# Quantencomputer einfach erklärt

QUBITS, ALGORITHMEN UND DER STAND DER TECHNIK

Drei mal fünf ist fünfzehn. Dass ein Rechner das herausfindet, ist keine Meldung wert, und trotzdem ging Ende 2001 eine Nachricht um die Welt, weil eine Gruppe um Isaac Chuang bei IBM in Kalifornien die Zahl 15 in ihre Faktoren 3 und 5 zerlegt hatte. Gerechnet hatten dabei sieben Atomkerne in einem eigens gebauten Molekül, gesteuert mit Radiowellen, und sie hatten es auf eine Weise getan, die nur die Quantenmechanik erlaubt [1]. Es war die erste experimentelle Umsetzung von Shors Algorithmus zum Zerlegen von Zahlen, so winzig das Beispiel auch war.

Seitdem sind aus sieben Qubits bei den führenden Systemen gut hundert bis mehrere Hundert geworden, bei einzelnen Anlagen sogar über tausend. Was ist ein Quantencomputer eigentlich, wie rechnet er, und wie weit ist die Technik heute? Und muss man sich um die Verschlüsselung beim Online-Banking Sorgen machen? Darum geht es auf dieser Seite, mit nur wenigen Formeln.

## Was ist ein Quantencomputer?

Ein Quantencomputer ist ein Rechner, der Information nicht in gewöhnlichen Bits speichert, sondern in Quantensystemen, und der dabei drei Eigenheiten der Quantenphysik ausnutzt: die Überlagerung von Zuständen, die Verschränkung mehrerer Teilchen und die Interferenz, bei der sich Möglichkeiten gegenseitig verstärken oder auslöschen. Die Idee stammt aus den frühen 1980er-Jahren. Richard Feynman fragte 1982, ob man die Natur, die nun einmal quantenmechanisch funktioniert, nicht am besten mit einem Rechner simuliert, der selbst nach Quantenregeln arbeitet [2]. David Deutsch beschrieb drei Jahre später, wie ein universeller Quantencomputer im Prinzip aussehen müsste [3].

Wichtig ist, was ein Quantencomputer nicht ist. Er ist kein schnellerer Laptop, auf dem Tabellen oder Spiele besser laufen würden. Für die allermeisten Aufgaben ist ein gewöhnlicher Computer schneller, billiger und zuverlässiger. Quantencomputer lohnen sich nur bei bestimmten Problemen, für die es geschickte Quantenalgorithmen gibt. Auch deshalb wird über Quantencomputer so viel übertrieben.

## Vom Bit zum Qubit

Ein gewöhnliches Bit ist ein Schalter: an oder aus, 1 oder 0. Ein Qubit kann ebenfalls 0 oder 1 sein, es kann sich aber auch in einer Überlagerung aus beidem befinden. In der Schreibweise der Quantenmechanik sieht das so aus:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1 \tag{1}$$

Die Zahlen $\alpha$ und $\beta$ heißen Amplituden. Ihre Betragsquadrate geben an, mit welcher Wahrscheinlichkeit man bei einer Messung 0 oder 1 erhält. Anschaulich kann man sich jeden möglichen Zustand eines Qubits als Punkt auf einer Kugel vorstellen, mit der 0 am Nordpol und der 1 am Südpol (Abb. 1). Nur: Wer misst, bekommt immer nur eine einzige Antwort, 0 oder 1, und die Überlagerung ist danach verloren. Was Überlagerung physikalisch bedeutet, zeigt besonders anschaulich das Gedankenexperiment von Schrödingers Katze.

