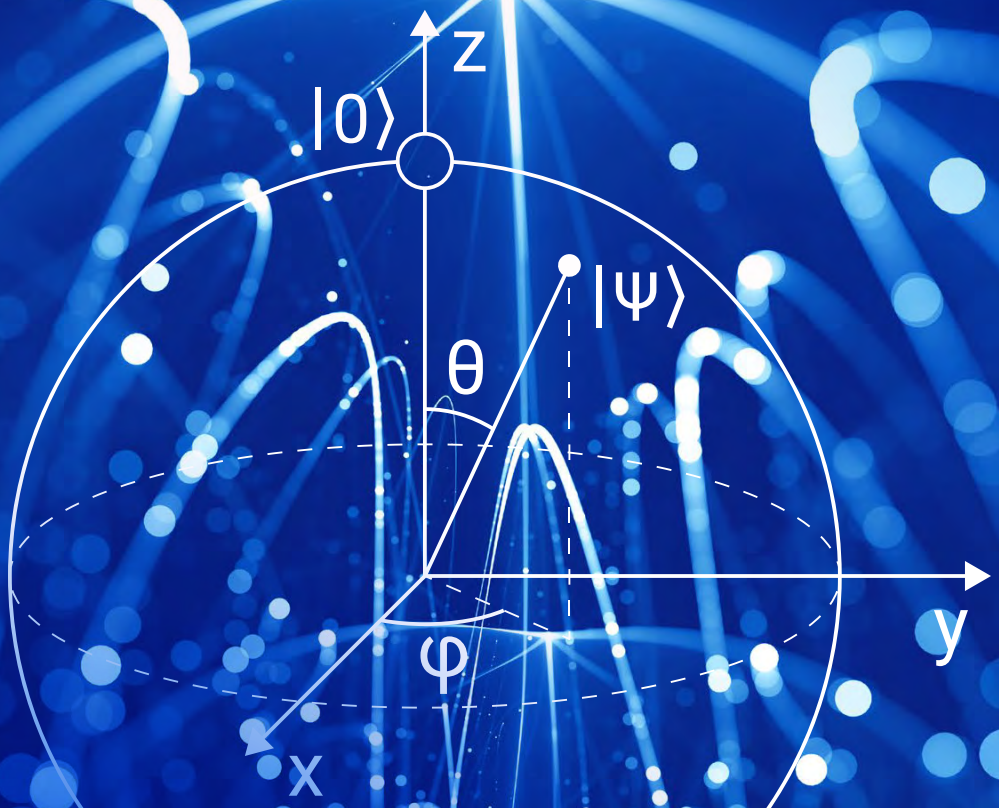
KPMG



Insurance Insights

Quantum computing
Opportunities and threats
for the insurance industry

QuantumBasel

LLOYD'S

October 2026

01 **Foreword**

02 **Executive summary**

04 **1 Quantum computing**

05 **1.1 Introduction to quantum computing**
07 **1.2 State of the art and expected timelines**

11 **2 Current state of quantum computing in the insurance industry**

14 **3 Opportunities: Deep dive into selected use cases**

15 **3.1 Portfolio and capital optimization**
3.1.1 Status and current challenges
3.1.2 Quantum approaches and maturity
17 **3.2 Fraud detection**
3.2.1 Status and current challenges
3.2.2 Quantum approaches and maturity
20 **3.3 Valuation, pricing, and product personalization**
3.3.1 Status and current challenges
3.3.2 Quantum approaches and maturity
22 **3.4 Risk modeling and catastrophe simulation**
3.4.1 Status and current challenges
3.4.2 Quantum approaches and maturity
23 **3.5 Other opportunities**
24 **3.6 Actuarial perspective on opportunities and challenges of optimization in the UK insurance industry**
26 **3.7 Interview with AXA on its quantum journey**

31 **4 Security threats**

33 **4.1 Quantum threat to encryption and data security**
4.1.1 Introduction to quantum threats
4.1.2 Insurance-specific threats
4.1.3 Impact on financial and blockchain systems used by insurance industry
36 **4.2 Post-quantum cryptography and quantum key distribution**
37 **4.3 Risk mitigation strategies and frameworks**
4.3.1 PQC transition roadmaps, risk assessment frameworks, and regulations
4.3.2 Preparing the organization for quantum threats (operational readiness)
4.3.3 QKD networks and dual strategies
40 **4.4 Interview with BreachBits on hackers in the quantum era**

43 **5 Emerging challenges for the insurance industry and recommended actions**

44 **5.1 Key challenges**
47 **5.2 Recommended actions**

50 **6 Outlook**

51 **6.1 Entering the quantum era**
52 **6.2 Lloyd's perspective on developments since the 2021 report, innovation, and the future of insurance**

57 **References**

66 **Contributors**

67 **Contacts and publication information**



Dear Readers,

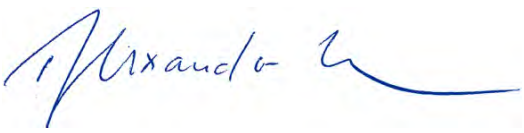
As part of the KPMG Insurance Insights series, we are pleased to present this white paper examining the opportunities and risks that quantum computing may create for the insurance industry.

Quantum computing has moved beyond the confines of research laboratories and academic debate. Across sectors, organizations are assessing its potential applications, strategic implications and associated risks, and the insurance industry is no exception. Although the pace and direction of technological development remain uncertain, quantum technologies already merit systematic analysis, informed dialogue and timely preparation.

Quantum computing is inherently multidisciplinary. Meaningful progress requires expertise and collaboration across scientific disciplines, organizations and industries. This white paper reflects that collaborative approach. Developed jointly with Lloyd's of London and QuantumBasel, and enriched by contributions from a broad range of organizations and specialists, it brings together perspectives from the insurance and quantum ecosystems as well as related fields. Collaboration across KPMG's global network further underscores the international relevance of the subject.

We extend our sincere thanks to all contributors for sharing their expertise, insights and perspectives. Their commitment and engagement were instrumental in bringing this publication to fruition.

We hope this publication will stimulate informed discussion, provide a foundation for further research and practical exploration, and foster collaboration within the insurance industry and beyond.



Dr. Alexander Lacher
Insurance Sector Head, KPMG Switzerland



Dr. Christoph Kloeffel
Quantum Technology Lead, KPMG Switzerland

Executive summary

In its 2021 report [1] on the impacts of quantum computing on insurance, Lloyd's of London expected to see industry applications emerge within five years and highlighted that quantum computing would likely have a significant impact on the insurance industry between 2025 and 2035. Five years later, we take the opportunity to review how these expectations compare with technological progress and industry developments.

Quantum computing has advanced rapidly owing to breakthroughs in areas such as hardware development and quantum error correction. According to the roadmaps published by several providers, a transition from today's noisy intermediate-scale quantum computers to large-scale fault-tolerant quantum computers, which are expected to enable certain high-impact applications, is projected around the end of the decade (Section 1).

This technological progress is matched by a continually rising global quantum effort through governmental initiatives. The growth in public funding underscores the strategic importance that governments around the world attach to quantum technologies and further accelerates research and innovation in the field.

Insurance and reinsurance companies have been pursuing a variety of activities related to quantum computing, such as exploring use cases on real quantum hardware, making strategic investments, and establishing consortia and alliances with partners from industry and academia (Section 2). Potential quantum computing applications in the short, medium, and long term could create a broad range of opportunities for insurance and reinsurance companies, including advancements in portfolio and capital optimization, fraud detection, valuation and pricing, as well as risk modeling and catastrophe simulation. Early progress has already been demonstrated across these areas. It is worth noting that, unlike AI, quantum computing will likely remain a specialized tool for selected applications. Beyond such use cases, the quantum era may also create new opportunities related to insurance products and services (Section 3).

Rapid progress in quantum computing gives rise not only to opportunities but also to risks. A prominent threat posed by future quantum computers is their potential to break today's public-key cryptography. Although cryptographically relevant quantum computers do not yet exist, threats like "harvest now, decrypt later" are already present. Recent advancements have prompted several organizations to accelerate their transition to post-quantum cryptography (PQC). For example, Google, Microsoft, and Cloudflare aim to complete their PQC migrations by 2029.

Across the globe, organizations are expected to build quantum resilience by developing and following a multi-year PQC transition roadmap, which is aligned with their strategy and facilitates cryptographic agility. First substantive steps include a cryptographic inventory and a quantum risk assessment to determine criticality. The Swiss Financial Market Supervisory Authority FINMA, for instance, recommends that supervised institutions develop a PQC roadmap by mid-2027 at the latest. In specific cases, quantum key distribution as a supplement to PQC may provide additional security benefits. However, the quantum era may also introduce new attack vectors and vulnerabilities that malicious actors could exploit (Section 4).

For insurers and reinsurers, maintaining trust and competitiveness in the quantum era is an overarching challenge (Section 5.1).



Key challenges

- Competition for quantum talent and expertise
- Quantum ecosystem dynamics and growing diversity of tools
- Global quantum race and geopolitical tensions
- Security threats and new attack vectors
- Compliance with laws and regulatory expectations
- Limitations imposed by existing process landscapes
- Impacts of evolving risk landscapes on products and services

Recommended actions that organizations in the insurance industry should pursue today.*

Strategy and Governance

1. Establishing quantum governance and executive ownership
2. Strengthening leadership understanding of the business implications of quantum technologies
3. Developing an internal R&D and innovation strategy

People and Ecosystem

4. Promoting organization-wide quantum literacy alongside specialist expertise
5. Actively engaging with the quantum ecosystem
6. Establishing mechanisms to monitor emerging developments

Security and Quantum Resilience

7. Establishing and maintaining a cryptographic inventory and assessing quantum-related risks
8. Developing a roadmap for the transition to PQC and cryptographic agility
9. Monitoring developments in quantum key distribution and related technologies

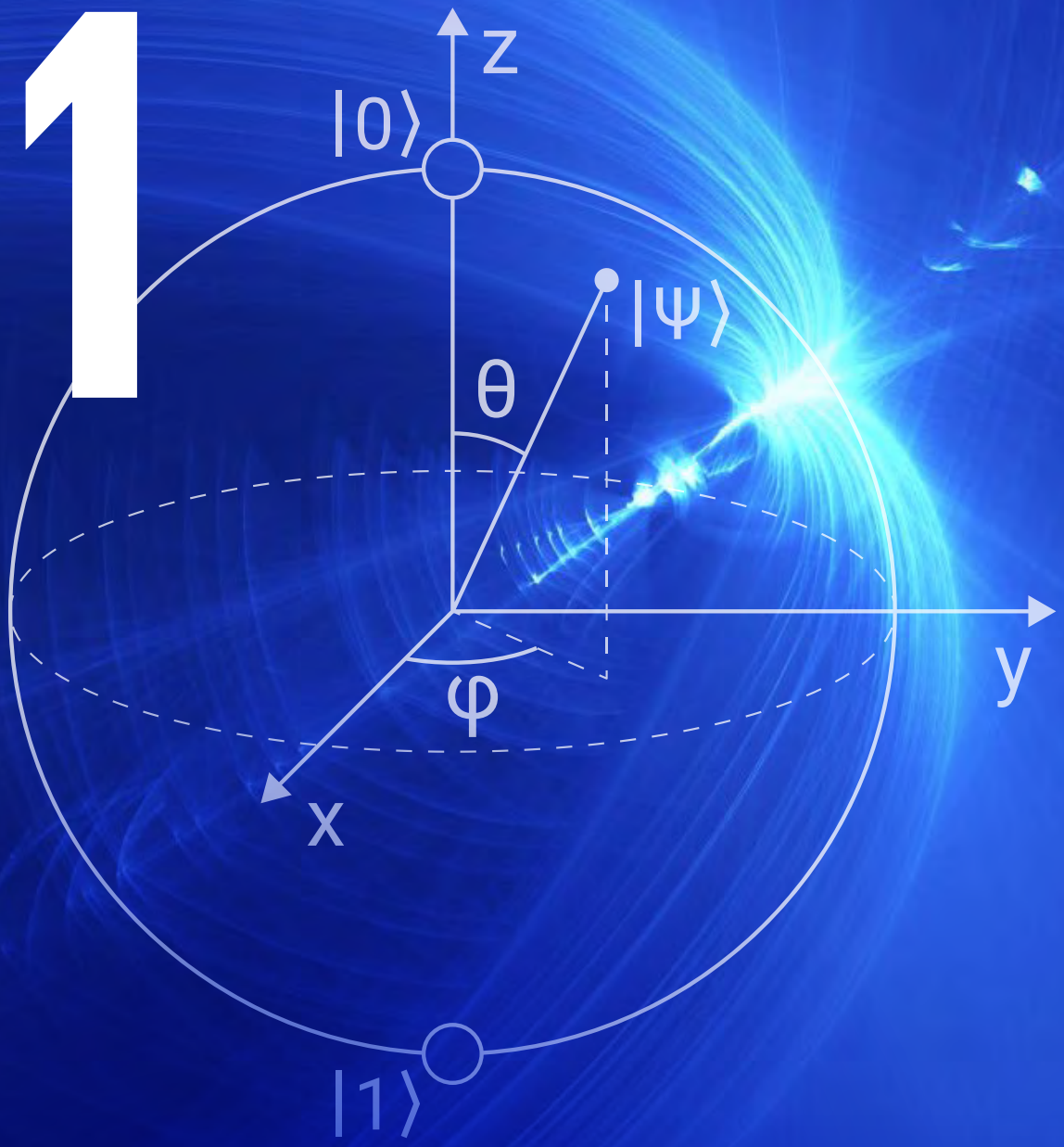
Quantum Technology Adoption and Insurance Innovation

10. Identifying and prioritizing promising quantum use cases
11. Exploring and validating prioritized quantum applications
12. Assessing the implications of the quantum era for insurance products and services

* These actions are grouped into four thematic categories and are listed in no particular order. Section 5.2 describes each recommendation.

Organizations that take meaningful steps today will be best positioned for the quantum era. We conclude with an outlook (Section 6), including Lloyd's perspective on developments since the 2021 report, innovation, and the future of insurance.

01



Quantum computing

By harnessing the principles of quantum mechanics and processing information in fundamentally new ways, quantum computers have the potential to solve certain high-impact problems beyond the reach of classical computers. Once a purely theoretical concept, they are now accessible via the cloud and continue to improve rapidly. This section explores the foundations, current state, and future evolution of this emerging technology.



Collaborators from KPMG and QuantumBasel in conversation, bringing together expertise across quantum computing, quantum resilience, insurance and reinsurance.

From left to right:
Sébastien Loesch (KPMG)
Pascal Pfister (KPMG)
Damir Bogdan (QuantumBasel)
Christoph Kloeffel (KPMG)
Frederik F. Flöther (QuantumBasel)
Thomas Schneider (KPMG)

1.1 Introduction to quantum computing

What is quantum computing? While the technology's potential is great, so are the misunderstandings which abound. Quantum mechanics, as a branch of physics, is nothing new. In fact, 2025 was celebrated as the International Year of Quantum Science and Technology to mark 100 years since the development of some of the early ideas. Moreover, a range of "first-generation" quantum technologies were already developed decades ago based on that theoretical foundation, ranging from lasers to solid-state electronics to superconductors and underpinning a sizable fraction of modern science and business.

Quantum computing, then, is part of a new generation of quantum technologies. These all leverage the principles of quantum mechanics, such as quantum entanglement, interference, and superposition, in order to go beyond the state of the art. Generally, one distinguishes between quantum communication (allowing secure communication between remote parties), sensing (enabling measurements with exceptional precision and sensitivity, for instance in biology), and computing. Of these, quantum computing is arguably the holy grail, as it is not just an evolution of high-performance computing (first misconception) but can address problems with entirely new algorithms that are based on novel hardware and software. The base unit of information is no longer a bit but a quantum bit (qubit). Such a qubit may be encoded in a number of different physical forms; leading systems leverage, for example, ions, neutral atoms, photons, and superconducting circuits as qubits. However, quantum systems generally lose their unique properties quite easily and become "classical" through a process known as decoherence. The field of quantum error correction is thus crucial with regard to moving the technology towards the mainstream.

Circuit-based quantum computing, also referred to as gate-based (or gate-model) quantum computing, must be differentiated from quantum annealing. The former is computationally universal while the latter is not, meaning it cannot efficiently implement any arbitrary quantum algorithm. Moreover, circuit-based quantum computing has quantum advantage possibilities that annealing does not have. Nevertheless, quantum annealers such as those from D-Wave already have larger numbers of qubits, making it in some cases easier to test data sets with more "real-world" character. Quantum annealers are mainly explored in the context of optimization problems.



Another important distinction concerns the current era of noisy intermediate-scale quantum (NISQ) systems and the future era of fault-tolerant machines. NISQ algorithms can already be implemented today, but evidence for potential advantages is rather limited. On the other hand, while fault-tolerant algorithms often come with better performance guarantees, their practical use today is rather limited.

Quantum computing is not a silver bullet for any arbitrary computational task (second misconception). While one could theoretically address any type of problem with a quantum computer, benefits compared with classical computers have only been discovered for very specific types of tasks. These are often grouped into chemistry (simulation of nature), machine learning, and optimization applications. The possible speedups vary (from heuristics to exponential speedups for future machines) and the benefits may often lie beyond raw speed (third misconception), instead allowing solutions with higher accuracy, higher (energy) efficiency, or lower input data requirements (for instance, handling noise better).

Use cases for quantum computing must be considered through careful mapping of quantum algorithms. Just having a lot of data is not a good criterion (fourth misconception) and, at least with today's generations of quantum computers, represents a challenge that necessitates further classical preprocessing. Instead, problems that are "computationally intensive" and have many potential solutions lend themselves better for exploration. One of the most prominent ones is the traveling salesman problem where the shortest possible route that visits each stop once is to be found.

Quantum computing alone is rarely the whole answer: it is the combination of technologies that often makes the difference. Some of the most promising use cases explored today lie at the intersection of quantum computing and artificial intelligence, where quantum processors are integrated into hybrid quantum-classical pipelines. Early research indicates that quantum computing could enhance specific AI capabilities for example in optimization, sampling from high-dimensional distributions, and machine learning models that achieve comparable performance with fewer parameters.

1.2 State of the art and expected timelines

The quantum (computing) sector has seen an acceleration over the past years. There used to be intense debate as to whether quantum computers can be built at all and if they will ever be useful. Now, the discourse centers on "when" rather than "if" and organizations are trying to estimate timelines, both from an opportunity and a security threat perspective, in order to optimally time talent development, architecture updates, and other investments.

In circuit-based quantum computing, quantum algorithms are executed via quantum circuits. These represent a series of operations by quantum gates on qubits (into which the input data was encoded), which are ultimately measured and return strings of 0s and 1s once again. In order to make quantum computers practical, both the circuit depth (how many gates can be carried out) and width (number of qubits) must be substantially increased. Quantum hardware vendors have been making progress on these fronts. Companies such as Google, IBM, IonQ, IQM, Pasqal, and QuEra have been rapidly developing systems that facilitate the execution of deeper and wider circuits that have more practical relevance. While the degree of near-term quantum advantages makes for intense debates [2], the rapid progress is clear.

Recently, several quantum computer providers accelerated their roadmaps and presented detailed timelines for their transition from NISQ to large-scale fault-tolerant quantum computing (FTQC). In the era of large-scale FTQC, users will be able to execute algorithms on thousands of quasi-ideal "logical" qubits (implemented through error correction across many underlying "physical" qubits), enabling quantum circuits of sufficient width and depth for a variety of high-impact applications. The roadmap acceleration reflects the remarkable technological developments of the past years, including significant progress in quantum error correction [3]. It is also worth noting that several quantum hardware providers have recently gone public or announced plans to do so. This increased access to capital can help accelerate technological developments. Furthermore, the growing competition and investor expectations may create additional pressure on companies to set and achieve highly ambitious goals. Based on the roadmaps published thus far, and subject to significant engineering challenges and technical uncertainty, some providers target large-scale FTQC around the end of this decade, as illustrated in Figure 1.

