From Space to Ground: Valuing Satellite Quantum-Communications Scenarios

A milestone-based valuation framework for satellites, optical ground stations and integrated quantum-secure services

Authored by Chennakeshav Adya
Independent Researcher
September 2026

Abstract

Satellite quantum communications have moved from isolated physical demonstrations towards integrated networks, smaller spacecraft, portable ground terminals and planned public infrastructure. The Micius programme demonstrated satellite-to-ground quantum key distribution over distances of up to 1,200 kilometres and later integrated more than 700 terrestrial fibre links with two satellite links across a 4,600-kilometre network. A 2025 microsatellite experiment reported real-time quantum key distribution with compact ground stations and an intercontinental demonstration between China and South Africa. Europe is developing the EuroQCI terrestrial and space segments, while ESA's Eagle-1 programme is intended to validate an end-to-end satellite quantum-key-distribution system. These developments establish technical possibility. They do not, by themselves, establish commercial availability, service-level performance, financeability or enterprise value.

This paper develops the Space-to-Ground Quantum Valuation Framework for boards, investors, lenders, governments, satellite operators, telecom companies and strategic customers. The framework values a programme through four linked systems: the spacecraft and payload; the optical ground-station network; key management and terrestrial integration; and the contracted service layer. It treats orbit, link budget, cloud cover, atmospheric loss, acquisition and pointing, pass geometry, terminal mobility, security certification, trusted-node design and customer workflow as drivers of usable service rather than engineering footnotes. Four tables and three figures translate those drivers into an investment perimeter, an availability model, a milestone-based valuation bridge and a capital-release plan.

The central proposition is that enterprise value should follow verified service capacity and commercial evidence. A payload demonstration creates scientific and engineering evidence. A network demonstration adds operational evidence. A service demonstration adds security, workflow and customer evidence. Recurring value emerges only after the operator can show repeatable key delivery across named routes, measured availability, accepted interfaces, bounded trust assumptions, accountable operations and contracted demand. Weather diversity, portable terminals and multi-orbit or multi-satellite architectures can improve availability, but they also add capital, coordination and operating cost. The appropriate valuation method therefore separates technology option value, replacement-cost evidence, milestone probability, contracted contribution and residual infrastructure value.

A wholly hypothetical operator case demonstrates the method. Every amount, terminal count, pass assumption, availability figure, customer characteristic, financing term and valuation outcome in that case is an illustrative management assumption. The case is neither observed company data nor a market forecast. It shows how capital can be released against evidence and how a valuation can *move from a probability-weighted development option to an operating-infrastructure and service business. The conclusion is that satellite quantum communications become investable when management can reconcile the physics of each route with the economics of each accepted service.*

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

Keywords: satellite quantum communications, quantum key distribution, optical ground stations, weather diversity, milestone valuation, technology financing, anchor demand, space infrastructure

1. DEFINE THE INVESTMENT DECISION

The investment decision is whether to fund, acquire, partner with or contract a satellite quantum-communications platform at its current level of maturity. A board needs to know which part of the system is being valued, what security service it will deliver, where it can operate, how often it can operate and which customers will pay for an accepted outcome. A description of a quantum payload or a record distance does not answer those questions.

The decision should identify the relevant perimeter. It may include a dedicated satellite, hosted payload, optical terminal, ground-station network, key-management layer, terrestrial fibre integration, secure application and operating organisation. Ownership can be divided across public agencies, satellite operators, telecom carriers, vendors and users. Valuation must follow the rights, obligations and cash flows attached to the actual entity.

The board should state the next value-inflecting decision. Examples include funding a payload qualification campaign, contracting launch, building a second ground station, accepting a customer pilot or scaling a regional service. Each decision needs a defined evidence package and downside response.

Table 1. The satellite quantum-communications investment perimeter

System layer	Primary valuation question	Evidence required	Principal value driver
Space segment	Can the payload generate and transmit the required quantum states through the intended orbit and mission life?	Qualification, pointing performance, link tests, radiation and thermal evidence, launch and operations plan	Accepted payload capability, mission life and replacement cost
Ground segment	Can terminals acquire the spacecraft and produce usable sessions under local weather and operating conditions?	Site data, optical design, pass results, cloud history, maintenance and staffing	Route availability, terminal utilisation and network diversity
Network and key management	Can raw link output become controlled, auditable keys inside customer systems?	Interfaces, key-management controls, authentication, monitoring, certification and incident processes	End-to-end security acceptance and integration repeatability
Service layer	Will customers contract for a defined service with accepted performance and liability terms?	Paid pilots, contracts, service levels, route commitments, renewal and collected cash	Recurring contribution, retention and strategic scarcity
Programme and ecosystem	Can suppliers, regulators and operating partners deliver the whole system on compatible dates?	Dependency register, licences, spectrum or optical approvals, procurement, launch and partner commitments	Completion probability, timing and cost to complete

Each layer requires a named owner, accepted interface, measurable output and funding source.

2. SEPARATE SCIENTIFIC PROOF FROM COMMERCIAL SERVICE

Satellite quantum communication has a strong body of experimental evidence. The 2017 Micius satellite-to-ground experiment demonstrated decoy-state quantum key distribution at kilohertz key rates over distances up to 1,200 kilometres. Later work integrated satellite and terrestrial links over 4,600 kilometres. The 2025 microsatellite work addressed smaller spacecraft, portable terminals and real-time key exchange. These results are material technical evidence.

Commercial service requires a wider evidence set. A customer needs keys at usable times, locations and assurance levels. The operator needs repeatable acquisition, stable operations, key-management integration, support, incident response and liability allocation. Weather, orbit and customer scheduling can reduce service availability even when the underlying experiment succeeds.

Valuation should therefore use an evidence ladder. Scientific publication supports feasibility. Mission qualification supports engineering readiness. Repeated route performance supports operational readiness. Accepted customer integration supports service readiness. Contracted and collected revenue supports commercial value. The discount applied at each stage should reflect what remains unproven.

