Swiss Banking

QuantumBasel

Quantum Computing in Banking

Funktionsweise, Anwendungsfelder und Handlungsempfehlungen für Schweizer Banken

November 2024

Expertenbericht der SBVg

Executive Summary

Die Anforderungen an die IT-Systeme bei Banken nehmen laufend zu. Die stetig wachsende Datenmenge und der zunehmende Einsatz künstlicher Intelligenz (KI) könnten diese Systeme in Zukunft an ihre Leistungsgrenzen bringen. Vor diesem Hintergrund rückt Quantum Computing immer mehr in den Fokus. Diese Technologie hat sich in den letzten Jahren von einem «Science-Fiction»-Thema zu einer wissenschaftlichen Realität entwickelt und wird bald den ersten Schritt vom Labor in die Industrie machen. Die entscheidende Frage ist daher nicht mehr, ob die Technologie Fuss fassen wird, sondern wann und in welcher Weise.

Auch wenn die physikalischen Prinzipien hinter Quantum Computing nicht leicht zu durchdringen sind und die Technologie noch nicht flächendeckend eingesetzt wird, werden ihre potenziellen Auswirkungen auf den Finanzsektor zunehmend sichtbar. Die Technologie stellt dabei sowohl eine Chance als auch eine Herausforderung dar. Mit der Fähigkeit, komplexe Berechnungen und Simulationen effizienter und präziser durchzuführen, eröffnen Quantencomputer neue Anwendungsmöglichkeiten. Dieser Expertenbericht identifiziert und beleuchtet beispielhaft vier Anwendungsbereiche von Quantum Computing im Bankensektor:

- Im **Risikomanagement und -Monitoring** erlauben Quantencomputer die Analyse komplexer Interdependenzen zwischen Vermögenswerten und Derivaten sowie ein beinahe Echtzeit-Monitoring.
- Im **Portfolio-Management** können Quantencomputer Portfolios durch parallele Berechnungen und bessere Simulationen optimieren und somit höhere Renditen ermöglichen.
- Im **algorithmischen Trading** besteht die Möglichkeit, durch Quantencomputer effizientere und genauere Algorithmen für den Handel an Finanzmärkten zu etablieren.
- Zuletzt ermöglichen Quantencomputer ein günstigeres und schnelleres **Bauen und Trainieren von KI-Modellen,** welche dann bei der Anwendung im Geschäftsalltag präzisere und effizientere Vorhersagemodelle liefern können.

«Die entscheidende Frage ist nicht mehr, ob die Technologie Fuss fassen wird, sondern wann und in welcher Weise.»

Nebst den Chancen schafft Quantum Computing auch neue Risiken, die insbesondere mittels Anpassung an quantensichere Verschlüsselungsverfahren adressiert werden müssen. Aufgrund der Risiken durch sogenannte «Harvest now, decrypt later»-Angriffe und der langen Vorlaufzeit zur Einführung quantensicherer Kryptographie stellt Quantum Computing in dieser Hinsicht schon jetzt eine ernstzunehmende Herausforderung dar.

Die Autoren empfehlen daher folgende Massnahmen auf unterschiedlichen Ebenen:

- **Banken** sollten bestehende Sicherheitsrichtlinien kontinuierlich anpassen und eine Roadmap zur Einführung quantensicherer Kryptographie entwickeln. Weiter sollten sie in Zusammenarbeit mit spezialisierten Organisationen und Forschungseinrichtungen ihre Fähigkeiten rund um Quantum

Computing stetig aufbauen, um so ihre Agilität im Hinblick auf die breitere Anwendung dieser Technologie zu erhöhen. Dies beinhaltet insbesondere auch die Unterstützung von Anwendungsforschung mit Schweizer Universitäten und Forschungseinrichtungen, um das gegenseitige Know-how zu stärken und in Zukunft einen ausreichend grossen Talentpool sicherzustellen.

- **Regulierungs- und Aufsichtsbehörden** in der Finanzindustrie sollten einen regelmässigen Dialog mit der Branche pflegen, um die Anwendungsbereiche von Quantum Computing in der Finanzindustrie zu verstehen und potenziellen Handlungsbedarf frühzeitig zu erkennen. Im regulatorischen Kontext ist aus unserer Sicht vorerst kein Handlungsbedarf absehbar. Die möglichen Risiken durch die Anwendung von Quantum Computing werden durch die derzeitige, technologieneutral und prinzipienbasiert ausgestaltete Regulierung ausreichend abgedeckt.
- Um die Wettbewerbs- und Innovationsfähigkeit sowie Resilienz des **Schweizer Finanzplatzes** langfristig zu sichern, ist der Einsatz neuer Technologien wie Quantum Computing, KI und Distributed Ledger Technology (DLT) entscheidend. Dafür braucht es weiterhin eine enge Zusammenarbeit der Branche mit Forschungseinrichtungen, kurze Kommunikationswege sowie eine hohe Anpassungsbereitschaft und -fähigkeit der Finanzinstitute. Dieses Erfolgsrezept ist auch in Zukunft zu erhalten und zu fördern.

«Die Banken sollten ihre aktuelle IT-Landschaft kontinuierlich auf potenzielle Schwachstellen hin analysieren und ihre Sicherheitsvorgaben aktualisieren.»

Entscheidungsträgerinnen und Entscheidungsträger aus der Finanzindustrie, Behörden und Politik müssen bereits heute die Weichen richtig stellen, um in den kommenden Jahrzehnten sowohl die Chancen von Quantencomputern in der Finanzindustrie ausschöpfen zu können als auch die damit verbundenen Risiken frühzeitig zu erkennen und zu vermindern. Mit dieser Weitsicht schaffen sie optimale Rahmenbedingungen für einen wettbewerbsfähigen, innovativen und resilienten Schweizer Finanzplatz – heute und in Zukunft.

1 Grundlagen des Quantum Computing

Das Bild einer sich schnell auf ihrer Kante drehenden Münze ist eine ausgezeichnete Metapher für das Herzstück des Quantum Computing. In herkömmlichen Computern ist das Bit die kleinste Informationseinheit, vergleichbar mit den zwei möglichen Seiten einer Münze – Kopf oder Zahl, 0 oder 1. Im Quantum Computing jedoch werden Informationen in sogenannten Qubits gespeichert, den Quantenbits. Ähnlich wie eine rotierende Münze, die gleichzeitig Kopf und Zahl zu zeigen scheint, kann ein Qubit sich in einem Zustand der Überlagerung befinden, bei dem es eine Kombination aus 0 und 1 gleichzeitig repräsentiert (siehe Box: «Die Funktionsweise von Quantencomputern»).

Diese Überlagerung bildet die Grundlage für die Entwicklung von Quantenalgorithmen, die Probleme auf völlig neue Art lösen – weit über die Fähigkeiten klassischer Computer hinaus. Komplexe Rechenaufgaben und Simulationen, die bisher nur mit grossem Aufwand und als Annäherungen lösbar waren, können durch Quantum Computing effizienter und schneller gelöst werden. Gerade die Bankenbranche, die stark von solchen aufwendigen Simulationen, Szenarioanalysen und der Verarbeitung unzähliger Daten geprägt ist, könnte somit erheblich von dieser Technologie profitieren.

