Security at Quantum Cost: Integration Economics in QKD M&A

A transaction framework for assessing real customer workflows and defensible integration value

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Quantum key distribution has moved beyond isolated laboratory experiments into testbeds, national programmes, standards, certification initiatives and early operational services. The transaction case remains difficult. A buyer can acquire strong optical science and still inherit an expensive integration problem: QKD modules must connect to classical key management, cryptographic applications, transport networks, monitoring, identity, authentication, orchestration and customer operating procedures. The security outcome also competes with post-quantum cryptography, which can often be deployed through software and is the preferred migration route of several national security authorities. Acquisition value therefore depends on the workflow that the target can secure, the interfaces it can support, the assurance it can demonstrate and the complete cost of delivering and operating that outcome.

This paper develops the Quantum Integration Economics Framework for strategic buyers, investors, boards and lenders evaluating QKD transactions. The framework separates scientific performance from deployable security value and traces five economic layers: route and optical fit, key-management integration, cryptographic-application adoption, assurance and operations, and customer outcome. It uses an integration bill, workflow-specific alternatives analysis, evidence-weighted revenue quality, transition-service planning and milestone-linked transaction terms. Four tables and three figures convert the approach into a repeatable diligence and deal-structuring method.

The current standards environment makes this analysis practical. ITU recommendations define QKD-network architecture, interworking, software-defined control, orchestration and protocol frameworks. ETSI has published a REST-based interoperable key-management API and maintains work on module protection profiles, monitoring, network architecture and orchestration. EuroQCI is funding national and cross-border infrastructure alongside testing and certification. The United Kingdom's 2026 research review records that most current deployments remain research, testbed or pilot activity, and that adoption depends on strong use cases, reference architectures and integration with conventional systems and post-quantum cryptography. NIST has standardised post-quantum cryptographic algorithms and continues to identify implementation limitations in QKD.

A wholly hypothetical acquisition case applies the framework to a QKD vendor with optical appliances, a key-management layer and several paid pilots. Every case amount, probability, price, customer characteristic, synergy and valuation outcome is an illustrative management assumption. The analysis shows why a buyer should value verified integration assets, contracted route access, reusable connectors, certification evidence, operational telemetry and paid workflow adoption. It should deduct the complete integration bill, protect against unsupported pipeline conversion and

stage consideration around observable customer and interoperability milestones. The central conclusion is that QKD acquisition value arises from a demonstrable security workflow delivered at an acceptable total cost, supported by transferable evidence and operated within a defensible hybrid cryptographic architecture.

JEL Classification: G24, G31, G32, L63, L96, O32, O33

Keywords: quantum key distribution, QKD, mergers and acquisitions, integration economics, post-quantum cryptography, key management, cybersecurity, interoperability, technology valuation, transaction diligence

This paper is an educational and structural analysis prepared for research purposes. It is not investment advice, an offer, or a solicitation. It contains no client information.

1. DEFINE THE ACQUISITION DECISION

The acquisition decision is whether the target can provide a security outcome that customers will adopt, fund and operate within their existing infrastructure. The buyer may seek optical engineering, quantum-safe product capability, public-sector eligibility, telecom distribution, standards influence or a position in a future quantum-network market. Each purpose implies a different perimeter, integration plan and valuation method.

The transaction thesis should identify the exact workflow that will change after closing. Examples include securing a data-centre interconnect, supplying fresh keys to an encryptor, protecting a metro fibre route, integrating quantum-generated keys into a managed security service or enabling cross-domain key exchange between network operators. A thesis framed only as quantum exposure cannot be tested against customer economics.

The buyer should state which target assets are required for the workflow: optical modules, random-number generation, key-management software, orchestration, monitoring, certification evidence, route engineering, customer contracts, deployment teams and intellectual property. The same company can contain valuable assets and costly dependencies. The acquisition model should price both.

Table 1. The five layers of QKD integration economics

Integration layer	Core question	Evidence required	Common valuation error
Route and optical fit	Can the system operate on the customer's fibre or free-space path?	Loss budget, coexistence tests, distance, topology, uptime and environmental envelope	Applying a laboratory distance record to an unsuitable route
Key management	Can generated keys enter the customer's control architecture safely?	Supported APIs, lifecycle controls, auditability, failover, policy and multi-vendor tests	Treating key generation as an end-to-end service
Cryptographic application	Can encryptors and applications consume keys without workflow disruption?	Connector tests, authentication, throughput, rotation, exception handling and rollback	Assuming every application can use QKD-derived keys
Assurance and operations	Can the system be evaluated, monitored, patched and supported?	Protection profile, vulnerability process, telemetry, service procedures and skills	Excluding certification and operating burden from the deal model
Customer outcome	Does the deployment solve a funded security need better than alternatives?	Paid scope, risk owner, procurement path, acceptance, usage and renewal	Capitalising pilot publicity as durable demand

A buyer should record the current evidence, remaining work, cost owner and acceptance test for every layer.

2. PLACE QKD INSIDE THE COMPLETE SECURITY ARCHITECTURE

QKD generates shared secret material through quantum and classical communication. It does not encrypt application data by itself. A production service also needs authenticated classical channels, key-management systems, cryptographic devices or applications, identity and access control, logging, monitoring, physical protection and incident response. The acquisition perimeter must include these dependencies.

The architecture usually contains a quantum layer, key-management layer, control layer, management layer, service layer and user-network layer. ITU-T Y.3802 describes this layered structure and its functional elements. Later recommendations address interworking between networks, software-defined control, orchestration and integration with user networks. The standards reveal the economic point: value is created through a system of interfaces and operating responsibilities rather than one optical appliance.

The buyer should model QKD as one component of a hybrid security architecture. Conventional symmetric cryptography remains responsible for data encryption. Post-quantum algorithms can authenticate sessions or establish keys. QKD may diversify key-establishment risk or support specific high-assurance routes. The architecture should specify what happens when the quantum link is unavailable, when key inventory is depleted, when an application rejects a key or when the authentication mechanism changes.

