ÖFIT-Trendschau

Bibliographische Angaben

Öffentliche Informationstechnologie in der digitalisierten Gesellschaft

Trendthema 61

Quantencomputing

Herausgeber:

Kompetenzzentrum Öffentliche IT
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut FOKUS
Kaiserin-Augusta-Allee 31, D-10589 Berlin
Telefon: +49 30 3463 - 7173
Telefax: + 49 30 3463 - 99 - 7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

Autorinnen und Autoren der Gesamtausgabe: Mike Weber, Stephan Gauch, Faruch Amini, Tristan Kaiser, Jens Tiemann, Carsten Schmoll, Lutz Henckel, Gabriele Goldacker, Petra Hoepner, Nadja Menz, Maximilian Schmidt, Michael Stemmer, Florian Weigand, Christian Welzel, Jonas Pattberg, Nicole Opiela, Florian Friederici, Jan Gottschick, Jan Dennis Gumz, Fabian Manzke, Rudolf Roth, Dorian Grosch, Maximilian Gahntz, Hannes Wünsche, Simon Sebastian Hunt, Fabian Kirstein, Jens Fromm

Autorinnen und Autoren einzelner Trendthemen: Michael Rothe, Oliver Schmidt

ISBN: 978-3-9816025-2-4

Autorinnen/Autoren: Jan Dennis Gumz

Bibliographische Angabe: Jan Dennis Gumz, Quantencomputing, In: Jens Fromm und Mike Weber, Hg., 2016: ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft. Berlin: Kompetenzzentrum Öffentliche IT, https://www.oeffentliche-it.de/-/quantencomputing

Quantencomputing

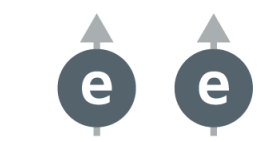
Computer übernehmen mit zunehmender Rechenleistung immer mehr Aufgaben, deren Lösung das menschliche Denkvermögen bei Weitem übersteigt. Allerdings existieren Fragestellungen, die sich auch zukünftig nicht mithilfe herkömmlicher Computer in akzeptabler Zeit beantworten lassen – die Leistungsfähigkeit der Speicherung und Verarbeitung von Informationen in Form von Bits stößt hier an grundsätzliche Grenzen. Einige der derzeit kaum lösbaren Aufgaben, beispielsweise die Simulation großer Quantensysteme, könnten mithilfe von Rechenmaschinen bewältigt werden, bei denen quantenmechanische Effekte eine deutlich zentralere Rolle spielen als bei herkömmlichen Computern. Während in den letzten Jahren einige Durchbrüche für Schlagzeilen gesorgt haben, sind immer noch viele Hindernisse zu überwinden, bis solche Quantencomputer praxistauglich sind.