Logical qubit counts reported in roadmaps

Due to the different qubit platforms, these quantum computers can also differ significantly in, e.g., gate speed and connectivity

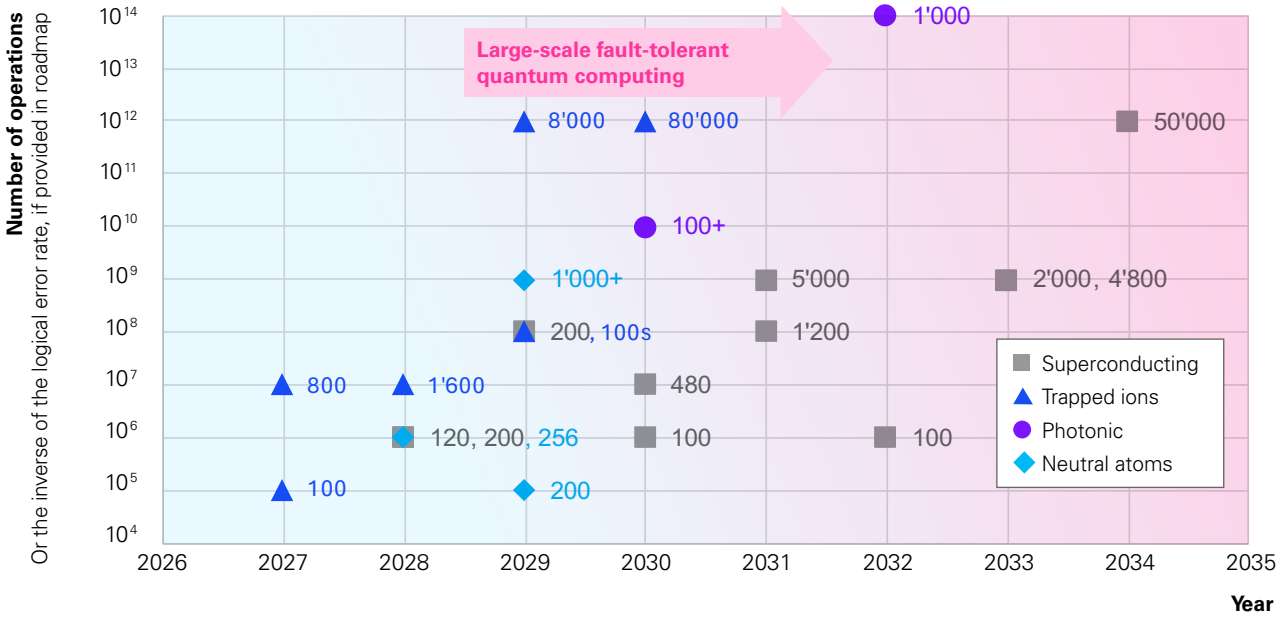


Figure 1 Overview of roadmap data published by quantum computer providers as of end-July 2026. Data points are included when the number of logical qubits is at least 100 and the logical error rate is at most 10^{-5} (the possible number of quantum operations is at least 10^5, respectively). If roadmaps contain a range of values for the qubit count or the error rate exponent, average values are considered. In cases where a logical fidelity F is provided, we use the common approximation 1/(100%-F) for the number of operations. The roadmap data were taken from the websites of the following providers and are grouped by qubit platform. Superconducting: Alice & Bob ("cat qubits") [4], D-Wave (gate-model roadmap) [5], IBM [6], IQM [7], OQC [8]. Trapped Ions: IonQ [9], Quantinuum [10]. Photonic: Quandela [11]. Neutral Atoms: Pasqal [12], QuEra [13].











Experts from KPMG and QuantumBasel discussing quantum technologies and their implications for the insurance industry.

Top photo [from left to right]
Sébastien Loesch (KPMG)
Pascal Pfister (KPMG)
Damir Bogdan (QuantumBasel)
Christoph Kloeffel (KPMG)
Frederik F. Flöther (QuantumBasel)
Thomas Schneider (KPMG)

Quantum computers can differ significantly in properties such as qubit connectivity and gate speed, which have a strong impact on the computation time for quantum algorithms.

The data presented in Figure 1 indicate the expected timeline for the width (logical qubit count) and depth (number of operations) of quantum circuits that will be executable on quantum hardware according to providers' roadmaps. Below, we highlight three noteworthy points not displayed in this figure.

- Depending on the specific qubit type and implementation details, quantum computers can differ significantly in properties such as qubit connectivity and gate speed, which have a strong impact on the computation time for quantum algorithms. In addition, the maintenance and operational requirements (e.g., recalibration, cooling) of available quantum computers will be relevant to users, as they may affect costs and access times.
- We focused on quantum roadmaps with specific information on all three dimensions (year, number of qubits and operations) of Figure 1. Several other roadmaps toward large-scale FTQC have been published, including those by Google [14] and Microsoft [15].
- Spin qubits [16] in silicon or germanium are particularly attractive for large-scale FTQC. They offer exceptional scaling potential by leveraging the semiconductor industry's experience in fabricating billions of transistors on chips as used, e.g., in mobile phones and laptops. Although current qubit counts are below those of other leading platforms, spin qubits feature high gate speed, small footprints, and can operate in the Kelvin regime (i.e., at temperatures above those typically required for superconducting qubits). For example, several companies including Diraq, Groove Quantum, Intel, Quantum Motion, Quobly, SQC, as well as the Swiss NCCR SPIN (National Center of Competence in Research), are pursuing spin qubits. They also play an important role in IBM's recent acquisition of HRL Laboratories [17].

We conclude this introductory section by highlighting three developments that demonstrate the growing global race for leadership in quantum computing.

First, according to a joint EPO-OECD report [18], the number of quantum-computing-related patents has surged in recent years. Applicants from China lead in the number of patent families in quantum technologies, although most of these correspond to national filings. In contrast, the United States leads in the number of international patent families, followed by the member states of the European Patent Convention and Japan [18]. According to an EconSight overview that evaluates patent quality rather than counts alone, the United States and China dominate in terms of world-class quantum computing patents [19].

Second, quantum technologies have become subject to increased export controls. For example, effective May 2025, Switzerland added new technologies such as quantum computing to its list of dual-use goods, thereby harmonizing Swiss export controls with those of main trading partners [20].

Finally, substantial public and private investments and strategic programs for quantum computing have been intensifying worldwide. Recent examples include President Trump's executive orders issued in June 2026 addressing quantum innovation [21] and quantum cybersecurity [22] in the United States, as well as IBM's announcement [23] of an additional USD 10 billion investment in quantum computing over the next five years. During the five years preceding the publication of the 2025 Quantum Europe Strategy [24], the EU (nearly EUR 2 billion) and its Member States (more than EUR 9 billion) invested more than EUR 11 billion in public funding across quantum technologies, including quantum computing, quantum sensing, and quantum communication. The UK presented its National Quantum Strategy in 2023 [25], and the Swiss Quantum Strategy was published in 2026 [26].



“What if the insurance industry’s greatest risk lies in the patterns it fails to see and the risks it cannot fully calculate?”

Frederik F. Flöther
Chief Quantum Officer, QuantumBasel

02



Current state of quantum computing in the insurance industry

Interest in quantum computing is growing rapidly across the insurance sector. Insurers, reinsurers, and industry organizations around the world are exploring quantum applications, conducting research, and building collaborations with academia and technology partners. What began as a largely theoretical discussion has evolved into a growing ecosystem of research initiatives, pilot projects, and cross-industry collaborations.

Quantum computing creates new opportunities and risks across a wide range of industries, including financial services and insurance. Driven by rapid technological advancements, several insurance-specific reports and review articles have been published in the past years. For example, Lloyd's of London presented a detailed report in 2021 about impacts of quantum computing on insurance [1], the Society of Actuaries published a research report in 2023 about the impacts on actuarial modeling [27], the American Academy of Actuaries featured an article on how quantum computing could both benefit and challenge insurers [28], and in 2025, the journal Science China Information Sciences published an article about quantum computational insurance and actuarial science [29]. The examples presented here and below demonstrate the growing global interest and progress in this field.

Research on insurance-relevant quantum algorithms and their potential use cases is a key enabler for practical quantum computing applications. Researchers worldwide have been developing and refining quantum computational approaches that can be advantageous for applications such as Monte Carlo simulations [30], [31], machine learning [32], [33], or complex optimization tasks [34], [35], [36]. Remarkably, several (re)insurance companies have been driving such research through their own activities, thereby ensuring high business relevance of the considered use cases, and through joining research centers and consortia that foster collaboration among interdisciplinary members from academia and industry.

The table below shows a non-exhaustive list of insurance and reinsurance organizations exploring quantum computing and provides examples of publicly available information on their activities. In addition, many (re)insurance companies not listed here have recently embarked on their quantum journey by participating in dedicated events such as roundtables and workshops. Furthermore, several companies in the insurance industry have already taken first steps toward building quantum resilience – a topic beyond the scope of this table that will be covered in Sections 4 and 5.

Examples of insurance and reinsurance organizations and their activities on quantum computing

Organization	Activities on quantum computing – Published examples
Allianz	Allianz France collaborated with LMU Munich to explore quantum generative modeling and quantum annealing for fraud detection. Evaluations were performed using quantum annealers provided by D-Wave [37]. In 2023, together with IQM and Multiverse Computing, Allianz France launched the project AQACYB (Avantage Quantique pour l'Analyse de CYBermenaces) on quantum-enhanced machine learning approaches to detect cybersecurity threats [38], [39]. Allianz X, the strategic investment arm of the Allianz Group, invested in companies such as 1QBit and SandboxAQ, which provide solutions in AI & quantum technology/software [40].
Allstate	In 2025, Allstate joined the Chicago Quantum Exchange (CQE) as a corporate partner [41]. Recently, Allstate and IBM developed a hybrid quantum-classical method for tackling a class of optimization problems that is relevant to insurance underwriting and other applications. Reported quantum hardware experiments for their proposed scheme were performed by running circuits with up to 3,443 gates and 150 qubits [42].
Antares a QIC Company	The R&D department of Antares Global studied quantum computing in insurance capital modeling under reinsurance contracts and implemented their approach with IBM's Qiskit framework [43]. In addition, they conducted a study in which motor insurance claim data from Qatar Insurance Company was analyzed using a quantum-enhanced machine learning algorithm to improve prediction accuracy [44]. Related projects include quantum-enhanced approaches to medical insurance and health data analysis [45].

Organization	Activities on quantum computing – Published examples
AXA	AXA launched its quantum computing research in 2019 and is a pioneer exploring quantum computing for (re)insurance applications [46], [47]. Quantum-related activities of AXA include research on, e.g., modern computational methods and potential future quantum speedups in reinsurance optimization [48]. As described in the interview in Section 3.7, the activities also include educational events such as workshops and hackathons. The World Economic Forum's Quantum Application Hub features a use case provided by AXA on the optimization of reinsurance contracts [49], [50]. AXA Konzern AG collaborated with Fraunhofer ITWM on a quantum computing project for potential applications such as insurance contract valuation, with exemplary circuits executed on simulators and real quantum hardware [51].
LLOYD'S	Lloyd's of London and collaborators have provided thought leadership on the implications of quantum computing for the insurance industry, particularly through their 2021 report [1] and related presentations and events [52].
MetLife	An actuarial working group on quantum computing has been established at MetLife [53].
MS&AD Holdings	Mitsui Sumitomo Insurance Company is one of the 24 inaugural members of the Quantum STrategic Industry Alliance for Revolution (Q-STAR), which was founded in Japan in 2021 to foster cross-industry collaboration and promote the growth and application of quantum technologies [54], [55], [56]. Aioi Nissay Dowa Insurance worked on quantum algorithms and business use cases through quantum optimization and quantum machine learning projects conducted by, e.g., the AIOI R&D LAB-OXFORD and Aioi Insurance Services USA [57], [58].
Munich RE	Since 2016, Munich Re and ERGO have been monitoring quantum computing as a trend in their annual Tech Trend Radar. Munich Re is a founding member of the Quantum Technology and Application Consortium (QUTAC), which was launched in 2021 and brings together leading corporations in Germany to drive innovative industrial applications and economically successful quantum computing solutions [59], [60], [61]. Within QUTAC, quoting from their website [59], "Munich Re analyses possible application scenarios and develops initial quantum-based business ideas, including for safeguarding quantum computing services or modelling risks in the financial world."
SOMPO	In 2022, it was announced that Sompo will use quantum-inspired computing technology (Hitachi's CMOS Annealing) in insurance operations, especially in non-life insurance underwriting operations [62].
Swiss Re	In its SONAR 2022 report, providing new emerging risk insights, Swiss Re assessed quantum computing as a source of high-impact risk [63]. Swiss Re also addresses risks from quantum computing in training programs, such as cyber insurance & underwriting courses [64], [65].
Unipol	Unipol Assicurazioni S.p.A is a member of the ICSC, Italy's national research center for high-performance computing, big data, and quantum computing, where Unipol and collaborators develop hybrid quantum-classical optimization methods for applications in the insurance sector and beyond [66]. Leithà, the Unipol group's excellence center for data and computer science, studied the implementation of an optimization algorithm. The evaluation included experimental runs on a neutral atom quantum computer by Pasqal [67].

03

Opportunities: Deep dive into selected use cases

Quantum computing has the potential to help address some of the insurance industry's most challenging computational problems. However, realizing this potential depends on various factors including the business relevance of a use case and the maturity of the relevant quantum technologies and approaches. The following pages examine where quantum computing may address significant challenges in the insurance industry and how the suitability of different quantum approaches varies across applications and time horizons.

In this section, a selection of promising quantum computing use cases spanning the near, medium, and long term are discussed in more detail. The overview is not intended to be exhaustive, as other use cases for the insurance industry exist or will be developed as the field evolves [68]. Moreover, a given quantum algorithmic primitive generally finds application across many different kinds of use cases.

The three types of computational tasks (optimization, machine learning, simulation) identified as particularly attractive for quantum computing apply also to financial services [32] and the insurance industry [29]. Here, "simulation" goes beyond the simulation of physical systems such as molecules and materials and encompasses scenario simulations relevant to financial services. The table below lists some of the insurance-specific examples covered in this section, along with quantum algorithms commonly proposed and explored for these types of tasks.

Overview of problem categories, quantum computational approaches, and specific application examples for the insurance industry

Task type	Quantum algorithms	Insurance industry examples	Subsections
Optimization	QAOA, annealing, Grover, optimization by decoded quantum interferometry	– Asset-liability management – Portfolio/contract optimization – Product personalization	3.1.2 3.3.2 3.4.2
Machine Learning	Variational quantum circuits (e.g., QNNs), quantum kernel methods, quantum reinforcement learning, quantum Boltzmann machines, quantum principal component analysis	– Fraud detection – Image classification – Data generation and enhancement	3.2.2 3.3.2 3.4.2
Simulation & Stochastic Modeling	Quantum Monte Carlo, quantum amplitude estimation, quantum walk	– Valuation – Actuarial pricing – Catastrophe simulation – Risk analysis	3.3.2 3.4.2

In each of the following Sections 3.1 to 3.4, we begin with a compact review of the topics considered, highlight their relevance for insurance and reinsurance companies, and describe the current situation including major challenges that companies are facing. Subsequently, we discuss how quantum computing may help address some of these challenges. In Section 3.5, we provide additional examples of quantum technology use cases for the insurance industry. Section 3.6 presents an actuarial perspective with focus on the UK market. Finally, in Section 3.7, AXA shares insights from its quantum journey.

3.1 Portfolio and capital optimization

3.1.1 Status and current challenges

Insurance contracts result in liabilities that can span over decades and depend on events that cannot be predicted exactly (e.g., whether/when an accident happens). The capital required to cover these liabilities depends on several factors, including the properties of the insurance products, reinsurance structures, list of assets, and the models that are used based on regulatory and internal requirements. As a result, the insurance industry is confronted with highly business-relevant optimization tasks and related challenges.

One important approach to balance risk and capital is identifying optimized allocations between insurance and reinsurance [48], [50]. This leads to combinatorial optimization problems with a vast number of possible combinations for consideration. A related example is intra-group retrocession, where risks are transferred between entities within a corporate group to enhance diversification, solvency, and capital management. For these approaches, as with many tasks across the insurance industry, challenges beyond computational limitations are often linked to the availability, granularity, and quality of data.

Another key question concerns the choice of assets. In the insurance industry, asset-liability management plays a particularly important role in remaining competitive while ensuring that all future obligations can be fulfilled and liquidity is sufficient. For example, the assets used to cover insurance liabilities are subject to additional regulatory constraints. The choice of assets and the relation between asset and liability cashflows can strongly impact the capital requirements. Identifying the right asset portfolio is a complex optimization task with several additional challenges. For example, different frameworks (e.g., local GAAPs for reserving, solvency-related frameworks such as Solvency II and the Swiss Solvency Test or reporting standards such as IFRS 17) and their specific rules need to be considered along with internal processes and guidelines, leading to several questions to be addressed to find a well-suited model, data, and approach to determine the optimized asset portfolio.

For a detailed perspective on the UK market, for instance, see the discussion on matching adjustment and other topics in Section 3.6.

3.1.2 Quantum approaches and maturity

Optimization is typically cited as one of the primary categories for quantum algorithm applications. It is a special category, as it allows both circuit-based and annealing approaches to be explored. The formulation often takes the shape of a quadratic unconstrained binary optimization (QUBO) problem. This lends itself to quantum annealing and, from a circuit-based angle, to the quantum approximate optimization algorithm (QAOA). Depending on the setup, additional constraints are included to bring the mathematics closer to the real world. One such example is the "no short selling constraint", which complicates the problem but can ensure it reflects regulatory requirements [69]. Such QUBO-based approaches can also be found in asset-liability management. For instance, a quantum annealer has been tested with regard to the Solvency II matching adjustment problem for insurers [70].

A widely used classical technique for tackling combinatorial optimization problems in the presence of constraints is branch-and-bound. A quantum branch-and-bound algorithm, which can accelerate classical branch-and-bound algorithms through a near-quadratic theoretical speedup [71], has recently been explored for reinsurance optimization [48].

Furthermore, as noted above, the availability of data can be a challenge for a wide range of optimization problems and other tasks across the insurance industry. Quantum algorithms are, in fact, being explored broadly with regard to synthetic data generation, with quantum generative adversarial networks (QGANs) being a leading candidate that has shown early promise [72].

Besides quantum computing and quantum annealing, which we focus on in this report, insurers and reinsurers can benefit from a variety of advanced optimization tools that run entirely on classical hardware. One example is quantum-inspired optimization (QIO), which uses optimization strategies motivated by quantum mechanics without the need for quantum hardware. QIO tools have been developed by companies such as Fujitsu, Microsoft, and Toshiba. Importantly, the QUBO formulation is a mathematical representation that allows optimization problems to be addressed on a variety of present and future platforms, including QIO solvers, quantum annealers, and circuit-based quantum computers, as discussed earlier.

3.2 Fraud detection

3.2.1 Status and current challenges [1]

Insurance fraud represents an important operational challenge across both life and non-life insurance, although fraud patterns differ considerably between business lines. Fraud detection is particularly relevant in claims management, where insurers process large volumes of claims while balancing efficient claims settlement with effective fraud prevention. Decisions frequently rely on information and supporting documentation provided by policyholders and external parties, creating an inherent information asymmetry that may be exploited through fraudulent activities. At the same time, insurers seek to maintain a positive customer experience by ensuring that legitimate claims are settled without unnecessary delays.