3. DISTINGUISH THE QUANTUM CHANNEL FROM THE CUSTOMER WORKFLOW

The quantum channel measures photons; the customer workflow protects information. These are connected through several transformations. A QKD module produces key material. A key manager stores, labels and allocates it. An interface supplies it to an encryptor or application. The

application uses it under policy. Operations teams monitor availability and security. The customer accepts a defined service level.

Technical diligence should map this chain from source to protected business process. It should identify every hand-off, trust boundary, data format, protocol, administrator and failure mode. A performance claim has economic value when it improves a customer outcome after all hand-offs are included.

The workflow map also defines the addressable market. A target may perform well on dedicated metro fibre between two controlled sites while offering little value for mobile users, cloud-native applications or dynamic multi-party networks. A narrow workflow can still support an attractive business if the customer loss exposure and willingness to pay are high. Precision improves underwriting.

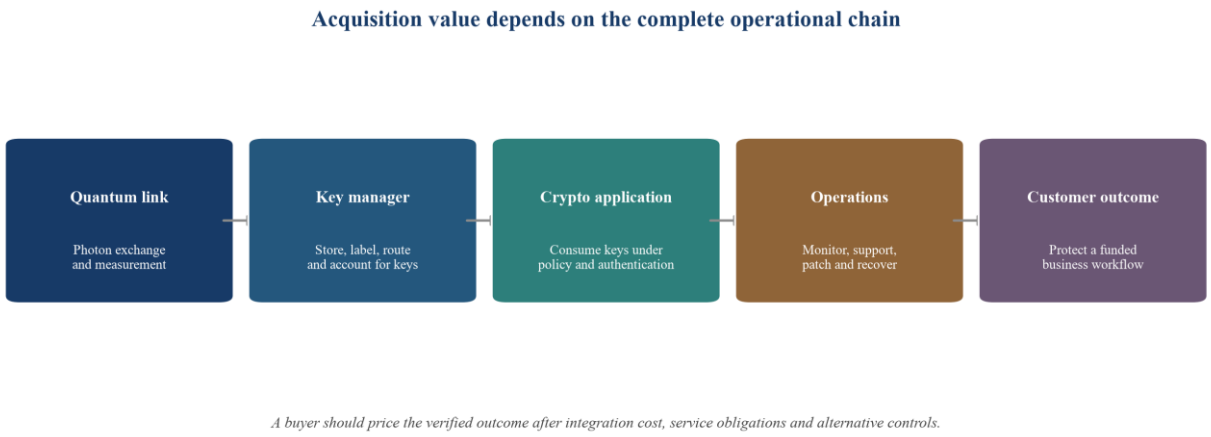

Figure 1. The QKD workflow from photons to a funded security outcome

Every interface adds cost, assurance requirements and an acceptance condition.

4. ESTABLISH THE ROUTE AND OPTICAL BASELINE

Route diligence begins with the physical path. Fibre length alone is insufficient. Connector loss, splices, wavelength plan, amplifiers, switching, dispersion, environmental exposure and coexistence with classical traffic can change the operating envelope. The buyer should obtain measured route data and reproduce the target's loss budget.

The deployment topology matters. Point-to-point links are simpler than switched networks. Trusted nodes extend distance while creating sites that require physical security and operational trust. Satellite links introduce weather, pointing, scheduling, ground stations and regulatory dependencies. A target's architecture should be valued against the routes that customers can actually provide.

The buyer should separate controlled test results from customer-route evidence. A demonstration on laboratory fibre, dark fibre or a purpose-built testbed can establish feasibility. It does not prove coexistence on an operator network or maintainability under field conditions. The acquisition model should assign value to each route only after configuration, acceptance and support requirements are understood.

5. UNDERWRITE KEY-RATE SUFFICIENCY AT THE APPLICATION LEVEL

QKD systems report secret-key rate under stated assumptions. The customer consumes key material according to its cryptographic design. The required rate can vary substantially between periodic key refresh, high-frequency session establishment and one-time-pad use. An attractive optical result can still be uneconomic when the application requires more key material, lower latency or greater availability.

The diligence team should build a key budget. It should reconcile generated, distilled, authenticated, reserved, expired, lost and consumed key material. It should record the buffer required for outages and the consequences of depletion. The model should distinguish average rate, minimum sustained rate and service-level rate.

Authentication also consumes or depends on cryptographic resources. QKD does not remove the need to authenticate the classical channel. A hybrid design may use pre-shared keys, conventional public-key methods or post-quantum signatures and key-establishment mechanisms. The buyer should cost the complete method and its migration path.

6. PRICE THE KEY-MANAGEMENT INTEGRATION

Key management is where optical performance enters enterprise security. The target's key-management system should support secure storage, metadata, allocation, deletion, separation of duties, audit records, policy enforcement, failover and recovery. Its interfaces should allow cryptographic applications to request keys and report status without exposing sensitive material.

ETSI's 2026 REST-based interoperable key-management API and continuing work on key delivery, monitoring and orchestration provide practical reference points. ITU recommendations define interworking at key-management, control and management layers. A target that implements stable, documented interfaces may reduce buyer integration cost. Standards claims should be tested through conformance and multi-vendor operation.

The buyer should inventory every connector and classify it as production, pilot, prototype or roadmap. Reusable connectors can create value when they address a meaningful installed base and have clear support ownership. A bespoke connector built for one pilot can become technical debt if the customer environment is unique.

7. TEST INTEROPERABILITY RATHER THAN MEMBERSHIP

Standards participation can improve technical awareness and market access. It does not prove interoperability. Diligence should require versioned interface specifications, test results, error handling, performance under load and evidence that independent systems can exchange keys and control information.

ITU-T Q.4165, approved in January 2026, specifies a protocol framework for QKD-network interworking. It distinguishes gateway and interworking approaches and identifies reference points for key management, control and management. ITU-T Y.3820 addresses software-defined control across different vendor domains. These frameworks help a buyer define acceptance tests.

The integration plan should include a compatibility matrix. It should name the QKD modules, key managers, controllers, encryptors, applications, network-management systems and versions

that have been tested. It should also identify interfaces that depend on a specific partner or unpublished extension. The valuation should reward demonstrated portability and reserve for untested combinations.