Funktionsweise im Vergleich mit herkömmlichen Computern

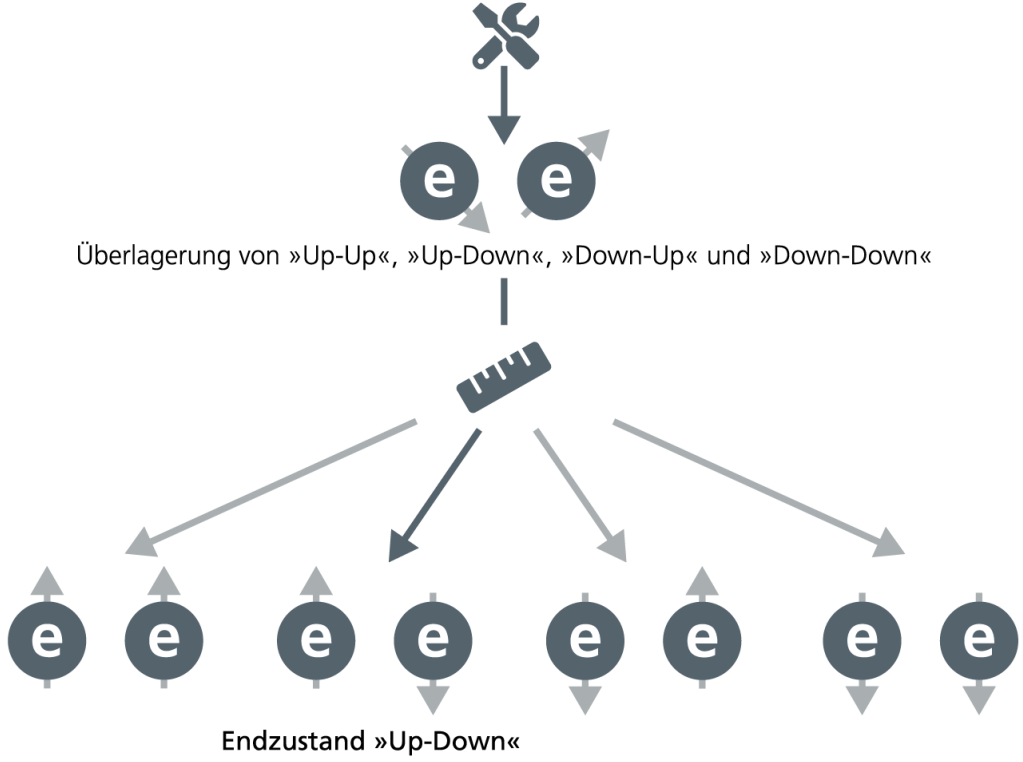
Bei Quantenobjekten handelt es sich z.B. um Photonen, Elektronen und Moleküle. Wie sich diese kleinen Objekte innerhalb eines Systems verhalten, wird durch die Gesetze der Quantenmechanik erklärt. Anhand dieser Gesetze lässt sich das Verhalten eines Quantensystems daher simulieren. Allerdings benötigen klassische Rechner für solche Simulationen enorme Rechenressourcen, die in Abhängigkeit von der Größe des Systems exponentiell wachsen. Diese Tatsache mündete Anfang der 1980er Jahre in der Überlegung, eine alternative Rechenmaschine zu entwickeln, die Quanteneffekte bereits beinhaltet und diese somit nicht in klassischer Weise simulieren muss.

Computer verarbeiten Information in Form von Binärfolgen, also als Zeichenfolgen, deren Alphabet genau zwei Symbole umfasst. Die kleinste Informationseinheit herkömmlicher Computer ist das Bit: Ein System, für das zwei Messergebnisse möglich sind, denen die Werte 0 und 1 zugeordnet sind. Der Zustand eines Bits ist bereits vor einer Messung entweder 0 oder 1. Als kleinste Informationseinheit eines Quantenrechners wird stattdessen das Quantenbit, kurz Qubit, genutzt. Es basiert auf einem Quantensystem, für das wie beim Bit genau zwei Messergebnisse möglich sind, die den Werten 0 und 1 entsprechen. Im Gegensatz zum Bit ist der Zustand des Qubits vor der Messung jedoch nicht auf eines der zwei möglichen Ergebnisse festgelegt. Das Ergebnis ergibt sich zufällig aufgrund einer Wahrscheinlichkeitsverteilung. Ein Qubit kann sich in einem Zustand befinden, bei dem beispielsweise mit 25 % Wahrscheinlichkeit 0 gemessen wird und mit 75 % Wahrscheinlichkeit die 1. Erst durch die Messung wird ein Zustand erreicht, der dann eindeutig entweder 0 oder 1 ist. So können sich 0 und 1 vor der Messung überlagern und somit auch gleichzeitig mithilfe eines einzigen Qubits repräsentiert werden. Dahingegen kann ein Bit immer nur einen dieser beiden Werte repräsentieren, weshalb zwei Bits zur gleichzeitigen Repräsentation der Werte 0 und 1 erforderlich sind. Ein Qubitregister kann deshalb deutlich mehr Information speichern als ein Register mit der gleichen Anzahl von Bits. Aufgrund der Überlagerung kann so auch in einem einzigen Arbeitsschritt eine Operation auf einer Vielzahl von Binärfolgen gleichzeitig, statt wie bei herkömmlichen Rechnern nur auf einer einzigen, angewendet werden. Diese Eigenschaft wird als Quantenparallelismus bezeichnet und ist der Grund für den theoretischen Geschwindigkeitsvorteil der Quantenrechner gegenüber klassischen Rechnern.

