Organizations will also build invaluable internal expertise in quantum networking. These skills will be foundational in the years ahead, and internal familiarity will be a significant market differentiator.

Operating a quantum network includes learning to monitor, manage, and optimize entangled channels, hardware resources, and user access. This kind of familiarity often leads to the development of new intellectual property, proprietary applications, and capabilities not yet imagined today. Just as the Internet gave rise to technologies like search engines, video conferencing, and real-time collaboration platforms, the Quantum Internet will similarly create entirely new product categories.

General quantum network hardware requirements

Scaling a quantum network from a pilot or testbed to a full-scale utility network requires very particular hardware components. Every link, memory, and detector must preserve fragile qubits as they traverse the network. Below is a basic overview inventory of core components you can expect to deploy.

- Entangled photon sources. Devices that reliably produce pairs of entangled photons.
- Single photon detectors. Devices capable of detecting individual photons.
- Quantum memories and repeaters. Devices that can maintain and hold qubits.
- Optical components: optical switches, modulators, and integrated optics that steer and manipulate quantum information encoded in photons.
- Dark fiber links. Passive terrestrial fibers with no inline amplifiers or routers.
- Free-space lasers. Ground-to-ground or ground-to-satellite links that bridge distances where fiber becomes impractical. Enabled by satellites and laser telescopes.
- Timing and synchronization systems. Sub-nanosecond scale timing and synchronization that keeps every node in temporal lockstep.
- Beam tracking systems. Precision hardware and sensors that hold free-space beams on target.

- Classical encryptors and decryptors. AES or PQC appliances that secure management traffic and conventional data riding alongside quantum services.
- Satellite deployments. Space-hardened, radiation resilient, low-SWaP versions of the critical components.

Technologies that scale Quantum Networks

Pilot quantum networks have demonstrated entanglement over metropolitan fibers and short terrestrial testbeds, but meaningful commercial or mission-critical services require entanglement over significant distance, with high throughput and reliability. Photons must successfully traverse hundreds of kilometers, qubits must be stored long enough to run necessary protocols, and every component must interoperate despite inevitable loss, noise, and vendor diversity.

Enabling technologies and practical engineering considerations are needed to deliver a full-scale, heterogeneous quantum network.

Single photons attenuate exponentially with distance. To make long distance fiber links, a quantum repeater can be used to break that distance into shorter elementary links, store the resulting entanglement in quantum memory, and perform a Bell-state measurement to "swap" the entanglement. After a series of swaps, the endpoints (Alice, Bob) share a high-fidelity pair even though no photon ever traveled the full path. This process is known as entanglement swapping and it's the primary function of a quantum repeater.

As quantum networks expand, quantum routers will become important for connecting complex topologies. To sustain high entanglement-generation rates and fidelity across these longer links, quantum networks will use multiplexing, a concept from classical communications that can be adapted for quantum communications. In practice, a single fiber (or free-space path) carries mixed traffic:

Quantum signals made up of quantum states encoded in single photons, or a higher dimensional state in a few photons.

Classical signals made up of bits that carry messages, Bell-state-measurement results, synchronization pulses, and management data.

There are different approaches to achieving this and each approach mitigates crosstalk differently, but all share the same objective: maximize resource utilization and preserve quantum fidelity.

