The Pilot-to-Product Gap: Commercialising GCC Quantum Networks

An evidence-gated framework for turning quantum-network demonstrations into governed, contractable and financeable services

Authored by Chennakeshav Adya
Independent Researcher

September 2026

Abstract

Quantum communications in the Gulf have crossed an important threshold. The Technology Innovation Institute and the UAE Space Agency demonstrated a UAE-built quantum-key-distribution system in 2024. In 2025, TII, VentureOne and e& introduced QuantumConnect as a fibre-integrated secure-connectivity offering, while TII and Space42 announced work on a space-to-ground quantum network. These developments establish regional capability and a credible route towards sovereign quantum-secure infrastructure. They also expose a difficult commercial question: what evidence must a pilot produce before a board, customer, investor or lender can treat the underlying capability as a repeatable product?

This paper develops the Quantum Network Commercialisation Framework for telecom operators, technology ventures, infrastructure investors, public agencies and regulated customers across the Gulf Cooperation Council. It separates scientific feasibility, engineered reliability, security assurance, customer acceptance and commercial repeatability. The framework defines a product perimeter across the quantum layer, key management, classical authentication, terrestrial integration, customer encryption systems and managed operations. It then converts that perimeter into measurable evidence gates covering topology, equipment cost, anchor demand, service levels, certification, operating responsibility and milestone valuation.

The central conclusion is that a quantum-network pilot creates enterprise value when it resolves a specific uncertainty that affects adoption, cost, risk or cash flow. A successful link test may establish physical performance. A product requires repeatable installation, documented interfaces, trained operations, auditable key lifecycle, incident procedures, service-level measurement, accepted customer workflows and a supportable commercial contract. The commercialisation plan should therefore fund a sequence of bounded service cells, beginning with one defined corridor and one customer problem, and release capital only after agreed evidence is independently verified.

Four tables and three figures translate this principle into an operating and investment method. A hypothetical regional operator case illustrates the framework. Every case figure is an illustrative management assumption rather than observed company information or a market forecast.

JEL Classification: G31, G32, L51, L96, O31, O32, O33

Keywords: quantum key distribution, GCC quantum networks, quantum-secure communications, commercialisation, service-level agreement, technology financing, anchor demand, milestone valuation

1. DEFINE THE COMMERCIALISATION DECISION

The decision is whether a quantum-network capability should remain a research programme, progress to a bounded customer pilot, become a supported product, or scale into a managed service. Each choice requires a different evidence package, funding instrument and governance model. A board should define the next decision before it authorises the next tranche of capital.

The practical question is narrower than whether quantum communications are scientifically promising. Management must identify the customer problem, route, security outcome, operating boundary and commercial unit. The investment case should state who owns the equipment, who operates the key-management layer, who integrates the customer system, who carries service liability and which party earns each revenue line.

A useful commercialisation decision has a dated gate. It states the minimum evidence required to proceed, the capital exposed before that evidence, and the response if the gate fails. This structure converts technical progress into an auditable investment process.

Table 1. Evidence gates from pilot to repeatable quantum-network service

Stage	Decision question	Required evidence	Suitable valuation lens
Scientific proof	Can the protocol and hardware generate secure key material under defined conditions?	Calibrated experiment, protocol record, raw and final key data, independent technical review	Replacement cost and probability-weighted option value
Engineered field pilot	Can the complete system operate repeatedly on the intended route?	Installation record, repeated sessions, environmental performance, anomaly log and recovery evidence	Milestone-adjusted cost and option value
Accepted customer pilot	Does the service integrate with a real workflow and satisfy agreed acceptance criteria?	Customer test plan, security review, interface evidence, service measurements and signed acceptance	Probability-weighted contracted contribution
Supported product	Can the supplier install, monitor, support and repair a documented configuration?	Product baseline, bill of materials, support model, training, spares, certification plan and price book	Comparable product economics and milestone-adjusted DCF
Repeatable managed service	Can multiple customers receive a governed service with measured performance and renewable revenue?	Standard contracts, recurring operations, service levels, renewal, margin and collected cash	Operating DCF and strategic infrastructure value

Each stage resolves a different commercial uncertainty and should have a named evidence owner.

2. ESTABLISH THE GCC EVIDENCE BASELINE

Regional evidence should be described precisely. In October 2024, TII and the UAE Space Agency announced a partnership to establish quantum-communication infrastructure and demonstrated a UAE-built quantum-key-distribution solution. TII subsequently described proof-of-concept QKD through optical fibre and work on a quantum ground station. These statements support the existence of indigenous capability and an active development programme.

In September 2025, TII, VentureOne and e& announced QuantumConnect. The release described a hardware-based solution integrated with fibre infrastructure and stated that live deployments had occurred with business clients. In November 2025, TII and Space42 announced a framework to develop, test and deploy a space-based QKD solution, including payload development, satellite integration and ground operations. Together, these developments show movement across terrestrial and space segments.

Public announcements do not provide the full evidence required for underwriting. A commercial diligence process still needs route-level performance, customer acceptance, operating cost, contract terms, security scope and collected revenue. The framework in this paper treats public evidence as a starting point and assigns value only to evidence available for verification in the transaction or financing process.