In practice, fraudulent activities generally fall into a limited number of recurring patterns rather than entirely new categories. Common examples include timing-related fraud, where claims are submitted shortly after policy inception, unusual claim frequency or multiple claims within a short period, exaggerated claims involving inflated repair costs or overstated losses, and fabricated or staged claims in which losses or accidents are deliberately created or entirely fictitious. In life and disability insurance, fraudulent behavior may also include the continued receipt of benefits despite a return to work or the existence of additional undeclared income. Although these fraud schemes differ across insurance products and jurisdictions, they continue to evolve as fraudsters adapt their methods to existing controls.

Artificial intelligence is further changing the fraud landscape by increasing the sophistication and scalability of existing fraud schemes. Rather than introducing fundamentally new fraud categories, AI enables existing fraud schemes through the generation of convincing forged documentation, manipulated images, synthetic identities, and other AI-generated supporting evidence. Consequently, insurers are increasingly challenged to verify the authenticity of submitted information while adapting existing fraud detection capabilities to increasingly realistic fraudulent material.

Current fraud detection approaches therefore combine multiple analytical methods. Traditional rule-based controls remain important for identifying predefined fraud indicators, while claims analytics detect unusual claim amounts, frequencies, timing patterns, or other statistical anomalies. Predictive models estimate the likelihood of fraudulent claims based on historical observations, and network analytics identify relationships between claimants, repair shops, medical providers, brokers, or other connected parties that may indicate organized fraud. More recently, text analytics and large language models have been introduced to analyze unstructured claim narratives, adjuster notes, medical reports, and other supporting documentation for unusual linguistic patterns, inconsistencies, or contextual anomalies. Depending on the insurer, these methods are applied either independently or combined into integrated fraud scoring frameworks that support the prioritization of claims for further investigation. Such integrated approaches aim to improve detection performance while reducing false positives and unnecessary investigations, thereby allowing insurers to focus investigative resources on cases with the highest likelihood of fraud.

Despite significant advances in analytics and artificial intelligence, fraud detection remains subject to several practical limitations. Increasing expectations for rapid claims handling, together with the growing amount of unstructured information, place considerable demands on existing fraud detection capabilities. Furthermore, insurers must balance effective fraud detection with customer satisfaction, as excessive investigations may delay legitimate claim settlements and negatively affect the customer experience. While AI increasingly supports information extraction, document analysis, and investigative activities, human expertise remains essential for assessing plausibility, validating evidence, and making final claim decisions. As a result, current developments focus not only on improving fraud detection accuracy, but also on increasing operational efficiency through the more effective use of structured and unstructured data.

[1] Expert interview with Ramona Müller, Allianz Suisse Versicherungs-Gesellschaft AG, Fraud Intelligence Expert, conducted by Cindy Hofmann (KPMG AG, Advisory, Forensic, Director), 9 July 2026.



Ramona Müller from Allianz Suisse [left] in conversation with Cindy Hofmann from KPMG [right]. Two experts on the topic of fraud detection.

3.2.2 Quantum approaches and maturity

Fraud detection lends itself to exploration with quantum algorithms due to the need for advanced pattern discovery. The objective here, at least in the near term, is generally not for quantum approaches to beat all conceivable classical methods. Rather, the idea is to leverage the inherent high-dimensional space in which quantum algorithms operate as an additional lens for pattern analysis and as a complementary tool to enhance specific sub-routines within hybrid fraud detection pipelines. While such quantum machine learning approaches are generally still more of a heuristic nature, competitive results are already possible [73]. Quantum circuit simulations [73] can provide valuable insights and help discover and apply promising methods on entirely classical hardware, an approach that can and has been adopted in other use case areas as well while quantum hardware continues to mature.

For example, quantum support vector machines are being studied with regard to finding separation boundaries for classification tasks that do not exist in lower-dimensional spaces. Careful selection or even engineering of features may ultimately enhance fraud detection workflows [74]. Moreover, a study also considered explicitly that while quantum models might not outperform their classical counterparts in fraud-detection-related metrics (accuracy and others), the quantum techniques do tend to discover other patterns in the data, which can then be leveraged to construct hybrid quantum-classical meta-models that beat the individual quantum and classical models [75]. Further quantum algorithms, such as quantum principal component analysis, may help in terms of preprocessing fraud detection data such that the data becomes more tractable and fraudulent claim likelihoods can be determined with higher confidence levels [76].









Ramona Müller [top left]
Fraud Intelligence Expert, Allianz Suisse

Cindy Hofmann [top right]
Forensic Expert, KPMG

3.3 Valuation, pricing, and product personalization

3.3.1 Status and current challenges [2]

The insurance industry relies on a wide spectrum of valuation techniques to support its underwriting, pricing, capital and risk management, and financial reporting. These valuations cover not only traditional insurance liabilities (e.g., policy reserves, guarantees, and options embedded in contracts), but also the increasingly complex financial instruments insurers hold and issue: derivatives (such as interest rate swaps, options, and forwards), structured credit, private placements, and other debt instruments.

Complexity in valuation is driven primarily by two factors:

1. The volume of underlying instruments (ranging from just a handful of financial instruments to very large portfolios of assets and obligations); and
2. The sophistication of the valuation methodologies that market participants consider standard.

Simple instruments, such as a single unsecured debt liability with fixed cash flows, are often valued using straightforward discounted cash flow (DCF) techniques that are computationally light. By contrast, portfolios of derivatives with correlated underlying metrics, products with embedded optionality and asymmetric payoffs, or risk and capital models that use Monte Carlo simulations for value-at-risk (VaR) and other tail measures require extensive scenario generation and aggregation, which quickly become resource-intensive as portfolios grow.

In practice, current computational and data constraints mean insurers and valuation specialists frequently rely on approximations, segmentation, and model simplifications to keep calculations tractable and timely. This can include using higher level scenario grids, simplifying credit migration and recovery assumptions, or limiting the number of risk factors and correlations that are modeled across a portfolio. While these shortcuts are often necessary to meet reporting timelines and system limits, they can restrict the ability to fully reflect important real-world behaviors—such as policyholder lapse and retention dynamics, the interaction between market movements and insurance experience, and the way correlated risks build up across lines of business. The result is a familiar trade-off: higher realism and granularity typically mean higher run-times and operational burden, so organizations must balance accuracy, speed, and explainability.

These challenges are particularly acute for U.S. insurers as scrutiny increases around credit portfolios, privately rated and structured investments, and the rigor of underlying credit analysis. Evolving expectations from state insurance regulators and the National Association of Insurance Commissioners (NAIC)—around documentation, transparency of assumptions, and defensibility of processes supporting ratings and capital treatment—are pushing insurers toward more robust analysis and stronger evidence trails. Importantly, for insurers, credit risk is often not just about whether a bond defaults, but also about rating migrations (e.g., BBB to BB and beyond) because these transitions can drive capital requirements and solvency metrics even before any default occurs. That naturally increases the demand for more granular transition analysis, more expansive sensitivities, and larger-scale scenario testing—often across very large portfolios—where computational limits can become the bottleneck.

[2] Content provided by George Chirbas, Joseph O. Trujeque, Thomas D'Arminio, and Yosef Lugashi from KPMG US.

In cases where quantum algorithms exhibit favorable scaling with problem and system size, future quantum computers can give rise to particularly powerful quantum-classical computing architectures.

From a business perspective, the problems that strain today's methods share a common feature: they involve complex risk, uncertainty, and very large "state spaces" (many possible future paths and interacting drivers). Insurance liabilities are not "binary" payoffs; they are probability-weighted outcomes over long horizons driven by mortality, morbidity, catastrophe experience, lapse behavior, economic conditions, and other variables. When this is combined with complex contract features (embedded options, guarantees, path-dependent benefits) and non-trivial units of account, classical valuation and risk calculations can become slow and difficult to run at the level of granularity management would prefer. As a result, organizations may limit the number of scenarios, reduce the complexity of assumptions, or run certain analyses less frequently than they would ideally like.

This is also visible in risk simulations and scenario analysis more broadly. Many insurers would benefit from running more – and more targeted – stresses, including better coverage of tail events, management actions, and interactions across market and insurance risks. However, large-scale Monte Carlo-style simulations, nested projections, and repeated reruns for sensitivity and governance review can be expensive in time and cost. Similarly, portfolio optimization questions (e.g., capital allocation, reinsurance optimization, and asset–liability management under multiple constraints) can become difficult to solve when the portfolio is large, risks are correlated, and the constraint set is complex. These are areas where additional computational power would reduce the need for shortcuts and enable more complete decision support.

3.3.2 Quantum approaches and maturity

Against this backdrop, quantum computing is relevant not because it replaces valuation judgement, but because it targets the exact pain points described above: complex uncertainty, high dimensionality, and optimization at scale. The large state spaces mentioned earlier have a fitting quantum state space analogue, namely the Hilbert space. There has already been research with regard to leveraging the Hilbert space as a quantum-enhanced feature space [77].

As we consider valuation and pricing, optimization across a combinatorially large number of possible solutions and options is often required. This opens opportunities for the aforementioned quantum optimization methods, including annealing and QAOA. At the same time, there are relevant techniques that belong to the fault-tolerant class of algorithms, which have significant potential in the medium term. These include quantum amplitude amplification and amplitude estimation. Work has already been done that shows the greater efficiency of such approaches compared with traditional Monte Carlo methods in estimating risk [30], [78], [79].

In parallel, quantum machine learning may enable enhanced actuarial predictions and personalization of insurance products and services [80], [81]. With the trade-offs between the NISQ and the fault-tolerant era (practical implementation today vs. performance guarantees), there are a range of quantum machine learning tools that are already explored today, ranging from, for example, quantum kernel methods to quantum neural networks (QNNs).

In addition, research suggests that quantum computing may offer useful extensions for regression tasks and generalized linear models (GLMs) [82], [83]. This is worth noting because, for instance, GLMs are currently widely used in non-life insurance pricing [84].

For several applications in the insurance industry that rely on enhanced computational capabilities, such as highly granular portfolio calculations at policy level (of particular interest in life insurance) and detailed simulations involving large numbers of scenarios, an ongoing trend is to leverage scalable cloud resources and/or graphics processing units (GPUs), which enable highly parallel computations via thousands of GPU cores. Quantum computers are typically regarded as attractive complements to such technologies, as quantum parallelism (based on superpositions of computational basis states) differs fundamentally from CPU and GPU parallelism (using available cores). In cases where quantum algorithms exhibit favorable scaling with problem and system size, future quantum computers can give rise to particularly powerful quantum-classical computing architectures.

Of course, just having suitable quantum algorithms with (potential) speedups and improvements is not sufficient. For example, KPMG US's valuation and credit analysis experience suggests the limiting factor is often not knowing what analysis should be done but being able to operationalize it – across millions of cash flows and many portfolios, with appropriate governance, documentation, and turnaround time. These are all factors that need to be considered and therefore require months and years of planning and tests as quantum algorithms gradually make their way from lab to industry.

3.4 Risk modeling and catastrophe simulation

Cyber insurance illustrates the continued importance of appropriately combining human expertise with advanced technologies and automation in catastrophe and risk modeling.

3.4.1 Status and current challenges

Risk modeling is a cornerstone of the insurance industry, supporting critical activities such as pricing, reserving, capital management, reinsurance optimization, and regulatory compliance. Insurers and reinsurers rely on quantitative models to estimate the likelihood and financial impact of future events, ranging from individual claims to large-scale catastrophes. Given that liabilities can extend over decades and depend on inherently uncertain future developments, reliable risk models are essential for maintaining solvency and ensuring long-term financial stability.

Today, companies employ a broad spectrum of techniques including actuarial methods, stochastic simulations, and increasingly data-driven and AI-enabled approaches for scenario generation and evaluation. Despite significant progress in modeling capabilities, the industry continues to face substantial challenges. In many cases, limitations are not primarily driven by computational power but by data quality, model governance, the uncertain evolution of financial and risk landscapes (e.g., inflation and climate change), and the difficulty of accurately capturing rare or unprecedented events. Moreover, insurers and reinsurers must balance model sophistication with explainability, regulatory expectations, practical usability, and business decision-making needs. For example, capital requirements under regulatory frameworks such as Solvency II (EIOPA) or the Swiss Solvency Test (FINMA) can be calculated via standard and internal models. On the one hand, internal models can enable more precise results through closer adaptation to company-specific details. On the other hand, they usually entail significantly higher documentation and validation requirements, particularly in areas where they differ from standard practice.

Catastrophe simulation is an essential component of insurance risk modeling. It helps companies assess potential losses arising from natural and man-made extreme events, including hurricanes, floods, earthquakes, wildfires, pandemics, large-scale cyber incidents, geopolitical conflicts, and terrorism-related attacks. While particularly relevant for non-life insurers and reinsurers, catastrophe simulation also applies to life and health insurers, especially for events with a significant impact on mortality and morbidity. Given the challenges and resources required to model such low-frequency, high-impact events, companies often leverage results from catastrophe simulation providers and, where appropriate, apply rescaling techniques to better reflect their specific risk profiles. Substantial efforts are underway to further advance risk modeling in the insurance industry. Examples include climate change risk assessments [85] and the use of new technologies such as remote sensing and AI to better anticipate and mitigate natural disasters [86].

Artificial intelligence offers powerful technological means to enhance risk modeling. At the same time, it introduces new sources of risk, such as AI-enabled cyber threats [87], [88], [89], [90]. As a result, cyber insurance represents a prime example of a domain in which unprecedented events may have a significant impact on insurance risk [91]. While available information and AI-based tools can provide valuable support in assessing such emerging risks, expert judgement will likely remain a critical component. More broadly, cyber insurance illustrates the continued importance of appropriately combining human expertise with advanced technologies and automation in catastrophe and risk modeling.

Climate and catastrophe simulations may benefit from both near-term (primarily through quantum-enhanced optimization and machine learning) and long-term quantum methods.

3.4.2 Quantum approaches and maturity

Risk analysis has long been one of the prominent research areas for quantum algorithms in finance due to the inherent complexity of many risk-related problems and the suitability of certain quantum algorithms. These algorithms could therefore become core routines in risk modeling and the processing of actuarial data [92]. However, relevant quantum algorithms, such as quantum amplitude estimation, typically require fault-tolerant quantum computers [30]. In anticipation of the availability of such quantum computers, potential applications in, for instance, internal Solvency II models and quantitative risk management have already been explored [93].

Nevertheless, climate and catastrophe simulations may benefit from both near-term (primarily through quantum-enhanced optimization and machine learning) and long-term quantum methods [94]. This is illustrated by the following example. In a recent report by the AXA Research Fund [86], the combination of AI and remote sensing technologies, including drones and satellite imagery, was highlighted as a powerful approach to improved understanding and anticipation of natural catastrophes, creating opportunities for more effective risk assessments, early warning systems, and targeted interventions. Remarkably, quantum-enhanced satellite image classification [95] has already been demonstrated on real quantum hardware and may further advance the use of remote sensing technologies for catastrophe risk assessments and broader risk modeling capabilities. For instance, quantum-enhanced image classification may also improve the forecasting of crop yields and the quantification of agricultural and related insurance risks.

Finally, emerging quantum threats (see Section 4), particularly those related to cybersecurity, will require increasingly refined risk models. As with AI, quantum technologies can enable the development of advanced models but also create new risks that themselves require modeling.

3.5 Other opportunities

There is a wide range of further opportunities that are beyond the scope of this report. Nevertheless, a few should at least be mentioned in order to illustrate the many changes which quantum technologies will likely bring to the insurance sector and beyond.

A specific example is quantum random number generation (QRNG), where quantum mechanics enables true randomness, in contrast to traditional pseudo-random number generation methods. Among other applications, QRNG may be used as an input for stochastic simulations and, according to recent studies, has the potential to improve the quality of scenario sets and enhance the accuracy and efficiency of actuarial modeling [96], [97].

Furthermore, as different sectors adopt quantum technologies, new or revised insurance products and services (e.g., parametric products that offer specified payouts based on trigger events) will likely be needed to cover the associated risks. Similarly, new business models and industries will evolve as quantum computing, communication, and sensing companies grow. Investments in quantum technologies may also become a significant pillar of financial portfolios. New underwriting data could become available through the deployment of quantum sensors in geospatial settings and different types of infrastructure. Finally, the cybersecurity implications of quantum computing will drive both internal transformation and new business opportunities, including quantum-secure operations, insurance products addressing quantum cyber risks, and related advisory services.

3.6 Actuarial perspective on opportunities and challenges of optimization in the UK insurance industry

While the previous sections explored potential opportunities and insurance applications of quantum technologies, practitioners often face further challenges related to modeling, governance, regulation, and operationalization. The actuarial perspective [3] below provides additional context on current optimization practices, modeling constraints, governance, regulatory requirements, and the role that future advances in computing may play within the UK insurance market.

In the UK market, portfolio and capital optimization has progressed most visibly through the development and application of the Matching Adjustment (MA). Over the past several years, the MA has become the dominant area of optimization activity, especially among large insurers who were the earliest adopters. Its use has since spread broadly across the sector, though implementation maturity varies significantly. Despite its importance, the optimization work involved remains relatively new, with many firms still building capability, refining methodologies, and translating evolving regulation into operational frameworks.

From a technology standpoint, the industry continues to rely primarily on classical computing methods for optimization—approaches that have proven adequate for current needs. Firms report that compute time is rarely the bottleneck: once models are established, MA calculations can often run in under three minutes, even at company level. Some optimization engines mimic quantum-style formulations, but in practice classical computing power is sufficient. The true constraints lie upstream—in modeling complexity, data preparation, parameterization, and codification of regulatory rules. Setting up an optimization model requires navigating circular dependencies, intricate Solvency Capital Requirement (SCR) rules, and granular asset-level stresses. As a result, the biggest delays arise not from solving the optimization problem, but from determining what exactly should be optimized and how to structure the data and constraints. There is also the risk of conflicting objectives, such as hedging strategies that reduce SCR capital but generate adverse outcomes under IFRS 17, especially when positive market movements cause derivatives to offset gains.

Beyond MA-related optimization, insurers show wide variation in sophistication around hedging and balance-sheet risk management. Many firms still rely on expert judgement and manual, relatively simple sensitivity-based techniques to construct hedging portfolios. Given the interconnected nature of risks—especially interest rate risk, which impacts nearly all components of the balance sheet—firms often struggle to maintain consistency across regulatory, accounting, and risk perspectives. More advanced hedging methodologies do exist, but they are complex, bespoke, and time-consuming. Any technology that increases modeling speed or enables more extensive scenario testing could meaningfully enhance hedging effectiveness. However, challenges remain: sophisticated modeling requires high-quality, granular data; and the process is often limited by review and governance bandwidth, not by compute power.

In contrast to optimization work, risk calibration and modeling (e.g., distribution-based approaches) are generally more straightforward and less computationally demanding. Firms are exploring whether more advanced compute technologies—such as GPUs today or quantum computing in the future—could remove the need for proxy models or drastically accelerate valuation and scenario generation. GPU adoption is already emerging, though models often require restructuring to make effective use of parallel computation. Quantum computing could someday enable more general and complex models, but current quantum use-cases appear hyper-specific; problems must be redesigned for quantum rather than quantum adapting to existing actuarial formulations. As a result, quantum's transformational impact remains uncertain.

Cost–benefit dynamics also shape adoption. Large insurers have been the first to invest in optimization because the potential capital upside is substantial. Smaller insurers face similar implementation costs but with much smaller balance sheets, making it harder to justify large-scale optimization programs. Nevertheless, once leading firms prove an approach workable, the methods tend to trickle down through the market—reflecting a pattern where early innovation by large players later becomes mainstream practice.

[3] Content provided by Matthew Dunbar, incorporating contributions from Maynard Kuona, Matthew Murphy, Thomas Murphy, and Karen Parkinson of KPMG UK.



Across all of this, insurers face operational bottlenecks that slow progress. Stress and scenario testing remains challenging, as sensitivities must be produced frequently and quickly to be useful, yet many firms lack the tooling or automation to do so. In many cases, limitations arise not from computing hardware, but from the availability of skilled reviewers and risk experts. Governance processes, model validation, and audit requirements can also create drag, with internal audit teams often relying on sample checking – an area that may offer future potential for automation or advanced analytics.

