Quantum Networks
The Next Frontier

Jim Ricotta
COO at Aliro Quantum

Why Quantum Networking Matters

Quantum networking is emerging as the foundational infrastructure for secure communications, distributed quantum computing, and next-generation sensing.

The Threat Landscape

- The rise of quantum computing threatens classical encryption
- Limitations of classical networking and security models
- "Harvest now, decrypt later" attacks are happening today
- Entanglement fundamentally changes what networking can do

Classical vs. Quantum Networks

Classical networks transmit bits — quantum networks distribute entanglement and quantum correlations, enabling capabilities that are physically impossible to replicate classically.

Current public-key cryptography is vulnerable to future quantum computers. Organizations must prepare now.

What is Quantum Networking?

A quantum network distributes entangled photons between distant nodes, enabling fundamentally new communication and computation capabilities.

Core Components

- Single Photon Detectors
- Entangled Photon Sources (lasers)
- Fiber & Free-Space Links
- Classical Control Channels
- Quantum Memories
- Quantum Repeaters

Key Concepts

→ **Entanglement**

Entangled particles (eg photons) must share the same state (physical law)

→ **No Cloning Theorem**

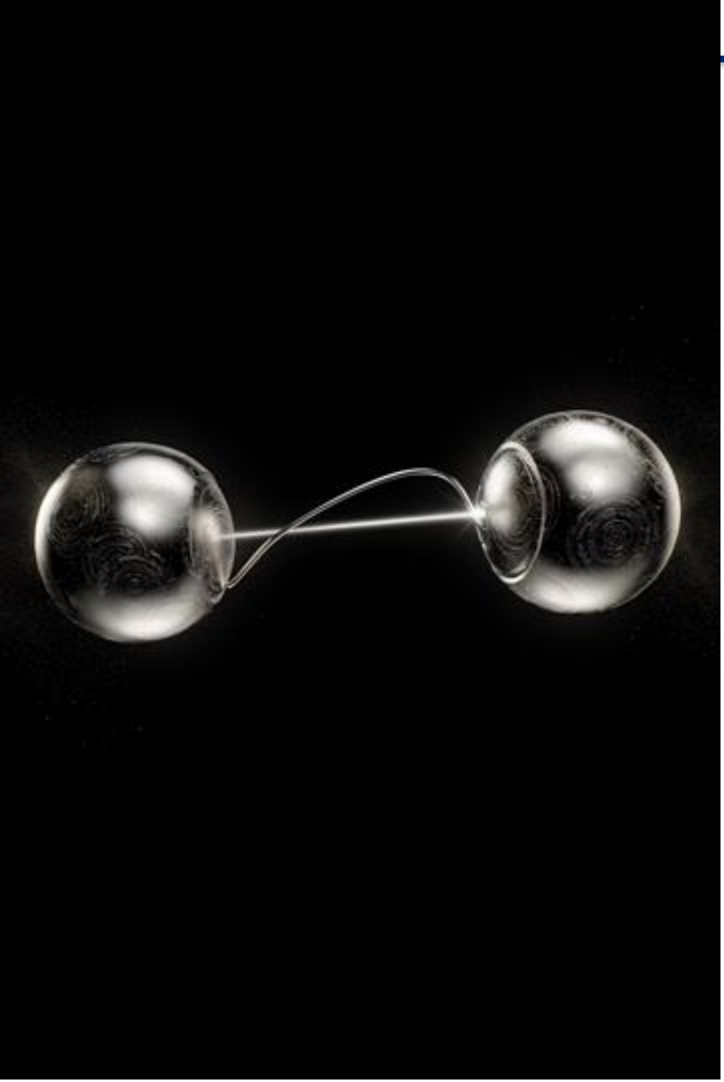
Quantum states cannot be copied — a fundamental security guarantee

→ **Only One Measurement Possible**

Observing a quantum state collapses it, making eavesdropping detectable

→ **No Quantum Computer required!**

Quantum Networks can be built and can run applications with No Quantum Computers involved!



Entanglement

What is Entanglement?

Entanglement is a quantum physics phenomenon where two or more particles become correlated in such a way that the quantum state of each particle cannot be described independently — even when separated by vast distances.

“Physics-based” security. Entanglement allows secrets to be shared without directly transmitting the secret itself.