3. SEPARATE A DEMONSTRATION FROM A PRODUCT

A demonstration proves a defined technical proposition under stated conditions. It may use specialist engineers, bespoke equipment, manual intervention and selected operating windows. These features are acceptable when the objective is learning. They become constraints when the objective is repeatable service.

A product needs a controlled configuration. Hardware versions, firmware, interfaces, environmental limits, installation procedures, calibration, monitoring, maintenance and support must be documented. A second team should be able to reproduce the installation and achieve an accepted result without relying on the original inventors for every operating decision.

A service adds continuing obligations. The provider must schedule capacity, manage identity and key lifecycle, monitor availability, respond to incidents, maintain spares, communicate with customers and report against service levels. Commercialisation is therefore an expansion of accountable operating capability, rather than a change in marketing language.

4. DEFINE THE PRODUCT PERIMETER

The perimeter begins with the quantum transmitter and receiver and extends through the optical path, authenticated classical channel, key managers, network controls, customer encryption systems and operating processes. A fibre service may include dark fibre, wavelength allocation, trusted sites and co-location. A free-space or satellite service adds atmospheric conditions, acquisition, pointing, scheduling and ground-terminal operations.

The contract perimeter can differ from the technical perimeter. A telecom operator may own fibre and customer relationships while a specialist supplier provides QKD equipment and key management. A government entity may own sovereign assets while a managed-service provider operates them. A technology venture may license components and retain intellectual property.

The business model should follow enforceable rights and obligations. Revenue belonging to a partner should not appear as revenue of the venture. Equipment controlled by a public agency should not be treated as transferable company property. The product architecture, operating model and financial model should use the same boundary.

5. MAP THE END-TO-END ARCHITECTURE

ITU-T Y.3800 describes QKD networks as layered systems containing quantum, key-management, control, management and service functions. The user network remains a distinct domain that consumes keys through defined interfaces. This architecture is useful because it prevents a successful quantum link from being treated as proof of the complete customer service.

The commercial architecture should show every location where key material is generated, stored, relayed, transformed, supplied or destroyed. It should identify trusted nodes, administrators, maintenance access, monitoring paths and dependencies on classical cryptography. Customer applications and encryption devices should appear explicitly.

Each boundary needs an owner and an acceptance test. Ambiguous ownership creates operational gaps and liability disputes. A product diagram should therefore serve engineering, security, contracting and financial diligence at the same time.

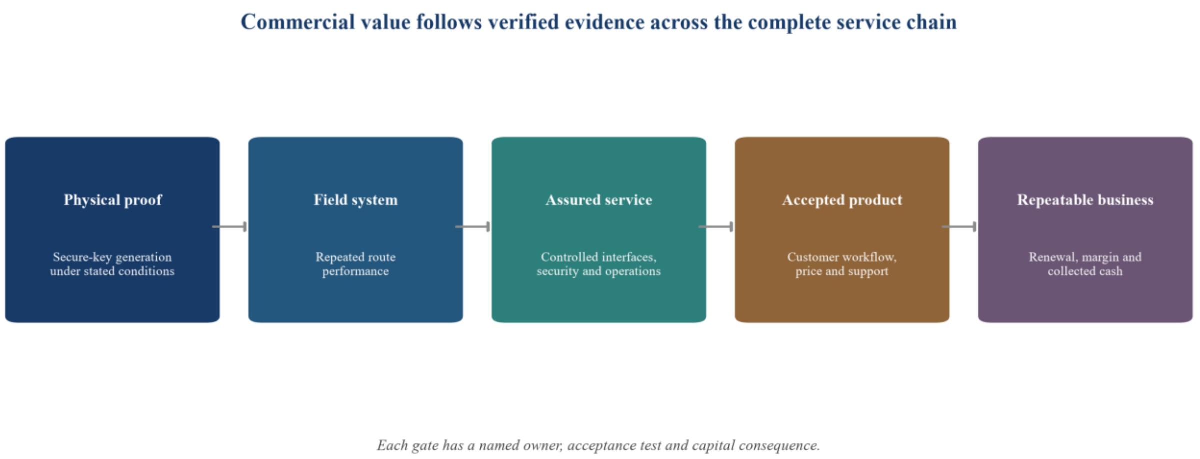

Figure 1. The evidence path from quantum-network pilot to commercial service

Value increases as the programme resolves technical, operating, security and customer uncertainties.

6. USE STANDARDS AS PRODUCT REQUIREMENTS

The ITU-T Y.3800 series covers network concepts, requirements, functional architecture, key management, control and management. ITU-T Y.3828 adds quality-of-service requirements for integrated QKD and user networks. ITU-T Y.3823, approved in April 2026, addresses allocation of end-to-end quantitative quality objectives across links, equipment and providers.

ETSI specifications cover interfaces, implementation security, software-defined networking and evaluation. ETSI GS QKD 016 provides a Common Criteria protection profile for a pair of prepare-and-measure QKD modules. Its scope includes secure states, access control, audit, key destruction, physical protection and authenticated classical channels.

Standards give the product team a requirements map. They do not establish that a particular implementation conforms or that a customer accepts it. The data room should state applicable standards, claimed conformance, exclusions, test evidence and the planned route to certification or accreditation.