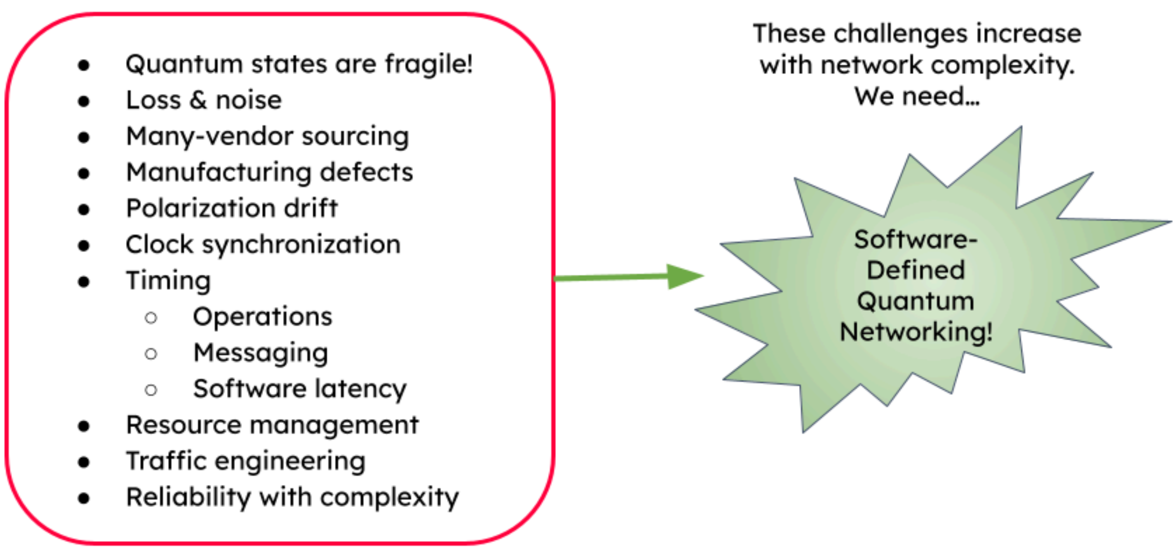
For very long distances, free space optics such as satellites and laser telescopes will play a key role in extending the reach of quantum networks. A satellite could communicate to a series of ground stations, which are geographically very far apart. A free space optical channel will be more beneficial for links in which the loss and noise are mitigated more readily in a free space channel rather than a series of terrestrial repeaters.

Higher-performing components translate directly into longer reach and high quality entanglement. Efficient photon sources and detectors boost the efficiency of the network. Long-lived quantum memories and robust light-matter interfaces store more qubits for a longer period of time enabling longer distances as well.

Well designed quantum control and classical messaging protocols determine how every node stores, swaps, and routes entanglement. Optimized protocols for scheduling resources, prioritizing traffic, and minimizing idle time aid the network in delivering higher entanglement generation rates, better fidelity, and longer reach.

Barriers to Full-Scale Deployment

Moving from a pilot quantum network to a live, multi-vendor quantum network spanning across long distances poses some unique challenges. Each additional node, component, and kilometer of distance multiplies exposure to loss, noise, timing drift, and architectural complexity. **Nearly all of these challenges can be addressed with software countermeasures.**



1. Fragility of quantum states.
    - Single photons are the preferred carriers of quantum information due to their compatibility with existing infrastructure, but they are notoriously fragile. Photon loss and environmental noise are common limiting factors for scaling a quantum network. For many quantum applications, fidelity below a certain threshold makes the network unusable.

2. Cross-vendor interoperability.
    - A commercial-grade network will likely content hardware components from a variety of vendors. Different laboratories and OEMs favor distinct photon sources, memories, and detectors, each with its own control API and calibration regime. Engineers face a tangle of proprietary interfaces that slows rollout and locks operators into a single supply chain.

3. Manufacturing imperfections at scale.
    - Minor variances in hardware quality are manageable in a tabletop quantum network. Multiply those imperfections across thousands of components, however, and this becomes a much more complex issue.

4. Polarization and phase drift.
    - Temperature fluctuations, vibrations, atmospheric effects, and a variety of environmental factors affect the encoding of the quantum state. As a result, a photon’s polarization or phase may wander during transit.

5. Nanosecond-scale timing and synchronization.
    - Photon generation, storage, retrieval, and detection must occur within tight coincidence windows, often within nanoseconds.

6. Resource management at scale.
    - Entangled pairs are finite resources. Large networks must decide in real time how to prioritize and manage network resources effectively and optimally

7. Traffic engineering and multi-tenancy.
    - Just as IP routers steer packets around congestion in a classical network, quantum networks will require dynamic routing and multi-tenancy.

8. Reliability and maintenance.
    - Rolling out firmware updates, replacing faulty hardware, or expanding capacity should not require a full network shutdown.