3. UNDERSTAND THE SYSTEM ARCHITECTURE

A satellite QKD service is an end-to-end system. The space segment carries a quantum transmitter, receiver or entangled-photon source, together with pointing, acquisition, tracking, timing, control and classical communications. The ground segment includes telescopes, detectors, timing, atmospheric monitoring, secure facilities and operations. Classical channels authenticate and coordinate the protocol.

The network layer receives, stores, routes and supplies keys to encryption or application systems. It must manage identity, authorisation, availability, audit and lifecycle. Terrestrial QKD or conventional secure links may connect ground stations to customers. Trust assumptions differ by architecture, especially where satellites or intermediate nodes are trusted.

The service layer converts these components into a customer proposition. It defines routes, key volume, scheduling, assurance, support and remedies. The valuation model should preserve these boundaries because a technically successful payload can coexist with an incomplete ground network or an unaccepted customer interface.

4. USE STANDARDS AS AN INTERFACE MAP

The ITU-T Y.3800 series describes QKD networks, functional requirements, architecture, key management and control. ITU-T TR.SQKDN, agreed in March 2025, reviews satellite-based QKD networks, use cases, technical information and standardisation gaps. ETSI's QKD programme addresses optical characterisation, implementation security, interfaces, software-defined networking and certification.

Standards do not certify a specific investment. They provide a common vocabulary and a basis for requirements, procurement and testing. The investor should map each claimed service to the relevant interface and assurance evidence. A proprietary component may add performance or intellectual property, but it should still connect to the wider system through documented boundaries.

Standards maturity also affects exit value. Interoperable terminals and key-management interfaces can widen the customer and partner universe. Dependence on one undocumented interface can create switching cost and buyer concentration. The diligence plan should record conformance, deviations and the cost of future change.

5. MODEL ORBIT AND PASS GEOMETRY

Low Earth orbit can provide lower path loss than higher orbits and has supported the leading satellite QKD demonstrations. It also produces short visibility windows and repeated handovers. Altitude, inclination, local horizon, elevation threshold and terminal location determine when a route is possible. The operator must schedule limited passes among commissioning, experiments, customer service and maintenance.

The financial model should convert orbit geometry into potential service minutes by route and month. It should then apply pointing, weather, background-light, equipment and operational constraints. A global coverage claim can conceal limited service for a specific customer pair. The correct unit is usable, accepted delivery on a named route.

Constellations can increase revisit and route availability. They also multiply spacecraft, launch, control, replenishment and coordination cost. Valuation should recognise constellation option value only when the architecture, deployment sequence and funding route are credible.

6. BUILD THE OPTICAL LINK BUDGET

The link budget connects transmitter output to detections that can produce secure key material. It includes wavelength, aperture, beam divergence, pointing loss, atmospheric absorption, turbulence, detector efficiency, background counts and protocol overhead. The result varies through a pass as range and elevation change.

An investor does not need to reproduce the complete security proof. The investment team needs an independently reviewed model tied to representative hardware and measured data. It should distinguish raw detections, sifted key and final secure key after error correction and privacy amplification. Quoting the most favourable instant in a pass can materially overstate service output.

The diligence data room should contain assumptions, calibration, uncertainty and pass-level results. Management should reconcile modelled and observed performance. A growing residual gap between model and field data is a capital-allocation signal because it changes terminal requirements, route capacity and service economics.

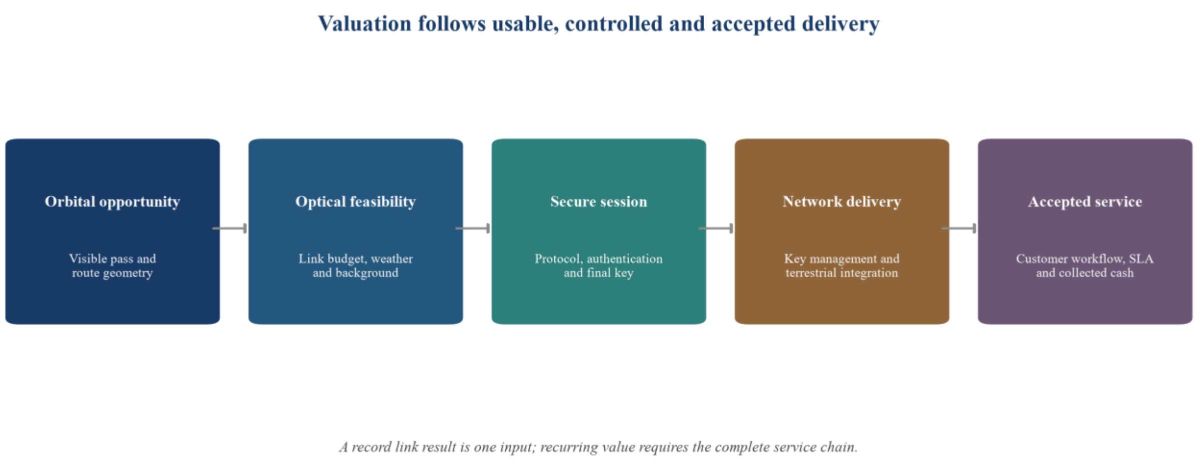

Figure 1. From physical opportunity to accepted customer service

Each gate removes unavailable passes and adds evidence needed for valuation.

7. PRICE WEATHER AS A NETWORK VARIABLE

Cloud can block an optical quantum link. Aerosol, humidity, turbulence and background light can degrade it. Weather is therefore part of the capacity model, rather than a general operational caveat. Historical data should be matched to the terminal's field of view, elevation constraints and required session conditions.

The operator should model conditional probability. Two nearby stations can share the same cloud system and provide limited diversity. Stations in different weather regimes can improve availability, subject to orbit and network connectivity. Five-year studies of optical-ground-station diversity show why location correlation matters when estimating service availability.

The investment model should state the weather dataset, time resolution, missing-data treatment and correlation assumptions. It should report potential passes, weather-eligible passes, attempted sessions and successful secure sessions. This sequence makes the cost of an additional site comparable with the availability it adds.

8. VALUE GROUND-STATION DIVERSITY

A ground-station network can increase the probability that at least one terminal has a usable pass. It can also extend geography and provide operational resilience. The incremental value depends on weather correlation, common orbital opportunities, terrestrial connectivity and customer routes.

