Quantenrechner für Finanzdienstleister?

Qubits-Computing vor der Marktreife

Mit einem völlig neuen Architekturansatz stellt der Quantenrechner eine komplett andere Art von Computing bereit. Finanzdienstleister werden von der Schnelligkeit der Quantenalgorithmen profitieren. Beispielsweise werden Berechnungen zur Preisentwicklung in der Finanzmathematik über klassische und schwer zu lösende Differentialgleichungen abgebildet, welche auf einem Quantencomputer dann auf Quantenalgorithmen adaptiert werden. Der Beitrag geht der Frage nach, was diese Rechner so einzigartig macht. (Red.)

Die Finanzindustrie steht aktuell vor großen Herausforderungen: durch künstliche Intelligenz (KI) getriebene Automation, auf Cloud-Lösungen basierende neue Geschäftsarchitekturen, Aufwendungen für Cybersecurity, der auf den Instituten lastende Kostendruck und vieles mehr.[1] Zusätzlich zeichnet sich am Horizont bereits das postklassische Computing ab.

Finanzunternehmen sind also aufgerufen, sich schon jetzt mit dem Paradigmenwechsel zum Quantencomputer auseinanderzusetzen, damit sie Vorreiter in der technischen Entwicklung – und bei ihrer Konkurrenz – sind. Im klassischen Computer werden Bits verarbeitet, diese können nur einen der zwei Werte 0 und 1 annehmen. Dieser Wert ist eindeutig definiert und eine Messung davon ändert den Wert nicht.

Neue Technologie

Ein Quantenbit, abgekürzt Qubit, ist ein Objekt mit quantenmechanischen Eigenschaften. Zum einen kann das Qubit auch die zwei Werte 0 und 1 annehmen, zusätzlich aber auch alle Werte dazwischen – dies ist die sogenannte Superposition. Erst eine Messung des Quantenbits liefert das Ergebnis 0 oder 1. Mit zwei klassischen Bits kann nur einer der Zustände 00, 01, 10 oder 11 zu einem Zeitpunkt dargestellt werden, zwei Qubits stellen durch das Superpositionsprinzip alle vier Zustände mit bestimmten Wahrscheinlichkeiten gleichzeitig dar. Mit drei Qubits erreicht man schon acht Zustände und so weiter. Die Zahl der Zustände steigt also exponentiell an und alle werden parallel verarbeitet.

Hinzu kommt das Phänomen der Quantenverschränkung: Zwei Qubits, die miteinander verschränkt sind, bilden dann ein 2-Qubit-Zustand, der sich nicht mehr in die unbestimmten 1-Qubit Zustände zerlegen läßt. Der Gesamtzustand über diese beiden Qubits ist nicht mehr unbestimmt, somit lässt sich durch die Messung eines dieser Qubits unmittelbar der Zustand des anderen Qubits bestimmen. Damit wird die Verschränkung – Albert Einstein sprach von "spukhafter Fernwirkung" –, da die Informationsübertragung sofort erfolgt, zum Gamechanger im postklassischem Computing.[2]

Qubits sind künstlich hergestellte Zwei-Level-Quantensysteme, die sich auf unterschiedliche Arten erzeugen lassen, zum Beispiel durch Ionenfallen (etwa bei den Anbietern Honeywell und IonQ) oder supraleitenden Transmonqubits (IBM, Google und andere). Die derzeit verfügbaren Quantencomputer interagieren zwar schon mit einer hohen zweistelligen Zahl von Qubits, allerdings reichen die Skalierbarkeit an Qubits und deren noch hohen Fehlerraten nicht aus, Probleme von geschäftsrelevanter Größenordnung zu berechnen. Die Verbesserungen der Quantensysteme ist Thema der aktuellen Forschung.[3]

Ein Quantenrechner arbeitet mit Logikgattern, die Quantengatter heißen und physikalische Manipulationen (zum Beispiel durch Mikrowellenpulse) am Qubit repräsentieren. Die wesentlichen sind das Hadamard-Gatter, welches eine Su-

DR. AXEL SAUERLAND

ist Leiter Service Finanzierungen, IBM Global Financing Deutschland GmbH, Düsseldorf. Er verantwortet die Finanzierungsaspekte in der Schnittstelle zur IBM Beratungssparte.

