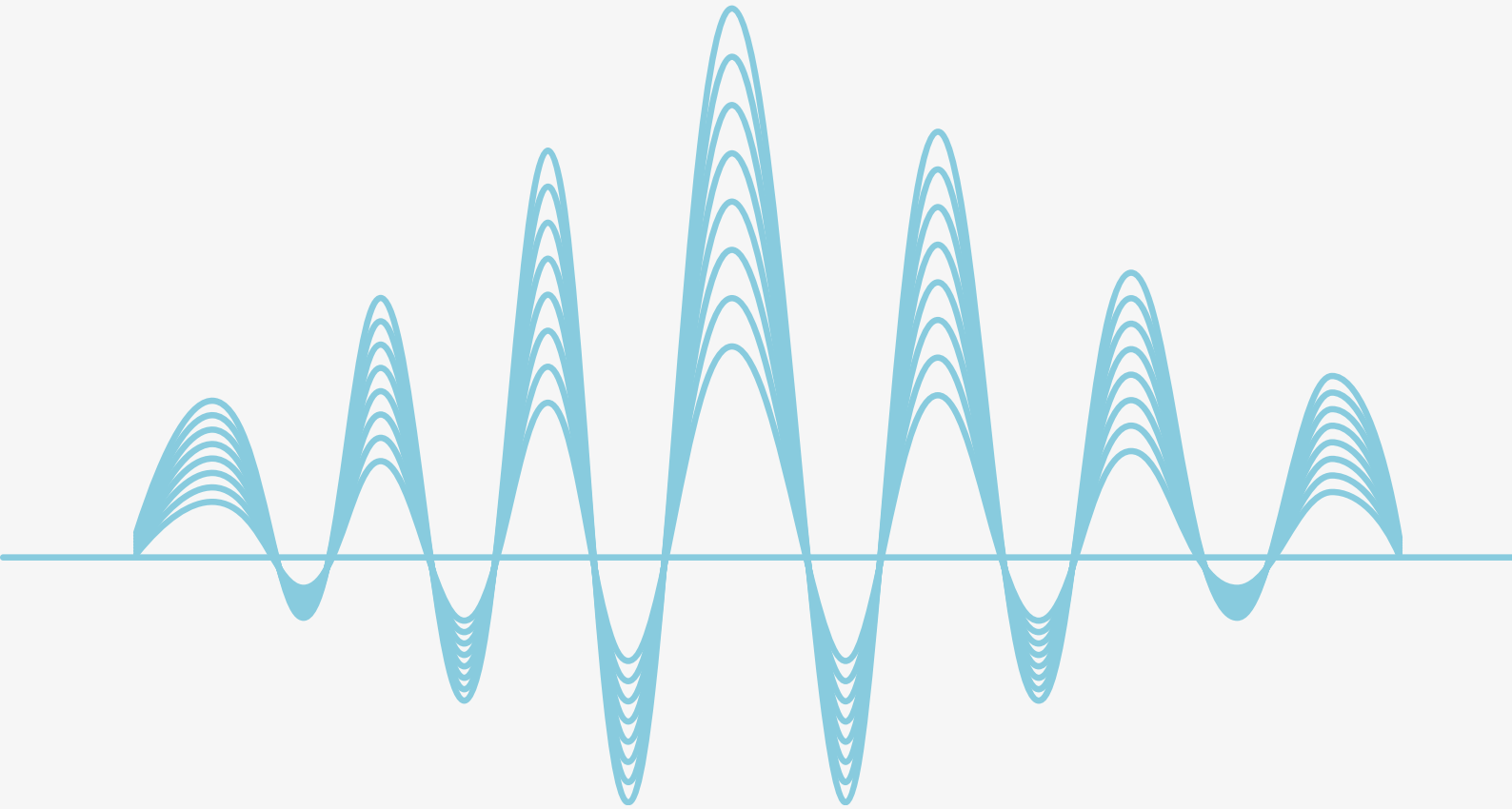
apexanalytix.

The Quantum Paradox

Separating Hype From Reality For Supply Chain Leaders



By William McNeill and Akhilesh Agarwal

Contents:

Executive Summary

Quantum computing represents one of the most consequential yet misunderstood technology shifts facing global supply chains. Often framed as distant or purely academic, it is simultaneously overhyped in the near term and underestimated in its long-term implications for supply chain risk management, data resilience, and competitive advantage. This creates a paradox: quantum computing may pose significant future disruption at the same moment many organizations believe it requires no immediate attention.