8. TREAT MONITORING AS PART OF THE PRODUCT

Enterprise buyers require visibility into service state. QKD monitoring should cover link availability, secret-key rate, quantum bit error rate, key inventory, alarms, environmental conditions, device health, interface status and policy events. The telemetry must integrate with network and security operations without revealing protected information.

Monitoring affects both cost and customer trust. Weak telemetry increases truck rolls, specialist intervention and outage duration. Excessive or poorly governed telemetry can create security exposure. The target should define which data is collected, where it is stored, who can access it and how long it is retained.

ETSI's active work on a QKD monitoring interface and data model indicates that this layer is still developing. A buyer should distinguish implemented capability from expected standard convergence. It should budget for interface updates, backward compatibility and the operating burden of mixed versions.

9. ASSESS ASSURANCE AND CERTIFICATION EVIDENCE

Security claims require evaluation of the implementation, not only the protocol. Real devices can contain side channels, imperfect sources, detectors, firmware, maintenance interfaces and supply-chain dependencies. NIST notes that physical equipment can create flaws. ETSI work covers optical characterisation, implementation security, protection profiles and evaluation.

The target's assurance package should include its security target, threat model, design evidence, vulnerability process, penetration testing, laboratory reports, configuration guidance and lifecycle controls. The buyer should understand which claims have been independently evaluated and which remain supplier assertions.

Certification can support procurement, particularly in regulated or public-sector markets. It can also impose cost, schedule and change-control constraints. EuroQCI's NOSTRADAMUS testing and evaluation infrastructure and the EUCC environment illustrate the direction of travel. The acquisition model should include initial evaluation, remediation, recertification and assurance-continuity costs.

10. COMPARE QKD WITH POST-QUANTUM ALTERNATIVES

The relevant alternative is often post-quantum cryptography rather than an unchanged legacy system. NIST published its first post-quantum cryptographic standards in 2024. Software and hardware vendors are implementing these algorithms across protocols, products and services. Migration remains substantial, yet it generally uses existing communication channels and enterprise software processes.

The UK's National Cyber Security Centre identifies post-quantum cryptography as the preferred approach to post-quantum security and does not support QKD for government or military applications. The United Kingdom's 2026 independent research report nevertheless identifies commercial learning and niche opportunities for QKD, while emphasising integration, hybrid

architectures and uncertain broad uptake. A buyer should incorporate this policy divergence into market access and product strategy.

The alternatives analysis should be workflow-specific. It should compare security properties, authentication, route constraints, availability, capex, operating cost, migration effort, vendor dependency, certification and residual risk. QKD can be justified where physical-path control, diversification of cryptographic assumptions or particular assurance requirements create incremental value. The model should avoid universal claims.

Table 2. Workflow-specific alternatives analysis

Decision factor	QKD-led hybrid	PQC-led migration	Conventional refresh
Security basis	Quantum measurement plus classical authentication and symmetric encryption	Computational hardness of standardised post-quantum algorithms	Existing classical algorithms and key-management controls
Infrastructure	Quantum channel, optical equipment, key managers, application integration and operations	Software, firmware, protocol and hardware updates across the estate	Lifecycle replacement and configuration changes
Route sensitivity	High; performance depends on physical topology and loss	Low to moderate; uses conventional networks	Low; uses conventional networks
Availability design	Requires key buffers, failover and hybrid fallback	Depends on software and platform resilience	Depends on existing platform resilience
Near-term scale	Targeted routes and specialised workflows	Broad estate migration potential	Existing deployment base
Transaction value driver	Verified integration, route access, assurance and paid use	Installed base, migration tooling, product integration and support	Distribution, compliance and operational efficiency

The appropriate architecture depends on the protected workflow, threat model, route and operating model.

11. CONSTRUCT THE COMPLETE INTEGRATION BILL

The purchase price should be evaluated alongside the cost of reaching an accepted operating service. The integration bill includes route surveys, optical engineering, racks and power, key managers, application connectors, identity and authentication, network changes, monitoring, certification, security testing, training, spare equipment, support, programme management and contingency.

The bill should separate one-time and recurring costs. It should identify costs borne by the buyer, target, customer, network operator and partners. A cost that is funded by a pilot grant may return when the deployment scales. A partner discount may disappear after the demonstration period.

The model should also include opportunity cost. Scarce security, network and quantum specialists may be diverted from core programmes. Long acceptance cycles can delay other revenue. Integration work can create reusable assets; the buyer should distinguish platform investment from customer-specific effort.

