A Monte Carlo Simulation for Sizing the Quantum Security Market

Methodological Framework and Results

Cambridge Frontier Technologies
Prepared for Entrokey Labs

August 8, 2025

Abstract

This analysis delineates the methodological framework employed to estimate the global market opportunity for quantum-resistant security solutions. A robust estimation of the total addressable market (TAM), serviceable addressable market (SAM), and serviceable obtainable market (SOM) for these emergent technologies was achieved through a Monte Carlo simulation involving 10,000 iterations. The probabilistic approach was selected to capture the significant uncertainty inherent in nascent technology markets, generating distributions of possible outcomes rather than deterministic point estimates. This method provides a more rigorous foundation for strategic planning, yielding conservative estimates that systematically account for ambiguity in key market drivers across the global quantum security landscape.

Prepared by Cambridge Frontier Technologies

1. Total Addressable Market Analysis

The investigation commences with the Total Addressable Market, which is conceptualized as the aggregation of two principal components. The first component, security transition costs, is modeled as a stochastic percentage of the $100 trillion global Gross Domestic Product. This percentage is drawn from a beta distribution with a range of 0.05% to 1.5%, reflecting diverse expert estimates of cryptographic infrastructure replacement costs across government, enterprise, and critical infrastructure sectors, with the mean cost converging to $480 billion.

This is complemented by the second component, infrastructure investment, which is derived from a bottom-up cost model. This model includes the deployment of 5 to 15 million miles of fiber optic networks at a cost of $60,000 to $80,000 per mile, the launch of 200 to 500 quantum satellites priced between $250 and $350 million each, and additional ancillary infrastructure costs represented by a log-normal distribution with a median of $500 billion. The combined infrastructure investment averages $1.37 trillion, leading to a total TAM estimate of **$1.85 trillion**, with a 90% confidence interval of $1.32 trillion to $2.40 trillion.

2. Serviceable Addressable Market Analysis

Following the establishment of the TAM, the analysis proceeds to define the Serviceable Addressable Market (SAM), which represents the segment of the TAM realistically accessible within a ten-year strategic horizon. This is calculated by applying sector-specific adoption rates, modeled as uniform distributions based on industry analysis, to the TAM. The modeled adoption rates encompass Financial Services at 8-12%, Government and Defense at 10-15%, Critical Infrastructure at 6-10%, Healthcare at 4-8%, and general Enterprise at 5-10%.

To more accurately model the typical S-curve adoption pattern of novel infrastructure technologies, a time-decay factor, governed by a beta distribution with parameters α=3 and β=2, is integrated into the model. This mathematical formulation accounts for the reality that technological adoption follows predictable patterns, with early phases characterised by slower uptake followed by rapid acceleration and eventual saturation. The resulting SAM is estimated to be **$490 billion**, with a 90% confidence interval of $240 billion to $760 billion.

3. Serviceable Obtainable Market Analysis

The final analytical stage refines the SAM to determine the Serviceable Obtainable Market (SOM) by integrating factors related to competitive dynamics and specific execution capabilities. These variables include probabilistic technology adoption rates that favor software-based solutions, modeled with a beta distribution; the significant impact of a projected 85% to 95% cost advantage over hardware-centric alternatives; the potential for a first-mover to capture up to 30% of the market; and adjustments for technology maturity and execution risk.

Furthermore, the model incorporates network effects, which are subject to diminishing returns and capped at a twofold multiplier. Network effects represent the increasing value proposition as more entities adopt the quantum security solution, creating a positive feedback loop that enhances market penetration potential. The confluence of these factors suggests an average market penetration of 4.5%, yielding a final SOM estimate of **$20 billion**, with a 90% confidence interval between $10 billion and $40 billion.

4. Monte Carlo Simulation Results

The Monte Carlo simulation results are presented in Figure 1, which illustrates the probability distributions for each market segment. The visualization demonstrates the spread of outcomes across 10,000 iterations, with clear convergence around the mean estimates while maintaining

realistic confidence intervals that reflect market uncertainties. The distributional approach provides stakeholders with a comprehensive understanding of potential market scenarios, enabling more informed strategic decision-making under uncertainty.