Die Informationsverarbeitung endet beim Quantencomputer mit der Messung, weshalb letztlich nur eine Binärfolge übrigbleibt. Um für ein gegebenes Problem tatsächlich die korrekte Lösung zu erhalten, ist es daher zielführend, die Messwahrscheinlichkeit der dieser Lösung entsprechenden Binärfolge zu maximieren. Die Informationsverarbeitung sollte also so gestaltet sein, dass sie die Wahrscheinlichkeitsverteilung der möglichen Messergebnisse gemäß dieser Zielsetzung verändert. Dies lässt sich auf zwei Wegen erreichen, anhand derer sich zwei Quantencomputertypen unterscheiden lassen. Beim adiabatischen Quantenrechner wird ausgehend von einem bekannten Startzustand eines Quantensystems der kontinuierlichen natürlichen Entwicklung dieses Systems freier Lauf gelassen, bis ein zumindest nahezu optimaler Endzustand erreicht ist und so ein Optimierungsproblem gelöst wurde. Im Gegensatz zu klassischen Computern erfolgt die Informationsverarbeitung bei adiabatischen Quantenrechnern also nicht schrittweise durch die Anwendung einer vorgegebenen Reihenfolge kleiner logischer Funktionen (z.B. UND oder NICHT), den sogenannten Gattern. Dies ist bei gatterbasierten Quantenrechnern anders, auch wenn die Gatter nicht die gleichen sind wie bei klassischen Rechnern. Um die Chance der Messung des korrekten Ergebnisses zu maximieren, wird ein Quantenalgorithmus ausgeführt, also eine Handlungsvorschrift, die vorgibt, welche Quantengatter in welcher Reihenfolge anzuwenden sind. Solche Algorithmen können so entworfen werden, dass sie außer Optimierungsproblemen auch weitere Probleme lösen können. Der gatterbasierte Quantenrechner hat gegenüber dem adiabatischen Quantenrechner daher den Vorteil, dass Lösungsverfahren für sehr unterschiedliche Problemtypen leichter entworfen werden können und schließlich sogar ein Allzweck-Quantenrechner entstehen könnte. Allerdings handelt es sich bei Quantengattern um zusätzliche Komponenten (und somit zusätzliche potenzielle Fehlerquellen) von Quantenrechnern, die auch ohne solche Gatter schon sehr fehleranfällig sind.

