

Ready to take off!

Quantencomputer sind startklar. Das meint David DiVincenzo. Im Interview erläutert der Physiker, wozu sie dienen werden und inwieweit sie nützlich oder bedrohlich sind.



Prof. DiVincenzo, wie erklären Sie einem Laien wie mir, was ein Quantencomputer überhaupt ist?

Ein Bit, das Objekt der heutigen digitalen Informationstechnik, besteht aus der Zahl 1 oder der Zahl 0. Und ob das jeweilige Objekt eine 1 oder eine 0 ist, steht unzweifelhaft fest. Das ist wie bei diesem Kugelschreiber vor mir: Er liegt entweder zweifelsfrei hier oder – wenn ich ihn woanders hinlege – zweifelsfrei dort. In der Quantenwelt ist das anders: Dort kann ein Objekt gleichzeitig hier und anderswo sein. Das widerspricht unserer Alltagserfahrung und unserer Intuition – wie auch andere Aspekte der Quantenphysik. Daher ist der Quantencomputer, der auf den Gesetzen der Quantenphysik beruht, so schwer zu verstehen. Beispielsweise kann das Qubit, das Objekt beim Quantencomputing, gleichzeitig 0 und 1 sein. Unter anderem diese Eigenschaft lässt sich ausnutzen, um manche Aufgaben schneller zu lösen, als es mit Bits und digitalen Rechnern möglich ist.

Wird der Quantencomputer künftig also unsere heutigen Computer ablösen?

Das halte ich für unwahrscheinlich. Unsere digitalen Computer sind nahezu universell einsetzbar. In vielen Bereichen wird ein Quantencomputer keinen zusätzlichen Nutzen gegenüber einem solchen Computer haben. Doch wir Wissenschaftler sehen schon seit Längerem einige spezifische Anwendungen, in denen der Quantencomputer dem herkömmlichen Computer deutlich überlegen sein wird.

Welche Anwendungen sind das?

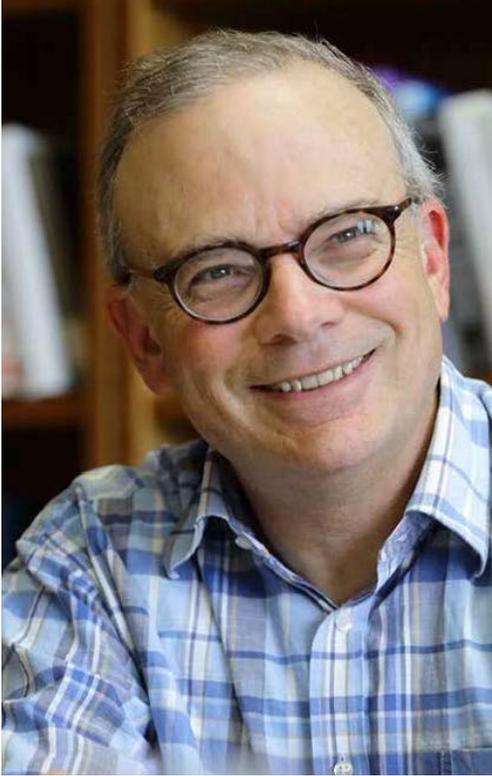
Erstens die Simulation von Materialien, da diese aus Atomen und Elektronen bestehen. Das sind Bausteine, die den Gesetzen der Quantenphysik gehorchen, daher werden wir ihre Eigenschaften mit Quantencomputern besser verstehen und

vorhersagen können als bislang. Zweitens könnten Quantencomputer zum Aufbau eines neuartigen Netzwerks dienen, in dem Daten sicherer ausgetauscht werden und Partner sicherer zusammenarbeiten als im digitalen Internet. Drittens wird ein Quantencomputer eine Reihe von komplexen mathematischen Problemen effizienter lösen können als bisherige Rechner. Das ist nicht nur für die reine Mathematik interessant, sondern zum Beispiel auch für die heute gängige Technik, um Daten zu verschlüsseln und zu entschlüsseln.

Stichwort Daten entschlüsseln: Aus diesem Grund gibt es Bedenken, dass Quantencomputer in den Händen von Geheimdiensten oder Kriminellen eine mächtige Waffe wäre. Was erwidern Sie?