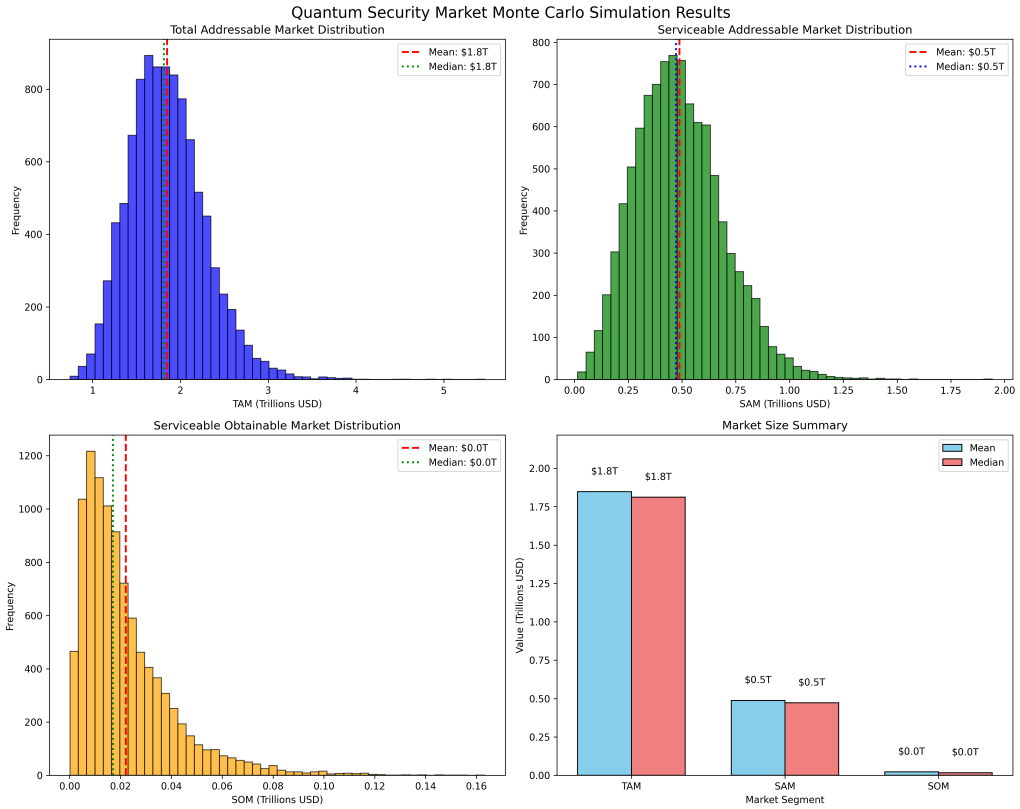

Figure 1: Monte Carlo simulation results showing probability distributions for TAM, SAM, and SOM estimates with 10,000 iterations. The plots demonstrate convergence around mean values while capturing uncertainty through distributional spread, providing a robust foundation for strategic planning in the quantum security sector.

The simulation outputs validate the conservative nature of our estimates while demonstrating the methodological rigor applied to this market sizing exercise. The probability distributions reveal well-defined central tendencies with appropriate variance ranges that reflect the inherent uncertainties in emerging technology markets.

5. Methodological Validation and Strategic Implications

In summation, this Monte Carlo approach establishes a robust and methodologically sound foundation for global market sizing within the quantum security sector. The resulting conservative estimates reflect realistic adoption scenarios while formally accounting for a wide array of technological, competitive, and execution uncertainties. The probabilistic framework is particularly valuable as it enables strategic planning across a plausible range of market outcomes, thereby avoiding the analytical fragility of relying on single-point projections for a highly dynamic and uncertain future market.

The methodology employed here represents a significant advancement over traditional market sizing approaches, which often rely on deterministic calculations that fail to capture the inherent uncertainty in emerging technology sectors. By embracing probabilistic modeling, this analysis provides Entrokey Labs with a more nuanced understanding of the market opportunity, complete with confidence intervals that can inform risk assessment and strategic planning

processes.

Note on Post-Quantum Cryptography (PQC)

It is important to contextualize these findings. The simulation models the competitive dynamic between software-based and hardware-based QKD solutions. Post-Quantum Cryptography (PQC), as standardized by NIST, is a critical and direct competitor in this market. While the overall TAM and SAM remain unchanged, PQC's presence shapes the serviceable market, creating a landscape where customers will evaluate PQC, QKD, and hybrid solutions. Entrokey's differentiation is its foundation in information-theoretic security, offering a higher level of assurance against future algorithmic threats that may compromise PQC.