Swiss Banking

QuantumBasel

Quantum Computing in Banking

How it works, areas of application, and recommendations for Swiss banks

November 2024

Expert report of the SBA

Executive Summary

The demands on banks' IT systems are steadily growing. The systems could eventually be overwhelmed by ever-increasing volumes of data and the spread of artificial intelligence (AI). Quantum computing is thus attracting more and more attention. This technology has developed from science fiction to scientific reality in recent years and will soon make the leap from the laboratory to industrial applications. The critical question, therefore, is no longer whether quantum computing will become established but when and how.

The physical principles underlying quantum computing are not easy to grasp, and the technology itself is not yet in widespread use, but its potential impact on the financial sector is becoming increasingly apparent. It represents both an opportunity and a challenge. With their ability to carry out complex calculations and simulations more efficiently and with greater accuracy, quantum computers open up new possibilities. This expert report identifies and explains four use cases of quantum computing in the banking sector:

- In **risk management and risk monitoring,** quantum computers allow for the analysis of complex interdependencies between assets and derivatives and the monitoring of these in real-time.
- In **portfolio management,** quantum computers can optimise portfolios by performing parallel calculations and better simulations, thus potentially improving returns.
- In **algo trading,** quantum computers can support more efficient and precise algorithms for trading on financial markets.
- Finally, quantum computers can speed up and reduce the cost of **building and training AI models** that deliver more accurate and efficient forecasting in day-to-day business.

"The critical question is no longer whether quantum computing will become established but when and how."

Besides these opportunities, quantum computing also gives rise to new risks that must be addressed, particularly by transitioning to quantum-safe encryption methods. Given the danger posed by "harvest now, decrypt later" attacks and the long lead time for introducing quantum-safe cryptography, quantum computing is a challenge that must be taken seriously right now.

With this in mind, the authors recommend the following measures at various levels:

- **Banks** should continually adapt their existing security policies and draw up a roadmap for introducing quantum-safe cryptography. They should also work with specialist organisations and research institutes to continuously build up their quantum computing capabilities and increase their agility in applying this technology more broadly. This includes, in particular, supporting applied research in partnership with Swiss universities and research institutes to improve know-how on both sides and ensure a sufficient pool of talent in the near future.

- **Regulatory and supervisory authorities** in the financial industry should foster regular dialogue with the industry in order to understand where it can use quantum computing and identify potential action areas at the earliest possible stage. No new regulation is needed for the time being. The current, technology-neutral, and principles-based regulation sufficiently covers the possible risks of using quantum computing.
- Using new technologies such as quantum computing, AI, and distributed ledger technology (DLT) is vital to the **Swiss financial centre's** long-term competitiveness, innovative power, and resilience. As ever, this requires close collaboration with research institutes, short communication pathways, and a high degree of adaptability on the part of financial institutions. This recipe for success must remain in place and be promoted going forward.

"Banks should track this progress closely and investigate potential weaknesses in their current IT landscape."

Financial industry decision-makers, authorities, and political circles must lay the foundations today for the financial industry to harness quantum computing opportunities in the decades ahead and identify and mitigate the associated risks as early as possible. Taking the long view will create an ideal framework for a competitive, innovative, and resilient Swiss financial centre now and in the future.

1 Principles of quantum computing

The image of a coin spinning quickly on its edge is an excellent metaphor for what lies at the heart of quantum computing. In conventional computers, the bit is the smallest unit of information. It can have a value of 0 or 1, comparable to the "heads" and "tails" sides of a coin. In quantum computing, however, information is stored in the form of quantum bits – qubits for short. Just as the spinning coin appears to show heads and tails simultaneously, a qubit can be in a state of superposition, meaning that its value is simultaneously both 0 and 1 (see info box 1).

This superposition forms the basis for developing quantum algorithms that solve problems in an entirely new way and far exceed the performance of the computers we are familiar with today. Up to now, complex calculations and simulations that have only been solvable in approximation could, with considerable effort, be solved faster and more efficiently with quantum computing. The banking industry, which uses many sophisticated simulations and scenario analyses and processes vast quantities of data, stands to profit considerably from this technology.

However, just like a spinning coin, the state of a qubit is volatile and can quickly change or be lost. Quantum computers, therefore, must often operate in highly stable, supercooled environments because even the tiniest change in conditions could damage their delicate qubits and make their calculations unusable. In Switzerland, universities such as ETH Zurich, EPFL, and the University of Basel contribute substantially to fundamental research in this field, particularly quantum sensors, encryption, and simulation. New initiatives such as QuantumBasel, startups, and established technology companies are also important in application development. Governments worldwide are investing significant sums in quantum research to secure competitive advantages and guard against potential cyber-attacks.[1]

These efforts are focused not only on achieving technological progress but also on foreseeable risks. One such risk is the ability of quantum computers to crack some of the most common encryption methods, which are also used in banks' IT systems. Banks, regulators, and supervisory authorities are thus already investigating quantum-safe cryptography.