Why Entanglement Enables Quantum Networking

1 Correlated Measurements

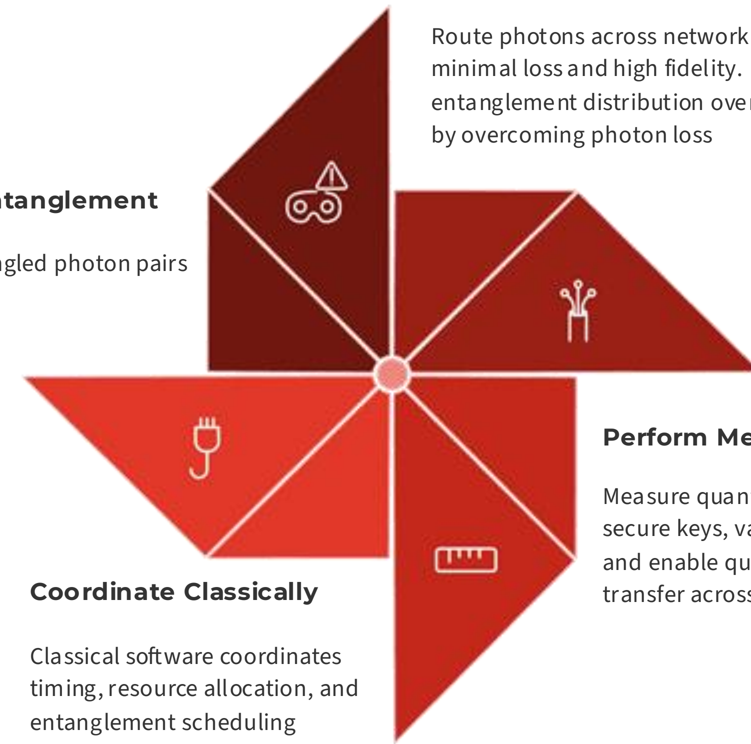
Measuring one entangled particle instantly determines the correlated state of its partner, regardless of distance

2 Detectable Eavesdropping

Any interception attempt disturbs the quantum state, revealing the presence of an eavesdropper

How Quantum Networks Work

Quantum networks combine photon generation, optical distribution, quantum measurement, and classical coordination into a unified architecture.



Generate Entanglement

Generate entangled photon pairs

Distribute Photons

Route photons across network paths with minimal loss and high fidelity. Extend entanglement distribution over long distances by overcoming photon loss

Perform Measurements

Measure quantum states to generate secure keys, validate entanglement, and enable quantum information transfer across the network.

Coordinate Classically

Classical software coordinates timing, resource allocation, and entanglement scheduling

Quantum Networking Use Cases

Networking Quantum Computers	Quantum Secure Communications	Quantum Position Verification	Networking Distributed Quantum Sensors
			
Quantum Compute Advantage	Secure Sensitive Data, Quantum Apps	Protects against spoofing	PNT, Exploration, Defense Advantage

Global Urgency for More Secure Networks

US Networking User Association

2025 Worldwide Threat Assessment

DEFENSE INTELLIGENCE AGENCY

Armed Services Subcommittee on Intelligence an

United States House of Represent

Jeffrey Kruse, Lieutenant General, U

How to factor 2048 bit RSA integers with less than a million noisy qubits

Craig Gidney

Google Quantum AI, Santa Barbara, California 93117, USA

May 23, 2025

Planning the transition to quantum-safe cryptosystems requires und
cost of quantum attacks on vulnerable cryptosystems. In Gidney+Ek
published an estimate stating that 2048 bit RSA integers could be fac
hours by a quantum computer with 20 million noisy qubits. In this paper,
reduce the number of qubits required. I estimate that a 2048 bit RSA
be factored in less than a week by a quantum computer with less than
qubits. I make the same assumptions as in 2019: a square grid of qubit
neighbor connections, a uniform gate error rate of 0.1%, a surface code
microsecond, and a control system reaction time of 10 microseconds.

The qubit count reduction comes mainly from using approximate resi
(Chevignard+Fouque+Schrottenloher 2024), from storing idle logical qub
surface codes (Gidney+Newman+Brooks+Jones 2023), and from alloca
to magic state distillation by using magic state cultivation (Gidney+
2024). The longer runtime is mainly due to performing more Toffoli g

Cisco shows quantum networking chip, opens new lab

By Stephen Nellis

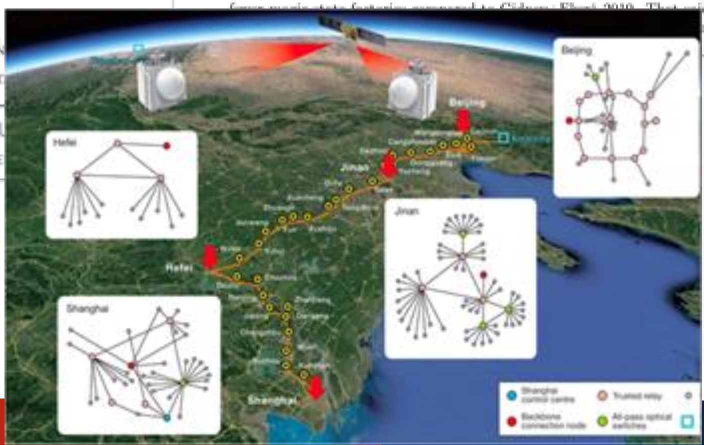
May 6, 2025 9:52 AM PDT · Updated 22 days ago