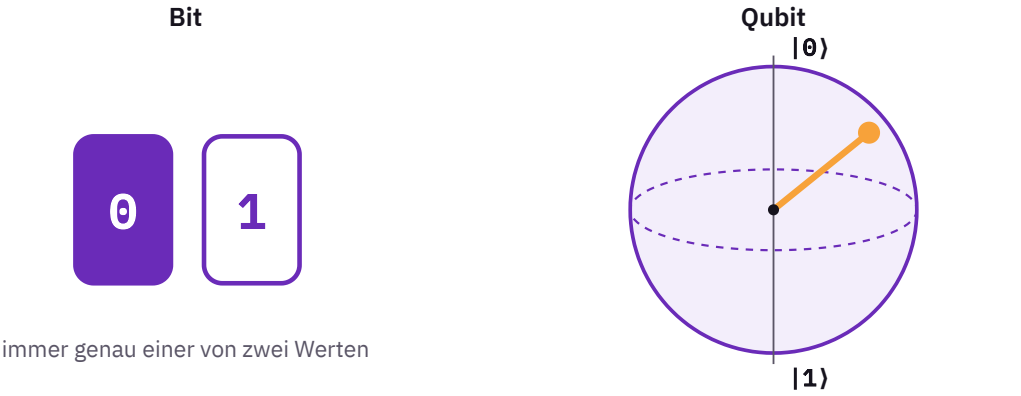


**Abb. 1:** Ein Bit kennt zwei Zustände, ein Qubit unendlich viele, die sich als Punkte auf einer Kugel darstellen lassen. Gemessen wird trotzdem immer 0 oder 1. Eigene schematische Darstellung.

Interessant wird es, wenn mehrere Qubits zusammenkommen. Zwei Qubits haben vier mögliche Grundzustände (00, 01, 10, 11), und ihr gemeinsamer Zustand braucht vier Amplituden. Bei drei Qubits sind es acht, und allgemein gilt:

$$\text{Anzahl der Amplituden bei } n \text{ Qubits} = 2^n \tag{2}$$

Schon bei 50 Qubits sind das rund eine Billiarde Zahlen. Wollte man sie auf einem normalen Computer speichern, mit 16 Byte pro Zahl, bräuchte man etwa 18 Petabyte Speicher, und mit jedem weiteren Qubit verdoppelt sich der Bedarf (eigene Rechnung). Hinzu kommt die Verschränkung: Die Qubits lassen sich nicht mehr einzeln beschreiben, sondern nur noch als Ganzes. Mehr über diese seltsame Verbindung steht im Artikel über Quantenteleportation und Verschränkung.

Daraus wird oft geschlossen, ein Quantencomputer probiere einfach alle Lösungen gleichzeitig durch. So einfach ist es nicht, denn am Ende liefert die Messung ja nur ein einziges Ergebnis, und das wäre ohne einen Trick ein zufälliges. Der Trick heißt Interferenz.

Ein guter Quantenalgorithmus ordnet die Rechnung so an, dass sich die Amplituden falscher Antworten gegenseitig auslöschen und die der richtigen sich verstärken. Erst dann ist die eine Messung am Ende auch die gesuchte Antwort.

## Wie rechnet ein Quantencomputer?

Gerechnet wird mit sogenannten Quantengattern, kleinen, genau dosierten Eingriffen in einzelne Qubits oder Paare von Qubits, je nach Bauart mit Mikrowellenpulsen, Laserlicht oder Radiowellen. Eine Folge solcher Gatter bildet einen Quantenschaltkreis. Welche Probleme sich damit schneller lösen lassen als auf einem klassischen Rechner, ist eine Frage der Algorithmen, und davon gibt es bisher nur eine Handvoll wirklich bedeutender.

Der bekannteste stammt von Peter Shor aus dem Jahr 1994. Er zerlegt große Zahlen in ihre Primfaktoren, und zwar dramatisch schneller als jedes bekannte klassische Verfahren: Der Aufwand wächst nur wie eine Potenz der Stellenzahl, während er bei den besten klassischen Verfahren schneller als jede Potenz zunimmt [4]. Lov Grover zeigte 1996, wie ein Quantencomputer einen Eintrag in einer ungeordneten Liste von $N$ Einträgen in etwa $\sqrt{N}$ Schritten findet [5]. Bei einer Million Einträgen sind das knapp tausend Schritte statt im Mittel einer halben Million. Das ist ein großer, aber kein exponentieller Gewinn. Als besonders vielversprechend gilt außerdem Feynmans ursprüngliche Idee, Moleküle und Materialien zu simulieren, etwa für die Chemie oder die Entwicklung neuer Werkstoffe.