7. SELECT A CUSTOMER PROBLEM WITH DURABLE VALUE

The first product should solve a specific problem for a customer whose information has long confidentiality life, high consequence of disclosure or strong sovereignty requirements. Finance, government, healthcare, defence, energy and critical infrastructure appear in ITU use-case material because these sectors can have such requirements. Sector membership alone does not prove willingness to pay.

Management should document the protected workflow, current cryptographic architecture, data lifetime, route, threat model, compliance obligations, budget owner and procurement process. It should explain why the proposed service is proportionate to the risk and how it complements post-quantum cryptography.

The customer problem determines the service design. A bank connecting two data centres may value scheduled key refresh, integration with existing encryptors and auditable operations. A sovereign customer may require local control of key material and restricted maintenance access. A satellite use case may value reach to remote locations. These are different products with different economics.

8. CHOOSE ONE ANCHOR CORRIDOR

A bounded corridor creates a practical unit of learning. It identifies two or more sites, fibre or free-space path, customer systems, interfaces and operating conditions. The team can measure installation time, key output, availability, incident response and customer effort against that defined route.

The corridor should combine strategic demand with engineering feasibility. Existing fibre access, secure facilities, data centres and operational support can reduce delivery risk. A route selected only for technical convenience may produce weak commercial evidence. A route selected only for a prestigious customer may create excessive bespoke cost.

The first corridor should establish reusable methods. Documentation, interfaces, security controls and monitoring should support later customers. Management should track which work is platform investment and which work is customer-specific implementation.

9. POSITION QKD WITHIN A QUANTUM-SAFE ARCHITECTURE

NIST published FIPS 203, FIPS 204 and FIPS 205 in August 2024 and encourages organisations to begin migration to post-quantum cryptography. These standards provide key-establishment and digital-signature mechanisms designed to resist future quantum attacks. QKD addresses secure key distribution across supported physical links.

A commercial product should explain the role of each control. Post-quantum cryptography can protect applications, authentication and systems that are outside the QKD footprint. QKD can add an independently rooted key-distribution mechanism for selected high-value routes. Hybrid designs may reduce dependence on a single mechanism when governance and implementation are sound.

The investment case should include the customer's broader cryptographic migration. A service sold as a complete replacement for post-quantum migration would create an inaccurate risk claim. A service integrated into an explicit defence-in-depth architecture has a clearer customer outcome and a more credible procurement case.

10. DEFINE ACCEPTANCE BEFORE BUILDING

The pilot agreement should define success before installation. Acceptance criteria may include route availability, final secure-key rate, quantum-bit-error-rate bounds, key-delivery latency, interface performance, failover, monitoring, audit evidence, incident handling and customer workflow completion. Every metric needs a measurement method and observation period.

The criteria should reflect the intended product. A scheduled service can have defined operating windows. An always-available managed service requires stronger redundancy and recovery. A research test can accept manual intervention that a production service cannot.

Acceptance should be signed by technical, security and business owners. The customer should record whether the system is accepted for a limited pilot, production use or a further test phase. Clear acceptance prevents technical success from being mistaken for commercial completion.

Table 2. Product metrics for a commercial quantum-network service

Metric family	Example measure	Evidence source	Commercial consequence
Physical link	Final secure-key output by route and operating window	Device logs, calibrated measurement and independent review	Capacity and equipment design
Availability	Eligible service time completed successfully	Scheduler, environmental data and incident record	Service-level commitment and redundancy cost
Key management	Authorised requests fulfilled, latency, storage and deletion controls	Key-manager logs, audit evidence and access review	Customer assurance and integration acceptance
Operations	Detection, response, restoration and change-control performance	Ticketing, monitoring, runbooks and exercises	Staffing, support price and liability
Customer workflow	Encryption sessions completed and accepted	Customer test record and signed acceptance	Revenue recognition and referenceability
Commercial performance	Contracted value, collected cash, renewal and contribution margin	Executed contracts, invoices and management accounts	Enterprise value and scale decision

Thresholds should be route-specific and agreed before the observation period.

11. MEASURE FINAL SECURE KEY

Raw detections, sifted key and final secure key are different measures. Error correction, privacy amplification, authentication and protocol overhead reduce the amount available to the application. Commercial capacity should therefore use final secure key delivered at the accepted interface.

Performance varies with fibre loss, detector characteristics, equipment stability and configuration. Free-space systems add atmospheric and pointing effects. The data room should preserve pass-level or session-level observations, calibration, software versions and excluded results.

An investor should reconcile modelled and observed output. Persistent unexplained variance can change equipment count, route reach, capacity and unit cost. Management should avoid pricing a service on the best demonstration result when routine operations produce a lower output.

12. TREAT ENVIRONMENTAL PERFORMANCE AS PRODUCT EVIDENCE

Gulf operating conditions can affect equipment housing, cooling, dust management, fibre access, optical alignment and outdoor maintenance. A product intended for the region should be qualified for the actual deployment environment. Laboratory conditions are inadequate evidence for field reliability.

The qualification plan should identify temperature, humidity, dust, vibration, power quality and physical-security requirements. Free-space terminals should also measure visibility, turbulence, background light and weather. Field results should feed maintenance intervals and spares planning.

