

# Quantencomputer

## Wie funktionieren sie und wozu werden wir sie nutzen können?

Seit der Erfindung des Halbleiter-Mikrochips wird unser Leben durch Digitaltechnik geprägt. Die Welt verlässt sich auf Milliarden von Smartphones und PCs, auf E-Autos und Satelliten. Einen Schritt weiter gehen Quantencomputer, an deren Etablierung weltweit fieberhaft gearbeitet wird. Angesichts grosser Erwartungen und offener Fragen lohnt es sich, Quantencomputer und ihre erstaunliche Funktionsweise, ihre verblüffenden Vorteile, aber auch Nachteile jetzt kennenzulernen.

### Spektakuläre 2. Quantenrevolution

Zunächst: Was haben die weitverbreiteten Mikrochips mit den noch kaum bekannten Quantencomputern zu tun? Mikrochips bedienen sich einiger quantenmechanischer Phänomene aus der sogenannten «1. Quantenrevolution» (auch «Quantum 1.0», vgl. Glossar). Was wir als Quantencomputer bezeichnen, wurde jedoch erst mit der 2. Quantenrevolution (oder «Quantum 2.0») möglich. Diese konnte dank neuer Einsichten in die Quantenphysik und laufender technischer Fortschritte realisiert werden.

Aufgrund der erwarteten Eigenschaften sollte die neue Quantencomputergeneration in Zukunft äusserst komplexe Probleme lösen können. An positiven Prophezeiungen mangelt es nicht, vor allem für Industrien wie Chemie, Materialwissenschaften, Finanzen, Logistik oder Meteorologie. Auch der Bereich Cybersecurity dürfte stark davon betroffen sein und muss sich massiv weiterentwickeln. Schon heute rüstet man klassische Netzwerkkomponenten auf, um sie «quantum-safe» zu machen, d.h. um sie gegen die Entschlüsselung gewisser Sicherheitscodes durch Quantencomputer zu sichern.

### Grosse Hoffnungen und (noch) grosse Hürden

Sind diese neuartigen Rechner eine disruptive Innovation und werden bald alle Computer mit Quanten rechnen? So viel vorweg: Quantencomputer werden unsere digitalen Alltagsgeräte auf absehbare Zeit zwar nicht ersetzen, aber für gewisse Aufgaben ergänzen. Für die Lösung von speziellen, enorm rechenintensiven Problemen werden sie heutigen Rechnern mit Sicherheit überlegen sein.

Zum Beispiel im Bereich Verschlüsselungstechnik. Die weltweit als Standard geltende RSA-Verschlüsselung, basierend auf der Faktorisierung von Primzahlen, wird mit einem Quantencomputer innert Stunden, wenn nicht Minuten geknackt sein – während konventionelle Computer Jahre oder Jahrzehnte dafür brauchen würden. Darum wird bereits an der «Post-Quanten-Kryptographie» gearbeitet. Kein Wunder, wird der Quantencomputer in Technik- und Investment-

Kreisen als «the next really big thing» gehandelt. Er könne «alles» verändern, heisst es bisweilen – typische Anzeichen eines Hypes.

### Entmystifizierung und Orientierung

Quantencomputer könnten unsere Welt tatsächlich grundlegend verändern. Für verschiedene Industriezweige, Forschungsrichtungen und Wirtschaftsgebiete dürften sie wegweisend werden – sobald stabile, verfügbare und wirtschaftliche Systeme entwickelt sind. Die Frage ist nur, wann und wie die Quantencomputer-Disruption oder zumindest -Transformation eintritt. Und was die Technologie wirklich kann, wenn sich der Spekulationsnebel verzogen hat.

Aktuell gibt es noch keinen universell einsetzbaren Quantencomputer, der klassischen Hochleistungsrechnern überlegen wäre. Hingegen kennen wir erprobte, «einfachere» Quantum-2.0-Anwendungen wie z.B. die Quanten-Messtechnik. Sie besticht durch eine Genauigkeit, die bisherige Methoden um Grössenordnungen übertrifft. Es dürfte aber noch einige Jahre dauern, bis Quantencomputer im Alltag angekommen sind.

## Inhalt

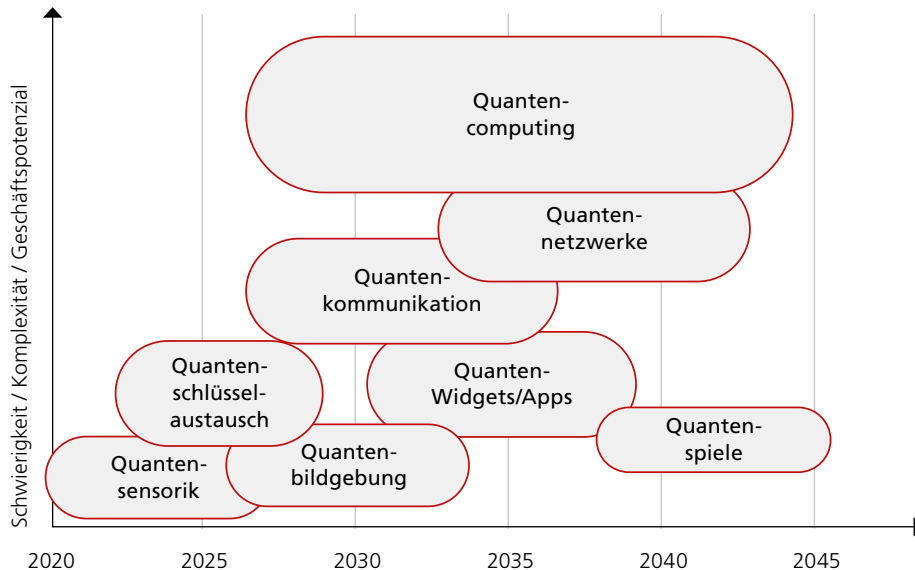
<b>Hightech-Revolution mit neuer Physik</b>	<b>2</b>
<b>Quantenphänomene</b>	<b>3</b>
<b>Was können Quantencomputer?</b>	<b>5</b>
<b>Quantencomputertechnologien «im Wettstreit»</b>	<b>6</b>
<b>Vor- und Nachteile</b>	<b>7</b>
<b>Die Schweiz, ein Quantencomputing-Hub</b>	<b>10</b>
<b>Prädestinierte Anwendungen</b>	<b>11</b>
<b>Erstaunliche (Quanten-)Computergeschichte</b>	<b>14</b>

# Hightech-Revolution mit neuer Physik

Von allen neuen Quantentechnologien der 2. Quantenrevolution gilt das Quantencomputing als Spitzendisziplin. Man muss so viele physikalische, technologische und programmiertechnische Probleme lösen, dass trotz enormer internationaler Anstrengungen erst in

einigen Jahren praktisch einsetzbare und effiziente Quantencomputer-Produkte erwartet werden. Andererseits hat das Quantencomputing auch ein enormes Potenzial dafür, gewisse Bereiche der Wirtschaft und Gesellschaft tiefgreifend zu verändern.

**Gewichtung und Prognose verschiedener Quantentechnologien.**



Quelle: QIDIS (Quantum industry day in Switzerland) 2021 / P. Seitz

## Quantentechnologien der 2. Quantenrevolution

Bereits heute werden sowohl weltweit als auch in der Schweiz Produkte hergestellt, welche die Einsichten der 2. Quantenrevolution praktisch nutzen:

- **Quantenschlüsselaustausch, Quantensensorik und -bildung:** Erkenntnisse aus diesen ersten «Früchten» der Quantentechnologie können bereits heute sowohl für praktische Anwendungen als auch für die weitere Forschung eingesetzt werden.
- **Quantennetze und -kommunikation:** In einigen Jahren sollten funktionsfähige, zuverlässige Quantenkommunikationsnetze möglich sein. Letztere werden dank Quantentechnik aus physikalischen Gründen absolut abhörsicher sein (secure by physics). Fachleute schätzen, dass kommerzielle Kommunikationskanäle mit Quantenkryptografie in rund fünf Jahren aufkommen könnten. Ein sicheres Quanteninternet könnte hingegen noch bis 2050 auf sich warten lassen.
- **Quanten-Widgets und -Games:** Schon immer ist der Mensch äusserst einfallsreich mit neuen Technologien umgegangen, und unerwartete Anwendungen haben bisweilen weite Verbreitung und grossen Nutzen gefunden. Wir wissen noch nicht, was «Quanten-Widgets» und «Quantum Games» sind, aber es könnte gut sein, dass uns ein kluger Kopf schon bald damit überraschen wird.

- **Quantencomputer:** Sie sind in gewisser Weise die ultimative Anwendung der Quantentechnologie, da sie dereinst Probleme lösen werden, die mit herkömmlicher Computerhardware in vernünftiger Zeit nicht lösbar sind.

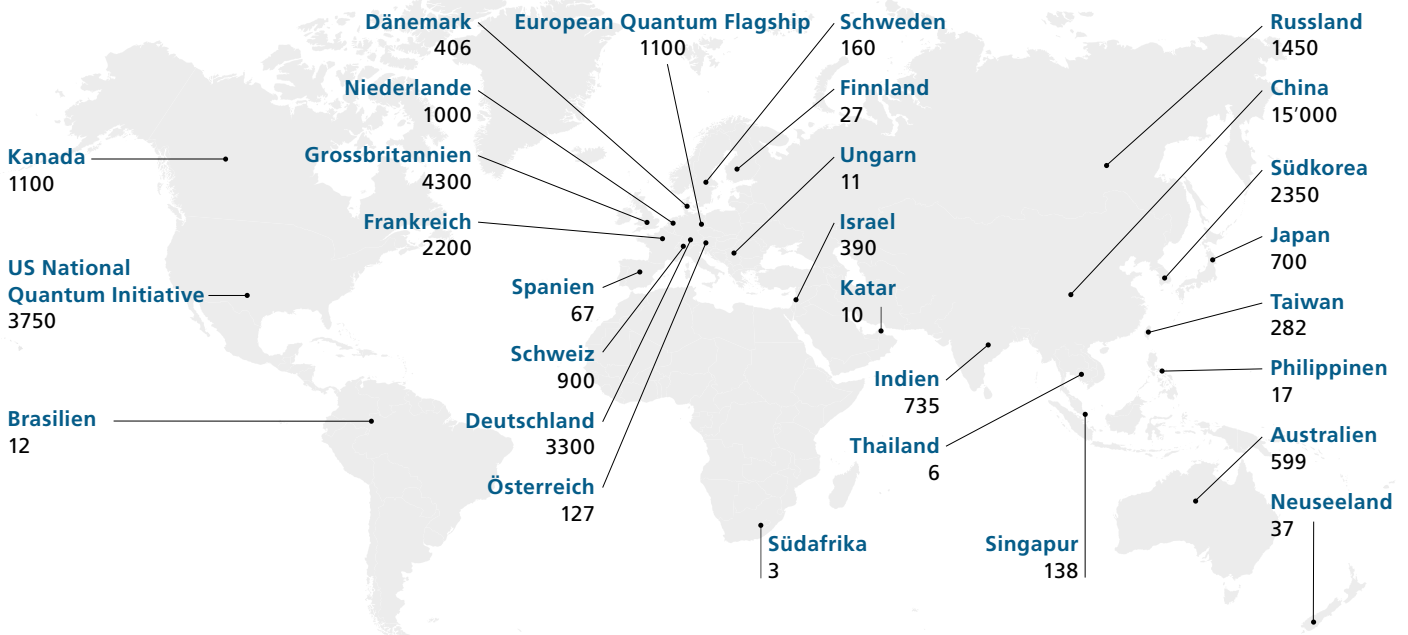
## Globales Quantencomputerrennen

Trotz vieler offener Fragen und enorm teurer Technik ist das Rennen um die effiziente Nutzung der Vorteile von Quantencomputern in vollem Gang. Denn es steht viel auf dem Spiel: Das grosse Potenzial vom Quantencomputing reicht über wissenschaftliche und technologische bis hin zu wirtschaftlichen Fortschritten.