Taken together, the current landscape shows a sector that has made meaningful progress – particularly through MA-driven optimization – yet continues to grapple with data, modeling, governance, and resourcing challenges. While compute constraints are rarely the primary obstacle, the complexity of the models, the breadth of regulatory requirements, and the capacity of people and processes remain the critical limiting factors. The next wave of progress will likely come not from raw computing power, but from better model design, smarter data infrastructure, more automated risk processes, and clearer alignment across regulatory and accounting frameworks.



3.7 Interview with AXA on its quantum journey

For insights from a pioneer in insurance-related quantum computing, we interviewed George Woodman (Quantum Computing Lead), Antoine Pietri (Thought Leadership Expert), and Marcin Detyniecki (Head of Research and Development & Group Chief Data Scientist) from AXA Group Operations.

Could you please tell us about your quantum journey at AXA?

When did it begin, and how have your activities and focus evolved over time?

We began our quantum journey at AXA in 2019. Our initial goal was to understand what quantum meant for us at a high level. We conducted a broad study on the state of the art, assessing the technical capabilities of existing hardware, monitoring large tech companies, and observing other financial institutions. We presented these findings internally to secure buy-in, which allowed us to form a full-time team dedicated to exploring quantum's potential in insurance.

Over the past seven years, our focus has evolved to become much more research driven and technical. Quantum is an extremely hyped technology, but we know it isn't going to solve every problem; it will only solve specific parts of highly complex problems. Our day to day involves identifying these precise use cases where quantum can deliver true value. We also prioritize aligning ourselves with international groups, other insurers, and tech companies. Cutting through the industry noise to discern what this technology means for our business is critical, and that remains our primary focus today.

Could you also share insights into your roles and activities at events like the EPFL Quantum Hackathon, as well as your key impressions from these experiences?

Our involvement with the EPFL Hackathon started because of our strong presence in both the quantum space and at EPFL. While all the other sponsors were quantum startups, our participation as an enterprise allowed us to bring a unique perspective to the hackathon. We created a specific challenge for the hackathon and acted as mentors.

A key differentiator for our challenge was that we didn't just give the students a pre-packaged optimization problem to run on a quantum machine. We required them to build the quantum algorithm themselves, starting from a classical insurance problem. In the real world, that translation step, mapping a classical problem to a quantum circuit is often the hardest part, and it was fascinating to see how students tackled that challenge.

Beyond hackathons, we regularly engage with internal communities to push quantum literacy. Our goal at all these events is to provide an unbiased, pragmatic perspective. Our priority isn't whether quantum arrives in two years or twenty; it's simply ensuring we are ready when it does.

What criteria guide your choice of quantum computing topics, and which use cases do you view as particularly promising for AXA in the short, medium, and long run?

Our team's criteria focus entirely on the calculation improvements the technology offers and how we can use these machines to generate value for AXA and our customers.

Short-term
We are focused on quantum-inspired algorithms. These are designed with quantum mechanics in mind but inherently run on classical computers, allowing us to extract value in production today.

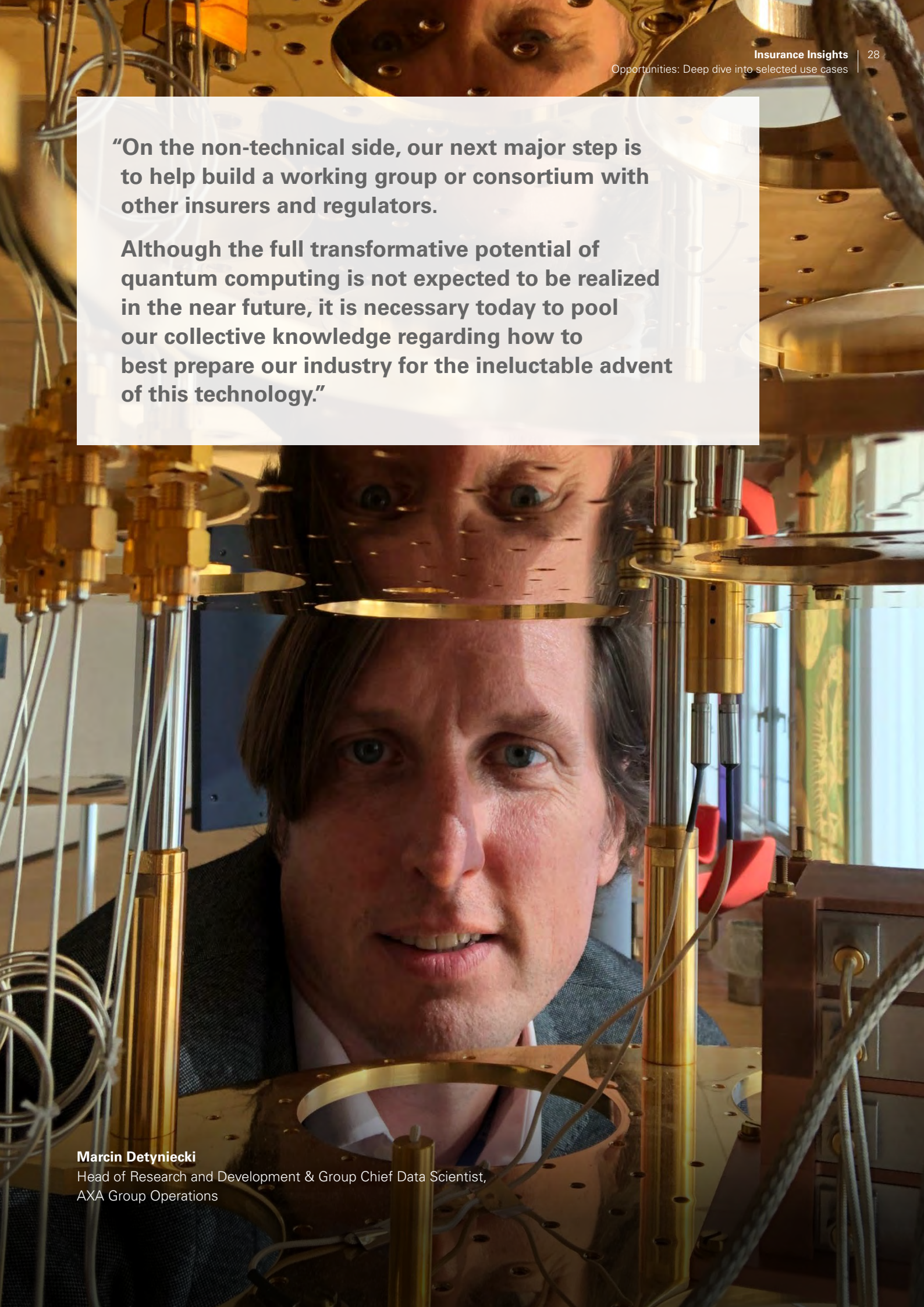
Medium-term
Optimization. The viability here depends heavily on the scale of the problem and the required speed and accuracy, but it is a highly promising area.

Long-term
Quantum machine learning and quantum-sped-up Monte Carlo simulations. These areas are far more nuanced and less understood within the quantum industry, but ones we are actively evaluating for their future impact, alongside ongoing engagements with our security teams to mitigate the threat quantum technologies pose.

In terms of similarities, differences, and expectations, how would you compare the emergence of quantum computing to the evolution of AI within AXA, and what benefits have you observed that inform your organization's path forward?

Both AI and quantum are highly complex, heavily hyped technologies where the early use cases weren't immediately understood. However, the differences are stark. AI is a general-purpose technology with a multitude of everyday applications. Quantum computing is much more focused. We can think of it as a highly specialized accelerator or co-processor, a very niche supercomputer, designed exclusively for the hardest possible mathematical problems.

Regarding expectations, I think quantum has suffered a bit from the AI comparison. People look at where AI is today compared to ten years ago and assume quantum will follow the exact same trajectory. That simply isn't true, which leads to fears of a "quantum winter." Quantum inherently requires entirely unique, highly complex hardware paradigms that AI never had to face.



"On the non-technical side, our next major step is to help build a working group or consortium with other insurers and regulators.

Although the full transformative potential of quantum computing is not expected to be realized in the near future, it is necessary today to pool our collective knowledge regarding how to best prepare our industry for the ineluctable advent of this technology."

Marcin Detyniecki
Head of Research and Development & Group Chief Data Scientist,
AXA Group Operations

"A great example is reinsurance optimization.

This was a massive number-crunching problem that simply wasn't being solved analytically within the business because it was too large to even tackle classically.

By taking it on with our quantum team, we managed to tackle it with quantum-inspired methods and deliver results."

Which misconceptions about quantum computing do you most often encounter?

How do you typically address them?

The most pervasive misconception is that a quantum computer gets its advantage by checking all possible solutions at the same time, like multiple classical computers executing in parallel. That's fundamentally incorrect. If it tried every outcome sequentially or in simple parallel, it wouldn't offer its unique advantage. Instead, a correctly designed solution can amplify good solutions and dampen bad ones.

Another major misconception is how quantum bits scale. While it takes an exponentially large number of classical bits to fully describe n quantum bits, most of that information disappears the moment you measure the quantum state. For example, just 10 quantum bits would require 2^{10} = 1,024 coefficients to fully describe, yet a single measurement collapses all of that down to just 10 classical bits. The advantage comes from the 2^{10} states interacting with each other before measurement.

Finally, the way we talk about speed is often misunderstood. It makes no sense to ask if a quantum computer is "a million times faster." The relevant question is whether it has an asymptotic advantage, meaning the advantage over its classical counterpart grows larger as the problem size scales toward infinity. Furthermore, quantum computers only provide this advantage for specific classes of problems, for example: factoring numbers, searching unstructured databases, and simulating other quantum systems.

What have been the key challenges in your quantum journey to date, how have they evolved, and what lessons learned or recommendations would you highlight?

The persistent challenge is finding actual, viable use cases within insurance. Finding complex problems is hard enough, but getting business buy-in is even harder. You are often dealing with problems that haven't even been fully modeled yet, or conversely, problems the business considers "solved" using classical methods. Selling the hype of quantum is easy; selling its practical application in a specific domain is very difficult.

Over the last few years, this has evolved positively as we've identified specific use cases. A great example is reinsurance optimization. This was a massive number-crunching problem that simply wasn't being solved analytically within the business because it was too large to even tackle classically. By taking it on with our quantum team, we managed to tackle it with quantum-inspired methods and deliver results. What was incredibly rewarding was that this effort catalyzed actuaries in other parts of the business to start exploring the same problem using other modern algorithms.

My biggest recommendation is to build an internal community early. Find the people dealing with those massive number-crunching problems and educate them on what quantum is. When the computing power finally scales up, having early access to that data, knowledge, and network of forward-looking people is invaluable.



As a short outlook, what are the next steps for AXA in quantum computing?

Technically, we are continuing our work on quantum-inspired algorithms to deliver immediate production benefits. We are also expanding our research into native quantum algorithms. Specifically, we have a workstream focused on Quantum Machine Learning, exploring how the expanded feature space offered by QML might improve our predictive models.

We are also deeply interested in very specific quantum optimization problems. Much of the optimization research currently shows near-quadratic speedups, meaning the improvement the quantum approach has over classical increases with problem size. We are actively looking for algorithms that offer super-polynomial speedups instead, where the advantage gets disproportionately larger the bigger the problem is. This distinction matters because, due to the quantum overhead required for error correction, quadratic speedups are often dragged down in practice, so we need the stronger compounding advantage that super-polynomial algorithms promise.

On the non-technical side, our next major step is to help build a working group or consortium with other insurers and regulators. This technology isn't arriving tomorrow and pooling our collective knowledge regarding how it can be properly utilized will benefit the entire industry.

04

Security threats

Quantum computing has the potential to break public-key cryptography (e.g., RSA, ECC) and may fundamentally reshape the cybersecurity landscape for the insurance industry. Advances in hardware, algorithms, and quantum error correction have accelerated progress toward cryptographically relevant quantum computers, increasing the urgency of action. We examine the implications for insurers and reinsurers, the evolving regulatory landscape, and practical considerations for building quantum resilience.

"Nobody is going to hold a press conference. The first cryptographically relevant quantum computer will be a state secret before it's a headline, and the people who need to know will be the last ones told. Plan for a threat you will never see announced."



Aaron C. Kemp
Senior Director of Quantum Research, KPMG US



The implications of quantum computing for the insurance industry are shaped by new opportunities (Section 3) as well as new threats and risks presented below. In Section 4.1, we introduce the threats that quantum computing poses to encryption and data security and examine those that are particularly relevant to the insurance industry. Section 4.2 provides an overview of post-quantum cryptography and quantum key distribution, while Section 4.3 discusses risk mitigation strategies, regulatory aspects, and typical steps toward quantum resilience. Finally, the interview with J. Foster Davis (BreachBits) in Section 4.4 sheds light on hackers' perspectives on the quantum era, their potential activities and attack vectors, and the resulting considerations and challenges for the insurance industry.

4.1 Quantum threat to encryption and data security

4.1.1 Introduction to quantum threats

Quantum computing threatens the asymmetric cryptography that secures nearly all digital communication today. The threat is not uniform. It falls almost entirely on public-key schemes. Two algorithms define it. Shor's algorithm, published in 1994, factors large integers and solves discrete logarithms in polynomial time, which breaks RSA, elliptic-curve cryptography (ECC), and Diffie-Hellman [98]. These schemes rest on the same underlying mathematical structure, so a method that breaks one can be adapted to break the others [99]. Grover's algorithm offers, in theory, a quadratic speedup against symmetric encryption and hashing [100]. Doubling key length restores the margin, so AES-256 and modern hash functions remain secure. The exposure is concentrated in RSA and ECC, which protect TLS sessions, digital signatures, VPNs, secure boot, e-banking, code signing and much more [99].

The resource estimates for an attack have fallen sharply and continue to fall. In 2021 the accepted figure for factoring a 2048-bit RSA integer was roughly 20 million noisy qubits. In 2025 Gidney reduced that to fewer than one million noisy qubits [101]. The same pattern now holds for ECC. In March 2026 Google Quantum AI, with co-authors from UC Berkeley, the Ethereum Foundation, and Stanford, estimated that the 256-bit elliptic-curve discrete logarithm over the secp256k1 curve, which underpins Bitcoin and Ethereum, can be solved with 1,200 logical qubits and 90 million Toffoli gates. On a superconducting architecture, the computations could run in minutes and would require fewer than half a million physical qubits, representing a near twentyfold reduction compared with prior estimates. The authors validated these figures with a zero-knowledge proof, allowing the estimates to be verified without publishing the attack itself [102].

Separate work shows Shor's algorithm running at cryptographically relevant scale on as few as 10,000 reconfigurable atomic qubits, with a P-256 discrete logarithm solvable in days on a 26,000-qubit machine [103]. Architectural work has lowered the count further, reporting up to a 138-fold reduction in physical-qubit overhead against a conventional monolithic baseline [104]. None of these machines exists yet, but the direction is consistent and the margin is narrowing. In September 2026, IonQ published an end-to-end blueprint for breaking secp256k1 with a 20,000-physical-qubit quantum computer [105], [106] and noted that the study is consistent with the company's hardware roadmap, which targets systems of that scale in the 2028 timeframe [9], [106]. In line with the rapid progress made in recent years, annual survey data indicate that quantum computers may be able to break current encryption standards sooner than previously expected [107].

Industry has moved from hedging to fixed dates. Google [108] and Microsoft [109] have each set 2029 as the target for completing the migration of their own systems to post-quantum cryptography, and Cloudflare [110] has committed to the same year. These are internal commitments, not predictions of when a quantum computer will arrive, but they indicate how the largest operators now read the risk.

The threat to confidentiality is present now, not only when a quantum computer arrives. In a "harvest now, decrypt later" attack, an adversary records encrypted traffic today and stores it until a capable machine can decrypt it [99]. Any data that must stay confidential beyond the arrival of that machine is already exposed. This is captured by Mosca's theorem (Figure 2), which compares three periods: the length of time data must remain secret, the time required to migrate to quantum-resistant systems, and the time until a quantum computer can break current encryption. Where the first two added together exceed the third, the organization is already behind [111].

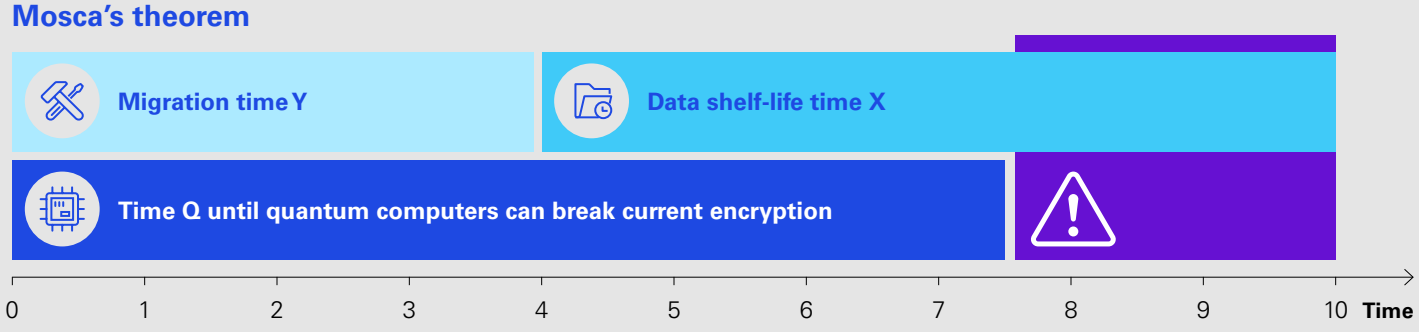


Figure 2 Illustration of Mosca's theorem using an exemplary timeline. If X + Y > Q, data that needs to remain secure can be exposed by cryptographically relevant quantum computers.

4.1.2 Insurance-specific threats

The quantum threat reaches the insurance sector through four specific exposures.

1 Actuarial and risk models

Pricing, reserving, and capital models, and the sensitive portfolio and claims data that feed them, sit behind the same public-key cryptography that quantum breaks. The exposure runs two ways. Confidentiality is lost when proprietary models and the data behind them are captured now and decrypted later. Integrity is lost when the digital signatures and authentication that protect model pipelines and their governance can be forged, allowing inputs, parameters, or outputs to be altered without detection [99].

2 Long-term confidentiality

This is the sharpest exposure for insurers, and it is most acute for health-related data. Swiss retention obligations for such records run long. A twenty-year retention applies in practice, driven by the twenty-year limitation period for personal injury in the Code of Obligations and reinforced by cantonal health law and the Electronic Patient Record Ordinance [112]. Under harvest now, decrypt later, anything captured today remains exposed for that entire window. On Mosca's terms, health insurers carry among the longest data shelf-lives of any sector, which moves their migration deadline forward rather than back [111].

3 Authentication infrastructure

Client portals, smartcards, and token systems that authenticate policyholders, brokers, and staff rely on RSA and ECC. The elliptic-curve discrete logarithm that secures TLS, passwordless and multi-factor authentication, electronic identity documents, and code signing is exactly the target of the latest resource estimates [102], [105]. Once it is broken, an attacker can impersonate users and forge the signatures these systems depend on, with no reliable way to tell a genuine credential from a forged one.

4 Partner ecosystem

Swiss health and accident insurers increasingly operate on shared infrastructure. Where such central platforms, their security operations providers, and other critical vendors are not made quantum-resistant, every insurer relying on them inherits the exposure. Under the revised FADP the insurer remains the controller and cannot transfer that responsibility to a supplier [113]; in the EU, the Digital Operational Resilience Act places the same third-party ICT risk directly on the board [114].