Doch wie eine Münze, die in Bewegung ist, ist auch der Zustand eines Qubits äusserst instabil und kann sich schnell verändern oder verloren gehen. Quantencomputer müssen daher oft in äusserst stabilen und stark gekühlten Umgebungen arbeiten, da selbst kleinste Störungen die empfindlichen Qubits beeinträchtigen und Berechnungen unbrauchbar machen können. In der Schweiz tragen Universitäten wie die ETH Zürich, die EPFL und die Universität Basel wesentlich zur Grundlagenforschung auf diesem Gebiet bei, insbesondere in den Bereichen Quantensensorik, Quantenverschlüsselung und Quantensimulation. Ebenso spielen neue Initiativen wie QuantumBasel, Startups und etablierte Technologieunternehmen eine wichtige Rolle bei der Anwendungsentwicklung. Staaten weltweit investieren erhebliche Summen in die Quantenforschung, um sowohl Wettbewerbsvorteile zu sichern, als auch potenziellen Cyberangriffen vorzubeugen.[1]

Die genannten Akteure konzentrieren sich nicht nur auf den technologischen Fortschritt, sondern auch auf die absehbaren Risiken. Eines dieser Risiken ist die Fähigkeit von Quantencomputern, einige der gängigen Verschlüsselungsverfahren zu knacken, die auch in IT-Systemen von Banken zum Einsatz kommen. Schon heute befassen sich Banken sowie Regulierungs- und Aufsichtsbehörden daher mit quantensicherer Kryptographie.

Die Entwicklungen im Quantum Computing und in der Quantenverschlüsselung werden das Finanzsystem ähnlich stark beeinflussen, wie es aktuell die Künstliche Intelligenz (KI) mit ihren Large-Language-Modellen (LLMs) in verschiedenen Bereichen tut. Dabei liegt der Fokus auf dem Quantum Computing, während andere Quantentechnologien wie Quantenkommunikation und Quantensensorik weniger im Mittelpunkt stehen.

---

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

Die Funktionsweise von Quantencomputern

Konventionelle Computer verarbeiten Informationen in Form von Bits. Diese beruhen auf elektrischen Spannungen (oder Stromimpulsen), die entweder über oder unter einem bestimmten Schwellenwert liegen, wodurch die binären Zustände 0 und 1 erzeugt werden. Um Berechnungen durchzuführen, werden Logikgatter verwendet, die durch Transistoren realisiert werden. Diese Gatter sind miteinander zu komplexen Netzwerken verbunden, die es dem Computer ermöglichen, verschiedene Rechenoperationen auszuführen.

Quantencomputer hingegen basieren auf den Prinzipien der Quantenmechanik, also den physikalischen Gesetzen, die das Verhalten von Teilchen wie Atomen und Elektronen bestimmen. Informationen werden im Quantum Computing durch sogenannte Qubits abgebildet. Qubits können in verschiedenen physikalischen Systemen realisiert werden, etwa in Atomen, Ionen, Photonen oder supraleitenden Materialien. Jedes dieser Systeme hat allerdings seine eigenen Vor- und Nachteile. Was sie gemeinsam haben, ist die Nutzung quantenmechanischer Effekte wie Interferenz, Überlagerung und Verschränkung, um völlig neue Ansätze zur Lösung von Problemen zu ermöglichen.

In der klassischen Welt kann man zwei Bits so kombinieren, dass sie die Zustände 00, 01, 10 oder 11 annehmen – also vier verschiedene Kombinationen. Zwei Qubits hingegen können nicht nur diese vier Zustände einnehmen, sondern eine Überlagerung davon bilden. Das bedeutet, sie können gleichzeitig in all diesen Zuständen sein und dadurch mit allen gleichzeitig rechnen. Diese Fähigkeit, viele Zustände parallel zu verarbeiten, erklärt die enormen Vorteile von Quantenalgorithmen. Mit jedem weiteren Qubit verdoppelt sich die Rechenleistung: Ein Computer mit 51 Qubits ist theoretisch doppelt so leistungsfähig wie einer mit 50. Diese exponentielle Skalierbarkeit ist ein Grund, warum Quantum Computing in den letzten Jahren so grosse Fortschritte gemacht hat und warum Banken und andere Unternehmen schon heute in die noch junge Technologie investieren.

Technologische und strukturelle Hürden im Quantum Computing

Quantum Computing operiert an der Grenze dessen, was derzeit technologisch machbar und physikalisch möglich ist. Ein Quantencomputer mit einer Rechenleistung von 400 Qubits kann beispielsweise mehr Zustände erzeugen als es Atome im sichtbaren Universum gibt. Um diese Technologie weiterzuentwickeln, müssen aber noch einige Herausforderungen bewältigt werden:

- **Fehlerkorrektur:** Quantencomputer sind äusserst anfällig für Fehler, weshalb umfangreiche Korrekturmechanismen erforderlich sind. Algorithmen zur Fehlerkorrektur werden ständig verbessert und neue Verfahren für effizientere Fehlerkorrektur entwickelt.[2]
- **Skalierbarkeit:** Bei der Skalierung von Quantencomputern entstehen zusätzliche Herausforderungen, etwa bei der parallelen Fehlerkorrektur oder der Zuverlässigkeit der Quantengatter – den Grundbausteinen von Quantencomputern, die es ermöglichen, Qubits gleichzeitig in mehreren Zuständen zu manipulieren.

2 So präsentierte beispielsweise Amazon Web Services (AWS) im März 2024 ein neues Verfahren, das eine effizientere Fehlerkorrektur ermöglicht

- **Software:** Software, die ursprünglich für klassische Computer entwickelt wurde, stellt für Quantencomputer ein Flaschenhals dar. Um das volle Potenzial von Quantencomputern auszuschöpfen, sind daher Verbesserungen bei den Algorithmen, Programmiersprachen und Optimierungstools nötig.
- **Standards und Protokolle:** Noch sind die verschiedenen Quantencomputer-Plattformen kaum miteinander kompatibel. Der Trend geht jedoch zunehmend dahin, dass unterschiedliche Systeme für unterschiedliche Anwendungsfälle genutzt werden.
- **Dateneinspeisung:** Es ist ein Irrglaube, dass Quantencomputer hauptsächlich für «Big-Data»-Probleme geeignet sind. Tatsächlich ist es momentan noch schwierig, grosse Datenmengen effizient in Quantencomputer einzuspeisen. Fortschritte, etwa bei «Quantum Random Access Memory» (qRAM), sind vielversprechend, aber Echtzeitanwendungen werden wohl noch auf sich warten lassen.
- **Fachkräftemangel:** In der Schweiz gibt es eine wachsende Zahl an Forschenden im Bereich Quantum, doch die Anzahl der Studierenden, die in diesem Bereich ausgebildet werden, reicht nicht aus, um den benötigten Talentpool aufzubauen. Trotz engagierter Programme an Universitäten wie der ETH Zürich, wo etwa 500 Personen in diesem Bereich arbeiten, bleibt der Fachkräftemangel eine zentrale Herausforderung.

«Angesichts der technologischen und strukturellen Hürden werden Quantencomputer in den kommenden Jahren – und voraussichtlich auch Jahrzehnten – konventionelle Rechner nicht ersetzen, sondern vielmehr ergänzen.»

Ein entscheidender Meilenstein in der Entwicklung der Quantencomputer war 2019, als Google erfolgreich demonstrieren konnte, dass bestimmte Aufgaben mit einem Quantencomputer schneller gelöst werden können als auf herkömmlichen Rechnern.[3] Obwohl diese Erfolge bisher noch keine breite praktische Relevanz erreicht haben, zeigen sie das Potenzial von diesen sogenannten «Noisy Intermediate-Scale Quantum» (NISQ)-Computern, die die derzeitige Entwicklungsstufe dieser Technologie markieren (vgl. Abbildung 1).

Angesichts dieser Entwicklungen haben viele namhafte Technologieunternehmen ehrgeizige Roadmaps für die Weiterentwicklung von Quantencomputern vorgelegt. Besonders erwähnenswert ist die detaillierte Planung von IBM bis 2029.[4] Banken und andere Organisationen können sich an diesen Roadmaps orientieren, um den optimalen Zeitpunkt für die Entwicklung eigener Anwendungen zu identifizieren und damit ihre Wettbewerbsfähigkeit im Zeitalter des Quantum Computing zu sichern.