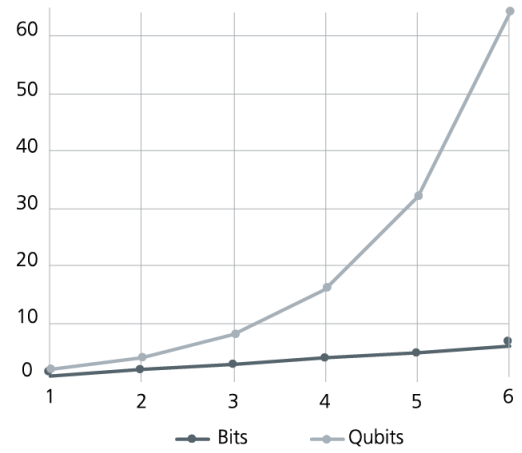


Startzustand Spin »Up-Up«

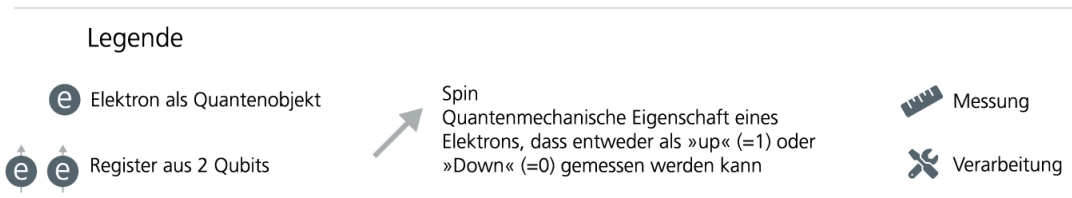


4 mögliche Messergebnisse mit unterschiedlichen Wahrscheinlichkeiten

Anzahl der gleichzeitig repräsentierten Binärwerte



Um genauso viel Information wie 6 Qubits zu speichern, werden bereits 64 herkömmliche Bits benötigt.