Developments in quantum computing and encryption will impact the financial system similarly to that which AI and its large language models (LLMs) have in various areas today. Here, the focus is more on quantum computing than on other quantum technologies, such as quantum communication and quantum sensors.

1 Forbes, Quantum Computing Takes Off With $55 Billion In Global Investments (2024)

How quantum computers work

Conventional computers process information in the form of bits. These are based on electrical voltages or impulses either above or below a particular value, creating the binary states of 0 and 1. Logic gates made up of transistors are used to perform calculations. These gates are connected to each other in complex networks that allow a computer to execute various mathematical operations.

Quantum computers, by contrast, are based on the principles of quantum mechanics: physical laws governing the behaviour of particles such as atoms and electrons. In quantum computing, information is represented by qubits. Qubits can be created in various types of physical systems (for example, atoms, ions, photons, or superconducting materials), each of which has its pros and cons. One thing they have in common is that they use quantum mechanics effects such as interference, superposition, and entanglement to enable entirely new approaches to problem-solving.

In conventional computing, two bits can be combined in four different combinations: 00, 01, 10, and 11. On the other hand, two qubits are not limited to these four states but can have superpositions of them as well. In other words, they can be in all these states at once and be used to calculate with all of them at once. This ability to process multiple states in parallel explains the enormous advantages of quantum algorithms. Each additional qubit doubles the computing power, i.e. a computer with 51 qubits is theoretically twice as powerful as one with 50. This exponential scalability is one reason quantum computing has made so much progress in recent years and why banks and other companies are already investing in this fledgling technology.

Technological and structural hurdles in quantum computing

Quantum computing operates at the limit of what is currently possible in physical and technological terms. For example, a quantum computer with 400 qubits of computing power can produce more states than there are atoms in the observable universe. However, there are several other challenges to overcome to develop this technology further:

- **Error correction:** Quantum computers are highly error-prone and require extensive correction mechanisms. Error correction algorithms are continually improved, and new, more efficient methods are being developed.[2]
- **Scalability:** Additional challenges arise in scaling quantum computers, for instance, regarding parallel error correction and the reliability of the quantum logic gates, the basic building blocks which make it possible to manipulate qubits in multiple states simultaneously.
- **Software:** Software developed initially for conventional computers creates a bottleneck for quantum computers. Therefore, improved algorithms, programming languages and optimisation tools are needed to unlock their full potential.

2 Amazon Web Services (AWS), for example, presented a new procedure in March 2024 that enables more efficient error correction

- **Standards and protocols:** The various quantum computer platforms that currently exist are scarcely compatible with each other. Still, there is a clear trend towards employing different systems for different use cases.
- **Data entry:** It would be wrong to assume that quantum computers are mainly suited to solving Big Data problems. In fact, it is still difficult to process large volumes of data efficiently with quantum computers. For example, some encouraging progress is being made with quantum random access memory (qRAM), but real-time applications are still far off.
- **Lack of qualified experts:** A growing number of people are working in quantum research in Switzerland, but the number of students learning in this field is not high enough to build up the talent pool that will be needed. Despite committed programmes at universities such as ETH Zurich, which has around 500 quantum researchers, the lack of qualified experts is a central challenge.

A key milestone in the development of quantum computers came in 2019 when Google successfully demonstrated that they could perform specific tasks faster than conventional machines.[3] While such successes have yet to achieve broad practical relevance, they show the potential of the current state of the art, known as "noisy intermediate-scale quantum" (NISQ) computers (see Figure 1).

"Given the technological and structural hurdles, quantum computers will not replace conventional computers in the next few years – perhaps even the next few decades – but will instead exist alongside them."

These developments have prompted many leading technology firms to present ambitious roadmaps for achieving advances in quantum computing. IBM's detailed plans for the period until 2029 are especially interesting in this respect.[4] Banks and other organisations can use these roadmaps as a guide in determining the ideal time to develop their own applications and thus ensure that they can stay competitive in the age of quantum computing.