E-Mail:
axel.sauerland@de.ibm.com

DR. STEFAN KISTER

ist Senior Client Technical Architect und Senior Quantum Ambassador im technischen Vertrieb, IBM Deutschland GmbH, Düsseldorf. Schwerpunkt ist die Beratung von Kunden aus dem Finanzsektor.

E-Mail:
dr.stefan.kister@de.ibm.com

perpostion erzeugt, und das Controlled-NOT-(C-NOT)-Gatter, welches zwei Qubits verschränkt und das Zielqubit invertiert, wenn das Controllqubit den Wert 1 hat. Wie beim klassischen Computer fasst man mehrere Qubits zu Quantenregistern zusammen. Der quantenmechanische Zustand der Qubits ist durch äußere Einflüsse (maßgeblich Temperatur) labil. Somit müssen die Operationen an den Qubits innerhalb eines Zeitfensters durchgeführt werden, in dem der Zustand noch als kohärent gilt. Es ist Teil der Forschung, die Dekohärenz, also das Zurückfallen in einen klassischen Zustand, möglichst lange hinauszuzögern, damit Quantenalgorithmen mit vielen oder zeitaufwendigen Operationen ablaufen können.

Anwendungsfälle für Finanzunternehmen

Es lassen sich außerhalb von naturwissenschaftlichen Simulationen aktuell drei wesentliche Kategorien von Anwendungsbereichen festhalten, in denen Quantencomputer in der Zukunft einen möglichen Vorteil gegenüber den heutigen klassischen Verfahren erzielen können: kombinatorische Optimierung, Szenariosimulation und maschinelles Lernen. In allen Bereichen gibt es schon wissenschaftliche Untersuchungen auf Basis illustrativer Fälle im Finanzsektor, zum Beispiel Portfoliooptimierung, Risikoanalyse und Betrugsaufdeckung,[4] was an folgenden Beispielen verdeutlicht werden soll:

Finanzdienstleister betrachten sehr häufig kombinatorische Optimierungsprobleme im Handel und im Portfoliomanagement. Da diese exponentiell skalieren, wird Quantencomputern das Potenzial zugeschrieben, in Zukunft schneller genügend gute Lösungen als klassische Rechner zu finden. Die Datenmodellierungsfähigkeiten von Quantencomputern könnten auch dazu genutzt werden, Muster zu finden und damit Wirtschaftskriminalität wie Betrugserkennung oder Geldwäsche wirksamer vorzubeugen. Eine Aufgabe, die heute aufgrund der Herausforderungen komplexer Datenstrukturen oft in angemessener Zeit so nicht möglich ist. Im Wertpapierhandel werden Szenarien und Investitionsoptionen zur Abschätzung der erwarteten Renditen simuliert. Für das Rebalancing des Anlageportfolios könnten Quantenrechner noch genauere Ergebnisse zur Entscheidungsunterstützung liefern.

Schlussendlich: Die immer größer werdenden regulatorischen Anforderungen (Basel III und IV) erfordern eine breite Palette von Stresstests. Die heute verwendeten Monte-Carlo-Simulationen, also die bevorzugte Technik zur Analyse der Auswirkungen von Risiko und Unsicherheit in Finanzmodellen, gelangen durch zunehmenden Umfang und die steigende Komplexität der Modelle auf klassischen Computern schnell an ihre Grenzen. Quantenrechner könnten in Zukunft die Simulation von Risikoszenarien mit einem größeren Assetvolumen schneller und mit höherer Präzision ermöglichen.

Was bringt die Zukunft?