On one side of this paradox, quantum computing introduces real long-term risk to today's supply chains. Sensitive supplier data, contracts, pricing models, and risk assessments are routinely exchanged across complex, multi-tier ecosystems, and adversaries are already pursuing "harvest now, decrypt later" strategies that could undermine current encryption in the future. These realities raise important questions about data longevity, supplier exposure, regulatory compliance, and the durability of existing risk controls.

On the other side, quantum computing holds the potential to fundamentally improve how supply chains operate. Advances in optimization, scenario modeling, and complex system analysis could enable more resilient sourcing strategies, better risk forecasting, and faster responses to disruption. Organizations that understand and prepare for these capabilities may gain meaningful advantages over those that wait.

What is Quantum Computing?

Quantum is a new approach that tackles problems traditional computers struggle with. Quantum takes a fundamentally different approach from today's computers by using qubits instead of the silicon-based binary bits found in classical systems. While a traditional bit is always a 0 or a 1, representing states of off and on, a qubit can represent multiple states at the same time, allowing quantum computers to explore many possible solutions in parallel.

For business audiences, the technical details matter less than the implication: by processing information in this new way, quantum computers have the potential to tackle highly complex optimization and risk problems, like those found in supplier networks, that quickly overwhelm conventional computing methods. In theory, a sufficiently advanced quantum computer could evaluate complex problems in minutes or hours that would take even the fastest classical supercomputers years to fully analyze.

The Threat of Quantum

As organizations enter 2026, many are relying on current encryption standards to protect their most sensitive data: supplier invoices and payment information, commercial contracts and pricing terms, banking and account details, and compliance and regulatory records. On the surface, everything appears secure.

However, adversaries are not attempting to break encryption today. They are quietly collecting it. This strategy, known as Harvest Now, Decrypt Later (HNDL), is not theoretical: it is actively happening. Nation-state actors and advanced persistent threat groups are systematically harvesting encrypted data and storing it for future decryption once quantum computing capabilities mature.

The implications are profound. Data encrypted today using RSA or Elliptic Curve Cryptography (ECC) will remain vulnerable indefinitely. When quantum computers reach sufficient capability, adversaries will be able to retroactively decrypt years of captured communications, transactions, and proprietary information.

The Promise of Quantum

While quantum computing poses significant security challenges, it simultaneously represents one of the most transformative business opportunities of the coming decade.

Organizations that successfully navigate the security transition while positioning themselves to leverage quantum capabilities will gain substantial competitive advantages across multiple business dimensions. For supply chain leaders, the promise of quantum computing lies in its potential to tackle problems that are currently computationally constrained such as optimizing supplier selection and allocation across thousands of variables, uncovering hidden concentration and dependency risks buried deep within multi-tier supplier networks, and stress-testing supply chains against an expanded range of disruption scenarios.

Quantum-enabled optimization could allow organizations to evaluate tradeoffs between cost, resiliency, compliance, and sustainability in near real time, rather than relying on static models or simplified assumptions. Over time, these capabilities may enable rapid re-optimization of supply plans in response to shocks, more accurate forecasting of systemic risk, and better-informed sourcing decisions that balance efficiency with resilience: reshaping how organizations design, manage, and protect their supply chains.

Quantum computing is no longer a distant theoretical concern. It's a practical risk that organizations must plan for today.

As post-quantum cryptography (PQC) standards solidify and external pressures mount, waiting to act only increases cost, complexity, and exposure. From partner and insurance demands to emerging regulations and talent constraints, the forces driving PQC adoption are converging faster than many leaders expect.

While quantum computing may be in the distant future, post-quantum cryptography is not. It's here today. The following seven reasons explain why forward-looking organizations are deploying PQC now rather than reacting later.

1 Business Partner Requirements

Business partners are increasingly driving post-quantum cryptography adoption through security requirements and procurement expectations. Large enterprises and public-sector organizations, in particular, are beginning to assess quantum risk across their supply chains to protect long-lived and shared data.

Vendors that cannot demonstrate a credible PQC roadmap may face longer sales cycles, additional audits, or outright disqualification.

As these expectations cascade downstream, even companies without direct regulatory exposure can be affected. Investing in PQC now helps organizations stay vendor-eligible, reduce friction in partnerships, and maintain trust across the ecosystem.