The Cisco logo is displayed, during the GSMA's 2023 Mobile World Congress (MWC) in Barcelona, Spain March 1, 2023. REUTERS/Nacho Doce/File photo Purchase Licensing Rights

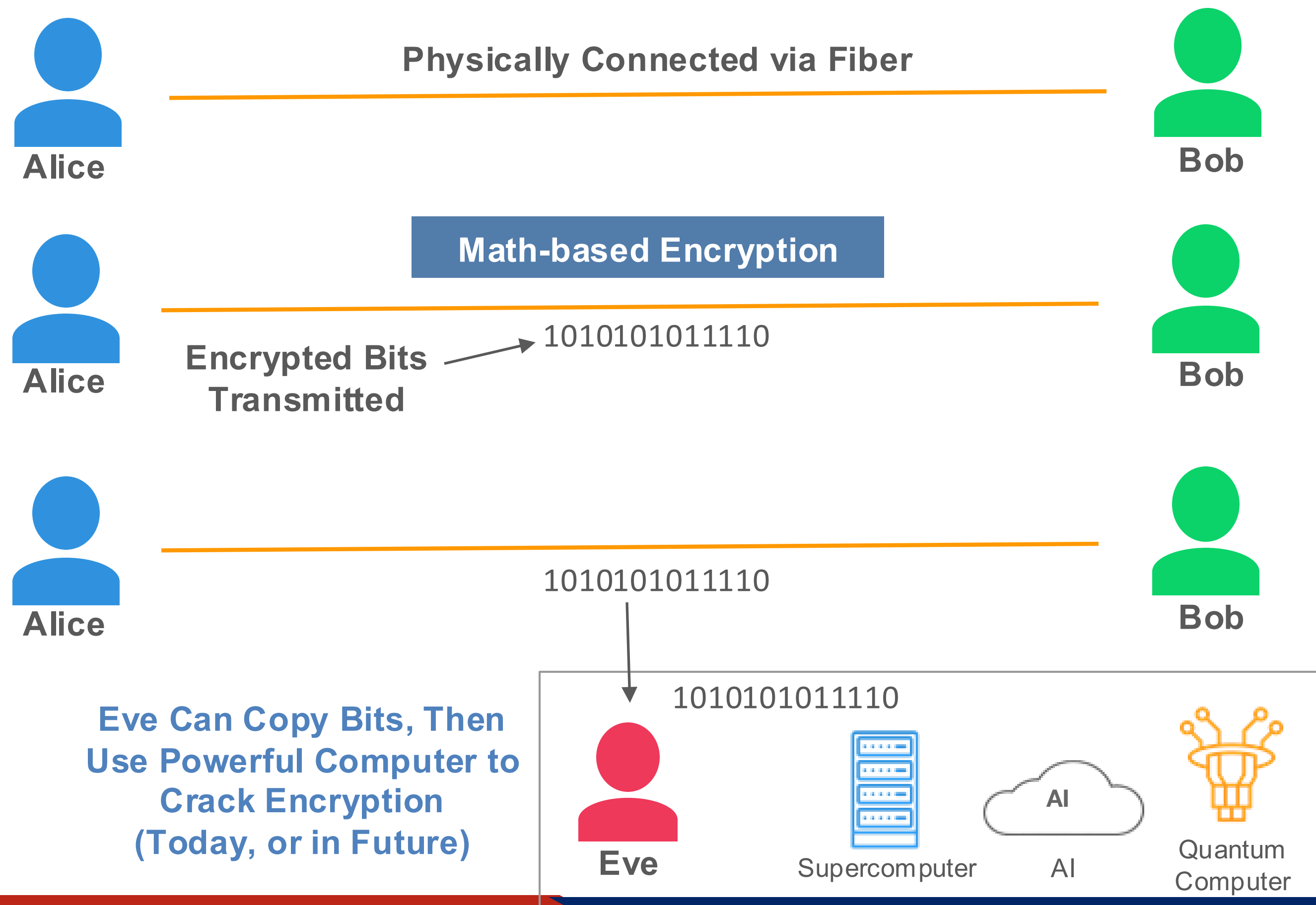
SAN FRANCISCO, May 6 (Reuters) - Cisco Systems on Tuesday showed a prototype chip for networking quantum computers together and said it is opening a new lab in Santa Monica, California, to further pursue quantum computing.