Regional optimisation can become valuable intellectual property when it is documented and repeatable. It may sit in enclosure design, calibration, control software, installation practice or operating analytics. The company should distinguish proprietary improvements from ordinary project adaptation.

13. CONVERT PERFORMANCE INTO A SERVICE LEVEL

A service-level agreement should connect business intent to measurable network behaviour. ITU-T Y.3828 describes service-driven and SLA-based quality planning, monitoring, provisioning, optimisation and protection or recovery. It includes concepts such as availability, reliability, routing, restoration and resource utilisation.

The provider should define service windows, exclusions, maintenance, measurement points, reporting frequency and remedies. A scheduled key-delivery service can be commercially useful if its timing is explicit. A customer requiring continuous protection may need diversified routes, local key buffers or an agreed cryptographic fallback.

The service level should be priced from the resources required to deliver it. Higher availability may require duplicate equipment, alternate fibre, additional sites, larger key reserves and round-the-clock support. The contract should avoid promising performance that the operating model and capital plan cannot support.

14. PRODUCTISE KEY MANAGEMENT

Key management turns quantum output into usable customer control. ITU-T Y.3803 describes storing keys, relaying keys and supplying keys to cryptographic applications. The commercial product must also manage identity, authorisation, audit, retention, deletion, resilience and exception handling.

The provider should demonstrate the path from a customer request to key delivery, use and destruction. Role separation, privileged access, backup, synchronisation and incident response should be tested. The interface should preserve customer policy and prevent unauthorised export.

Reusable key-management software can support multiple devices, routes and applications. Its value depends on documented interfaces, secure development, accepted deployments, upgradeability and support. A bespoke integration maintained by one engineer has limited scale value.

15. PROVE INTEROPERABILITY

Interoperability affects procurement, resilience and exit value. A customer may want to combine equipment from different vendors, integrate with existing encryptors or change network components over time. Proprietary interfaces can accelerate early development and create future switching cost.

The pilot should test the interfaces expected in the commercial configuration. These include key delivery, network control, telemetry, authentication, service orchestration and customer encryption. Where a standard exists, the test should record the relevant version and any deviation.

Interoperability evidence should be specific. A successful laboratory connection between two components does not establish field support for every configuration. The product baseline should list supported combinations, responsibilities, regression tests and upgrade policy.

16. ESTABLISH SECURITY EVALUATION

QKD security depends on protocol assumptions and implementation behaviour. Sources, detectors, control electronics, interfaces and physical access can introduce vulnerabilities. ETSI GS QKD 016 provides a structured protection profile for QKD modules, including secure-state behaviour, audit, role-based access, physical protection and key destruction.

The programme should define the required assurance for each customer group. Product evaluation, network accreditation and customer acceptance are separate activities. Certification scope, laboratory availability, evidence ownership and remediation time should be included in the roadmap and cost baseline.

Security findings require governance. The supplier should maintain vulnerability intake, patching, configuration control, secure updates and customer notification. A strong theoretical protocol cannot compensate for weak operational security around the device.

17. BUILD AN ACCOUNTABLE OPERATING MODEL

The operating model should identify who monitors the quantum layer, key managers, classical channel, fibre, customer interface and supporting infrastructure. It should define first-line response, escalation, maintenance access, change approval and customer communication.

Specialist engineering may remain necessary during early deployment. The product plan should reduce single-person dependency through runbooks, training, remote diagnostics and structured handover. Every recurrent manual action should be measured for time, skill and error risk.

Operations evidence should include exercises and failures. Restoration performance, spares use and repeated fault patterns are more informative than a successful launch event. The service price should recover the complete operating burden.

18. ALIGN REGULATION, ASSURANCE AND PROCUREMENT

Quantum-network deployment can touch telecommunications licensing, cryptographic controls, cybersecurity, data protection, critical-infrastructure rules and public procurement. Requirements differ by jurisdiction and customer. The product team should maintain a regulatory matrix tied to the actual service and route.

The matrix should identify permissions, responsible entities, evidence and lead times. Cross-border routes require particular attention to network ownership, data handling, key control and government approvals. A technology claim cannot resolve a legal or procurement requirement.

The commercial schedule should include regulatory and assurance gates. Revenue should not be recognised in a forecast before required approvals, customer accreditation and budget authority are realistically sequenced.

19. PRESERVE SOVEREIGNTY WITHOUT CREATING ISOLATION

Sovereign control can influence equipment location, key custody, software access, maintenance and data residency. It can support adoption by government and regulated customers. It can also create cost when every component must be unique to one customer or jurisdiction.

The architecture should identify which elements require sovereign ownership or control and which elements can remain standard. Local operation, controlled source-code access, trusted maintenance and domestic spare holdings may provide assurance without rebuilding the complete product.

A modular design can preserve local control while supporting repeatable delivery. The supplier should document jurisdictional variants, common components and restricted features. Investors should value transferable platform capability separately from customer-specific sovereign assets.