Each additional station requires land or hosting, civil works, telescope and detector equipment, secure facilities, connectivity, staffing, maintenance and local permission. Portable terminals can reduce fixed infrastructure and support temporary or sovereign deployment, while adding logistics, calibration and operating complexity.

The valuation model should optimise a portfolio of sites rather than rank stations independently. The selected network should minimise complete cost for a target route-availability profile. A station that adds little standalone capacity may still have high option value if it unlocks a strategic customer or cross-border corridor.

9. UNDERWRITE POINTING, ACQUISITION AND TRACKING

Quantum links operate at very low received photon levels. The space and ground terminals must acquire each other, maintain pointing and preserve optical quality through a moving pass. Coarse orbit knowledge, beacon systems, fine steering, timing and control loops work together. Failure in any one function can turn a visible pass into no usable session.

Management should present acquisition probability, tracking stability, pointing loss and recovery by elevation and weather condition. Results should cover repeated passes rather than selected demonstrations. The model should identify whether the constraint sits in the spacecraft, ground terminal, ephemeris, control software or operations.

Pointing performance affects capital in two ways. Better performance can increase usable key output and permit smaller terminals. Weak performance may require larger apertures, more stations or conservative scheduling. The valuation bridge should therefore connect pointing evidence to terminal cost and service capacity.

10. DISTINGUISH DAY AND NIGHT OPERATIONS

Background photons can increase detector noise and quantum bit error rate, particularly in daylight. Filters, field of view, timing and protocol design can mitigate the effect. The service plan should state whether performance is limited to night, twilight or specified daylight conditions.

A night-only system may still support valuable scheduled services. It has a different capacity and customer profile from an on-demand service. Marketing language should not combine the two. The financial model should allocate revenue to the available delivery window and include customer scheduling constraints.

Daylight capability should be valued after repeated route evidence. It may expand capacity and reduce seasonality, but it can also require additional equipment or stricter operating conditions.

The investor should seek pass-level evidence and final secure-key output under the claimed conditions.

11. TRANSLATE KEY RATE INTO CUSTOMER UTILITY

Secret-key rate is a technical output. Customer utility depends on how keys are used. A high-rate demonstration does not automatically create an application, and a modest rate can be valuable for key refresh in a high-value secure channel. The required volume depends on encryption architecture, session design, buffering and assurance policy.

The service specification should define delivered key, location, freshness, availability and integration. It should identify whether keys are used with symmetric encryption, one-time-pad applications or other controls. It should also explain fallback when the quantum link is unavailable.

Valuation should use accepted service units. Examples include secure route-hours, managed endpoints, reserved key capacity or assured sessions. A unit should be measurable, billable and linked to cost. Technical metrics remain necessary for operations, while commercial metrics determine recurring value.

12. MAKE TRUST ASSUMPTIONS EXPLICIT

Satellite QKD architectures can use trusted satellites or trusted ground nodes. The security claim depends on where key material exists, who controls the node and how it is protected. Entanglement-based approaches may change trust assumptions but create their own performance and implementation requirements.

The operator should document the threat model, trusted components, authentication, key handling and compromise response. A customer with sovereign or classified requirements may reject an architecture accepted by a commercial enterprise. The addressable market therefore depends on the exact trust model.

Valuation should separate technical capability from market eligibility. A route can be operational yet unavailable to customers whose policy prohibits a particular trusted node or jurisdiction. Investment cases should avoid applying one revenue multiple across customer groups with different acceptance criteria.

13. INTEGRATE TERRESTRIAL NETWORKS

Space links rarely complete the customer route. Ground stations must connect to national networks, data centres, encryption devices and users. EuroQCI explicitly combines terrestrial fibre networks with a space segment. The Chinese integrated network combined hundreds of fibre links with satellite links. These architectures show the importance of the terrestrial layer.

The investor should map the complete route, including trusted relays, fibre availability, cross-border dependencies, key management and customer premises. Terrestrial constraints can dominate latency, availability, security and cost after the satellite session succeeds.

Partnerships with telecom carriers can accelerate access to fibre, facilities and enterprise customers. They can also divide economics and control. The valuation model should use the rights and margins retained by the subject company, rather than total system revenue.

14. TREAT KEY MANAGEMENT AS A CORE PRODUCT

The key-management system receives or derives keys, controls access, monitors inventory and supplies applications. It must manage identity, authorisation, storage, expiry, audit and exception handling. ETSI and ITU work on QKD interfaces and key-management architectures provides a basis for interoperability.

The operator should demonstrate how a key moves from a secure session into a customer's encryption workflow. Evidence should include interface conformance, role separation, logging, resilience, backup and incident response. Security evaluation should cover implementation weaknesses as well as protocol theory.

Key management can create reusable software value when it supports multiple payloads, terminals, networks and applications. That value depends on accepted deployments, maintainable code, documented interfaces and customer retention. A proprietary layer with no external integration evidence remains development option value.

15. UNDERWRITE AUTHENTICATION AND CLASSICAL CHANNELS

QKD requires an authenticated classical channel. The initial authentication method and later key lifecycle are part of the security design. The operator must also secure command, control, telemetry, scheduling and software updates through conventional means.

Post-quantum cryptography can complement QKD by protecting authentication, signatures and wider systems. ETSI describes QKD as one component in a layered quantum-safe strategy. The investment case should avoid presenting satellite QKD as a replacement for all cryptographic migration.

Diligence should review the complete security architecture, including certificate management, privileged access, software supply chain and incident response. A weakness in the classical environment can impair the service even when the quantum channel performs as designed.

16. ESTABLISH SECURITY EVALUATION AND CERTIFICATION

Laboratory performance does not prove implementation security. Sources, detectors, control electronics and interfaces can introduce side channels and operational vulnerabilities. ETSI has published a Common Criteria protection profile for prepare-and-measure QKD modules, and Europe is building testing and evaluation capability through NOSTRADAMUS.

The programme should define which components require product evaluation, system accreditation or customer acceptance. Certification scope, laboratory capacity, evidence ownership and schedule should appear in the cost-to-complete model. A certificate for one module does not establish end-to-end service assurance.