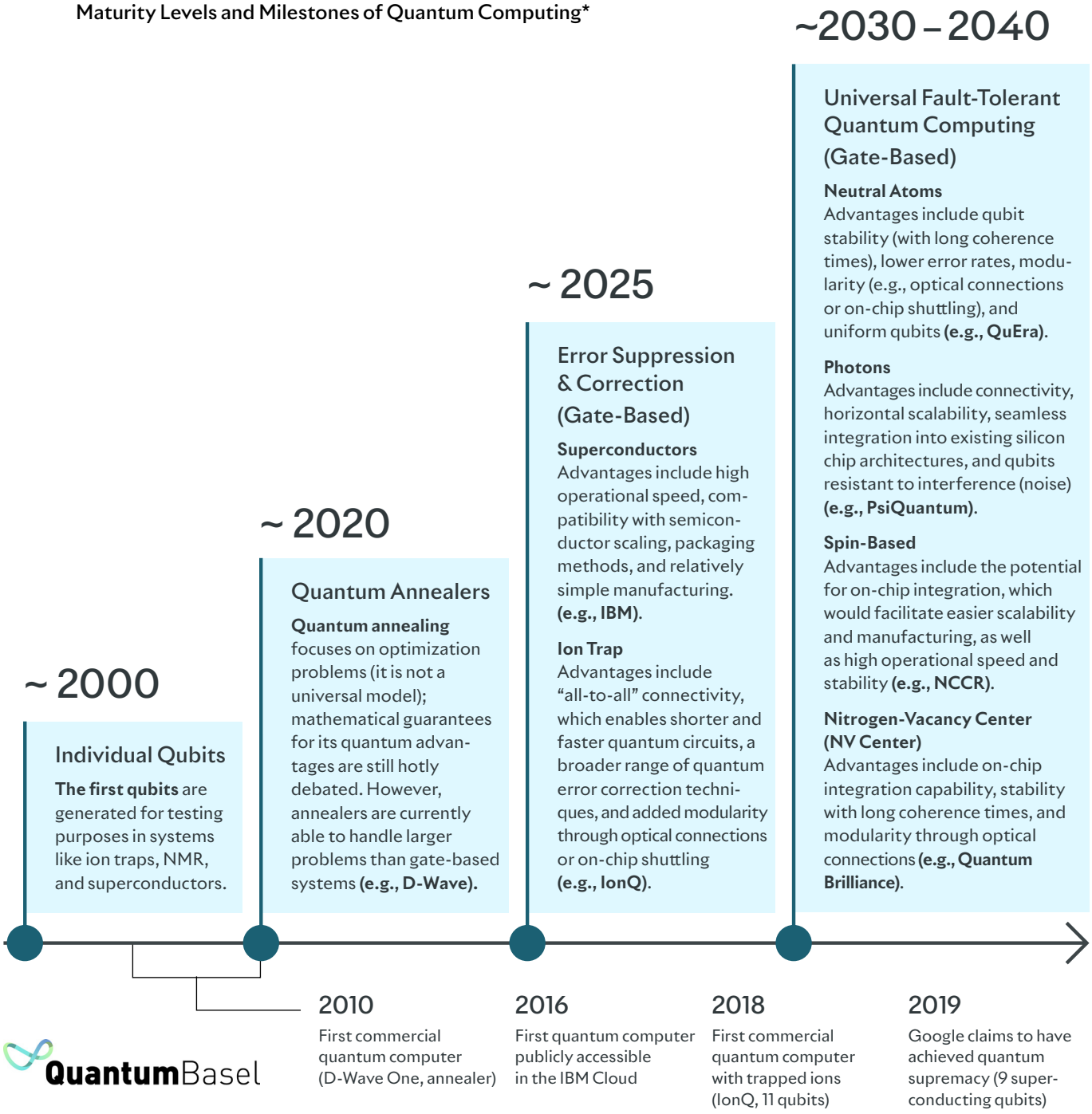
Given the technological and structural hurdles, quantum computers will not replace conventional computers in the next few years – perhaps even the next few decades – but will instead exist alongside them. They will bring their strengths to bear, first and foremost, in tasks that require substantial amounts of computing power, for which unique quantum algorithms are already being developed. Combining conventional and quantum computers – called hybrid quantum-classical systems – maximises both benefits and opens promising opportunities in various fields.

3 Nature, Google uncovers how quantum computers can beat today's best supercomputers (2024)

4 IBM, Quantum roadmap (2024)

Figure 1

Maturity Levels and Milestones of Quantum Computing*



* This overview is not exhaustive and does not consider that developments took place over several years; the highlighted years display only the major milestones.

Source: QuantumBasel, based on WEF, The Quantum Insider, and McKinsey. [5,6,7]

5 WEF, State of Quantum Computing (2022)

6 The Quantum Insider, The History of Quantum Computing (2024)

7 McKinsey Digital, Enabling the next frontier of quantum computing (2024)

2 Specific use cases in the banking sector

It is still uncertain when quantum computers will be used on a large scale. Estimates range from the late 2020s up to well into the 2030s. Despite this uncertainty over the pace of technological progress, banks nevertheless need to act now by starting to build up know-how and test their first applications. These should be based on assigning quantum algorithms to specific problems in the industry. The literature essentially distinguishes between three main categories of quantum algorithms:

1. Chemical and physical simulations
2. Machine learning and AI
3. Optimisation

While the first of these is not relevant for banks, the other two offer many use cases for the financial industry that will be discussed in detail below. It is essential to understand that the value added by quantum algorithms is highly dependent on the use case: some are focused on speed, others on the precision and quality of models (even when the data used to train them is incomplete), and others on energy efficiency. This means that the success of quantum computing applications always hinges on choosing suitable quantum algorithms.