2 Mitigating Third-Party Risk

Third-party risk increasingly extends beyond today's controls to how well suppliers can protect data against future quantum threats.

Even if an organization adopts PQC internally, sensitive data may still be exposed through vendors, service providers, or embedded technologies that rely on quantum-vulnerable cryptography.

Starting early allows companies to identify these dependencies, assess exposure, and set PQC expectations across their supply chain. It also creates leverage to influence vendor roadmaps before quantum readiness becomes urgent.

Addressing PQC as part of third-party risk management helps prevent hidden weaknesses from undermining an otherwise secure posture.

3 New Standards and Regulations

Standards bodies and regulators are rapidly turning post-quantum cryptography from guidance into expectation. NIST's selection and standardization of PQC algorithms signals a clear direction of travel for U.S. federal agencies and the private sector that supports them.

Internationally, organizations such as ETSI, ISO, and national cybersecurity agencies in the EU, UK, and Asia-Pacific are issuing timelines, migration guidance, and quantum-risk advisories that point to mandatory adoption.

As with past transitions like TLS upgrades or strong encryption requirements, once standards are formalized, regulations and enforcement tend to follow. Organizations that begin aligning now will be far better positioned than those forced into rushed compliance later.

4 Insurance Requirements

Cyber insurance requirements are evolving quickly, and cryptographic resilience is becoming part of how insurers evaluate risk. As quantum threats gain visibility, insurers are likely to scrutinize how long sensitive data must remain protected and whether organizations have a roadmap for post-quantum security.

Waiting may result in higher premiums, reduced coverage, or exclusions tied to cryptographic weaknesses. At the same time, third-party partners may be pressured by their insurers to demand stronger security assurances from vendors and suppliers. Investing in PQC now helps organizations protect insurability, reduce downstream friction, and avoid being caught unprepared as underwriting standards tighten.

5 Cryptoagility Timelines

Cryptoagility is often underestimated because replacing cryptographic algorithms is rarely a simple swap.

Encryption is deeply embedded across applications, infrastructure, devices, and third-party dependencies, many of which were never designed to be updated easily.

Organizations that wait risk discovering too late that legacy systems, certificate lifecycles, or hardware constraints significantly slow progress. Beginning the transition now allows teams to inventory cryptography, test hybrid and PQC-safe approaches, and modernize incrementally rather than under deadline pressure.

In practice, crypto agility is a multi-year capability, not a last-minute project.

Even today companies are discovering older standards like SHA-1 still in use even though it was disallowed for cryptographic security by NIST in 2013. A cryptographic discovery process today can yield results regardless of post-quantum implications.

6 Competitive Differentiation

Deploying post-quantum cryptography early creates a meaningful opportunity for competitive differentiation and stronger customer trust. As awareness of quantum risk increases, organizations that can credibly demonstrate PQC readiness signal long-term data protection and technical maturity.

This is especially compelling for enterprise, regulated, and global customers with extended procurement cycles and high security expectations. Rather than being viewed as a future compliance task, PQC becomes a trust-building feature that influences buying decisions. Early adopters can position security leadership as a business advantage, not just a defensive measure.

7 Avoiding Talent and Resource Shortages

As demand for post-quantum cryptography grows, the availability of skilled talent and implementation resources will tighten quickly.

The recent scramble for AI expertise offers a clear parallel: organizations that waited faced higher costs, longer timelines, and intense competition for a limited pool of qualified professionals.

PQC expertise is already niche, spanning cryptography, infrastructure, and compliance, and demand will spike as mandates accelerate. Companies that start now can build internal knowledge gradually, partner deliberately, and avoid paying a premium later when PQC skills become scarce.

Acting early turns a looming resource constraint into a manageable transition.

Supply chain management especially as it pertains to risk is a classic wicked problem. There's no single "right" answer, the variables keep changing, and every decision reshapes the problem itself. You can improve visibility, add controls, and refine scorecards, but uncertainty never really goes away. One unexpected event can still ripple across a supplier network in ways no one fully anticipated.

That's exactly why quantum computing has entered the conversation. Not because it offers a silver bullet, but because wicked problems tend to overwhelm traditional approaches. Supplier risk is deeply interconnected, probabilistic, and constrained by real-world trade-offs. As supply networks grow more complex, exploring all the possible outcomes with classical tools becomes increasingly difficult.