Certification can support market access and reduce customer diligence. It can also delay deployment and expose redesign cost. Valuation should recognise the benefit only after the applicable scope and target customer requirements are clear.

Table 2. Evidence gates for satellite quantum-communications valuation

Gate	Required evidence	Valuation lens	Main residual risk
Qualified subsystem	Environmental qualification, calibrated performance and interface baseline	Replacement cost plus probability-weighted option value	Integration, launch and end-to-end performance
Successful mission demonstration	Repeated passes, final secure key, anomaly record and independent review	Probability-weighted milestone value	Availability, operations and customer integration
Accepted network pilot	Multi-site delivery, key management, security review and customer acceptance	Comparable transactions and milestone-adjusted DCF	Scale, certification and repeatable unit economics
Contracted initial service	Paid term, route commitment, service definition, support and collected cash	Contracted contribution and infrastructure value	Renewal, concentration and cost to serve
Repeatable operating platform	Multiple customers, measured SLA, stable margins and replenishment plan	Operating DCF, infrastructure and strategic value	Competition, obsolescence and capital intensity

Each gate supports a different valuation method and should be independently verified.

17. BUILD THE COMPLETE COST BASELINE

The complete baseline includes payload design, spacecraft integration, qualification, launch, insurance, mission operations, ground terminals, sites, terrestrial connectivity, key management, security evaluation, customer integration, sales, support, replenishment and contingency. Internal engineering and partner contributions should be visible even when funded through grants.

Costs should be organised by work package and evidence gate. Historical spend is not equivalent to replacement cost or value. The investor needs remaining cost, committed cost, cancellation exposure, schedule and the probability that each package reaches acceptance.

Public funding can reduce company cash requirements while creating procurement, reporting, intellectual-property and service obligations. The model should record the economic terms of each contribution. A grant-funded asset may have restricted use or limited transferability in a transaction.

18. VALUE LAUNCH AND MISSION RISK

Launch timing, orbit injection and early operations are discrete risk events. A hosted payload can reduce spacecraft cost while creating dependency on the host mission. A dedicated small satellite can give greater control and require a complete platform, launch and operations capability.

Insurance may cover defined losses, subject to exclusions, pricing and market capacity. It does not replace schedule or customer confidence after a failure. The financing plan should include replacement lead time and the capital required to rebuild.

Valuation should use milestone probabilities rather than a single discount rate for all development risk. The value before launch equals the probability-weighted value after successful commissioning, less remaining cost and downside obligations. Probabilities should come from the programme's evidence and comparable mission data, with sources and governance recorded.

19. MODEL SPACECRAFT LIFE AND REPLENISHMENT

Mission life depends on spacecraft platform, components, orbit, radiation, degradation, propulsion where applicable and operations. Optical payload alignment and detector or laser performance may change over time. A commercial service needs continuity beyond one experimental mission.

The operator should present a replenishment plan covering design freeze, procurement, launch cadence, spares and obsolescence. A constellation requires overlap between generations. Customers may require continuity commitments that extend beyond the current satellite's expected life.

The valuation model should fund replenishment before distributing free cash flow. Treating all launch expenditure as one-time development can overstate steady-state margins. Residual value should reflect transferable ground and software assets separately from the finite-life space asset.

20. COMPARE DEDICATED, HOSTED AND SHARED ARCHITECTURES

A dedicated satellite provides mission control and a tailored orbit. A hosted payload can share platform and launch cost. A public or consortium mission can share infrastructure and demand. Each model changes governance, schedule, data rights and commercial freedom.

The investor should assess control over payload operations, customer scheduling, technical changes, security evidence and replacement. A low-cost hosted route can have limited capacity or priority. A dedicated system can preserve strategic rights while concentrating capital risk.

Shared architectures need allocation rules. The valuation should reflect the subject company's reserved capacity and contractual rights. An association with a large public programme has strategic significance, while cash-flow value depends on enforceable access and monetisation.

21. PRICE OPTICAL GROUND TERMINALS

Ground-terminal cost includes telescope, mount, enclosure, acquisition and tracking, detectors or sources, timing, electronics, secure computing, site works, environmental control and integration. Complete cost also includes staffing, calibration, spares, connectivity and maintenance.

Terminal economics vary with aperture, mobility, automation and assurance. A fixed observatory can provide performance and stability. A compact or portable terminal can widen deployment and reduce site dependence. The 2025 microsatellite demonstration is relevant because it links smaller space hardware with compact mobile ground stations.

The investor should obtain a bill of materials, supplier quotes, yield, installation time and acceptance history. Terminal gross margin should include warranty, field service and upgrade obligations. Strategic value can sit in manufacturing know-how, pointing software, detector integration and deployable operations.

22. CHOOSE ANCHOR ROUTES BEFORE BROAD COVERAGE

An early network should prioritise routes where customer need, geography, weather, terrestrial integration and regulatory permission align. Broad coverage can dilute terminal utilisation and engineering attention. A defined corridor creates a measurable service and an accountable cost base.

Anchor routes may connect government sites, data centres, financial centres, energy infrastructure or research networks. The operator should avoid assuming willingness to pay from sector labels. It needs a named problem, customer acceptance criterion, procurement route and budget owner.

The first route should create reusable evidence. It should test interfaces and operating processes that can support later customers. A bespoke route with no transferable architecture may produce revenue and limited platform value.

23. CONVERT ANCHOR DEMAND INTO FINANCEABLE COMMITMENTS

Letters of support and research collaboration can assist development. Financing requires stronger evidence. A paid pilot, reserved capacity agreement, take-or-pay commitment or term service contract can support capital when conditions and remedies are clear.

The commitment should specify locations, service definition, integration work, acceptance, start date, price, liability and termination. Public-sector programmes may use milestone procurement or availability payments. Commercial customers may contract for managed encryption or assured key services.

Revenue should enter the valuation according to enforceability and probability. Unfunded interest belongs in pipeline analysis. Conditional contracts should be linked to the condition and remaining cost. Collected cash and renewal provide the strongest evidence of willingness to pay.