20. CHOOSE A BILLABLE SERVICE UNIT

A clear commercial unit links customer value, capacity and cost. Possible units include a protected route, managed endpoint pair, reserved key capacity, scheduled secure session, wavelength service or integrated encryption service. The chosen unit should be measurable and appear consistently in engineering, contracts and financial reporting.

The unit should reflect the scarce resource. A fibre route may be constrained by equipment pairs, loss and operational support. A shared network may be constrained by key-generation capacity, scheduling or trusted-node policy. A satellite service may be constrained by passes and weather.

Management should avoid charging for a technical metric customers do not use. Key rate remains important for capacity planning, while the customer may buy an assured protected connection. The price book should state included installation, support, monitoring and reporting.

21. BUILD A DISCIPLINED PRICING MODEL

Pricing should recover equipment, installation, integration, operations, spares, certification, customer support and capital. A one-time installation fee can recover route-specific work. Recurring charges can cover managed service, monitoring, maintenance and reserved capacity.

Early customers may receive pilot pricing in exchange for access, feedback and reference rights. The agreement should state the future production price or a conversion method. A heavily subsidised pilot without a conversion mechanism gives weak evidence of willingness to pay.

The supplier should compare customer value with complete cost. Avoided risk is difficult to monetise directly, so procurement often depends on compliance, sovereignty, contractual requirements or the cost of an alternative architecture. Pricing should use evidence from the customer's decision process.

22. CONTRACT THE PILOT AS A LEARNING ASSET

The pilot contract should define scope, responsibilities, equipment ownership, data access, test plan, acceptance, security, intellectual property, publication, liability and termination. It should give the supplier access to operating evidence while protecting customer information.

Milestone payments can align capital with evidence. A contract may pay for design approval, installation, successful commissioning, observation-period completion and final acceptance. Retention can remain until documentation and handover are complete.

The pilot should have a conversion path. The agreement can include an option, reserved capacity, production order or price schedule triggered by acceptance. This structure improves the evidence available to investors and prevents a completed pilot from ending without a commercial decision.

23. DESIGN CUSTOMER ACCEPTANCE

Acceptance should cover technical performance, security controls, operational readiness and the customer workflow. A customer may need to approve integration with encryptors, identity systems, monitoring, incident management and change control. The test should use the intended production configuration.

The observation period should be long enough to reveal stability and support requirements. Scheduled maintenance and agreed exclusions should be transparent. Every failure should be classified, corrected and included in the final report.

Signed acceptance should state the authorised use. Limited acceptance for a pilot is different from production accreditation. The financial model should recognise revenue and milestone value according to the actual acceptance status.

24. CONVERT ANCHOR DEMAND INTO FINANCING EVIDENCE

A named customer with a funded requirement can reduce commercial uncertainty. The strength of evidence depends on the commitment. General interest, a memorandum, a paid pilot, a conditional production order and a multi-year service contract have different value.

Anchor commitments should specify route, configuration, acceptance, start date, price and termination. Public-sector demand may support shared infrastructure through milestone procurement or availability payments. Telecom partners may aggregate demand across customers.

The financing model should weight demand by enforceability and remaining conditions. Pipeline should remain separate from contracted backlog. Collected cash provides the clearest evidence that the customer values the service.

25. BUILD A PRODUCT ROADMAP FROM EVIDENCE

The roadmap should sequence reusable capability. The first release may support one fibre configuration and one customer encryption interface. Later releases can add network orchestration, multiple vendors, additional distances, free-space links or satellite integration.

Each release should have entry and exit criteria. Engineering work should resolve a named product constraint. Features should be added when supported by customer demand and operational capacity.

The roadmap should preserve compatibility where practical. Customers in regulated sectors may require long support periods and controlled changes. The cost of maintaining old versions should appear in pricing and valuation.

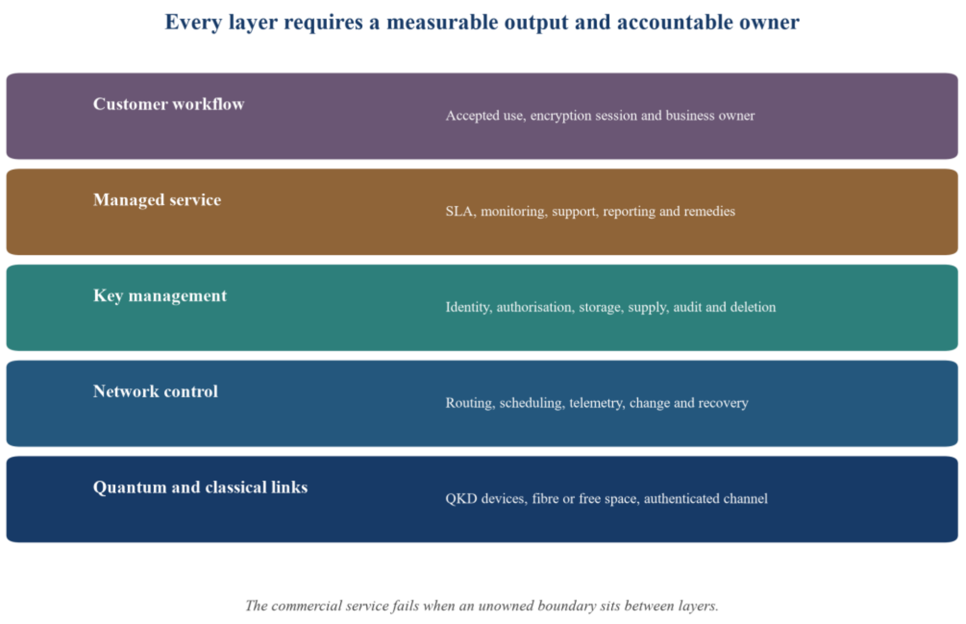

Figure 2. Commercial quantum-network service stack and evidence ownership

The product team should assign an owner and acceptance record to every layer.

