Entrokey Labs

Executive Summary

A Software-Defined Paradigm for Quantum-Resistant Security

Abstract

This document provides a comprehensive overview of the imminent quantum computing threat to global security and the unique, disruptive market opportunity for Entrokey Labs. Entrokey presents a patented, software-only solution that addresses the flaws of hardware-based Quantum Key Distribution (QKD), offering unparalleled cost savings, scalability, and rapid deployment to mitigate a $1.85 trillion crisis. This analysis is structured to inform strategic investment and executive decision-making. All statistics within this report are sourced from credible, publicly available data, with a full citation list provided in the accompanying documentation.

Prepared by Cambridge Frontier Technologies

August 7, 2025

1. Executive Overview: The Trillion-Dollar Quantum Security Crisis

The advent of cryptographically relevant quantum computing represents an existential threat to the integrity of global data security. Current encryption standards will be rendered obsolete, exposing the world's most sensitive government, corporate, and personal data to compromise. This impending reality creates a $1.85 Trillion Total Addressable Market (TAM) for quantum-resistant security solutions, as validated through Monte Carlo simulation modeling[1]. The urgency of this threat cannot be overstated. Adversaries are actively engaged in *"Harvest Now, Decrypt Later"* attacks, exfiltrating and storing encrypted data today with the intent to break it once quantum computers become available. The Global Risk Institute's 2024 report projects a **10% probability of a quantum breach by 2027-2028**[2], a risk threshold that, in meteorology, would trigger widespread emergency alerts for a tornado. The global response must be equally decisive.

Current hardware-based Quantum Key Distribution (QKD) solutions, while conceptually sound, are operationally and financially untenable for widespread adoption, requiring an estimated $1.37 Trillion in new global infrastructure. Entrokey Labs introduces the definitive alternative: a proprietary, patented, software-only quantum-resistant encryption platform. The Entrokey solution eliminates the need for any new hardware, deploys over existing network infrastructure, significantly reduces total ownership costs, and secures global assets in days rather than years. While other companies are still developing their solutions, Entrokey's platform is available today, offering a decisive first-mover advantage. This positions Entrokey Labs to capture a $20 Billion Serviceable Obtainable Market (SOM) by democratizing access to quantum-safe security for all sectors. While Post-Quantum Cryptography (PQC) algorithms provide a vital baseline for security, Entrokey's software-only QKD offers a higher level of assurance against future computational threats. It is critical to distinguish Entrokey's approach from "software-enabled" competitors, who still require specialized hardware, thereby failing to solve the core issues of cost and scalability.

2. Market Analysis and Opportunity

The demand for quantum-safe solutions is accelerating, driven by government mandates and heightened private sector awareness. The hardware QKD market, despite its significant limitations, serves as a clear indicator of this growing urgency. Market research firms project the hardware QKD segment to grow from $484 million in 2024 to $2.63 billion by 2030, reflecting a compound annual growth rate of 32.6%[3]. This growth demonstrates a clear market pull for the security principles of QKD.

However, the growth of hardware-based solutions is fundamentally constrained by several inherent flaws. Primarily, the extreme cost of deployment requires specialized fiber optic cables, which cost between $60,000 and $80,000 per mile to install[4], and even quantum satellites priced at €280 million each[5]. Furthermore, these systems suffer from severe distance limitations, typically becoming ineffective beyond 100 kilometers, which prevents true global security without a chain of trusted nodes that themselves introduce vulnerabilities. This physical inflexibility is compounded by slow deployment timelines, often exceeding two years for a modest enterprise installation. Entrokey's proposed software solution would capture demand from organizations

[1] Market sizing derived from 10,000-scenario Monte Carlo simulation analyzing security transition costs (0.05-1.5% of global GDP) and infrastructure requirements (fiber networks, quantum satellites, and repeaters). The underlying models account for projected global GDP growth rates, technology adoption curves, and increased digitization.

[2] Global Risk Institute & evolutionQ, 2024 Quantum Threat Timeline Report.

[3] Markets and Markets, "Quantum Key Distribution Market", 2024. Projections are corroborated by Grand View Research, which estimates a 33.5% CAGR.

[4] The Network Installers, Fiber Installation Cost Data.