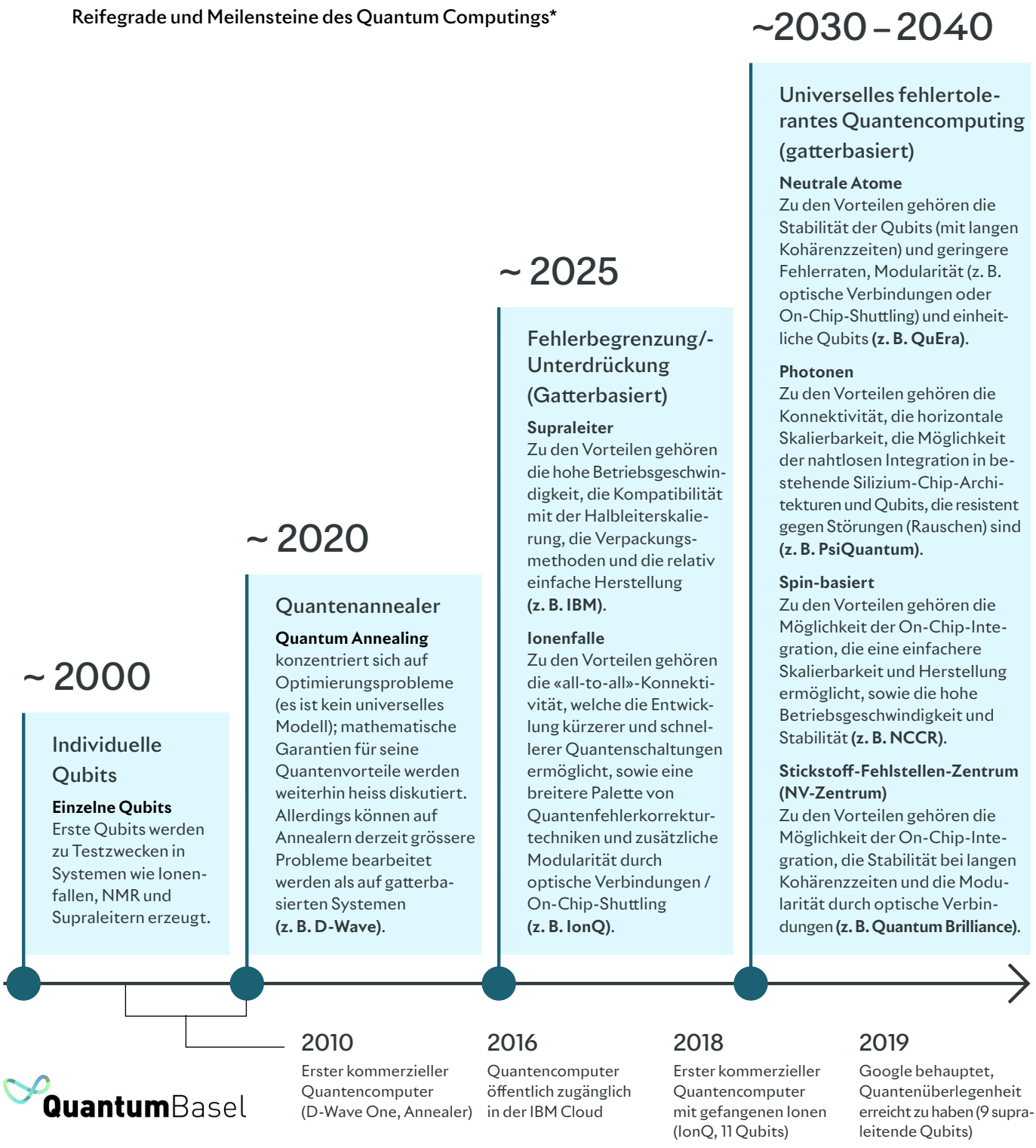
Angesichts der technologischen und strukturellen Hürden werden Quantencomputer in den kommenden Jahren – und voraussichtlich auch Jahrzehnten – konventionelle Rechner nicht ersetzen, sondern vielmehr ergänzen. Quantencomputer werden ihre Stärken vor allem bei besonders rechenintensiven Aufgaben ausspielen können, für die bereits spezielle Quantenalgorithmen entwickelt wurden. Die Kombination aus konventionellen Rechnern und Quantencomputern – sogenannte hybride quantum-klassische Systeme – schöpft die Vorzüge beider Entwicklungen optimal aus und eröffnet vielversprechende Perspektiven für verschiedene Anwendungsbereiche.

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

4 IBM, Quantum roadmap (2024)

Abbildung 1

Reifegrade und Meilensteine des Quantum Computings*



* Dieser Überblick ist nicht umfassend und die Entwicklungen haben sich über mehrere Jahre hinweg vollzogen; die hervorgehobenen Jahre dienen nur als grobe Wegweiser.

Quelle: QuantumBasel, basierend auf WEF, The Quantum Insider und 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 Konkrete Anwendungsbereiche im Bankensektor

Der genaue Zeitpunkt für einen Einsatz von Quantencomputern in grossem Stil ist noch ungewiss. Die Schätzungen reichen von den späten 2020er- bis weit in die 2030er-Jahre. Trotz dieser Unsicherheit in Bezug auf die Geschwindigkeit der technologischen Entwicklung ist jetzt der richtige Zeitpunkt für Banken, um aktiv zu werden. So kann bereits heute Know-how aufgebaut und in ersten Anwendungen getestet werden. Diese Anwendungen basieren auf der Zuordnung von Quantenalgorithmen zu konkreten Problemen in der Branche. In der Literatur werden grundsätzlich drei Hauptkategorien von Quantenalgorithmen unterschieden:

1. Chemische und physikalische Simulation
2. Maschinelles Lernen und Künstliche Intelligenz
3. Optimierung

Die erste Kategorie ist für Banken irrelevant. Quantenalgorithmen in den Kategorien zwei und drei hingegen bieten vielfältige Anwendungsfelder, die im Folgenden genauer betrachtet werden. Dabei ist wichtig zu verstehen, dass der Mehrwert von Quantenalgorithmen je nach Anwendungsfall unterschiedlich ausfällt – manchmal steht die Geschwindigkeit im Vordergrund, manchmal die Genauigkeit und Qualität der Modelle (selbst bei unvollständigen Trainingsdaten) und in anderen Fällen spielt die Energieeffizienz eine zentrale Rolle. Entscheidend für den Erfolg eines Quantencomputer-Einsatzes ist folglich immer die Zuordnung der richtigen Quantenalgorithmen zu den jeweiligen Anwendungsfällen.

Schon heute hat KI, ohne den Einsatz von Quantencomputern, erhebliche Fortschritte in der Finanzindustrie ermöglicht, etwa bei Risikoanalysen oder auch statistischen Vorhersagemodellen.[8] Mit Quantum Computing könnten die Vorteile von KI noch weiter ausgebaut werden, indem schneller und kostengünstiger präzisere KI-Modelle entwickelt werden, welche dann mit konventionellen Computern angewandt werden. In diesem Zusammenhang entsteht potenziell eine Symbiose: Quantencomputer ermöglichen bessere und effizientere KI-Modelle,[9] während KI wiederum die Entwicklung leistungsfähigerer Quantencomputer unterstützt,[10] zum Beispiel durch die Verbesserung experimenteller Verfahren oder Methoden.

