RAIFFEISEN

Raiffeisen Schweiz
Raiffeisen Economic Research
economic-research@raiffeisen.ch

30.10.2024

Die Sicht des Raiffeisen Chefökonomen

Ein Quantum Trost

«Ein Quantum Trost», im Original «Quantum of Solace», ist der Titel des James-Bond-Films von Marc Forster, der Ende 2008 in die Kinos kam, und der zweite Bond-Film mit dem britischen Darsteller Daniel Craig in der Hauptrolle. Der Film sollte ursprünglich «Ein Minimum an Trost» heissen, wurde später aber abgeändert, um die Verbindung zur Geheimorganisation zu betonen, die Bond im Film bekämpft. Etwas Trost bleibt auch, wenn wir uns mit Quantencomputing beschäftigen. Während momentan alles von der künstlichen Intelligenz spricht, dürfte schon bald Quantencomputing «the next big thing» sein. Eine vielversprechende Technologie, die sich in rasantem Tempo entwickelt, aber auch bereits Schatten auf das Hier und Jetzt wirft.

Wie funktionieren Quantencomputer?

Quantencomputer arbeiten mit sogenannten Quantenbits, auch Qubits genannt. Diese können nicht nur die Zustände 0 und 1 gleichzeitig annehmen, sondern auch jeden Zustand dazwischen. Diese Fähigkeit, «Superposition» genannt, erlaubt es dem Quantencomputer, eine Vielzahl von Berechnungen gleichzeitig durchzuführen. Darüber hinaus ist es möglich, dass Qubits aufgrund des Prinzips der «Verschränkung» über weite Distanzen miteinander in Verbindung bleiben. Diese beiden Eigenschaften verleihen dem Quantencomputer das Potenzial, Probleme zu lösen, die für klassische Computer unlösbar oder nur mit gigantischem Aufwand zu bewältigen sind.

Gängige Verschlüsselungsverfahren werden nutzlos

Dies führt zu einer der grössten Sorgen: der Datensicherheit. Da Quantencomputer ein viel höheres Leistungsvermögen als herkömmliche Superrechner haben, werden alle derzeit geläufigen Verfahren zur Datenverschlüsselung nicht mehr genügen. Der Algorithmus, um die heutigen Verschlüsselungsmethoden zu knacken, liegt bereits vor. Es fehlt nur noch ein hinreichend leistungsfähiger Rechner, der ihn ausführen kann. Der Q-Day, der Tag, an dem die Quantencomputer diese Schwelle erreichen, liegt allerdings noch einige Jahre in der Zukunft. Dennoch resultiert daraus schon heute ein erheblicher Handlungsbedarf.

Dringender Handlungsbedarf

Die Datensicherheit ist ein zentraler Pfeiler unserer Welt und die Verschlüsselung ist allgegenwärtig. Das Aufrufen einer sicheren Website oder die Überweisung eines Geldbetrages läuft verschlüsselt ab. Ohne Schutz sensibler Informationen würde das Vertrauen in das weltweite Finanzsystem zusammenbrechen. Oder die Steuerung kritischer nationaler Infrastrukturen wäre ohne Verschlüsselungsschutz dem Zugriff dunkler Mächte ausgesetzt. Ein Albtraum. Auch für das geistige Eigentum und die Unternehmensgeheimnisse vieler Unternehmen. Bereits heute stehlen und speichern Kriminelle und Schurkenstaaten verschlüsselte Daten, um sie in ein paar Jahren mit einem Quantencomputer zu entschlüsseln. Man bezeichnet diese Strategie auch als «harvest now, decrypt later». Es ist also höchste Zeit, auf ein besseres Verschlüsselungsverfahren umzustellen. Forscher weltweit arbeiten bereits an «post-quantum» oder «quantenresistenten» Verschlüsselungsmethoden, die gegen die Rechenleistung von Quantencomputern resistent sind.

Kleiner Trost

Immerhin besteht ein kleiner Trost darin, dass wir gemäss Experten noch rund zehn Jahre von der Quantenrevolution entfernt sind und somit noch etwas Zeit bleibt. Nützliche Berechnungen durch Quantencomputer benötigen eine riesige Zahl von Qubits. Der aktuell grösste Quantencomputer von Atom Computing hat deren 1180. Das Knacken einer Verschlüsselung, die auf dem neuesten Stand ist, würde gemäss Craig Gidney, Wissenschaftler bei Google, 20 Millionen Qubits erfordern. Hinzu kommt das Problem, dass die Quantenbits fehleranfällig sind. Thermische Vibrationen, kosmische Strahlen, elektromagnetische Interferenzen oder anderweitige Störungen können pro hundert bis zehntausend Operationen einen Fehler verursachen. Mit einer solchen Fehlerrate können

Raiffeisen Schweiz
Raiffeisen Economic Research
economic-research@raiffeisen.ch

30.10.2024

Die Sicht des Raiffeisen Chefökonomen

Ein Quantum Trost

komplexe Aufgaben nicht gelöst werden, die Millionen von Rechenschritten benötigen. Doch auch auf diesem Feld geht die Entwicklung rasch voran. Forschenden von Google ist es neulich gelungen, die Fehlerrate stark zu senken, indem sie mehrere Quantenbits schachbrettartig zu einem logischen Quantenbit gruppiert haben, wodurch sich Fehler erkennen und korrigieren lassen.

Es ist faszinierend, die Entwicklung der Quantencomputing-Technologie mitzuverfolgen. Sie birgt enormes wirtschaftliches Potenzial. Anwendungen sind beispielsweise denkbar in den Bereichen Risikomanagement, Optimierung von Logistikprozessen sowie Entdeckung neuer Materialen und chemischer Prozesse, die inskünftig auch bahnbrechende neue Medikamente und damit das Ausmerzen gewisser Krankheiten erwarten lassen. Doch die Quantencomputer erinnern uns auch daran, wie fragil unsere Welt geworden ist. Im Juli kam es beispielsweise zum grössten IT-Systemausfall aller Zeiten, für welchen die Sicherheitssoftwarefirma Crowdstrike verantwortlich war. Ein fehlerhaftes Update legte weltweit Flughäfen, Spitäler und Medienunternehmen lahm. In der realen Welt schützen mechanische Schlösser Wertvolles. Ein Schloss kann mit entsprechendem Aufwand aufgebrochen werden, aber nicht gleichzeitig alle Schlösser. Doch mit der Ankunft der Quantencomputer können auf einen Schlag die seit Jahrzehnten eingesetzten digitalen Schlösser geöffnet werden, wenn wir sie nicht schleunigst austauschen. Vielleicht ist auch das mit ein Grund, weshalb der Preis von Gold laufend neue Rekordmarken erreicht.

Fredy Hasenmaile,
Chefökonom Raiffeisen Schweiz

RAIFFEISEN

Raiffeisen Schweiz
Raiffeisen Economic Research
economic-research@raiffeisen.ch

30.10.2024

Die Sicht des Raiffeisen Chefökonomen

Ein Quantum Trost