**«Die Quanteninformatik ist eine ganz neue Art, sich die Natur zunutze zu machen. Sie wird es als erste Technologie ermöglichen, nützliche Aufgaben zwischen parallelen Universen zu erledigen.»**

David Deutsch,  
Dirac- und Isaac-Newton-Medaillepreisträger

## Investitionen des öffentlichen Sektors in Quantentechnologien weltweit in Mio. USD



Quelle: «Overview of Quantum Initiatives Worldwide 2023», QURECA, 19. Juli 2023. Department of Industry, Science and Resources, Austria; ETH Domain (ETH Zurich, EPFL, PSI).

Die Grafik zeigt weltweite Investitionen in die Quantentechnologie 2023, wobei das Quantencomputing als Hauptanwendung der Quantentechnologien gilt (für das Gebiet Quantencomputing allein liegen leider keine verlässlichen

Zahlen vor). Zum Vergleich: China wendet jährlich rund 15 Milliarden USD dafür auf, die Schweiz 900 Millionen Dollar. Während die meisten Nationen und Unternehmen – auch aus Ressourcengründen – auf eine oder wenige

Implementierungsarten (vgl. Kap. 4) setzen, verfolgen solche, die hohe Investitionen tätigen, meist mehrere Ansätze zeitgleich, um möglichst schnell Fortschritte und Resultate zu erzielen.

## Quantenphänomene

Heute stossen die besten herkömmlichen Mikroprozessoren mit ihren wenige Nanometer breiten Halbleiterstrukturen an ihre physikalischen Grenzen. Das bekannte «Moore's Law» (streng genommen kein Gesetz, sondern eine bisher gut zutreffende, selbsterfüllende Prophezeiung) von Intel-Mitgründer Gordon Moore besagt, dass sich die Zahl der Transistoren auf einem integrierten Schaltkreis aufgrund der Anstrengungen der Forschung und Industrie im Schnitt alle zwei Jahre verdoppelt.

Diese stetige Miniaturisierung führt irgendwann in den atomaren Bereich. In den kleinsten Dimensionen unseres Universums versagen die Gesetze der klassischen Mechanik, wie sie Isaac Newton formuliert hat. In Systemen, die aus nanoskaligen Teilchen wie Photonen und Elektronen bestehen, herrschen die Gesetze der Quantenmechanik, die oft im Widerspruch zu unserer Wahrnehmung der alltäglichen Gesetzmässigkeiten stehen.

### «Viel Platz im Kleinsten»

Paradoxerweise tut sich dort, wo es nach unseren gängigen Massstäben immer kleiner wird, eine riesige Welt auf – die Welt der Quanten. «There's plenty of room at the bottom» (Es gibt jede Menge Platz da unten) ist der Titel eines visionären Vortrages, den der Physiker und Nobelpreisträger Richard Feynman 1959 hielt. Dabei stellte er seine Ideen vor, wie Technologie auf submikroskopischer Ebene funktionieren könnte – oder noch weiter «unten», in der nicht mehr sichtbaren, nanoskaligen Welt. Erst allmählich entdecken

wir, wie die Welt auf der kleinsten Dimensionsstufe der Atome aufgebaut ist (vgl. Glossar).

Wie kann man sich diese unglaublich kleinen Teilchen vorstellen? Je nach Element sind Atome nur etwa 1–5 Zehntel Nanometer klein. Ein Nanometer ist ein Milliardstel Meter. So enthält ein Staubkorn etwa 100 Millionen Milliarden Atome – mehr, als es Sterne im Universum gibt. Unsere heutige Mikroelektronik, die Halbleitertechnik und die Optoelektronik mit ihren LEDs, Laserdioden und Displays beruhen auf der Klasse «Quantum 1.0», wobei die einfacheren Phänomene der Quantenphysik eingesetzt werden, wie die Quantisierung von Energiezuständen, die Existenz von reinen Energiepaketen (Photonen) und die Wechselwirkung von Elektronen mit diesen Photonen – auch als QED (Quantenelektrodynamik) bezeichnet.

Die neuen Quantentechnologien der Klasse «Quantum 2.0» nutzen die physikalischen Phänomene und Prozesse der Quantenmechanik auf dem atomaren und subatomaren Level. Sie machen sich drei zusätzliche Quantenphänomene zunutze: Überlagerung (Superposition von Grundzuständen, wobei Messresultate nur durch Wahrscheinlichkeiten vorausgesagt werden können), Verschränkung (Entanglement, wobei alle Komponenten von verschränkten Systemen «voneinander wissen») und Interferenz (die Möglichkeit, Quantensysteme so zu manipulieren, dass «störende» Zustände wegsubtrahiert werden).

## Drei Voraussetzungen für Quantencomputing



### Überlagerung

Das Bit, die kleinste Einheit eines herkömmlichen, digitalen Rechners, kann nur zwei Zustände einnehmen – entweder 0 oder 1 – und Rechenoperationen werden meist sequenziell vorgenommen. Es sei denn, der Rechner besitzt Cores, die parallel arbeiten. Ein Quantenbit (Qubit) in einem Quantencomputer hingegen befindet sich während der Rechnung in einem Zustand der Überlagerung von – meist zwei – Basiszuständen. Die «Rechnung» in einem Quantencomputer wird ausgeführt, indem die Wahrscheinlichkeiten, dass sich die Qubits in bestimmten Basiszuständen befinden, systematisch manipuliert werden. Das Resultat einer Quantenrechnung wird durch Auslesen der Qubits erhalten, wobei diese mit einer bestimmten Wahrscheinlichkeit in einem der Basiszustände gefunden werden. Das ist auch der Grund dafür, dass ein Quantencomputer keine «perfekten» Resultate liefern kann, sondern nur «Wahrscheinlichkeiten». Je öfter man eine Quantenrechnung wiederholt, desto genauer ist deshalb auch das Resultat.

Die physikalischen Eigenschaften einer Quanteneinheit bleiben demnach undefiniert, bis sie gemessen werden. Niemand weiss, welchen Wert ein Qubit «wirklich» hat, nicht einmal das Universum. Albert Einstein fühlte sich mit der Vorstellung, dass die Physik durch den Zufall bestimmt ist, sehr unwohl – er meinte: «Gott würfeln nicht». Und doch weiss man heute, dass es so ist. In einem quantenphysikalischen System gibt es jedoch (vor der Messung) keine Gewissheit, wo sich ein Quantenteilchen befindet oder in welchem Zustand es ist – es gibt lediglich Wahrscheinlichkeiten dafür. Mehr als diese Wahrscheinlichkeiten kann man über ein Teilchen nicht wissen.

Unsere Alltagserfahrung fusst darauf, dass alle Objekte immer und überall einen wohldefinierten Zustand haben. Aber genau das trifft für Quantenobjekte nicht zu. Manchmal wird dieses Verhalten damit erklärt, dass sich Quantenobjekte gleichzeitig in verschiedenen Basiszuständen befinden – das wird als Superpositionsprinzip bezeichnet. Aber diese Beschreibung ist nur eine «Vorstellungshilfe» für die Identität von Quantenobjekten, die nur mit mathematischen Wahrscheinlichkeiten korrekt beschrieben werden kann. Entsprechend schwierig, ja schier unmöglich ist es, dieses Verhalten bildlich umzusetzen.

Unsere Alltagserfahrung fusst darauf, dass alle Objekte immer und überall einen wohldefinierten Zustand haben. Aber genau das trifft für Quantenobjekte nicht zu. Manchmal wird dieses Verhalten damit erklärt, dass sich Quantenobjekte gleichzeitig in verschiedenen Basiszuständen befinden – das wird als Superpositionsprinzip bezeichnet. Aber diese Beschreibung ist nur eine «Vorstellungshilfe» für die Identität von Quantenobjekten, die nur mit mathematischen Wahrscheinlichkeiten korrekt beschrieben werden kann. Entsprechend schwierig, ja schier unmöglich ist es, dieses Verhalten bildlich umzusetzen.



### Interferenz

Die quantenmechanische Interferenz ist die Konsequenz davon, dass das Verhalten eines Quantensystems durch Kombination aller möglichen Verläufe der Entwicklung des Quantensystems beschrieben wird. Diese «Kombination» erfolgt aber nicht durch einfache Addition der Endzustände, sondern man muss berücksichtigen, dass Quantenzustände durch Wellenfunktionen dargestellt werden. Deshalb muss man für die korrekte Kombination jeweils die Amplituden von allen beteiligten Wellenfunktionen zusammen-

zählen – wie man es etwa von Wasserwellen kennt. Dadurch wird es möglich, dass sich verschiedene Wellenbeiträge für ein Endresultat gegenseitig aufheben. Dies bedeutet, dass man Quantenteilchen an gewissen Aufenthaltsorten oder in Endzuständen nicht findet, wo man sie in der klassischen Physik erwarten würde. Diese gegenseitige Auslöschung von Wellenfunktionen ist ein zentrales Werkzeug der Programmierung von Quantencomputern, denn es ist das Ziel von jedem effizienten Quantencomputer-Algorithmus, die Wahrscheinlichkeitsverteilung von Endresultaten so schmal wie möglich machen, damit die statistische Aussagekraft der erhaltenen Resultate so hoch wie praktisch machbar wird.