The chip uses some of the same technology as current networking chips and would help link together smaller quantum computers into larger systems. But Cisco also believes it will have practical applications before those computers become mainstream, such as helping financial firms sync up the timing of trades

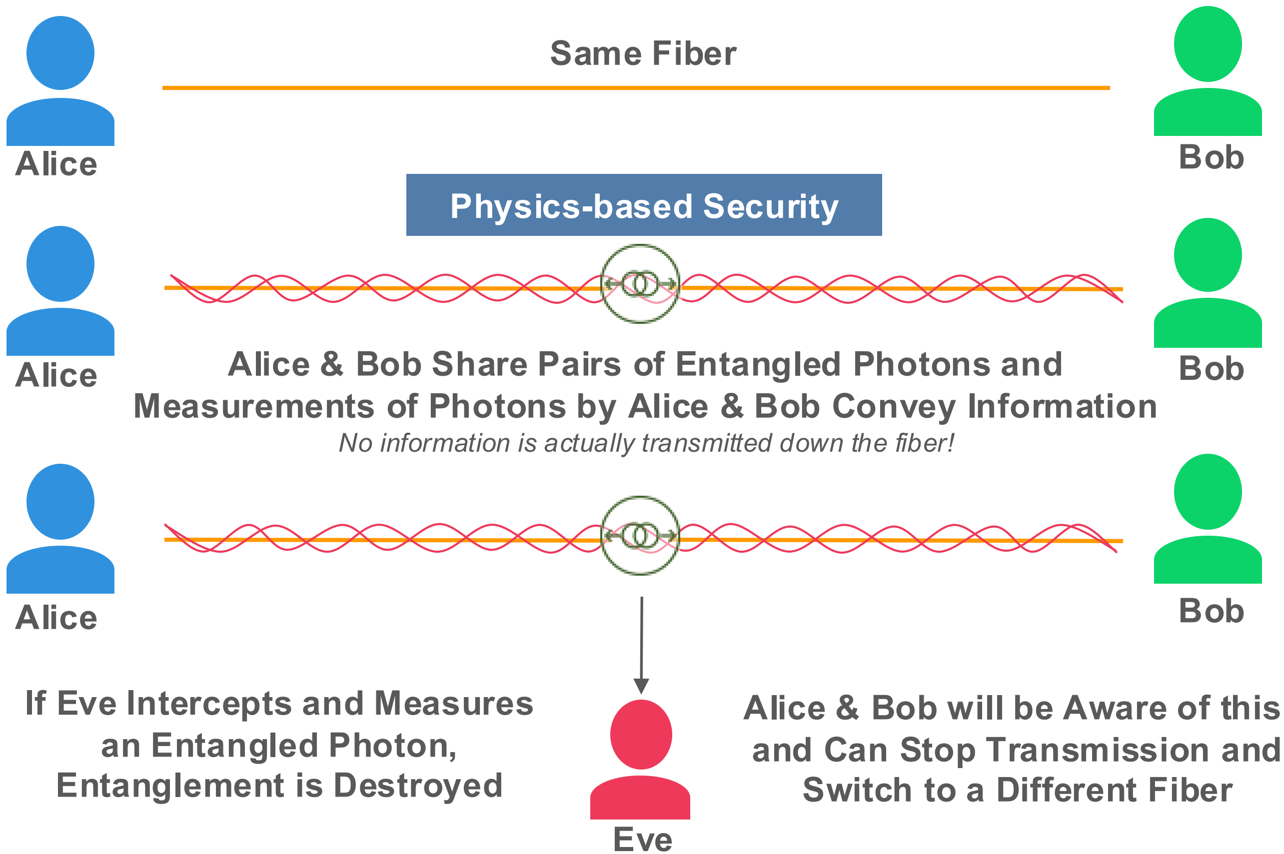
JPMorgan Chase establishes quantum-secured crypto-agile network



Today's Secure Communications



Quantum Secure Communications



No Amount of Computing Power Alone (Today or Future) Can Break!

Quantum Secure Communications (QSC)

Core Capabilities

- Entanglement-based Key generation
- Eventually use entanglement for entire message
- Complements Post-Quantum Cryptography (PQC)

Benefits

- Future-proof encryption
- Protection against quantum attacks
- Eavesdropper Detection