Even without quantum computing, AI has already enabled significant advances in the financial industry, such as risk analysis and statistical forecasting models.[8] With quantum computing, the advantages of AI can be further maximised by developing more accurate AI models for use on conventional computers faster and more cheaply. This could give rise to a form of symbiosis whereby quantum computers enhance the quality and efficiency of AI models,[9] while AI, in turn, supports the development of more powerful quantum computers.[10] For example, by improving experimental procedures and methods.

Risk management, portfolio management, and derivative pricing applications also require enormous computing power. With demand for computing capacity rising steadily in the age of real-time trading, powerful computers are essential to remaining competitive. Below are some immediately relevant use cases of quantum computers in the banking sector.

8 University of Technology Sydney, Australia, AI in Finance: Challenges, Techniques and Opportunities (2021)

9 Jerbi, S., Fiderer, L.J., Poulsen Nautrup, H. et al. Quantum machine learning beyond kernel methods (2023)

10 Krenn M., Landgraf J., Foesel T. and Marquardt F. Artificial intelligence and machine learning for quantum technologies, (2023)

2.1 Risk management and risk monitoring

Quantum computers have an exceptionally high potential in risk management. According to the industry association UK Finance, banks today face significant challenges in analysing complex interactions between assets and their derivatives.[11] Banks such as Goldman Sachs, J. P. Morgan, Citi, and HSBC hope to gain a faster and more accurate insight into "tail risks" using quantum computers. Once identified with the aid of quantum algorithms, these risks can be more precisely pinpointed and mitigated using conventional computers. Faster identification of risks could also speed up reporting on risks to the supervisory authorities.

In the future, quantum computers could be capable of monitoring and analysing individual market players or even entire markets almost in real time. However, since it is not currently possible to efficiently feed sufficient conventional data into quantum computers, solutions will be based on hybrid quantum-classical approaches (including AI) in the medium term. Such systems would be able to analyse interdependencies between assets, their derivatives, intermediaries, portfolio managers, and clients more comprehensively.

Today's systems can, in many cases, only track cascading developments and, depending on the situation, trigger stops on individual investment positions. On the other hand, systems based on quantum computers could harness their ability to identify complex patterns by spotting triggers, interpreting spread patterns, and shedding light on complicated interactions. For example, they could analyse the relationships between movements in the price of underlying assets and their hedging instruments, including actual counterparty and default risks. These risks are often represented as constant in current systems, and their effects are only apparent after a delay of hours or even days. Still, quantum computers could track their behaviour dynamically almost in real-time, thus providing a basis for much faster and more precise decision-making.

Furthermore, some central banks are already interested in monitoring payment flows and started to collect data for this purpose. The Bank for International Settlements (BIS) has initiated several research projects in this area.[12]

2.2 Portfolio-Management

Portfolio optimisation is among the most challenging tasks in the financial industry and is also one of the most demanding in terms of computing power. Speed and accounting for multiple dependencies simultaneously are essential, and constant recalculation is needed regarding a portfolio's efficient frontier. Banks are working on continually enlarging portfolios and enhancing software solutions, for example, so that several portfolio strategies can be simulated at once. In some markets, AI running on conventional computers is already generating alpha (an excess return relative to the portfolio's benchmark). Using quantum computers in the future will allow for even higher alpha through the optimal combination with AI-supported forecasting.

11 UK Finance, Minimising the risks: quantum technology and financial services (2023)

12 BIS, Project Pyxtrial: monitoring the backing of stablecoins (2024)

2.3 Impact on encryption methods and quantum-safe approaches

One significant and, at the same time, risky use case for quantum computers is encryption – especially when it comes to cracking encryption methods that are in use today. Many of the encryption methods currently used by banks' IT systems are under threat from quantum computers. Shor's algorithm, for instance, threatens asymmetrical encryption methods like Rivest-Shamir-Adleman (RSA) because it can determine prime factors exponentially faster. Grover's algorithm, meanwhile, works on symmetrical methods like the Advanced Encryption Standard (AES) by achieving quadratic speed increases in searching unstructured databases or lists. This vulnerability can be reduced for symmetrical keys by doubling their length, but longer keys also affect the speed and efficiency of encryption.

The National Institute of Standards and Technology (NIST) in the US, the global leader in this field, has been working to develop quantum-safe cryptography since 2016. These new methods are also known by various other names, including post-quantum cryptography (PQC), quantum-proof and quantum-resistant. NIST published four such methods in July 2022: CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+, and FALCON. The first three processes based on these methods were officially standardised in the summer of 2024 – although they employ conventional cryptographic approaches for which quantum computers are not known to offer any advantage.[13, 14]

There are also encryption approaches that exploit the laws of quantum mechanics and are thus mathematically uncrackable, even by quantum computers. In practice, however, many of these are still underdeveloped compared with quantum-safe conventional protocols. One example is quantum key distribution (QKD), in which two parties share random numbers and can use them for secure communication, e.g. via the one-time pad or other protocols.[15]

In addition, work is already underway to encrypt existing data owned by financial service providers and other vital organisations using quantum-safe methods. The aim is to prevent "harvest now, decrypt later" attacks, in which unauthorised third parties steal data today in the hope of decrypting it using high-powered quantum computers at some point in the future.