### Verschränkung

Die zweite Einsicht der Physiker:innen, welche das enorme Potenzial von Quantencomputern erklärt, liegt im Verständnis eines weiteren merkwürdigen quantenphysikalischen Phänomens: Quantenobjekte kann man so miteinander verbinden/verschränken, dass sie einander beeinflussen, auch über lange Distanzen. Sobald man den Wert des einen Quantenobjekts durch Messung kennt, ist auch der Wert seines verschränkten Zwillings klar – und zwar sofort, noch bevor er auch gemessen wird. Wenn man den Quantenzustand eines Qubits ändert, dann «spüren» alle anderen verschränkten Qubits diese Änderung auch und ihr Quantenzustand ändert sich entsprechend.

In einem klassischen Computer werden die Bits unabhängig voneinander gespeichert und verarbeitet. Bei einem Quantencomputer ist das nicht so: Jeder Rechenschritt betrifft immer alle verschränkten Qubits und damit den gesamten Quantencomputer. Das hat zur Folge, dass die Anzahl der Variablen, mit denen man in einem klassischen Computer rechnen kann, linear mit der Anzahl Bits zunimmt. Bei einem Quantencomputer hingegen nimmt die Anzahl von speicher- und verarbeitbaren Informationseinheiten exponentiell mit der Anzahl Qubits zu.

Auch der überraschende Effekt der «Verschränkung» von Quantensystemen, selbst über astronomische Entfernungen hinweg, war Albert Einstein sein Leben lang suspekt. Er nannte ihn «spooky action at a distance». Der definitive Nachweis der Quantenverschränkung, der heute als die zentrale Eigenschaft von Quantencomputern anerkannt ist, wurde erst 2015 experimentell geführt und 2022 mit dem Nobelpreis an Alain Aspect, John Clauser und Anton Zeilinger gekrönt.

## Was können Quantencomputer?

Diese einfache und offensichtliche Frage hat überraschenderweise noch keine definitive Antwort. Die mathematische Komplexitätstheorie kümmert sich um genau solche zentralen Fragen: Was ist die «Komplexität» eines Problems, d.h. wie steigt der Aufwand zur Lösung eines Problems, wenn man die Anzahl Parameter (die Problemgrösse) erhöht? Gutmütige Probleme zeigen einen Aufwandanstieg, der mit einer Potenz (z.B. quadratisch) mit der Problemgrösse steigt. Solche Probleme kann man mit klassischen Computern mit vernünftigem Zeitaufwand lösen.

Leider zeigen viele wichtige Problemstellungen ein exponentielles Komplexitätsverhalten: Der Rechenaufwand nimmt exponentiell mit der Problemgrösse zu, und bald ist eine Grenze erreicht, wo auch der schnellste klassische Computer für die Lösung eines Problems viel zu viel Zeit braucht. Solche praktischen Probleme sind zum Beispiel die Faktorisierung von Zahlen (was für die herkömmliche Verschlüsselung verwendet wird), das Packproblem (wie kann man eine maximale Anzahl von Päckchen verschiedener Dimensionen in ein vorgegebenes Volumen packen), das «Travelling-Salesman-Problem» (wie kann man eine Route, die durch gegebene Besuchsorte führen muss, in minimaler Zeit durchfahren, vgl. Use Case 2) oder die Simulation von Quantensystemen (speziell von Molekülen und ihren Wechselwirkungen mit anderen Molekülen).

### Noch unbestimmtes Rechenvermögen

Obwohl sich die Komplexitätstheoretiker:innen ihrer Verantwortung bewusst sind, endlich Ordnung in der Komplexitätswelt zu schaffen, ist es ihnen bisher nicht gelungen, die Grenzen des Rechenvermögens von Quantencomputern genau zu definieren. Man weiss heute nur, dass sowohl das Faktorisierungsproblem wie auch die Quantensystem-Simulation mit Quantencomputern nicht exponentiell mit der Problemgrösse zunehmen, sondern nur mit einer Potenz ansteigen. Hingegen ist für die wichtigsten Optimierungsprobleme nach wie vor ungeklärt, ob der Rechenaufwand von Quantencomputern wie für klassische Computer exponentiell mit der Problemgrösse zunimmt.

Die nebenstehende Grafik illustriert die heute von den meisten Komplexitätstheoretiker:innen vermutete Komplexitätskarte von Rechenproblemen. Der gezeigte Raum P-SPACE (Polynomraum)

besteht aus der Menge von Rechenproblemen, bei denen der Speicherbedarf mit konventionellen Rechnern nicht exponentiell – d.h. mit einem Polynom – ansteigt. Der Bereich NP (nichtdeterministische Polynomzeit) umfasst die Rechenprobleme, deren Lösung mit konventionellen Computern mit polynomialem Aufwand überprüft werden kann. Die Menge P beschreibt die Teilklasse von NP-Problemen, die mit konventionellen Computern auch mit polynomialem Aufwand gelöst werden können. Eine ganz besonders wichtige Klasse sind die Probleme, welche als NP-complete bezeichnet werden. Es wurde mathematisch bewiesen, dass das Auffinden einer einzigen polynomialen Lösung für eines der NP-complete Probleme auch für alle anderen funktionieren würde. Man vermutet aber, dass konventionelle Computer für die Lösung dieser Problemklasse exponentiellen Aufwand treiben müssten.

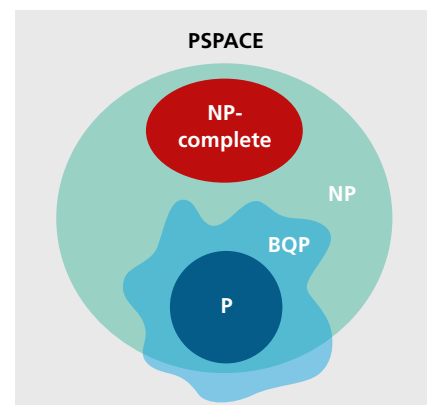


Illustration der wahrscheinlichen Komplexitätskarte von Rechenproblemen. Nach Scott Aaronson, *The Limits of Quantum*, Scientific American, 2008

Und wie steht es jetzt mit den Fähigkeiten der Quantencomputer? Diese Fähigkeit wird umschrieben mit der Klasse BQP («Bounded error Quantum Polynomial time»), welche alle Probleme beinhaltet, die von einem Quantencomputer in polynomialer Zeit gelöst werden können. Falls die Klasse BQP auch die eminent wichtigen NP-complete Probleme umfassen würde, könnte das die Einsatzmöglichkeiten der Quantencomputer enorm erweitern und der Technologie grosse praktische Wichtigkeit geben. Aber die Komplexitätstheorie konnte das bis heute nicht beweisen. Vielmehr wird vermutet, dass sich die NP-complete Probleme ausserhalb der BQP-Klasse befinden und die praktische Bedeutung von Quantencomputern deshalb beschränkt bleibt. Diese unsichere Situation ist mit der wolkigen Begrenzung in der Grafik illustriert.

**«Bei KI ist die Praxis der Theorie weit voraus: Das wissenschaftliche Verständnis befindet sich in einem Wettlauf mit der reinen Skalierung neuronaler Netze und der zum Training dieser Netze verwendeten Rechenleistung und Daten. Beim Quantencomputing ist es umgekehrt: Die Praxis befindet sich in einer Aufholjagd auf den Stand, den die Theorie seit Mitte der 1990er Jahre erreicht hat.»**

Scott Aaronson, *Quantum Computing between hope and hype*, 2024

# Quantencomputertechnologien «im Wettstreit»

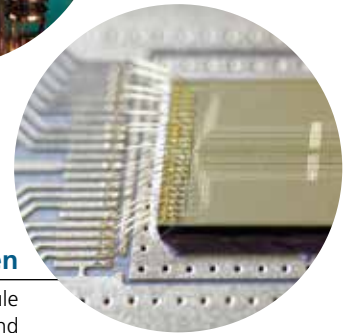
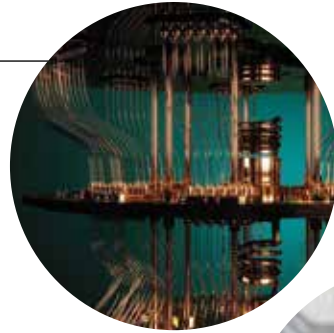
Derzeit bestehen weltweit rund 15 teils völlig verschiedene Ansätze, um dem Quantencomputing zum Durchbruch zu verhelfen. Alle diese Systeme bauen auf die Phänomene der Überlagerung und der Verschränkung von Qubits, und jedes davon hat Vorzüge und Defizite.

## Supraleitende Schaltkreise

Eine der am weitesten verbreiteten Arten sind supraleitende Qubits. Diese bestehen aus supraleitenden Mikrowellenschwingkreisen mit einer Frequenz im Bereich zwischen 4–8 GHz. Sie werden so tief wie möglich heruntergekühlt, bis zu wenigen Millikelvin über der (nicht erreichbaren) absoluten Nulltemperatur. Diese Qubits können einfach durch Mikrowellenpulse manipuliert werden und verlieren praktisch keine Energie, da der Strom ohne Widerstand fließt (Supraleitung).

Die extreme Kälte stabilisiert dabei die empfindlichen Quantenzustände in den Qubits, indem sie thermisches Rauschen stark reduziert.

Charakteristisch für diese Methode ist der «Kronleuchter», engl. «chandelier» genannte Kühltank (Misch-Kryostat), gekühlt und elektrisch verbunden mit unzähligen feinen Kabeln (vgl. Titelbild). Die Recheneinheit mit den Qubits befindet sich zuunterst und damit im kältesten Teil und wird mehrfach isolierend ummantelt. Auf diesen Typ Quantencomputer setzen u.a. IBM, Google, IQM oder Rigetti.



## Ionenfallen

Bei dieser Art von Quantencomputern werden Atome oder Moleküle eingefangen und – oft im Vakuum – durch elektromagnetische Felder und Laser manipuliert, um Informationen zu verarbeiten und zu speichern. Sie eignen sich für Präzisionsmessungen und Anwendungen, die grosse Stabilität und Kontrolle erfordern.

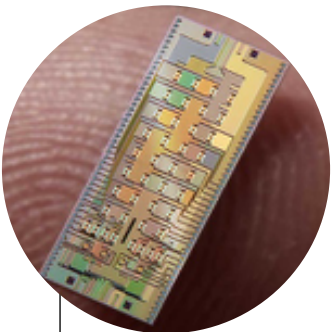
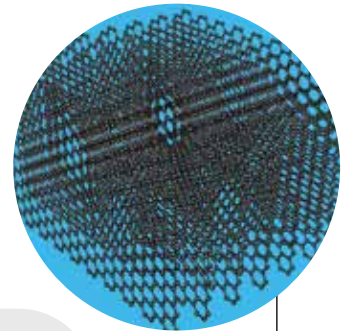
Akteure in diesem Bereich sind IonQ, AQT, Infineon, Oxford Ionics, Universal Quantum, Quantinuum, eleQtron etc.