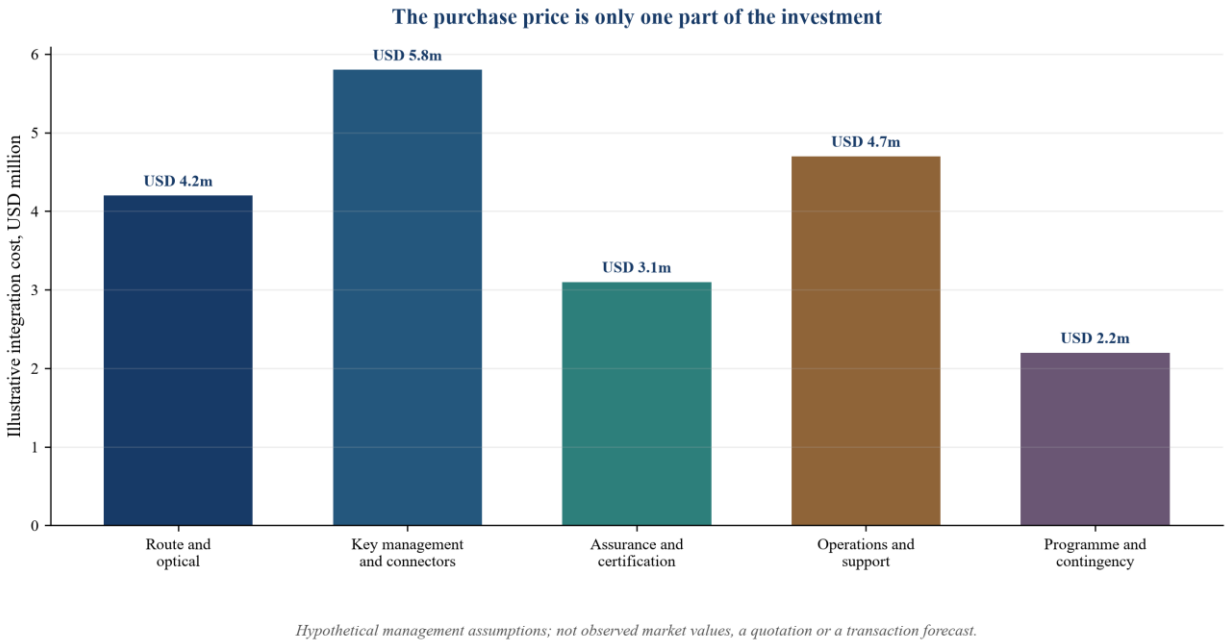

Figure 2. Illustrative QKD integration bill by cost layer

Amounts are hypothetical management assumptions used solely to demonstrate the framework.

12. CONVERT TECHNICAL DEBT INTO TRANSACTION ADJUSTMENTS

Technical debt in a QKD target can sit in hardware, firmware, control software, interfaces, deployment tooling and documentation. A prototype architecture may rely on manually configured equipment, laboratory instruments or unsupported libraries. Customer pilots can conceal this debt because specialist staff intervene directly.

The diligence team should convert identified debt into cost, schedule and dependency. It should estimate redesign, productisation, test, certification, inventory and customer migration. It should identify whether the work can be completed without invalidating performance evidence.

The transaction model can address debt through a purchase-price adjustment, specific indemnity, escrow, completion condition, earn-out or funded integration reserve. The appropriate mechanism depends on whether the uncertainty concerns a known cost, a future milestone or a potential liability.

13. ANALYSE THE TALENT AND KNOWLEDGE PERIMETER

QKD companies often depend on a small group of optical scientists, hardware engineers, security architects and field specialists. Their knowledge may span tacit calibration methods, component selection, deployment workarounds and customer relationships. Retention is therefore part of asset transfer.

The buyer should map critical roles to products, evidence, customers and future milestones. It should examine employment terms, incentives, immigration, academic affiliations, consulting commitments, publication obligations and access to source data. It should establish whether the integration plan creates unwanted attrition.

Knowledge transfer should be an explicit workstream. Source code, design files, test scripts, bill of materials, configuration baselines, field records and supplier knowledge should be documented

before key people leave. Retention awards should link to transferable outcomes rather than mere continued employment.

14. VERIFY INTELLECTUAL-PROPERTY CONTROL

The target's intellectual-property position may include patents, know-how, software, hardware designs, university licences, consortium rights and partner contributions. A strong publication record does not establish ownership. The buyer should trace rights from inventors and institutions to the transaction perimeter.

Public funding and testbed participation can create reporting, access, licensing, procurement or dissemination obligations. University spin-outs may face field restrictions, revenue shares or sublicensing conditions. Joint demonstrations can generate foreground intellectual property with unclear control.

The diligence team should test freedom to operate for the intended product and geography. It should also identify assets that retain value if the current QKD architecture changes, such as photonic packaging, control software, key-management connectors, test equipment and deployment expertise.

15. EXAMINE SUPPLY-CHAIN AND MANUFACTURING ECONOMICS

Production hardware can depend on specialised lasers, detectors, optical components, random-number sources, cooling, timing equipment, secure processors and precision packaging. The buyer should identify single-source items, lead times, export controls, obsolescence and minimum-order quantities.

Prototype bills of material often exclude test fixtures, yield loss, calibration, spares, warranty and field replacement. The acquisition model should use landed, tested and supportable cost. It should model learning curves conservatively and state which improvements require volume, redesign or supplier negotiation.

Manufacturing strategy affects capital intensity and assurance. Outsourcing can reduce fixed cost while increasing supplier dependence and security scrutiny. Internal production can improve control while requiring equipment, skills and quality systems. The buyer should align the choice with customer assurance requirements and expected volume.

16. TEST CUSTOMER EVIDENCE AND PROCUREMENT QUALITY

Customer evidence should be classified by economic substance. A research collaboration, memorandum, unpaid demonstration, grant-funded pilot, paid pilot, framework agreement, purchase order, accepted deployment and renewal represent different levels of commitment. The acquisition model should not apply one conversion rate to all.

The buyer should identify the risk owner and budget source. A quantum innovation team can sponsor a demonstration while the security operations team controls production adoption. A public programme can fund infrastructure without committing an operating budget. The path from experiment to service should name the decision makers, acceptance criteria and procurement steps.

Referenceability also matters. A customer may restrict publicity, architecture disclosure or performance data. Confidential evidence can still support diligence if access is properly

controlled. The buyer should avoid treating an announced partnership as stronger than a quiet paid deployment with measurable usage.

17. SEPARATE PUBLIC FUNDING FROM COMMERCIAL DEMAND

National and regional programmes create testbeds, route infrastructure, procurement opportunities, standards work and technical learning. EuroQCI is developing terrestrial and space components, cross-border links and testing infrastructure. These programmes can reduce development cost and create credible reference environments.

Public funding does not establish broad willingness to pay. It can concentrate demand in grant cycles, national suppliers or policy priorities. The target should show which revenues depend on a programme, whether follow-on funding is available, and who pays for operation after a project ends.

The buyer should value public-programme access as a specific capability: eligibility, consortium position, route access, certification knowledge or customer relationship. It should avoid capitalising the full programme budget as target revenue.

18. CALCULATE REVENUE QUALITY AFTER DELIVERY BURDEN

Revenue quality depends on cash collection, gross margin, acceptance risk, concentration, recurrence and delivery effort. QKD contracts can include hardware, engineering, installation, research, maintenance and managed service. Each stream should be modelled separately.

Paid pilots can be valuable when they fund reusable integration, produce acceptance evidence and create a credible expansion path. They are less valuable when bespoke scope, grant subsidy or founder intervention prevents replication. The buyer should measure engineering hours, hardware use, travel, partner fees and support alongside invoice value.