[5] European Space Agency, Quantum Satellite Program Data.

deterred by these barriers, offering the security promise of QKD with the scalability and cost-effectiveness of a modern software platform.

3. Technology Advantages and Scalability

Entrokey's core proposal is a paradigm shift from physical to software-defined quantum security. This approach has the potential to deliver overwhelming technical and financial advantages, chief among them being the elimination of any new infrastructure requirements. The proposed Entrokey solution operates over existing enterprise and public networks, removing the need for dark fiber, specialized repeaters, or dedicated physical appliances. The system is designed for seamless integration with virtually any existing security architecture, making adoption frictionless.

This software-centric model collapses the deployment timeline from years to days, enabling organizations to quickly achieve a quantum-resistant posture. While a typical hardware QKD deployment involves extensive planning, procurement, physical installation, and testing cycles that can span over 20 months, the Entrokey platform can be provisioned, configured, and operational globally in a fraction of that time. This capability for rapid, scalable deployment is a decisive advantage for enterprises facing imminent threats and regulatory deadlines.

4. Financial Implications and Total Cost of Ownership

The financial benefits of Entrokey's software-defined approach would be significant. By eliminating capital expenditures on hardware and the associated operational costs of infrastructure, this solution reduces the 5-year Total Cost of Ownership (TCO) by an average of 90% across all major sectors. This dramatic cost reduction fundamentally changes the market dynamic, making robust quantum security accessible to the entire enterprise market, not just well-funded government agencies or large financial institutions.

This financial model allows organizations to reallocate capital from prohibitive infrastructure projects toward broader security enhancements and core business objectives. The savings are not merely theoretical; they represent a direct and substantial impact on an organization's budget, enabling a more efficient and comprehensive path to quantum readiness.

Table 1: 5-Year TCO Comparison: Hardware QKD vs. Entrokey Software

Deployment Scenario	Hardware QKD Cost	Entrokey Cost	Savings
Single Secure Link	$850,000	$165,000	81%
Regional Bank (5 sites)	$4,500,000	$750,000	83%
Telecom Metro (10 nodes)	$11,000,000	$1,100,000	90%
National Security (Air-gapped)	$9,500,000	$1,200,000	87%

5. Strategic Positioning and First-Mover Advantage

Entrokey Labs is positioned not as an incremental competitor to hardware QKD, but as its market-disrupting successor. Entrokey's strategy is to define and lead a new category of scalable, software-defined quantum resistance, thereby becoming the "QKD democratizer" by targeting the vast majority of the market that is currently priced out of quantum security or paralyzed by the operational complexity of hardware solutions. The first-mover advantage in this software-only space is critical, allowing Entrokey to establish the standard for this new approach.

Entrokey's go-to-market strategy should focus initially on clear beachhead markets, including financial services, telecommunications, and government contractors, all of whom face imme-

diate and intense pressure from both threat actors and regulators. The API-first architecture of the Entrokey platform is designed for seamless integration, making it an ideal solution for channel partners such as cloud providers, Managed Security Service Providers (MSSPs), and system integrators. This channel-friendly model will facilitate rapid market penetration and establish Entrokey as the foundational layer for quantum-safe communications.

6. Risk Mitigation and The Regulatory Imperative

The primary risk to Entrokey's strategy is not technological but rather the market's pace of adoption. This risk, however, is being actively mitigated by a powerful forcing function: stringent and non-negotiable government deadlines for quantum-resistant migration. These regulatory mandates create a ticking clock that compels organizations to act. The process began in 2024 with NIST's publication of final Post-Quantum Cryptography standards. It will intensify as we approach the 2030-2033 window when CNSA 2.0 becomes mandatory for national security systems.

The ultimate deadline is the National Security Memorandum 10 (NSM-10), which mandates that all U.S. national security systems must be fully migrated to quantum-resistant cryptography by **2035**. Failure to meet this deadline constitutes operational failure. Given the multi-year timelines associated with hardware solutions, Entrokey's rapid and cost-effective deployment model represents the only viable path for the majority of public and private sector entities to achieve compliance. By acting now, organizations can protect their data from today's "harvest now, decrypt later" attacks and secure their future in the quantum era. Entrokey Labs provides the essential key to this transition.