26. CONTROL MANUFACTURING AND SUPPLY

Commercial delivery needs a stable bill of materials, qualified suppliers and configuration control. Lasers, detectors, optical components, timing systems, secure processors and specialist packaging can have long lead times or export constraints.

The supplier should identify single-source items, substitutes, yield, calibration time, warranty and field-replacement procedure. Inventory policy should reflect customer criticality and replenishment time. The cost model should include test equipment and acceptance labour.

Manufacturing evidence affects valuation. A working prototype built from scarce components has scientific value. A controlled product with repeatable yield, supply commitments and supportable margin has stronger commercial value.

27. BUILD REGIONAL OPERATING CAPABILITY

Quantum networks require skills across optics, communications, cryptography, software, network operations and cybersecurity. The staffing plan should distinguish scarce specialist roles from operational roles that can be trained and scaled.

Partnerships with universities and research institutes can support talent and testing. Commercial operations still need clear employment, security clearance, knowledge transfer and succession. Contractors should be governed through access control and documentation.

The model should include hiring time, training, retention and on-call coverage. A product dependent on continuous intervention by a small research team has a capacity ceiling and concentration risk.

28. PROTECT AND LICENSE INTELLECTUAL PROPERTY

The intellectual-property map should identify patents, software, designs, know-how, data and third-party rights. Public funding, research collaboration and supplier agreements may create ownership, licensing or publication obligations.

The company should preserve invention records, assignments, source-code control and licence compliance. Customer contracts should distinguish background intellectual property from customer-specific deliverables and improvements.

Intellectual property creates value when it supports defensible performance, lower cost, faster deployment or customer access. Broad claims without enforceable ownership or implementation evidence should receive limited valuation weight.

29. MEASURE REVENUE QUALITY

Revenue quality depends on contract duration, acceptance, renewal, concentration, payment terms, support burden and cancellation rights. Equipment sales can provide early cash while creating volatile revenue. Managed services can provide recurring revenue while requiring continuing capital and operations.

Management should report contracted annual value, billed revenue, collected cash, deferred revenue, renewal and contribution margin by customer and route. Pilot revenue should remain separate from production service revenue.

Concentration may be acceptable during commercialisation when the anchor customer funds reusable capability. The risk should be visible. The scale plan should show how the product becomes attractive to additional customers without repeating the complete development cost.

30. BUILD THE COMPLETE COST BASELINE

The baseline should include product engineering, equipment, fibre or site access, installation, key management, customer integration, security evaluation, operations, support, spares, insurance, sales and programme management. Partner and grant contributions should be recorded with their economic conditions.

Costs should be assigned to product platform, route infrastructure and customer implementation. This distinction supports pricing and valuation. Platform cost can benefit future customers, while route and customer cost should be recovered through the relevant contract.

Contingency should relate to unresolved risks. A generic percentage can conceal uncertainty. The model should identify the cost consequence of interface redesign, certification delay, component replacement, route change and additional support.

31. MATCH FINANCING TO THE ASSET AND EVIDENCE

Corporate equity is appropriate for early intellectual property, integration and commercial risk. Grants and public programmes can fund research and sovereign capability. Customer prepayments can support route-specific installation. Vendor finance or leasing may suit standard equipment with clear ownership and useful life.

Debt becomes more credible when assets, contracts and cash flows are defined. A lender will examine acceptance, cancellation, residual value, maintenance, insurance and step-in rights. Revenue dependent on future certification or discretionary renewal provides weak debt support.

The financing plan can combine instruments by tranche. Platform equity may fund core product development, while customer-backed facilities fund accepted deployments. The model should prevent short-term debt from funding open-ended research risk.

32. RELEASE CAPITAL AGAINST EVIDENCE

Capital should be released when the programme resolves the uncertainty attached to the previous tranche. The first tranche may complete design, route survey and acceptance plan. The next may procure equipment and install the corridor. Later tranches may fund observation, certification, production conversion and replication.

Each tranche should have a maximum exposure, evidence owner, decision date and downside action. A failed gate may lead to redesign, narrower scope, partner change or termination. Sunk cost should not determine the next decision.

Milestone governance also improves external financing. Investors can see how technical evidence connects to commercial value and how management limits loss. Customers can align payments to accepted outcomes.