Auch Anwendungen wie das Risiko- und Portfoliomanagement oder die Preisfindung von Derivaten sind äusserst rechenintensiv. Da im Zeitalter des Echtzeitgeschäfts der Bedarf an Rechenkapazität stetig steigt, ist der Einsatz von leistungsfähigen Rechnern entscheidend, um wettbewerbsfähig zu bleiben. Im Folgenden werden einige der unmittelbar relevanten Anwendungsbereiche von Quantencomputern im Bankensektor vorgestellt.

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 Risikomanagement und -Monitoring

Im Risikomanagement haben Quantencomputer besonders viel Potenzial. Laut dem britischen Branchenverband UK Finance stehen Banken heute vor grossen Herausforderungen bei der Analyse der komplexen Wechselwirkungen zwischen Vermögenswerten und deren Derivaten.[11] Durch den Einsatz von Quantencomputern versprechen sich Banken wie bspw. Goldman Sachs, J.P. Morgan, Citi und HSBC bereits heute schnellere und präzisere Einblicke in sogenannte «Tail Risks». Diese Risiken können, sobald sie mit Hilfe von Quantenalgorithmen identifiziert sind, mit herkömmlichen Computern genauer lokalisiert und begrenzt werden. Auch das Risiko-Reporting an die Aufsichtsbehörden könnte durch die schnellere Identifizierung von Risiken beschleunigt werden.

In der Zukunft könnten Quantencomputer in der Lage sein, einzelne Marktakteure oder ganze Teilmärkte nahezu in Echtzeit zu überwachen und zu analysieren. Da derzeit jedoch noch nicht genügend klassische Daten effizient in Quantencomputer eingelesen werden können, werden mittelfristig Lösungen auf hybriden quantum-klassischen Ansätzen (einschliesslich KI) basieren. Solche Systeme könnten dann die Interdependenzen zwischen Vermögenswerten, Derivaten, Intermediären, Portfoliomanagern und Kunden umfassender analysieren.

Heutige Systeme sind oft nur in der Lage, kaskadenartige Entwicklungen nachzuzeichnen und, abhängig von der Situation, Stopps bei einzelnen Positionen auszulösen. Quantencomputer-basierte Systeme könnten jedoch mit ihrer Fähigkeit, komplexe Muster zu erkennen, Auslöser identifizieren, Ausbreitungs- und Fortpflanzungsmuster verstehen und dabei auch komplizierte Wechselwirkungen erfassen. Sie könnten beispielsweise das Zusammenspiel von Preisbewegungen bei Basiswerten und deren Absicherungsinstrumenten analysieren, inklusive der realen Gegenpartei- und Ausfallrisiken. Während diese Risiken in heutigen Systemen oft nur als Konstanten abgebildet werden und ihre Effekte erst Stunden oder sogar Tage später deutlich werden, könnten Quantencomputer die Dynamik solcher Risiken nahezu in Echtzeit erfassen und so wesentlich schnellere und genauere Entscheidungen ermöglichen.

Weiter zeigen einige Zentralbanken bereits heute Interesse am Monitoring von Zahlungsströmen und sammeln hierzu entsprechende Daten. Die Bank für Internationalen Zahlungsausgleich (BIZ) hat mehrere Forschungsprojekte zu diesem Thema ins Leben gerufen.[12]

2.2 Portfolio-Management

Die Optimierung von Portfolios zählt zu den anspruchsvollsten und rechenintensivsten Aufgaben in der Finanzindustrie. Hier kommt es auf Geschwindigkeit und die gleichzeitige Berücksichtigung zahlreicher Abhängigkeiten an, die ständig im Hinblick auf die Effizienzgrenze der Portfolios neu berechnet werden müssen. Banken arbeiten an der Fähigkeit, Portfolios kontinuierlich zu vergrössern und gleichzeitig Softwarelösungen zu verbessern, um beispielsweise mehrere Portfoliostrategien gleichzeitig zu simulieren. In einigen Märkten wird mithilfe von KI und unter dem Einsatz herkömmlicher Computer bereits heute

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

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

ein Alpha erzielt – also eine Überschussrendite im Vergleich zu einem Benchmark-Index. In Zukunft dürfte der Einsatz von Quantencomputern noch höhere Renditen gegenüber Marktindizes erzielen, da er sich hervorragend mit KI-gestützten Prognosen kombinieren lässt.

2.3 Einfluss auf Verschlüsselungsverfahren und quantensichere Ansätze

Ein besonders wichtiger, aber gleichzeitig risikobehafteter Anwendungsbereich von Quantencomputern liegt in der Verschlüsselung – vor allem, wenn es um das Knacken heutiger Verschlüsselungsverfahren geht. Viele der derzeit in IT-Systemen von Banken verwendeten Verschlüsselungsmethoden sind durch Quantencomputer gefährdet. So bedroht der Shor-Quantenalgorithmus zum Beispiel asymmetrische Verschlüsselungsverfahren wie Rivest-Shamir-Adleman (RSA), da er die Primfaktorzerlegung exponentiell beschleunigen kann. Der Grover-Quantenalgorithmus wirkt sich dagegen auf symmetrische Verfahren wie den Advanced Encryption Standard (AES) aus, indem er die Suche in unsortierten Datenbanken oder Listen quadratisch beschleunigt. Bei symmetrischen Schlüsseln lässt sich diese Schwachstelle zwar durch eine Verdopplung der Schlüssellänge abmildern, aber längere Schlüssel haben wiederum direkte Auswirkungen auf die Laufzeit und Effizienz der Verschlüsselung.

Das weltweit führende National Institute of Standards and Technology (NIST) arbeitet bereits seit 2016 an der Entwicklung quantensicherer Kryptographie. Diese neuen Verfahren sind unter verschiedenen Bezeichnungen bekannt, wie Post-Quantum Cryptography (PQC), Quantum-Proof, Quantum-Safe oder Quantum-Resistant. Im Juli 2022 hat das NIST vier Verfahren veröffentlicht: Crystals-Kyber, Crystals-Dilithium, Sphincs und Falcon. Die ersten dieser Verfahren wurden im Sommer 2024 offiziell standardisiert.[13, 14] Diese Verfahren basieren jedoch auf klassischen kryptographischen Ansätzen, bei denen Quantencomputer – soweit bekannt – keinen Vorteil bieten.

Zusätzlich gibt es Verschlüsselungs-Ansätze, die die Gesetze der Quantenmechanik nutzen und daher sogar mathematisch gegen Entschlüsselungsversuche, selbst durch Quantencomputer, abgesichert sind. In der Praxis sind diese quantenmechanischen Methoden jedoch oft noch weniger weit entwickelt als die quantensicheren klassischen Protokolle. Ein Beispiel hierfür ist der Quantenschlüsselaustausch, bei dem zwei Parteien Zufallszahlen teilen und diese für eine sichere Kommunikation nutzen können, etwa über das One-Time-Pad oder andere Protokolle.[15]

Darüber hinaus wird bereits an der quantensicheren Verschlüsselung bestehender Datenbestände von Finanzdienstleistern und anderen wichtigen Einrichtungen gearbeitet. Damit soll verhindert werden, dass Unbefugte schon heute Daten stehlen, um sie in einigen Jahren mit leistungsstarken Quantencomputern zu entschlüsseln – eine Bedrohung, die im Cyber-Security-Kontext oft als «harvest now, decrypt later»-Angriff bezeichnet wird.

---

13 Eine wichtige Rolle bei der Entwicklung dieser Verfahren spielte im Übrigen das in der Schweiz ansässige IBM-Forschungszentrum in Rüschlikon.

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

15 Ein Schweizer Beispiel in diesem Kontext ist das Unternehmen ID Quantique, das die Kommerzialisierung von Systemen zur Quantenkommunikation (QKD) vorantreibt.