### Wie Shors Algorithmus die 15 zerlegt

Das Experiment von 2001 lässt sich auf dem Papier nachvollziehen. Shors Verfahren macht aus dem Zerlegen eine andere Aufgabe: Man wählt eine Zahl, etwa 7, und sucht die Periode der Reihe $7^1$, $7^2$, $7^3$, … , jeweils mit Rest bei Division durch 15:

$$7^x \bmod 15: \quad 7, 4, 13, 1, 7, 4, \ \ldots \quad \Rightarrow \quad r = 4 \tag{3}$$

Die Reihe wiederholt sich nach vier Schritten, die Periode ist also $r = 4$. Diese Periode zu finden, ist der Teil, den der Quantencomputer übernimmt, und hier spielt er seine Stärke aus, weil sich Perioden mit Interferenz sehr effizient herausfiltern lassen. Der Rest ist Schulmathematik. Aus der Periode berechnet man $7^2 = 49$ und bestimmt den größten gemeinsamen Teiler von 48 und 15 sowie von 50 und 15:

$$\mathrm{ggT}(7^2 - 1, 15) = 3, \quad \mathrm{ggT}(7^2 + 1, 15) = 5 \tag{4}$$

Heraus kommen genau die beiden Faktoren. Für die 15 braucht man natürlich keinen Quantencomputer. Bei Zahlen mit Hunderten Stellen aber wird die Periodensuche für klassische Rechner hoffnungslos, für einen ausreichend großen Quantencomputer dagegen nicht [4]. *Rechnung nach dem Verfahren in* [4],[1].

## Warum ist ein Quantencomputer so schwer zu bauen?

Das größte Hindernis ist die Empfindlichkeit der Qubits. Jede kleine Störung aus der Umgebung, ein Wärmequant, ein Streufeld, eine Erschütterung, kann eine Überlagerung zerstören. Physiker nennen diesen Vorgang Dekohärenz, und er ist auch der Grund, warum wir im Alltag keine Katzen sehen, die zugleich lebendig und tot sind (mehr dazu bei Schrödingers Katze). Supraleitende Qubits werden deshalb bis auf rund ein Hundertstel Grad über dem absoluten Nullpunkt gekühlt, Ionen in Vakuumfallen festgehalten und mit Lasern gesteuert.

Gegen die unvermeidlichen Fehler hilft die Quantenfehlerkorrektur. Man verteilt die Information eines einzigen, sogenannten logischen Qubits auf viele physikalische Qubits und prüft laufend, ob sich irgendwo ein Fehler eingeschlichen hat, ohne die eigentliche Information auszulesen. Das funktioniert aber nur, wenn die einzelnen Qubits gut genug sind. Sind sie es nicht, macht jedes zusätzliche Qubit die Sache schlimmer statt besser.

Genau diese Schwelle hat Google mit dem Chip Willow Ende 2024 überschritten. Auf 105 supraleitenden Qubits wurden logische Qubits in immer größeren Gittern kodiert, von 3 × 3 über 5 × 5 bis 7 × 7. Mit jeder Vergrößerung sank der Fehler ungefähr auf die Hälfte, genauer um den Faktor 2,14, und das logische Qubit hielt seine Information 2,4-mal länger als das beste einzelne Qubit auf dem Chip (Abb. 2) [6]. Klingt nach wenig, doch damit war erstmals klar belegt, dass größere Codes den Fehler systematisch und deutlich senken, so wie es die Theorie verlangt.