24. DEFINE SERVICE-LEVEL MEASURES

Relevant measures can include scheduled opportunity, weather-adjusted availability, acquisition success, secure-session completion, delivered key volume, latency to application, incident response and restoration. The service level should distinguish causes within and outside the operator's control.

A customer may value assured windows rather than continuous access. Another may require route diversity and stored key inventory. The contract should match the operating reality. Remedies should be supportable within the operator's capital and insurance structure.

Performance reporting becomes a valuation asset when it is consistent across customers and periods. It supports pricing, renewal, capacity planning and diligence. A dashboard should preserve pass-level data while presenting contracted outcomes to management.

25. BUILD CUSTOMER INTEGRATION PLAYBOOKS

Customer integration can involve encryption devices, network management, identity, compliance, data centres and application owners. The operator should create standard architectures for common use cases and document the boundary between its service and the customer's controls.

Integration time and specialist labour belong in customer acquisition cost. A highly customised pilot can produce attractive headline revenue and weak repeatability. The company should track configuration variance, deployment time, defects and reusable components.

Accepted playbooks support scaling through telecom, systems-integration and cybersecurity partners. Partner economics, certification and support responsibilities should be included in gross margin. The valuation premium for software or platform repeatability requires evidence from multiple deployments.

26. ASSESS SOVEREIGN AND CROSS-BORDER CONSTRAINTS

Quantum communications can involve national-security, export-control, encryption, data, space, spectrum and procurement rules. Ground stations and trusted nodes can create jurisdictional sensitivities. Cross-border routes require compatible permissions and operating arrangements.

The company should maintain a jurisdiction matrix covering licences, ownership restrictions, data or key handling, customer eligibility and transfer of technology. Legal analysis should be current and specific to the proposed route. A demonstration permission does not necessarily authorise commercial service.

Regulatory access can create scarcity value when it is transferable and durable. It can also constrain a transaction or customer mix. Valuation should reflect the rights held by the company and the approvals still required after a change of control.

27. PROTECT INTELLECTUAL PROPERTY AND DATA RIGHTS

Value may reside in optical design, pointing algorithms, source or detector engineering, protocol implementation, terminal manufacturing, key management, mission data and operating procedures. Collaboration with universities, agencies and prime contractors can divide ownership and use rights.

Diligence should trace background intellectual property, project results, licences, field restrictions, publication rights and employee or contractor assignments. The company should identify which rights are necessary to build, operate, sell and transfer the service.

Mission data can improve link models and site selection. Its value depends on ownership, quality, coverage and lawful commercial use. A buyer should avoid capitalising data whose rights or reproducibility are uncertain.

28. SELECT THE VALUATION METHODS

Replacement cost provides a reference for qualified hardware, software and infrastructure. It does not capture commercial demand or the probability that a new team can reproduce the system. Comparable transactions can assist when stage, rights and architecture are genuinely similar. Public market multiples are usually too broad for a development-stage platform.

A milestone probability model is appropriate before stable revenue. It starts with value at the next accepted stage, applies the probability and timing of reaching that stage, deducts cost to complete and recognises downside obligations. Scenario DCF becomes more useful after contracted services and repeatable costs exist.

Strategic value can exceed standalone DCF when an acquirer gains sovereign access, a missing technology, scarce engineering or a route into a public infrastructure programme. That value should be tied to buyer-specific synergies and integration cost rather than added as an unsupported premium.

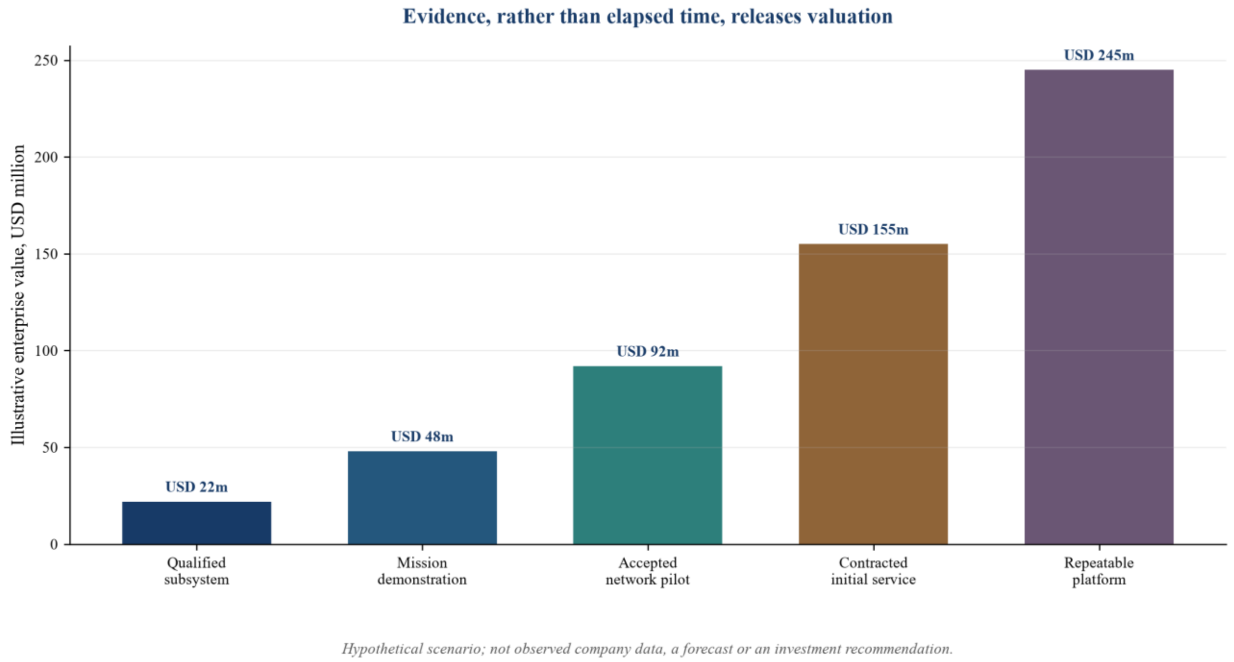

Figure 2. Illustrative valuation bridge across evidence milestones

Values are hypothetical management assumptions used only to demonstrate the framework.

