

QUANTUM COMPUTING IN DER CLOUD

Wegweisende Symbiose

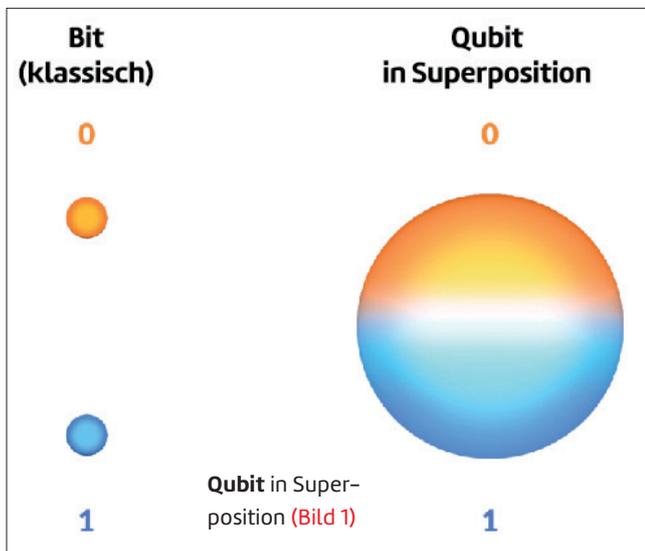
Leistungsstarke Quantum-Computing-Rechenressourcen in der Cloud werden die Art und Weise revolutionieren, wie wir Probleme angehen und Lösungen entwickeln.

Quantum Computing als eine neue und faszinierende Disziplin innerhalb der Informatik hat in den letzten Jahren zunehmend an Bedeutung gewonnen und die Aufmerksamkeit von Forschern, Unternehmen und der breiten Öffentlichkeit auf sich gezogen. Dieser Bereich repräsentiert nicht nur eine Evolution, sondern vielmehr eine Revolution in der Art und Weise, wie man klassische Probleme der Informatik angeht und löst. Die Entwicklungen im Quantum Computing könnten sogar einen Paradigmenwechsel für die gesamte IT-Branche bedeuten. In diesem Artikel soll zunächst ein kurzer Blick auf die Hintergründe des Quantum Computing geworfen werden, um die Grundlagen dieses aufstrebenden Feldes zu verstehen und die bahnbrechenden Möglichkeiten zu entdecken, die es bietet.

Grundbausteine von Quantum Computing

Zu den fundamentalen Einheiten im Bereich des Quantum Computing gehören Quantenbits (kurz Qubits). Die Qubits unterscheiden sich grundlegend von Bits in einem klassischen Computer. Um die einzigartige Natur von Qubits zu verstehen, ist es entscheidend, einen Einblick in die Welt der Quantenmechanik zu gewinnen, da Qubits auf den Prinzipien dieser physikalischen Theorie beruhen.

Im Gegensatz zu herkömmlichen Bits, die in einem klassischen Computer entweder den Zustand 0 oder den Zustand 1 annehmen können, können Qubits aufgrund eines Phänomens namens Quantenüberlagerung (englisch: Quantum Superposition, siehe auch Kasten [Quantenüberlagerung](#)) nicht nur 0 oder 1, sondern auch gleichzeitig eine Kombination dieser beiden Zustände annehmen. Dies bedeutet, dass ein Qubit nicht eine klare Identität hat, sondern sich in einem Zustand der Superposition befindet (siehe [Bild 1](#)).



Quantenüberlagerung

Quantenüberlagerung (englisch: Quantum Superposition) ist ein fundamentales Prinzip der Quantenmechanik, das besagt, dass Quantenobjekte wie zum Beispiel Photonen, Elektronen, Ionen und Atome gleichzeitig in mehreren Zuständen existieren können, bis sie gemessen werden. Dies steht im Kontrast zur klassischen Physik, in der ein System sich in einem eindeutigen Zustand befindet. Es bedeutet, dass Quantenobjekte wie Qubits (Quantenbits) in einem Quantencomputer nicht nur den Zustand 0 oder 1 aufweisen, sondern eine lineare Kombination beider Zustände.

Quantenüberlagerungsphänomene werden für parallele Berechnungen in Quantencomputern, für sichere Kommunikation in Quantennetzwerken und für komplexe Probleme in Quantenalgorithmen verwendet.

perposition, siehe auch Kasten [Quantenüberlagerung](#)) nicht nur 0 oder 1, sondern auch gleichzeitig eine Kombination dieser beiden Zustände annehmen. Dies bedeutet, dass ein Qubit nicht eine klare Identität hat, sondern sich in einem Zustand der Superposition befindet (siehe [Bild 1](#)).

Der Qubit-Status in Quantenüberlagerung wird mathematisch als normalisierter komplexer Zustandsvektor dargestellt:

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Dabei gilt: $|\alpha|^2 + |\beta|^2 = 1$

Die Ausdrücke α und β stellen hier als komplexe Zahlen sogenannte Wahrscheinlichkeitsamplituden für die jeweiligen Qubit-Zustände 0 und 1 dar. Werte von α und β geben an, wie „nahe“ das Qubit jeweils am Zustand 0 oder 1 ist.

$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ ist ein Vektor, der ein Qubit im Zustand 0 repräsentiert, und $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ ist ein Vektor, der für ein Qubit im Zustand 1 steht. Das sind sogenannte Basiszustände, die in der für die Quantenmechanik üblichen Dirak-Notation [1] wie folgt geschrieben werden:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Damit können alle möglichen Quantenzustände eines Qubits noch einfacher ausgedrückt werden:

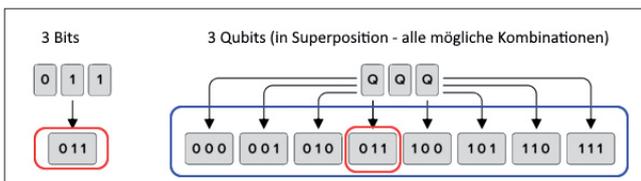
$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha |0\rangle + \beta |1\rangle$$

oder für einen beliebigen Ψ -Vektor:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

Ein Qubit kann somit eine Kombination aus 0 und 1 sein, und dies nicht als diskrete Werte, sondern als kontinuierliche Wahrscheinlichkeitsverteilung. Man kann sich das bildlich auch als Gedankenexperiment mit der berühmter Schrödinger-Katze [2] vorstellen, bei dem die Katze gleichzeitig „tot“ und „lebendig“ ist, oder anhand einer sich in der Luft drehenden Münze, bei der die beiden Seiten der rotierenden Münze „verschmelzen“, bis zu dem Zeitpunkt, an dem man die Kiste mit der Katze öffnet beziehungsweise die Münze in der Hand landet und aufgedeckt wird. Damit wird ein endgültiger Zustand „gemessen“ – und die Katze für „tot“ oder „lebendig“ erklärt beziehungsweise Kopf oder Zahl einer Münze festgestellt, was jeweils dem Zustand 0 oder 1 entsprechen kann. Eine verbreitete Fehlvorstellung liegt dabei in der Sichtweise, ein Qubit wäre immer im Zustand 0 oder im Zustand 1 (es sei bloß unbekannt), und man erfahre erst bei einer Messung, in welchem Zustand es sich befindet. Das ist aber nicht korrekt. Ein Qubit in der Superposition befindet sich in einer linearen Kombination der Zustände 0 und 1. Bei der Messung wird das Qubit dazu gezwungen, sich für eine der möglichen Varianten zu „entscheiden“. Anders ausgedrückt: Die Messung eines Qubits ist ein drastischer Prozess, der ursprünglichen Superposition-Zustand des gemessenen Qubits zerstört, und dann kollabiert es zu einem der möglichen Zustände.

Im Superposition-Zustand ist ein Qubit also in der Lage, alle möglichen Zustände parallel zu repräsentieren. Diese Pa-



Qubit-Daten-Repräsentation (Bild 2)

rallelität ermöglicht es Quantencomputern, eine enorme Anzahl von Berechnungen gleichzeitig durchzuführen, was bei bestimmten Problemstellungen zu erheblichen Geschwindigkeitsvorteilen führen kann. Dieser Effekt ist in Bild 2 ersichtlich – während bei „klassischen“ drei Bits für alle möglichen Kombinationen $3 \times 8 = 3 \times 2^3 = 24$ Bits nötig wären, kann man das Gleiche mit nur drei Qubits in Superposition abbilden. Weiterdenkend wären statt vier überlagerten Qubits schon $4 \times 2^4 = 64$ Bits nötig und so weiter. Wie man an diesen einfachen Beispielen sieht, ist ein Qubit-Rechner 2^N -fach effektiver als ein klassischer.