A quantum break does not just expose individual holdings; it undermines the enforceability of instruments that regulators have brought inside the financial system. PQC readiness is therefore a supervisory question as much as a technical one.

4.1.3 Impact on financial and blockchain systems used by insurance industry

Blockchain systems are more exposed than most, because their security rests almost entirely on elliptic-curve signatures. Ownership and transfer of a cryptocurrency or a tokenized asset is established by a signature over the secp256k1 curve, the same 256-bit elliptic-curve discrete logarithm that the latest resource estimates target [102], [105]. On a blockchain there is usually no recourse: forging a single signature enables theft that cannot be reversed. The Google Quantum AI analysis distinguishes two attack modes. A fast-clock machine can mount an "on-spend" attack, intercepting a transaction, breaking the key, and substituting a fraudulent transaction within the block time. A slower machine is limited to "at-rest" attacks on public keys that have been exposed on the ledger for long periods. Not everything is vulnerable. Bitcoin's proof-of-work consensus is unaffected and funds whose public keys remain hidden behind a hash are protected until the key is reused. The practical mitigations are to eliminate public-key reuse, minimize key exposure, and migrate to post-quantum signatures [102].

Within the Bitcoin community the migration has already begun to take concrete shape [115]. BIP-360, part of the official Bitcoin Improvement Proposals repository since February 2026, introduces a new output type that removes the quantum-vulnerable spending path exposing public keys on-chain, laying the structural foundation for post-quantum signatures. BIP-361, which followed shortly thereafter, complements this with a phased migration path that would gradually restrict and ultimately disable spending from quantum-vulnerable addresses [115].

This matters directly for insurance products built on distributed ledgers. Parametric and usage-based cover with automated smart-contract payouts, tokenized risk transfer, and on-chain reinsurance instruments all depend on the integrity of the signatures that authorize a payout or a settlement. If those signatures can be forged, a fraudulent claim can be triggered or a settlement redirected, and the automation that makes these products efficient becomes the channel through which they are attacked.

The regulatory position compounds the exposure. Under its 2018 ICO guidelines, FINMA classifies blockchain tokens as payment, utility, or asset tokens, with asset tokens treated as securities, and every transfer of such a token is signed with the holder's private key [116]. Switzerland's DLT Act gave ledger-based securities statutory footing in 2021 [117], and in the EU the Markets in Crypto-Assets Regulation now governs crypto-assets across the single market [118]. Each of these regimes assumes the integrity of the underlying signature. A quantum break does not just expose individual holdings; it undermines the enforceability of instruments that regulators have brought inside the financial system. PQC readiness is therefore a supervisory question as much as a technical one.

4.2 Post-quantum cryptography and quantum key distribution

PQC's security rests on computational hardness assumptions rather than formal proof, but the algorithms are standardized, deployable now, and differ only modestly from the cryptography they replace.

Two approaches are proposed to counter the quantum threat. They are not equivalent, and they solve different problems.

Post-quantum cryptography (PQC) replaces today's public-key algorithms with new ones built on mathematical problems believed to be hard for both classical and quantum computers. It runs in software on existing networks and covers the full range of public-key functions, both key establishment and digital signatures. NIST published the first three standards in August 2024: ML-KEM for key establishment (FIPS 203), and ML-DSA and SLH-DSA for signatures (FIPS 204 and 205). A FALCON-based signature standard (FIPS 206) is in draft, and in March 2025 NIST selected HQC, a code-based scheme, as a backup key-establishment algorithm built on a different mathematical basis to ML-KEM so that a weakness in one family does not compromise both [119]. PQC's security rests on computational hardness assumptions rather than formal proof, but the algorithms are standardized, deployable now, and differ only modestly from the cryptography they replace [99].

Quantum key distribution (QKD) takes a different route. It uses the properties of quantum physics to distribute a shared key between two parties, and any attempt to intercept the exchange disturbs it and can be detected. Its security is grounded in physics rather than computational difficulty. The limitations are practical and structural [120]. QKD needs dedicated hardware and a direct fiber or line-of-sight channel, it is distance-limited and point-to-point, and it requires trusted intermediate nodes over longer routes. It distributes keys but does not authenticate the parties and does not provide digital signatures, so it cannot replace public-key cryptography on its own and still relies on classical or pre-shared authentication. Its theoretical security also does not carry fully to real devices, which remain immature and exposed to physical side-channel attacks for which no established evaluation methodology yet exists [121].

The European and UK positions align. In a joint paper of January 2024, the security agencies of France, Germany, the Netherlands, and Sweden concluded that QKD is suitable only for niche use, is not yet mature enough from a security standpoint, and that clear priority should go to PQC [121]. In the UK, the NCSC advises PQC as the preferred approach and does not support QKD for government or military use. A 2026 study commissioned by the UK Department for Science, Innovation and Technology, drawing on interviews with 38 experts, found that the only current users of QKD outside academia are in banking and aerospace, and only in research, testbeds, and pilots rather than operational systems. Its consensus was that QKD suits specific high-value links, is unlikely to become a standalone technology, and would at most sit as an additional layer alongside PQC [122]. Work continues in parallel, most visibly through the European Commission's EuroQCI program, but as a supplement rather than a substitute. For an insurer, PQC is the primary path; QKD may be an additional measure for specific high-value links, discussed below.

4.3 Risk mitigation strategies and frameworks



"The transition to post-quantum cryptography is unlikely to happen all at once. Unlike Y2K, there is no single date when the world suddenly becomes quantum-safe.

Legacy systems will remain in place for many years, creating a prolonged period where cyber risk becomes a challenge not just for individual organizations, but for entire interconnected ecosystems.

The fact that regulators such as FINMA are already encouraging firms to develop PQC roadmaps shows that this is becoming a resilience issue today, rather than a technology issue for tomorrow."

Jakob Thyme
General Rep. & Country Manager for Switzerland,
Regional Manager SWIG (Switzerland, Israel & Gibraltar),
Lloyd's

4.3.1 PQC transition roadmaps, risk assessment frameworks, and regulations

Every major jurisdiction now has a PQC transition roadmap, and they converge on 2035 while differing in the detail. In the EU, the Commission issued a Recommendation in April 2024, and the NIS Cooperation Group published a coordinated implementation roadmap in June 2025. It takes a risk-based approach: Member States are to have national plans in place by the end of 2026, high-risk systems quantum-resistant by the end of 2030, and the transition substantially complete by 2035 [123]. The UK NCSC sets three milestones: discovery and planning by 2028, migration of high-priority systems by 2031, and full migration by 2035 [124]. In the US, NIST intends to deprecate RSA-2048 and ECC P-256 by 2030 and disallow them by 2035 [125], and the executive order of 22 June 2026 requires federal systems to migrate key establishment by 2030 and digital signatures by 2031 [22], [126].

The end dates are close, but the intermediate milestones, risk tiers, algorithm preferences, and legal force are not. Sector regulation adds a further layer. In the EU, the Digital Operational Resilience Act already requires financial entities to maintain encryption policies, key lifecycle management, and cryptographic agility [114], and NIS2 and the GDPR bear on the same systems; in Switzerland, FINMA supervision (see also the recent guidance on quantum computing [127]) and the FADP apply. For an international group, or one that spans several industries, reconciling these regimes into a single program is itself a substantial undertaking, and it is a recurring reason large organizations struggle to start.

What the roadmaps share is a prioritized, risk-based method, and two references make it concrete. The PQC Migration Handbook from TNO, CWI, and the Dutch AIVD sets out a quantum risk assessment methodology in its section 2.4, within a three-step structure of diagnosis, planning, and execution [128]. Europol's 2026 report for financial services builds a prioritization framework on a Quantum Risk Score, combining the shelf-life of the data, its exposure, and the severity of a compromise, together with a Migration Time Score for each use case [129]. This is Mosca's theorem applied at the level of individual systems. These frameworks describe what a company-specific roadmap must contain. Building one is addressed next.

4.3.2 Preparing the organization for quantum threats (operational readiness)

Readiness begins with a Quantum Security Readiness Program: a named owner, a multi-year plan with measurable milestones, and integration into the existing security and risk functions rather than a standalone project. The first substantive step, and one worth taking regardless of the quantum timeline, is a cryptographic inventory. The organization discovers where cryptography is used across applications, networks, identities, certificates, stored data, and third-party services, records what each instance protects and who owns it, and maintains that inventory as a living asset [128]. Without it, no reliable judgement of urgency or scope is possible.

The inventory is then classified by criticality. Client and health data, signature and authentication mechanisms, TLS, and backup encryption do not carry equal risk, and the ranking follows the same three factors used in the Europol framework: how long the data must stay confidential, how exposed it is, and the severity of a compromise [129]. High shelf-life, high-exposure assets are migrated first. Migration paths are then planned in line with the EU, BSI, and NIST roadmaps, favoring standardized hybrid schemes that run post-quantum and classical algorithms together during the transition, and building cryptographic agility so that algorithms can be replaced later without re-engineering the systems that use them [123], [128]. Existing risk taxonomies are extended to carry a distinct "quantum-induced threats" category, so that the exposure is tracked, owned, and reported through the same governance as every other enterprise risk rather than sitting outside it [128]. Finally, the organization assesses whether QKD adds anything for specific high-value links; for most, PQC is sufficient, and QKD is considered only as a supplementary measure [121], [122], addressed next in Section 4.3.3.

The second line of defense (risk management, compliance, and oversight) has important responsibilities throughout the transition to PQC [130], such as ensuring that the program is auditable, progresses according to plan, is defensible to boards, regulators, and clients, and that PQC implementations are resilient against side-channel attacks and other implementation risks. The role will extend beyond the migration itself and include ongoing cryptographic auditing, monitoring developments in complementary technologies, and updating risk management frameworks as appropriate [130].

The intended model is not QKD instead of PQC, but PQC as the foundation with QKD as an additional layer on a small number of high-value links.

4.3.3 QKD networks and dual strategies

QKD today exists mainly as metropolitan testbeds rather than production systems. Switzerland has been a center of this work for two decades. The state of Geneva used QKD to protect the transmission of vote counts in its 2007 elections, the first government use of the technology [131], and the SwissQuantum network ran QKD across the Geneva metropolitan area, with one node at CERN, for more than eighteen months in 2009 to 2011 [132]. A new cantonal Geneva Quantum Network launched in 2025, linking the University of Geneva, CERN, and HEPIA over the canton's fiber backbone [133]. Comparable testbeds run elsewhere: BT and Toshiba operate the London Quantum-Secured Metro Network, and Singapore runs the National Quantum-Safe Network. All remain pilots, consistent with the finding that QKD has no fully operational deployments at scale [122].

The intended model is not QKD instead of PQC, but PQC as the foundation with QKD as an additional layer on a small number of high-value links. Several banks are testing exactly this. HSBC was the first bank to join the London metro network, trialing QKD between its Canary Wharf headquarters and a data center in Berkshire [134] and later using it to protect a simulated foreign-exchange transaction [135], [136]. JPMorgan Chase has demonstrated a network that layers the two, with QKD securing lower network layers and PQC at the application layer [137], [138]. In Singapore, the Monetary Authority of Singapore ran a QKD sandbox with several banks, including DBS, HSBC, OCBC, and UOB, and concluded that QKD can add protection on high-value links but that its trusted nodes need stronger, auditable assurance and its providers greater interoperability before wider use [139]. Further examples of banks with QKD pilot projects include Danske Bank [140], Erste Group [141], Santander [136], and Wells Fargo [142].

For a Swiss insurer, the reading is consistent with the European and UK agency positions set out above. PQC is the mandatory foundation and the priority. QKD is worth monitoring and, for a small number of fixed high-value connections between owned sites, such as a headquarters and a disaster-recovery center, may add defense in depth. But it does not authenticate the parties, does not provide signatures, and is not yet mature enough to rely on alone. It is a supplement, not a substitute, and it does not change the migration priorities already set out.

4.4 Interview with BreachBits on hackers in the quantum era



J. Foster Davis
Co-Founder & COO,
BreachBits

To complement the perspectives presented throughout this white paper, we conducted an interview with J. Foster Davis, Co-Founder and COO of BreachBits, to explore how malicious actors may identify and exploit emerging vulnerabilities in the quantum era.[4]

The discussion focused on four topics from a hacker's point of view: industry adoption of quantum computing, post-quantum cryptography, quantum key distribution, and the implications of cryptographically relevant quantum computers. For each topic, we examined potential vulnerabilities, attack scenarios, mitigation measures, and what these developments may mean for insurers and reinsurers.

The summary below highlights key insights from the interview, including considerations for insurers and reinsurers seeking to strengthen resilience against quantum-related risks.

Focus on economically motivated external attackers

Before discussing specific vulnerabilities and attack scenarios, it is important to clarify the type of attacker considered throughout this interview. Not all malicious actors have the same capabilities, motivations, or level of access, and they may pursue very different objectives.

At one end of the spectrum are threat actors who combine deep technical expertise, extensive domain knowledge, and privileged access to an organization's systems, processes, and personnel. Such a combination can significantly increase an attacker's ability to identify and exploit vulnerabilities and therefore represents one of the most dangerous threat scenarios organizations may face. However, as such scenarios are comparatively uncommon, they are not the primary focus of this discussion.

Likewise, nation-state actors, insider threats, and hacktivists are largely outside the scope of this analysis. While such actors may pose significant risks, their motivations, resources, capabilities, and access often differ substantially from those considered in this discussion.

Instead, the interview focuses on economically motivated external attackers seeking financial gain through activities such as theft, fraud, extortion, or ransomware. These attackers typically operate from the public internet and do not possess privileged access to an organization's systems or processes. While their level of sophistication may vary, ranging from opportunistic individuals to highly organized and mature criminal groups, their primary objective is typically to identify a viable path to monetizing unauthorized access, stolen information, or disruption.

[4] The interview sessions with J. Foster Davis (BreachBits, backed by Lloyd's) were conducted jointly by Christoph Kloeffel (KPMG) and Jakob Thyme (Lloyd's of London) between April and June 2026.

TOPIC 1

Industry adoption of quantum computing

For the attackers considered here, some of the most attractive opportunities may arise not from quantum computing itself, but from the organizational changes surrounding its adoption. New teams, employees, vendors, and business processes may create opportunities for social engineering and impersonation attacks. Attackers may attempt to gain trust by posing as newly hired specialists, external partners, or other stakeholders involved in quantum initiatives. The increasing use of AI may enhance the sophistication and credibility of such attacks.

Additional opportunities for exploitation may emerge through quantum-related systems and services, including cloud-based quantum computing platforms (e.g., API keys for access), proprietary algorithms and other intellectual property, as well as sensitive project information. Where quantum hardware is operated directly, supporting infrastructure such as cooling systems, power infrastructure, and other operational technology may also become potential targets. Such incidents may affect not only organizations using quantum computing but also suppliers and service providers operating the infrastructure that enables quantum computing services.

Overall, these attackers are likely to focus less on the underlying quantum technology and more on the people, processes, IT systems, and infrastructure surrounding quantum initiatives.

TOPIC 2

Post-quantum cryptography

The migration to post-quantum cryptography (PQC) is a complex, multi-year transformation involving numerous internal and external stakeholders. As a result, many of the social engineering risks discussed before may also apply to the PQC transition. New tools, vendors, processes, and responsibilities may create opportunities for impersonation, trust-based attacks, and other forms of exploitation.

A key consideration is the prioritization of systems, applications, and information assets. Since not everything can realistically be migrated at once, organizations need to determine which assets require the highest level of protection and should therefore be addressed first. From an attacker's perspective, unclear priorities or inconsistent implementation may create opportunities to identify gaps and vulnerable areas that receive less attention in PQC transition programs.

At the same time, migrations of this scale are likely to involve many mistakes and lessons learned along the way, especially at the beginning. While protecting critical assets remains the primary objective, it may be beneficial to validate technologies, procedures, and governance processes on lower-priority systems and data before applying them to crown-jewel assets. Penetration testing, red teaming, and related activities can identify and address weaknesses early in the process. Robust backup, recovery, and key-management practices may help reduce the risk of accidental data loss, corruption, or operational disruption during the migration and beyond.

Even where PQC is implemented as intended, data must be accessed, processed, and presented to users. As a result, attackers will often focus on endpoints, people, or the processes surrounding the use of protected information rather than attempting to compromise the cryptographic algorithms. Strong cryptography therefore reduces only part of the attack surface. The effectiveness of a PQC program depends largely on how the migration is planned, prioritized, governed, tested, and executed.

TOPIC 3

Quantum key distribution

Quantum key distribution (QKD) introduces dependencies on specialized hardware, communication infrastructure, service providers, and processes. As a relatively new technology for many organizations, QKD deployments may involve a significant learning curve and related challenges.

While imperfections in practical QKD implementations may give rise to additional attack vectors, malicious actors may seek opportunities in the surrounding ecosystem, including hardware, infrastructure, suppliers, and personnel, particularly during installation and deployment. Disruptions to communication links or supporting infrastructure may force users to rely on alternative procedures, potentially creating additional opportunities for exploitation.

Consequently, the security of a QKD deployment depends not only on the protocol itself, but also on the integrity, availability, and trustworthiness of the surrounding ecosystem.

TOPIC 4

Cryptographically relevant quantum computers

The prospect of cryptographically relevant quantum computers (CRQCs) may alter attacker incentives long before such systems become widely available. Attackers may balance the delayed benefits of future decryption against the immediate gains available through traditional attacks. As storage costs are already low and continue to decline, attackers may increasingly be willing to collect large volumes of encrypted data today and defer exploitation until future quantum computing capabilities become accessible.

The cost-benefit analysis for such harvest-now-decrypt-later attacks depends largely on the expected future value of the information. Intellectual property, sensitive personal information, and other forms of long-lived or "evergreen" data may therefore become particularly attractive targets. Malicious actors with access to an organization's information may also seek to remain undetected for longer periods in order to maximize data collection.

Access to CRQC resources may itself become a valuable target. Attackers may attempt to gain such access through compromised accounts, fraudulent identities, social engineering, or other means designed to circumvent access controls. More broadly, future quantum computing capabilities may influence not only which data attackers seek to obtain, but also how they prioritize, time, and monetize their attacks.

The insurance industry as an enabler of quantum innovation and resilience

Several of the discussed threats present particular challenges for the insurance industry because their consequences could emerge only after extended periods of time. For example, harvest-now-decrypt-later attacks create long-tail exposures in which data is compromised today but only becomes exploitable years later. This latency may complicate risk assessment, underwriting, policy design, and the management of future liabilities.

Organizations holding intellectual property or other information with enduring value are likely among the first to seek protection against such risks. At the same time, uncertainty regarding the timing, probability, and severity of quantum-related incidents may make underwriting decisions difficult. Helping policyholders assess how these risks apply to their own organization may therefore become increasingly important.

Beyond risk transfer, insurers can play an important role in strengthening quantum resilience. Just as cyber insurers have helped drive the adoption of controls such as multi-factor authentication, insurers can contribute to identifying, shaping, and promoting quantum resilience practices. By focusing first on the most tangible and relevant quantum-related challenges, the insurance industry can help improve preparedness before quantum-related attacks become widespread.

In addition, insurers can support the broader adoption of quantum technologies by providing risk transfer mechanisms for organizations developing, operating, or relying on quantum-enabled products and services. Insurance can therefore serve as a vehicle for both resilience building and the enablement of quantum technologies and innovation.

05

Emerging challenges for the insurance industry and recommended actions

Quantum technologies have implications that extend far beyond individual use cases or cybersecurity considerations. Insurers and reinsurers must navigate an evolving landscape shaped by new opportunities, emerging risks, regulatory expectations, and growing ecosystem complexity. The resulting challenges call for actions that can help organizations maintain trust, remain competitive, and build long-term resilience in the quantum era.

5.1 Key challenges

Quantum technologies create numerous challenges for the insurance industry. While many of these have already been discussed in detail in previous sections, we highlight eight key challenges below.