2.4 Algorithmisches Trading

Algorithmisches Trading (kurz: Algo-Trading) ist seit einigen Jahrzehnten eine etablierte Disziplin an der Schnittstelle zwischen Finanzmärkten und ultraschnellen, hochpräzisen High-Tech-Systemen. Die Banken arbeiten dabei mit immer komplexeren Algorithmen, um durch zahlreiche einzelne Transaktionen am Kapitalmarkt Gewinne zu erzielen. In der Praxis ist es dabei jedoch sehr anspruchsvoll, nach Abzug der Kosten regelmässig Gewinne zu erzielen, da Algo-Trading-Systeme häufig gegen andere Systeme mit gegensätzlichen Erwartungen und Voreinstellungen handeln. Zwar schneiden KI-gestützte Systeme in bestimmten Situationen besser ab, aber in Phasen plötzlicher Trendwechsel reagieren sie oft zu langsam auf den Umschwung.

Quantencomputer versprechen in diesem Bereich erhebliche Fortschritte. Ihre erhöhte Rechenleistung ermöglicht es, nicht nur mehrere Märkte gleichzeitig und parallel zu überwachen, sondern auch statt herkömmlicher Monte-Carlo-Simulationen die sogenannte «Amplitude Estimation» zu verwenden. Diese Methode erlaubt präzisere Schätzungen von stochastischen Modellen mit weniger Datenaufwand.

2.5 Bankenspezifische und branchenübergreifende KI

Die meisten Verfahren und Methoden im Bereich der KI lassen sich in nahezu allen Bereichen der zunehmend digitalisierten Industrie anwenden. Die zugrunde liegenden «Large Language Models» (LLMs) können branchenübergreifend auf ähnliche Weise eingesetzt werden. Mit der weiteren Entwicklung der Quantencomputer werden solche KI-Verfahren voraussichtlich in Bezug auf Geschwindigkeit, Genauigkeit, Qualität und Energieeffizienz noch weiter verbessert.

Neben der allgemeinen KI gibt es auch bankenspezifische KI-Lösungen, die auf die besonderen Herausforderungen der Finanzbranche ausgerichtet sind. Hier stehen Themen wie das Risiko- und Portfoliomanagement, entsprechende Simulationen sowie die Ablösung bisheriger Annahmen und Methoden durch präzisere Ansätze im Vordergrund. Auch die Integration zusätzlicher Faktoren und Entwicklungen wird immer wichtiger. Dazu zählen Finanzderivate und die zunehmende Nutzung von Distributed Ledger Technology (DLT) bzw. Blockchain-Technologie, wie sie in der Schweiz beispielsweise im Zusammenhang mit Wholesale-Central Bank Digital Currency (CBDC) oder dem digitalen Schweizerfranken zurzeit erprobt wird.[16, 17]

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

17 Swiss Banking, Schweizer Banken unterzeichnen Absichtserklärung, um die Machbarkeit eines gemeinsam emittierten Schweizer Franken Buchgeld-Tokens zu prüfen (2024)

Zukunftsmusik! Welche weiteren Anwendungen sind in der Finanzbranche denkbar?

Monitoring ganzer Finanzmärkte und tiefere Einblicke in die Realwirtschaft

Spätestens wenn Banken an den Märkten unter Einbezug von Quantencomputern investieren, könnte es sich anbieten, die Märkte in ebenso grosser Breite und Tiefe zu überwachen, um Krisen rechtzeitig entgegenwirken zu können. Die bisher punktuelle Beobachtung einzelner Teilmärkte oder bestimmter Zahlungsströme würde dann nicht mehr ausreichen, da diese schon heute nur ein unzureichendes Bild der tatsächlichen Verhältnisse liefert.

Das Monitoring ganzer Finanzmärkte dient nicht nur dazu, risikobehaftete Entwicklungen frühzeitig zu erkennen. Es ermöglicht auch neue Einblicke für Wissenschaft und Behörden in die Funktionsweise der Finanzmärkte und der Realwirtschaft sowie in Themen wie das Aufkommen und Abklingen von inflationären Tendenzen, die zwar gut beschrieben, aber empirisch wenig untersucht sind.

Klima, Nachhaltigkeit, Naturkatastrophen und die daraus entstehenden finanziellen Risiken

Erst- und Rückversicherungen sind oft die ersten Unternehmen, die die Folgen des Klimawandels direkt in ihrem operativen Geschäft und in ihren Bilanzen spüren. Banken und private Investoren folgen ihnen jedoch rasch – teilweise sogar gleichzeitig. Sie stehen vor der Entscheidung, Immobilien in gefährdeten Gebieten entweder teuer abzusichern oder aufzugeben. Die immer präziseren und umfangreicheren Datenbestände ermöglichen zunehmend genauere Prognosen zu potenziellen zukünftigen Risiken. Wenn sich diese Risiken häufen und sich bei Finanzdienstleistern unerwartet akkumulieren, könnten daraus Kaskadeneffekte für den gesamten Finanzmarkt resultieren.

Quantencomputer können ihre Stärken bei Simulationen und komplexen Bewertungsaufgaben auf verschiedenen Ebenen ausspielen. Zunächst sind sie wertvoll für Wetter- und Klimamodelle und darauf basierende Risikomodelle, die auch geologische und topografische Faktoren einbeziehen. Darüber hinaus eignen sich Quantencomputer zur Bewertung der daraus abgeleiteten Risiken für Privatpersonen und Unternehmen sowie zur Analyse der möglichen Herausforderungen, die sich daraus für einzelne Finanzmarktteilnehmer oder die gesamte Wirtschaft ergeben könnten.

Erste Erfahrungen aus der Branche

Quantum Computing und neue Verschlüsselungsverfahren sind nicht nur für global tätige oder grosse Banken relevant. Auch mittelgrosse und kleinere Institute können von der Kombination aus Quantum Computing und KI profitieren. Das zeigt sich an Beispielen von Finanzinstituten, die sich bereits heute mit dieser Technologie auseinandersetzen und erste Anwendungen entwickeln.

Ausgewählte Beispiele aus der Schweiz

UBS
Die UBS beschäftigt sich seit 2018 mit Quantum Computing. Dafür wurden spezielle Arbeitsgruppen eingerichtet, die gezielt Anwendungen von Quantencomputern untersuchen, um deren Vorteile im Finanzsektor zu quantifizieren und potenzielle Risiken zu identifizieren. Verschiedene Projekte, wie etwa zur Portfolio-Optimierung und zur Bewertung von Finanzderivaten, wurden bereits mit spezialisierten Firmen getestet. Die UBS analysiert mit einer weiteren Arbeitsgruppe die Risiken der Technologie und entwickelt Massnahmen, um ihnen zu begegnen.

Migros Bank
Die Migros Bank hat als Teil ihres Risikomanagements und ihres Fokus auf digitale Innovation ihre «Quantum-Reise» begonnen. In Partnerschaft mit QuantumBasel werden Migros-Bank-Mitarbeitende geschult und Anwendungsfälle für das Quantum Computing evaluiert. Dieses Programm umfasst sowohl das Verständnis und die Minderung von Sicherheitsrisiken, die durch kryptografisch relevante Quanten-algorithmen entstehen, als auch die Erkundung neuen Kundennutzens durch Quantum Computing.