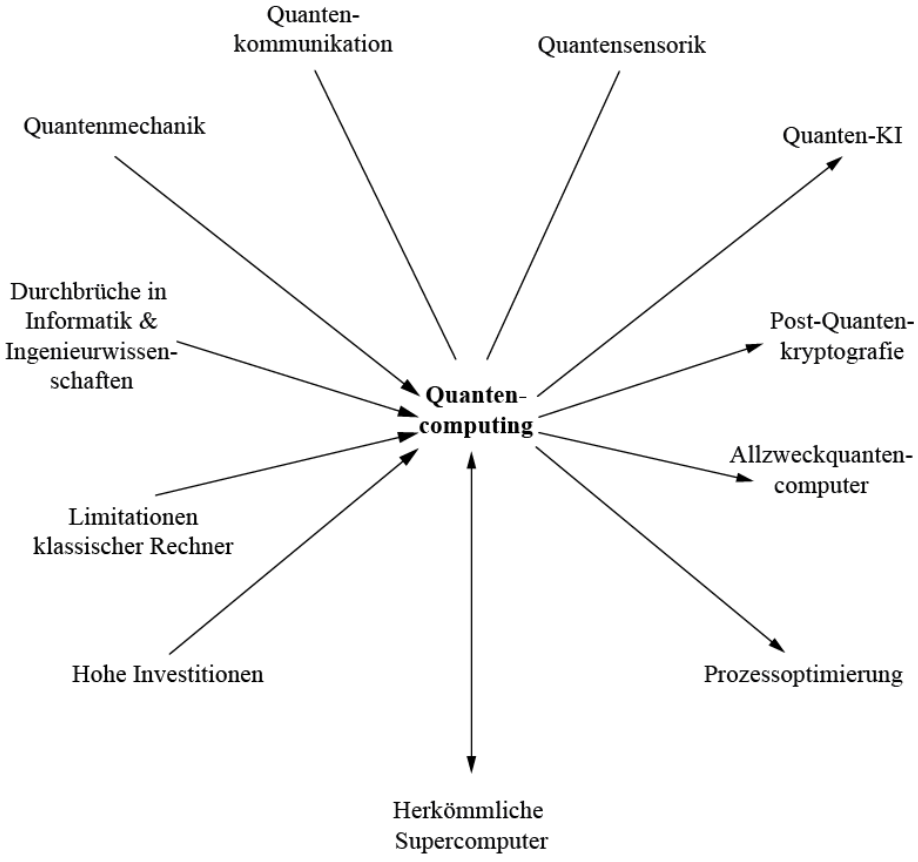


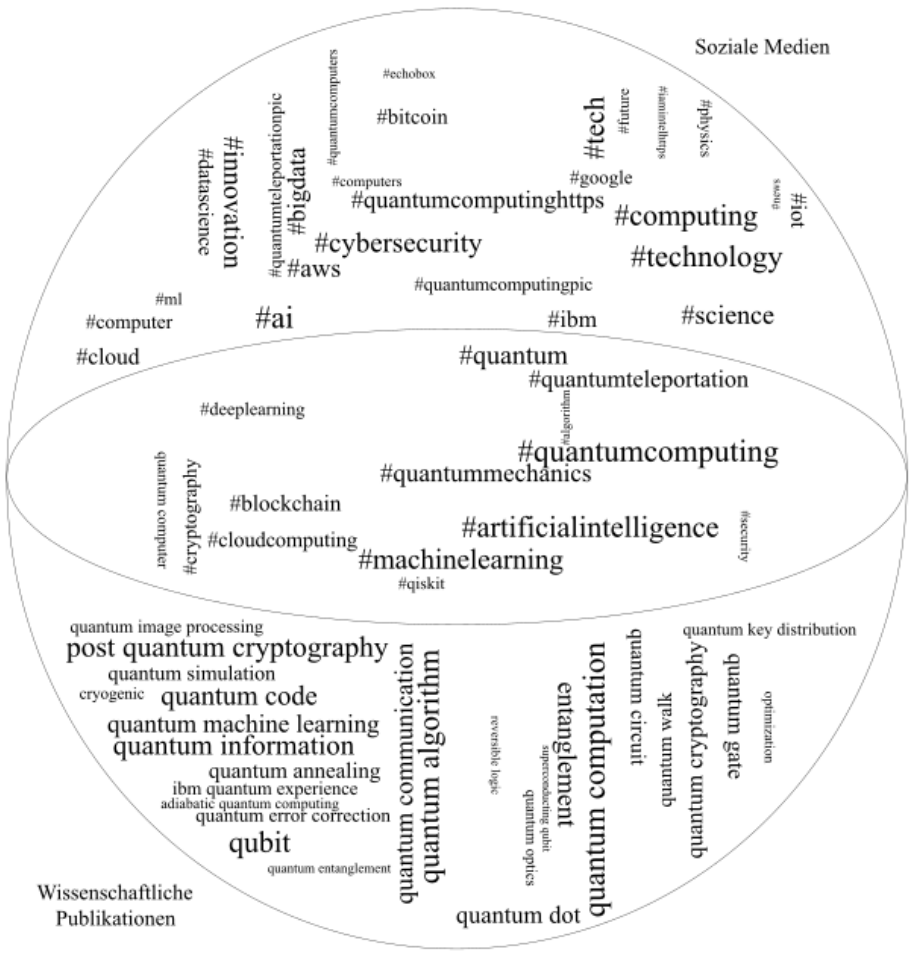
Anwendungen

Quantencomputer sollen unter anderem eingesetzt werden, um Quantensysteme zu simulieren. So können die Quanteneffekte chemischer Prozesse berechnet werden, um langlebigere Batterien und effektivere Medikamente zu entwickeln.
Quantencomputer werden außerdem zur Lösung mathematischer Optimierungsprobleme erprobt, was beispielsweise zu energieeffizienteren Abläufen in der Logistik beitragen kann. Zudem sind die Lösung von Optimierungsproblemen und die schnelle Verarbeitung großer Datenmengen für Machine Learning relevant. Der Einsatz von Quantenrechnern im Bereich der künstlichen Intelligenz (s. **Denkende Maschinen**) wird als Quanten-KI bezeichnet.

