Practitioner Brief

AI IN ASSET MANAGEMENT

Quantum Computing for Finance

Oswaldo Zapata, PhD

Practitioner Brief written by Mark Fortune

CFA Institute Research Foundation

CFA Institute Research & Policy Center

Quantum computing will not remake finance overnight, but practitioners should prepare now. This chapter of *AI in Asset Management: Tools, Applications, and Frontiers* argues for the implementation of near-term, hybrid quantum–classical pilots that target hard optimization, Monte Carlo simulation, and machine learning (ML) while beginning a shift to post-quantum cryptography (PQC) to mitigate "harvest-now, decrypt-later" risk.

Fully reliable, large-scale machines remain a distant aspiration, so value today is derived from practical, small-scale techniques on noisy devices plus disciplined benchmarking against strong classical baselines. This chapter also refreshes ML foundations and highlights workhorses—*k*-Nearest Neighbor (kNN), *k*-means, and principal component analysis (PCA)—for credit, fraud, market/risk analytics, and portfolio design.

Who Should Read This Chapter?

If you steer money or models, this chapter is for you. For practitioners, it:

- shows chief investment officers (CIOs) and portfolio managers where near-term quantum can sharpen portfolio optimization and scenario analysis; gives heads of quant and researchers a clear benchmarking brief—QAOA/VQE for discrete constraints, quantum Monte Carlo for pricing and risk, and early quantum machine learning (QML) where data encoding is tractable;
- helps chief risk officers (CROs) and model-risk teams trust (and audit) noisy intermediate-scale quantum (NISQ)-era outputs with tight governance; guides traders and ML/data engineers to targeted wins that drop into existing pipelines without rewiring the desk;
- hands chief information security officers (CISOs) and security architects a playbook for post-quantum cryptography now, with quantum key distribution (QKD) reserved for ultra-secure links; and
- guides chief technology officers (CTOs) and enterprise architects to design the hybrid tech stack and select vendors, while innovation leads, chief financial officers (CFOs), and Treasury evaluate ROI, partnerships, and potential stress-testing speedups.

November 2025

Why This Chapter Matters Now

Quantum computing is important now because with it, practitioners can capture upside and avoid real risks today. Cyber attackers can grab encrypted data now and decrypt it later. As such, firms should now start moving to PQC. Firms should run small hybrid pilots—quantum approximate optimization algorithm/variational quantum eigensolver (QAOA/VQE) for constrained portfolios and quantum-enhanced Monte Carlo for pricing and risk—to cut run times and test solution quality.

What Does this Chapter Deliver?

- **A clear reality check on quantum today.** It explains the NISQ era, what current hardware can and cannot do, and where that leaves practitioners.
- **An actionable roadmap for pilots.** It shows how to run hybrid quantum–classical proofs of concept in portfolio optimization (QAOA/VQE), quantum-enhanced Monte Carlo, and targeted QML—plus how to benchmark against strong classical baselines.
- **A security playbook.** It lays out why to start post-quantum cryptography now, how to inventory and migrate crypto, when (if ever) to use QKD, and how to handle "harvest-now, decrypt-later" risk.
- **A practical ML refresher.** It recaps supervised/unsupervised/neural methods and the workhorses (kNN, *k*-means, PCA), tying them to areas where quantum may help.
- **Governance and data guidance.** It provides A/B testing rules, validation expectations, and data-pipeline requirements so model risk and audit can sign off.
- **Teams, tools, and next steps.** It names the roles that should engage, suggests a vendor-agnostic stack (with emulation/HPC), and gives checklists and KPIs to move from ideas to results.

"Some experts predict that finance may be one of the first industries to undergo a transformation driven by quantum computing."

Oswaldo Zapata, PhD

Practical Applications

- **Portfolio optimization:** Try small pilots with hybrid quantum–classical methods (QAOA/VQE) on real portfolios; compare solution quality and run time with your best classical tools.
- **Pricing and risk simulations:** Test quantum-style Monte Carlo that needs fewer samples; check accuracy and total time end to end (including setup).
- **Quantum ML (carefully):** Run small experiments on clean datasets for credit scoring or fraud; track any accuracy gains and the cost of loading data into the model.
- **Trading execution/routing:** Frame discrete trading or hedging choices as small optimization problems; see if QAOA cuts slippage or improves fills compared with today's approach.
- **Security upgrade:** Audit your encryption, prioritize data vulnerable to "harvest-now, decrypt-later," and start pilots of post-quantum cryptography; consider QKD only for ultra-secure links.
- **Process and ownership:** Use side-by-side tests, log error-mitigation steps, keep pipelines reproducible, and assign a small cross-functional team to run these pilots.

Practitioner Toolkit

The following provides a guide for how practitioners in key financial roles can apply quantum computing techniques.