Recurring revenue should be tested for genuine recurrence. A maintenance line can carry substantial specialist cost. A managed service can require route availability and replacement inventory. The model should use contribution after complete delivery and support.

Table 3. Evidence-weighting customer revenue

Evidence state	Commercial meaning	Diligence evidence	Valuation treatment
Research collaboration	Technical access and learning	Scope, funding, rights and deliverables	Value transferable learning and access; exclude unsupported recurring revenue
Unpaid demonstration	Customer interest with limited commitment	Named sponsor, acceptance criteria and follow-on decision	Treat as pipeline subject to explicit probability and cost
Paid pilot	Budgeted experiment and integration evidence	Contract, cash, delivery effort, acceptance and expansion gate	Credit paid contribution and reusable assets
Accepted deployment	Operational use under defined service	Acceptance record, telemetry, support and security ownership	Underwrite contracted economics and renewal risk
Repeatable service	Comparable deployments with stable delivery	Cohort margin, implementation time, uptime, renewal and cash conversion	Apply forward valuation only after complete cost and concentration analysis

Weightings are transaction-specific; the categories prevent unlike forms of demand from being treated as equivalent.

19. BUILD UNIT ECONOMICS AROUND A PROTECTED ROUTE

The useful unit is usually a protected route, site pair, managed service or application workflow. Revenue per device can mislead when several devices, nodes and integration services are required. The model should define the complete bill of materials and labour for one accepted unit.

Direct cost should include hardware, testing, installation, route engineering, connectors, licences, partner charges, support, spares, monitoring and warranty. Working capital can be material when equipment is purchased before customer acceptance. The model should show cash conversion as well as accounting margin.

Scaling assumptions should distinguish repeatable platform work from site-specific work. A connector can be reused; every route still requires measurement and commissioning. Certification evidence can be leveraged; major product changes may trigger new evaluation. The model should identify which cost curve can improve and why.

20. MODEL AVAILABILITY AND FALLBACK ECONOMICS

Security services need a defined response to quantum-link interruption. Key buffers can sustain operation for a period. Hybrid key establishment can maintain service using post-quantum or conventional mechanisms. The fallback may preserve availability while changing the security assurance.

The customer contract should describe service state, alarms, fallback, restoration and reporting. The buyer should verify that applications behave safely when keys are delayed, exhausted or rejected. Failure should not create silent downgrade.

Fallback economics include redundant routes, spare equipment, field response, additional cryptographic licences and operating procedures. These costs belong in the integration bill. A robust hybrid architecture can improve adoption by allowing a phased deployment; it should be valued through customer evidence rather than assertion.

21. IDENTIFY CONCENTRATION AND ECOSYSTEM DEPENDENCIES

Early QKD markets can concentrate around governments, telecom operators, research networks, defence-adjacent programmes, financial institutions and critical infrastructure. A few customers or national programmes may represent most revenue. Several contracts can share the same budget source or procurement authority.

The target may also depend on encryptor vendors, fibre operators, cloud platforms, system integrators, component suppliers and certification laboratories. The buyer should map revenue and delivery to these ecosystem relationships. It should inspect exclusivity, change-of-control, liability, support and termination provisions.

A strong partnership creates value when rights, responsibilities and economics are transferable. A press release or informal technical cooperation does not. The transaction should obtain required consents before closing.

22. EVALUATE PRODUCT-ROADMAP COMPATIBILITY

The buyer and target may pursue different architectures, standards profiles, hardware platforms or customer segments. Integration can destroy value if the combined roadmap forces customers to migrate, invalidates assurance evidence or distracts critical engineers.

The roadmap review should compare product boundaries, release cycles, interfaces, support commitments, certifications and technical milestones. It should identify which components will be retained, integrated, sunset or sold separately. Customer communication should follow a tested migration plan.

The combined company should preserve optionality where standards and demand remain unsettled. Modular interfaces, documented data models and separable components can support multiple architectures. The buyer should avoid funding every possibility without an evidence gate.

23. DESIGN THE INTEGRATION OPERATING MODEL

The integration operating model should name accountable leaders for technology, product, security, customers, operations, finance and people. Scientific decisions and commercial decisions require a shared evidence framework. Neither function should be able to convert an internal milestone into an external claim without review.

The first hundred days should protect customer service, retain key staff, secure repositories, establish configuration baselines and reconcile product claims. It should also create a joint integration backlog with cost, owner, dependency, acceptance test and customer relevance.

The target may need some operational independence while products and certifications remain distinct. The buyer should define decision rights and escalation. Excessive separation can delay synergies; premature consolidation can break evidence and customer trust. The appropriate structure follows the integration risks.

24. USE A VALUE BRIDGE RATHER THAN A HEADLINE MULTIPLE

A headline revenue multiple is weak when revenue mixes research, hardware, grants and services. A more defensible bridge begins with transferable assets and contracted contribution, then adds evidence-weighted commercial options and buyer-specific synergies. It deducts the complete integration bill, capital required, customer concentration and execution risk.

Transferable assets include verified designs, software, documentation, intellectual property, certification evidence, route access, connectors, customer contracts and retained teams. Options include workflows that can be reached through defined integration and acceptance milestones. Synergies should be included only when the buyer has the channel, product and execution capacity to realise them.

The bridge should show a range and the variables that move it. It should avoid converting uncertain pipeline into precise enterprise value. Transaction terms can preserve upside while protecting the buyer from paying immediately for unverified adoption.