Die hohe Rechenleistung von Quantenrechnern könnte zukünftig auch ein Problem darstellen, da sich ab einer gewissen Qubitanzahl gegenwärtige Verschlüsselungsverfahren in kurzer Zeit überwinden lassen (relevant z.B. für **sichere Fahrzeugkommunikation**). Daher wird in der Post-Quantenkryptografie schon heute an neuen Verfahren geforscht. Während Quantencomputing eine Bedrohung für den sicheren Informationsaustausch darstellt, könnte ein verwandter Forschungszweig gleichzeitig die Lösung darstellen: Bei der Quantenkommunikation sollen quantenmechanische Effekte so eingesetzt werden, dass sich Abhörversuche durch Dritte prinzipiell nicht vor den Kommunikationspartner:innen verbergen lassen. Dies könnte zu abhörsicherer Kommunikation führen.
Der Quantenrechner ist ein vielversprechendes Werkzeug und könnte zu zahlreichen Durchbrüchen führen. Viele Prozesse und Produkte könnten effektiver und effizienter gestaltet werden, was von hoher Relevanz für die Wettbewerbsfähigkeit von Wirtschaftsstandorten ist sowie zur Realisierung großer gesellschaftlicher Ziele, etwa Gesundheitsversorgung, Umwelt- und Datenschutz, genutzt werden könnte, wie beispielsweise zur Entwicklung langlebigerer Batterien oder ressourcenschonender Logistik.