2.4 Algorithmic trading

Algorithmic trading (algo trading for short) has been an established discipline for some decades at the interface between financial markets and ultra-fast, high-precision technology. Banks are working with ever more complex algorithms to make profits on the capital market through large numbers of individual transactions. In practice, however, achieving regular profits net of costs is highly challenging because algo-trading systems often trade against other systems with opposing expectations and parameters. AI-supported systems perform better in certain situations but frequently react to sudden trend reversals too slowly.

---

13 IBM's research centre in Rüschlikon, Switzerland, played a key role in developing these.

14 NIST, NIST Releases First 3 Finalized Post-Quantum Encryption Standards (2024)

15 A Swiss example of this is the company ID Quantique, which is working to bring QKD-based communication systems to market.

Quantum computers hold the potential for significant progress in this respect. Their higher computing power makes it possible not only to monitor multiple markets simultaneously but also to use amplitude estimation instead of the conventional Monte Carlo simulation technique. Amplitude estimation allows stochastic models to make more accurate estimates with less data processing.

2.5 Bank-specific and cross-sector AI

Most AI processes and methods can be applied to almost all areas of the increasingly digital industrial landscape. The underlying large language models (LLMs) can be employed similarly in any sector. As quantum computers evolve, AI can be expected to improve further in speed, precision, quality, and energy efficiency.

Alongside general AI, bank-specific AI solutions are geared to the unique challenges in the financial sector. The focus here is on risk and portfolio management, related simulations, and replacing existing assumptions and methods with more precise approaches. Integrating additional factors and developments is also an increasingly important consideration. These include financial derivatives and the growing use of distributed ledger technology (DLT), also known as blockchain. For example, Switzerland tests the latter with the wholesale central bank digital currency (CBDC) and the digital Swiss franc.[16, 17]

16 BIS, Project Helvetia: a multi-phase investigation on the settlement of tokenised assets in central bank money (2024)

17 Swiss Banking, Swiss banks sign memorandum of understanding to explore the feasibility of a jointly issued Swiss franc deposit token

Dreaming of the future! Which other financial applications are conceivable?

Monitoring entire financial markets and gaining a deeper insight into the real economy

When banks start to use quantum computers to invest in the financial markets, if not sooner, monitoring them in similar breadth and depth could make sense to respond quickly to crises. The current practice of monitoring individual markets or payment flows on a snapshot basis – which even today provides an incomplete picture of reality—would no longer be sufficient.

In addition to identifying high-risk developments early, monitoring entire financial markets would also give researchers and authorities new insights into how financial markets and the real economy function. This could include aspects such as ups and downs in inflationary pressure, which are well described but have not been subject to much empirical observation.

Climate, sustainability, natural disasters, and the attendant financial risks

Primary insurers and reinsurers are often the first companies to feel the impact of climate change directly in their operations and on their balance sheet. Still, banks and private investors are not far behind – sometimes not behind at all. They are faced with deciding whether to pay large sums to insure buildings in at-risk areas or sell them. As the volume and detail of available data increase, forecasts regarding potential risks become more accurate. When financial service providers experience an unexpected accumulation of these risks, it can have a knock-on effect on the entire financial market.

The power of quantum computers can be harnessed in simulations and complex analysis tasks at various levels. First and foremost, they are helpful for weather and climate models and risk models based on these that also consider geological and topographical factors. They can also be used to assess the attendant risks for individuals and companies and to analyse the challenges that may arise for specific financial market participants or the economy as a whole.

Initial industry experience

Quantum computing and new encryption methods are not only relevant for large banks and those that operate internationally. Small and medium-sized institutions can also benefit from combining quantum computing and AI. In fact, a number of them are already developing their first applications in this field.

Selected Swiss examples

UBS
UBS has been researching quantum computing since 2018 and has set up special working groups to investigate specific applications, quantify their advantages for the financial sector, and identify potential risks. Various projects have already been tested with the aid of specialist firms, such as portfolio optimisation and the valuation of financial derivatives. Another UBS working group is analysing the risks this technology poses and developing measures to counteract them.

Migros Bank
Migros Bank has embarked on its "quantum journey" as part of its risk management and focus on digital innovation. In partnership with QuantumBasel, Migros Bank employees are trained to evaluate quantum computing use cases. This program encompasses understanding and mitigating security risks posed by cryptographically relevant quantum algorithms and exploring new customer benefits through quantum computing.

Open Quantum Institute
The Open Quantum Institute (OQI) is a multilateral governance initiative that promotes global and inclusive access to quantum computing and the development of applications for the benefit of humanity. As a science diplomacy instrument, OQI forms partnerships with industry providers who donate capacity on their quantum computers to develop use cases to achieve the UN Sustainable Development Goals. OQI is a cooperation between CERN and the Geneva Science and Diplomacy Anticipator Foundation (GESDA), supported by UBS, the Federal Department of Foreign Affairs (FDFA), and the Swiss universities ETH Zurich and EPFL.