Open Quantum Institute
Das Open Quantum Institute (OQI) ist eine multilaterale Governance-Initiative, die den globalen und inklusiven Zugang zu Quantum Computing sowie die Entwicklung von Anwendungen zum Wohle der Menschheit fördert. Im Rahmen der Wissenschaftsdiplomatie baut das OQI Partnerschaften mit Industrie-anbietern auf, die Kapazitäten auf ihren Quantencomputern für die Entwicklung von Anwendungsfällen zur Erreichung der Ziele für nachhaltige Entwicklung (SDGs) bereitstellen. Das OQI ist eine Kooperation zwischen dem CERN und der Geneva Science and Diplomacy Anticipator Foundation (GESDA), unterstützt von der UBS. Zudem wird die Initiative vom Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) sowie von den Schweizer Hochschulen ETH Zürich und EPFL begleitet.

Swiss Quantum Initiative
Die Swiss Quantum Initiative (SQI) ist die nationale Initiative zur Förderung der Schweizer Forschung und Innovation in den Quantenwissenschaften und wurde 2022 vom Bundesrat gestartet. Für den Zeitraum 2025–2028 stehen der SQI CHF 82,1 Millionen zur Verfügung. Mit wettbewerbsorientierten Ausschrei-bungen sowie durch Wissens- und Technologietransfer soll die internationale Wettbewerbsfähigkeit der Schweiz gestärkt werden.

Ausgewählte Beispiele aus dem Ausland

J.P. Morgan

Die US-Grossbank arbeitet seit einigen Jahren an eigenen Forschungsprojekten im Bereich Quantum Computing.[18] Diese Projekte umfassen Themen wie IT-Sicherheit, verbesserte Datenverschlüsselung und optimiertes Hedging an den Finanzmärkten. Die Bank gibt an, dass ihr Ziel darin besteht, Quantum-Computing-Lösungen in den für die Bank relevanten Bereichen zu etablieren, um die Vorteile dieser Technologien vor den Mitbewerbern zu nutzen.[19] Dabei werden auch Verbindungen zur Blockchain-Technologie untersucht, die auf Verschlüsselung basiert und im Interbanken-Bereich zunehmend an Bedeutung gewinnt.

HSBC

Die global agierende britische Grossbank hat sich im Bereich Quantentechnologie drei Ziele gesetzt.[20] Sie arbeitet mit Partnern wie IBM, Fujitsu und Quantinuum zusammen, um eine führende Rolle in der Finanzindustrie einzunehmen und herauszufinden, wie Quantum Computing in Produkte und Dienstleistungen integriert werden kann. Zudem hat die Bank ein eigenes Team von Fachleuten aufgebaut, das weitere Forschung betreibt, Produkte entwickelt und eigene Innovationen patentieren soll. Darüber hinaus strebt die Bank an, in allen Geschäftsbereichen praktische Anwendungsfälle zu entwickeln, um sich auf die quantensichere digitale Wirtschaft vorzubereiten. Als konkrete Beispiele nennt HSBC die Optimierung des Pricings (zum Beispiel bei Finanzderivaten), die Optimierung von Sicherheiten (da unnötige Sicherheiten teuer sind) und Verbesserungen bei Monte-Carlo-Simulationen für Prognosen und Simulationen in stochastischen Modellen.

Bank for International Settlement (BIS)

Die Organisation arbeitet im Rahmen des Projekts «Leap» an Themen wie quantensichere Finanzsysteme und Finanzmarktstabilität. Ziel ist es, die beteiligten Notenbanken darauf vorzubereiten, rechtzeitig auf kommende Entwicklungen reagieren zu können.[21] Zu den beteiligten Institutionen gehören unter anderem die Banque de France und die Deutsche 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 Folgerungen und Handlungsempfehlungen

3.1 Für die Schweizer Banken

Auch wenn Quantum Computing noch in den Kinderschuhen steckt, erfordert es bereits heute konkrete Schritte von Banken. Die Technologie zum jetzigen Zeitpunkt zu ignorieren oder nur passiv zu beobachten, birgt verschiedene Risiken. Dazu gehören Datendiebstahl durch «harvest now, decrypt later»-Angriffe, der Wettlauf um knappe Quantum-Talente (ähnlich wie bei der Entwicklung der KI) und die Gefahr, von Wettbewerbern langfristig verdrängt zu werden, die neue oder verbesserte Geschäftsmodelle auf der Grundlage von Quantenalgorithmen entwickeln. Die Zahl der Patente im Bereich Quantum Computing, auch im Finanzsektor, wächst kontinuierlich und verstärkt damit den Innovationsdruck.[22, 23, 24]

Bei allen nötigen offensiven und defensiven Sicherheitsmassnahmen im Hinblick auf Quantum Computing ist der Faktor Zeit entscheidend. Auch wenn heute noch unklar ist, ab welchem Zeitpunkt viele der heute gängigen Verschlüsselungsverfahren gefährdet sein könnten, besteht bereits zum jetzigen Zeitpunkt Handlungsbedarf. Es wird Jahre dauern, bestehende IT-Architekturen in Banken anzupassen, Post-Quantum-Kryptographie einzuführen und Sicherheitsprotokolle zu ersetzen. In Kombination mit weiteren Technologien wie KI und DLT hat Quantum Computing mittel- bis langfristig das Potenzial, die Kosten- und Risikostrukturen sowie das Produkt- und Dienstleistungsangebot einer Bank wesentlich zu beeinflussen.

Um diese Chancen zu nutzen und Risiken frühzeitig zu identifizieren, zu mindern oder ganz zu vermeiden, haben die Autoren aus der gemeinsamen Expertengruppe von SBVg und QuantumBasel die folgenden Handlungsempfehlungen für Banken erarbeitet:

- **Ist-Landschaft analysieren und überwachen:** Quantum Computing und quantensichere Kryptographie entwickeln sich schnell. Banken sollten den Fortschritt dieser Technologien kontinuierlich verfolgen und ihre aktuelle IT-Landschaft – einschliesslich Applikationen, Netzwerke, Partnerkommunikation und Sicherheitskomponenten – auf potenzielle Schwachstellen hin analysieren.
- **Klassifizieren und Risiken bewerten:** Nicht alle Daten werden in fünf oder zehn Jahren noch schützenswert sein, und nicht alle Daten und Protokolle sind durch Quantenalgorithmen gefährdet. Ein Inventar der vorhandenen Informationen ist nötig, um zu klassifizieren, welche Daten und Verfahren wie stark bedroht sind und welchen langfristigen Wert sie haben. Die kritischsten Informationen sollten priorisiert und die Bedrohungen bewertet werden. Die Ergebnisse können in einer Heatmap visualisiert werden, um die wichtigsten Bedrohungen und Chancen übersichtlich darzustellen.
- **Roadmap erstellen und Migrationen planen:** Auf Basis des Inventars sollten die Architekturpläne angepasst und Migrationen zur quantensicheren Kryptographie geplant werden. Krypto-Agilität ist dabei essenziell, da in Zukunft weitere Migrationen nötig sein könnten, etwa bei der Einführung quantenmechanischer Lösungen wie dem Quantenschlüsselaustausch. Eine Roadmap mit den erforderlichen Handlungsfeldern und Massnahmen bietet dabei die notwendige Orientierung.

---

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)

Um die Reise ins quantensichere Zeitalter effektiv anzugehen, können die folgenden Massnahmen helfen:[25]

- **Sensibilisierung und Schulungen beginnen:** Mitarbeitende und Führungskräfte sollten über die Risiken und Chancen der Quantentechnologie informiert werden. Dies kann durch gezielte Kommunikation und Schulungen geschehen, einschliesslich der Ausbildung von IT-Sicherheits- und Kryptographie-Teams zu den neuesten Algorithmen und Methoden.
- **Sicherheitsvorgaben aktualisieren:** Eine kontinuierliche Überarbeitung der bestehenden Sicherheitsrichtlinien und Prozesse ist notwendig, um neue quantensichere Algorithmen zu integrieren. Dazu gehört auch die Definition eines Zielbilds und die Entwicklung einer langfristigen Strategie, die die benötigten Fähigkeiten und Technologien im Bereich Quantensicherheit festlegt.
- **Lieferanten und Partner überprüfen:** Banken sollten die quantensicheren Massnahmen ihrer Lieferanten und Partner bewerten, um sicherzustellen, dass diese auf einem angemessenen Stand sind.