Real-World Drivers

National Security

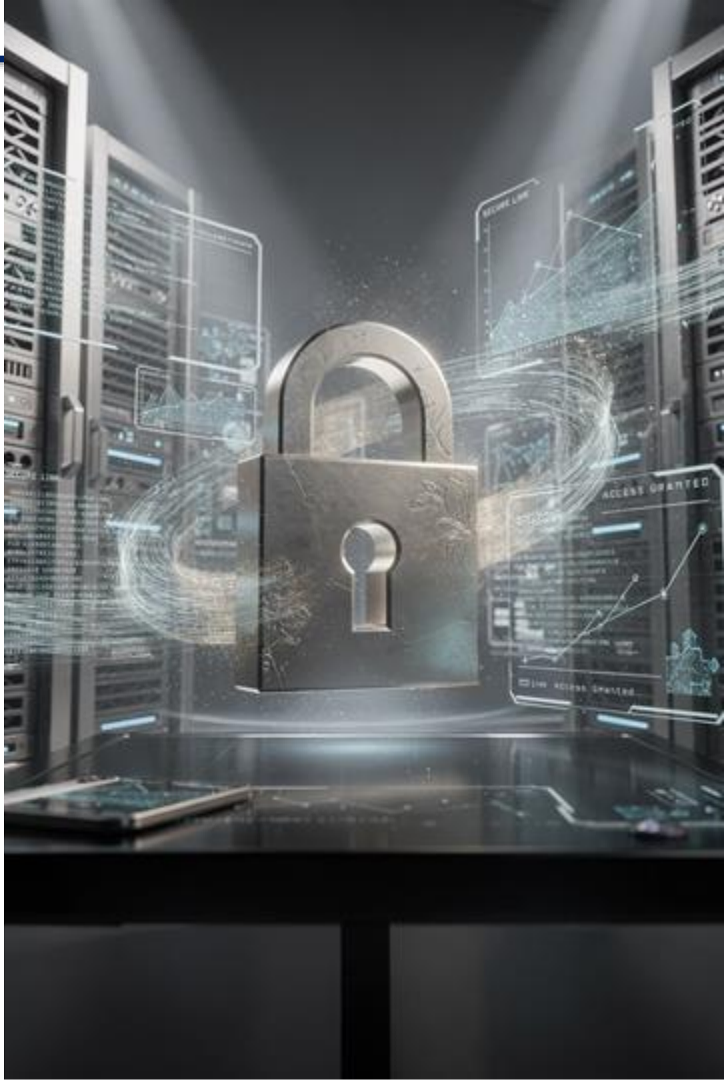
Governments require communications that remain secure against future quantum adversaries

Telecom Backbone Protection

Protecting the fiber infrastructure that carries critical national communications

Critical Infrastructure

Energy grids, financial systems, and healthcare networks require quantum-resilient security



Quantum Position Verification (QPV)

Quantum networking can verify location using the laws of physics — not just cryptographic assumptions.

How QPV Works

QPV leverages the "No Cloning" of quantum states
A sender's location is authenticated by demonstrating they can respond to quantum challenges that only someone at a specific position could answer within the required time window.

Position Authentication

Verifies that a party is physically located where they claim to be.

Anti-Spoofing

Quantum no-cloning prevents relay attacks that defeat classical GPS authentication.

Timing & Synchronization

Precise quantum timing enables sub-meter location verification.

Potential Applications

🛡️ Defense & Military

Authenticated command and control systems resilient to spoofing.

🛰️ GPS-Resilient Auth

Location verification that works even when GPS is jammed or denied.

🏛️ Secure Facility Access

Physical access control tied to verified quantum location proofs.

🤖 Autonomous Systems

Trusted positioning for drones, vehicles, and robotic systems.

Networking Quantum Processors

Quantum networking enables multiple QPUs to operate as one larger quantum system, breaking through the scaling limits of single-chip architectures.

The Scaling Problem

Current quantum processing units (QPUs) are too small for many commercially and scientifically useful applications.
Physical constraints limit the number of qubits on a single chip.
Quantum networking provides the path to scale.

Quantum data centers may eventually interconnect many quantum processors using quantum networks, analogous to how classical data centers interconnect CPUs & GPUs.

Key Concepts

Networked QPUs

Multiple quantum processors linked via entanglement channels to share quantum state

Private Quantum Computing

Use QSC for connections to QPUs; Obscure both algorithms & data

Modular Quantum Architectures

Build larger quantum systems from smaller, manufacturable modules connected optically

Distributed Quantum Computing (DQC)

Run quantum algorithms across geographically distributed processors as a unified system

US NUA
US Networking User Association

Networking Quantum Sensors

Entangled quantum sensors can achieve precision beyond classical limits, enabling entirely new sensing capabilities when networked together.

How Distributed Quantum Sensing Works

Quantum networking allows geographically separated sensors to behave like a single coordinated quantum system. Correlated measurements across nodes achieve sensitivity that no individual sensor could reach alone.

Distributed Sensing

Sensors at different locations share entanglement to perform correlated measurements.

Enhanced Sensitivity

Quantum correlations push measurement precision beyond the standard quantum limit.

Time Synchronization

Quantum clocks networked together achieve unprecedented timing precision.