Zunächst einmal ist das Internet auch heute schon keineswegs sicher – dazu bedarf es keines Quantencomputers. Richtig ist, dass die Verschlüsselungstechnik, die heute etwa beim Home-Banking und bei Messenger-Diensten eingesetzt wird, in rund zehn Jahren so unsicher sein wird, dass sie in den Ruhestand versetzt werden sollte. Doch es gibt eine gute Nachricht: Es existieren für solche klassischen Internetdienste bereits alternative Verschlüsselungsmethoden, die auch mit einem Quantencomputer nicht zu knacken wären. Diese Methoden werden in zehn Jahren hoffentlich auf breiter Front einsatzbereit sein. Zusätzlich bieten reine Quanten-Kommunikationsnetze langfristige Sicherheit. Es liegt in der Natur dieser Systeme, dass man jeden Lauschangriff bemerkt.

Schon Anfang der 1990er Jahre gab es Meldungen darüber, dass Forscher Quantencomputer auf Basis organischer Moleküle verwirklicht hätten. Wie weit ist man heute?



Die Experimente vor 20 Jahren waren gut geeignet, um Prinzipien der Quantenmechanik zu demonstrieren und einzelne Qubits herzustellen. Ich habe jedoch schon damals aufgrund von theoretischen Überlegungen vorhergesagt, dass sich Quantensysteme, die auf organischen Molekülen beruhen, nicht von einigen Qubits auf 100 oder noch mehr Qubits vergrößern lassen werden. Diese fehlende Skalierbarkeit bestätigte sich. Ende der 1990er Jahre kam dann unter Theoretikern die Idee auf, Qubits in Festkörpern zu verwirklichen. Was dann Anfang der 2000er Jahre auch gelang. Inzwischen gibt es Festkörper-Systeme, die meiner Meinung nach von derzeit fünf bis zehn auf deutlich mehr Qubits skalierbar sind: Der Quantencomputer ist „ready for take-off“.

Das US-Unternehmen D-Wave hat bereits einige Exemplare eines Gerätes verkauft, das es als Quantencomputer bezeichnet. Experten streiten darüber, ob es wirklich einer ist. Ihre Meinung?

Der D-Wave-Rechner hat gewisse Eigenschaften eines Quantencomputers. Ich würde ihn aber nicht als solchen bezeichnen. Unter anderem deshalb, weil sich seine Qubits nur für Nanosekunden (milliardstel Sekunden) in einem Zwischenzustand zwischen 0 und 1 befinden können. Daher wird er vermutlich selbst in künftigen Versionen nur sehr wenige Aufgaben effizienter lösen können als ein herkömmlicher Computer.

Sie beschäftigen sich als Theoretiker mit Quantencomputern. Was heißt das?

Anders als Praktiker bin ich nicht an eine Laborausstattung, eine Technik oder eine Methode gebunden. Und auch nicht an Supercomputer oder Codes, wie manche anderen Theoretiker. Mir reicht ein Stück Papier zum Schreiben, um Ideen zu

entwickeln. Dabei denke ich auch darüber nach, wie diese Ideen im Experiment nützlich sein können oder wie man sie anwenden kann.

Haben Sie ein Beispiel für eine solche Idee?

Bei heutigen Qubit-Experimenten setzt man Bauteile zur Signalverarbeitung ein, die schon in einem Buch aus den 1960er Jahren beschrieben sind. Je mehr Qubits in einem System verwirklicht sind, umso mehr von diesen zentimetergroßen Zirkulatoren werden benötigt. Als ich vor einiger Zeit wieder in dem Buch las, hatte ich die Idee zu einem alternativen Zirkulator, der nach einem völlig anderen Prinzip arbeitet. Sein großer Pluspunkt: Er ist kleiner als der herkömmliche und kann in großen Mengen in einen einzigen Chip integriert werden. Zusammen mit einem Postdoc arbeite ich diese Idee immer weiter aus. Ich habe darauf inzwischen ein Patent und zusätzlich einige Publikationen darüber geschrieben.

DAS INTERVIEW FÜHRTE FRANK FRICK.

Zur Person

Prof. David DiVincenzo gilt als Pionier im Bereich Quanteninformation. Mit seinem Namen ist unter anderem die Entwicklung von Kriterien verbunden, die ein Quantencomputer erfüllen muss, die sogenannten „DiVincenzo criteria“. Der Physiker ist Direktor des Jülicher Peter Grünberg Instituts, Bereich Theoretische Nanoelektronik (PGI-2), und lehrt an der RWTH Aachen am JARA-Institute for Quantum Information. Der US-Amerikaner wurde 2010 mit der Alexander von Humboldt-Professur ausgezeichnet, dem höchstdotierten internationalen Forschungspreis Deutschlands.