1 Competition for quantum talent and expertise

As interest in quantum technologies grows, insurers and reinsurers face increasing competition for a limited pool of subject matter experts. Demand for quantum talent extends across industries, including technology firms, startups, large corporations, and academia [143]. Particularly scarce are professionals who combine quantum expertise with deep industry knowledge and can translate technological developments into business-relevant applications. This may limit the ability of insurers and reinsurers to identify opportunities, understand risks, and make informed strategic decisions.

2 Quantum ecosystem dynamics and growing diversity of tools

The quantum ecosystem is evolving rapidly, as reflected in the large number of startups, partnerships, and technological innovations in recent years. While the range of available tools, platforms, and providers continues to expand, assessing competing solutions and identifying those most relevant to specific business needs may become increasingly difficult.

3 Global quantum race and geopolitical tensions

Quantum technologies are increasingly shaped by national technology strategies and international competition. Considerations relating to technology sovereignty, export controls, data protection, and cross-border data transfers may influence how organizations access and use emerging technologies. For example, questions regarding where sensitive data may be stored or processed, and where quantum hardware is physically located, could become increasingly relevant. As a result, geopolitical developments may influence technology choices, partnerships, and operating models across jurisdictions.

4 Security threats and new attack vectors

Quantum technologies introduce security challenges for organizations, ranging from threats to cryptographic systems and sensitive data to vulnerabilities associated with the adoption of new technologies. At the same time, advances in areas such as quantum computing and artificial intelligence may enable increasingly sophisticated and previously unseen attack methods. Identifying, assessing, and mitigating emerging security risks may therefore become significantly more complex for organizations in the insurance industry and beyond.

5 Compliance with laws and regulatory expectations

The regulatory landscape surrounding quantum technologies is likely to continue evolving as governments and regulators respond to emerging opportunities and risks. For example, the Swiss Financial Market Supervisory Authority FINMA recently issued guidance on quantum computing and announced that it will continue to actively monitor developments while increasing its supervisory focus on the topic [127]. Across the globe, several frameworks for building quantum resilience have been published, and some of the associated timelines have already accelerated. For multinational and cross-industry organizations, navigating diverse legal requirements and applicable frameworks may add further complexity to their compliance efforts.









Jakob Thyme from Lloyd's [top center] in conversation with KPMG's Christoph Kloeffel [left] and Alexander Lacher [right], discussing emerging challenges and recommended actions.

> **"One of the more interesting questions for the insurance industry is whether data stolen today could lead to losses many years from now if it becomes decryptable in the future.**
>
> **That challenges us to think differently about long-term cyber exposure, how it may develop over time, and how those risks should be reflected in our scenarios and risk assessments."**

Jakob Thyme
General Rep. & Country Manager for Switzerland,
Regional Manager SWIG (Switzerland, Israel & Gibraltar),
Lloyd's



6 **Limitations imposed by existing process landscapes**
Many potential quantum applications may not align naturally with existing workflows, operating models, and decision-making processes. In the insurance industry, tightly coordinated processes such as financial and actuarial closing activities are subject to strict timelines, internal control requirements, and the demands of multiple reporting frameworks, such as local GAAP, IFRS 17, SST, and Solvency II. Consequently, approaches that appear promising in isolated proofs of concept may be difficult to integrate into productive environments if the required data, dependencies, approvals, or control activities are not available at the necessary point in time. Technological feasibility therefore does not automatically translate into operational feasibility.

7 **Impacts of evolving risk landscapes on products and services**
Insurers and reinsurers may face increasing pressure to ensure that their products, services, underwriting approaches, and pricing methodologies remain aligned with changing customer needs and risk environments shaped by quantum technologies. Keeping pace with these developments may prove critical for maintaining a market-relevant, competitive, and responsible portfolio.

8 **Overarching challenge: Maintaining trust and competitiveness in the quantum era**
Taken together, the challenges discussed above highlight a broader strategic imperative for insurers and reinsurers: maintaining trust, competitiveness, and long-term resilience in an increasingly quantum-enabled world. This overarching challenge also encompasses related considerations such as governance, intellectual property, and digital transformation.

5.2 Recommended actions



While the details of the journey toward quantum readiness will vary across organizations in the insurance industry, many foundational priorities are shared. We have identified twelve recommended actions, grouped thematically and presented in no particular order, that should be pursued today to address the challenges outlined above.

Unlike a typical technology-innovation agenda, these actions are not purely opportunity-driven. While some recommendations focus on exploring potential applications of quantum technologies, others address security threats (e.g., harvest-now-decrypt-later attacks) and regulatory requirements that apply regardless of whether and when an organization adopts quantum computing itself. In addition, insurers and reinsurers should assess the potential implications of the quantum era for products, services, and risk transfer mechanisms. Innovation-related activities follow the more familiar pattern of structured exploration, with the caveat that quantum computing is expected to remain a specialist rather than a general-purpose technology.

Strategy and Governance

1. **Establish quantum governance and executive ownership**
   Define clear roles, responsibilities, and accountability for quantum-related opportunities, risks, and preparedness activities.
2. **Strengthen leadership understanding of the business implications of quantum technologies**
   Enable informed prioritization, resource allocation, and strategic decision-making.
3. **Develop an internal R&D and innovation strategy**
   Establish a structured approach to identifying, evaluating, and testing emerging technologies and trends, including quantum computing, to enhance organizational flexibility and preparedness.

People and Ecosystem

4. **Promote organization-wide quantum literacy alongside specialist expertise**
   Enable employees to recognize potential quantum-related opportunities and risks, while building deeper expertise in teams responsible for evaluating and implementing quantum solutions. Unlike AI, quantum computing is likely to remain a specialist capability applied to selected use cases.
5. **Actively engage with the quantum ecosystem**
   Build relationships with technology providers, academic institutions, startups, and industry peers. Participate in dedicated events, industry consortia, and collaborative initiatives to keep pace with the evolving quantum landscape, foster an innovation culture, accelerate capability building, and access scarce expertise.
6. **Establish mechanisms to monitor emerging developments**
   Maintain a structured view of technological, regulatory, market, and ecosystem developments to identify relevant opportunities, risks, and strategic implications early.

Security and Quantum Resilience

7 **Establish and maintain a cryptographic inventory and assess quantum-related risks**
Identify cryptographic assets and dependencies to understand exposure to quantum threats and inform prioritization. Progressively evolve the initial cryptographic inventory into a comprehensive and continuously maintained asset that supports detailed quantum risk assessments and monitoring.

8 **Develop a roadmap for the transition to PQC and cryptographic agility**
Establish a multi-year transition plan with measurable milestones, aligned with the organization's strategy and informed by the cryptographic inventory and quantum risk assessments. Prioritize migration activities based on criticality and implementation dependencies. FINMA recommends that supervised institutions develop a PQC roadmap by mid-2027 at the latest [127] and underscores the importance of cryptographic agility. The need to support crypto-agility is likewise emphasized in several international initiatives and publications, including the coordinated implementation roadmap for EU Member States [123], the PQC Migration Handbook [128], and a recent report by the G7 central banks [144].

9 **Monitor developments in quantum key distribution and related technologies**
Evaluate potential use cases where QKD may provide additional security benefits, taking into account regulatory and technological developments, implementation and security requirements, and infrastructure dependencies. Participation in pilot projects can help provide practical insights and support informed decision-making.

Quantum Technology Adoption and Insurance Innovation

10 **Identify and prioritize promising quantum use cases**
Assess potential applications of quantum technologies across the insurance value chain and the organization's existing processes. Prioritize opportunities based on business relevance, expected value, technical feasibility, data availability, and implementation requirements.

11 **Explore and validate prioritized quantum applications**
Actively investigate opportunities through proofs of concept and pilot projects, leveraging simulations and experiments on available classical and quantum platforms, in line with the organization's broader R&D and innovation strategy. Such initiatives can help build practical expertise, assess technical feasibility, benchmark performance against existing approaches, validate expected benefits, and prepare for future integration into business processes, data pipelines, and internal control systems.

12 **Assess the implications of the quantum era for insurance products and services**
Establish dedicated working groups to evaluate how quantum technologies may affect insurance and reinsurance products, underwriting, pricing, and risk transfer mechanisms. For example, insurers may need to assess how cyber insurance coverage and policy conditions should evolve in response to emerging quantum-related risks and PQC transition expectations (e.g., implications if a company delays its PQC migration). As risk carriers, insurers and reinsurers play an important role not only in providing coverage for emerging risks, but also in incentivizing effective risk mitigation measures and strengthening resilience across industries.



"The real-world value of quantum computing applications will depend on how well they integrate with surrounding processes, modeling frameworks, internal controls, regulatory requirements, data pipelines, and business timelines.

As insurers and reinsurers face constraints that extend well beyond computational power, they should not treat use case development as a standalone innovation project.

The most successful quantum initiatives will likely be those designed from day one with the broader operating environment in mind."

Christoph Kloeffel
Quantum Technology Lead,
KPMG Switzerland

06

Outlook $|\psi\rangle$

The quantum era will not be shaped by technology alone, but also by how effectively stakeholders across the ecosystem work together. As quantum technologies continue to evolve, collaboration, knowledge sharing, and coordinated action can help strengthen resilience and accelerate innovation. For the insurance industry, the years ahead are likely to be both demanding and defining, offering new possibilities while requiring careful preparation.

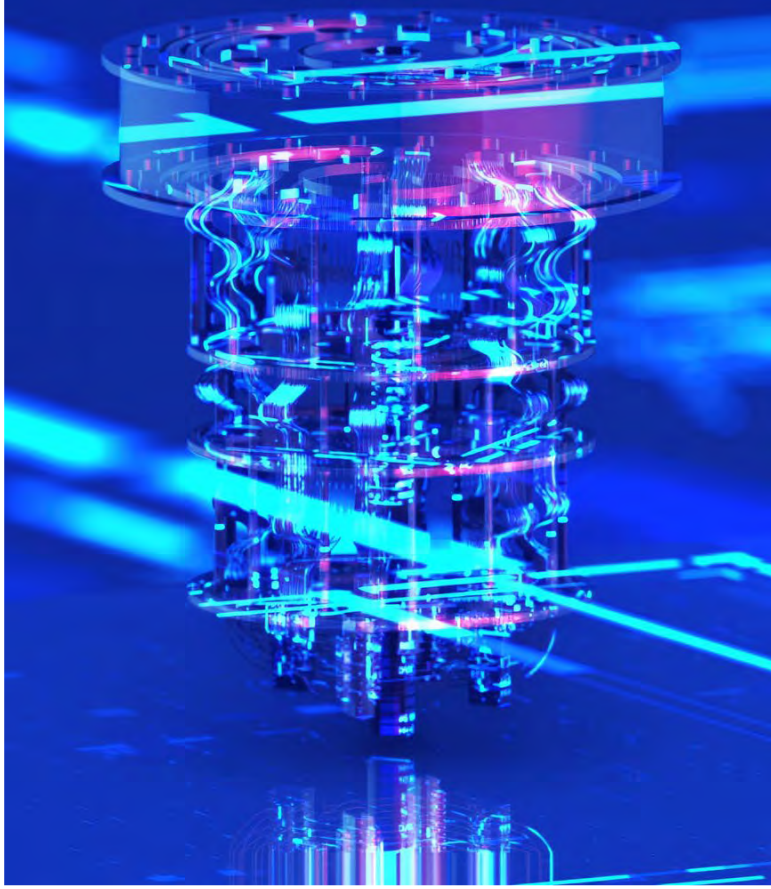
6.1 Entering the quantum era

As discussed throughout this report, quantum technologies have transformative potential for the insurance industry while also creating new risks that organizations must address. Although the pace and ultimate impact of future developments remain uncertain, recent progress has underscored the need for insurers and reinsurers to pursue quantum readiness.

Organizations across the insurance industry are approaching this journey from different starting points. While some have already been actively exploring quantum technologies, assessing potential use cases, and implementing quantum resilience initiatives, others are at an earlier stage. The path toward quantum readiness will vary across organizations and functions, reflecting different strategic priorities, business needs, and operating environments. Nevertheless, many foundational priorities are shared across the industry and provide opportunities for organizations to learn from one another and advance collectively.

Cooperation across industry, academia, technology providers, regulators, and other stakeholders can accelerate progress, foster innovation, and help insurers and reinsurers navigate the evolving quantum ecosystem. An exciting and challenging period lies ahead. Organizations that start early and take meaningful steps today will be best positioned to build resilience, maintain trust, and strengthen competitiveness in the quantum era.

Organizations that start early and take meaningful steps today will be best positioned to build resilience, maintain trust, and strengthen competitiveness in the quantum era.





6.2 Lloyd's perspective on developments since the 2021 report, innovation, and the future of insurance

We spoke with Dawn Miller, Chief Commercial Officer of Lloyd's and CEO of Lloyd's Americas, whose responsibilities include market development, regulatory engagement, strategic partnerships and innovation across Lloyd's global network.



Ben Harris [left]
Head of Commercial & Speciality and
Lloyd's Relationship Lead, KPMG UK

Dawn Miller [right]
Chief Commercial Officer, Lloyd's
CEO, Lloyd's Americas

Ben Harris Looking back at Lloyd's 2021 report on the impacts of quantum computing on insurance, which developments since then stand out to you?

Dawn Miller What stands out most is that quantum computing has moved from being a long-term, theoretical topic to a practical resilience issue that insurers have the opportunity to address today, with a clear focus on driving meaningful impact at scale.

Lloyd's 2021 report highlighted both the opportunities and the cyber security risks associated with quantum computing. Since then, progress in quantum hardware, error correction and technology roadmaps has made those developments feel much more tangible and immediate.

For insurers, the opportunity is not only the potential to improve areas such as risk modeling, optimization and fraud detection. We also need to be clear-eyed about the resilience implications. As the white paper highlights, organizations should already be preparing for risks such as "harvest now, decrypt later" attacks by understanding their cryptographic exposure, assessing quantum-related risks and planning their transition to post-quantum security.

At its heart, this is about trust. Insurance depends on confidence in the systems, data and relationships that underpin our industry. As technology evolves, maintaining that trust must remain a priority.

Reflecting on your experience, including work with the Lloyd's Lab and the Lloyd's Academy, what broader lessons can the insurance industry draw from preparing for emerging technologies such as quantum computing?

One of the most important lessons is that preparation needs to begin before technology reaches maturity. Emerging technologies rarely arrive as a single disruptive moment. More often, they develop gradually, creating opportunities and risks long before widespread adoption. The organizations that are best positioned tend to be those that build understanding early, test assumptions and develop capability in advance. The Lloyd's Lab was created to foster exactly that kind of collaboration, bringing together innovation and market expertise to develop and explore new solutions.

A second lesson is the value of structured experimentation. Through programs such as the Accelerator, ICX and Lab Discovery, the Lab helps organizations test ideas, validate solutions, identify practical applications and consider how successful ideas can be scaled. Parsyl is a good example of that journey; after joining the inaugural Lloyd's Lab cohort in 2018, it established Syndicate 1796 as a Syndicate-in-a-Box in 2021, providing a framework to test and prove its model, and has now received in-principle approval to transition to a full Lloyd's syndicate.

The third lesson is the importance of building capability early. As the white paper highlights, that includes governance, executive ownership, quantum literacy, specialist expertise and active engagement with the wider ecosystem. The Lloyd's Academy supports that by helping insurance professionals build the knowledge and confidence needed to navigate emerging risks and technologies.

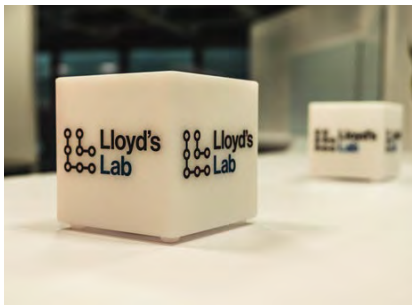
The question is not whether technology will continue to change our industry. It is how prepared we are to respond to those changes with discipline, confidence and a clear understanding of the risks involved.



“At its heart, quantum resilience is about trust.”

Dawn Miller





"Innovation is strongest when different parts of the market contribute different strengths."

Dawn Miller

How can insurers and reinsurers balance peer collaboration on innovative solutions with competitive considerations such as the development and protection of intellectual property?

The principle is straightforward: collaborate where the industry faces shared challenges, but compete on how those challenges are addressed.

We see that through Lloyd's Lab, which provides an environment where market participants can test ideas, share insights and explore new solutions together, reducing the cost and risk of innovation for individual firms.

That distinction is particularly important when we think about quantum computing. As the white paper highlights, building awareness, developing standards, strengthening resilience and understanding emerging risks are challenges that benefit from collaboration across insurers, technology providers, academia and regulators.

At the same time, firms will continue to differentiate themselves through their underwriting expertise, product innovation, proprietary data, technology capabilities and client service. That approach can strengthen the market, while allowing organizations to compete on the value they create for their customers.

How do you see the roles of large and small insurers and reinsurers evolving to drive innovation, and how might company size or other characteristics influence opportunities to shape the future of quantum in insurance?

Innovation is strongest when different parts of the market contribute different strengths.

Large insurers and reinsurers bring scale, capital, data and operational capability, while smaller insurers, MGAs, coverholders and start-ups often bring agility, specialist expertise and fresh thinking. The Lloyd's Lab helps bring those groups together, connecting innovators with market experts to test and refine solutions.

Quantum computing is likely to follow a similar pattern, it will remain a specialist technology for selected use cases, and success will depend on combining broad market awareness with deeper expertise in specific areas. Smaller firms may lead in developing innovative tools and services, while larger organizations may help drive adoption through their scale, resources and market influence.

This is where the Lloyd's market is particularly well placed through its ability to make innovation accessible to firms of all sizes. Through the Lloyd's Lab, organizations can access expertise, develop promising ideas and support their wider adoption, helping the whole market prepare more effectively for future opportunities and risks.



What skills, capabilities, and mindsets will be most important for insurance professionals in the years ahead, and what can their companies do to support their development?

The skills that will matter most are adaptability, commercial judgement and the ability to translate new ideas into practical outcomes.

As technology, risk and customer expectations continue to evolve, insurance professionals will need a combination of technical understanding, business insight and strong collaboration skills. Alongside that they must bring curiosity, continuous learning and a willingness to embrace change.

For organizations, the priority should be continued investment in people. That means creating opportunities for learning, encouraging cross-functional collaboration and exposing teams to emerging risks, technologies and customer challenges.

The Lloyd’s Academy supports this by helping insurance professionals build expertise, strengthen networks and apply their learning to the challenges clients face.

Ultimately, resilience is not only about systems and technology. It is also about people. The organizations that invest in capability today will be best positioned to navigate the opportunities and challenges ahead.

Looking ahead, what is your vision for innovation and the future of the insurance industry?

I believe the future of insurance should be defined by resilience, relevance and responsible innovation.

At the heart of Lloyd’s strategy is a simple ambition: we bring together the world’s leading risk takers to advance global progress. That is supported by a focus on underwriting excellence, marketplace efficiency, capital strength and maintaining a market that continues to attract the best talent and ideas.

Quantum computing is just one example of the broader opportunities and challenges facing our industry. It reinforces the need to anticipate emerging risks, invest in new capabilities and bring together expertise from across insurance, technology, academia and government.

Innovation is not an end in itself. Its value lies in helping us understand risk more clearly, make better decisions and strengthen resilience for customers, businesses and communities.

The priority is to use innovation responsibly, combining new technology with human expertise to ensure our industry remains trusted, relevant and able to support progress for generations to come.