Table 3. Illustrative milestone capital-release structure

Tranche	Use of capital	Release evidence	Value created
Design	Route engineering, architecture, customer requirements and test plan	Approved baseline, measured route, signed pilot scope and acceptance criteria	Bounded product and customer problem
Build	Equipment, integration, installation and commissioning	Qualified configuration, installed route and controlled commissioning results	Field-system capability
Assure	Observation period, security evaluation, operations and documentation	Repeated performance, closed anomalies, audit evidence and trained support	Assured service capability
Convert	Production configuration, contract conversion and billing	Signed acceptance, production order, collected cash and support start	Contracted commercial value
Replicate	Additional routes, inventory, automation and sales	Reusable installation record, measured margin and qualified pipeline	Repeatable platform value

Amounts and timing are programme-specific; this table defines the evidence logic rather than market pricing.

33. USE A MILESTONE VALUATION FRAMEWORK

Early valuation should separate replacement-cost evidence, intellectual-property option value, remaining cost and milestone probability. Historical spend is an input, rather than a valuation floor. Work that cannot be reused or transferred may have limited value.

After an accepted pilot, the model can add probability-weighted contracted contribution. A supported product with repeat installations can support unit-economics and comparable-company analysis. A managed service with renewals and stable margins can support a discounted cash-flow approach.

The valuation bridge should show what changed between rounds. An increase should be tied to resolved uncertainty, enforceable customer value or reusable capability. General market enthusiasm should remain separate from the evidence-based base case.

34. APPLY THE FRAMEWORK TO A HYPOTHETICAL OPERATOR

Consider a hypothetical Gulf-based venture developing a fibre QKD service between two secure data-centre locations. It owns key-management software and regional integration know-how, procures QKD modules from qualified suppliers and partners with a telecom operator for fibre access. A regulated customer has signed a paid pilot with defined technical and security acceptance.

Management estimates a total programme cost of USD 8.4 million to reach the first supported product. This includes USD 2.1 million for platform engineering and key management, USD 2.4 million for two route configurations and spares, USD 1.3 million for security evaluation and customer integration, USD 1.5 million for operations and support readiness, and USD 1.1 million of contingency. These amounts are hypothetical.

The pilot contract pays USD 0.9 million across design, commissioning and acceptance. A production conversion would provide a hypothetical USD 1.2 million installation payment and USD 0.78 million annual managed-service fee for three years. Management assumes no value for unsigned customers in the base case.

35. MODEL COMMERCIAL SCENARIOS

The downside case assumes the field system works but customer security acceptance requires redesign. Production conversion is delayed by twelve months, cost rises by USD 1.6 million and the pilot remains the only paid deployment. The programme retains intellectual property and equipment but has limited recurring value.

The base case assumes acceptance after a nine-month observation and conversion of the anchor route. Two additional customers adopt the supported product over the following twenty-four months. Management estimates a steady-state contribution margin of 42 percent after field support and spares. The upside case assumes a telecom-channel agreement and five total routes, with further automation reducing installation time.

These scenarios are management illustrations. The valuation should apply probability to each outcome, deduct remaining funding and include downside obligations. Probabilities should be approved by an investment committee and updated when evidence changes.

Table 4. Hypothetical commercialisation scenarios

Scenario	Accepted production routes after three years	Incremental cost to reach scale	Annual recurring service revenue	Valuation interpretation
Downside	0	USD 1.6m above plan	USD 0	Recoverable equipment, intellectual property and development option
Base	3	Within USD 8.4m plan	USD 2.34m	Contracted contribution plus probability-weighted replication value
Upside	5	USD 2.2m replication capital	USD 3.90m	Operating platform value subject to renewal, margin and concentration

Every figure is an illustrative management assumption and should not be treated as observed market data.