Example Applications

🧭 Navigation Without GPS

Inertial navigation using quantum accelerometers and gyroscopes.

🌍 Gravitational Sensing

Mapping subsurface geology, mineral deposits, and underground structures.

🌊 Submarine Detection

Detecting submerged objects through quantum magnetic field sensing.

🔭 Scientific Instrumentation

Earth observation and astronomical sensing at quantum-enhanced resolution.

(US)NUA US Networking User Association

The Quantum Networking Stack

Like classical networking, quantum networks can be understood through a layered architecture, from physical photons at the bottom to applications at the top.

Layer	Function	Examples
Applications	End-user quantum services	QSC, QPV, DQC, Sensing
Orchestration	Resource mgmt & provisioning	Entanglement brokering, job queuing
Entanglement Management	Measuring/verifying entanglement	Protocols like BBM92, E91, BB84
Physical Layer	Quantum hardware & transmission	Photons, fiber, detectors

Future Enhancements

Quantum Repeaters

Extend entanglement distribution beyond direct fiber loss limits using entanglement swapping.

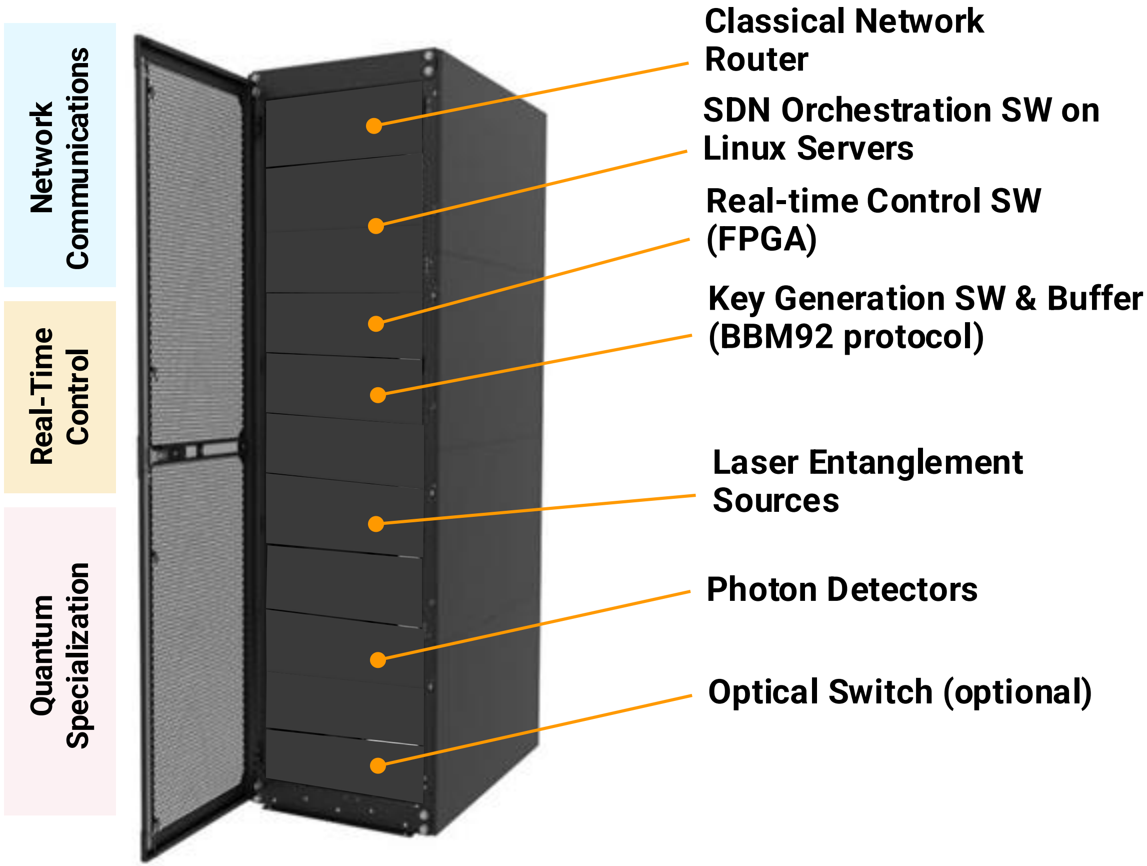
Multi-path Quantum Routing

Protocols for selecting optimal paths for entanglement distribution across a network.

Error Correction

Quantum error correcting codes protect fragile quantum states during transmission and storage.