29. CONSTRUCT THE MILESTONE VALUATION BRIDGE

The bridge should explain why value changes between stages. Successful qualification reduces redesign risk. Mission demonstration reduces launch, pointing and link risk. A multi-site pilot reduces availability, operations and integration risk. A paid contract supports demand and pricing. Repeatable service supports margin and renewal assumptions.

Each step should reconcile new evidence, remaining cost and dilution. A financing round that follows a milestone can still reduce per-share value if the capital need expands. Management should present enterprise value and equity value separately, including debt, grants with repayment conditions and committed obligations.

The bridge is a governance tool as well as a valuation output. It tells the board which evidence has the highest value per unit of capital. It can prevent premature investment in coverage before the operator proves an accepted end-to-end service.

30. LINK CAPITAL RELEASE TO GATES

Early capital funds qualification, interfaces, one or two representative terminals and mission readiness. Later capital funds network diversity, customer integration and service capacity after core risks reduce. A single fully funded plan can obscure the evidence needed before scale.

Milestones should be objective. Examples include environmental qualification, launch readiness, repeated final secure-key delivery, multi-site availability, accepted key-management integration, certification and a paid customer term. Each milestone needs an evidence owner and independent reviewer.

Financing instruments can include equity, strategic investment, grants, milestone procurement, vendor finance and asset facilities for separable equipment. Debt becomes more appropriate as contracted cash flow and recoverable assets emerge. Core development risk should not be hidden inside long-dated leverage.

31. APPLY A HYPOTHETICAL OPERATOR CASE

Consider a hypothetical operator developing a low-Earth-orbit quantum-key-distribution service for government and regulated-enterprise routes. It owns payload and key-management intellectual property, contracts satellite-platform and launch services, and plans four optical ground stations across two weather regions. A telecom partner provides terrestrial connectivity.

Illustrative management assumptions place remaining development and deployment cost at USD 64 million. The programme allocates USD 20 million to space segment and launch, USD 24 million to ground terminals and sites, USD 8 million to key management and security evaluation, USD 7 million to customer integration and USD 5 million to programme contingency.

Every amount, schedule, terminal characteristic, weather assumption, contract term and valuation in this case is hypothetical. The case demonstrates the method. It is not observed operator information, a market forecast, a financing offer or an investment recommendation.

32. MODEL THE HYPOTHETICAL ROUTE CAPACITY

The operator models 1,460 annual orbital opportunities across the intended routes. Hypothetical management assumptions remove 28 per cent for geometry and scheduling conflicts, 34 per cent of the remainder for weather and optical conditions, and 12 per cent of attempted sessions for acquisition, protocol or operating failure. The result is approximately 540 successful secure sessions before planned maintenance and customer allocation.

The company does not treat every session as revenue. It reserves capacity for commissioning, recovery, public obligations and buffer. Commercial capacity is assigned to two anchor routes and a smaller innovation service. The service model specifies scheduled windows and stored key inventory rather than continuous availability.

The board tests a downside with correlated cloud, one unavailable terminal and lower acquisition performance. The downside reduces customer capacity and delays contract acceptance. This result informs the value of a geographically diverse fifth site.

33. BUILD THE HYPOTHETICAL COMMERCIAL CASE

The operator assumes two paid pilots begin after multi-site commissioning. A public-sector customer converts to a three-year availability contract after security acceptance. A financial-services customer converts after its encryption appliance and operating controls pass testing. No revenue is included before the applicable acceptance condition.

Illustrative management assumptions produce USD 9 million of first full-year revenue and USD 3 million of contribution after direct operations, partner share, support and terminal maintenance. Revenue grows only when additional route capacity and customer integration are funded. The model includes customer concentration and renewal downside.

The commercial case separates contracted, probability-weighted and pipeline revenue. Pipeline descriptions support strategy but carry no base-case value. The board reports collected cash and contribution alongside bookings because long implementation periods can separate contract signature from economic delivery.

34. DERIVE THE HYPOTHETICAL VALUATION

At the qualified-subsystem stage, hypothetical replacement cost and intellectual-property option value support an enterprise value of USD 22 million. After successful mission demonstration, the probability-weighted value rises to USD 48 million. An accepted multi-site network pilot supports USD 92 million. Contracted initial service supports USD 155 million, subject to cost to complete and concentration.

The hypothetical repeatable-platform case reaches USD 245 million after multiple customers, measured availability, stable contribution and a funded replenishment plan. These values are management scenarios, not market observations. The model uses stage probabilities, remaining capital, dilution and downside obligations to bridge equity value.

The largest sensitivity is not the headline key rate. It is the probability of repeatable accepted service across the contracted routes. Weather diversity, terminal cost, customer integration and replenishment determine how much of the technical achievement becomes durable enterprise value.