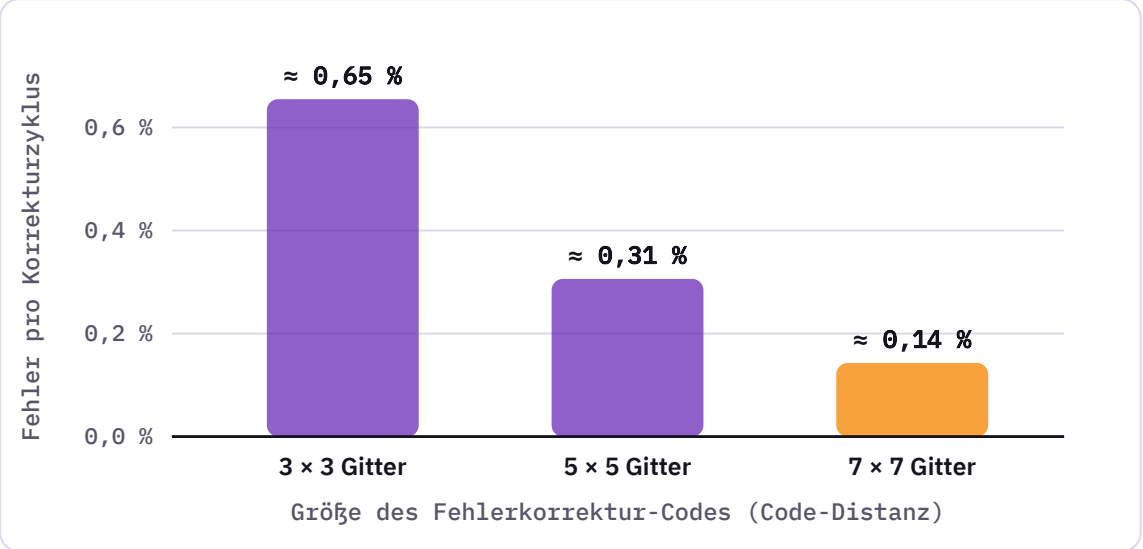


**Abb. 2:** Fehler eines logischen Qubits pro Korrekturzyklus auf Googles Willow-Chip. Der Wert für das 7 × 7-Gitter (0,143 %) ist gemessen, die beiden anderen sind mit dem gemessenen Faktor Λ = 2,14 zurückgerechnet. Eigene Darstellung nach [6].

Gebaut werden Qubits heute auf sehr unterschiedliche Weise. Google und IBM setzen auf winzige supraleitende Schaltkreise, deren Quantenverhalten John Clarke, Michel Devoret und John Martinis in den 1980er-Jahren erstmals nachwiesen, wofür sie 2025 den Physik-

Nobelpreis erhielten [7]. Wie solche Qubits aus Metall funktionieren und warum sie so tief gekühlt werden müssen, beschreibt der Artikel über Festkörper-Quantencomputer. Andere Firmen und Forschungsgruppen arbeiten mit einzelnen Ionen in elektrischen Fallen, mit neutralen Atomen, die von Laserstrahlen festgehalten werden, oder mit Lichtteilchen. Welche Technik sich durchsetzt, ist offen.

## Was können Quantencomputer heute?

2019 meldete Google, sein Prozessor Sycamore mit 53 Qubits habe eine speziell konstruierte Aufgabe, das Ziehen von Stichproben aus zufälligen Quantenschaltkreisen, in 200 Sekunden erledigt, für die ein Supercomputer nach Googles Schätzung 10 000 Jahre gebraucht hätte [8]. Die Schätzung wurde bald angezweifelt, unter anderem von IBM, und klassische Rechenverfahren holten in den folgenden Jahren deutlich auf. Mit Willow wiederholte Google 2024 den Vergleich in größerem Maßstab: unter fünf Minuten auf dem Quantenchip gegenüber einer geschätzten Rechenzeit von $10^{25}$ Jahren auf einem der schnellsten Supercomputer [9].

Solche Vergleiche zeigen, dass Quantencomputer etwas können, was klassische Rechner kaum nachbilden. Einen praktischen Nutzen haben diese Testaufgaben allerdings nicht, sie wurden gerade so gewählt, dass sie für klassische Rechner möglichst schwer sind. Im Oktober 2025 legte Google deshalb nach: Mit einem Verfahren namens „Quantum Echoes“ berechnete Willow eine physikalische Messgröße, deren Ergebnis sich im Prinzip auf einem anderen Quantencomputer oder im Experiment überprüfen lässt, nach Googles Schätzung rund 13 000-mal schneller als mit den besten klassischen Methoden. Auch das war noch eine Testaufgabe, und eine erste Anwendung auf echte Moleküle ist nach Angaben der Forscher noch nicht jenseits dessen, was klassische Rechner schaffen [10]. Ob und wann Quantencomputer bei Aufgaben mit echtem Nutzen klassische Rechner verlässlich schlagen, ist unter Fachleuten weiter umstritten. Die Zahl der Qubits allein sagt dabei wenig. IBM stellte schon im Dezember 2023 mit Condor einen Prozessor mit 1121 Qubits vor, setzte für den praktischen Einsatz aber auf den kleineren Heron mit 133 Qubits und deutlich niedrigeren Fehlerraten [11].

## Ist meine Verschlüsselung in Gefahr?

Hier liegt der Grund, warum Geheimdienste und Banken das Thema so aufmerksam verfolgen. Viele Verschlüsselungsverfahren im Internet, allen voran RSA, beruhen darauf, dass sich das Produkt zweier großer Primzahlen praktisch nicht zerlegen lässt. Im Kleinen sieht man das Prinzip schon an 875 747. Dass diese Zahl gleich 547 · 1601 ist, prüft jeder Taschenrechner in einer Sekunde, die Zerlegung selbst zu finden, ist dagegen mühsam. Bei Zahlen mit über 600 Dezimalstellen, wie sie bei RSA mit 2048 Bit verwendet werden, ist sie für klassische Computer aussichtslos. Shors Algorithmus würde genau diese Annahme aushebeln.