Während die Leistung eines klassischen Computers linear wächst, verläuft bei einem Quantencomputer die Leistungssteigerung exponentiell – das bedeutet, mit nur einem einzigen zusätzlichen Qubit verdoppelt man die Berechnungsmöglichkeit! Diese Potenzpower macht einige Aufgaben mit einem Quantencomputer lösbar, die auf einem klassischen Weg sonst weiterhin ungelöst blieben. Zum Beispiel kann es

Quantenverschränkung

Quantenverschränkung (englisch: Quantum Entanglement) ist ein fundamentales Phänomen der Quantenmechanik, bei dem ein System mit mehreren Elementarteilchen als Ganzes betrachtet einen wohldefinierten Zustand einnimmt, ohne dass man jedem der Teilsysteme einen eigenen wohldefinierten Zustand zuordnen kann. Dabei sind zwei oder mehr Teilchen so miteinander verbunden, dass der Zustand eines Teilchens sofort den Zustand des anderen beeinflusst, unabhängig von der Entfernung zwischen diesen Teilchen.

im Go-Spiel [3] bei einem 19×19 -Brett $2,08 \times 10^{170}$ oder circa 2^{565} verschiedene Stellungen geben. Das ist eine unvorstellbar große Zahl, wenn man bedenkt, dass es im beobachtbaren Universum mit geschätzt 2 Billionen Galaxien, von denen jede einzelne noch Hunderte Milliarden von Sternen enthält, „nur“ zwischen 10^{84} (2^{278}) und 10^{89} (2^{296}) Atome gibt! Also wäre es offensichtlich unmöglich, alle mögliche Go-Stellungen in klassischer binärer Form zu berechnen – auch wenn man pro Bit nur ein Atom reserviert, reicht das ganze (bekannte) Universum schon lange nicht! Mit circa 600 kohärenten verschränkten Quantenbits wäre die Berechnung aller Go-Stellungen lösbar, für eine binäre Abbildung aller Atome des Universums hätte sogar die Hälfte davon ausgereicht!

Ein einzelnes Quantenbit bedeutet keinen großen Unterschied gegenüber einem klassischen Bit und findet kaum praktische Anwendung. Mit jedem weiteren hinzugefügten Qubit verdoppeln sich jedoch Leistung und Möglichkeiten eines Quantencomputers. Man muss also einen Weg finden, mehrere Quantenbits „zusammenzukleben“. Dafür wird ein weiteres Phänomen der Quanten-Welt verwendet: die Quantenverschränkung (siehe Kasten [Quantenverschränkung](#)).

Die Verschränkung der Qubits spielt vor allem in Quantencomputer-Berechnungen eine zentrale Rolle – einerseits durch Verschränkung vieler Qubits im Verlauf der Rechnung mit Quantenalgorithmen, andererseits im Verfahren zur ►

Dekohärenz

Dekohärenz [4] ist ein Phänomen der Quantenphysik, das teilweise oder vollständig zu einem Verlust der Kohärenz oder der quantenmechanischen Superposition zwischen Teilchen führt. Durch Wechselwirkungen mit ihrer Umgebung, beispielsweise durch externe Einflüsse wie Wärme oder Strahlung oder durch Messungen, verlieren Quantenzustände ihre speziellen Eigenschaften und werden „klassischer“ Natur. Dieser Prozess führt dazu, dass die einzigartigen, nichtklassischen Merkmale von Quantensystemen allmählich verschwinden, was eine Herausforderung für die Aufrechterhaltung quantenmechanischer Eigenschaften in realen Umgebungen darstellt.

Fehlerkorrektur, die nötig ist, um die Quantenbits vor Dekohärenz (siehe Kasten **Dekohärenz** und [4]) zu schützen.

Außerdem bildet die Quantenverschränkung eine Grundlage für Quantenkommunikationsprotokolle wie Quantenschlüsselverteilung [5] (englisch: Quantum Key Distribution, QKD). Ein weiteres faszinierendes Anwendungsgebiet von Quantenverschränkung ist die Quantenteleportation [6], bei der der Zustand eines Teilchens von einem Ort zum anderen übertragen wird, ohne dass das Teilchen selbst den Raum dazwischen durchläuft.

Wenn die Quantenzustände nicht als individuelle Qubit-Zustände geschrieben werden können, spricht man von nicht separierbaren Quantensystemen, auch als verschränkte Systeme bezeichnet. Wenn ein Zustand als Produktzustand der einzelnen Teilsysteme geschrieben werden kann, ist dieser Zustand nicht verschränkt. Verschränkung ist eine quantenmechanische Korrelation, die sich deutlich von klassischen Korrelationen unterscheidet. Bei Verschränkung ist der Zustand der Teilsysteme nicht festgelegt, und es kann nur über die Wahrscheinlichkeiten der Ergebnisse gesprochen werden. Das globale System muss als Einheit betrachtet werden.

Die Quantenverschränkung ist ein entscheidender Baustein im Quantencomputer-Konzept. Sie ermöglicht es, die Qubits so zu verknüpfen, dass sie sich nicht wie Einzelteile, sondern wie ein großes, komplexeres System verhalten. In verschränkten Systemen ändert die Messung eines Qubits den Zustand der anderen Qubits und gibt uns Informationen über ihren Zustand. Man betrachte zum Beispiel zwei überlagerte Qubits A und B (in Superposition), sodass der Zustand des globalen Quantensystems folgendermaßen wäre:

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$$

In einem solchen Zustand wären nur zwei Ergebnisse möglich, wenn man den Zustand beider Qubits in der Standardbasis misst: $|00\rangle$ und $|11\rangle$, wobei jedes Ergebnis die gleiche Wahrscheinlichkeit von $\frac{1}{2}$ hätte. Dabei wäre es unmöglich

● Quanteninterferenz

Quanteninterferenz ist ein Phänomen in der Quantenmechanik, das aus der wellenartigen Natur von quantenmechanischen Teilchen wie Elektronen oder Photonen resultiert. Wenn ein Teilchen in einer Überlagerung (Superposition) mehrerer Zustände ist, können diese Zustände miteinander interferieren und zu konstruktiver (Verstärkung) oder destruktiver Interferenz (Unterdrückung) führen. Diese Interferenz kann spezifische Muster von Ergebnissen bei der Messung des Teilchens erzeugen. In der Quanteninformatik wird Interferenz auf verschiedene Weisen genutzt, um Quantenzustände zu manipulieren, zu kontrollieren und somit Rechenaufgaben auszuführen. Durch Anwendung von Quantengattern [12], die Überlagerungen von Qubits erzeugen, und durch Kontrolle der relativen Phasen der Zustände kann Interferenz verwendet werden, um bestimmte Ergebnisse zu verstärken und andere zu unterdrücken.

● Logisches Qubit

Ein logisches Qubit ist eine abstrakte, fehlertolerante Einheit in der Quanteninformatik, die aus mehreren physischen Qubits konstruiert wird. Im Gegensatz zu physischen Qubits, die anfällig für Fehler und Dekohärenz sind, wird ein logisches Qubit durch Fehlerkorrekturtechniken geschützt, um zuverlässige Quanteninformationen zu speichern. Die Verwendung von Fehlerkorrekturcodes ermöglicht es logischen Qubits, stabilere und länger anhaltende Quantenzustände aufrechtzuerhalten, was für die Realisierung von zuverlässigen Quantencomputern von entscheidender Bedeutung ist.

(Wahrscheinlichkeit gleich 0), die Ergebnisse $|01\rangle$ und $|10\rangle$ zu bekommen. Wenn man nun das erste Qubit A misst und feststellt, dass es im Zustand $|0\rangle$ ist, kann man sicher sein, dass das zweite Qubit B sich ebenfalls im Zustand $|0\rangle$ befindet, ohne es zu messen zu müssen! Die Messergebnisse in diesem Fall korrelieren zueinander, und die Qubits A und B sind verschränkt. Diese Verschränkungseigenschaft wird sehr intensiv in vielen Quantenalgorithmien genutzt. Die Quantenverschränkung ermöglicht es also, dass die Qubits in einer gemeinsamen Informationseinheit arbeiten, wodurch sie kollektiv Informationen verarbeiten können.

Ein weiteres wichtiges Konzept der Quantenmechanik, das in Quantencomputern intensiv benutzt wird ist die Quanteninterferenz (siehe Kasten **Quanteninterferenz**). Interferenz bildet die Grundlage vieler Quantenalgorithmien und kann zu erheblichen Beschleunigungen in der Berechnung führen. Ein Beispiel für eine solche Anwendung ist der Grover-Algorithmus [7], der für die unstrukturierte Suche verwendet wird. Ein weiteres Beispiel für die Nutzung von Interferenz in einem Algorithmus ist die Quanten-Fourier-Transformation (QFT) [8], die eine effiziente Berechnung bestimmter mathematischer Funktionen ermöglicht. Quanteninterferenz wird auch in der Quantenphasenschätzung verwendet, einer Technik, die in verschiedenen Quantenalgorithmien zur Schätzung der Phase eines Quantenzustands eingesetzt wird. Die Quantenphasenschätzung umfasst die Interferenz zwischen verschiedenen Quantenzuständen, die durch Anwendung von Quantengattern gesteuert und durch Messung der resultierenden Wahrscheinlichkeitsverteilung gemessen werden kann. Darüber hinaus ist Interferenz neben dem logischen Qubit (siehe Kasten **Logisches Qubit**) ein Schlüsselkonzept in der Quantenfehlerkorrektur, die notwendig ist, um Quanteninformation vor den möglichen Fehlern zu schützen. Durch Messung des Interferenzmusters von Qubits können Quantencomputer Fehler erkennen und korrigieren, die während der Berechnung aufgetreten sein könnten.