Begriffliche Verortung



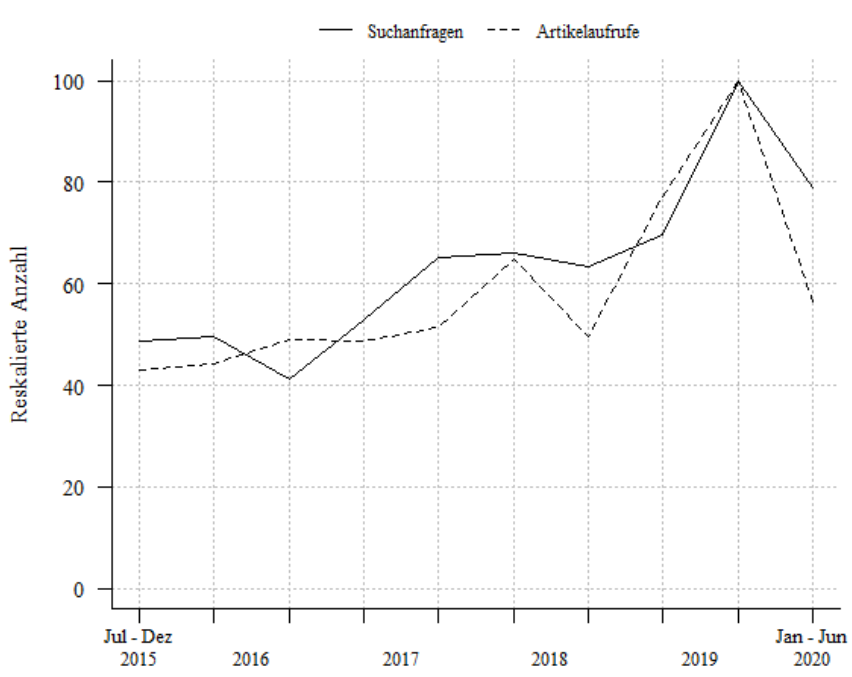


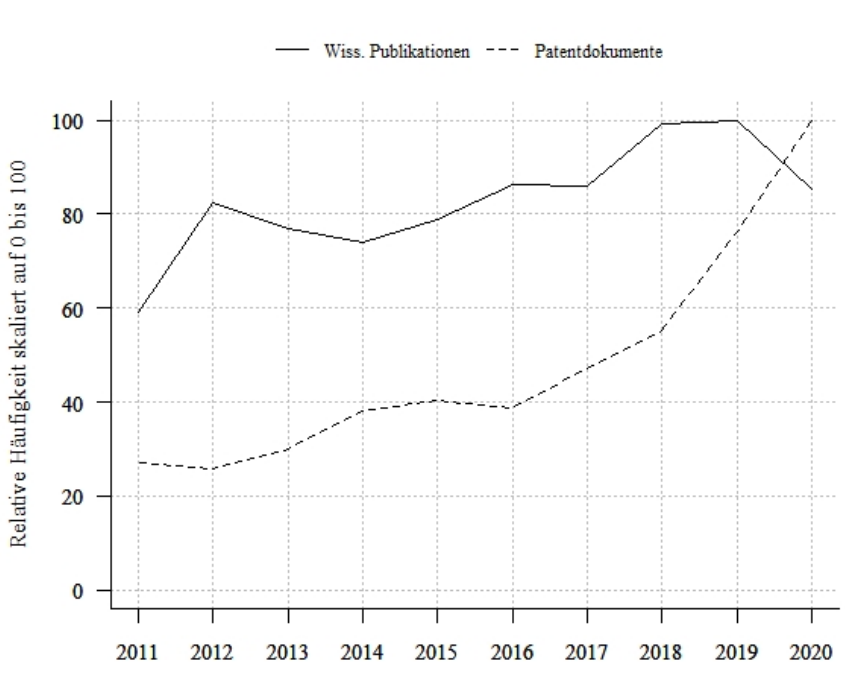
Derzeitiger Stand und Hindernisse

Es existieren verschiedene Möglichkeiten zur Konstruktion von Qubits. Die derzeit populärsten Optionen sind supraleitende Schaltkreise und in Vakuumkammern gefangene Ionen. Unabhängig von der Konstruktionsweise gilt, dass es äußerst schwierig ist, Qubits so gegen Umwelteinflüsse zu isolieren, dass die in den Qubits gespeicherten Zustände nicht verloren gehen und gleichzeitig schnelle und fehlerfreie Operationen auf dem Qubitregister möglich sind. Weil diese technische Hürde bisher nicht genommen worden ist, sind Quantencomputer derzeit noch teure und fehleranfällige Prototypen mit geringer Qubitanzahl, die nur selten praxisrelevante Probleme lösen. Auch deshalb ist der technologische Vorsprung der derzeit führenden Unternehmen und Staaten keineswegs uneinholbar. Weil bisher nur wenige Prototypen existieren, sind die Zugänge zu diesen Quantenrechnern begrenzt und umkämpft, was es wiederum erschwert, Algorithmen für mögliche nützliche Anwendungen zu testen.

Daher fehlt es auch noch an gesicherten Erkenntnissen, bei welchen Anwendungen tatsächlich nicht nur theoretische, sondern praktische Geschwindigkeitsvorteile der Quantenrechner gegenüber herkömmlichen Computern bestehen. Zusätzlich hat sich bisher noch kein einheitliches Verfahren zur Evaluierung der Leistung von Quantencomputern durchgesetzt, was die Vergleichbarkeit verschiedener Konstruktionsweisen erschwert. Weil bei Quantencomputern z.B. Algorithmen grundsätzlich anders als herkömmliche Algorithmen funktionieren, ein Verständnis quantenmechanischer Prinzipien erforderlich ist und aus ingenieurwissenschaftlicher Sicht neue Herausforderungen zu meistern sind, lassen sich Kenntnisse der klassischen Informatik nicht einfach übertragen. Dies bedeutet auch, dass die Anzahl spezialisierter Fachkräfte noch gering ist und Kenntnisse bei Entscheider:innen aus Wirtschaft und Verwaltung oftmals noch fehlen. All dies sind Hindernisse, die die Skalierung des Quantencomputings erschweren.

Themenkonjunkturen





Der Weg zu großen Quantenrechnern

Sowohl große Technologieunternehmen als auch Startups und Forschungseinrichtungen beschäftigen sich mittlerweile verstärkt mit Quantencomputing. Zusätzlich wurde staatliche Förderung in Milliardenhöhe versprochen, u. a. in Deutschland und auf EU-Ebene. Trotzdem geht die Mehrheit der Expert:innen

Bis zum endgültigen Durchbruch sind allerdings Zwischenschritte wahrscheinlich. So werden beispielsweise schon heute hybride Algorithmen entwickelt, die Teilaufgaben auf herkömmliche und quantenmechanische Prozessoren verteilen sollen. Die Funktionalität von Quantenalgorithmen lässt sich bereits heute testen, indem ein herkömmlicher

von einem Zeitraum von 10 bis 20 Jahren bis zu verlässlichen Quantenrechnern mit großer Qubitanzahl aus. Diese Quantencomputer werden wahrscheinlich vorerst teure Spezialwerkzeuge sein, die in Rechenzentren (s. **Cloud Computing**) stehen und als Dienst aus der Ferne erreichbar sind.