Wie groß ein Quantencomputer dafür sein müsste, wurde immer wieder neu abgeschätzt. Craig Gidney von Google kam 2025 zu dem Ergebnis, dass weniger als eine Million physikalische Qubits genügen könnten, um eine 2048-Bit-Zahl in weniger als einer Woche zu zerlegen, vorausgesetzt, jedes Qubit arbeitet mit einer Fehlerrate von etwa 0,1 Prozent [12]. Ein noch nicht begutachteter Entwurf vom Februar 2026 kommt unter denselben Annahmen sogar mit weniger als 100 000 physikalischen Qubits aus [13]. Ähnlich sieht es bei den elliptischen Kurven aus, die ebenfalls in vielen Internetverbindungen und in Kryptowährungen stecken: Im März 2026 schätzte Google, dass weniger als 500 000 physikalische Qubits genügen könnten, um 256-Bit-Schlüssel in wenigen Minuten zu brechen [14]. Auch das ist weit mehr, als irgendein heutiger Quantencomputer bietet, und für das Online-Banking von heute besteht keine akute Gefahr. Die Abschätzungen sind in den letzten Jahren aber deutlich gesunken.

Warten kann man trotzdem nicht. Wer heute verschlüsselte Daten abfängt und speichert, kann sie womöglich in einigen Jahren entschlüsseln. Für Informationen, die lange geheim bleiben sollen, ist das ein reales Risiko. Deshalb hat die US-Standardbehörde NIST im August 2024 die ersten Verfahren der Post-Quanten-Kryptographie standardisiert, die auch Quantencomputern standhalten sollen, darunter ML-KEM für den Schlüsselaustausch und ML-DSA für digitale Signaturen [15]. Im März 2025 wählte sie mit HQC ein weiteres Verfahren aus [16]. In Deutschland empfiehlt das Bundesamt für Sicherheit in der Informationstechnik in seiner Technischen Richtlinie TR-02102-1, rechtzeitig auf solche Verfahren umzustellen, und zwar vorzugsweise in Kombination mit klassischen Verfahren, als sogenannte hybride Lösung [17]. Google selbst hat sich vorgenommen, seine Systeme bis 2029 umzustellen [18].

## Quantencomputer in Deutschland

Auch hierzulande kann man inzwischen auf echten Quantencomputern rechnen. Im Juni 2021 nahmen Fraunhofer und IBM in Ehningen bei Stuttgart ein IBM Quantum System One mit 27 Qubits in Betrieb [19]. Am selben Ort eröffnete IBM im Oktober 2024 sein erstes Quanten-Rechenzentrum außerhalb der USA [20]. Das Forschungszentrum Jülich betreibt seit 2019 mit JUNIQ eine Nutzer-Infrastruktur für Quantencomputing und nahm 2022 dort unter anderem einen Quanten-Annealer mit mehr als 5000 Qubits in Betrieb, eine Spezialmaschine für Optimierungsaufgaben [21]. Und über die Quantencomputing-Initiative des Deutschen Zentrums für Luft- und Raumfahrt förderte der Bund an den Standorten Hamburg und Ulm in einer ersten Phase den Bau von Quantencomputern durch die Industrie, mit rund 740 Millionen Euro über vier Jahre [22]. Seit Sommer 2026 läuft die Folgephase QCI Next [23].

Von der Zahl 15 bis zu einer Maschine, die verschlüsselte Nachrichten knacken könnte, ist es noch ein weiter Weg. Aber anders als 2001 zweifeln heute nur noch wenige daran, dass er sich gehen lässt. Wer wissen will, worauf all das beruht, findet die Grundlagen im Artikel Was sind Quanten?, die Rolle des Spins, mit dem 2001 gerechnet wurde, bei Fermionen und Bosonen.