In einigen Quantencomputern kann sich ein Elementarteilchen nicht in zwei, sondern in drei oder noch mehr überlagerten Zuständen befinden. Dabei spricht man jeweils von Qutrit [9] beziehungsweise Qudit [10] (siehe Kasten **Qutrit und Qudit**) als mehrdimensionalen Quanteninformations-Bauste-

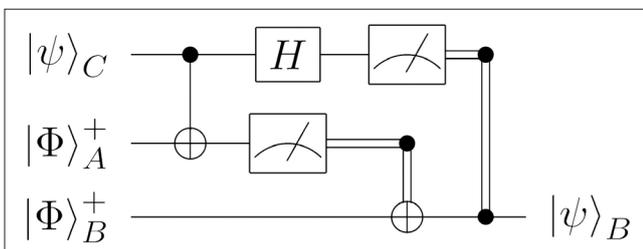
nen. Qutrits und Qudits bieten eine höhere Kapazität für Quantenparallelismus. Anwendungen von Qudits finden sich in verschiedenen Bereichen, darunter die Fourier-Transformation, Quantenverschlüsselung und spezifische Quantenalgorithmien. Die Implementierung von Qudits bringt jedoch technische Herausforderungen mit sich, insbesondere in Bezug auf die Kontrolle und Messung von Zuständen in höheren Dimensionen.

Rechenmodelle im Quantencomputing

Quantencomputing umfasst verschiedene Rechenmodelle, die auf unterschiedlichen physikalischen Prinzipien beruhen. Jedes Modell hat seine eigenen spezifischen Stärken und Schwächen sowie spezifische Anwendungsbereiche. In den nachfolgenden Abschnitten sollen die wichtigsten Quantencomputing-Modelle vorgestellt werden.

Schaltkreis-/Quantum-Gate-Modell

Ein maßgeblicher Akteur im Bereich des Quantencomputing ist das Schaltkreis-Modell [11] (englisch: Quantum Circuit), auch als Quantum-Gate Computing bekannt. Dieses Modell basiert auf der Anwendung von Quantengattern [12] (englisch: Quantum logic gate), um Qubits zu manipulieren und komplexe Berechnungen durchzuführen. In diesem Kontext werden Quantenalgorithmien als Schaltkreise von Quantengattern repräsentiert, wodurch fundamentale Quantenprinzi-



Schaltkreis für Quantenteleportation (Bild 3)

● Qutrit und Qudit

Qutrit [9] und Qudit sind Erweiterungen des Konzepts von Qubits in der Quanteninformatik [10]. Während Qubits binäre Einheiten von Quanteninformation sind, die die Zustände 0, 1 oder eine Superposition von beiden zweidimensional repräsentieren, können Qutrits und Qudits in einem höherdimensionalen Raum existieren. Anders ausgedrückt: Während Qubits zwei mögliche Zustände haben, können Qutrits drei und Qudits noch mehr Zustände in einem Quantensystem darstellen. Die höheren Dimensionen der Qutrits beziehungsweise Qudits eröffnen erweiterte Möglichkeiten für die Speicherung und Verarbeitung von Quanteninformationen. Die Quantenüberlegungen und Prinzipien, die für Qubits gelten, können auf Qutrits und Qudits erweitert werden, wodurch komplexere und leistungsfähigere Quantenalgorithmien und -protokolle möglich wären.

● Quantenteleportation

Die Quantenteleportation [6] ist ein Prozess, der den quantenmechanischen Zustand eines Quantensystems, wie beispielsweise eines Photons oder eines Qubits (Quelle), auf ein anderes Quantensystem (Ziel) überträgt. Während dieser Übertragung wird der Zustand der Quelle verändert. Das Verfahren bedient sich dabei zweier Kanäle: eines Quantenkanals und eines klassischen Kanals. Als Quantenkanal dient ein Paar von verschränkten Teilchen. Die Quantenteleportation nutzt die Eigenschaften der Quantenverschränkung sowie beide Kanäle, um den Zustand von der Quelle zum Ziel zu übertragen, ohne dabei eine Messung vorzunehmen.

Die Quantenteleportation spielt eine entscheidende Rolle beim Aufbau von Quantennetzwerken. Es ist wichtig zu betonen, dass der Begriff „Teleportation“ in diesem Kontext nicht mit der Teleportation aus der Science-Fiction gleichzusetzen ist. In der Realität setzt die Quantenteleportation voraus, dass am Zielort bereits ein vorbereitetes Zielsystem vorhanden ist, auf das der Zustand der Quelle übertragen wird.

pien wie Superposition und Verschränkung genutzt werden. Dieser Ansatz wird zum Beispiel in dem berühmten Shor-Algorithmus [13] für die Faktorisierung von Primzahlen (Entschlüsselung) und dem Grover-Suchalgorithmus [7] angewandt. Gate-basierte Quantencomputer können ähnlich wie aktuelle klassische digitale Computer betrachtet werden, bei denen eine Reihe von Transformationen (Logikgatter) durchgeführt werden, um ein bestimmtes Ergebnis zu erhalten.

Ein Quantenschaltkreis ist ein Modell für Quantenberechnungen, ähnlich den klassischen Schaltkreisen, bei dem eine Berechnung eine Abfolge von Quantengattern, Messungen, Initialisierungen von Qubits auf bekannte Werte und möglicherweise anderen Aktionen ist. Die Schaltkreise werden so geschrieben, dass die horizontale Achse die Zeit darstellt, beginnend auf der linken Seite und endend auf der rechten Seite. Horizontale Linien repräsentieren Qubits, doppelte Linien stehen für klassische Bits. Die Elemente, die durch diese Linien verbunden sind, sind Operationen, die an den Qubits durchgeführt werden, wie Messungen oder Gatter-Transformationen. Diese Linien definieren die Abfolge der Ereignisse und sind normalerweise keine „physischen“ Leitungen im eigentlichen Sinne.

Zur Veranschaulichung ist in Bild 3 ein Schaltkreis für Quantenteleportation (siehe Kasten **Quantenteleportation** und [6]) dargestellt. Zu den Vorteilen des Quanten-Schaltkreis-Rechenmodells gehören vor allem:

- **Klarheit:** Das Schaltkreis-Modell bietet eine klare und intuitive Darstellung von Quantenalgorithmien. Die Verwendung von Quantengattern ermöglicht eine präzise Repräsentation von Schritten in einem Algorithmus.
- **Verbreitung:** Das Schaltkreis-Modell ist vielseitig einsetzbar und eignet sich für verschiedene Quantenalgorithmien, zum Beispiel den Shor-Algorithmus [13] oder den Grover- ▶

Suchalgorithmus [7], und es deckt eine breite Palette von Anwendungen ab.

- **Quantenparallelismus:** Das Schaltkreis-Modell nutzt Quantenparallelismus effektiv aus, wodurch mehrere Berechnungen gleichzeitig durchgeführt werden können. Dies kann zu erheblichen Geschwindigkeitsvorteilen bei bestimmten Problemstellungen führen.
- **Programmierbarkeit:** Das Schaltkreis-Modell ermöglicht die präzise Programmierung von Quantenoperationen. Durch die Anwendung von Quantengattern kann der Algorithmus gezielt gesteuert und angepasst werden.

Wenn man die Nachteile von Schaltkreis-Rechenmodellen betrachtet, sind folgende Herausforderungen festzustellen:

- **Fehleranfälligkeit:** Schaltkreise mit vielen Qubits sind anfällig für Fehler, insbesondere durch Dekohärenz [4] und Rauschen in der Quantenhardware. Dies erfordert komplexe Fehlerkorrekturmechanismen.
- **Komplexe Hardware:** Die Umsetzung von Schaltkreis-Modellen erfordert hochentwickelte Quantenhardware. Die Realisierung von stabilen Quantengattern mit einer großen Anzahl von Qubits stellt technologische Herausforderungen dar (Qubit-Skalierung, Störeinflüsse et cetera).
- **Schaltkreis-Komplexität:** Bei längeren Schaltkreisen mit vielen Quantengattern kann die Komplexität und damit die Anzahl der benötigten Qubits schnell ansteigen. Dies erhöht die Anforderungen an die Hardware und erschwert die Fehlerkorrektur.
- **Fragilität:** Die Leistungsfähigkeit des Schaltkreis-Modells kann durch Umgebungsstörungen (zum Beispiel Strahlung, Wärme et cetera) und physikalische Einschränkungen (zum Beispiel die Erfordernis von Tieftkühlung für Supraleitung) beeinträchtigt werden, was seine Robustheit gegenüber externen Einflüssen begrenzt.

Technologisch führende Unternehmen wie Google, IBM, Intel, Honeywell und viele mehr investieren intensiv in diesen Ansatz, um die Grenzen der Leistungsfähigkeit von Quantum-Gate Computing weiter zu erforschen, und haben bereits einige Schaltkreis-basierte Quantenprozessoren (QPUs) hergestellt. Manche davon stehen via IBM, AWS, Azure und Google Cloud für benutzerspezifische Quanten-Schaltkreisalgorithmen bereits zur Verfügung.

Analoge Quantencomputing-Modelle

Im Unterschied zu diskreten Quanten-Rechenmodellen wie dem Schaltkreis-/Gate-basierten Modell gibt es analoge Quanten-Rechenmodelle, die sich auf die Art und Weise beziehen, wie die Informationen in einem Quantencomputer dargestellt und verarbeitet werden. Hier sind die wichtigsten Unterscheidungsmerkmale:

- **Kontinuierliche Zustände:** Im analogen Ansatz werden physikalische Quantenzustände kontinuierlich dargestellt und manipuliert. Die Veränderungen der Zustände erfolgen stufenlos und können als analog zu den kontinuierlichen Werten in klassischen analogen Systemen betrachtet werden.