## Neutrale (kalte) Atome

Beim Quantencomputer mit neutralen Atomen werden diese oft in einem Ultrahochvakuum mit Hilfe von vielen gebündelten Laserstrahlen, sogenannten optischen Pinzetten, berührungsfrei «eingefangen».

Diese Quantencomputer sind weniger empfindlich gegenüber elektrischen Streufeldern, was sie geeignet macht für Quantenprozessoren. Pasqal, Atom Computing, ColdQuanta, Planqc und QuEra sind Vertreter dieses Ansatzes. Bild: Eine Anordnung vieler neutraler Caesium-Atome in einem unsichtbaren Lasergitter.



Alternativen für den Bau eines funktionsfähigen Quantencomputers sind Elektronen auf Helium, Diamanten mit eingebauten Stickstoffatom-Fehlstellen (NV-Diamant) und der topologische Ansatz von Microsoft.

## Photonische Quantencomputer

Bei dieser Bauart werden Photonen (Lichtteilchen) verwendet, um Quanteninformationen zu speichern, zu übertragen und zu verarbeiten. Für Quanten-Grosscomputer sind photonische Qubits eine vielversprechende Alternative zu Quantencomputern auf Basis von gefangenen Ionen oder von neutralen Atomen, die eine kryogene oder lasergenerierte Kühlung erfordern. Allerdings müssen diese Quantencomputer Photonen «im Flug» verwenden, und ihre Programmierbarkeit ist deshalb verglichen mit anderen Architekturen eingeschränkt.

In diesem Bereich sind Unternehmen wie PsiQuantum, Quantum Computing Inc, ORCA Computing oder Xanadu tätig, wobei die technischen Ansätze sehr unterschiedlich sind.

## Quantenpunkte (QD, Quantum Dots)

Quantenpunkte sind künstliche Atome aus Halbleitermaterial, wo das Potenzial für die Ladungsträger nicht durch den Atomkern, sondern durch Spannungen an Metallelektroden auf der Halbleiteroberfläche definiert wird. Meist wird das QD-Qubit dann durch zwei magnetische Spinzustände definiert, welche durch unterschiedliche Anwendungen von Spin-Resonanz manipuliert werden.

Zu den Unternehmen, die hier tätig sind, gehören Diraq, Siqance und Quantum Motion.

## Nutzung verschiedener physikalischer Effekte für die Implementierung von Qubits

	Natürliche Qubits			Synthetische/künstliche Qubits			
	Ionenfallen	Neutrale Atome	Photonik	Supraleitende Qubits	Silizium-Quantenpunkte	Topologische Qubits	Stickstoff-Fehlstellen in künstlichen Diamanten
<b>Qubit Kohärenzzeit (Sek.)</b>	>1.000	1	_____	0.00005	0.03	k.A.	k.A.
<b>Güte</b>	99.9%	97%	_____	99.4%	~99%	k.A.	99.2%
<b>Anz. verbundener Qubits</b>	Hoch	Sehr hoch, tiefe individuelle Kontrolle	_____	Hoch	Sehr tief	k.A.	Tief
<b>Unternehmen</b>	IonQ, Quantinuum (früher Honeywell)	Inflektion (früher ColdQuanta), QuEra Computing, Atom Computing, Q-Block Computing Inc.	PsiQuantum, Xanadu, QC82, Quantum Computing Inc.	Google, IBM, Quantum Circuits, Rigetti und a.m.	HRL, Intel, SQC	Microsoft, Bell Labs	Quantum Brilliance, Xeeq, SaXonQ
<b>Vorteile</b>	<ul style="list-style-type: none"> <li>– Sehr stabil</li> <li>– Höchste erreichte Gattertreue</li> </ul>	Viele 2D-Qubits, ev. 3D	<ul style="list-style-type: none"> <li>– Linearoptische Gatter</li> <li>– Integriert auf dem Chip</li> </ul>	Kann physikalische Schaltungen auf dem Chip abbilden	Baut auf existierender Halbleitertechnologie auf	Reduziert Fehler signifikant	Kann bei Raumtemperatur betrieben werden
<b>Nachteile</b>	<ul style="list-style-type: none"> <li>– Langsamer Ablauf</li> <li>– Braucht viele Laser</li> </ul>	<ul style="list-style-type: none"> <li>– Schwierig, individuelle Qubits zu kontrollieren und zu programmieren</li> <li>– Störanfällig</li> </ul>	<ul style="list-style-type: none"> <li>– Jedes Programm braucht seinen eigenen Chip mit speziellen optischen Kanälen</li> <li>– Kein Speicher</li> </ul>	<ul style="list-style-type: none"> <li>– Muss auf nahe dem absoluten Nullpunkt abgekühlt werden</li> <li>– Grosse Variabilität in der Herstellung</li> <li>– Sehr empfindlich auf Störfaktoren</li> </ul>	<ul style="list-style-type: none"> <li>– Nur wenige verbunden</li> <li>– Muss auf beinahe absolute Nulltemperatur abgekühlt werden</li> <li>– Hohe Variabilität in der Fertigung</li> </ul>	Existenz noch nicht belegt	<ul style="list-style-type: none"> <li>– Schwierig, eine grosse Anzahl Qubits zu kreieren</li> <li>– Limitierte Berechnungskapazität</li> </ul>

Quelle: Science / Chris Monroe. Mit Genehmigung von Klea Dhimitri, Hamamatsu Photonics USA

## Vor- und Nachteile

Es besteht kein Zweifel daran, dass Quantencomputer in der Lage sind, wichtige Rechnungs- und Optimierungsaufgaben in nützlicher Zeit durchführen zu können. Allerdings muss noch ein enormer Aufwand für die Entwicklung von Hardware- und Software-Lösungen betrieben werden, bevor Quantencomputer tatsächlich alltags-tauglich sind und von vielen Programmierer:innen für die Lösung ihrer Probleme effizient eingesetzt werden können.

Bereits gibt es eine Reihe von Quantencomputer-Anwendungen, die teils explorativen, teils demonstrativen Charakter haben. Meist handelt es sich um Probleme, die klassische Computer nur mit sehr viel Rechenkapazität bzw. mit Näherungsmethoden lösen können. Durch die Weiterentwicklung von klassischen Algorithmen haben konventionelle Rechner aktuell dennoch die Nase vorn.

Dies liegt daran, dass die Nützlichkeit heutiger Quantensysteme durch das Auftreten von Fehlern limitiert ist. Um den fragilen Zustand eines komplett verschränkten Quantensystems mit Hunderten und Tausenden von Qubits aufrechtzuerhalten, muss ein Quantencomputer in der Praxis immer nach wenigen Dutzend Rechenschritten wieder fehlerkorrigiert werden, oder die ausgeführten Programme beschränken sich auf einige Hundert sequenzielle Operationen.

So wird aktuell auch intensiv daran geforscht, die für einen kommerziell einsetzbaren Quantencomputer auftretenden Fehler während des Betriebs durch eine eingebaute kontinuierliche Fehlerkorrektur zu eliminieren. Alternative Ansätze versuchen, durch eine Nachbereitung der Ergebnisse die nötige Qualität der Resultate zu erreichen. Wenn es gelingt, die zum Rechnen benutzten Quantenprozessoren weiter zu verbessern und zu skalieren, werden Quantencomputer bei wichtigen Problemstellungen schon in wenigen Jahren effizienter sein als herkömmliche Supercomputer.

## Die Nadel im Heuhaufen finden

Quantencomputer sind besonders dafür geeignet, komplexe Probleme in einem definierten Bereich zu lösen. Sie werden die heute am meisten benutzten Verschlüsselungsprotokolle (basierend auf der Faktorisierung von Primzahlen) wahrscheinlich innert weniger Stunden oder Minuten knacken können. Dies, weil die Komplexitätsmathematik bewiesen hat, dass die Faktorisierung von grossen Zahlen mit Quantencomputern nicht exponentiell mit der Zahlengrösse zunimmt. Das Knacken von Verschlüsselungsprotokollen wird vermutlich nicht eine Aufgabe sein, die jeder Heimcomputer bewältigen muss. Doch es gibt einen wachsenden Markt für IT-Sicherheitsfirmen, Regierungen, Geheimdienste und weitere Kreise. Das Problem der zu wenig sicheren Verschlüsselungsprotokolle ist erkannt, und es wird weltweit erfolgreich an quantensicheren Verschlüsselungen gearbeitet.



### Die Natur simulieren!

Der Physiker Richard Feynman hat es 1981 einprägsam ausgedrückt: Die Natur verhält sich nicht nach der «klassischen» Physik. Wer eine Simulation der (kleinsten Teilchen in der) Natur machen will, sollte besser die Quantenmechanik dafür nutzen. Dies war der Startschuss zum Quantencomputing.

**«Die Natur ist nicht klassisch, verdammt. Wenn man die Natur simulieren will, muss man es quantenmechanisch angehen.»**

**Richard Feynman** (1918–1988), Physik-Nobelpreisträger, spielt auf die «klassische, newtonsche Physik» an, welche quantenmechanische Vorgänge in der Natur nicht beschreiben kann.

Es hat sich als sehr schwierig herausgestellt, die Quantensysteme der Natur mit einem anderen, besser kontrollierbaren Quantensystem – dem Quantencomputer – zu simulieren. Die enormen Fortschritte bei der Isolierung, Manipulation und Erkennung einzelner Quantenobjekte, insbesondere im letzten Jahrzehnt, zeigen aber, dass diese physischen Implementierungen von «Quantensimulatoren» Realität – allerdings noch nicht marktreife Realität – geworden sind.

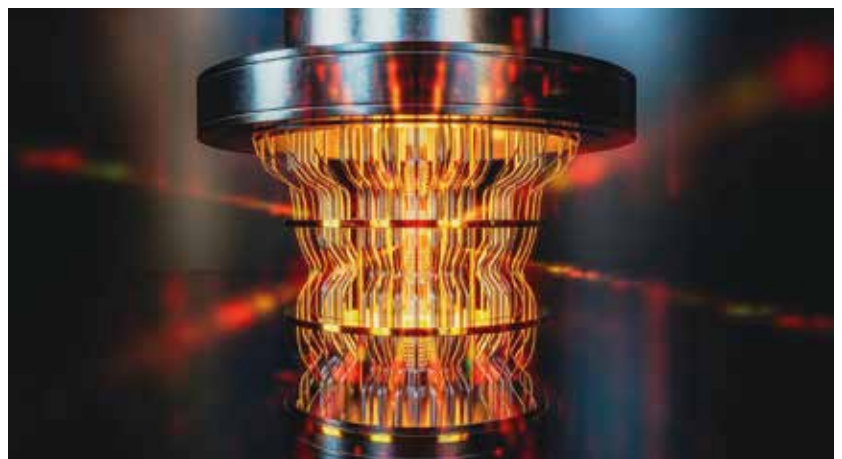
Viele Expert:innen erwarten, dass gerade diese Anwendungen der Quantencomputer-Technologie die Life Sciences nachhaltig verändern können: Wenn man die Eigenschaften von grossen Molekülen und ihre Interaktion mit ihrer chemischen Umgebung effizient berechnen kann, dann wird die «computational chemistry» auch für Moleküle grosser Komplexität bald Alltag.