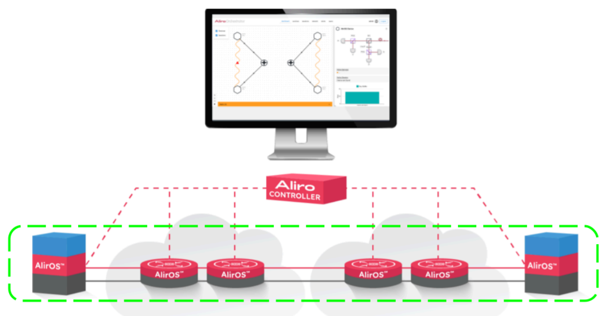
Software requirements of Full-Scale Quantum Networks

Building and running a full-scale quantum network requires a software-defined networking approach that can mitigate the barriers to quantum communications.

Application Layer
- User interface & API
- Orchestration, scheduling
- Operator interface

Management Layer
- Monitoring
- Resource optimization
- Eavesdropper detection
- Dynamic routing

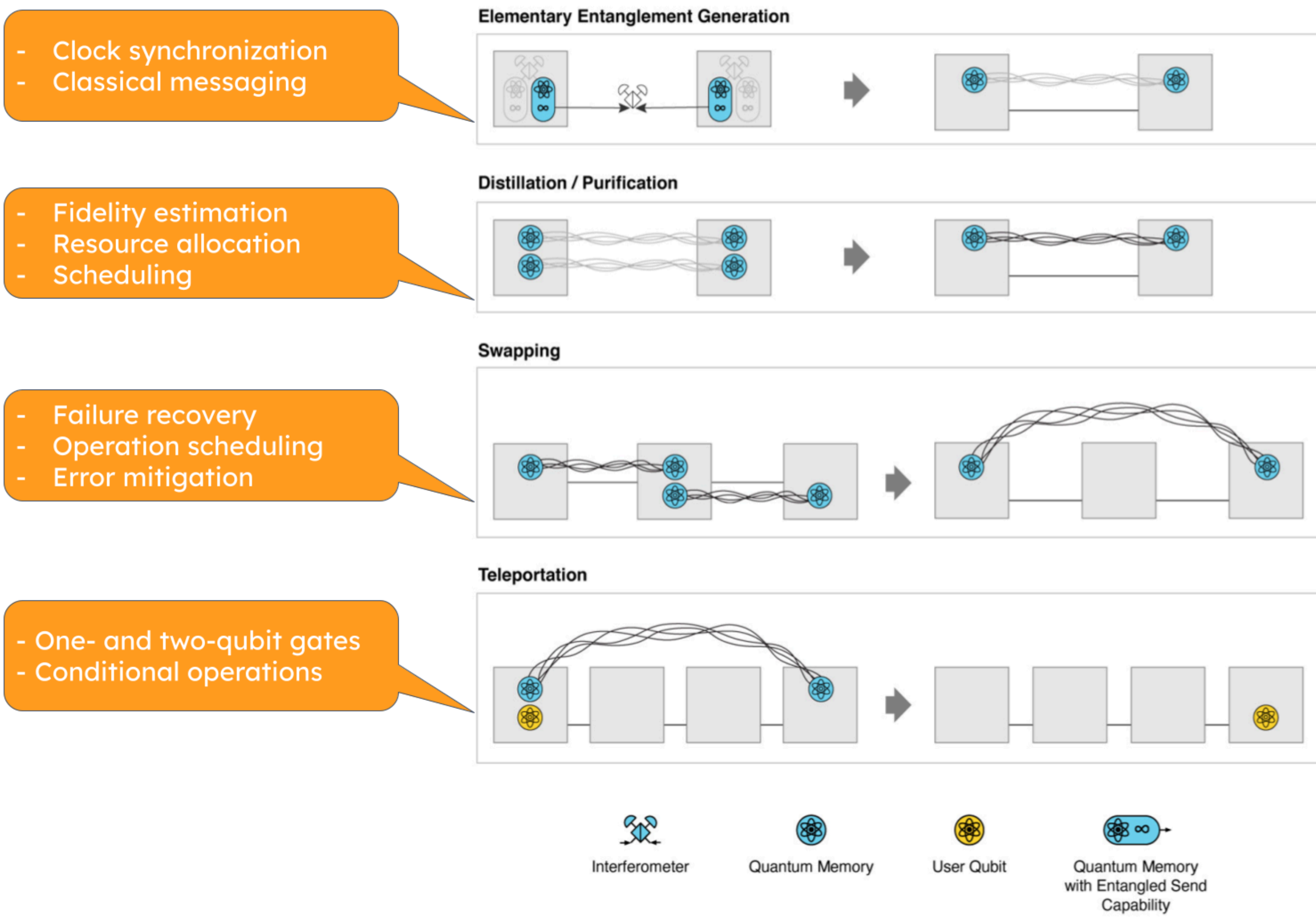
Control Plane/Data Plane
- Protocols for entanglement generation, distillation, swapping, teleportation, error mitigation
- Calibration/synchronization
- Hardware agnostic interface