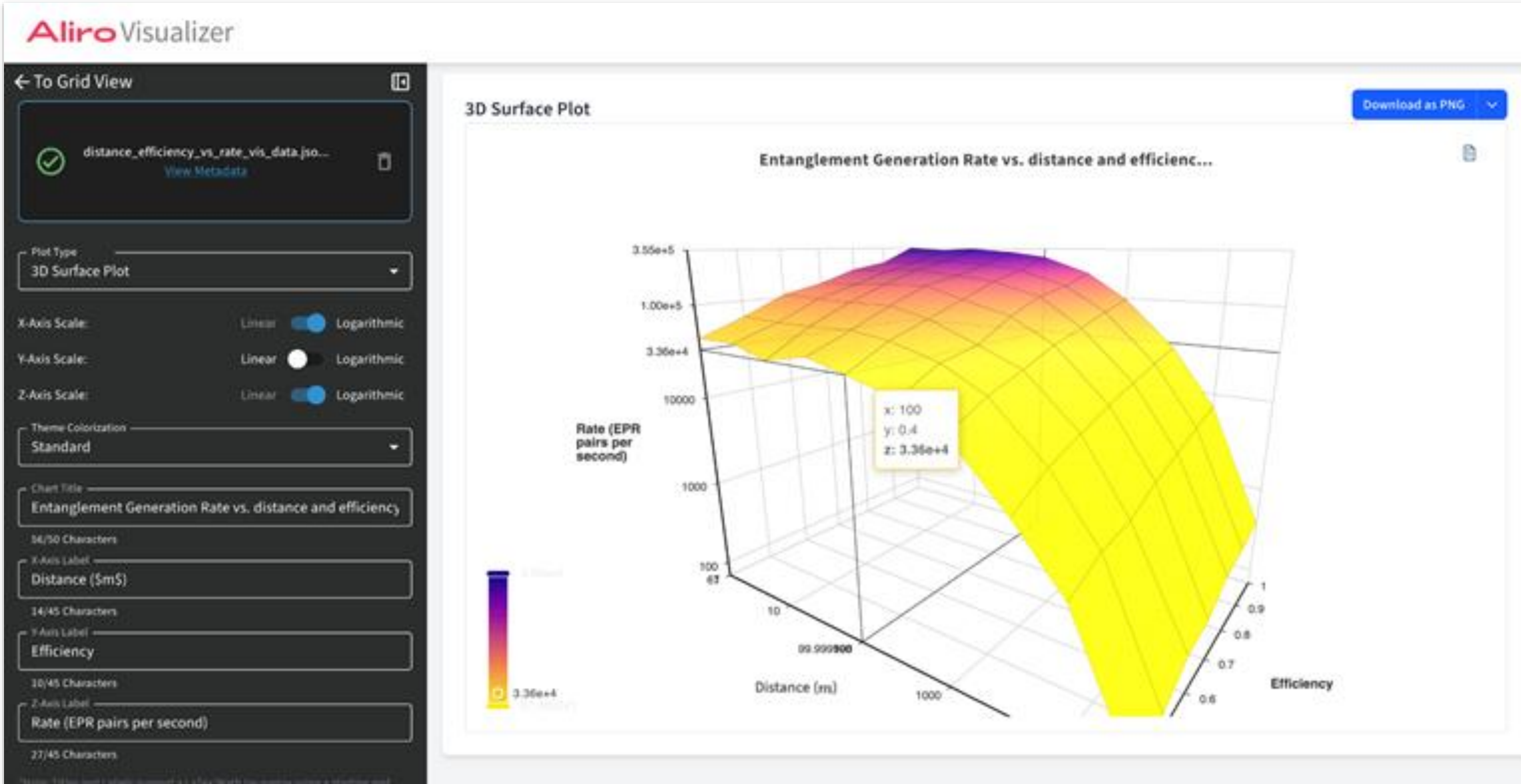
Sample Quantum Network Rack



(US)NUA
US Networking User Association

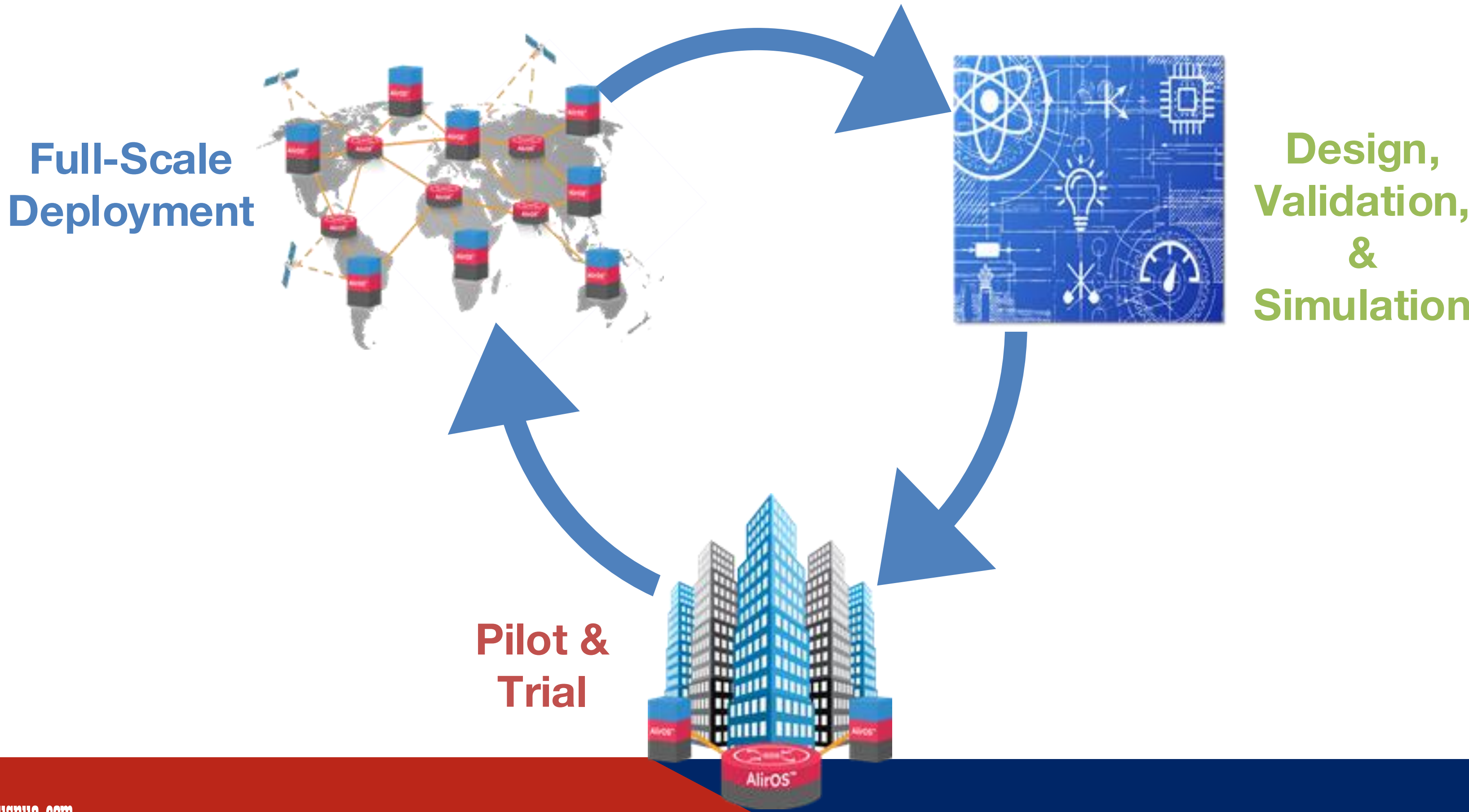
Design, Validate, and **Simulate** Before Buying Any Hardware

Digital Twin for Quantum Networks



Quantum Networks - Continuous Operational Cycle

Design, Deployment, and Ongoing Operational Updates



Current State of the Industry

Quantum networking is transitioning from laboratory research toward deployable infrastructure, with a growing ecosystem of government programs, industry players, and research institutions.

Government Initiatives

National quantum programs in the US, EU, China, UK, and others are funding quantum networking research, testbeds, and standards development at scale.

Telecom Involvement

Major telecommunications carriers are piloting quantum key distribution over existing fiber infrastructure and evaluating quantum networking integration roadmaps.

Cloud Providers

Hyperscale cloud providers are investing in quantum computing and beginning to explore quantum networking as a path to distributed quantum cloud services.

Startups & Research Labs

A vibrant ecosystem of quantum networking startups and university research labs is developing entangled photon sources, quantum memories, repeaters, and orchestration software.

Quantum networking testbeds are now operational in multiple cities worldwide, and early commercial QKD deployments are live in several countries.

Key Takeaways

Quantum networking represents a fundamental shift in how we think about communications, computing, and sensing, with implications that will unfold over the coming years

🔗 Entanglement, Not Just Data

Quantum networks distribute entanglement between nodes, enabling capabilities that are physically impossible on classical networks.

🔒 Security is the Near-Term Driver

Quantum Secure Communications and QKD are the most mature applications, with real deployments happening today.

🌐 Evolves Alongside Classical Networks

Quantum networking will complement and integrate with classical infrastructure, not replace it, for the foreseeable future.

The quantum networking era is here.
The organizations that understand and invest in this technology today will be best positioned for the quantum-enabled future.

Thank you!

Jim Ricotta
COO at Aliro Quantum

jimr@aliroquantum.com

Want to discuss more?