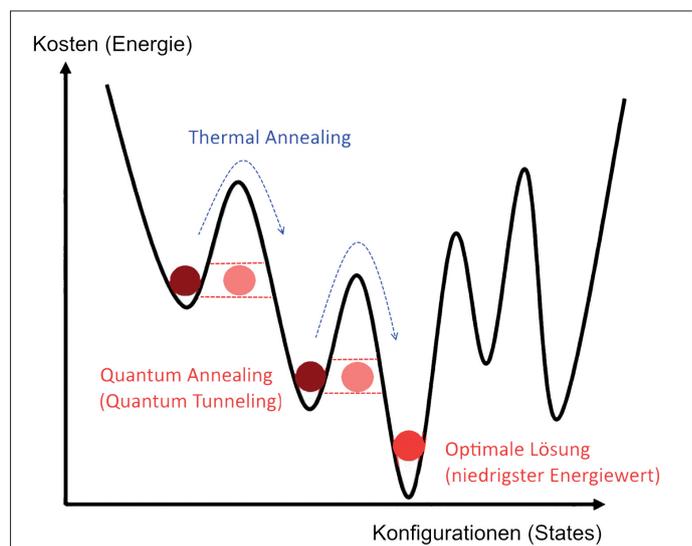
- **Kontinuierliche Transformationen:** Analoge Quantencomputer nutzen kontinuierliche physikalische Transformationen, um Informationen zu repräsentieren und zu verarbeiten. Dies geschieht oft über Prozesse wie adiabatisches Quantencomputing [14] oder Quantum Annealing [15].

Analoge Quanten-Rechenmodelle haben ihre eigenen spezifischen Merkmale. So sind für adiabatisches Quantencomputing die folgenden Punkte hervorhebenswert:

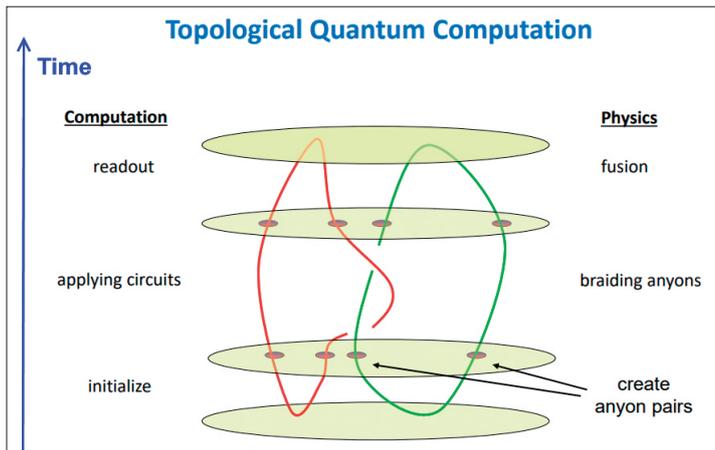
- **Prinzip:** Sie basieren auf dem adiabatischen Theorem, das den langsamen Übergang eines Systems zwischen Zuständen beschreibt.
- **Funktionsweise:** Durch adiabatische Evolution wird der Quantenzustand eines Systems kontinuierlich verändert, um eine Lösung für ein Optimierungsproblem zu finden.
- **Anwendungen:** Gut geeignet für spezifische Optimierungsprobleme wie das Handlungsreisenden-Problem [16] und das Maximum-Schnitt-Problem [17].
- **Vorteile:** Robust gegenüber bestimmten Fehlern und natürlich anwendbar für bestimmte physikalische Systeme.
- **Herausforderungen:** Begrenzte Vielseitigkeit für allgemeine Berechnungen und technologisch anspruchsvollere Skalierung.

Beim Annealing-Quantencomputing sind folgende Punkte erwähnenswert:

- **Prinzip:** Verwendung von Quanten-Annealing, einem Prozess, der darauf abzielt, das globale Energieminimum eines Systems zu finden.
- **Funktionsweise:** Das Quanten-Annealing-Verfahren [15] sucht nach der minimalen Energiekonfiguration eines Systems, was als Ergebnis für ein relevantes Optimierungsproblem zu betrachten ist. Quantum Annealing (rote Linie in Bild 4) durchläuft Energielandschaften effizient, indem es Quanten-Tunneling nutzt, um das globale Minimum zu finden. Quantum Annealing bietet einen erheblichen Leistungsvorteil gegenüber simuliertem Annealing (blaue Linie)



Lösungsfindung (globales Minimum) mit Quantum Annealing (Bild 4)



Topologisches Quantencomputing-Modell (Bild 5)

in Bild 4) und ermöglicht die Lösung komplexer Optimierungsprobleme, die auf andere Weise nur schwer oder gar nicht gelöst werden konnten.

- **Anwendungen:** Effektiv für bestimmte Optimierungsprobleme, insbesondere in Bezug auf das Finden globaler Minima.
- **Vorteile:** Effektiv für bestimmte Optimierungsprobleme, kann in bestimmten Anwendungen Gate-basierte Ansätze ergänzen.
- **Herausforderungen:** Begrenzte Vielseitigkeit, hohe Anforderungen an das Design von Quantenhardware.

Technologisch ist die kanadische Firma D-Wave Systems [18] im Bereich Quantum Annealing am weitesten fortgeschritten. Im Mai 2011 wurde „D-Wave One“ als „der welterste kommerziell verfügbare Quantencomputer“ vorgestellt. Heute kann jeder via D-Waves Cloud-Plattform Leap [19] eigene Quantum-Lösungen bauen.

Ein weiteres Beispiel für analoge Quantencomputing-Rechenmodelle ist Quantencomputing mit kontinuierlichen Variablen (englisch: Continuous-variable quantum computing [20], [21]). Quantencomputing mit kontinuierlichen Variablen basiert auf der Nutzung von Quantenzuständen, die nicht diskret, sondern kontinuierlich sind. Im Gegensatz zu herkömmlichen zweidimensionalen Qubits beziehungsweise drei- oder mehrdimensionalen Qutrits/Qudits, die diskrete Zustände aufweisen, verwenden diese Systeme kontinuierliche Größen wie Phasen- oder Amplitudenmodulationen. Die Vorteile dieses Ansatzes liegen unter anderem in der hohen Redundanz, die eine robuste Fehlerkorrektur ermöglicht, sowie in der effizienten Codierung von Informationen, die komplexe Rechenoperationen erleichtern kann. Zudem könnten Modelle mit kontinuierlichen Variablen in einigen Fällen weniger Hardwarekomponenten erfordern. Es gibt jedoch auch Herausforderungen in diesem Feld wie zum Beispiel präzise Kontrolle und Messung kontinuierlicher Variablen oder Empfindlichkeit gegenüber externen Störungen. Quantencomputing mit kontinuierlichen Variablen ist ein vielversprechendes Forschungsfeld, das bereits verschiedene praktische [22] sowie experimentelle Implementierungsansätze gefunden hat (siehe Kapitel 5 in [20]).

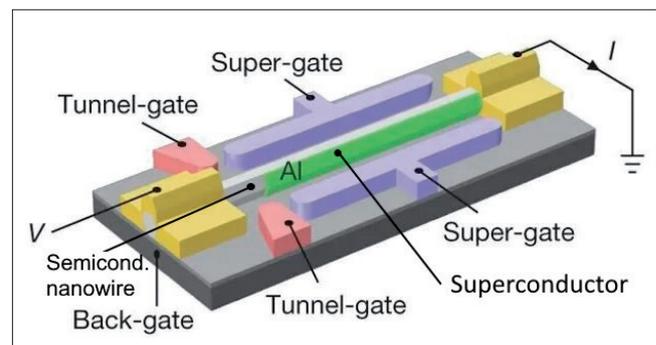
Analog-Quantencomputer sind auch leistungsstark bei der Quantensimulation, da sie flexible Anregungs- und Antriebsparameter bieten. Ihre Vielseitigkeit erstreckt sich über verschiedene komplexe Aufgaben in den Bereichen Optimierung, maschinelles Lernen und Simulation von Quantensystemen.

Und schließlich ist es noch an dieser Stelle zu bemerken, dass „digitale“ Quantencomputer (zum Beispiel Gatter-/Schaltkreis-basierte) im Unterschied zu analogen Modellen aufgrund ihrer diskreten Natur vielseitiger einsetzbar sind. Sie können eine breitere Palette von Quantenalgorithmen implementieren, darunter auch solche, die für klassische Computer schwer zu simulieren sind. Die Unterscheidung zwischen „digitalen“ (diskreten) und „analogen“ Ansätzen spiegelt die verschiedenen Strategien wider, die bei der Realisierung von Quantencomputern verfolgt werden und für die sich dann jeweils eigene Vor- und Nachteile in Bezug auf Anwendbarkeit und Implementierung ergeben.

Experimentelle Rechenmodelle im Quantencomputing

Quantencomputing hat sich zu einem faszinierenden Forschungsbereich entwickelt, der verschiedene experimentelle Rechenmodelle umfasst. Während gängige Gate-basierte und Annealing-Modelle bereits ihre technologische Realisierung und kommerzielle Anwendung gefunden haben, eröffnen experimentelle Ansätze weiterer Quanten-Rechenmodelle neue Perspektiven für die Realisierung von Quantencomputern. Im Folgenden werfen wir einen Blick auf einige dieser experimentellen Modelle, um ihre Besonderheiten sowie Vor- und Nachteile zu erkunden.