At the top of the stack is the application layer, which turns quantum resources into straightforward services for both end-users and operators. The application layer must provide a portal for scheduling quantum services, set performance targets, and managing user access, as well as handling user priority levels, usage metering, and billing. The management layer relies on a single, software-defined network controller. It provides one interface for upgrades, real-time network health monitoring, optimizing resources, as well as usage accounting and billing. The control plane makes decisions about when to create entanglement, which route to use, and how to allocate resources. The data plane carries out necessary actions such as moving qubits through fibers and memories. Protocols for entanglement generation, distillation, swapping, teleportation, error mitigation are performed at this layer. Clock synchronization and timing systems ensure accurate compensation for errors and that devices are performing as intended. A hardware-agnostic interface ensures that any new photon source, quantum memory, or single photon detector can be added to the network without changing how the network is managed.

Protocols for Quantum Networking

Quantum networks are built on a small set of powerful protocols that are managed via software.



These four core protocols power entanglement-based quantum networks:

Elementary Entanglement Generation. This protocol creates entangled photon pairs between two adjacent nodes.

Software requirements:

- Synchronization to ensure photons arrive at an interferometer within nanoseconds of each other.
- Classical messaging to communicate click data and measurement data to each of the nodes.

Entanglement Purification or Distillation. This protocol uses several lower-fidelity entangled photon pairs to create one high-fidelity pair, trading the quantity of entangled photon pairs for better quality entanglement between photons.

Software requirements:

- Resource allocation and scheduling to perform purification at the right moment.
- Ability to estimate and track fidelity.

Entanglement Swapping. This protocol performs a Bell-state measurement at an intermediate node, stitching two links into one longer link. This is typically performed with quantum repeaters.

Software requirements:

- Coordinated scheduling of entanglement swapping operations.
- Coordinated, automated retry routines when entanglement swapping fails.
- Coordination of error-mitigation.

Quantum Teleportation. This protocol moves a qubit's state from point A to point B without sending the qubit itself. First, the two nodes share an entangled pair. The sender then measures its data qubit together with its half of the entangled photon pair, producing two classical bits. Those bits travel over a regular network link to the recipient, who applies one of four simple correction gates based on the bits it receives. This causes the receiver's qubit to become an exact replica of the original state. Software must time the quantum gates, deliver the classical bits with minimal delay, and trigger the right correction gate at the destination.

Software requirements:

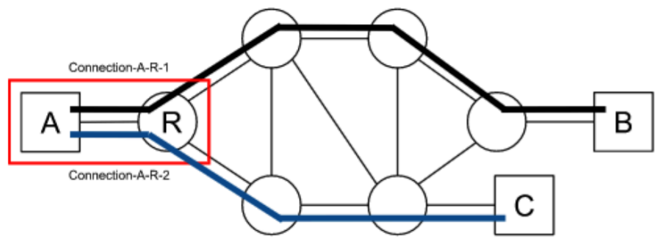
- Gate orchestration.
- Deliver the classical bits with minimal delay.
- Precision quantum-classical hand-off so the operation is completed before the entangled pair decoheres.