References

[1] A. Zardoshti, "The impacts of quantum computing on insurance," Lloyd's of London, 2021. Available: https://www.scribd.com/document/558127949/Quantum-Paper

[2] E. Gibney, "Google claims 'quantum advantage' again – but researchers are sceptical," Nature, 22 October 2025. Available: https://www.nature.com/articles/d41586-025-03300-4

[3] D. Castelvecchi, "Quantum computers will finally be useful: what's behind the revolution," Nature, vol. 650, pp. 24-26, 2026. Available: https://www.nature.com/articles/d41586-026-00312-6

[4] Alice & Bob, "Quantum Computing Roadmap," [Online]. Available: https://alice-bob.com/wp-content/uploads/2024/12/Alice-Bob-Roadmap.pdf

[5] D-Wave, "D-Wave Charts a New Course to Fault-Tolerant Quantum Computing with Gate-Model Roadmap," 1 June 2026. [Online]. Available: https://www.dwavequantum.com/company/newsroom/press-release/d-wave-charts-a-new-course-to-fault-tolerant-quantum-computing-with-gate-model-roadmap/

[6] IBM Quantum, "IBM Quantum Roadmap," 2025. [Online]. Available: https://www-api.ibm.com/adobe/assets/urn:aaid:aem:6c6c3b12-ff63-45f3-8eff-b519cba3372d/original/as/ibm_quantum_development_innovation-roadmap_explainer_nov_2025.pdf

[7] IQM, "Development Roadmap: Our journey to fault-tolerant quantum computing and beyond," [Online]. Available: https://iqm.tech/technology/roadmap/

[8] OQC, "The OQC Roadmap: Fastest path to commercial advantage," [Online]. Available: https://oqc.tech/tech/technical-roadmap

[9] IonQ, "Industry-leading roadmap," [Online]. Available: https://www.ionq.com/roadmap

[10] Quantinuum, "Technical perspective: By the end of the decade, we will deliver universal, fully fault-tolerant quantum computing," 17 September 2024. [Online]. Available: https://www.quantinuum.com/blog/technical-perspective-by-the-end-of-the-decade-we-will-deliver-universal-fault-tolerant-quantum-computing

[11] Quandela, "Roadmap 2026-2033," [Online]. Available: https://www.quandela.com/wp-content/uploads/2026/03/Quandela-Roadmap-190326-web.pdf

[12] Pasqal, "Our Quantum Roadmap," 2026. [Online]. Available: https://www.pasqal.com/wp-content/uploads/2026/04/Pasqal-Roadmap-2026.pdf

[13] QuEra, "The Road to Commercially Valuable Fault-Tolerant Quantum Computing," [Online]. Available: https://www.quera.com/our-quantum-roadmap

[14] Google Quantum AI, "Our Quantum Computing Roadmap," [Online]. Available: https://quantumai.google/roadmap

[15] Microsoft Quantum, "Our Quantum Roadmap," [Online]. Available: https://quantum.microsoft.com/en-us/vision/quantum-roadmap

[16] C. Kloeffel and D. Loss, "Prospects for Spin-Based Quantum Computing in Quantum Dots," Annual Review of Condensed Matter Physics, vol. 4, pp. 51-81, 2013. Available: https://doi.org/10.1146/annurev-conmatphys-030212-184248

[17] IBM Quantum, "What are spin qubits? Spin qubits are an important element of IBM's recent HRL Laboratories acquisition," 23 July 2026. [Online]. Available: https://www.ibm.com/quantum/blog/spin-qubits

[18] European Patent Office and OECD, "Mapping the global quantum ecosystem: A comprehensive analysis based on innovation, firm, investment, skills, trade and policy data," December 2025. Available: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/12/mapping-the-global-quantum-ecosystem_47891dd2/20251217-0001.pdf

[19] EconSight, "Quantum computing technology overview - Quantum computing: Top countries, companies and technology applications," [Online]. Available: https://www.econsight.com/quantum-technology/

[20] Swiss Federal Council, "Federal Council to harmonise export controls for dual-use goods: Amendment of the Goods Control Ordinance," 2 April 2025. [Online]. Available: https://www.admin.ch/en/nsb?id=104712

[21] The White House, "Executive Order 14413: Ushering in the Next Frontier of Quantum Innovation," 22 June 2026. [Online]. Available: https://www.whitehouse.gov/presidential-actions/2026/06/ushering-in-the-next-frontier-of-quantum-innovation/

[22] The White House, "Executive Order 14412: Securing the Nation against Advanced Cryptographic Attacks," 22 June 2026. [Online]. Available: https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/

[23] IBM, "IBM Commits More Than $10 Billion to Quantum Computing, Funding Its Roadmap from Today's Leading Systems to the World's First Fault-Tolerant Quantum Computers," 2 June 2026. [Online]. Available: https://newsroom.ibm.com/2026-06-02-ibm-commits-more-than-10-billion-to-quantum-computing,-funding-its-roadmap-from-todays-leading-systems-to-the-worlds-first-fault-tolerant-quantum-computers

[24] European Commission, "COM(2025) 363 final - Quantum Europe Strategy: Quantum Europe in a Changing World," 2 July 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0363

[25] UK Department for Science, Innovation and Technology, "National quantum strategy: A 10-year vision and strategy missions for the UK to be a leading quantum-enabled economy, recognising the importance of quantum technologies for the UK's prosperity and security," 2023. [Online]. Available: https://www.gov.uk/government/publications/national-quantum-strategy

[26] Swiss Quantum Commission, "Swiss Quantum Strategy," Swiss Academy of Sciences, 2026. Available: https://quantum.scnat.ch/en/science_and_innovation/swiss_quantum_strategy

[27] K. Shang, "Quantum Computing and its Impact on Actuarial Modeling," Society of Actuaries Research Institute, 2023. Available: https://www.soa.org/resources/research-reports/2023/actuarial-modeling-quantum-computing

[28] S. K. Margan, "The Quest for Quantum," American Academy of Actuaries, 2023. Available: https://actuary.org/article/the-quest-for-quantum/

[29] H. Y. Liu, X. N. Zhuang, C. Wang, Q. S. Li, M. H. Dou, Z. Y. Chen, C. Xue, Y. C. Wu, G. P. Guo and G. C. Guo, "Quantum computational insurance and actuarial science," Science China Information Sciences, vol. 68, no. 10, pp. 1-28, 2025. Available: https://doi.org/10.1007/s11432-024-4411-8

[30] S. Woerner and D. J. Egger, "Quantum risk analysis," npj Quantum Information, vol. 5, no. article 15, pp. 1-8, 2019. Available: https://www.nature.com/articles/s41534-019-0130-6.pdf

[31] A. Montanaro, "Quantum speedup of Monte Carlo methods," Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, vol. 471, no. 2181, pp. 1-20, 2015. Available: https://doi.org/10.1098/rspa.2015.0301

[32] D. Herman, C. Googin, X. Liu, A. Galda, I. Safro, Y. Sun, M. Pistoia and Y. Alexeev, "A Survey of Quantum Computing for Finance," arXiv:2201.02773, 2022. Available: https://arxiv.org/abs/2201.02773

[33] D. Peral-García, J. Cruz-Benito and F. J. García-Peñalvo, "Systematic literature review: Quantum machine learning and its applications," Computer Science Review, vol. 51, pp. 1-20, 2024. Available: https://www.sciencedirect.com/science/article/pii/S1574013724000030

[34] A. Abbas, A. Ambainis, B. Augustino, A. Bärtschi, H. Buhrman, C. Coffrin, G. Cortiana, V. Dunjko, D. J. Egger, B. G. Elmegreen, N. Franco, F. Fratini, B. Fuller, J. Gacon, C. Gonciulea, S. Gribling, S. Gupta, S. Hadfield, R. Heese, G. Kircher, T. Kleinert, T. Koch, G. Korpas, S. Lenk, J. Marecek, V. Markov, G. Mazzola, S. Mensa, N. Mohseni, G. Nannicini, C. O'Meara, E. Peña Tapia, S. Pokutta, M. Proissl, P. Rebentrost, E. Sahin, B. C. Symons, S. Tornow, V. Valls, S. Woerner, M. L. Wolf-Bauwens, J. Yard, S. Yarkoni, D. Zechiel, S. Zhuk and C. Zoufal, "Challenges and Opportunities in Quantum Optimization," arXiv:2312.02279, 2023. Available: https://arxiv.org/abs/2312.02279

[35] T. Koch, D. E. Bernal Neira, Y. Chen, G. Cortiana, D. J. Egger, R. Heese, A. Gomez Cadavid, N. N. Hegade, R. Huang, T. Itoko, T. Kleinert, P. M. Xavier, N. Mohseni, J. A. Montanez-Barrera, K. Nakano, G. Nannicini, C. O'Meara, J. Pauckert, M. Proissl, A. Ramesh, M. Schicker, N. Shimada, M. Takeori, V. Valls, D. Van Bulck, S. Woerner and C. Zoufal, "The Quantum Optimization Benchmarking Library," Nature Computational Science, vol. 6, no. 6, pp. 653-671, 2026. Available: https://www.nature.com/articles/s43588-026-00991-1

[36] S. P. Jordan, N. Shutty, M. Wootters, A. Zalcman, A. Schmidhuber, R. King, S. V. Isakov, T. Khattar and R. Babbush, "Optimization by decoded quantum interferometry," Nature, vol. 646, pp. 831-836, 2025. Available: https://www.nature.com/articles/s41586-025-09527-5

[37] J. Stein, D. Schuman, M. Benkard, T. Holger, W. Sajko, M. Kölle, J. Nüßlein, L. Sünkel, O. Salomon and C. Linnhoff-Popien, "Exploring Unsupervised Anomaly Detection with Quantum Boltzmann," arXiv:2306.04998, 2023. Available: https://arxiv.org/abs/2306.04998

[38] Allianz France, IQM, Multiverse Computing, "Project AQACYB: Avantage Quantique pour l'Analyse de CYBermenaces," Région île de France, pp. 1-10, 2024. Available: https://www.teratec.fr/library/pdf/2024/TQCI_240424/AQACYB.pdf

[39] GENCI, "Cyberthreats: the Ile-de-France region supports the first exploration of quantum computing," 2023. [Online]. Available: https://www.genci.fr/en/news/cyberthreats-ile-de-france-region-supports-first-exploration-quantum-computing

[40] Allianz X, "Our promising, digital growth companies.," 2026. [Online]. Available: https://allianzx.com/ourcompanies

[41] Chicago Quantum Exchange (CQE), "Allstate, aiming to shape insurance of the future, joins Chicago Quantum Exchange," 2025. [Online]. Available: https://chicagoquantum.org/news/allstate-aiming-shape-insurance-future-joins-chicago-quantum-exchange

[42] M. Bordelon, M. Garfinkel, V. Dixit, T. Whitehead, J. Holzbauer, G. Mijares Vilarino, A. Maldonado Romo, A. Mitra, V. Kumar and J. Utke, "A Quantum Approach to Stochastic Optimization in Insurance Underwriting," arXiv:2605.01169, 2026. Available: https://arxiv.org/abs/2605.01169

[43] M. Tamturk and M. Carenzo, "Quantum Computing in Insurance Capital Modelling under Reinsurance Contracts," AppliedMath, vol. 3, no. 4, pp. 741-757, 2023. Available: https://www.mdpi.com/2673-9909/3/4/40

[44] M. Tamturk, E. Ginossar, M. Carenzo and C. Perret, "Motor insurance data analysis by quantum machine learning," Discover Quantum Science, vol. 2, no. 3, 2026. Available: https://doi.org/10.1007/s44464-026-00007-x

[45] M. Tamturk, E. Ginossar and M. Carenzo, "Advantage with quantum reservoir computing in medical insurance and health data analysis," Quantum Machine Intelligence, vol. 8, no. 41, 2026. Available: https://doi.org/10.1007/s42484-026-00384-7

[46] G. Woodman, "Is Quantum Computing Worth the Effort?," AXA, pp. 1-5, 2021. Available: https://www-axa-com.cdn.axa-contento-118412.eu/www-axa-com/ec3d8026-1a7a-4134-b08b-53c71f7590c6_Article_R%26D_article3_quantum%5B4%5D.pdf

[47] Y. Boger, M. Detyniecki and G. Woodman, "Podcast with AXA," Classiq, 2021. Available: https://www.classiq.io/insights/axa-podcast

[48] G. Woodman, R. S. Andrist, T. Häner, D. S. Steiger, M. J. A. Schuetz, H. G. Katzgraber and M. Detyniecki, "Modern Computational Methods in Reinsurance Optimization: From Simulated Annealing to Quantum Branch & Bound," arXiv:2504.16530, 2025. Available: https://arxiv.org/abs/2504.16530

[49] The Quantum Economy Network, "Quantum Application Hub," World Economic Forum, 2024. [Online]. Available: https://initiatives.weforum.org/quantum/application-hub

[50] AXA XL, "Optimization of Reinsurance Contracts," World Economic Forum, 2024. [Online]. Available: https://initiatives.weforum.org/quantum/case-study-details/optimization-of-reinsurance-contracts/aJYTG0000000CnZ4AU

[51] M. Adam, "Potential Applications of Quantum Computing for the Insurance Industry," arXiv:2210.06172, 2022. Available: https://arxiv.org/abs/2210.06172

[52] Quantum London, "The big quantum debate: How will quantum computing impact the insurance industry (Lloyd's Lab event)," 16 February 2021. [Online]. Available: https://www.youtube.com/watch?v=dqIC2dE5tmo

[53] J. Knight, "MetLife actuarial working group," Linkedin, 2026. Available: https://www.linkedin.com/posts/jameswmknight_just-wrapped-up-our-second-metlife-actuarial-share-7438214685671337984-jmQu/

[54] Q-STAR: Quantum STrategic Industry Alliance for Revolution, "Member list," 2021. [Online]. Available: https://qstar.jp/en/memberlist

[55] Q-STAR: Quantum STrategic industry Alliance for Revolution, "Pamphlet," pp. 1-10, 2026. Available: https://cdn.prod.website-files.com/69e516fadb24e5ec6ce515b2/6aa8ba8e3806ce2302bf8e88_98141f5123b42c230c039d2d55cc0f7a_EN_Pamphlet.pdf

[56] Q-STAR: Quantum STrategic Industry Alliance for Revolution, "Establishment of Quantum Strategic Industry Alliance for Revolution (Q-STAR)," 2021. Available: https://www.mcgc.com/english/news_mcc/2021/__icsFiles/afieldfile/2021/09/29/210901qstar.pdf

[57] AIOI R&D LAB-OXFORD, "Quantum Computing," 2022. [Online]. Available: https://www.aioilab-oxford.eu/quantum-computing

[58] M. Fischer, D. Brooks, P. Lougovski and T. Takeshita, "Using Quantum Machine Learning with Amazon Braket to Create a Binary Classifier," AWS Quantum Technologies Blog, 2021. Available: https://aws.amazon.com/blogs/quantum-computing/aioi-using-quantum-machine-learning-with-amazon-braket-to-create-a-binary-classifier/

[59] QUTAC: Quantum Technology and Application Consortium, "Our Members," 2026. [Online]. Available: https://www.qutac.de/en/our-members/

[60] QUTAC: Quantum Technology and Application Consortium, "Munich Re: Understanding, calculating and hedging complex risks," 2022. Available: https://www.qutac.de/en/munich-re-securing-the-goods-transfer-of-tomorrow-with-the-help-of-quantum-computing-based-route-planning/

[61] QUTAC: Quantum Technology and Application Consortium, "Industry quantum computing applications," EPJ Quantum Technology, vol. 8, no. 1, pp. 1-17, 2021. Available: https://link.springer.com/article/10.1140/epjqt/s40507-021-00114-x

[62] Hitachi, Ltd., "Sompo Japan Insurance Begins Using Quantum Inspired Computer in Insurance Underwriting Operations," 2022. [Online]. Available: https://www.hitachi.com/New/cnews/month/2022/03/220329d.pdf

[63] Swiss Re Institute, "Quantum computing – a threat before an opportunity," 2022. [Online]. Available: https://www.swissre.com/institute/research/sonar/sonar2022/quantum-computing.html

[64] Swiss Re, "Cyber Insurance & Underwriting (2026)," 2026. [Online]. Available: https://campus.swissre.com/explore/cyber-insurance-underwriting-2026

[65] Swiss Re, "Cyber Insurance & Underwriting (2027)," 2027. [Online]. Available: https://campus.swissre.com/explore/cyber-insurance-underwriting-2027

[66] Unipol Assicurazioni SPA, "QDOMC – Quantum algorithm for the Detection of the Optimal Maximal Clique," ICSC Centro Nazionale di Ricerca in HPC, Big Data and Quantum Computing. Available: https://www.supercomputing-icsc.it/qdomc-quantum-algorithm-for-the-detection-of-the-optimal-maximal-clique/

[67] S. Tibaldi, L. Leclerc, D. Vodola, E. Tignone and E. Ercolessi, "Analog QAOA with Bayesian Optimisation on a neutral atom QPU," arXiv:2501.16229, 2025. Available: https://arxiv.org/abs/2501.16229

[68] A. Bohnert, A. Dotterweich and S. Ernst, "Quantum Computing in the Insurance Industry: Insights From the Literature," Zeitschrift für die gesamte Versicherungswissenschaft, vol. 115, no. 1, pp. 177-202, 2026. Available: https://doi.org/10.3790/zverswiss.2026.1474502

[69] J. Zhou, "Quantum Finance: Exploring the Implications of Quantum Computing on Financial Models," Computational Economics, pp. 1-30, 2025. Available: https://link.springer.com/content/pdf/10.1007/s10614-025-10894-4.pdf

[70] T. Berry and J. Sharpe, "Asset–liability modelling in the quantum era," British Actuarial Journal, vol. 26, no. e7, pp. 1-13, 2021. Available: https://doi.org/10.1017/S1357321721000076

[71] A. Montanaro, "Quantum speedup of branch-and-bound algorithms," Physical Review Research, vol. 2, no. 013056, 2020. Available: https://doi.org/10.1103/PhysRevResearch.2.013056

[72] M. Liepelt and J. Baglio, "Exponential capacity scaling of classical GANs compared to hybrid latent style-based quantum GANs," arXiv:2601.05036, 2026. Available: https://arxiv.org/abs/2601.05036

[73] N. Innan, M. A.-Z. Khan and M. Bennai, "Financial fraud detection: A comparative study of quantum machine learning models," International Journal of Quantum Information, vol. 22, no. 02, 2350044, 2024. Available: https://doi.org/10.1142/S0219749923500442

[74] S. N. Pushpak, S. Jain and S. Kalra, "Quantum Machine Learning Technique for Insurance Claim Fraud Detection with Quantum Feature Selection," Journal of Information Systems Engineering and Management, vol. 10(8s), pp. 1-7, 2025. Available: https://www.jisem-journal.com/index.php/journal/article/view/1193/453

[75] M. Grossi, N. Ibrahim, V. Radescu, R. Loredo, K. Voigt, C. von Altrock and A. Rudnik, "Mixed Quantum–Classical Method for Fraud Detection With Quantum Feature Selection," IEEE Transactions on Quantum Engineering, vol. 3, pp. 1-12, 2022. Available: https://ieeexplore.ieee.org/document/9915517

[76] G. Lancellotti, A. Guerrini, G. Ranieri, V. Zaffaroni and P. Cremonesi, "Quantum Principal Component Analysis for Financial Fraud Detection," 2025 IEEE International Conference on Quantum Artificial Intelligence (QAI), pp. 41-48, 2025. Available: https://doi.org/10.1109/QAI63978.2025.00014

[77] V. Havlíček, A. D. Córcoles, K. Temme, A. W. Harrow, A. Kandala, J. M. Chow and J. M. Gambetta, "Supervised learning with quantum-enhanced feature spaces," Nature, vol. 567, pp. 209-212, 2019. Available: https://www.nature.com/articles/s41586-019-0980-2

[78] D. J. Egger, R. García Gutiérrez, J. C. Mestre and S. Woerner, "Credit Risk Analysis Using Quantum Computers," IEEE Transactions on Computers, vol. 70, no. 12, pp. 2136-2145, 2021. Available: https://doi.org/10.1109/TC.2020.3038063