Computer einen Quantenrechner simuliert. Zudem werden

Ansätze untersucht, die mehrere Qubits zu einem einzigen logischen Qubit zusammenfassen. Ein Qubit dient dabei als eigentliche Informationseinheit, während die weiteren Qubits dann die bei der Informationseinheit auftretenden Fehler erfassen, wodurch diese korrigiert werden können. Ein logisches Qubit ist so weniger fehleranfällig als ein einzelnes Qubit. Die Forschung zu verwandten Quantentechnologien wie der Quantenkommunikation und der Quantensensorik, also Sensoren, deren Leistungsfähigkeit auf quantenmechanischen Prinzipien beruht, werden derzeit intensiviert. Fortschritte in diesen Bereichen könnten auch dem Quantencomputing zugutekommen und teilweise zu sprunghaften Entwicklungen führen.

Folgenabschätzung

Möglichkeiten

- Fortschritte beim Verständnis von Quantensystemen
- Verbesserte Effizienz und Effektivität bei einer Vielzahl von Prozessen und Produkten und dadurch sprunghafte Fortschritte in wirtschaftlich und gesellschaftlich relevanten Bereichen
- Abhörsichere Kommunikation
- Zukunftsmarkt mit überwindbaren technologischen Eintrittsbarrieren

Wagnisse

- Hohe Investitionen erforderlich
- Schwierige Skalierung
- Unsicherheit bezüglich des Zeitpunktes der Praxistauglichkeit
- Gefahr für heutige Verschlüsselungsverfahren
- Fachkräftemangel sowie die bislang geringe Verbreitung von Kenntnissen unter Entscheidungsträger:innen, z.B. zur Erprobung von Algorithmen

Handlungsräume

Förderung verschiedener Ansätze

Für die Konstruktion von Qubits existieren mehrere, teilweise bisher rein theoretische Ansätze. Auch wenn derzeit mit supraleitenden Qubits die größten Fortschritte erzielt werden, könnte sich die Fokussierung auf einen einzigen Ansatz als Sackgasse herausstellen.

Quantencomputing gesamtheitlich betrachten und fördern

Die Entwicklung von Software, Material (z.B. für Supraleitung bei höheren Temperaturen), Algorithmen, Mess- und Steuerungsinstrumenten sowie Anwendungsmöglichkeiten sind allesamt relevant für Quantencomputing und stellen Chancen dar.

Frühzeitig auf Post-Quantenkryptografie setzen

Quantencomputer besitzen das Potenzial, etablierte Verschlüsselungen leicht zu überwinden. Die Kommunikationsinfrastruktur sollte frühzeitig entsprechend angepasst werden, um selbst bei unerwartet frühen Durchbrüchen bei Quantencomputern gewappnet zu sein.

Frühzeitige Auseinandersetzung mit Quantenrechnern

Die Funktionalität von Quantenalgorithmen lässt sich mit herkömmlichen Computern, die Quantenrechner simulieren, prüfen. So könnten Quantencomputer schon relativ schnell nach Durchbrüchen für nützliche Anwendungen verwendet werden. Um Chancen ergreifen zu können, sollten Entscheider:innen frühzeitig versuchen, Anwendungsfälle innerhalb ihrer Branche zu identifizieren. Um einem Fachkräftemangel vorzubeugen, sollten bereits heute (Weiter-)Bildungsangebote für Arbeitnehmer:innen und Studierende mit naturwissenschaftlichem oder technischem Schwerpunkt geschaffen werden.