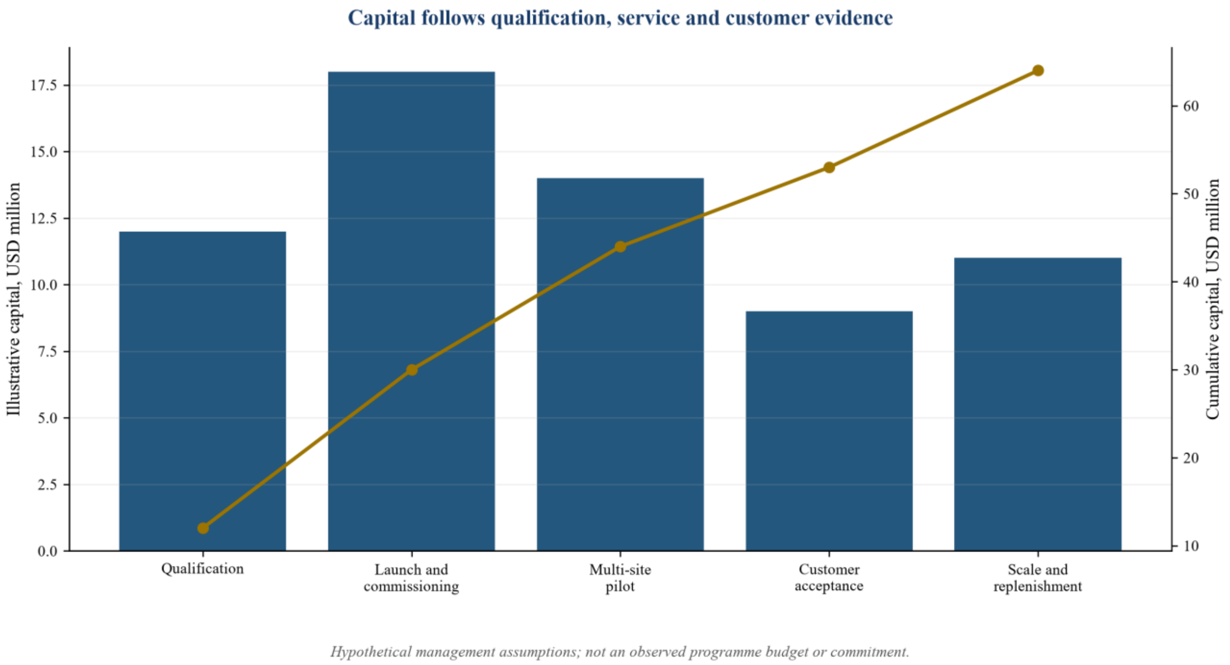

Figure 3. Illustrative capital release by evidence gate

Amounts are hypothetical and demonstrate staged financing rather than an observed funding plan.

35. STRESS-TEST WEATHER AND TERMINAL FAILURE

The downside model should combine correlated cloud with terminal downtime. Independence assumptions can overstate diversity. The operator should test regional weather systems, seasonal concentration, maintenance and common suppliers. It should also test loss of a site whose geography enables a specific route.

Responses include an additional station, portable backup, alternate routing, stored key inventory and revised service windows. Each response has complete cost and customer implications. The cheapest response may be a narrower service commitment rather than more infrastructure.

Financing agreements should preserve capital for restoration and avoid revenue covenants that assume maximum theoretical capacity. Insurance, spares and service credits should be reconciled with the same downside model.

Table 4. Illustrative sensitivities in the hypothetical operator case

Sensitivity	Hypothetical change	Operational effect	Valuation response
Correlated cloud	Weather-eligible passes fall 20 per cent below base case	Fewer customer windows and lower terminal utilisation	Reduce contracted capacity, test a fifth site and defer scale capital
Terminal outage	One strategic ground station is unavailable for 60 days	A named route loses geographic redundancy	Apply restoration cost, service credits and route-specific revenue downside
Acquisition weakness	Successful acquisition falls from 88 per cent to 72 per cent of attempts	Lower secure-session output despite visible passes	Fund corrective engineering before crediting additional coverage
Customer delay	Initial service acceptance moves by nine months	Cash collection and reference-customer evidence are delayed	Increase funding need, discount milestone value and re-test concentration
Launch delay	Commissioning moves by twelve months	Team and supplier carrying costs rise while customer dates move	Add complete delay cost and update probability, dilution and contract exposure

All values are hypothetical management assumptions and demonstrate model behaviour rather than observed performance.

36. STRESS-TEST PROGRAMME AND DEMAND DELAY

Launch delay, qualification failure, certification queues and customer procurement can move on different timelines. A technical programme can consume cash while commercial acceptance remains conditional. The board should model combined delay and the capital required to preserve the team and supply chain.

Management should define stop, redesign and partner triggers. A failed payload test may justify another build. Repeated failure against the same model can require architecture change. A customer delay may support a revised corridor if the underlying platform remains transferable.

The valuation should reduce for both time and additional capital. Extending a milestone without updating cost, dilution and probability overstates equity value. Investors should receive the evidence that supports any revised date.

Table 3. Board decision gates and capital consequences

Gate	Acceptance evidence	Board decision	Capital consequence
Payload qualified	Environmental results, calibrated link model, interfaces and open anomalies	Authorise launch integration	Release launch and commissioning capital
Mission commissioned	Repeated acquisition, final secure key, anomaly closure and operations handover	Authorise multi-site pilot	Fund additional terminals and integration
Network pilot accepted	Route performance, weather model, key management, security review and recovery test	Authorise customer service	Fund customer deployment and working capital
Customer accepted	Paid scope, technical acceptance, SLA baseline and collected cash	Authorise controlled scale	Release capacity and partner investment
Platform repeatable	Multiple routes and customers, stable operations, contribution and replenishment	Approve long-term financing or transaction	Apply operating valuation and optimise capital structure

Capital is released when the relevant uncertainty has been reduced by accepted evidence.

37. ESTABLISH GOVERNANCE, REPORTING AND LIMITATIONS

Governance should combine mission engineering, quantum security, network operations, finance, legal, commercial and customer responsibility. One executive forum should own the integrated schedule, cost to complete, evidence gates, exceptions and service commitments. Technical and financial work packages should use the same identifiers.

Board reporting should include potential passes, weather-eligible passes, attempted sessions, successful sessions, final key delivered, accepted customer windows, incidents, cost, liquidity and milestone forecast. Benefits should distinguish contracted revenue, collected cash and management scenarios. Independent review should focus on material gates.

This framework does not predict the timing of quantum computers or guarantee the security of a particular system. It does not replace cryptographic, space, engineering, regulatory, legal, tax, accounting or investment advice. The hypothetical case is not a benchmark. Each programme requires its own route data, threat model, customer evidence and financing terms.

38. CONCLUSION

Satellite quantum communications have credible physical demonstrations and expanding public infrastructure programmes. Investment value depends on the step from a successful link to a repeatable, controlled and accepted service. That step crosses orbit, weather, terminals, key management, terrestrial networks, certification, customer integration and replenishment.

The Space-to-Ground Quantum Valuation Framework makes those dependencies visible. It values qualified subsystems, mission evidence, network operations, customer acceptance and recurring contribution separately. It uses ground-station diversity and terminal economics to convert weather from a caveat into a capacity decision. It releases capital when evidence reduces a defined risk.

The practical question for a board or investor is precise: what usable, secure and contractually accepted service can this system deliver on a named route, at what complete cost, with which remaining dependencies? A programme that can answer that question can support a defensible valuation and a disciplined financing plan.