Darüber hinaus sollten Banken auch die Chancen erkennen und folgende Massnahmen verfolgen:

- **Zusammenarbeit mit spezialisierten Organisationen suchen:** Banken sollten für die experimentelle Phase die Zusammenarbeit mit spezialisierten Unternehmen und Organisationen suchen, um Erfahrungen zu sammeln und gemeinsame Frameworks und Vorgehensweisen zu entwickeln.
- **Cloud-basierte Nutzung von Quantum Computing fördern:** Ähnlich wie bei grossen KI-Anwendungen wird Quantum Computing mittelfristig vor allem über eine Cloudinfrastruktur zugänglich sein. Banken sollten sich daher auch intensiv mit ihrer «Cloud-readiness» befassen.[26]

3.2 Für die Behörden

Aufgrund der technologieneutralen und prinzipienbasierten Schweizer Regulierung dürfte der rechtliche und regulatorische Anpassungsbedarf im Hinblick auf Quantum Computing vorerst begrenzt sein. Für die Aufsicht und Regulierung von Quantum Computing gelten in der Schweiz grundsätzlich die gleichen Prinzipien wie bei anderen neuen Technologien: Technologieneutralität, Verhältnismässigkeit, der Schutz der Reputation des Finanzplatzes und Rechtssicherheit.

Um den tatsächlichen Anpassungsbedarf festzustellen, sollte zunächst eine Analyse der aktuellen Rahmenbedingungen in Bezug auf die erwartete Nutzung von Quantum Computing durchgeführt werden. Dadurch könnte punktueller Anpassungsbedarf erkennbar werden. Mit zunehmender Erfahrung liessen sich weitere Lücken identifizieren, die dann zu gegebener Zeit adressiert werden können. Im regulatorischen Kontext lässt sich Quantum Computing aus unserer Sicht grob in zwei Bereiche unterteilen: Zum einen sind dies die Sicherheitsaspekte, insbesondere die Post-Quantum-Kryptographie (PQC), und zum anderen die Regulierung neuer Produkte und Dienstleistungen, die durch Quantum Computing erst möglich werden.[27]

---

25 Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet einen ausführlichen Leitfaden für die Einführung von PQC: Kryptografie quantensicher gestalten – Grundlagen, Entwicklungen, Empfehlungen.

26 Als Wegweiser für sicheres Cloud Banking empfehlen wir den SBVg Cloud-Leitfaden.

27 Die Industrievereinigung für GSM-Mobilfunkanbieter «GSM Association» führt eine Liste über die Initiativen verschiedener Länder im Bereich der Post-Quanten-Kryptografie (PQC).

Der Übergang zur PQC wird alle Sektoren betreffen, nicht nur die Finanzindustrie. Es gibt bereits Vorschriften, die Banken zu Sorgfalt, Datenschutz und Vertraulichkeit verpflichten. Von Banken wird erwartet, dass sie organisatorische und technische Massnahmen ergreifen, um die Daten- und Informationssicherheit zu gewährleisten. Da sich die Sicherheitsanforderungen ständig weiterentwickeln, wird auch erwartet, dass die Banken ihr Sicherheitskonzept ebenfalls kontinuierlich anpassen. Regulierungsbehörden wie die Eidgenössische Finanzmarktaufsicht (FINMA) überwachen die Umsetzung dieser Massnahmen im Rahmen ihrer Aufsichtstätigkeit.[28]

Während die potenziellen Auswirkungen von Quantum Computing auf die Cybersicherheit bereits recht konkret sind, sind die Implikationen aus der Anwendung von Quantencomputern im Geschäftsalltag noch weniger klar (bspw. in Bezug auf den Datenschutz). Ein regelmässiger Dialog zwischen der Industrie und den Regulatoren bleibt daher zentral, um Erfahrungen auszutauschen und frühzeitig potenziellen Handlungsbedarf zu erkennen.

Die wachsende Bedeutung von Quantum Computing zeigt sich auch in nationalen und geopolitischen Initiativen. Die G7 haben im September 2024 in Rom einen Workshop abgehalten, um den Aufbau eines quantensicheren Finanzsystems zu diskutieren und die Rollen von Regulierungsbehörden und privaten Akteuren zu evaluieren. In ihrer Abschlussmitteilung ermutigen die G7 die Finanzaufsichtsbehörden, eng mit Unternehmen und anderen relevanten Parteien zusammenzuarbeiten, um das Bewusstsein für den Übergang zu quantenresistenten Technologien zu schärfen.[29] In der Schweiz gibt es für diesen übergreifenden Austausch bereits das Open Quantum Institute, das Quantum Economy Network des WEF und die Swiss Quantum Initiative.[30, 31, 32] Diese Beispiele verdeutlichen das Interesse der Politik und die Bedeutung von Partnerschaften im Kontext von Quantum Computing.

3.3 Für den Schweizer Finanzplatz

Um die Wettbewerbsfähigkeit des Schweizer Finanzplatzes mittel- und langfristig zu sichern, ist der Einsatz neuer Technologien zur Verbesserung von Produkten und Dienstleistungen im globalen Wettbewerb unerlässlich. Dabei spielt Quantum Computing zusammen mit Technologien wie KI und DLT eine entscheidende Rolle. Es ist zu erwarten, dass die Faktoren, die die Wettbewerbsfähigkeit einzelner Banken sichern, auch zur Stärkung des gesamten Finanzplatzes beitragen. Für den Schweizer Finanzplatz ist es daher sehr zu begrüssen, dass an Schweizer Universitäten und Forschungseinrichtungen sowohl Grundlagen- als auch Anwendungsforschung betrieben wird. Kurze Wege, schnelle formelle und informelle Kommunikationskanäle, das hohe fachliche Niveau der Beteiligten sowie deren Bereitschaft zur Anpassung und Veränderung schaffen eine solide Grundlage für die erfolgreiche Nutzung dieser neuen Technologie.

28 Die Europäische Kommission hat im April 2024 EU-Mitgliedstaaten empfohlen, eine gemeinsame Roadmap für die Umstellung auf Post-Quanten-Kryptografie (PQC) zu entwickeln. Ziel ist es, den öffentlichen Sektor und kritische Infrastrukturen im EU-Raum koordiniert auf quantensichere Kryptographie umzustellen.

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 Fazit

Die Entwicklungen im Bereich Quantum Computing stellen für den Schweizer Finanzsektor sowohl Chancen als auch Herausforderungen dar. Mit ihrer Fähigkeit, komplexe Berechnungen und Simulationen effizienter und präziser durchzuführen, eröffnen Quantencomputer neue Anwendungsmöglichkeiten, beispielsweise im Risikomanagement und in der Portfoliooptimierung. Gleichzeitig müssen heutige Sicherheitsprotokolle mit quantensicherer Kryptographie verbessert werden. Die damit einhergehenden technologischen Anforderungen sind nicht zu unterschätzen, und die Finanzinstitute sollten daher bereits heute die Weichen für den künftigen Einsatz richtig stellen, um auf diese Veränderungen vorbereitet zu sein.