Quantum computing is interesting because it's designed for problems like this where the challenge isn't a lack of data, but the sheer number of possibilities. While the technology is still maturing, its potential to help organizations reason through complex supplier risk decisions is becoming harder to ignore.

Supplier optimization, selection, and allocation

Choosing suppliers isn't just about or shouldn't always be just about lowest cost. It's about balancing cost, resilience, compliance, and risk exposure across an entire network.

As constraints multiply and trade-offs become less obvious, traditional optimization methods are often forced to simplify the problem or settle for “good enough” solutions.

Quantum approaches could eventually help search those massive constraint spaces more effectively than today’s heuristics, enabling organizations to evaluate more options and make sourcing decisions that better reflect real-world risk.

Identifying hidden concentration risk across multi-tier supplier networks

Hidden concentration risk is one of the hardest supplier risk challenges because it often sits several tiers upstream, outside direct contractual visibility. Multiple tier-1 suppliers may appear diversified on paper, while relying on the same sub-tier manufacturers, regions, or raw material beneath the surface.

This creates single points of failure that only surface during a disruption. Quantum computing could eventually help by analyzing large, multi-tier network graphs more efficiently, making it easier to surface shared dependencies and concentration risks that are difficult to detect with traditional analytical approaches.

Stress-testing supplier ecosystems against large numbers of correlated disruption scenarios

Risk teams rely heavily on scenario analysis and Monte Carlo simulations which can get costly quickly in terms of both time and money, especially when modeling correlated disruptions and tail risk.

As supplier networks grow more interconnected, the number of plausible disruption combinations increases dramatically, limiting how deeply organizations can stress-test their ecosystems. Certain quantum algorithms promise faster probabilistic estimation, which could mean more scenarios explored more often, and greater confidence in how supplier risk might unfold under extreme but plausible conditions.

Combined with AI, quantum computing can even test scenarios that no human or existing computer would have even thought of analyzing.

Rapidly re-optimizing supply chains during disruptions as constraints change in real time

When a disruption hits, supply plans rarely fail catastrophically all at once (although it can and has happened). Typically, constraints change hour by hour. Capacity shifts, lead times slip, transportation options disappear, and new compliance or geopolitical constraints emerge mid-decision.

Re-optimizing plans under these conditions is computationally intense, forcing teams to rely on simplified models or manual overrides just when speed matters most. Quantum computing could eventually help by enabling faster re-optimization across many changing constraints, allowing organizations to evaluate more feasible recovery options in near real time rather than reacting one step behind the disruption.

Challenges to Quantum Computing adoption

That said, quantum computing comes with real challenges.

First, it can't fix bad data. Poor visibility, incomplete supplier mapping, or unreliable risk signals will limit outcomes no matter how advanced the technology.

Second, cost remains a barrier: quantum hardware, specialized talent, and the supporting infrastructure required to experiment meaningfully are still expensive and not widely accessible. On top of that, the technology itself is still maturing, standards are evolving, and most organizations will need to rely on hybrid quantum-classical approaches for years to come.

In short, quantum computing holds promise, but realizing value will require strong data foundations, clear use cases, and realistic expectations.

Possibly never. Detractors think quantum computing is just hype and may never see widespread adoption in enterprise software in our lifetime.

At apexanalytix, we take a more optimistic, yet practical approach. Right now, quantum computing is still early. Today's quantum machines are real and improving quickly, but they're noisy, fragile, expensive, and best suited for experimentation rather than everyday business use. In other words, the technology works, but is not yet at the scale or reliability needed to run core supplier risk decisions.

Now through about 2028

This is the experimentation phase. Most activity will focus on pilots and proofs of concept, often using hybrid approaches that combine quantum techniques with classical optimization.

Around 2029 into the early 2030s

This is when things start to get interesting. As more stable, fault-tolerant quantum systems come online, we're likely to see early advantages for very specific, high-complexity problems.

Organizations that have already done the groundwork will be best positioned to take advantage.

Mid-2030s and beyond

If current roadmaps hold, quantum computing becomes more practical and more integrated into enterprise platforms. At that point, it's less about experimentation and more about using quantum capabilities to augment planning, optimization, and risk analysis at scale.