Swiss Quantum Initiative
Launched by the Federal Council in 2022, the Swiss Quantum Initiative (SQI) promotes Swiss research and innovation in the quantum sciences. From 2025 to 2028, it has been allocated funding of CHF 82.1 million. The initiative aims to strengthen Switzerland’s international competitiveness through competitive calls for proposals and knowledge and technology transfer.

Selected international examples

J.P. Morgan

The large US bank has been researching quantum computing for several years.[18] It covers topics such as IT security, improved data encryption, and optimised hedging on financial markets. The bank's stated aim is to establish quantum computing solutions in relevant areas to exploit this technology's advantages before its competitors.[19] It also investigates links to blockchain technology, which relies on encryption and is becoming increasingly important in interbank business.

HSBC

The UK-based global bank has set itself three goals in quantum technology.[20] Working with partners like IBM, Fujitsu and Quantinuum, it wants to be at the forefront of the financial services industry by exploring how to integrate quantum computing into its products and services. In addition to building a dedicated in-house team of experts to conduct further research and develop products and patent innovations, it strives to create real-world use cases in all business areas to prepare for a quantum-secure digital economy. It cites various examples, including pricing optimisation (e.g., for financial derivatives), collateral optimisation (since redundant collateral is expensive), and improved Monte Carlo simulations for stochastic forecasting models.

Bank for International Settlement (BIS)

The BIS addresses topics such as quantum-proofing the financial system and financial market stability in Project Leap, which aims to prepare the participating central banks to respond to upcoming developments in good time.[21] Participating institutions include the Banque de France and Germany's Bundesbank.

---

18 J.P. Morgan, Global Technology Applied Research (2024)

19 J.P. Morgan, JPMorgan Chase, Toshiba and Ciena Build the First Quantum Key Distribution Network Used to Secure Mission Critical Blockchain Application (2024)

20 HSBC, HSBC and Quantum (2024)

21 BIS, Project Leap: quantum-proofing the financial system (2024)

3 Conclusions and recommendations

3.1 For Swiss banks

Quantum computing may still be in its infancy, but banks and other financial service providers must act on it today. Ignoring it for now or just being a passive observer would give rise to various risks, including data theft via "harvest now, decrypt later" attacks, competition over scare quantum talents (just like in AI development) and the threat of being edged out over the long term by rivals that have devised new or improved business models based on quantum algorithms. The number of quantum computing patents, including those specific to the financial sector, is growing steadily and thus increasing the pressure to innovate.[22, 23, 24]

Timing is critical for all offensive and defensive security measures based on quantum computing. Even though it is not yet clear when many of the encryption methods in use today might come under threat, action is needed right now. It will take years to adapt banks' existing IT architecture, roll out post-quantum cryptography, and replace the current security protocols. Combined with other technologies such as AI and DLT, quantum computing has the potential to influence banks' cost and risk structures as well as their product and service offerings significantly over the medium to long term.

The authors, members of a joint SBA and QuantumBasel expert group, have drawn up the following recommendations for identifying the opportunities and risks at an early stage and mitigating or avoiding the risks:

- **Analyse and monitor the current landscape:** Progress in quantum computing and quantum-safe cryptography is fast. Banks should track this progress closely and investigate potential weaknesses in their current IT landscape, including applications, networks, partner communication, and security components.
- **Classify data and assess risks:** Not all data will be worth protecting in five or ten years, and not all data and protocols are threatened by quantum algorithms. An inventory of current information is needed to classify the long-term value of data and processes and the extent to which they are at risk. Critical information should be prioritised, and the threats to which it is exposed should be assessed. The findings could be visualised in a heatmap that provides an overview of the critical threats and opportunities.
- **Create a roadmap and a migration plan:** Based on the inventory, architecture plans should be adapted, and a migration to quantum-safe cryptography should be planned. Crypto-agility is essential here as further migrations may be needed soon, for example, to roll out quantum mechanics-based solutions like quantum key distribution. A roadmap containing the action areas and measures can serve as a guide.

22 The Quantum Insider, EPO: Quantum Computing's Patent Growth is Multiplying, Leads Tech Industry (2023)

23 QED-C, Quantum patent trends update 2022 (2023)

24 Deloitte, Industry spending on quantum computing will rise dramatically. Will it pay off? (2023)

The following measures can help in making the first step into the quantum age:[25]

- **Train and raise awareness:** Staff and managers should be informed about the risks and opportunities associated with quantum technology. This can be done through targeted communication and training, including teaching IT security and cryptography teams the latest algorithms and methods.
- **Update security rules:** Existing security guidelines and processes must be continually revised to account for new, quantum-safe algorithms. This entails defining a target state and drafting a long-term strategy that sets out the required quantum security capabilities and technologies.
- **Review suppliers and partners:** Banks should assess the quantum-safe precautions taken by their suppliers and partners to ensure they are adequate.