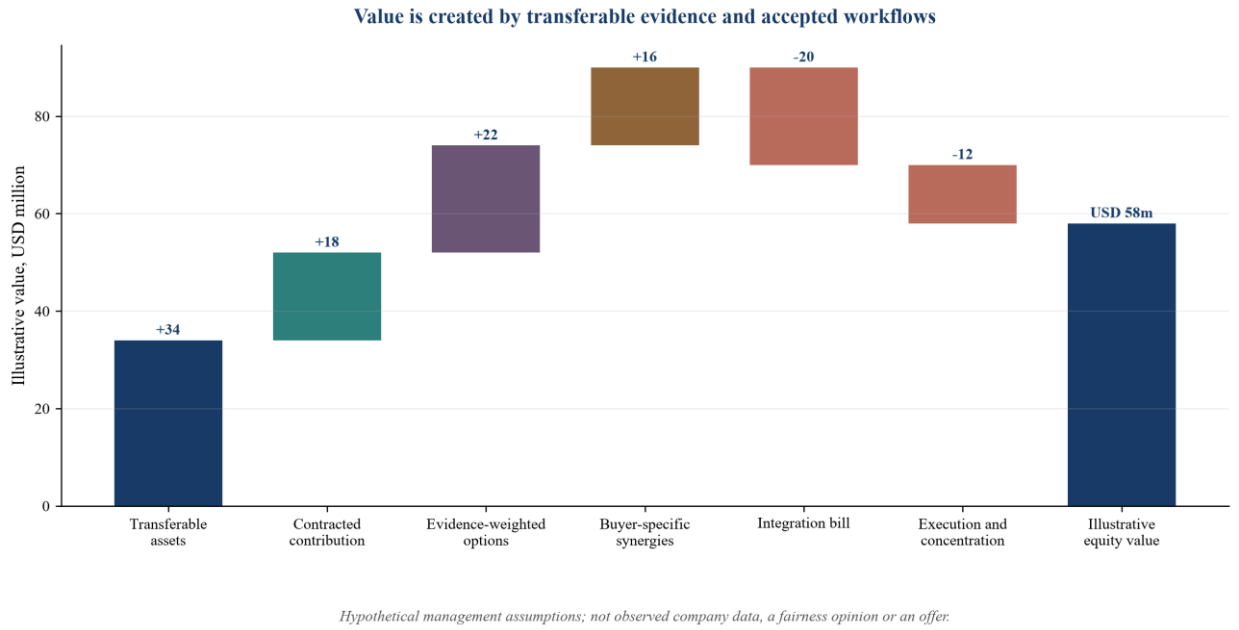

Figure 3. Illustrative QKD acquisition value bridge

All amounts are hypothetical management assumptions and do not represent an observed company, market valuation or transaction opinion.

25. APPLY TRANSACTION TERMS TO UNRESOLVED EVIDENCE

Milestone-linked consideration can align price with integration evidence. An earn-out can depend on accepted deployments, recurring contribution, certified product release or multi-vendor interoperability. The metric should be objective, auditable and within the influence of the selling shareholders where appropriate.

Escrow or holdback can address specific remediation, intellectual-property or customer-consent risks. Completion conditions can require critical employee arrangements, licence transfers, source-code access or regulatory approvals. Representations should match the technical and commercial evidence reviewed.

The buyer should avoid an earn-out based solely on reported revenue when revenue can be accelerated through low-margin bespoke work. Contribution, cash collection and acceptance may provide stronger alignment. The terms should also prevent the buyer from unintentionally frustrating achievement through integration decisions.

26. CREATE AN EVIDENCE-BASED DILIGENCE WORKPLAN

The workplan should begin with the target workflow, then trace evidence through architecture, performance, security, operations, customers and economics. Specialists should review raw evidence alongside management presentations. Findings should be linked to valuation, integration or transaction protection.

Technical diligence should reproduce selected results, inspect design and software, test interfaces, review field data and evaluate productisation. Security diligence should examine threats, authentication, key handling, implementation weaknesses, monitoring and vulnerability management. Commercial diligence should verify customer scope, budgets, acceptance, alternatives and delivery effort.

Financial diligence should reconcile revenue, grants, hardware, services, gross margin, working capital and cash. Legal diligence should examine intellectual property, funding obligations, export controls, data, customer contracts, partners and change-of-control. The streams should meet around one dependency register.

Table 4. QKD M&A diligence and decision gates

Workstream	Primary tests	Decision output	Transaction response
Technology	Reproduce performance; inspect route fit, productisation and roadmap	Verified operating envelope and remaining engineering	Price adjustment, milestone or funded development plan
Cybersecurity and assurance	Review threats, authentication, key handling, side channels and certification	Assurance boundary and remediation cost	Condition, covenant, indemnity or integration reserve
Commercial	Verify workflows, budget owners, alternatives, acceptance and repeatability	Evidence-weighted demand and revenue quality	Forecast adjustment and earn-out metric
Operations and supply chain	Test monitoring, support, manufacturing, spares and dependencies	Complete delivery cost and resilience plan	Working-capital provision, supplier consent or TSA
Finance and legal	Reconcile cash, grants, rights, contracts and liabilities	Transferable value and contingent exposure	Purchase-price bridge, escrow and closing conditions

Each workstream should produce a transaction decision, an integration action or a priced risk.

27. APPLY A HYPOTHETICAL ACQUISITION CASE

Consider a hypothetical target that sells point-to-point QKD appliances, a key-management layer and integration services. It has two accepted paid pilots, three grant-funded testbed deployments and a pipeline of proposed projects. It depends on one detector supplier and one encryptor partner. Its current architecture supports dedicated metro fibre and a proprietary application connector.

Illustrative management assumptions place current annual revenue at USD 9 million, of which USD 3 million is grant-linked research and USD 4 million is hardware and engineering. Collected contribution after direct delivery is assumed at USD 1.8 million. The company holds USD 11 million of cash and uses USD 13 million annually. Management estimates USD 20 million of engineering and operating expenditure to complete a standardised key-management interface, assurance programme and three reference deployments.

Every amount, customer characteristic, probability and outcome in this case is hypothetical. The case is designed to demonstrate the framework. It is not observed company data, a market forecast, a fairness opinion, an investment recommendation or an offer.

28. MAP THE HYPOTHETICAL WORKFLOW AND ALTERNATIVES

The target's strongest workflow is a high-value metro data-centre interconnect operated on controlled fibre. The customer has a funded cryptographic-modernisation programme, dedicated security ownership and an existing encryptor estate. The QKD architecture would supply keys through a key-management connector and retain post-quantum authentication and fallback.

The alternative is a post-quantum migration across the existing network without dedicated optical equipment. The QKD-led hybrid requires higher capex, route engineering and specialist support. Its potential value lies in diversifying key-establishment mechanisms on a small number of critical links. The customer should decide whether that incremental assurance justifies the complete cost.