## Quellen


1. L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, I. L. Chuang: *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance.* In: Nature 414 (2001), S. 883–887, doi:10.1038/414883a.
2. R. P. Feynman: *Simulating physics with computers.* In: International Journal of Theoretical Physics 21 (1982), S. 467–488, doi:10.1007/BF02650179.
3. D. Deutsch: *Quantum theory, the Church–Turing principle and the universal quantum computer.* In: Proceedings of the Royal Society of London A 400 (1985), S. 97–117, doi:10.1098/rspa.1985.0070.
4. P. W. Shor: *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* In: SIAM Journal on Computing 26 (1997), S. 1484–1509, doi:10.1137/S0097539795293172 (erste Fassung 1994).
5. L. K. Grover: *A fast quantum mechanical algorithm for database search.* In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing (1996), S. 212–219, doi:10.1145/237814.237866.
6. Google Quantum AI and Collaborators: *Quantum error correction below the surface code threshold.* In: Nature 638 (2025), S. 920–926, doi:10.1038/s41586-024-08449-y.
7. Nobel Prize Outreach: *The Nobel Prize in Physics 2025* (J. Clarke, M. H. Devoret, J. M. Martinis). nobelprize.org/prizes/physics/2025.
8. F. Arute u. a.: *Quantum supremacy using a programmable superconducting processor.* In: Nature 574 (2019), S. 505–510, doi:10.1038/s41586-019-1666-5.
9. H. Neven: *Meet Willow, our state-of-the-art quantum chip.* Google, 9. Dezember 2024, blog.google.
10. Google Quantum AI and Collaborators: *Observation of constructive interference at the edge of quantum ergodicity.* In: Nature 646 (2025), S. 825–830, doi:10.1038/s41586-025-09526-6; Erläuterung: Google Research, *A verifiable quantum advantage*, 22. Oktober 2025, research.google.
11. HPCwire: *IBM Quantum Summit: Two New QPUs, Upgraded Qiskit, 10-Year Roadmap and More.* 4. Dezember 2023, hpcwire.com.
12. C. Gidney: *How to factor 2048 bit RSA integers with less than a million noisy qubits.* Preprint, Mai 2025, arXiv:2505.15917.
13. P. Webster u. a.: *The Pinnacle Architecture: Reducing the cost of breaking RSA-2048 to 100 000 physical qubits using quantum LDPC codes.* Preprint, Februar 2026, arXiv:2602.11457.

14. R. Babbush, H. Neven: *Safeguarding cryptocurrency by disclosing quantum vulnerabilities responsibly.* Google Research, 31. März 2026, research.google; Whitepaper: arXiv:2603.28846.
15. National Institute of Standards and Technology: *FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA).* 13. August 2024, doi:10.6028/NIST.FIPS.203, doi:10.6028/NIST.FIPS.204, doi:10.6028/NIST.FIPS.205.
16. National Institute of Standards and Technology: *Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process* (NIST IR 8545). 11. März 2025, nist.gov.
17. Bundesamt für Sicherheit in der Informationstechnik: *Technische Richtlinie TR-02102-1. Kryptographische Verfahren: Empfehlungen und Schlüssellängen.* bsi.bund.de, abgerufen am 10. Oktober 2026.
18. H. Adkins, S. Schmieg: *Quantum frontiers may be closer than they appear.* Google, 25. März 2026, blog.google.
19. Fraunhofer IAF: *Curtain up: Fraunhofer and IBM unveil quantum computer.* 15. Juni 2021, iaf.fraunhofer.de.
20. IBM: *First IBM Quantum Data Center in Europe Opens.* 1. Oktober 2024, newsroom.ibm.com.
21. Forschungszentrum Jülich: *Europe's First Annealing Quantum Computer with More Than 5,000 Qubits Launched at Jülich.* Pressemitteilung, 17. Januar 2022, fz-juelich.de.
22. Deutsches Zentrum für Luft- und Raumfahrt: *The DLR Quantum Computing Initiative (QCI).* dlr.de, abgerufen am 10. Oktober 2026.
23. Deutsches Zentrum für Luft- und Raumfahrt: *QCI Next.* qci.dlr.de/en/next, abgerufen am 10. Oktober 2026.

## Zitiervorschlag

**quanten.de: *Quantencomputer einfach erklärt.* Stand: Oktober 2026. URL: https://quanten.de/quantencomputer.html (PDF: https://quanten.de/pdf/quantencomputer.pdf)**

Texte und Abbildungen © 2026 quanten.de. Nutzung mit Quellenangabe und Link gern, kommerzielle Nutzung nach Absprache: info@quanten.de

**Weiterlesen:** Was sind Quanten? · Quantenteleportation · Schrödingers Katze · Die Unschärferelation

Online-Fassung mit aktualisierten Quellen: https://quanten.de/quantencomputer.html