Banks should also take account of the opportunities with the following measures:

- **Seeking cooperation with specialist organisations:** Banks should seek to cooperate with specialist firms and organisations in the experimental phase to gather experience and develop shared frameworks and approaches.
- **Promoting cloud-based use of quantum computing:** As with large AI applications, quantum computing will be accessible primarily via cloud infrastructures in the medium term. Banks should, therefore, address their cloud readiness intensively.[26]

3.2 For the authorities

Thanks to Switzerland's technology-neutral and principles-based regulatory framework, the need for changes to laws and regulations will likely be limited for the time being. In essence, the same principles apply to the supervision and regulation of quantum computing in Switzerland as to other new technologies: technology neutrality, proportionality, protection of the financial centre's reputation, and legal certainty. To assess where changes may be needed, the current framework should first be analysed considering the expected uses of quantum computing. Increasing experience will expose further gaps that can then be addressed at the appropriate time. We believe that regulatory considerations regarding quantum computing can be divided into two main categories: security aspects – in particular, post-quantum cryptography (PQC) – and regulation of new products and services made possible by quantum computing.[27]

The transition to PQC will affect all sectors, not just the financial industry. Banks are already subject to due diligence, data protection, and confidentiality requirements. They are expected to take organisational and technical precautions to ensure data and information security. Since security requirements are constantly evolving, banks are also expected to adapt their security concepts on an ongoing basis.

---

25 The German Federal Office for Information Security (BSI) offers a comprehensive guide for implementing PQC: Kryptografie quantensicher gestalten – Grundlagen, Entwicklungen, Empfehlungen (German only).

26 As a guide to secure cloud banking, we recommend the SBA Cloud Guidelines.

27 The GSM Association, the industry association for GSM mobile providers, maintains a list of initiatives by various countries in the field of post-quantum cryptography (PQC).

Monitoring the implementation of these measures forms part of the remit of supervisory authorities such as FINMA.[28]

While the potential impact of quantum computing on cyber security is already evident, far less is known about the implications for day-to-day business (for example, in terms of data protection). Regular dialogue between industry and regulators is thus vital for sharing experiences and identifying potential action areas at an early stage.

The growing importance of quantum computing is also reflected in national and geopolitical initiatives. The G7 held a workshop in Rome in September 2024 to discuss the construction of a quantum-safe financial system and evaluate the roles of regulatory authorities and private actors. In its concluding statement, it encourages financial authorities to work closely with firms and other relevant parties to raise awareness of the importance of the transition to quantum-resilient technologies.[29] This high-level exchange is already happening in Switzerland via the Open Quantum Institute, the World Economic Forum's Quantum Economy Network, and the Swiss Quantum Initiative.[30, 31, 32] These examples clearly show the political interest and the importance of partnerships in quantum computing.

3.3 For the Swiss financial centre

Using new technologies to improve products and services is essential to securing the Swiss financial centre's international competitiveness over the medium to long term. Quantum computing is pivotal alongside other technologies, such as AI and DLT. Factors that allow individual banks to remain competitive can be expected to strengthen the financial centre as a whole. From the Swiss financial centre's perspective, therefore, the fact that Swiss universities and research institutes are engaging in both fundamental and applied research is to be welcomed. Short pathways enabling fast communication on a formal and informal basis, high levels of expertise, and a readiness to adapt to change will lay a solid foundation for the successful deployment of this new technology.

28 In April 2024, the European Commission recommended that EU member states develop a joint roadmap for transitioning to post-quantum cryptography (PQC). The goal is to coordinate the shift to quantum-safe cryptography for the public sector and critical infrastructures across the EU.

29 G7 Cyber Expert Group, Statement on Planning for the Opportunities and Risks of Quantum Computing (2024)

30 Open Quantum Institute (OQI) (2024)

31 WEF Quantum Economy Network (2024)

32 Swiss Quantum Initiative (SQI) (2024)

4 Conclusion

Developments in the field of quantum computing give rise to both opportunities and challenges for the Swiss financial sector. With their ability to carry out complex calculations and simulations more efficiently and with greater accuracy, quantum computers open up new possibilities, for example, in risk management and portfolio optimisation. At the same time, however, today's security protocols must be improved using quantum-safe cryptography. The technology requirements this entails must not be underestimated, so financial institutions should start planning to prepare for these eventual changes.

They must invest in quantum readiness as early as possible to ensure they are equipped for a quantum-safe future. Targeted development of their own capabilities and cooperation with specialist organisations can secure a long-term competitive edge for banks while minimising the risks associated with quantum computing. These investments represent not only a commitment to innovation but also an essential step towards sustainably enhancing the resilience of the entire Swiss financial centre.

"Investments in this domain of computing represent not only a commitment to innovation but also an essential step towards sustainably enhancing the resilience of the entire Swiss financial centre."