The buyer should value the target's two accepted pilots as evidence for a bounded workflow. It should exclude broad enterprise demand that has not been tested. It should model expansion after standard interface, operational telemetry and contribution targets are met.

29. BUILD THE HYPOTHETICAL INTEGRATION BILL

The illustrative bill totals USD 20 million: USD 4.2 million for route and optical engineering, USD 5.8 million for key-management interfaces and application connectors, USD 3.1 million for assurance and certification, USD 4.7 million for operations and support, and USD 2.2 million for programme management and contingency.

The bill is staged. The first tranche establishes the production architecture, interface baseline and supplier plan. The second completes multi-vendor tests and customer acceptance. The third funds assurance continuity, support tooling and repeatable delivery.

The buyer should treat the bill as part of invested capital. If sellers claim that platform synergies remove the cost, the diligence team should identify the actual people, products and evidence that do so. An unstaffed synergy is not a reduction.

30. CONSTRUCT THE HYPOTHETICAL VALUE BRIDGE

Assume transferable technology, team and customer assets support a value range centred on USD 34 million. Contracted contribution and accepted deployments add USD 18 million. Evidence-weighted options add USD 22 million and buyer-specific distribution and product synergies add USD 16 million. The model deducts the USD 20 million integration bill and USD 12 million for concentration and execution risk, producing an illustrative equity value of USD 58 million before customary debt, cash and transaction adjustments.

The result is not a market valuation. It shows how value moves when evidence changes. If the standard connector fails, the option value and synergies fall while the integration bill rises. If three customers accept the combined service at target contribution, contracted value and repeatability improve.

The bridge supports transaction design. The buyer could pay for transferable assets at closing and release contingent consideration after multi-vendor interoperability, accepted production deployment and collected contribution are independently verified.

31. STRESS-TEST CUSTOMER ADOPTION

The base case should test slower security approval, procurement delay, limited route availability and a lower willingness to pay. Each delay increases cash need and can reduce employee retention. The model should separate technical completion from customer acceptance.

The buyer should also test a policy scenario in which target customers choose post-quantum cryptography without QKD. Residual value may remain in key management, photonics,

deployment capability or public-programme access. The acquisition case should identify that downside before signing.

Adoption can improve if the service is packaged around a specific workflow, uses standard interfaces and integrates with existing monitoring and fallback. The buyer should fund those capabilities against acceptance evidence, not generic market forecasts.

32. STRESS-TEST STANDARDS AND CERTIFICATION CHANGE

The QKD standards environment continues to develop. ETSI has active work on monitoring, architecture, orchestration, authentication and implementation security. ITU recommendations continue to expand interworking and integration. A product can comply with one profile and still require change for another market or customer.

The model should estimate interface maintenance, conformance testing, recertification and product migration. It should identify design choices that preserve compatibility. Modular key-management and monitoring layers can reduce dependence on one optical protocol or vendor.

The buyer should not assume that future standards will validate the target's current architecture. Standards can commoditise proprietary interfaces or expose gaps. Participation creates information value; implemented conformance creates transaction value.

33. STRESS-TEST SUPPLY AND OPERATING RESILIENCE

A detector shortage, specialist departure or failed field unit can delay acceptance and cash. The buyer should test alternate suppliers, inventory, repair time, remote diagnostics and support staffing. It should include import, export and security restrictions where relevant.

Service resilience should be tested during quantum-link failure, key-manager failover, network change and software upgrade. The customer should receive an explicit security state and documented fallback. Silent degradation is unacceptable.

The integration plan should establish incident ownership across the target, buyer, network operator, encryptor vendor and customer. Contractual responsibility should align with technical control.

34. GOVERN CLAIMS AFTER CLOSING

Quantum security attracts strong public interest. The combined company should establish a claims-review process covering product, sales, investor and public communications. Claims should identify the protocol, implementation, operating conditions, authentication, certification and limits.

The buyer should preserve raw evidence and version history. A result achieved under one configuration should not migrate to another product release without validation. Customer case studies should state the deployed workflow and acceptance basis.

Accurate claims reduce diligence friction, regulatory exposure and customer disappointment. They also help the company distinguish genuine integration capability from broad quantum language.

35. EXECUTE A HUNDRED-DAY INTEGRATION PLAN

During the first thirty days, the buyer should secure repositories, equipment, customer service, critical staff and configuration baselines. It should confirm intellectual-property access, supplier continuity and current product claims. It should create the joint dependency register and freeze uncontrolled interface changes.

During days thirty-one to sixty, teams should reproduce priority tests, validate the key-management architecture, map customer workflows, complete route and supply assessments and confirm the integration bill. Commercial teams should contact customers under an agreed communication plan.

During days sixty-one to one hundred, the combined company should approve the product boundary, interface roadmap, assurance plan, operating model and evidence-gated investment schedule. It should stop or defer initiatives that lack a funded workflow or strategic option value.

36. USE EXPLICIT INVESTMENT AND TRANSACTION RULES

Proceed when the target has a defined customer workflow, reproducible technical evidence, compatible routes, transferable rights, implemented interfaces, an assurance path and sufficient capital to reach acceptance. Price verified assets and contracted contribution at closing. Stage uncertain adoption and synergies.

Proceed with conditions when the science is credible but integration, certification, route access or customer acceptance remains incomplete. Fund the specific evidence path. Use milestones, reserves, covenants and contingent consideration.

Pause when performance cannot be reproduced, key handling is opaque, customer demand cannot be distinguished from grants, critical rights are unstable, the integration bill is unknown or the buyer cannot support the operating model. A pause preserves negotiating leverage and prevents enthusiasm from becoming irreversible cost.

37. LIMITATIONS

The framework does not establish that QKD is appropriate for every security workflow or jurisdiction. Threat models, routes, cryptographic policy, standards, certification and customer economics differ. Technology and policy positions can change.

The hypothetical case excludes tax, detailed purchase accounting, financing structure, foreign exchange, regulatory approval, export licensing and jurisdiction-specific legal advice. All numerical inputs are hypothetical management assumptions. They should not be used as market benchmarks.