Vielversprechende Kandidaten für neue Medikamente oder neue Werkstoffe können im Rechner bestimmt werden und benötigen viel weniger experimentellen Aufwand. Interaktionen von neuen Medikamenten im menschlichen Körper müssen nicht mehr mit unzähligen klinischen Studien untersucht werden – der «digitale Patient» könnte mit Quantencomputern mit zunehmender Verlässlichkeit simuliert werden.

### Enormer Aufwand

Um die Freiheit der Teilchen einzuschränken – nur schon deren Bewegung – müssen diese möglichst stillgelegt werden: durch extreme Kühlung. Dazu benötigt man flüssiges Helium, und leider kann Helium nicht aus der Luft extrahiert werden – es ist so leicht, dass die Schwerkraft es nicht in der Erdatmosphäre halten kann. Helium ist das einzige Edelgas, das als Bestandteil des Erdgases abgetrennt wird, d.h. Helium ist vor allem fossilen Ursprungs. Deshalb ist es unerlässlich, mit geschlossenen Kühlkreisläufen zu arbeiten, die das verwendete Helium so gut einschliessen, dass es auch während Jahren nicht aus dem Kühlkreislauf entweichen kann.

Für noch einfachere und weiter miniaturisierbare Quantencomputer könnte es langfristig auch wünschbar sein, dass auf die extreme Kühlung mit Helium verzichtet wird und dass die Systeme bei höheren Temperaturen – vielleicht sogar bei Raumtemperatur – funktionieren.



## Fehlertoleranz und Dekohärenz

Allerdings hat ein Quantencomputer aufgrund seiner physikalischen, wahrscheinlichkeitsgegebenen Eigenschaften eine unangenehme Konstante: Das Rechenresultat ist nicht eine präzise Zahl, sondern eine statistisch verteilte Antwort. Deshalb muss dieselbe Rechnung viele Male wiederholt werden, und das Endresultat muss dann durch statistische Analyse, im einfachsten Fall eine Mittelwertbildung, bestimmt werden. Aus diesem Grund ist schon von vornherein klar, dass ein Quantencomputer nicht für alle Rechenprobleme eingesetzt werden kann: Was nützt beispielsweise die extrem schnelle Berechnung eines grossen, komplexen Spreadsheets, wenn die Rechenresultate darin nicht präzise sind?

Die Resultate eines Quantencomputers sind also nicht präzise Zahlen, sondern müssen aufwändig aus statistischen Ergebnissen von vielen Quantenrechnungen aggregiert werden.

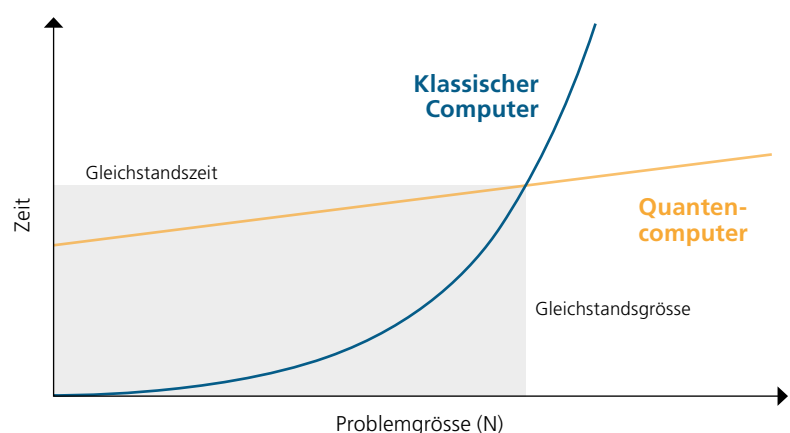
Darüber hinaus kann die Quantenverschränkung schnell aus dem Gleichgewicht geraten, falls nicht mehr alle Qubits perfekt miteinander verschränkt sind. Damit können sich Rechenfehler akkumulieren, und das Rechenresultat könnte vollständig falsch sein. Ausserdem können Umgebungsstörungen verschiedener Art zur Dekohärenz der entscheidenden Phänomene Superpositionierung und Verschränkung führen. Deshalb muss man Quantencomputer-Architekturen wenn immer möglich fehlertolerant implementieren: Ein logisches Qubit wird durch eine kleine Armada von 10 bis 20 physikalischen Qubits dargestellt. Diese physikalischen Qubits können dann dazu verwendet werden, mögliche Fehler und Inkonsistenzen in regelmässigen «Konsolidierungsoperationen» zu erkennen und zu eliminieren.

## Das Input/Output-Problem

Im Vergleich zu klassischen Computern können Quantencomputer schneller sein, wenn es um Probleme von grosser Komplexität bezogen auf relativ kleine Datenmengen geht. Theoretisch übertreffen Quantencomputer klassische Computer in puncto Rechengeschwindigkeit bei weitem, falls der Rechenaufwand in einem Quantencomputer für ein bestimmtes Problem nicht exponentiell mit der Problemgrösse zunimmt. Doch durch die in kurzen Abständen nötige Fehlerkorrektur – auch beim Speichern eines Datensatzes für eine Problemstellung – kann der Quantencomputer nur einen beschränkten Datensatz aufnehmen und abgeben (input/output, I/O). Ausserdem hängen die Resultate stark von der Eignung der angewandten Algorithmen ab. Bisläng gibt es nur wenige grundlegende Quantencomputer-Algorithmen, die wichtige Probleme effizient lösen können. Entsprechend macht sich der anfangs höhere Zeitaufwand beim Quantencomputer erst nach einer gewissen Zeit bezahlt.

Expert:innen gehen deshalb davon aus, dass sich auf absehbare Zeit Quantencomputer in erster Linie für «rechenintensive, datenarme» Probleme eignen. Bei der Verarbeitung von riesigen Datensätzen – wie zum Beispiel beim Trainieren von künstlicher Intelligenz – sind die herkömmlichen Supercomputer-Lösungen mit einer riesigen Anzahl von spezialisierten, parallel rechnenden Chips mit konventioneller Architektur dem Quantencomputing überlegen.

### Vergleich klassischer Computer und Quantencomputer: Berechnungszeit bei steigender Problemgrösse



Für Probleme kleiner Grösse ist ein klassischer Computer unschlagbar, denn er errechnet das Resultat in einer Serie von Schritten exakt. Wird das Problem aber sehr gross, braucht er plötzlich exponentiell mehr Zeit für diese vielen Schritte (blaue Linie). Ein Quantencomputer legt hingegen einen linearen, flach ansteigenden Leistungsverlauf hin: Er rechnet parallel, aber ungenau und muss immer wieder Fehlerkorrekturen vornehmen. Für eine in unseren Augen sehr leichte Aufgabe wie  $2 + 2$  braucht er zwar seine Zeit, doch die Lösung einer riesigen Aufgabe dauert dafür nicht viel länger. Für grosse Probleme ist der Quantencomputer deshalb im Vorteil. Ebenbürtig sind sich die beiden Computer dort, wo sie gleich lange für ein Problem der Grösse  $N$  haben (Schnittpunkt).  
(Quelle: ETH Zürich, Microsoft, ACM / P. Seitz)

«Wer von der Quantenmechanik nicht verwirrt ist, hat sie nicht wirklich verstanden.»

Niels Bohr (1885–1962),  
Physik-Nobelpreisträger

# Die Schweiz, ein Quantencomputing-Hub

Das Wettrennen um die vordersten Plätze in Sachen Quantencomputer wird immer härter. Die Schweiz hat auf diesem Gebiet jahrzehntelang international bedeutende Pionierarbeit geleistet und ein grosses Netzwerk an Quantenforschungs-Know-how aufgebaut. Im Mai 2021 hat sich die Schweiz von den Verhandlungen der bilateralen Verträge mit der EU zurückgezogen. Als Folge davon beschloss die Europäische Kommission, die Schweiz bei Horizon Europe zu einem nicht assoziierten Drittland herabzustufen. Aufgrund der strategischen Bedeutung der grossen Quantenprogramme der EU sind die Schweizer Forschenden von der Mitarbeit in diesen Programmen nun ausgeschlossen. Dies bedeutet eine Schwächung des Forschungsstandorts Schweiz auf dem Quantengebiet, denn wenn wir nicht mehr direkt mit den Besten auf diesem Gebiet zusammenarbeiten dürfen, erfahren wir nur mit Verzögerung von den vielversprechendsten neuen Forschungsansätzen und disruptiven Durchbrüchen.



Quelle: SWISSNEX, 2023

Es ist kaum möglich, die vielen Dutzend Akteure in der dynamischen Landschaft der Schweizer Quantentechnik abzubilden. Die Karte zeigt die wichtigsten Forschungs- und Innovationszentren für Quantentechnik, sowohl öffentliche als auch private.

Die Schweiz ist dennoch gut positioniert, um sich als eines der führenden Ökosysteme für Quantentechnologien weiterzuentwickeln. Ihre Stärken liegen in der partnerschaftlichen Zusammenarbeit, dem langfristigen Engagement in der Forschung, den Weltklasse-Universitäten und der Spitzentechnologie, die bereits zu industriellen Top-Produkten schweizerischer Provenienz geführt hat. Last but not least hat die Schweiz als Sitz des europäischen Kernforschungszentrums CERN einen direkten Zugang zur Grundlagenforschung, um ein tiefes Verständnis des Aufbaus von Materie zu erlangen. Dabei sind auch neue Einsichten im Bereich Quantenphysik zu erwarten.

Eine grosse Bedeutung dürfte Quantencomputern in der Schweiz nur schon deshalb zukommen, weil die Wertschöpfung hierzulande zum grossen Teil in Sektoren stattfindet, die für die neuen Quantencomputer-Berechnungen prädestiniert sind. Über 55% der Schwei-

zer Exporte fallen auf die Kategorien Pharma und Chemie. Banken und Versicherungen sind ebenfalls sehr wichtig, weil hier Aufgaben aus der Optimierung, dem Risikomanagement und der Betrugsprävention anfallen, die mit Quantencomputern effizient gelöst werden können.