Der Ansatz des topologischen Quantencomputing (englisch: Topological Quantum Computing) basiert auf topologischen Quantenzuständen und -operationen, die in der Theorie widerstandsfähiger gegenüber Fehlerquellen sein könnten. Dabei verwendet ein topologischer Quantencomputer topologische Zustände von Qubits, um Quanteninformationen zu speichern und zu verarbeiten. Er nutzt Quasiteilchen in zweidimensionalen Systemen, auch als Anyons [23] bezeichnet. Die Weltlinien [24] (eine zeitartige Kurve in einer mehrdimensionalen, relativistischen Raumzeit) von Anyons verlaufen umeinander und bilden sogenannte Braids [25] (Flechten) ►



Struktur des topologischen Qubit-Geräts (Bild 6)

in einem dreidimensionalen Raum-Zeit-Gefüge (also einer zeitlichen plus zwei räumlicher Dimensionen, siehe **Bild 5**).

Kombinationen dieser Flechten fungieren als die Logikgatter, die einen Computer auf einer elementaren logischen Ebene ausmachen. Die grundlegende Struktur eines topologischen Qubits platziert einen geeigneten Halbleiter-Nanodraht in unmittelbarer Nähe zu einem Supraleiter (siehe **Bild 6**). Aufgrund dieser Nähe wird der Halbleiter-Nanodraht ebenfalls supraleitend, und unter den richtigen Bedingungen (einschließlich eines geeigneten Magnetfelds entlang des Drahts und angelegter Spannungen an der Vorrichtung) tritt der Halbleiter-Nanodraht in die topologische Phase ein.

Die topologische Phase zeichnet sich durch sogenannte Majorana Zero Modes (MZMs) an jedem Ende des Drahts und eine „Lücke“ (Gap) in der übrigen Länge des Drahts aus, wobei die Lücke ein Bereich von Energie oder Spannung ohne erlaubte quantenmechanische Zustände ist. Der Vorteil eines topologischen Quantencomputers liegt darin, dass er deutlich stabiler ist, da die Informationen in topologischen Qubits durch topologische Eigenschaften geschützt sind, die schwerer zu destabilisieren wären. Dadurch braucht man deutlich weniger physikalische Qubits, um ein logisches Quantenbit zu bilden. Dieser inhärente Schutzmechanismus macht topologische Qubits zu vielversprechenden Kandidaten für den Aufbau stabiler Quantencomputer für komplexe Berechnungen mit minimalen Fehlerquoten. Um komplexe wissenschaftliche und kommerzielle Probleme lösen zu können, werden mindestens eine Million stabile Qubits benötigt, die eine Trillion Operationen bei Fehlerquoten weit unter 0,1 Prozent durchführen können. Zu den Herausforderungen des Ansatzes mit topologischen Qubits gehören unter anderem die komplexe Implementierung und die Fehleranfälligkeit bei thermalen Fluktuationen. Microsoft packt diese Herausforderungen bereits an und arbeitet an der Entwicklung ei-

nes topologischen Quantencomputers. Weitere Informationen zum Thema findet man unter [26], [27] und [28].

Ein weiteres experimentelles Quantencomputing-Rechenmodell wird in Form des messbasierten oder Einweg-Quantencomputing [29] realisiert (englisch: Measurement-Based/One-way Quantum Computing). Im Gegensatz zu traditionellen Gate-basierten Modellen, die auf der schrittweisen Anwendung von Quantengattern beruhen, verwendet man eine interessante Herangehensweise: Anstatt die Zustände der Qubits durch Gatter zu manipulieren, werden diese in einem vorbereiteten Verschränkungszustand platziert. Durch selektives Messen einzelner Qubits wird der Quantenzustand dann schrittweise verändert, wodurch der Computer schließlich zu einem Zielzustand gelangt.

Dieses Rechenmodell nennt man „One-way“-Computing, da die Ursprungszustände durch die Messung verändert (zerstört) werden. „One-way“-Quantencomputing bietet interessante Perspektiven für bestimmte Quantenalgorithmen und hat Potenzial für die Bewältigung spezifischer Herausforderungen im Bereich der Fehlerkorrektur. Als Herausforderung dabei gelten der hohe Bedarf an Verschränkung und die anspruchsvollen Hardware-Anforderungen.

In der Reihe der experimentellen Quantencomputing-Modelle lohnt es sich noch, das holonomische Quantencomputing (HQC) [30] als eine vielversprechende Variante zu erwähnen. HQC hat das Potenzial, die traditionellen gatterbasierten Modelle zu ergänzen und verbessern. Es wird als experimentelles Modell erforscht, um seine Eignung für bestimmte Quantenaufgaben und -anwendungen zu verstehen. Der Ansatz von HQC unterscheidet sich grundlegend von gatterbasierten Quantencomputern, da er auf geometrischen Phasen und Transformationen basiert. Die Idee ist, Quantengatter durch die Gestaltung von Pfaden im Quantenzustandsraum zu realisieren, wodurch geometrische Phasen genutzt werden, um Quantenoperationen durchzuführen. Obwohl HQC noch in der Forschungs- und Entwicklungsphase ist, werden experimentelle Fortschritte in diese Richtung gemacht. Wichtig zu beachten ist jedoch, dass sich die Technologie und die Forschung ständig weiterentwickeln und bestimmte Umsetzungen oder Anwendungen von HQC möglicherweise noch nicht weit verbreitet sind.

Neue und experimentelle Quantencomputing-Rechenmodelle bringen einzigartige Prinzipien, Vor- und Nachteile sowie Herausforderungen mit sich. Während topologisches beziehungsweise holonomisches Quantencomputing die Stabilität von Qubits durch topologische beziehungsweise geometrische Phasen und Transformationen versprechen, setzt One-way Quantum Computing auf die Vereinfachung von Quantenberechnungen durch spezielle Zustandspräparation, und Continuous-Variable Quantum Computing wiederum nutzt kontinuierliche Variablen für Rechenoperationen, was deutlich höhere Skalierbarkeit im Vergleich zu den Rechenmodellen mit diskreten Qubits und Qudits bedeutet.

Die Vielfalt dieser experimentellen Modelle trägt dazu bei, das Verständnis von Quantencomputing zu vertiefen und neue Wege für die Entwicklung von robusten, fehlertoleranten Quantenrechnern zu erforschen.

● QPU – Quantum Processing Unit

Eine QPU (Quantum Processing Unit) [31] ist eine Hardwareeinheit, die speziell für die Durchführung von Quantenberechnungen entwickelt wurde. Im Gegensatz zu herkömmlichen Computern, die auf Bits basieren, die den Zustand 0 oder 1 annehmen können, arbeitet ein QPU mit Qubits, welche aufgrund von Quantenüberlagerung (Superposition) und Verschränkung (Entanglement) gleichzeitig mehrere Zustände repräsentieren. Auf einer QPU werden Quantenalgorithmen ausgeführt, die aus mehreren Quantenoperationen bestehen.

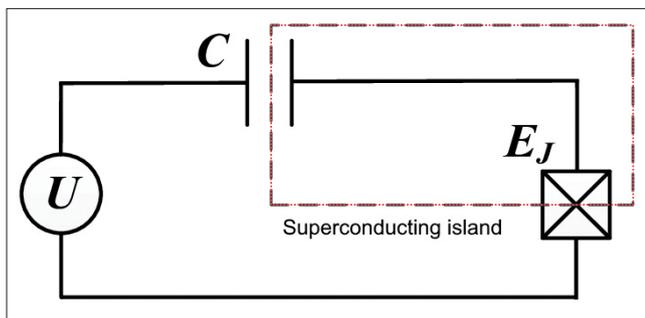
Es ist wichtig zu beachten, dass QPUs aufgrund ihrer besonderen Natur und der Herausforderungen der Quantenfehlerkorrektur noch in einem frühen beziehungsweise experimentellen Stadium stehen. Unternehmen und Forschungseinrichtungen arbeiten jedoch intensiv daran, QPUs zu verbessern und ihre Anwendungen in verschiedenen Bereichen wie Kryptografie, Optimierung, Simulation und maschinelles Lernen zu ermöglichen und zu verbessern.

● **Quantum Volume**

Quantum Volume wurde ursprünglich 2018 von Nikolaj Moll als Metrik vorgeschlagen und im darauffolgenden Jahr von IBM erweitert. Quantum Volume misst als Metrik die Fähigkeiten und Fehlerquoten eines Quantencomputers. Sie gibt die maximale Größe von quadratischen Quantenschaltungen an, die erfolgreich von einem Computer implementiert werden können.

Die Form der Schaltungen ist unabhängig von der Architektur des Quantencomputers, aber der Compiler kann sie transformieren und optimieren, um die Funktionen des Computers optimal zu nutzen. Auf diese Weise können Quantum Volumes verschiedener Architekturen miteinander verglichen werden. Es handelt sich also um eine umfassende Metrik, die nicht nur die Anzahl der Qubits, sondern auch andere wichtige Faktoren wie Fehlerkorrektur, Gatterfehlerraten und die Qualität der Verbindungen zwischen den Qubits berücksichtigt. Dies ermöglicht eine ganzheitliche Bewertung und Vergleichbarkeit der Leistungsfähigkeit von Quantencomputern.

Ein höheres Quantum Volume deutet auf einen leistungsfähigeren und robusteren Quantencomputer hin.