Even if quantum computing does not materialize during your career, that doesn't mean there aren't lessons to be learned by examining its potential. While quantum computing is not a near-term replacement for today's supplier risk platforms, it is something worth preparing for. This is especially true for organizations dealing with large, global, highly constrained supply networks. Teams that understand their hardest supplier risk problems now will be the ones ready when the technology catches up. While the use of quantum computing may be many years away, there are tangential areas that can be deployed today. For example, new algorithms for post-quantum cryptography have been developed and mandated by standards organizations (ex: NIST). See our blog, "The Quantum Threat: Preparing Supply Chain Data for 2030" for more information.

Additionally, there are alternative technologies a company can use to further enhance supplier risk management today while waiting for quantum to mature. To learn more about how AI can help supplier risk management, read our blog, "AI Supplier Management Revolution in 2026."

Call to Action

Even if quantum computing does not materialize during your career, that doesn't mean there aren't lessons to be learned by examining its potential. While quantum computing is not a near-term replacement for today's supplier risk platforms, it is something worth preparing for.

This is especially true for organizations dealing with large, global, highly constrained supply networks. Teams that understand their hardest supplier risk problems now will be the ones ready when the technology catches up. While the use of quantum computing may be many years away, there are tangential areas that can be deployed today.

For example, new algorithms for post-quantum cryptography have been developed and mandated by standards organizations (ex: NIST). See our blog, "The Quantum Threat: Preparing Supply Chain Data for 2030" for more information.

The Taleaway

Quantum computing won't fix bad data, poor visibility, or unclear business processes. It can, however, provide genuine long-term potential for supplier risk management where complexity and uncertainty are serious problems.

Next steps should include:

- Invest in quantum expertise and talent: don't fall behind the curve and have to pay premium prices later like many companies did for AI experts.
- Conduct a cryptographic inventory: you may be surprised what older already deprecated and disallowed standards you find still in use.
- Invest in post-quantum cryptography: remember it could take you five years or more to fully transition to new algorithmic standards.
- Update third-party contracts: incorporate your new cryptographic standards into contracts along with responsibilities and timelines.
- Improve your data foundation and n-tier visibility: remember even the most sophisticated technologies work best with good data.
- Define your wicked problems in supplier chain: list and prioritize your complex supply chain problems today and look for potential existing technologies such as AI to help solve them in addition to planning for quantum

The companies that take these steps will be well prepared for when quantum computing becomes a reality.

How apexanalytix Can Help

Quantum computing may still be emerging, but the decisions organizations make today will shape how exposed or prepared they are when its impact becomes real. That's where apexanalytix comes in. Our platform is designed to help enterprises build resilience now, with the visibility, intelligence, and controls needed to manage quantum-era risk across complex supplier ecosystems.

Apexanalytix enables organizations to protect sensitive supplier data using quantum-resistant security approaches, assess supplier preparedness across the supply chain, and identify vulnerabilities before they become breaches. It also supports evolving compliance requirements and helps organizations demonstrate due diligence to regulators, partners, and stakeholders.

Our Cyber Risk solution can also help you gauge your supply chain's quantum readiness through automated vulnerability scanning, dark web monitoring, and framework-aligned assessments. Plus, our golden graph of more than 280M entity records provides a solid data foundation for your efforts based on more than $10T worth of supply chain transactions every year.

Quantum readiness isn't about charging headlong into the unknown without a plan. It's about strengthening trust, resilience, and risk management for the long term. apexanalytix is ready for the quantum future, and we're here to help ensure your organization is ready too.

William McNeill

VP - Market Intelligence, apexanalytix

William McNeill is Vice President of Market Intelligence at apexanalytix, where he leads analyst relations and public relations and develops thought leadership on supplier risk management, artificial intelligence, and emerging technologies such as quantum computing.

Prior to joining apexanalytix, Will spent more than 17 years as a research analyst at Gartner, covering supplier risk management, global trade compliance, and sourcing and procurement. He brings deep industry expertise and a forward-looking perspective to helping organizations navigate an increasingly complex and technology-driven supply chain landscape.

Akhilesh Agarwal

President of P2P Solutions and Technology at apexanalytix

Akhilesh Agarwal leads the apexanalytix solutions practice responsible for apexportal.

He leads the development of new client-focused software innovations. He also oversees pre-sales, product management, project planning and reviews, risk mitigation and the delivery of seamless solutions to large global clients across country borders.

Akhilesh has extensive background in product design and execution in accounts payable, accounts receivable and related areas.

Before joining apexanalytix, he was vice president of technology for iQor, a provider of intelligent customer interaction solutions. He also is a former associate director of software development for Receivable Management Services and a former project manager for Aditya International.