Beispiel Chemie: Wollte man z.B. die chemischen Eigenschaften des Koffeinmoleküls genau berechnen, würde man 10 hoch 48 Bits (1048 = eine Oktillion, also eine 1 mit 48 Nullen) benötigen – was derzeit mit einem konventionellen Computer unmöglich ist. Mit einem Quantencomputer sind idealerweise gerade mal 160 Qubits dazu nötig. Die Tatsache, dass IBM, einer der führenden Hersteller, einen Teil seiner Quantencomputer-Grundlagenforschung in der Schweiz angesiedelt hat, spricht für die vielen positiven Faktoren, die in der Schweiz zusammenkommen.

## National Initiatives (Headquarters)

- 1 Swiss Quantum Initiative
- 2 NCCR SPIN
- 3 NCCR SwissMAP

## University Centers and Research Hubs

- 1 The Quantum Center at ETH Zurich
- 2 The Basel Quantum Center and Swiss Nanoscience Institute at the University of Basel
- 3 The Center for Quantum Science and Engineering (QSE) at EPFL
- 4 The ETHZ-PSI Quantum Computing Hub
- 5 The Quantum Center at University of Geneva
- 6 Swiss Federal Laboratoires for Materials Science and Technology (EMPA)
- 7 Università della Svizzera italiana (USI)
- 8 University of Applied Sciences and Arts Northwestern Switzerland (FHNW)
- 9 Lucerne University of Applied Sciences and Arts (HSLU)

## Ecosystem Builders and Accelerators

- 1 Switzerland Innovation Park Basel
- 2 Switzerland Innovation Park Innovaere
- 3 Switzerland Innovation Park West EPFL
- 4 QuantumBasel
- 5 QAI Ventures
- 6 CERN
- 7 The Geneva Science and Diplomacy Anticipator (GESDA)
- 8 Verve Ventures

## Private Companies and Centers

- 1 IBM Research
- 2 ID Quantique
- 3 Basel Precision Instruments
- 4 Zurich Instruments
- 5 Qnami
- 6 Swiss Centre for Electronics and Microtechnology (CSEM)
- 7 Swisssphotonics
- 8 Mieaex
- 9 QZabre
- 10 Ligintec
- 11 Enlightra
- 12 Terra Quantum
- 13 IonQ

## Government

- 1 Swissnex HQ

## Other

- 1 World Economic Forum (WEF)

## Prädestinierte Anwendungen

### Quantencomputing: Ein wachsendes Ökosystem und industrielle Anwendungen



#### Pharma, Medizin:

- Entdeckung neuer Medikamente
- Digitale Zwillinge
- Präzisionsmedizin



#### Chemie:

- Neue Katalysatoren
- Energieoptimierung
- Präzisionslandwirtschaft



#### Automation, Logistik:

- Streckenplanung
- Verkehrsoptimierung
- Lieferketten-Management



#### Finanzindustrie:

- Portfolio-/Risiko-Mgmt
- Kreditwürdigkeitsprüfung
- Betrugsprognose

Quelle: McKinsey, Dec. 2021

Bei welchen Aufgaben können Quantencomputer tatsächlich ihre Stärken ausspielen? Die Vermutung ist: Bei Quantensystem-Simulation, bei Optimierungsaufgaben (z.B. Ressourcen/Verkehrsplanung), bei Risikoabschätzungen (z.B. Bank- und Finanzbereich). Vermutlich die grösste Bedeutung werden Quantencomputer in der Berechnung von Quantenvorgängen selbst haben: Pharmazeutische und chemische Produkte können wohl in absehbarer Zeit exakt simuliert, ihre therapeutische Wirksamkeit und ihre wahrscheinlichen Nebenwirkungen zuverlässig vorausgesagt werden.

### Welchen Stellenwert hat die Quantentechnologie in der Schweiz?

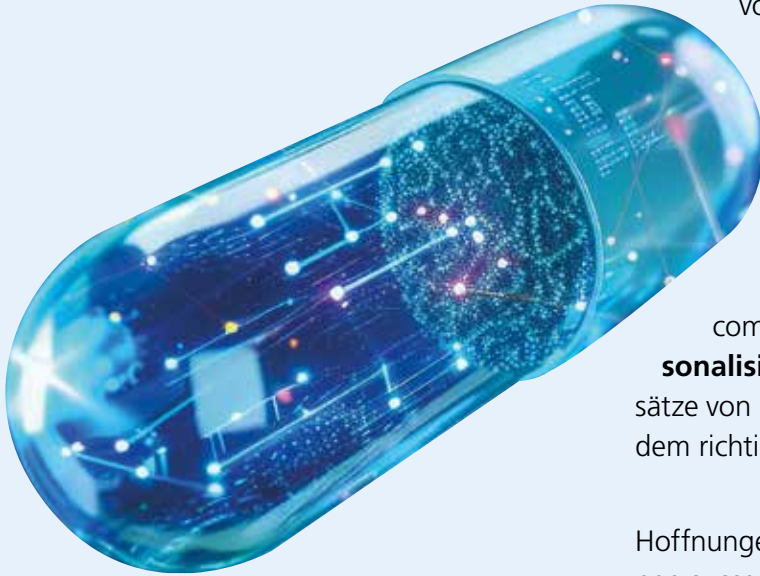


#### Dr. Andreas Fuhrer

Manager Superconducting Quantum Hardware  
IBM Research Europe – Zurich

«Die Quantentechnologie wurde durch enorme Fortschritte in der Material- und (Nano)-technologie vorangetrieben. Das ermöglicht uns heute, die Quanteneigenschaften von Materialien und Bauelementen mit noch nie dagewesener Genauigkeit zu kontrollieren. Der hohe Grad an technologischer Innovation, der eine extrem saubere, präzise und zuverlässige Herstellung von Komponenten erfordert, und die voraussichtlich revolutionären Anwendungsmöglichkeiten in den Bereichen der Kommunikation, dem Finanzwesen, der Chemie und bei Prozessoptimierungen machen Quantencomputing und Quantentechnologie generell zu einem sehr attraktiven Markt für Schweizer Unternehmen – von Start-ups über etablierte KMU bis hin zu grossen, globalen Unternehmen.»

## Use Case 1: Chemie, Biologie, Pharmazie



Beim computergestützten Wirkstoffdesign und der molekularen Modellierung können selbst Supercomputer nur relativ ungenaue Resultate liefern. Der Quantencomputer könnte jahrelange Labortests überflüssig machen und Entdeckungen stark beschleunigen.

**Die Entwicklung von Medikamenten oder Impfstoffen** dauert in der Regel Jahre – noch. Quantencomputer und KI könnten zusammen die Schlüsselprozesse der Synthese und Wirksamkeitsprüfung massiv verkürzen: indem das Verhalten von Molekülen und chemische Reaktionsabläufe bald genau simuliert werden können und der Aufwand für chemisch-biologische Tests zurückgeht. Dies dürfte die Entwicklung von Behandlungen und Arzneimitteln beschleunigen, nachhaltiger und präziser machen. Die Entwicklung neuartiger biologischer Produkte basierend auf **Simulationen der Proteinfaltung** könnte dank dem Quantencomputer zum Durchbruch gelangen. Ebenso in der **personalisierten und Präzisionsmedizin**, wo riesige Datensätze von Genomen und Therapieresultaten in kurzer Zeit nach dem richtigen Ansatz durchkämmt werden könnten.

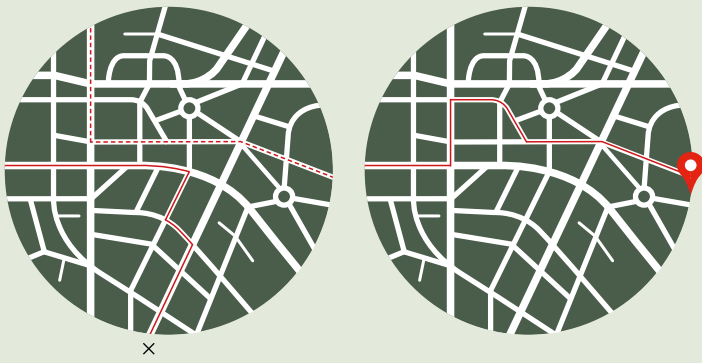
Hoffnungen in den Quantencomputer legen die Entwickler:innen ausserdem bei der Entwicklung **neuer Medikamente aus niedermolekularen Verbindungen**. Sie haben den Vorteil, durch Zellmembranen zu schlüpfen und interzelluläre Ziele erreichen zu können. Auch die Entwicklung **widerstandsfähigerer Nutzpflanzen, aggregierter Nahrungsmittel** oder das **Recycling von Kunststoffabfällen durch Bakterien** könnte mithilfe des Quantencomputers einen Entwicklungsschub erfahren. Ein Beispiel: Die überaus komplexe, dreidimensionale Faltung eines Proteins bestimmt, wie und ob es seine Funktionen im Körper richtig ausführen kann. Die Vorhersage der räumlichen Struktur (Faltung) eines Eiweisses auf der Basis der Aminosäuresequenz ist deshalb heute so etwas wie der heilige Gral der Biochemie. Da der Quantencomputer gut darin ist, andere Quantensysteme abzubilden, sollte er hier seine Stärken ausspielen können.



**«Wenn Sie die Art und Weise ändern, wie Sie die Dinge betrachten, ändern sich die Dinge, die Sie betrachten.»**

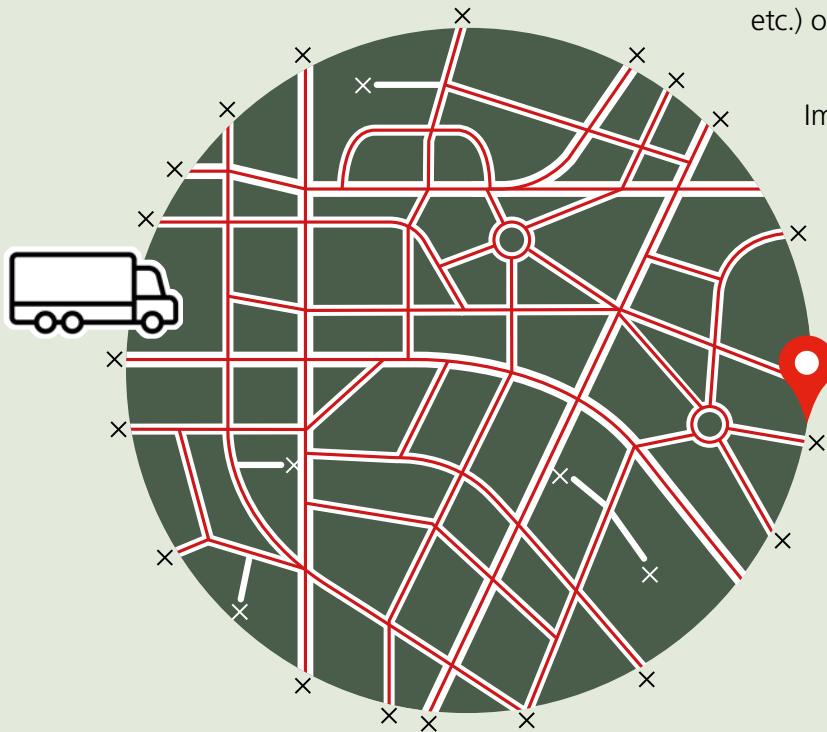
Nobelpreisträger **Max Planck** (1858–1947)

## Use Case 2: Logistik, Handel, Produktion



Ein konventioneller Computer sucht für einen Camion die Route von einem Ausgangsort ins Ziel (rote Nadel). Dazu fährt er nacheinander sämtliche möglichen Strassen ab, bis er entweder eine Verbindung findet (Bild rechts) oder feststellt, dass er am falschen Ort landet (Bild links).