Schaltkreis von Charge-Qubit (Bild 7)

Während noch viele Herausforderungen bestehen und weitere Forschung erforderlich ist, eröffnen diese experimentellen Ansätze vielversprechende Perspektiven für die Zukunft der Quanteninformatik.

Quantenprozessoren und ihre Archetypen

Das „Herz“ jedes Quantencomputers bildet eine Quantenverarbeitungseinheit – Quantenprozessor (englisch: Quantum Processing Unit, QPU, siehe Kasten **QPU – Quantum Processing Unit** und [31]). Im Folgenden werden zunächst verschiedene Typen und Ausführungen der Quantenprozessoren betrachtet, die bereits ihre Anwendung in zurzeit hergestellten Quantencomputern finden. Im Anschluss daran stellt ein weiterer Abschnitt übersichtsartig wichtige Archetypen von Quantenprozessoren vor.

Superconducting-QPU

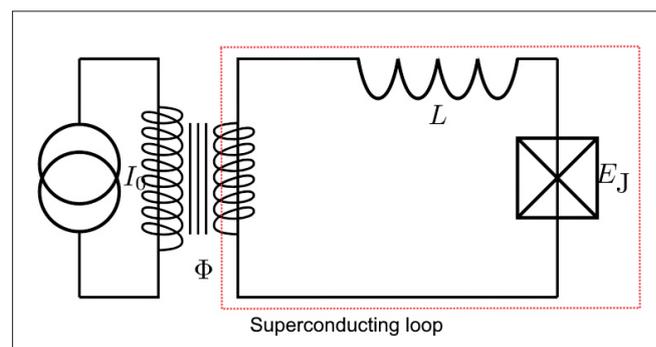
Ein Quantenprozessor mit supraleitenden Schaltkreisen [32] (superconducting circuits) repräsentiert eine vielversprechen-

de und weitverbreitete Technologie für die Realisierung von Quantencomputern. Die Herangehensweise basiert auf den Prinzipien der Supraleitung, bei denen bestimmte Materialien bei extrem niedrigen Temperaturen keinen elektrischen Widerstand aufweisen. Im Zentrum dieser Technologie stehen Josephson-Übergänge (siehe „E_J“ in Bild 7, Bild 8 und Bild 9 sowie „Josephson junction“ in [32]): schwache Verbindungen zwischen zwei supraleitenden Materialien. Diese Josephson-Übergänge ermöglichen den ungehinderten Fluss von Cooper-Paaren, also Paaren von Elektronen, ohne elektrischen Widerstand. Die grundlegenden Bausteine sind hier supraleitende Qubits, die auf Josephson-Übergängen basieren. Diese Qubits können aufgrund von quantenmechanischer Überlagerung in mehreren Zuständen gleichzeitig existieren.

Die Operationen auf diesen Qubits werden durch die Anwendung von Mikrowellenimpulsen und Magnetfeldern durchgeführt, wodurch Quantengatter entstehen, die spezifische Operationen ausführen. Die Quantenphänomene der Verschränkung und Überlagerung werden genutzt, um komplexe Rechenoperationen durchzuführen. Die Leistungsfähigkeit von Quantenprozessoren mit supraleitenden Schaltkreisen wird durch Metriken wie das Quantum Volume (siehe Kasten **Quantum Volume**) bewertet, wobei Aspekte wie die Konnektivität der Qubits, Gattergenauigkeiten und Fehlerquoten berücksichtigt werden.

Zurzeit werden drei Archetypen von supraleitenden Qubits (siehe „Qubits Archetypes“ in [32]) umgesetzt:

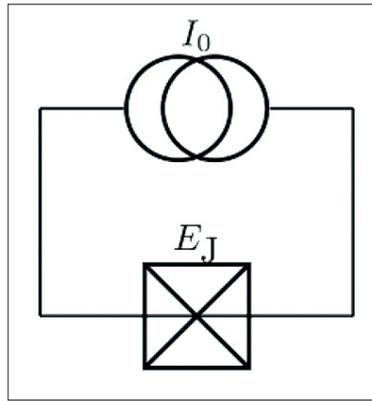
- **Charge-Qubits:** Charge-Qubits (siehe Bild 7) nutzen die elektrische Ladung als Basis für die Repräsentation von Quanteninformation. Die Information wird in diskreten Ladungszuständen eines elektrischen Systems gespeichert. Ein einzelnes Elektron kann beispielsweise in zwei verschiedenen Ladungszuständen existieren, die als 0 und 1 codiert werden. Die Quantenüberlagerung ermöglicht es Charge-Qubits, gleichzeitig in beiden Zuständen zu existieren, was zu parallelen Berechnungen führt.
- **Flux-Qubits:** Flux-Qubits (siehe Bild 8) verwenden magnetische Flüsse als Basis für die Codierung von Qubit-Informationen. Hierbei werden supraleitende Schleifen genutzt, durch die ein magnetischer Fluss fließen kann. Die Flussquantisierungseigenschaften in Supraleitern ermöglichen es, die Qubit-Information in den Flusszuständen zu speichern. Durch Superposition von Flusszuständen kann ►



Schaltkreis für das Flux-Qubit (Bild 8)

ein Flux-Qubit in mehreren Zuständen gleichzeitig existieren.

- **Phase-Qubits:** Phase-Qubits (siehe Bild 9) nutzen die Phasenunterschiede in supraleitenden Materialien, um Quanteninformation zu repräsentieren. Hierbei wird die Phase eines supraleitenden Rings verwendet, um zwischen den Zuständen 0 und 1 zu wechseln. Die Superposition von Phasenzuständen ermöglicht es Phase-Qubits, mehrere Berechnungen parallel durchzuführen. Sie sind bekannt für ihre hohe Kohärenzzeit, was bedeutet, dass sie länger in einem superpositionierten Zustand bleiben können.

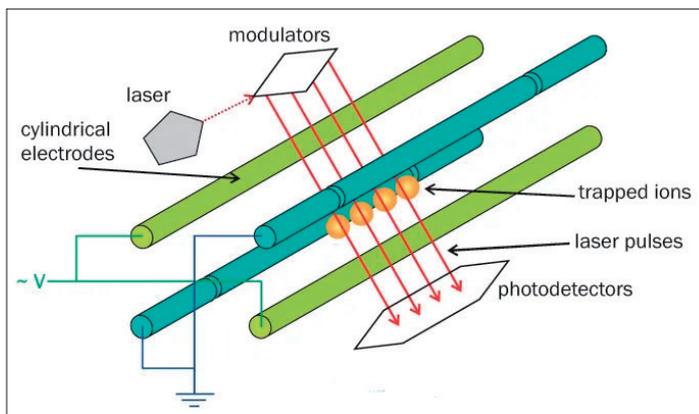


Schaltkreis von Phase-Qubits (Bild 9)

Jeder Qubit-Typ hat seine spezifischen Vor- und Nachteile, die bei der Auswahl für bestimmte Anwendungen berücksichtigt werden müssen:

- **Charge-Qubits** sind durch ihre einfachere Implementierung in herkömmlichen Halbleitermaterialien gekennzeichnet, was ihre Verwendung erleichtert. Sie können jedoch anfällig für begrenzte Kohärenzzeiten und Umgebungsstörungen sein, die durch elektrisches Rauschen verursacht werden.
- **Flux-Qubits** hingegen bieten eine geringere Anfälligkeit für elektrische Rauschquellen und nutzen die natürliche Quantisierung der magnetischen Flüsse in supraleitenden Schleifen. Dies ermöglicht eine präzise Codierung von Qubit-Informationen. Allerdings erfordert ihre Implementierung spezielle supraleitende Materialien und komplexe Schaltungen.
- **Phase-Qubits** zeichnen sich durch eine hohe Kohärenzzeit aus und sind weniger empfindlich gegenüber elektromagnetischen Störungen. Allerdings erfordert ihre Herstellung spezialisierte Techniken und Materialien, und sie können empfindlich gegenüber thermischen Effekten sein.

Fortschritte in der Forschung könnten dazu führen, dass bestimmte Einschränkungen in Zukunft überwunden werden und die Effizienz aller Qubit-Typen verbessert wird. Es bleibt spannend zu sehen, wie sich diese Technologien weiterent-



Qubits-Modell mit „Trapped Ions“ (Bild 10)

wickeln und welche Rolle sie in der Zukunft der Quanteninformatik spielen werden.

Namhafte Unternehmen wie IBM und Google sowie aufstrebende wie Rigetti Computing und einige andere sind aktiv an der Weiterentwicklung von supraleitenden Quantenprozessoren beteiligt. Google hat sogar im Oktober 2019 mit seinem Sycamore-Quantenprozessor eine Quantenüberlegenheit (Quantum Supremacy) deklariert – die 53-Qubit-Sycamore-QPU von Google habe ein Problem in 200 Sekunden gelöst, für das der zu diesem Zeitpunkt fortschrittlichste Supercomputer „Summit“ von IBM etwa 10 000 Jahre gebraucht hätte [33].

Auch wenn IBM widerspricht und „nur“ 2,5 Tage dafür veranschlagt, ist die Performance-Steigerung immer noch beträchtlich. Trotz bestehender Herausforderungen bieten diese Systeme vielversprechende Perspektiven für die Realisierung praktischer und skalierbarer Quantencomputer in der Zukunft und sind Vorreiter im Quantencomputing-Rennen.