Um den Weg in eine quantensichere Zukunft zu ebnen, ist es unerlässlich, frühzeitig in die eigene «Quantum Readiness» zu investieren. Durch gezielte Förderung der eigenen Fähigkeiten sowie durch Zusammenarbeit mit spezialisierten Organisationen können sich Banken nachhaltig Wettbewerbsvorteile sichern und gleichzeitig die mit Quantum Computing verbundenen Risiken minimieren. Diese Investitionen sind nicht nur ein Bekenntnis zur Innovation, sondern auch ein wichtiger Schritt zur nachhaltigen Stärkung der Resilienz des gesamten Schweizer Finanzplatzes.

«Quantum Readiness ist nicht nur ein Bekenntnis zur Innovation, sondern auch ein wichtiger Schritt zur nachhaltigen Stärkung der Resilienz des Schweizer Finanzplatzes.»

Die Empfehlungen dieses Berichts bieten eine erste Grundlage, um sich dem Thema anzunähern und diesen Wandel erfolgreich zu gestalten. Weitere Analysen zu den Chancen, aber auch zu den Risiken des Quantum Computings werden notwendig sein, sobald die Technologie in der Finanzindustrie und anderen Sektoren breitere Anwendung findet. Gleichzeitig muss der aktive Dialog zwischen der Branche und den Behörden gepflegt und gefördert werden, um die Entwicklungen in diesem Bereich laufend zu beobachten und Handlungsbedarf frühzeitig zu erkennen. Die Zusammenarbeit der Branche mit führenden Forschungseinrichtungen und Unternehmen in diesem Bereich stimmt auf jeden Fall optimistisch, dass sich die Schweiz auf einem guten Weg befindet, eine führende Rolle im Bereich der Quantentechnologie einzunehmen.

Glossar

Algorithmus: Eine endliche Abfolge von Anweisungen zur Lösung eines spezifischen Problems oder zur Ausführung einer Aufgabe. In der Quanteninformatik gibt es spezielle Algorithmen, wie den Shor- und den Grover-Algorithmus, die Quantenmechanik nutzen, um bestimmte Berechnungen schneller durchzuführen als klassische Algorithmen.

Dekohärenz: Der Zerfall des Quantenverhaltens eines Qubits, wenn es mit seiner Umgebung interagiert, was zu Informationsverlust führt. Dekohärenz ist eine der grössten Herausforderungen für Quantencomputer.

Fehlerkorrektur: Da Quantencomputer anfällig für Fehler sind, erfordern sie komplexe Fehlerkorrekturmethoden, um stabile Berechnungen zu ermöglichen.

Grover-Algorithmus: Ein Quantenalgorithmus, der bei der Suche in unsortierten Datenbanken quadratische Geschwindigkeitsvorteile gegenüber klassischen Algorithmen bietet. Er kann die Sicherheit von symmetrischen Verschlüsselungsverfahren beeinträchtigen.

Krypto-Agilität: Die Fähigkeit, schnell auf neue kryptografische Bedrohungen zu reagieren, indem Kryptosysteme flexibel auf neue Standards und Algorithmen umgestellt werden.

Noisy Intermediate-Scale Quantum (NISQ): Eine Klasse von Quantencomputern, die derzeit verfügbar ist und begrenzte Leistung bietet. Diese Systeme sind noch anfällig für Fehler und haben eine geringe Anzahl von Qubits, können aber bereits spezifische Probleme schneller lösen als klassische Computer.

One-Time Pad (OTP): Ein Verschlüsselungsverfahren, das bei korrekter Anwendung theoretisch nicht zu knacken ist. Ein One-Time Pad verwendet einen zufälligen Schlüssel, der genauso lang ist wie die Nachricht selbst. Dieser Schlüssel wird nur einmalig genutzt und danach verworfen, was das Verfahren gegen alle kryptografischen Angriffe immun macht, solange der Schlüssel geheim und wirklich zufällig ist. Die sichere Übertragung des Schlüssels ist erforderlich, was die praktische Umsetzung erschwert.

Post-Quantum Cryptography (PQC): Eine neue Generation von kryptografischen Algorithmen, die resistent gegen Angriffe durch Quantencomputer sind. NIST hat bereits drei dieser Verfahren standardisiert.

Qubit: Die grundlegende Informationseinheit eines Quantumcomputers. Im Gegensatz zu klassischen Bits, die entweder 0 oder 1 annehmen können, können Qubits dank Überlagerung gleichzeitig beide Zustände annehmen.

Quantengatter: Quantengatter sind die grundlegenden Bausteine eines Quantumcomputers. Sie manipulieren Qubits, um Berechnungen auszuführen, und ermöglichen durch Quantenphänomene wie Überlagerung und Verschränkung parallele Zustände. Im Gegensatz zu klassischen logischen Gattern, die nur mit 0 und 1 arbeiten, können Quantengatter komplexere Operationen effizienter umsetzen.

Quantum Key Distribution (Quantenschlüsselaustausch, QKD): Ein Verfahren, das die Gesetze der Quantenmechanik nutzt, um sichere Kommunikationsschlüssel zwischen zwei Parteien zu teilen. Es ist gegen klassische und Quantenangriffe resistent.

Quantum Random Access Memory (qRAM): Ein Konzept für einen Speicher, der die parallele Verarbeitung grosser Datenmengen in einem Quantencomputer ermöglicht. Es ist eine potenzielle Lösung für die aktuelle Einschränkung der (klassischen) Dateneinspeisung in Quantencomputer.

Shor-Algorithmus: Ein Quantenalgorithmus, der in der Lage ist, die Primfaktorzerlegung grosser Zahlen exponentiell schneller durchzuführen als klassische Algorithmen. Er stellt eine Bedrohung für asymmetrische Verschlüsselungsverfahren wie RSA dar.

Überlagerung (Superposition): Ein quantenmechanisches Phänomen, bei dem ein Qubit gleichzeitig in mehreren klassischen Zuständen (0 und 1) existieren kann. Dies ermöglicht eine massive parallele Verarbeitung in Quantencomputern.

Verschränkung (Entanglement): Ein Zustand, in dem zwei Qubits so miteinander verbunden sind, dass die Änderung des Zustands des einen Qubits sofort den Zustand des anderen beeinflusst, unabhängig von der Entfernung.

Redaktion

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

Experten

QuantumBasel

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

SBVg-Mitgliedsinstitute

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

Über die Schweizerische Bankiervereinigung (SBVg)

Die Schweizerische Bankiervereinigung (SBVg) ist der Spitzenverband des Schweizer Finanzplatzes und vertritt die Interessen von rund 270 Mitgliedsinstituten. Seit 1912 setzt sich die SBVg für optimale Rahmenbedingungen ein, um den Schweizer Bankenplatz wettbewerbsfähig und innovativ zu gestalten. Sie fördert den Dialog mit Politik und Behörden, treibt zentrale Themen wie Sustainable Finance und digitale Währungen voran und unterstützt die Aus- und Weiterbildung in der Branche. Als Wissenszentrum engagiert sie sich für eine nachhaltige Weiterentwicklung des Bankensektors.

swissbanking.ch

Über QuantumBasel

QuantumBasel ist ein Privatunternehmen, welches auf dem Innovationscampus uptownBasel Quantentechnologie und KI nutzt, um zusammen mit Startups, Konzernen und Universitäten nachhaltige Innovationen voranzutreiben. Mit einem globalen Technologie-Ökosystem, das Forschung und Expertenwissen vereint, fördert QuantumBasel den Übergang von Quantum Computing von der Forschung zur industriellen Anwendung. Ende 2024 wird auf dem Campus der erste, kommerziell nutzbare Quantencomputer der Schweiz in Betrieb genommen.

quantumbasel.com

Schweizerische
Bankiervereinigung
Aeschenplatz 7
Postfach 4182
CH-4002 Basel
office@sba.ch
www.swissbanking.ch