Die Logistik ist heute weltweit verflochten und komplexer denn je. Um die Wirtschaftlichkeit zu erhöhen und gleichzeitig Energiespar- und Klimaziele zu erreichen, könnten Quantencomputer einen wichtigen Beitrag leisten. Zum Beispiel in der nachhaltigen Optimierung der Fahrstrecken von Containerschiffen und Lastwagen, bei der Reduktion von Leergut-Rücktransporten, bei der Verteilung, Lagerung und Frischhaltung von Lebensmitteln oder bei der Überbrückung der letzten Liefermeile mit dem cleveren Einsatz von Transportern, Fahrradboten oder Drohnen. In ähnlicher Weise könnten Waren- und Energieströme für Produktionsabläufe (Rohstoffgewinnung, Landwirtschaft etc.) optimiert werden.



Im Vorteil sind Quantencomputer immer dann, wenn es gilt, bei plötzlichen Unterbrechungen oder Lieferengpässen neue Mittel und Wege zu finden. Das «Turbo-Management» solcher Disruptionen ist für den mit sehr vielen Informationen gleichzeitig arbeitenden Quantencomputer eine leichte Aufgabe im Vergleich zu konventionellen Rechnern.

Der Quantencomputer hingegen berechnet alle Routen gleichzeitig und findet blitzschnell den richtigen Weg.

**«Quantencomputer haben für eine bestimmte, aber sehr wichtige und praktisch relevante Klasse von kombinatorischen Optimierungsproblemen einen grundlegenden Vorteil gegenüber klassischen Computern».**

**Jens Eisert** und sein Team untersuchten 2024 das «Problem des Handelsreisenden», nämlich  $N$  Referenzpunkte (Städte etc.) auf dem kürzesten Weg zu besuchen. Bei steigender Anzahl  $N$  explodiert auf einem klassischen Computer die Rechenzeit (z.B. 10 Städte: über 3,6 Mio. mögliche Wege) – nicht so auf einem Quantencomputer.

# Erstaunliche (Quanten-)Computergeschichte

Die Verschränkung von Qubits wird erstmals definitiv bewiesen. **Alain Aspect, John F. Clauser und Anton Zeilinger** erhalten dafür den Nobelpreis in Physik.



2022

D-Wave stellt den ersten kommerziellen Quantencomputer mit 128 Qubits vor.



2011

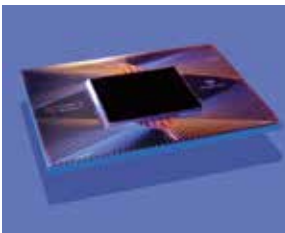
Der erste Quanten-Annealer-Rechner wird demonstriert.

2007

Gründung der Swiss Quantum Initiative SQI.

2023

Google beansprucht mit seinem Sycamore Chip die erste «Quantenüberlegenheit» erreicht zu haben. Dass sein Quantencomputer schneller als jeder konventionelle Rechner ist, stimmt jedoch nur für ein ganz bestimmtes Problem.



2019

IBM startet mit «Quantum Computing as a Service» (Cloud-Zugang).

2016

Der erste 12-Qubit-Quantencomputer von Forschern aus Kanada und den USA wird entwickelt.

2006

**William Shockley, John Bardeen und Walter Brattain** erfinden den Transistor. Er ist die Grundlage der modernen Mikroelektronik und der Digitalisierung unserer Welt.

1947



1964



**John Stewart Bells** Ungleichung besagt, dass sie in der klassischen Physik nie verletzt wird – bei Systemen mit Quantenverschränkung aber schon. Damit war Einsteins Überzeugung «Gott würfelt nicht!» (d.h. die Physik kennt keine Zufälle oder Wahrscheinlichkeiten) theoretisch widerlegt. Den Beweis dazu erbrachten erst die Nobelpreisträger von 2022.



**Hertha Spöner** leistet umfassende Beiträge zur Anwendung quantentheoretischer Methoden in der Atom- und Molekülphysik. Mit Hedwig Kohn bestätigt sie in Experimenten eine Reihe von quantenmechanischen Vorhersagen.

1960

**Erich Hückel** formuliert die Grundlagen der Quantenchemie.



**Alexander Holevo** zeigt, dass  $n$  Qubits mehr Informationen speichern können als  $n$  klassische Bits.

1973

1940



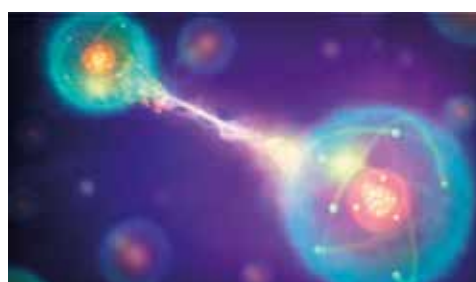
**Erwin Schrödinger** formuliert eine quantenmechanische Wellengleichung zur Berechnung der Wahrscheinlichkeitsverteilung beim Transport von Quantenteilchen und ihrer möglichen energetischen Zustände.

**Werner Heisenberg, Max Born und Pascual Jordan** veröffentlichen die erste konzeptuell autonome und logisch konsistente Formulierung der Quantenmechanik auf der Basis von Matrix-Rechnungen.



1925

**Albert Einstein, Boris Podolsky und Nathan Rosen** lösen das nach ihnen benannte EPR-Paradoxon: In der Theorie sollte es möglich sein, eine «Messung» an einem Teilchen durchzuführen, ohne es direkt zu stören, indem diese Messung an einem entfernten, verschränkten Teilchen durchgeführt wird. Bewiesen werden konnte diese Tatsache erst rund 90 Jahre später.



1935

**Albert Einstein** beschreibt das Photon und den Photoeffekt. Seine revolutionäre Lichtquantenhypothese besagt, dass Licht aus Portionen (Quanten) von Energie besteht. 1921 erhält er dafür den Physik-Nobelpreis.

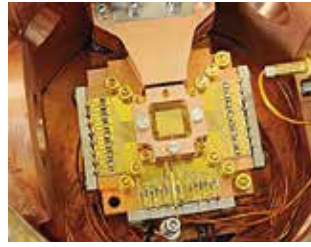
Die erste Fünf-Photonen-Verschrankung wird von **Jian-Wei Pan** demonstriert.



2004

### Das Rennen um funktionsfähige Quantencomputer

Erster Ionenfallen-Quantencomputer, erste Idee des adiabatischen Quantencomputers.



2000

1996

**Lov Grover** zeigt den ersten Quanten-Suchalgorithmus. **David DiVincenzo** definiert die Kriterien für einen Quantencomputer. **Seth Lloyd** stellt einen Algorithmus vor, der quantenmechanische Systeme simulieren kann.

**Emanuel Knill, Raymond Laflamme und Gerard Milburn** begründen das lineare optische Quantum computing.



**Lieven Vandersypen (I) and Matthias Steffen** publizieren die erste Quantencomputer-Implementierung von Shors Algorithmus, indem sie die Zahl 15 auf ihre Primzahlen 3 und 5 faktorisieren.

2001

### Entwicklung von Quantenalgorithmen



1994/95

1981

### Quantencomputing im Labor

**Richard Feynman** schlägt vor, Quantenphänomene mit einem Computer zu berechnen, der einzelne Quantenzustände nutzt/manipuliert, und schlägt vor, wie ein Quantencomputer funktionieren könnte.

**David Deutsch** formuliert die Idee des universellen Quantencomputers und die Prinzipien von Quantencomputing-Algorithmen. Deshalb wird er von vielen als Begründer des Quantencomputings angesehen.

1985

**Peter Shor** veröffentlicht einen Algorithmus, mit dem ein künftiger Quantencomputer grosse ganze Zahlen schnell faktorisieren und damit gängige Verschlüsselungstechniken knacken können sollte. Er schlägt auch die ersten Schemata zur Quantenfehlerkorrektur vor.

Zusammen mit **Paul Benioff** und **David Deutsch** versucht **Richard Feynman**, Quantenmechanik und Informatik zu verbinden. Das heisst: mit Quantensimulatoren bestimmte Probleme zu simulieren, die mit einem klassischen Supercomputer nicht modelliert werden können.



1982

1992

**Ben Schumacher** entwickelt die ersten Qubits und um die Jahrtausendwende erste Q-Dots.



### Theoretische Grundlagen des Quantencomputings

**Max Plancks** formuliert die Hypothese, dass Energiezustände quantisiert sind. Für die Begründung der Quantentheorie erhält er 1919 den Nobelpreis für Physik.

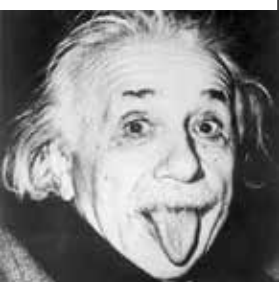


1900

### Erfindung der binären Datenverarbeitung

1725 tüftelt **Basile Bouchon** aus Lyon an einer Arbeitserleichterung beim Textilweben. Mit einer gelochten Papierrolle, die seine Mechanik abtastet, gelingt es ihm, Stoffmuster zu programmieren. Weiterentwickelt verhilft **J.-M. Jacquard** den – 300 Jahre später immer noch verwendeten! – Lochkarten mit dem automatisierten Webstuhl zum Durchbruch.

18. Jhdt.



1905

Um 1890 verwenden **Herman Holleriths** Electromechanical Tabulating Machines für die US-amerikanische Volkszählung bereits Millionen von Lochkarten als Verarbeitungsspeicher. Dafür braucht es ein ganzes System aus Stanz-, Lese- und Sortiergeräten.

Um 1820 erfindet **Charles Babbage** die Difference Engine und 1837 die erste universelle Rechenmaschine, die Analytical Engine, beide rein mechanisch betrieben. Die Adlige **Ada Lovelace** schreibt für die Analytical Engine als erster Mensch ein Computerprogramm.