„Trapped Ions“-QPU

Der Ansatz des Quantencomputing mit „Trapped Ions“ („gefangenen Ionen“) basiert auf der Verwendung von einzelnen Ionen, die in elektromagnetischen Fallen eingefangen werden, um als Qubits zu fungieren. In [34] ist dieser Prozess schematisch dargestellt (siehe Bild 10).

In diesem Ansatz werden die Ionen in einer Ionenfalle mithilfe elektromagnetischer Felder eingefangen, wobei ihre internen Zustände als logische 0 und 1 dienen. Durch die präzise Manipulation dieser internen Zustände mithilfe von elektromagnetischen Pulsen und Laserstrahlen werden Quantengatter implementiert, um komplexe Berechnungen durchzuführen. Die gezielte Verschränkung der Ionen ist ein Schlüsselement, um Quantenalgorithmen effizient auszuführen. Am Ende der Berechnung wird der Quantenzustand der Ionen ausgelesen, um das Ergebnis zu erhalten.

Die Vorteile dieses Ansatzes liegen in den in der Regel längeren Kohärenzzeiten der Gefangene-Ionen-Systeme im Vergleich zu einigen anderen Qubit-Technologien. Die präzise Kontrolle über die Qubits durch elektromagnetische Felder erleichtert die Implementierung von Quantengattern. Forschungen zur Fehlerkorrektur bei Qubits in Fallen könnten dazu beitragen, Fehler in Quantenberechnungen zu reduzieren.

Allerdings steht dieser Ansatz vor Herausforderungen, insbesondere im Hinblick auf die Skalierbarkeit. Das Vernetzen und Skalieren von Gefangene-Ionen-Systemen bleiben technisch anspruchsvoll. Zudem erfordert die komplexe Apparatur, darunter elektromagnetische Fallen und Kontrollmechanismen, beträchtlichen technologischen Aufwand.

Unternehmen wie IonQ, Honeywell Quantum Solutions, Quantinuum und Alpine Quantum Technologies konzentrieren sich auf die Weiterentwicklung dieser

Technologie, um ihre Potenziale im Bereich des Quantencomputing zu erschließen.

Neutral-Atom-QPU

Die Neutral-Atom-QPU basiert auf der Verwendung neutraler Atome als perfekte Qubits. Diese Atome werden mit Laserstrahlen und elektromagnetischen Feldern manipuliert, um quantenmechanische Phänomene zu erzeugen.

Die Neutral-Atom-Technologie bietet den Vorteil, dass neutrale Atome im Vergleich zu geladenen Ionen weniger anfällig für Störungen sind. Allerdings erfordert die effektive Kontrolle der neutralen Atome technische Raffinesse und sehr niedrige Temperaturen.

Neutral-Atom-QPUs verwenden Rubidium-Atome als Qubits. Laser dienen als „optische Pinzetten“, um einzelne Atome einzufangen und bei nahezu absoluter Kälte zu stabilisieren. Optische „Gitter“, die in Bild 11 dargestellt sind, verwenden Laser, welche Rubidium-Atome (rot) voneinander trennen, um sie als Informationseinheiten in Neutral-Atom-Quantenprozessoren zu verwenden.

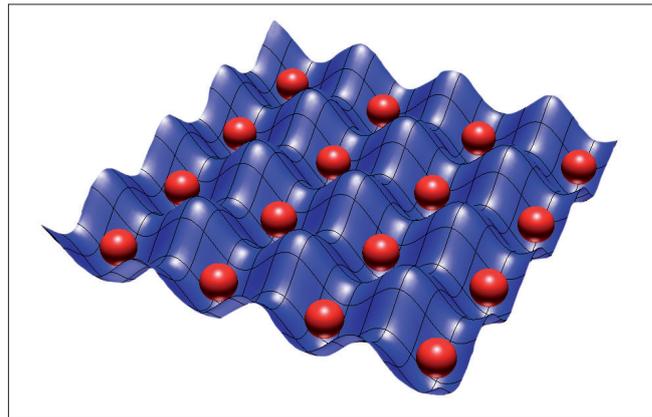
Die Rydberg-Blockade [35] ermöglicht die Implementierung von Multi-Qubit-Gates und verringert Fehler. Mit Rydberg-Wechselwirkungen können hochwertige Multi-Qubit-Gates realisiert werden. Die Technologie ermöglicht es, Qubits effizient zu manipulieren und in verschiedenen Modi zu arbeiten. Diese QPUs unterstützen analoge und digitale beziehungsweise hybride Berechnungsmodi. Der digitale Modus ermöglicht universelle Funktionalität, während der analoge Modus direkt zu Antworten führt und weniger anfällig für Fehler ist.

Die flexible Anordnung von Qubits erlaubt rekonfigurierbare Layouts und eine hohe Skalierbarkeit. Die QPUs mit neutralen Atomen erreichen eine nicht simulierbare Phase, die klassische Supercomputer übertrifft, wie zum Beispiel „Aquila“ – eine 256-Qubit-Neutral-Atom-QPU von Quera [22]. Diese Technologie zeichnet sich durch Robustheit gegenüber Fehlern und effiziente Kontrolle aus.

Die Modulbauweise des Neutral-Atom-Prozessors ermöglicht die Integration verschiedener Funktionalitäten wie digitale Quantengatter, Fehlerkorrektur, Speicher und Verarbeitungszonen. Dies bewirkt Flexibilität und Anpassungsfähigkeit an verschiedene Problemstellungen. Zudem erlaubt die hohe Skalierbarkeit die Erhöhung der Qubit-Zahl.

Durch das gezielte Anregen der Atome zu Rydberg-Zuständen [36] (hoch angeregte Zustände, bei denen ein oder mehrere Elektronen sich in energetisch weit entfernten Bahnen vom Atomkern bewegen) können die Elektronenwolken der Atome vergrößert werden. In diesem Zustand können verschiedene Atome über große Entfernungen miteinander interagieren, was den Quanteninformationstransfer ermöglicht. Dies führt zur Entstehung von Quantenverschränkung, einer Schlüsselkomponente für die Manipulation von Quanteninformation.

Die Anwendungsmöglichkeiten für Neutral-Atom-QPUs sind vielfältig. Dazu zählen die Simulation quantenmechanischer Systeme, Optimierungsalgorithmen, maschinelles Lernen und viele mehr. Die Flexibilität in der Anordnung der



Qubits als neutrale Atome im optischen „Gitter“ (Bild 11)

Qubits erlaubt es, die Konnektivität nach Bedarf anzupassen.

Die Kombination aus Robustheit, Skalierbarkeit, Flexibilität und verschiedenen Betriebsmodi positioniert die Neutral-Atom-QPU-Technologie als vielversprechende Plattform für zukünftige Quantenberechnungen. Firmen wie Quera und Pasqual haben schon Neutral-Atom-QPUs hergestellt – es stehen bereits erste Generationen von Queras 256-Qubit-Quantenprozessor Aquila [31] und von Pasquals 100-Qubit-Quantensystem (bald 200 Qubit) via Cloud zur Verfügung, und für die Zukunft wird die noch höhere Marke von 1000 Qubits angepeilt.

Aufstrebende QPU-Archetypen

Die in drei den vorigen Abschnitten vorgestellten QPU-Archetypen repräsentieren am meisten verbreitete und bereits via Cloud zur Verfügung stehende Quantenprozessoren – Superconducting-, „Trapped Ion“- und Neutral-Atom-QPUs. Es gibt jedoch noch weitere aufstrebende und vielversprechende Quantentechnologien, die einen kurzen Überblick verdienen, um den Gesamtblick über die ganze technologische Landschaft der Quantenprozessoren abzurunden:

- **Quantum Dot** oder **Spin Qubit QPU**: Ein Schlüsselement dabei sind Quantum-Dot-Qubits, kleine Halbleitervorrichtungen, die ein einzelnes Elektron einfangen können [37]. Der Spin des Elektrons wird als Qubit genutzt und durch ein Magnetfeld gesteuert. Die hohe Skalierbarkeit von Quantum Dots ermöglicht die Bildung von Qubit-Arrays, wobei jedes Dot unabhängig gesteuert werden kann. Trotz vielversprechender Aspekte müssen noch Herausforderungen wie die Aufrechterhaltung der Qubit-Kohärenz überwunden werden. Intel bietet bereits seine 12-Qubit-QPU „Tunnel Falls“ [38] zu Forschungszwecken für Universitäten und Forschungslabore an.
- **Photonics QPU**: Diese QPUs verwenden Photonen als Quantenbits (Qubits) und speichern Informationen in Form von Lichtquanten. Der Ansatz basiert auf der Quanteninformation von Photonen, wobei Quantenverschränkung und Superposition durch die Manipulation der Eigenschaften von Lichtteilchen erreicht werden. Die Vorteile umfassen schnelle Datenverarbeitung und geringe Anfälligkeit für Störeinflüsse. Allerdings können einige Herausforde- ▶

rungen wie zum Beispiel die Photonen-Wechselwirkung und der Bedarf an hochentwickelten Photonenquellen und hochpräzisen Detektoren die Marktreife der brauchbaren photonischen Quantencomputer noch in die fernere Zukunft verschieben. Einige Firmen und Forschungseinrichtungen haben markante Erfolge mit photonischen QPUs erzielt – die kanadische Firma Xanadu etwa bietet bereits Lösungen mit ihren X-Series-Photonic-Quantencomputern an, das französische Unternehmen Quandella positioniert sich als erster europäischer Cloud-Anbieter für Quantencomputing [39], und schließlich hat die Chinesische Universität für Technologie und Wissenschaft (USTC) mit ihrem Photonic-Quantencomputer „Jiuzhang“ im Dezember 2020 die Quantenüberlegenheit und den Titel „mächtigster Quantencomputer der Welt“ für sich beansprucht [33].