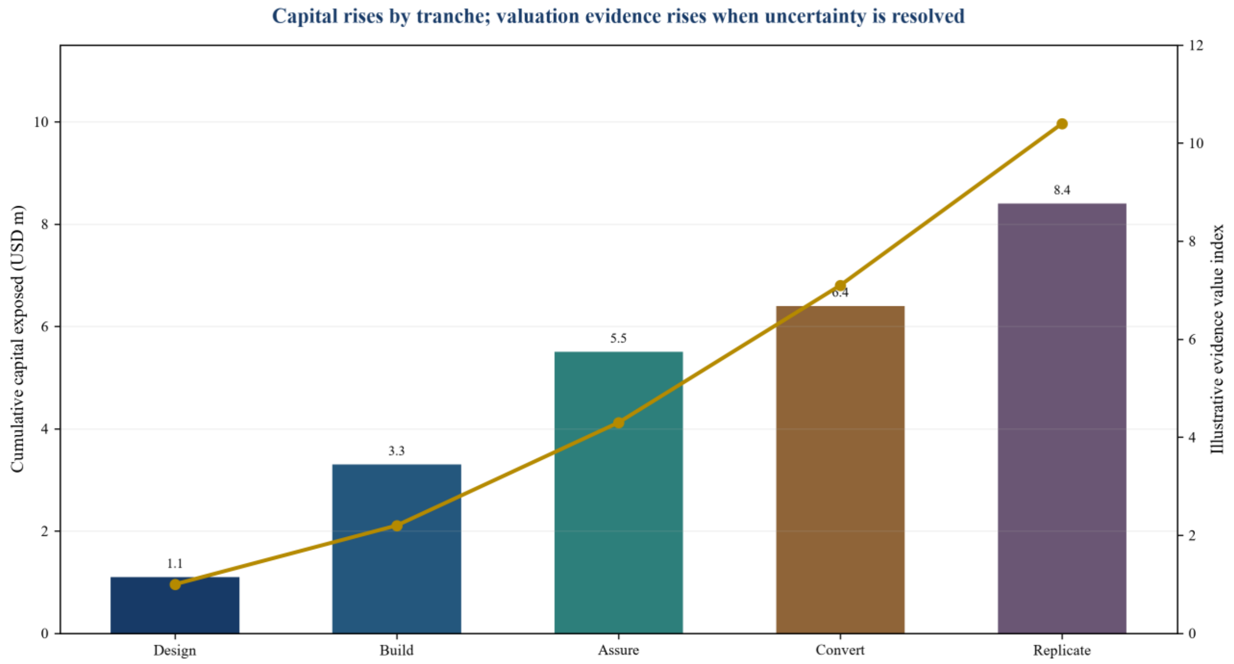

Figure 3. Hypothetical capital exposure and valuation evidence by gate

Values are illustrative management assumptions and do not represent observed market prices.

36. STRESS-TEST THE PLAN

The model should test certification delay, lower key output, equipment replacement, fibre-route change, customer cancellation, higher support cost and slower replication. Each sensitivity should have an operational explanation and a management response.

The largest risk may change by stage. Before installation, supply and route access can dominate. During observation, reliability and acceptance can dominate. After launch, renewal, support burden and customer concentration can determine value.

A reverse stress test should identify the conditions under which the programme loses its funding case. The board can then set early-warning indicators and avoid incremental spending after the commercial thesis has failed.

37. ESTABLISH GOVERNANCE AND REPORTING

The steering group should include product, engineering, security, operations, finance, legal and customer ownership. It should approve the product baseline, exceptions, evidence, capital release and contract conversion.

Monthly reporting should reconcile technical performance, open anomalies, security findings, customer acceptance, schedule, cost, cash and commercial commitments. Measures should use stable definitions and preserve source evidence.

An independent review function should challenge security claims, milestone completion and valuation assumptions. Governance should preserve a clear distinction between management estimates, customer evidence and observed operating results.

38. BUILD THE DILIGENCE DATA ROOM

The data room should contain architecture, requirements, route surveys, bill of materials, supplier commitments, source-code ownership, test plans, calibrated results, anomaly logs, security assessments, certification records, operations manuals, customer contracts, acceptance and financial models.

Documents should be versioned and tied to the product baseline. Technical results should preserve raw evidence and methodology. Contract and financial schedules should reconcile to management accounts and bank evidence where applicable.

A buyer or financier should be able to trace each valuation claim to a source. Missing evidence should remain an open item. The data room becomes a commercial asset when it shortens customer, investor and lender diligence without weakening security controls.

39. CONCLUDE WITH A BOUNDED SCALE DECISION

The Gulf has credible quantum-communications capability, early product activity and an expanding sovereign-infrastructure agenda. The next value-creation task is disciplined conversion from impressive demonstrations to accepted services. This requires an explicit product perimeter, measurable service levels, security assurance, accountable operations and anchor demand.

The recommended sequence is one corridor, one defined customer workflow and one complete evidence pack. Capital should be released after design, field performance, assurance, customer acceptance and production conversion are verified. Replication should begin after complete cost and contribution margin are measured.

The pilot-to-product gap can be managed as an investment process. Technical evidence defines what works. Customer acceptance defines what is usable. Contracts and collected cash define what has commercial value. A programme that keeps those distinctions visible can build a financeable quantum-network business while protecting scientific integrity and public trust.

REFERENCES

ABOUT THE AUTHOR

Chennakeshav (CK) is a corporate finance and investment banking executive with 25+ years of global experience in deal origination, structuring and execution across M&A, growth capital and corporate strategy. He has led value-creation mandates for founders, corporates and funds — bridging the boardroom view to hands-on execution and close.

His career spans Morgan Stanley, HSBC, Lloyds Banking Group, EWEC, ADQ portfolio companies and Emirates Growth Fund, across TMT, real estate, fintech, deeptech, cleantech, infrastructure and energy. He has partnered with C-suite leaders, private equity and venture funds, sovereign wealth funds and family offices to finance complex fund raises and scale-up ventures, and has led M&A due diligence, post-merger integration and business-transformation initiatives to create value.

At Matchpoint Partners he is Managing Partner, leading the firm's corporate finance, M&A and capital-raising practice. He holds an MBA from London Business School, an engineering degree from VTU and a Master of Laws (LLM, in progress) from UCL London.

An active start-up mentor, CK mentors at Techstars, DIFC FinTech Hive, Startup Grind, Founder Institute and IN5, serves as Entrepreneur Mentor in Residence (EMiR) at London Business School, and judges the Entrepreneurship World Cup.

https://www.linkedin.com/in/ckadya/

https://www.matchpoint-partners.com/team/ck-adya.html

Disclaimer. This paper is part of a continuing series on the structure of private and alternative markets. The views expressed are the author's own. The paper is for information only, describes market structure in general terms, and does not constitute investment, legal, tax or regulatory advice or a recommendation in respect of any security, vehicle or counterparty.