Realizing the potential of a Full-Scale Quantum Network

Pilot quantum networks typically start with a few links and a single application. Once the proof-of-concept succeeds, stakeholders quickly ask the bigger question: how do we run a dense, multi-user quantum network at meaningful scale? Below are the key architecture and software principles that turn a lab-grade test bed into an enterprise-class service.

Resource management

- Multi-tenancy. In a deployed network, many users will request entanglement simultaneously. A might want to connect to B as well as C.



  Both requests will go through quantum repeater R. The network needs to manage and orchestrate servicing both of these connections simultaneously by gauging resource usage, resource optimization, and multi-tenancy.

- Rate/fidelity tradeoffs. Some applications may require very high quality of entanglement, whereas other applications may require a higher entanglement rate. Navigating this trade off and meeting the different quality and rate requirements for different users and applications is best accomplished via software.
- Overlay networks. During off-peak hours when few users are requesting entanglement, control software can generate and store extra entangled pairs in quantum memories. Ongoing research is looking at these kinds of reserves to use during demand surges. The overlay network smooths out supply-and-demand spikes, improving service quality without over-provisioning hardware.
- Support multiple topologies. The software-defined network maintains several viable routing patterns (for example: mesh, star, and ring). For any new entanglement request, the network software can select the path that best fits current link health, latency, and resource load. If one route becomes congested or a repeater fails, the system instantly switches to an alternate topology, keeping every user and application online without wasting qubits or bandwidth.

Agility

- Test new protocols and applications as technology matures (e.g. multipartite entanglement). Successful full-scale quantum network deployments have the ability to upgrade and adapt the network in order to trial new protocols and applications, add new upgraded hardware, and roll out software updates as the network matures.

Building for easy iteration now means the network will be able to seamlessly integrate advancements later.
- Connect and leverage other quantum ecosystems. Linking your quantum network with nearby networks lets you share entanglement resources, expand geographic reach, and open new commercial partnerships.

Avoiding the hidden pitfalls of scaling a Quantum Network

There are hidden hazards that emerge the moment your network leaves the pilot phase, with limited users and use cases, and scales up to a production-grade multi-tenant quantum network. Organization-level pitfalls include:

- Failing to consider business use cases prior to acquiring hardware and building new links and nodes.
- Not detailing your constraints, preferences, tradeoffs, and user model before you scale up the quantum network.

System-level pitfalls include:

- Not testing your network's integrations with other services.
- Not hardening the security of the quantum / classical system.
- Not developing an internal team for maintenance, upgrades, repeatability.