Die bisher hier vorgestellten QPU-Archetyphen – Superconducting, „Trapped Ions“, Neutral-Atom, Quantum-Dot und Photonic – spiegeln weitverbreitete und etablierte beziehungsweise vielversprechende Lösungen wider. Es gibt aber noch viele weitere aufstrebende Ansätze, die eines Tages zu einem Durchbruch führen könnten. Interessierte Leser finden in [40] entsprechende Verweise.

Fazit

Die Cloud ist die beste und sehr häufig die einzig mögliche beziehungsweise tragbare Option für den Zugriff auf einen Quantencomputer. Durch die Auslagerung von Quantum-Computing-Ressourcen in die Cloud können Unternehmen und Forschungseinrichtungen auf leistungsstarke Quantencomputer zugreifen, ohne in eigene teure Hardware und Software investieren zu müssen. Dies eröffnet eine neue Ära der Zusammenarbeit und Innovation, indem es selbst kleinen Unternehmen und Forschungsteams Zugang zur Quantenrechenleistung ermöglicht.

Die Cloud wird zu einem zentralen Ort für Quantum-Computing-Ressourcen, der es Nutzern ermöglicht, komplexe Quantenalgorithmen auszuführen, und innovative Anwendungen zu entwickeln. Die Integration von Quantum-Computer- und Cloud-Provider schafft eine flexiblere und skalierbare Umgebung für Quantum Computing, die es jedem ermöglicht, sich auf Anwendungen mit Quantum-Algorithmen zu konzentrieren, ohne sich um die Komplexität der zugrundeliegenden Hardware kümmern zu müssen.

Insgesamt wird Quantum Computing in der Cloud nicht nur den Zugang zu leistungsstarken Rechenressourcen revolutionieren, sondern auch die Art und Weise, wie man Probleme angeht und Lösungen entwickelt. Dieser symbiotische Ansatz zwischen Quantum Computing und Cloud-Technologien verspricht nicht nur Effizienzsteigerungen, sondern könnte auch zu Durchbrüchen in Bereichen wie künstlicher Intelligenz, Verschlüsselung und Simulation führen. Der Weg in die Zukunft der Informationstechnologie wird nun nicht zuletzt durch die Konvergenz von Quantum Computing und Cloud-Computing-Ressourcen geebnet.

Etablierte Cloud-Plattformen wie Azure Quantum [41], Amazon Braket [42], IBM Quantum [43] und Google Quantum

AI [44] sowie ganze Reihe weiterer noch aufstrebender Unternehmen bieten bereits Quantum-Computing-Zugänge über die Cloud – sowohl für Simulatoren als auch zu den „echten“ Quantencomputern. Damit bieten sie für Entwicklerinnen und Entwickler bereits heute Einstiegspunkte, an denen mit modernen Programmiersprachen wie Python und Q# und mit Frameworks beziehungsweise SDKs wie zum Beispiel Microsoft QDK und Amazon Braket SDK das Eintauchen in die faszinierende Welt der Quantenprogrammierung auf Haupt-Cloudplattformen möglich gemacht wird. ■

- [1] Dirac-Notation bei Wikipedia, www.dotnetpro.de/SL2502QuantumCloud1
- [2] „Schrödingers Katze“ bei Wikipedia, www.dotnetpro.de/SL2502QuantumCloud2
- [3] Go-Spiel bei Wikipedia, www.dotnetpro.de/SL2502QuantumCloud3
- [4] Dekohärenz bei Wikipedia, www.dotnetpro.de/SL2502QuantumCloud4
- [5] Quantenschlüsselaustausch bei Wikipedia, www.dotnetpro.de/SL2502QuantumCloud5
- [6] Quantenteleportation bei Wikipedia, www.dotnetpro.de/SL2502QuantumCloud6
- [7] Azure-Quantum-Dokumentation, Grover-Algorithmus, www.dotnetpro.de/SL2502QuantumCloud7
- [8] QFT – Quanten-Fouriertransformation bei Wikipedia, www.dotnetpro.de/SL2502QuantumCloud8
- [9] Qutrit bei Wikipedia, www.dotnetpro.de/SL2502QuantumCloud9
- [10] N. Lossau, Von Qubits zu Qudits, Welt.de, www.dotnetpro.de/SL2502QuantumCloud10
- [11] Quantum circuit bei Wikipedia, www.dotnetpro.de/SL2502QuantumCloud11
- [12] Quantengatter bei Wikipedia, www.dotnetpro.de/SL2502QuantumCloud12
- [13] Shor's algorithm bei Wikipedia, www.dotnetpro.de/SL2502QuantumCloud13
- [14] Adiabatic Quantum Computation bei Wikipedia, www.dotnetpro.de/SL2502QuantumCloud14
- [15] Quantum annealing bei Wikipedia, www.dotnetpro.de/SL2502QuantumCloud15
- [16] Problem des Handlungsreisenden bei Wikipedia, www.dotnetpro.de/SL2502QuantumCloud16
- [17] Maximaler-Schnitt-Problem bei Wikipedia, www.dotnetpro.de/SL2502QuantumCloud17
- [18] D-Wave Systems bei Wikipedia, www.dotnetpro.de/SL2502QuantumCloud18
- [19] Leap – D-Wave Quantum Cloud-Service, www.dotnetpro.de/SL2502QuantumCloud19
- [20] Olivier Pfister, Continuous-variable quantum computing in the quantum optical frequency comb, 2020 J. Phys. B: At. Mol. Opt. Phys. 53 012001, www.dotnetpro.de/SL2502QuantumCloud20
- [21] Quera.com, What is analog quantum computing?, www.dotnetpro.de/SL2502QuantumCloud21
- [22] Quera.com, 256-qubit quantum Computer Aquila, <https://www.quera.com/aquila>

- [23] Anyon bei Wikipedia,
www.dotnetpro.de/SL2502QuantumCloud22
- [24] Welllinie bei Wikipedia,
www.dotnetpro.de/SL2502QuantumCloud23
- [25] Braid group bei Wikipedia,
www.dotnetpro.de/SL2502QuantumCloud24
- [26] Azure Quantum, Topological qubits,
www.dotnetpro.de/SL2502QuantumCloud25
- [27] nLab.org, Topological Quantum Computation.
www.dotnetpro.de/SL2502QuantumCloud26
- [28] arXiv.org, E.C. Rowell, Z. Wang, Mathematics of Topological Quantum Computer,
<https://arxiv.org/pdf/1705.06206.pdf>
- [29] One-way Quantum-Computer bei Wikipedia,
www.dotnetpro.de/SL2502QuantumCloud27
- [30] arXiv.org, Geometric and holonomic quantum computation. <https://arxiv.org/abs/2110.03602>
- [31] Nvidia.com, R. Merrit, What is a QPU,
www.dotnetpro.de/SL2502QuantumCloud28
- [32] Superconducting quantum computing bei Wikipedia,
www.dotnetpro.de/SL2502QuantumCloud29
- [33] Quantenüberlegenheit,
www.dotnetpro.de/SL2502QuantumCloud30
- [34] J.Hui. How to build a Quantum Computer with Trapped Ions, www.dotnetpro.de/SL2502QuantumCloud31
- [35] Quera.com, Rydberg-Blockade,
www.dotnetpro.de/SL2502QuantumCloud32

- [36] Rydberg-Zustand bei Wikipedia,
www.dotnetpro.de/SL2502QuantumCloud33
- [37] Spin qubit quantum computer bei Wikipedia,
www.dotnetpro.de/SL2502QuantumCloud34
- [38] Intel.com, Intel's New Chip to Advance Silicon Spin Qubit Research for Quantum Computing,
www.dotnetpro.de/SL2502QuantumCloud35
- [39] Quandela Cloud, <https://cloud.quandela.com/>
- [40] List of proposed Quantum registers bei Wikipedia,
www.dotnetpro.de/SL2502QuantumCloud36
- [41] Microsoft Learn, Azure Quantum,
www.dotnetpro.de/SL2502QuantumCloud37
- [42] Amazon Braket,
www.dotnetpro.de/SL2502QuantumCloud38
- [43] IBM Quantum, <https://quantum.ibm.com/>
- [44] Google Quantum AI, <https://quantumai.google>



Mykola Dobrochynskyy

ist Senior Architekt bei der Porsche AG. Seine Schwerpunkte sind Softwarearchitektur, modellgetriebene Softwareentwicklung, generative Programmierung, KI sowie Cloud- und dienstorientierte Softwarearchitekturen.
www.xing.com/profile/Mykola_Dobrochynskyy

dnpCode

A2502QuantumCloud

DEV ACADEMY

HANDS-ON-WORKSHOPS UND
WEITERBILDUNG FÜR SOFTWARE-
ENTWICKLER UND -ARCHITEKTEN



2 TAGE
REMOTE/INHOUSE

Erste Schritte mit Docker für .NET-Entwickler

TRAINING!

Was wird behandelt

- Einführung in Docker
- Source-Code mit Container verwenden
- Images erstellen und bereitstellen
- Container-Kommunikation und Management
- Docker-Compose in Aktion
- Security
- Monitoring



Gregor
Biswanger
Trainer