Transaction teams should supplement the framework with specialist quantum, optical, cybersecurity, network, accounting, tax, regulatory and legal diligence. Customer security owners should determine the acceptable architecture and residual risk.

38. CONCLUSION

QKD acquisition value is created when quantum-generated keys become a secure, accepted and supportable customer workflow. Optical performance is necessary. Integration determines

whether it produces commercial value. The buyer must connect route engineering, key management, applications, assurance, operations and customer economics.

The Quantum Integration Economics Framework makes those dependencies visible. It prices the complete integration bill, compares workflow-specific alternatives, weights revenue by acceptance and delivery burden, and uses transaction terms to align consideration with evidence. Current ITU and ETSI standards make interfaces and tests more concrete. Public infrastructure and certification initiatives create valuable learning and procurement access. Post-quantum cryptography remains a powerful alternative and part of many hybrid architectures.

The decisive diligence question is practical: what funded security workflow will operate after closing, at what total cost, with what verified assurance and under whose responsibility? A transaction that can answer that question has an investable integration thesis. A transaction that cannot should remain conditional.

REFERENCES

[1] International Telecommunication Union, Recommendation ITU-T Y.3800, Overview on Networks Supporting Quantum Key Distribution, 2019, https://www.itu.int/rec/T-REC-Y.3800

[2] International Telecommunication Union, Recommendation ITU-T Y.3801, Functional Requirements for Quantum Key Distribution Networks, 2020, https://www.itu.int/rec/T-REC-Y.3801

[3] International Telecommunication Union, Recommendation ITU-T Y.3802, Quantum Key Distribution Networks Functional Architecture, 2020 with 2023 amendment, https://www.itu.int/epublications/publication/itu-t-y-3802-2020-amd-1-2023-11

[4] International Telecommunication Union, Recommendation ITU-T Y.3803, Quantum Key Distribution Networks Key Management, 2020, https://www.itu.int/rec/T-REC-Y.3803

[5] International Telecommunication Union, Recommendation ITU-T Y.3810, Quantum Key Distribution Network Interworking Framework, 2024, https://www.itu.int/rec/T-REC-Y.3810

[6] International Telecommunication Union, Recommendation ITU-T Y.3813, Quantum Key Distribution Network Interworking Functional Requirements, 2024, https://www.itu.int/rec/T-REC-Y.3813

[7] International Telecommunication Union, Recommendation ITU-T Y.3818, Quantum Key Distribution Network Interworking Architecture, 2024, https://www.itu.int/rec/T-REC-Y.3818

[8] International Telecommunication Union, Recommendation ITU-T Y.3820, Quantum Key Distribution Network Interworking Software-Defined Networking Control, 2024, https://www.itu.int/epublications/publication/itu-t-y-3820-2024-09-quantum-key-distribution-network-interworking-software-defined-networking-control

[9] International Telecommunication Union, Recommendation ITU-T Y.3831, Integration of Quantum Key Distribution Network and User Networks Supporting End-to-End Modern Cryptography Services, 2025, https://www.itu.int/rec/T-REC-Y.3831-202512-I

[10] International Telecommunication Union, Recommendation ITU-T Y.3832, Quantum Key Distribution Networks Framework for Orchestration, 2025, https://www.itu.int/rec/T-REC-Y.3832-202512-I

[11] International Telecommunication Union, Recommendation ITU-T Q.4165, Quantum Key Distribution Network Interworking Protocol Framework, 2026, https://www.itu.int/epublications/en/publication/itu-t-q-4165-2026-01-quantum-key-distribution-network-interworking-protocol-framework

[12] International Telecommunication Union, Technical Report TR.SQKDN, Standardization Consideration of Satellite-Based Quantum Key Distribution Networks, 2025, https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-QKD-2025-1-PDF-E.pdf

[13] European Telecommunications Standards Institute, Quantum Key Distribution Work Programme and Published Standards, accessed September 2026, https://www.etsi.org/technical-groups/qkd/

[14] European Telecommunications Standards Institute, ETSI GS QKD 020 V1.1.1, Protocol and Data Format of REST-Based Interoperable Key Management System API, 2026, https://www.etsi.org/deliver/etsi_gs/QKD/001_099/020/01.01.01_60/gs_qkd020v010101p.pdf

[15] European Telecommunications Standards Institute, ETSI GR QKD 007 V1.2.1, Vocabulary, 2026, https://www.etsi.org/deliver/etsi_gr/QKD/001_099/007/01.02.01_60/gr_qkd007v010201p.pdf

[16] European Telecommunications Standards Institute, ETSI GS QKD 016 V2.1.1, Common Criteria Protection Profile for a Pair of Prepare-and-Measure QKD Modules, 2024, https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/02.01.01_60/gs_QKD016v020101p.pdf

[17] UK Department for Science, Innovation and Technology, Quantum Key Distribution Research Report, 2026, https://www.gov.uk/government/publications/quantum-key-distribution-research-report/quantum-key-distribution-research-report

[18] UK National Cyber Security Centre, Quantum Security Technologies, 2026, https://www.ncsc.gov.uk/paper/quantum-security-technologies

[19] UK National Cyber Security Centre, Quantum Networking Technologies, 2026, https://www.ncsc.gov.uk/sites/default/files/pdfs/publication/quantum-networking-technologies.pdf

[20] National Institute of Standards and Technology, What Is Quantum Cryptography?, 2025, https://www.nist.gov/cybersecurity-and-privacy/what-quantum-cryptography

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

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

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

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

[25] 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

[26] European Union Agency for Cybersecurity, EUCC Certification Scheme, accessed September 2026, https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

[27] European Union Agency for Cybersecurity, Quantum Key Distribution Briefing, https://www.enisa.europa.eu/sites/default/files/publications/Briefing_Quantum_Key_Distribution.pdf

[28] International Organization for Standardization, ISO/IEC 23837-1:2023, Security Requirements, Test and Evaluation Methods for Quantum Key Distribution, 2023, https://www.iso.org/standard/81287.html

[29] IFRS Foundation, IFRS 3 Business Combinations, https://www.ifrs.org/issued-standards/list-of-standards/ifrs-3-business-combinations/

[30] 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.