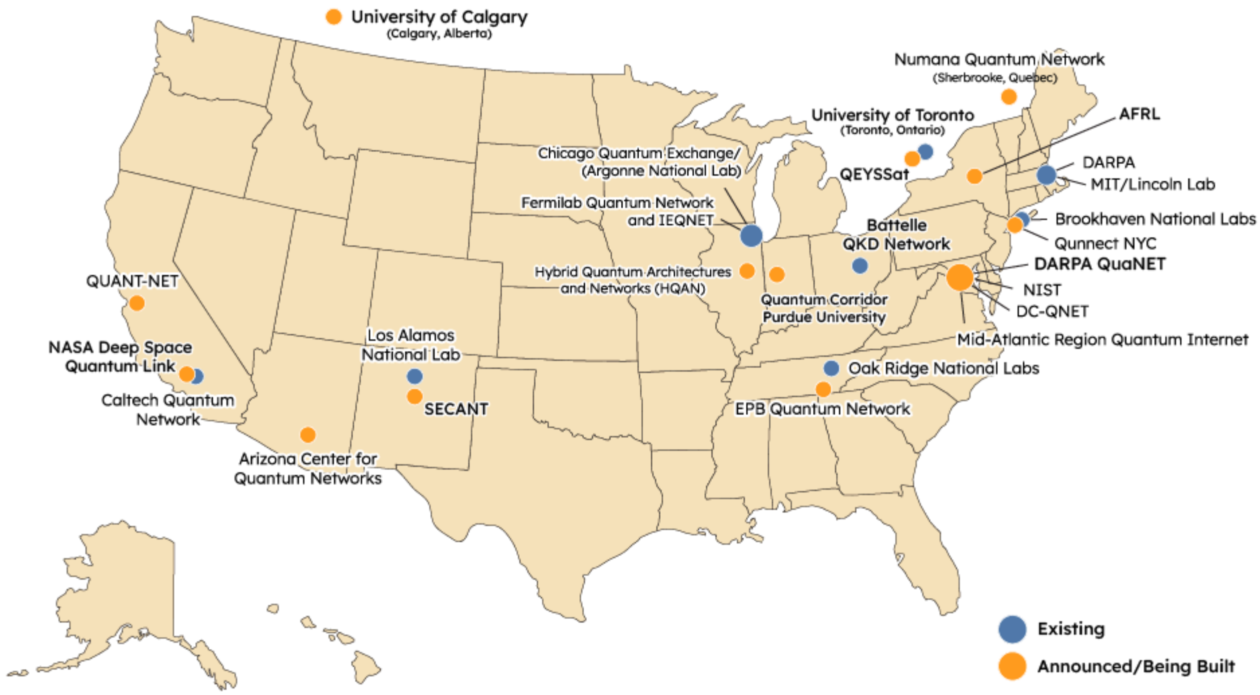
Setting up a full-scale quantum network for success includes considerations for business strategy, security posture, and operational discipline. Nail these foundations early on and subsequent upgrades to the network can be effective and efficient.

Building the Quantum Internet

The vision of the future is bright: a borderless quantum internet where computers, sensors, and yet-to-be-imagined quantum devices exchange entanglement as effortlessly as today's data packets. Organizations that scale beyond a pilot quantum network, and even linking to neighboring quantum networks, are turning an ambitious vision into practical reality.

Organizations that adopt a standards-first mindset fuel the momentum of the Quantum Internet. Hardware upgrades fall seamlessly into place. New partners connecting via well-defined interfaces. This future growth is made possible through the championing of open standards today.

Signs of progress are everywhere. Across North America, testbeds already hum with live traffic, and newly announced networks are springing up from coast to coast. Europe and Asia are accelerating in parallel, creating a virtuous cycle of innovation, investment, and shared learning. We are entering an exhilarating phase of quantum networking where we see continual leaps in reach, reliability, and performance.



Plan boldly, scale confidently, and start now!

A full-stack solution for Quantum Networking

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 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℠ 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.
info@alirotech.com www.alirotech.com

References

Barker, E. Recommendation for Key Management: Part 1 – General. NIST Special Publication 800-57 Part 1, Revision 5 (2020). https://doi.org/10.6028/NIST.SP.800-57pt1r5

Bartee, S.K., Gilbert, W., Zuo, K. et al. Spin-qubit control with a milli-kelvin CMOS chip. Nature (2025). https://doi.org/10.1038/s41586-025-09157-x

Brock, B.L., Singh, S., Eickbusch, A. et al. Quantum error correction of qudits beyond break-even. Nature 641, 612–618 (2025). https://doi.org/10.1038/s41586-025-08899-y

Google Quantum AI and Collaborators. Quantum error correction below the surface code threshold. Nature 638, 920–926 (2025). https://doi.org/10.1038/s41586-024-08449-y

Singkanipa, P., Kasatkin, V., Zhou, Z. et al. Demonstration of algorithmic quantum speedup for an Abelian hidden subgroup problem. Phys. Rev. X (2025). https://doi.org/10.1103/PhysRevX.15.021082

Thomas, J.M., Yeh, F.I., Chen, J.H. et al. Quantum teleportation coexisting with classical communications in optical fiber. Optica (2024). https://doi.org/10.1364/OPTICA.540362

Vermeer, M.J.D., Bicksler, B., Trail, J.M. et al. Preparing for post-quantum critical infrastructure. RAND Corporation (2022). https://www.rand.org/pubs/research_reports/RRA1367-6.html