REFERENCES

[1] International Telecommunication Union, Technical Report ITU-T TR.SQKDN, Standardization consideration of satellite-based QKDN, March 2025, https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-QKD-2025-1-PDF-E.pdf

[2] International Telecommunication Union, Recommendation ITU-T Y.3800, Overview on networks supporting quantum key distribution, https://www.itu.int/rec/T-REC-Y.3800

[3] International Telecommunication Union, Recommendation ITU-T Y.3801, Functional requirements for quantum key distribution networks, https://www.itu.int/rec/T-REC-Y.3801

[4] International Telecommunication Union, Recommendation ITU-T Y.3802, Quantum key distribution networks - Functional architecture, https://www.itu.int/rec/T-REC-Y.3802

[5] International Telecommunication Union, Recommendation ITU-T Y.3803, Quantum key distribution networks - Key management, https://www.itu.int/rec/T-REC-Y.3803

[6] International Telecommunication Union, Recommendation ITU-T Y.3828, Integration of QKDN and user networks supporting end-to-end modern cryptography services, 2025, https://www.itu.int/rec/T-REC-Y.3828-202504-I

[7] European Telecommunications Standards Institute, Quantum Key Distribution standards and work programme, accessed September 2026, https://www.etsi.org/technical-groups/qkd/

[8] European Telecommunications Standards Institute, ETSI GS QKD 014, Protocol and data format of REST-based key delivery API, https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/

[9] European Telecommunications Standards Institute, ETSI GS QKD 015, Control interface for software defined networks, https://www.etsi.org/deliver/etsi_gs/QKD/001_099/015/

[10] European Telecommunications Standards Institute, ETSI GS QKD 016 V2.1.1, Common Criteria Protection Profile for prepare-and-measure QKD modules, 2024, https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/02.01.01_60/

[11] European Telecommunications Standards Institute, ETSI GS QKD 018, Orchestration interface of software defined networks, https://www.etsi.org/deliver/etsi_gs/QKD/001_099/018/

[12] European Telecommunications Standards Institute, ETSI GS QKD 020 V1.1.1, REST-based interoperable key management system API, 2026, https://www.etsi.org/technical-groups/qkd/

[13] European Commission, European Quantum Communication Infrastructure, accessed September 2026, https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

[14] European Commission, EuroQCI Concept of Operations, updated 2024, https://digital-strategy.ec.europa.eu/en/miscellaneous/euroqci-conops-concept-operations

[15] European Commission, Future EuroQCI activities to be supported by the European Commission, 2026, https://digital-strategy.ec.europa.eu/en/consultations/future-euroqci-activities-be-supported-european-commission

[16] European Space Agency, Eagle-1, accessed September 2026, https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Eagle-1

[17] European Space Agency, EAGLE-1 mission architecture, accessed September 2026, https://resilience.esa.int/archives/partnership-projects/eagle-1

[18] Liao, S.-K. et al., Satellite-to-ground quantum key distribution, Nature 549, 43-47, 2017, https://doi.org/10.1038/nature23655

[19] Chen, Y.-A. et al., An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature 589, 214-219, 2021, https://doi.org/10.1038/s41586-020-03093-8

[20] Yin, J. et al., Entanglement-based secure quantum cryptography over 1,120 kilometres, Nature 582, 501-505, 2020, https://doi.org/10.1038/s41586-020-2401-y

[21] Liao, S.-K. et al., Satellite-relayed intercontinental quantum network, Physical Review Letters 120, 030501, 2018, https://doi.org/10.1103/PhysRevLett.120.030501

[22] Takenaka, H. et al., Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite, Nature Photonics 11, 502-508, 2017, https://doi.org/10.1038/nphoton.2017.107

[23] Liao, S.-K. et al., Microsatellite-based real-time quantum key distribution, Nature, 2025, https://doi.org/10.1038/s41586-025-08739-z

[24] University of Science and Technology of China, Quantum microsatellite and real-time QKD with mobile ground stations, 2025, https://en.ustc.edu.cn/info/1011/5033.htm

[25] Bedington, R., Arrazola, J. M. and Ling, A., Progress in satellite quantum key distribution, npj Quantum Information 3, 30, 2017, https://doi.org/10.1038/s41534-017-0031-5

[26] Bourgoin, J.-P. et al., A comprehensive design and performance analysis of low Earth orbit satellite quantum communication, New Journal of Physics 15, 023006, 2013, https://doi.org/10.1088/1367-2630/15/2/023006

[27] Oi, D. K. L. et al., CubeSat quantum communications mission, EPJ Quantum Technology 4, 6, 2017, https://doi.org/10.1140/epjqt/s40507-017-0060-1

[28] Polnik, M. et al., Scheduling of space-to-ground quantum key distribution, EPJ Quantum Technology 7, 3, 2020, https://doi.org/10.1140/epjqt/s40507-020-0079-6

[29] Khatri, S. et al., Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet, npj Quantum Information 7, 4, 2021, https://doi.org/10.1038/s41534-020-00327-5

[30] National Institute of Standards and Technology, Quantum Information Networks, accessed September 2026, https://www.nist.gov/ctl/smart-connected-systems-division/quantum-information-networks

[31] National Institute of Standards and Technology, FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, 2024, https://doi.org/10.6028/NIST.FIPS.203

[32] National Institute of Standards and Technology, FIPS 204, Module-Lattice-Based Digital Signature Standard, 2024, https://doi.org/10.6028/NIST.FIPS.204

[33] National Institute of Standards and Technology, FIPS 205, Stateless Hash-Based Digital Signature Standard, 2024, https://doi.org/10.6028/NIST.FIPS.205

[34] International Organization for Standardization, ISO 31000:2018 Risk management guidelines, https://www.iso.org/iso-31000-risk-management.html

[35] IFRS Foundation, IAS 16 Property, Plant and Equipment, https://www.ifrs.org/issued-standards/list-of-standards/ias-16-property-plant-and-equipment/

[36] IFRS Foundation, IAS 38 Intangible Assets, https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/

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

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.