Applications of Quantum Computing by Role

Role	Potential Main Benefits	Suggested Primary Applications
CIOs and portfolio managers	Optimization and scenario-analysis gains	Pilot hybrid portfolio optimization and scenario engines; measure against strong classical baselines
Heads of quant and researchers	New algorithms to benchmark (VQAs, QML, quantum Monte Carlo)	Design rigorous A/B tests; publish internal benchmarks vs. classical; build reusable code modules
CROs and model-risk management (MRM) teams	Faster, more reliable risk metrics with strong governance	Trial quantum-enhanced Monte Carlo; define validation standards and controls for NISQ outputs
Traders and ML/data engineers	Targeted latency/quality wins and clean integration	Run small POCs on routing/hedging and fraud/credit models; ensure pipelines and infra integrate cleanly
CISOs and security architects	Migration to post-quantum cryptography; QKD for niche links	Inventory cryptography, prioritize sensitive data, start PQC pilots; evaluate QKD for ultra-secure links
CTOs and enterprise architects	Hybrid stack design and vendor/tool mix	Select tool chains and partners; plan high-performance computing (HPC)/quantum access and orchestration; budget for emulation
Innovation/R&D leads	Proofs-of-concept and partnerships	Stand up sandboxes; manage vendor collaborations; track key performance indicators (KPIs) and learning outcomes
Treasury and anti-money laundering (AML) teams	Simulation speedups for stress testing	Assess quantum Monte Carlo for liquidity and rate stress tests; compare runtime and accuracy
Compliance and internal audit teams	Standards and controls during transition	Align with National Institute of Standards and Technology's PQC timelines; document model governance and crypto migration controls
CFOs and strategy owners	ROI and option value of early capability building	Build staged investment cases; fund small pilots now to buy future scaling option value

Implementation

- **Select the right problems and targets:** Inventory workflows (portfolio optimization, Monte Carlo, select ML), rank by pain/cost, and set success metrics (time-to-solution, quality, cost, robustness).
- **Stand up a lean team and tool chain:** Assign a small cross-functional squad (quant, engineering, security); choose vendor-agnostic software development kits/emulators and arrange limited hardware access.
- **Prep data and strong baselines:** Clean/label datasets; map problems to formulations (e.g., quadratic unconstrained binary optimization [QUBO]/Ising for optimization, amplitude-estimation Monte Carlo); build tuned classical benchmarks and an A/B test plan.
- **Run small pilots in shadow mode:** Implement QAOA/VQE or quantum-style Monte Carlo with shallow circuits; log data-loading and error-mitigation overhead; compare against baselines and iterate quickly.
- **Embed governance and security:** Involve MRM/compliance early; document validation and reproducibility; start post-quantum cryptography pilots and inventory "harvest-now, decrypt-later" exposures.
- **Integrate—or kill—decisively:** If a pilot wins, wrap it as an API/microservice, add monitoring, train users, and budget scale-up; if not, document lessons and move to the next use case.

Metrics That Matter

End-to-end time to result (wall-clock). Measure data load → decision, including encoding, transpilation, and error-mitigation overhead.

Solution quality and feasibility (optimization). Track objective, P&L/risk, and constraint violations; speed is useless if rules break or returns lag.

Accuracy/error for simulations and ML. Use root mean square error/confidence interval (RMSE/CI) for Monte Carlo and AUC/KS/F1 (area under the ROC curve/Kolmogorov–Smirnov/F1 score) for classification.

Robustness and reproducibility. Check variance across shots/seeds and stability under noise/hyperparameters. Model risk, audit, and production must be reliable.

Cost-to-quality efficiency. Dollars (or compute hours) per unit of accuracy or basis-point improvement, used to prove ROI against well-tuned classical baselines.

Quantum-safe coverage. Share of systems and data flows migrated to post-quantum cryptography and reduction in "harvest-now, decrypt-later" exposure, thereby cutting immediate security risk.

Glossary

Hybrid quantum–classical methods: Workflows pairing small quantum routines with classical optimizers to tackle hard problems on current hardware.

Noisy intermediate-scale quantum (NISQ): Today's era of small, error-prone quantum chips; favors short circuits and hybrids. Fault tolerance is years away.

Quantum approximate optimization algorithm (QAOA): Hybrid algorithm for discrete/combinatorial optimization, such as constrained portfolio selection.

Quantum key distribution (QKD): Physics-based key exchange that detects eavesdropping; powerful but niche due to cost and infrastructure limits.

Post-quantum cryptography (PQC): Encryption/signature schemes designed to resist quantum attacks.

Variational quantum eigensolver (VQE): Hybrid method recasting problems as energy minimization; useful for mapping some portfolio choices to quantum form.

Related Content

Pisaneschi, Brian. 2025. "Agentic AI for Finance: Workflows, Tips, and Case Studies." CFA Institute Research and Policy Center. https://rpc.cfainstitute.org/research/the-automation-ahead-content-series/agentic-ai-for-finance.

Spyrou, Alex, and Brian Pisaneschi. 2024. "Practical Guide for LLMs in the Financial Industry." CFA Institute Research and Policy Center. https://rpc.cfainstitute.org/research/the-automation-ahead-content-series/practical-guide-for-llms-in-the-financial-industry.

Tait, James. 2025. "Synthetic Data in Investment Management." CFA Institute Research and Policy Center. https://rpc.cfainstitute.org/research/reports/2025/synthetic-data-in-investment-management.

Wilson, Cheryll-Ann. 2025. "Explainable AI in Finance: Addressing the Needs of Diverse Stakeholders." CFA Institute Research and Policy Center. https://rpc.cfainstitute.org/research/reports/2025/explainable-ai-in-finance.

CFA Institute Research Foundation

CFA Institute Research & Policy Center

Find *AI in Asset Management: Tools, Applications, and Frontiers* and more on the CFA Institute Research and Policy Center website: https://rpc.cfainstitute.org.

Read the full chapter