[79] N. Stamatopoulos, B. D. Clader, S. Woerner and W. J. Zeng, "Quantum Risk Analysis of Financial Derivatives," arXiv:2404.10088, 2024. Available: https://arxiv.org/abs/2404.10088

[80] J. Taylor, "Leveraging Quantum Machine Learning for Actuarial Predictions in Health Insurance," Artificial Intelligence, Quantum Computing, Robotics, Science and Technology Journal, vol. 3, no. 1, pp. 29-34, 2025. Available: https://www.researchgate.net/publication/395982257_Leveraging_Quantum_Machine_Learning_for_Actuarial_Predictions_in_Health_Insurance

[81] M. Brown, "Bridging Actuarial Science and Quantum Machine Learning: Applications in Health Insurance," Artificial Intelligence, Quantum Computing, Robotics, Science and Technology Journal, vol. 3, no. 1, pp. 15-28, 2025. Available: https://www.researchgate.net/publication/395983504_Bridging_Actuarial_Science_and_Quantum_Machine_Learning_Applications_in_Health_Insurance

[82] C. M. Farrelly, S. Namuduri and U. Chukwu, "Quantum Generalized Linear Models," arXiv:1905.00365, 2019. Available: https://arxiv.org/abs/1905.00365

[83] C. Liu and Z. Ji, "Accelerating Regression Tasks with Quantum Algorithms," arXiv:2509.24757, 2025. Available: https://arxiv.org/abs/2509.24757

[84] M. Goldburd, A. Khare, D. Tevet and D. Guller, "Generalized Linear Models for Insurance Rating, Second Edition (2025 revision)," Casualty Actuarial Society Monograph Series, vol. 5, 2025. Available: https://www.casact.org/sites/default/files/2021-01/05-Goldburd-Khare-Tevet.pdf

[85] The Geneva Association, "Climate Change Risk Assessment for the Insurance Industry," February 2021. [Online]. Available: https://www.genevaassociation.org/sites/default/files/climate_risk_web_final_250221.pdf

[86] AXA Research Fund, "New Tech for Nat Cat: Unlocking the Power of Remote Sensing & Artificial Intelligence to Anticipate and Mitigate Natural Disasters," 2025. [Online]. Available: https://axafoundation.org/storage/media/4596/New-Tech-For-Natcat-Remote-Sensing-Report_AXA-Research-Fund.pdf

[87] Hugging Face, "Security incident disclosure - July 2026," 16 July 2026. [Online]. Available: https://huggingface.co/blog/security-incident-july-2026

[88] L. H. Newman, "Anthropic's Mythos Will Force a Cybersecurity Reckoning—Just Not the One You Think," WIRED, 2026. Available: https://www.wired.com/story/anthropics-mythos-will-force-a-cybersecurity-reckoning-just-not-the-one-you-think/

[89] F. Landymore, "Anthropic Warns That "Reckless" Claude Mythos Escaped a Sandbox Environment During Testing," Futurism, 2026. Available: https://futurism.com/artificial-intelligence/anthropic-claude-mythos-escaped-sandbox

[90] M. Chen, "Anthropic's Claude Code Source Code Leak: Inside the 512,000-Line npm Packaging Error That Exposed AI's Biggest Secret Roadmap," Tech Insider, 2026. Available: https://tech-insider.org/anthropic-claude-code-source-code-leak-npm-2026/

[91] A. Day, "Cyber market challenged by AI threats increasing in scale and persistence: AI attacks are difficult to identify, which makes them almost impossible to price for," 5 August 2026. [Online]. Available: https://www.portal.insuranceinsider.com/article/2gpwi36mcja26uqs490qp/lines-of-business/cyber/cyber-market-challenged-by-ai-threats-increasing-in-scale-and-persistence?gift=f47649b4-8201-456f-83dd-1ea0d046d9e2&utm_campaign=giftlink

[92] A. A. Samuel, "Quantum Risk Modeling Redefining Actuarial Science with Quantum Algorithms," Journal of Science Technology and Engineering Research, vol. 2, no. 1, pp. 71-82, 2024. Available: https://www.researchgate.net/publication/395132999_Quantum_Risk_Modeling_Redefining_Actuarial_Science_with_Quantum_Algorithms

[93] M. A. Amjad, "Quantum internal models for Solvency II and quantitative risk management," British Actuarial Journal, vol. 30, no. e1, pp. 1-41, 2025. Available: https://doi.org/10.1017/S135732172400031X

[94] M. Schwabe, L. Pastori, I. de Vega, P. Gentine, L. Iapichino, V. Lahtinen, M. Leib, J. M. Lorenz and V. Eyring, "Opportunities and challenges of quantum computing for climate modeling," Environmental Data Science, vol. 4, no. e35, pp. 1-20, 2025. Available: https://doi.org/10.1017/eds.2025.10010

[95] Q. Zhang, A. Simen, C. Flores-Garrigós, G. Alvarado Barrios, P. A. Erdman, E. Solano, A. C. Kemp, V. Beltrani, V. Pathak and H. Mohammadbagherpoor, "Quantum-enhanced satellite image classification," arXiv:2602.18350, 2026. Available: https://arxiv.org/abs/2602.18350

[96] R. Shelbaya, Z. Zaharieva, M. Taylor, D. Fallet and P. Intallura, "Chaos theory: How quantum science generates true randomness," 4 July 2025. [Online].
Available: https://www.theactuary.com/2025/07/04/chaos-theory-how-quantum-science-generates-true-randomness

[97] The Quantum Economy Network, World Economic Forum, "Enhancing Simulations with Quantum Entropy," 17 December 2025. [Online]. Available: https://initiatives.weforum.org/quantum/application-hub/enhancing-simulations-with-quantum-entropy/aJYTG00000011i14AA

[98] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithm and Factoring," Proceedings of 35th Annual Symposium on Foundations of Computer Science, 1994. [Online].
Available: https://doi.org/10.1109/SFCS.1994.365700

[99] R. Krishnakumar, "Quantum Threats. Quantum Technologies: Trends and Implications for Cyber Defense," Springer Nature Switzerland, pp. 95-106, 2026. Available: https://link.springer.com/chapter/10.1007/978-3-031-90727-2_10

[100] L. K. Grover, "A fast quantum mechanical algorithm for database search," Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC), arXiv:quant-ph/9605043, 1996. [Online].
Available: https://arxiv.org/abs/quant-ph/9605043

[101] C. Gidney, "How to factor 2048 bit RSA integers with less than a million noisy qubits," arXiv:2505.15917, 2025. Available: https://arxiv.org/abs/2505.15917

[102] R. Babbush, A. Zalcman, C. Gidney, M. Broughton, T. Khattar, H. Neven, T. Bergamaschi, J. Drake and D. Boneh, "Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations," arXiv:2603.28846, 2026. Available: https://arxiv.org/abs/2603.28846

[103] M. Cain, Q. Xu, R. King, L. R. B. Picard, H. Levine, M. Endres, J. Preskill, H.-Y. Huang and D. Bluvstein, "Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits," arXiv:2603.28627, 2026. Available: https://arxiv.org/abs/2603.28627

[104] P. S. Mundada, A. Khindanov, Y. Wang, C. L. Edmunds, P. Coote, M. J. Biercuk, Y. Baum and M. Hush, "Heterogeneous architectures enable a 138x reduction in physical qubit requirements for fault-tolerant quantum computing under detailed accounting," arXiv:2604.06319, 2026. Available: https://arxiv.org/abs/2604.06319

[105] T. Häner, F. Tripier, J. Young, M. Naehrig, A. Maksymov, S. Alam, D. Maslov, M. Parrott, Y. de Sereville, J. Sullivan, M. Webster, N. Delfosse, J. Gamble and M. Roetteler, "Computing 256-bit elliptic curve discrete logarithms in 26 days on a fault-tolerant trapped-ion quantum computer with 20,000 qubits," arXiv:2609.05625, 2026.
Available: https://arxiv.org/abs/2609.05625

[106] IonQ, "IonQ Publishes World's First Fully Compiled, End-to-End Blueprint for Breaking 256-Bit Elliptic-Curve Signatures," 8 September 2026. [Online]. Available: https://www.ionq.com/news/ionq-publishes-worlds-first-fully-compiled-end-to-end-blueprint-for-breaking-256-bit-elliptic-curve-signatures

[107] M. Mosca and M. Piani, "Quantum Threat Timeline Report 2025," Global Risk Institute (GRI), pp. 1-75, 2026. Available: https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/

[108] H. Adkins and S. Schmieg, "Quantum frontiers may be closer than they appear," 2026. [Online]. Available: https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/

[109] M. Russinovich, "Microsoft advances quantum-safe security as the risk timeline shifts," Microsoft Security Blog, 30 June 2026. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2026/06/30/microsoft-advances-quantum-safe-security-as-the-risk-timeline-shifts/

[110] B. Westerbaan, "Cloudflare targets 2029 for full post-quantum security," Cloudflare Blog, 7 April 2026. [Online]. Available: https://blog.cloudflare.com/post-quantum-roadmap/

[111] M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?," IACR ePrint 2015/1075, 2015. [Online]. Available: https://eprint.iacr.org/2015/1075

[112] Swiss Federal Data Protection and Information Commissioner (FDPIC), "Inspection, storage and deletion of patient data," (twenty-year retention rule), [Online]. Available: https://www.edoeb.admin.ch/en/inspection-storage-and-deletion-of-patient-data

[113] Swiss Confederation, "Revised Federal Act on Data Protection (FADP)," Fedlex SR 235.1 (controller remains responsible for outsourced processing), [Online]. Available: https://www.fedlex.admin.ch/eli/cc/2022/491/en

[114] EUR-Lex, "Digital Operational Resilience Act, Regulation (EU) 2022/2554 (DORA)," published 2022; in application since 17 January 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[115] W. A. Vitale, "Migration Is the Hard Part," 16 July 2026. [Online]. Available: https://bitcoinsuisse.com/industry-blog/bitcoin-post-quantum-migration

[116] FINMA, "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)," 16 February 2018. [Online]. Available: https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

[117] Swiss Confederation, "Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (DLT Act)," in force 2021 (ledger-based securities). [Online]. Available: https://www.newsd.admin.ch/newsd/message/attachments/67575.pdf

[118] EUR-Lex, "Markets in Crypto-Assets Regulation (MiCA), Regulation (EU) 2023/1114," 2023. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng

[119] NIST, "Post-Quantum Cryptography Standardization," (FIPS 203/204/205 published August 2024; HQC selected March 2025; FIPS 206 in development). [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[120] L. Pupillo, S. Ashworth, A. Ferreira and C. Polito, "Strengthening the EU transition to a quantum-safe world: Technology, market, governance and policy challenges," Task Force Report, Centre for European Policy Studies (CEPS), Brussels, December 2025. Available: https://cdn.ceps.eu/2025/12/2025-12-Quantum-TF-report-formatted.pdf

[121] ANSSI, BSI, NLNCSA, Swedish NCSA, "Position Paper on Quantum Key Distribution," January 2024. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf

[122] UK Department for Science, Innovation and Technology (research by Technopolis), "Quantum key distribution research report," 10 June 2026. [Online]. Available: https://www.gov.uk/government/publications/quantum-key-distribution-research-report/quantum-key-distribution-research-report

[123] European Commission / NIS Cooperation Group, "A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography," (Recommendation April 2024; Roadmap June 2025). [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[124] UK National Cyber Security Centre (NCSC), "Timelines for migration to post-quantum cryptography," 2025. [Online]. Available: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[125] NIST IR 8547, "Transition to Post-Quantum Cryptography Standards," 2024. [Online]. Available: https://csrc.nist.gov/pubs/ir/8547/ipd

[126] Executive Office of the President, Office of Management and Budget, "OMB Memorandum M-26-15: Execution of the Migration to Post-Quantum Cryptography," 24 June 2026. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2026/06/M-26-15-Execution-of-the-Migration-to-Post-Quantum-Cryptography.pdf

[127] Swiss Financial Market Supervisory Authority FINMA, "FINMA Guidance 05/2026: Quantum Computing," 2026. Available: https://www.finma.ch/en/news/2026/07/20260709-mm-am-05-26/

[128] A. Amadori, T. Attema, M. Bombar, J. D. Duarte, V. Dunning, S. Etinski, D. van Gent, M. Lequesne, W. van der Schoot, M. Stevens and AIVD Cryptologists and Advisors, "The PQC Migration Handbook - Guidelines for migrating to post-quantum cryptography - Revised and extended second edition," TNO (Netherlands Organization for Applied Scientific Research), December 2024.
Available: https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf

[129] Europol, "Prioritising post-quantum cryptography migration activities in financial services," Luxembourg: Publications Office of the European Union, 2026. Available: https://www.europol.europa.eu/publications-events/publications/prioritising-post-quantum-cryptography-migration-activities-in-financial-services

[130] A. Kemp, R. Padbury and C. Reeves, "The Role of the Second Line of Defense in Post-Quantum Cryptography Migration and Cryptographic Auditing: Responsibilities and Adaptations," SSRN, 2026.
Available: https://dx.doi.org/10.2139/ssrn.7225698

[131] N. Aquina, B. Cimoli, S. Das, K. Höverlmanns, F. J. Weber, C. Okonkwo, S. Rommel, B. Škorić, I. T. Monroy and S. Verschoor, "A Critical Analysis of Deployed Use Cases for Quantum Key Distribution and Comparison with Post-Quantum Cryptography," arXiv:2502.04009 (documents the 2007 Geneva election deployment), 2025.
Available: https://arxiv.org/abs/2502.04009

[132] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta and H. Zbinden, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," New Journal of Physics, vol. 13, no. 123001, 2011.
Available: https://iopscience.iop.org/article/10.1088/1367-2630/13/12/123001

[133] Greater Geneva Bern area, "Geneva launches its first quantum communication network," 15 October 2025. [Online].
Available: https://ggba.swiss/en/geneva-launches-its-first-quantum-communication-network/

[134] HSBC, "HSBC becomes first bank to join the UK's pioneering commercial quantum secure metro network," 5 July 2023. [Online]. Available: https://www.hsbc.com/news-and-views/news/media-releases/2023/hsbc-becomes-first-bank-to-join-the-uks-pioneering-commercial-quantum-secure-metro-network

[135] HSBC, "HSBC pioneers Quantum protection for AI-powered FX trading," 6 December 2023. [Online].
Available: https://www.hsbc.com/news-and-views/news/media-releases/2023/hsbc-pioneers-quantum-protection-for-ai-powered-fx-trading

[136] R. J. Vicente, J. Gómez García, J. P. Brito, Y. Lobaina, J. S. Buruaga, D. Gómez Aguado, M. Á. Sánchez Serrano, S. Ovsyannikov, S. Gherdaoui, J.-S. Pegon, M. Cofano and V. Martín, "Quantum-safe IPsec in the banking industry," arXiv:2604.12985, 2026. Available: https://arxiv.org/abs/2604.12985

[137] ID Quantique, "Why the financial sector is embracing a dual quantum-safe strategy," 12 December 2024. [Online].
Available: https://www.idquantique.com/why-the-financial-sector-is-embracing-a-dual-quantum-safe-strategy/

[138] O. Alia, A. Huang, H. Luo, O. Amer, M. Pistoia and C. Lim, "100 Gbps Quantum-safe IPsec VPN Tunnels over 46 km Deployed Fiber," arXiv:2405.04415, 2024. Available: https://arxiv.org/abs/2405.04415

[139] FinTech Global, "MAS and banks trial quantum security for finance," 29 September 2025. [Online].
Available: https://fintech.global/2025/09/29/mas-and-banks-trial-quantum-security-for-finance/

[140] Danske Bank, "Danske Bank helps researchers reach milestone within it-security," 23 February 2022. [Online].
Available: https://danskebank.com/news-and-insights/news-archive/news/2022/23022022

[141] Erste Group Bank AG, "Erste Group sets new standards in quantum encryption," 23 February 2026. [Online].
Available: https://www.erstegroup.com/en/news-media/press-releases/2026/02/23/erste-group-sets-new-standards-in-quantum-encryption

[142] T. Rezaei, A. Rao, J. Stapleton and P. Bordow, "Evaluation of Integration of Hardware Based QKD and Emerging Software-Based Cryptographic Innovations in Banking Security: Case Studies from Wells Fargo," 2025 IEEE Conference on Pervasive and Intelligent Computing (PICom), pp. 273-278, 2025.
Available: https://doi.org/10.1109/PICom68402.2025.00049

[143] QED-C, "State of the Global Quantum Industry 2026," 14 April 2026. [Online].
Available: https://quantumconsortium.org/publication/2026-state-of-the-global-quantum-industry-report

[144] G7 Central Banks' Quantum Technologies Working Group, "Preparing for Quantum Technologies: Key Considerations for Financial Sector Participants," May 2026. Available: https://www.banque-france.fr/en/press-release/g7-central-banks-publish-first-reference-report-quantum-technologies-and-their-implications

Contributors

Authors

Lead author & project coordinator
Christoph Kloeffel
KPMG Switzerland

Marcel Ambrus
KPMG Switzerland

Damir Bogdan
QuantumBasel

Frederik F. Flöther
QuantumBasel

Aaron C. Kemp
KPMG US

Alexander Lacher
KPMG Switzerland

Pascal Pfister
KPMG Switzerland

Eva Lia Tarquini
KPMG Switzerland

Jakob Thyme
Lloyd's of London

Acknowledgements

We gratefully acknowledge the valuable contributions of the following individuals:

Pascal Baerenfaller
KPMG Switzerland

Natalia Chebotar
KPMG UK

George Chirbas
KPMG US

Thomas D'Arminio
KPMG US

J. Foster Davis
BreachBits

Marcin Detyniecki
AXA

Matthew Dunbar
KPMG UK

Paul Guthrie
DataStream and Envelop Risk

Benjamin Harris
KPMG UK

Max Henderson
DataStream

Gustav Hermann
KPMG Switzerland

Cindy Hofmann
KPMG Switzerland

James Isden
KPMG UK

John Kelly
Envelop Risk

Leandro Kuenzli
KPMG Switzerland

Maynard Kuona
KPMG UK

Sébastien Loesch
KPMG Switzerland

Yosef Lugashi
KPMG US

Kruti Malde
KPMG UK

Dawn Miller
Lloyd's of London

Aravind Mohan
KPMG UK

Ramona Müller
Allianz Suisse Versicherungs-Gesellschaft

Matthew Murphy
KPMG UK

Thomas Murphy
KPMG UK

Wolfgang Naumann
SWICA

Richard Padbury
KPMG US

Karen Parkinson
KPMG UK

Antoine Pietri
AXA

Cian C. Reeves
KPMG US

Thomas Schneider
KPMG Switzerland

William Southwell
KPMG Switzerland

Joseph O. Trujeque
KPMG US

George Woodman
AXA

For more information on Insurance Insights please contact:

Alexander Lacher
Partner, Insurance Sector Head
KPMG Switzerland
+41 79 671 65 12
alacher@kpmg.com

Huw Evans
Partner, Head of Insurance
KPMG UK
+44 7821 303638
huw.evans@kpmg.co.uk

Publisher
KPMG AG
Badenerstrasse 172
Postfach
8036 Zurich

+41 58 249 31 31

Project management
Christoph Kloeffel
KPMG Switzerland

Simon Basarte
KPMG Switzerland

Design
Geertjan van Beusekom
van Beusekom Gestaltung + Fotografie

Articles may only be republished by written permission of the publisher and quoting the source "KPMG's Insurance Insights".

The views and opinions expressed herein are those of the author and do not necessarily represent the views and opinions of the publisher.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. If you would like to know more about how KPMG AG processes personal data, please read our **Privacy Policy**, which you can find on our homepage at **www.kpmg.ch**.

© 2026 KPMG AG, a Swiss corporation, is a group company of KPMG Holding LLP, which is a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.



Insurance Insights
kpmg.ch/insurance