Quantencomputer-Technologie wird für all die Bereiche eingesetzt werden, die enorme Datenmengen und komplexe Modelle verarbeiten, also auch in der Finanzindustrie. Die Entwicklung geht einerseits in die Erhöhung der Anzahl von Qubits – damit steigt die Rechenleistung exponentiell an – und andererseits in einen universellen, fehlerfreien Quantenrechner, der über APIs an die klassischen Systeme angebunden ist. Als Kenngröße der Leistungsfähigkeit eines Quantenrechners ist aber nicht nur die reine Anzahl der verbauten Qubits wichtig, sondern all umfassend die Qualität des gesamten quantenphysikalischen Systems hinsichtlich Fehlerkorrekturmöglichkeit, Kohärenzzeit, Konnektivität, Leistung von Compilern und dem Software-Stack. Zur Beurteilung dessen werden dazu hardwareagnostische Metriken eingeführt, wie etwa das Quantenvolumen. Ziel aller Entwicklungen ist es, den sogenannten Quantenvorteil (quantum advantage) beziehungsweise die Quantenüberlegenheit (quantum supremacy) eines Quantencomputers gegenüber einem herkömmlichen Supercomputer in ausgewählten Problemfällen nachzuweisen.

Neben den Vorteilen, die sich durch den Einsatz von Quantencomputern in der Zukunft ergeben können, stellt ein leistungsfähiger und fehlertoleranter Quantencomputer aber auch eine Gefahr für aktuelle Verschlüsselungsverfahren dar, die auf Basis der Faktorisierung arbeiten.[5] Es gibt schon aktuelle auf klassischen, mathematischen Verfahren basierende Forschungsarbeiten, die als Quantum-safe eingeordnet werden. Eine abschließende Zertifizierung durch das National Institute of Standards and Technology liegt aber noch nicht vor. Trotzdem ist eine Analyse der Umgebung schon heute wichtig und die Vorbereitung durch einen kryptoagilen Ansatz sehr ratsam.

Der Fortschritt der Quantencomputer-Technologie bietet zukünftig also auch für die Finanzdienstleistungsbranche ein hohes Potenzial. Sowohl die Herangehensweise, Probleme auf dem Quantencomputer abzubilden, als auch Programmierung und Integration in bestehende IT-Systemen unterscheiden sich jedoch deutlich von bekannten Konzepten. Daher ist ein früher Einstieg in die Thematik essenziell für den Aufbau der richtigen Fähigkeiten und geistigen Eigentums in Quantencomputing-Technologie.

Fußnoten

1) Siehe ergänzend Axel Sauerland, Die digitale Zukunft der Finanzdienstleister - Entwicklungen und Trends im Bereich Technologie, in: FLF 3/2021, S. 146 ff.

2) Ein Quantenbit ist die elementare Einheit der Quanteninformation. Zu den Begründern der Quantentheorie gehört neben Max Planck, Werner Heisenberg, Erwin Schrödinger und vielen weiteren auch Albert Einstein. Den Physik-Nobelpreis bekam er für seine Lichtquantenhypothese, aber nicht für seine bahnbrechenden Arbeiten zur Relativität.

3) Am IBM Standort Ehningen ist 2021 ein Kompetenznetzwerk als offene Forschungsplattform rund um den Quantencomputer IBM Q System One mit 27 Qubits für die Fraunhofer-Gesellschaft und ihre Partner installiert worden. Dies ordnet sich ein in die kürzlich vorgestellte Quanten-Roadmap von IBM: Im Jahr 2023 soll ein 1 121 Qubits umfassender Quantenprozessor namens Condor vorgestellt werden, der dann für einen breiten Einsatz in der Wirtschaft bereitstehen wird.

4) Siehe ausführlich den Forschungsbericht des Institute for Business Value IBV: Exploring quantum computing use cases for financial services.

5) Nach der Position des Bankenverbandes sind die kryptographischen Verfahren der Kreditwirtschaft im Online-Banking, Prozesse bei Geldzahlungen und auch Blockchaintechnologien betroffen, siehe https://bankenverband.de/themen/quantencomputer-bei-banken/