19. Jhdt.

Bilder: Wikipedia

# Abstract

Statt wie herkömmliche Computer rechnen Quantencomputer nicht mit digital codierten Bits (0 und 1), sondern mit einer Überlagerung der Quantenzustände mehrerer Quanten-Bits (Qubits). In diesen Systemen, die aus wechselwirkenden (verschränkten) nanoskaligen Teilchen wie Photonen und Elektronen bestehen, herrschen die Gesetze der Quantenmechanik. Quantencomputer haben dadurch das bisher ungekannte Potenzial, hochkomplexe Rechnungs- und Optimierungsaufgaben schnell zu lösen, benötigen jedoch noch erhebliche Entwicklungsarbeit in Hardware und Software, um alltagstauglich zu werden.

Aktuelle Anwendungen von Quantencomputern zeigen, dass klassische Computer mit optimierten Algorithmen derzeit noch effizienter sind, da die Fehleranfälligkeit und Instabilität von Quantencomputern ihre Nützlichkeit einschränkt. Grosse Fortschritte in der Material- und Nanotechnologie haben die Quantentechnologie erheblich vorangebracht, was eine immer präzisere Kontrolle der Quanteneigenschaften ermöglicht.

Die neue Technologie verspricht neue, revolutionäre Anwendungsmöglichkeiten. Die Schweiz verfügt über exzellente Quantenforschung an Universitäten, Forschungsinstitutionen sowie Start-ups. Da einige der prognostizierten Anwendungsfelder von Quantencomputern – u.a. Kommunikation, Finanzen, Chemie, Pharma, Logistik und Prozessoptimierung – mit etablierten Stärken der Schweizer Industrie und Wirtschaft korrelieren, könnte unser Land in den kommenden Jahren bedeutend von dieser Entwicklung profitieren.

Die Schweizerische Akademie der Technischen Wissenschaften SATW ist das bedeutendste Netzwerk von Expert:innen im Bereich Technikwissenschaften in der Schweiz und in Kontakt mit den höchsten Schweizer Gremien für Wissenschaft, Politik und Industrie. Das Netzwerk besteht aus gewählten Einzelmitgliedern, Mitgliedsgesellschaften sowie Expertinnen und Experten. Die SATW identifiziert im Auftrag des Bundes industriell relevante technologische Entwicklungen und informiert Politik und Gesellschaft über deren Bedeutung und Konsequenzen. Als einzigartige Fachorganisation mit hoher Glaubwürdigkeit vermittelt sie unabhängige, objektive und gesamtheitliche Informationen über die Technik als Grundlage für eine fundierte Meinungsbildung. Die SATW fördert auch das Technikinteresse und Technikverständnis in der Bevölkerung, insbesondere bei Jugendlichen. Sie ist politisch unabhängig und nicht kommerziell.

## Impressum

**Autoren:** Prof. Peter Seitz, Caspar Türler

**Lektorat:** Translingua AG

**Bilder:** Adobe Foto Stock | Wikimedia Commons

**Gestaltung:** Andy Braun

**Druck:** Egger Druck

Oktober 2024

# Glossar

---

## Absolute Nulltemperatur

Der absolute Nullpunkt, also die physikalisch tiefstmögliche Temperatur, liegt noch ungefähr drei Grad niedriger als die Weltraumtemperatur, nämlich bei minus 273.15 Grad Celsius oder 0 Grad Kelvin. Bis auf wenige millionstel Grad wird diese niedrigste Temperatur in den Labors der Tieftemperaturphysiker:innen erreicht. Im Labor ist es möglich, mit einem Heliumgemisch Temperaturen bis etwa 1 Millikelvin zu erzeugen, also bis ca. ein Tausendstel Grad Celsius an den absoluten Nullpunkt zu gelangen.

## Atom

Der antike Philosoph Leukippos von Milet und sein Schüler Demokritos von Abdera entwickelten im 5. Jh. vor Chr. die Vorstellung, die Welt bestehe aus einer Anzahl kleinster, unteilbarer Teilchen, den Atomen (griech: átomos, «das Unzerlegbare»). Heute kennen wir 118 Atome im Periodensystem der chemischen Elemente und woraus sie bestehen: aus den Protonen und Neutronen, die den Kern bilden, sowie den Elektronen, die diesen Kern umgeben. Protonen und Neutronen sind wiederum zusammengesetzt aus Up-Quarks und den Down-Quarks. Das Atom mit seiner Wolke aus Elektronen ist etwa 100'000-mal grösser als sein Kern. Hätte der Atomkern die Grösse eines Apfels, dann besäße das Atom einen Durchmesser von etwa 10 km. Obwohl wir Materie als fest wahrnehmen, sind die einzelnen Atome weitgehend leer. Auch ein Diamant besteht hauptsächlich aus leerem Raum!

## Bit

Kofferwort aus binary digit, binäre Zahl, hat den Wert 1 oder 0. Masseinheit für die Datenmenge digital repräsentierter (gespeicherter, übertragener) Daten.

## Quant, Quanten (engl. Quantum)

Von lat. quantum «wie gross? wie viel?», kleinste bekannte Mengeneinheit. Ein Teilchen, das in einen endlichen Raum eingesperrt ist, kann nur eine beschränkte Zahl von Energiezuständen einnehmen – die Energie des Teilchens ist quantisiert. Ein Quant ist deshalb ein Objekt, das durch einen Zustandswechsel in einem System mit diskreten (quantisierten) Werten einer physikalischen Grösse erzeugt wird. Quantisierte Grössen werden im Rahmen der Quantenmechanik und davon inspirierten Teilgebieten der theoretischen Physik wie der Quantenelektrodynamik beschrieben. Beispielsweise liefert Licht einer festen Frequenz Energie in Form von Quanten, die «Photonen» genannt werden. Jedes Photon dieser Frequenz hat die gleiche Energiemenge, und diese Energie kann nicht in kleinere Einheiten zerlegt werden. Jedes Atom im Universum beinhaltet Quanten. Nur schon der menschliche Körper besteht durchschnittlich aus rund  $7 \times 10^{27}$  Atomen, also 7 Quadrilliarden (oder 7 Milliarden Milliarden) Atomen.

## Quantenrevolution 1.0

Technologien, die auf dem Verständnis der grundlegenden quantenmechanischen Effekte beruhen, v.a. die Quantisierung von Energie, die Existenz von reinen Energiepaketen (Photonen), die Wechselwirkung von Photonen und Elektronen, Quanten-Tunnelphänomene oder dem Spin. Damit können so wertvolle Produkte wie Transistoren und Chips, Halbleiter-Sensoren, LEDs, Laserdioden, Photovoltaikzellen und Magnetresonanz-Tomografen realisiert werden.

## Quantenrevolution 2.0

Technologien, die zusätzliche Quantenphänomene nutzen, v.a.

- Superposition (der Zustand eines Quantenobjektes kann nur als Wahrscheinlichkeitsverteilung beschrieben werden, bei einer Messung die verschiedenen Basiszustände vorzufinden);
- Interferenz (Quantenzustände können so manipuliert werden, dass bestimmte Endzustände ausgeschlossen werden können, d.h. ihre Wahrscheinlichkeit wird auf ein Minimum subtrahiert);
- Verschränkung («Entanglement», wobei die Komponenten eines verschränkten Quantensystems instantan voneinander wissen, d.h. die Komponenten-Messresultate sind streng korreliert). Damit können Produkte mit enorm gesteigerter Leistungsfähigkeit realisiert werden, wie Quantencomputer, absolut abhörsichere Quantenkommunikations-Netzwerke, Quantensensoren mit einer um mehrere Grössenordnungen erhöhten Empfindlichkeit oder Quantenmikroskopie.

## Qubit: Quantum Bit

Ein System aus zwei Zuständen, das nur durch die Quantenmechanik korrekt beschrieben werden kann und das nur zwei durch Messung sicher unterscheidbare Zustände hat. Das Qubit spielt dabei die analoge Rolle zum klassischen Bit bei herkömmlichen Computern: Es dient als kleinstmögliche Speichereinheit und definiert gleichzeitig ein Mass für die Quanteninformation. Heutige Qubits haben eine Grösse zwischen  $10^3$  Meter (= 1 Millimeter) und  $10^{-10}$  Meter (= 0.1 Nanometer oder 1 Zehnmilliardstel eines Meters).

# Referenzen

---

Bloch, Immanuel et. al: Agenda Quantensysteme 2030. BMBF, 2021, <https://zurl.co/crkm>

Ensslin, Klaus: «Die Schweiz kann eine Schlüsselrolle spielen». Über wissenschaftliche Durchbrüche und die Rolle der Schweiz in der Quantenforschung, ETHU, Dezember 2022, <https://zurl.co/dy2w>

IBM Institute for Business Value: Exploring quantum computing use cases for logistics, <https://zurl.co/1VMq>

Kagermann, Henning et al.: Innovationspotenziale der Quantentechnologien der zweiten Generation. Acatech, Berlin/München 2020, <https://zurl.co/x3nW>

Meyer, Florian: «For very small problem sizes a classical computer is faster», ETHZ, 26.5.2023, <https://zurl.co/YOMk>

Quantencomputing. In: SATW Technology Outlook 2023, <https://zurl.co/NdmU>

Rucherhaupt, Ulf: Erst verschränkt und dann auch noch herumgeschubst. Forscher setzen Atome als Qubits ein (FAZ, 29.04.2022), <https://zurl.co/8ar6>

Speicher, Christian: Grösser als die Erfindung des Feuers? Quantencomputer – der Hype nimmt ungesunde Züge an, NZZ, 27.1.2023, <https://zurl.co/hnPN>

SRF Wissen: Quantencomputer, was kommt auf uns zu?, <https://zurl.co/9V3M>

Switzerland: A Hub for Quantum (Swissnex 2023), <https://zurl.co/Bgj7>

The Quantum Insider (2023): Types of Quantum Computers, <https://zurl.co/rGvO>

Walliman, Dominic: The animated map of Quantum Computing, <https://zurl.co/tBWW>

Zeuch, D.: Quantencomputing für KMU. Wissenstransferstudie des Peter-Grünberg-Institute for Quantum Computing Analytics, Jülich, Dezember 2022, <https://zurl.co/uVTn>

Zitat Aaronson: Quantum Computing between hope and hype, <https://zurl.co/r2pH>

Zitat Bohr: Schockierende Quantenwelt, <https://zurl.co/X2Gv>

Zitat Deutsch: Proso AI, <https://zurl.co/B4rW>

Zitat Eisert: «Where quantum computers can score.» ScienceDaily, <https://zurl.co/7qee>

Zitat Feynman: Nature, Quantum Simulation, <https://zurl.co/0mPR>

Zitat Fuhrer: Quantentechnologie – was kommt auf die Tech-Industrie zu? Swissmem, Jan. 2024, <https://zurl.co/r9L9>

Zitat Planck: Rostocker Physiktag, <https://zurl.co/BFDQ>