The recommendations in this report offer an initial guide to addressing this topic and successfully shaping the technological transformation. Further analyses of the opportunities and risks associated with quantum computing will be necessary as soon as the technology enters broader use in the financial industry and other sectors. At the same time, active dialogue between the industry and authorities must be fostered and encouraged so that developments in this field can be constantly monitored and action areas can be identified at an early stage. The industry's collaboration with leading research institutes and companies certainly gives grounds for optimism that Switzerland is on the right track to assume a leading role in quantum technology.

Glossary

Algorithm: A finite sequence of instructions to solve a specific problem or perform a particular task. Unique algorithms exist in quantum computing, such as Shor's and Grover's, that use quantum mechanics to perform particular calculations faster than conventional algorithms.

Crypto-agility: The ability to respond quickly to new cryptographic threats by adapting crypto systems flexibly to new standards and algorithms.

Decoherence: The collapse of a qubit's quantum behaviour when it interacts with its environment leads to a loss of information. Decoherence is one of the greatest challenges for quantum computing.

Entanglement: A phenomenon whereby two qubits are connected in such a way that changing the state of one immediately influences the state of the other, regardless of the distance between them.

Error correction: Since quantum computers are prone to errors, they require complex error correction methods to enable stable calculations.

Grover's algorithm: A quantum algorithm that offers quadratic speed advantages compared with conventional algorithms in searching unstructured databases. It can compromise the security of symmetrical encryption methods.

Noisy intermediate-scale quantum (NISQ): A class of quantum computers that is currently available and offers limited performance. These systems are still error-prone and have a small number of qubits, but they can already solve specific problems more quickly than conventional computers.

One-Time Pad (OTP): An encryption method that is theoretically unbreakable when used correctly. A one-time pad involves a random key that is as long as the message itself. This key is used only once and then discarded, making it immune to any cryptographic attack as long as it remains secret and truly random. The one-time pad requires the secure exchange of keys, making it challenging to implement in practice.

Post-quantum cryptography (PQC): A new generation of cryptographic algorithms that are resistant to attacks by quantum computers. NIST has already standardised three such methods.

Quantum key distribution (QKD): A process that uses the laws of quantum mechanics to share secure communication keys between two parties. It is resistant to both conventional and quantum attacks.

Quantum logic gate: The fundamental building-block of a quantum computer. Quantum logic gates manipulate qubits to perform calculations and enable parallel states through quantum phenomena such as superposition and entanglement. They can perform more complex operations more efficiently than conventional logic gates, which only work with values of 0 and 1.

Quantum random access memory (qRAM): A concept for computer memory that enables the parallel processing of large quantities of data in a quantum computer. It is a potential solution to the current limitations of using conventional data entry to feed quantum computers.

Qubit: The basic unit of information in a quantum computer. Unlike conventional bits, which can have a value of either 0 or 1, qubits can have both values at once, thanks to superposition.

Shor's algorithm: A quantum algorithm that can find the prime factors of large numbers exponentially faster than conventional algorithms. It poses a threat to asymmetrical encryption methods such as RSA.

Superposition: A phenomenon in quantum mechanics whereby a qubit can exist in multiple conventional states (0 and 1) at the same time. This makes quantum computers capable of massive parallel processing.

Edited by

Andrea Luca Aerni, Policy Advisor Digital Finance, SBVg
Richard Hess, Head of Digital Finance, SBVg
Panagiotis Psomas, Intern Digital Finance, SBVg

Experts

QuantumBasel

Damir Bogdan, CEO, QuantumBasel
Frederik F. Flöther, Chief Quantum Officer, QuantumBasel

SBA member institutions

Marco Foglia, Information Security Officer, Raiffeisen Schweiz
Christian Hostettler, Lead Technology Architect, PostFinance
Cedric Membrez, Head Applied Research, Group Emerging Technology, UBS

About the Swiss Bankers Association (SBA)

The Swiss Bankers Association (SBA) is the Swiss financial sector's leading industry organisation and represents the interests of some 270 member institutions. Founded in 1912, it ensures optimal framework conditions for a competitive and innovative Swiss banking industry. It promotes dialogue with politicians and authorities, drives vital topics such as sustainable finance and digital currencies, and supports education and professional development in the industry. As a knowledge center, it is dedicated to the sustainable development of the banking industry.

swissbanking.ch

About QuantumBasel

QuantumBasel is a private company based at the uptownBasel innovation campus that uses quantum technology and AI to drive sustainable innovation in partnership with startups, large corporations, and universities. With a global technology ecosystem that combines research and expertise, QuantumBasel promotes the transition of quantum computing from research to industrial application. Switzerland's first commercially usable quantum computer is set to enter operation at the campus at the end of 2024.

quantumbasel.com

Swiss Bankers Association
Aeschenplatz 7
P.O. Box 4182
CH-4002 Basel
office@sba.ch
www.swissbanking.ch